

PROPOSED FRAMEWORK FOR DIGITAL VIDEO AUTHENTICATION

by

GREGORY SCOTT WALES

A.S., Community College of the Air Force, 1990

B.S., Champlain College, 2012

M.S., Champlain College, 2015

A thesis submitted to the
Faculty of the Graduate School of the
University of Colorado in partial fulfillment
of the requirements for the degree of
Master of Science
Recording Arts
2019

© 2019

GREGORY SCOTT WALES

ALL RIGHTS RESERVED

This thesis for the Master of Science degree by

Gregory Scott Wales

has been approved for the

Recording Arts Program

by

Catalin Grigoras, Chair

Jeffrey M. Smith

Marcus Rogers

Date: May 18, 2019

Wales, Gregory Scott (M.S., Recording Arts Program)

Proposed Framework for Digital Video Authentication

Thesis directed by Associate Professor Catalin Grigoras.

ABSTRACT

One simply has to look at news outlets or social media to see our society video records events from births to deaths and everything in between. A trial court's acceptance of videos supporting administrative hearings, civil litigation, and criminal cases is based on a foundation that the videos offered into evidence are authentic; however, technological advancements in video editing capabilities provide an easy method to edit digital videos. The proposed framework offers a structured approach to evaluate and incorporate methods, existing and new, that come from scientific research and publication. The thesis offers a quick overview of digital video file creation chain (including factors that influence the final file), general description of the digital video file container, and description of camera sensor noises. The thesis addresses the overall development and proposed use of the framework, previous research of analysis methods / techniques, testing of the methods / techniques, and an overview of the testing results. The framework provides the forensic examiner a structured approach to subjecting the questioned video file to a series of smaller tests while using previously published and forensic community recognized methods / techniques. The proposed framework also has a proposed workflow optimization option for use by management in an effort to manage resources and personnel.

The form and content of this abstract are approved. I recommend its publication.

Approved: Catalin Grigoras

DEDICATION

I dedicate this paper to God and family. To God I thank for guidance, strength, power of mind, making me a lifelong learner, and for giving me so many blessings that frequently comes out of adversity.

I also dedicate this paper to my wife Maricon and my son Scott. My wife has encouraged me for over 36 years of marriage with her firm belief in the value of education. Thank you for giving me the strength when I thought of giving up during times of difficulty, and continually providing moral, spiritual, and emotional support at all times. My son challenged me to be a positive role model who responds to hardships and misfortune by using these things as challenges to improve myself.

ACKNOWLEDGEMENTS

I would like to express my appreciation to Dr. Catalin Grigoras and Jeff Smith for their continued support in my study of multimedia forensics and their continued encouragement to contribute to our scientific community. I also want to express my gratitude to both for their continued support and efforts to help law enforcement when we need help in our investigations that involve multimedia. I wish to thank Dr. Marcus Rogers, the other member of my thesis committee, for challenging me in this project and especially during my thesis defense.

I want to express my gratitude to an unsung hero in my pursuit of the degree at UC Denver and especially completing my thesis research paper, Leah Haloin. You keep us on-track with our milestones and deliverables, but you also go the extra mile in your editing role to help us produce papers that meet the school's standards. You obviously care about the graduate students.

I also want to thank Cole Whitecotton for your IT support when I visit the National Center for Media Forensics (NCMF). And I want to thank my cohort classmates and the other cohorts who provided invaluable assistance and contributions to this paper.

I want to thank Steven Futrowsky for your feedback on Chapter I and II. I also want to thank Gregory Scott Wales Jr. for your feedback on Chapter I. My thanks to Jesus Valenzuela and Gretchel Lomboy, Forensic Digital Imaging Section, Seattle Police Department for providing a couple of videos for a case study included in this paper. Thank you to previous NCMF researchers and others researchers in the forensic community whose scientific research I used to contribute to my paper.

TABLE OF CONTENTS

CHAPTER

I.	INTRODUCTION	1
	Public Perception	2
	Forensic Science	2
	Forensic Video Enhancement or Manipulation	4
	Video Manipulation Example	4
	Forensic Audio Enhancement or Manipulation	6
	Challenges	6
	Challenge From Artificial Intelligence	7
	Challenge From Different Types of Video Recorders	9
	Challenge From Mobile Devices	9
	Challenge From Advances In Technology & New CODECs	10
	Scope	11
II.	LEGAL CONSIDERATIONS OF AUTHENTICATION	14
	Legal Aspects For Use In Proposed Framework	14
	Scientific Method	15
	Criteria Used To Assess Techniques	15
	Expert Testimony Approach Using Proposed Framework	18
III.	LIGHT TO DIGITAL VIDEO FILE	20
	Video Creation Chain	20

Audio Stream Creation Chain	21
Video Stream Creation Chain	21
Influences on Audio Stream During Creation	21
Influences on Video Stream During Creation	22
Combined Audio & Video Creation Chain With Influences	23
Digital Multimedia File	23
Sensor Noises	24
CMOS Sensor	24
CCD Sensor	26
Overview of Sensor Noise Types	27
IV. PROPOSED FRAMEWORK	30
File Structure Analysis	30
Workflow Optimization	31
File Preparation For Audio & Video Stream Analysis	32
Audio Authentication	32
Video Authentication	32
Device Identification / Verification	32
V. FRAMEWORK JUSTIFICATION – RESEARCH, TESTING, & RESULTS	34
Framework Development & Use	34

Analysis Questions	34
Digital Multimedia File	35
Tools For Video Authentication Toolbox	39
Research For Analysis Tools	40
File Structure Analysis Techniques	41
Audio Stream(s) & Video Stream(s) Bifurcated Approach	44
Audio Authentication Analysis Tools	44
Video Authentication Analysis Tools	45
Testing of Methods & Proposed Framework	57
Adding New Method To Video Authentication Toolbox - Case	
Study 1	57
Clone Alteration Test Videos – Case Study 2	58
Axon Fleet 2 Camera Video – Case Study 3	64
Proposed Framework Overall Test Results	70
VI. CONCLUSION	71
REFERENCES	72
APPENDIX	
A. ADDITIONAL LEGAL INFORMATION	79
B. SCIENTIFIC METHOD	93
C. DIGITAL VIDEO AUTHENTICATION FRAMEWORK WORKFLOW	

ANALYSIS FORM	94
D. CASE STUDY 1	98
E. CASE STUDY 2	134
F. CASE STUDY 3	163

LIST OF TABLES

TABLE

1	CMOS Sensor Noise Types	25
2	CCD Sensor Noise Types	26
3	File Structure Analysis Authentication Method / Technique Relevance	43
4	Audio Stream Authentication Methods / Techniques Relevance	44
5	Clone / Duplicate Frame Detection Analysis Authentication Method / Technique Relevance	46
6	Directional Lighting Inconsistency Detection Analysis Authentication Method / Technique Relevance	47
7	Local (Spatio-Temporal) Tampering Detection Analysis Authentication Method / Technique Relevance	47
8	Interlaced & Deinterlaced Video Inconsistency Detection Analysis Authentication Method / Technique Relevance	49
9	MPEG Double Compression Detection Analysis Authentication Method / Technique Relevance	50
10	Color Filter Array Analysis Authentication Method / Technique Relevance ...	52
11	Source Video Camera Identification Using PRNU Detection Method For Authentication Relevance	53
12	Source Camera Successful Identification Rates Using Different Interpolations & Dimensions	54

13	Source Camera Identification Rates	55
14	G-PRNU & Image Resize For Camera Identification Detection	
	Method For Authentication Relevance	55
15	Block Level Manipulation Detection Method For Authentication	
	Relevance	56
16	2D Phase Congruency CC Detection Method For Authentication	
	Relevance	56
17	Test Results For Method Validation	100
18	Planned Test Scenarios	103
19	Original Audio Stream Hash Listing	117
20	Original Video Stream Hash Listing	120
21	Validation Test Comparison Of Original Versus Copied Audio Stream	
	Hashes	125
22	Validation Test Comparison Of Original Versus Copied Video Stream	
	Hashes	130
23	Test Results	134
24	Test Video Tampering Method	136
25	Planned Test Scenarios	137

LIST OF FIGURES

FIGURE

1	Selected Frames From “Extreme Crosswind Airliner Spins 360”	
	YouTube Video	5
2	Frame 1 of Deepfake YouTube Video	8
3	Person 1 Body, Hair, Ears, & Face Combined With Person 2 Face	
	Used To Create Deepfake Video	8
4	Final Video Creation Chain With Influence Factors	20
5	Example of Digital Multimedia File Using Book Analogy	23
6	General Block Diagram of CMOS Sensor Noise Model	25
7	General Block Diagram of CCD Sensor Noise Model	26
8	Proposed Video Authentication Framework	30
9	Workflow Optimization Based On File Structure Analysis	31
10	Framework Development General Areas of Analysis	36
11	Case Study 2 Test 1 Test Validation Results	60
12	Case Study 2 Test 2 Test Validation Results	61
13	Case Study 2 Test 3 Test Validation Results	62
14	Case Study 2 Test 4 Test Validation Results	63
15	Temporal Analysis of Y Plane Revealing Current Frame Versus Preceding	
	Frame Differences	65

16	Comparison of Frame 598, 599, & 600 Visual Content Using Temporal Difference Filter	66
17	2D Phase Congruency With Correlation Coefficient of Adjacent Frames	66
18	Temporal Analysis of Y Plane Revealing Current Frame Versus Preceding Frame Differences	67
19	Comparison of Frame 1074 & 1075 Visual Content	68
20	2D Phase Congruency With Correlation Coefficient of Adjacent Frames	69
21	Diagram of Scientific Method Used In Proposed Framework	93

LIST OF ABBREVIATIONS

Abbreviations	Explanations
<i>AAFS</i>	American Academy of Forensic Sciences
<i>ADC</i>	Analog to Digital Converter
<i>AES</i>	Audio Engineering Society
<i>AI</i>	Artificial Intelligence
<i>ASTM</i>	American Society for Testing and Materials
<i>CC</i>	Correlation Coefficient
<i>CCD</i>	Charge Coupled Device
<i>CODECs</i>	Coder-Decoders
<i>CFA</i>	Color Filter Array
<i>CGI</i>	Computer-Generated Imagery
<i>CMOS</i>	Complementary Metal-Oxide-Semiconductor
<i>CYGM</i>	Cyan, Yellow, Green, & Magenta
<i>DAP</i>	Digital Audio Processing
<i>DC</i>	Direct Current
<i>DCT</i>	Discrete Cosine Transform
<i>DFRWS</i>	Digital Forensic Research Workshop
<i>DFT</i>	Discrete Fourier Transform
<i>DVP</i>	Digital Video Processing
<i>ENF</i>	Electronic Network Frequency

<i>ESI</i>	Electronically Stored Information
<i>FPN</i>	Fixed Pattern Noise
<i>FRE</i>	Federal Rules of Evidence
<i>HEIF</i>	High Efficiency Image File
<i>HEVC</i>	High Efficiency Video Coding
<i>ICC</i>	International Criminal Court
<i>IR</i>	Infrared
<i>JFS</i>	Journal of Forensic Sciences
<i>JDI</i>	Journal of Digital Investigation
<i>JPG / JPEG</i>	Joint Photographic Expert Group
<i>MMS</i>	Multimedia Message Systems
<i>NCMF</i>	National Center for Media Forensics
<i>PCM</i>	Pulse-Code Modulation
<i>PRNU</i>	Photo Response Non-Uniformity
<i>G-PRNU</i>	Green Photo Response Non-Uniformity
<i>RGBE</i>	Red Green Blue Emerald
<i>SWGDE</i>	Scientific Working Group on Digital Evidence
<i>VFX</i>	Visual Effects

CHAPTER I

INTRODUCTION

Our society has become obsessed with recording videos of anything and almost everything that happens in their lives. One simply has to look at news outlets or social media to see people video record events from births to deaths and everything between. News outlets and social media websites encourage our society to provide them with videos of news worthy events for further dissemination through their respective venues.

Terrorist elements in our society record and post videos of violent acts involving beheadings and suicide bombings. Criminals record sexual assaults, child exploitation, kidnapping, aggravated assaults, armed robberies, arsons, and murders on videos. Some criminals seek their “five minutes of fame” by posting the videos or broadcasting them live on the Internet for the world to see.

Witness testimony is frequently less than perfect; however, our society has learned to be better witnesses by using video recordings of a crime to help recall events and better illustrate what they observed. Law enforcement agencies have seen a significant increase over the last few years in the reporting of criminal activity along with a video recording of the crime to support witness testimony. Witnesses have provided videos of almost every type of crime.

Video recording of contentious events have also increased in non-criminal matters. Videos supporting civil litigation have become in vogue. A party, or witness in, litigation may have recorded an event that is the heart of the litigation. Videos may be offered in personal injury, breach of contract, family law, property disputes, and landlord and tenant disputes.

A trial court’s acceptance of videos supporting administrative hearings, civil litigation, and criminal cases is based on a foundation that the videos offered into evidence in court are

authentic; however, technological advances in video editing capabilities provide an easy method to edit digital videos.

Public Perception

The average person tends to believe much of what they see in movies and television shows regarding crime scene investigation and the ability of forensics to solve a crime within five minutes or less. Frequently, the science presented to the audience is inaccurate and the time to conduct forensic analysis is unrealistic. Many people believe that these things are possible because they see it in a video form. What many people do not understand is that videos may be edited or altered to manipulate the content of what the viewer observes similar to still images that are “photoshopped” to manipulate the viewers perspective. The authenticity of a digital video recording offered into evidence can be problematic if the video is offered as an original and someone, judge or jury, must make a decision based on that video without authenticity being proven.

Forensic Science

Forensic science is generally defined as the use of scientific methodology to answer questions of relevance for the legal system while meeting legal requirements for the answers and the evidence to be accepted into a legal system. Our society needs impartial forensic scientists to analyze physical and digital evidence and help solve crimes and other wrongs.

Anyone who has watched crime dramas on television or the movies understands a key point made by criminalist Richard Saferstein (2007) who noted that physical evidence establishes a crime has been committed and provides a link between the crime, its victims, and those who perpetrated the crime [1]. Digital Forensic Researcher Eoghan Casey (2000) expanded the physical evidence concept and advocated that digital evidence also establishes that a crime has

been committed, can provide a link between a crime and its victim, or can provide a link between a crime and the perpetrator [2].

Physical evidence and digital evidence have similarities and differences. Both digital and physical evidence have the same legal requirements for introduction into the U.S. court system. Two of the digital and physical evidence similarities are that the evidence must be relevant and authentic. Rule 401 of the Federal Rules of Evidence (FRE) (Test for Relevant Evidence), is (a) has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action [3]. Additionally, FRE Rule 901 (Authenticating or Identifying Evidence) stated that the test for authentication follows a general rule that the party offering the evidence “must produce evidence sufficient to support a finding that the item is what the proponent claims it is” [4].

The differences between digital and physical evidence are based upon the substance or materials that make up the evidence. Physical evidence may take the form of blood, saliva, tissue, fire arms, bullets, tools, marks, prints, or any other substance that has been collected. Digital evidence presents its own challenge to authentication in that it can be much more volatile and may be constantly changing in content if a single computer or series of computers are powered on. Digital evidence may be:

- Easy to alter without any trace of the alteration.
- Encrypted, encoded, or in a digital format that may not be easy to view or read.
- Easy to duplicate.
- Stored in multiple locations or across multiple storage devices.

Forensic Video Enhancement or Manipulation

The Scientific Working Group on Digital Evidence (SWGDE) defines video enhancement as “any process intended to improve the visual appearance of video sequences or specific features within video sequences” [5]. Video enhancement is usually associated with forensic concepts of accuracy and precision, repeatability by the same examiner, and the ability of other equally qualified examiners to reproduce the same results. The average person does not usually conduct video enhancement with the exception of improving the visual appearance of a video. These enhancements may take the form of rotation, stabilizing a movie because of the videographer’s shaking hand, sharpening, adjusting lighting, adjusting contrast, and other techniques. These changes alter the video but are not necessarily accomplished with the intent to influence the viewer perceptions.

Video manipulation on the other hand may involve frame deletions and insertions, copy and paste inside a frame (intra-frame), copy and paste to another frame (inter-frame), and content aware (removing objects and / or people) and with the intent to change the meaning of events or manipulate the viewer’s perspective. Additionally, not all video frame deletions have negative implications. Video montages summarizing a trial, Congressional hearing, or other lengthy event presented by news outlets with the intent to present the viewer with an unbiased summary of key events is not necessarily manipulative.

Video Manipulation Example

Video manipulation is no longer reserved for Hollywood or advanced computer users. The Internet provides low cost and open source computer-generated imagery (CGI) and visual effects (VFX) software to create and manipulate video. There are websites with extensive open-source CGI and VFX training that will allow the average computer user to create or manipulate

videos to influence viewers. The public has seen a significant increase in “fake” videos that influence people from all corners of our society.

Washington Post Technology Columnist Geoffrey Fowler (2018) wrote a column titled “I fell for Facebook fake news. Here's why millions of you did, too” [6]. In that column, Fowler discussed a Facebook video he received in his news feed that was linked to YouTube. The YouTube video was titled “Extreme Crosswind | Airliner Spins 360” [7]. As Fowler noted he and millions of others believed the video of an airliner spinning 360 degrees just prior to landing was real. Fowler researched the video’s origin and discovered the video was part real video and part CGI. He talked to a Hollywood film director who told him that in 2017, he created a YouTube video using CGI that showed an airplane doing a 360 degree spin that was used in the YouTube video he referenced. According to Fowler, miscreants combined the film director’s CGI video with real video of a plane landing and then published the video as fake news [6]. The fake news video spread across the Internet and social media, influencing many people to believe that an actual airliner conducted a 360 degree spin as it was landing. Fowler reported in his column that the video had been viewed on Facebook almost 14 million times [6]. Figure 1 below contains selected frames from the YouTube video titled “Extreme Crosswind | Airliner Spins 360.”



Figure 1 - Selected Frames From “Extreme Crosswind | Airliner Spins 360” YouTube Video [7]

This video and the frames noted in Figure 1 are indicative of why videos offered as evidence in civil litigation or criminal prosecution should be authenticated using sound forensic science.

The video manipulation example above illustrates a major effort to influence the viewers' perception; however, manipulation may simply involve the addition or deletion of an object in a few frames or the cropping of a video to exclude an object or person along one edge of a video.

Forensic Audio Enhancement or Manipulation

Video frequently contains an audio stream that supports the visual contents of a video. SWGDE defines audio enhancement as “processing of recordings for the purpose of increased intelligibility, attenuation of noise, improvement of understanding the recorded material and/or improvement of quality or ease of hearing” [5]. Similar to video enhancement, audio enhancement is usually associated with forensic concepts of accuracy and precision, repeatability by the same examiner, and the ability of other equally qualified examiners to reproduce the same results. The average person does not usually conduct audio enhancement except for improving what they hear. The enhancements may involve removing background sounds, clicks or pops, and other techniques. These changes alter the overall audio, but are not necessarily accomplished with the intent to influence the listener's perceptions.

Audio manipulation on the other hand may involve audio snippet deletions or copying and moving segments of conversations into positions that change the meaning of speaker's conversation or manipulate the perception of the listener. Not all audio segment deletions have negative implications. Audio montages summarizing a trial, Congressional hearing, or other lengthy event presented by news outlets with the intent to present a listener with an unbiased summary of key events is not necessarily manipulative.

Challenges

Forensic video examiners who conduct video authentication face many challenges today and in the future. These challenges include multiple types of video recording systems with

various operating systems and video storage locations, increased availability and usability of video editing software, multiple video coder-decoders (codecs), and continuous advances in technology that directly impact video authentication process.

Challenge From Artificial Intelligence

In 2017, researchers in Artificial Intelligence (AI) successfully used open source software and a computer with a basic gaming video card to conduct machine deep learning on input data and then used two input data sources to transfer select portions of one data set to another data set to create a fake video in a process called “deepfake.” The first data set included celebrity faces from digital photos and videos publicly available on the Internet. The second data set contained pornographic videos. The researchers repeatedly transferred celebrity faces onto the pornographic videos and posted them to the Internet for public display of their work.

Shortly after this technological breakthrough, an Internet website appeared that aided the novice in producing pornographic videos using a celebrity’s face and the faces of other innocent people using the same methodology. The impact of this advancement means that it has become easier to manipulate videos, for malicious purposes without the need for high end computers and CGI or VFX software. A well-informed computer user now only needs a computer and the knowledge of a publicly available website tailored to this process to edit a video for nefarious purposes.

An example of a non-pornographic deepfake video is offered in Figure 2 below.



Figure 2 - Frame 1 of Deepfake YouTube Video [8]

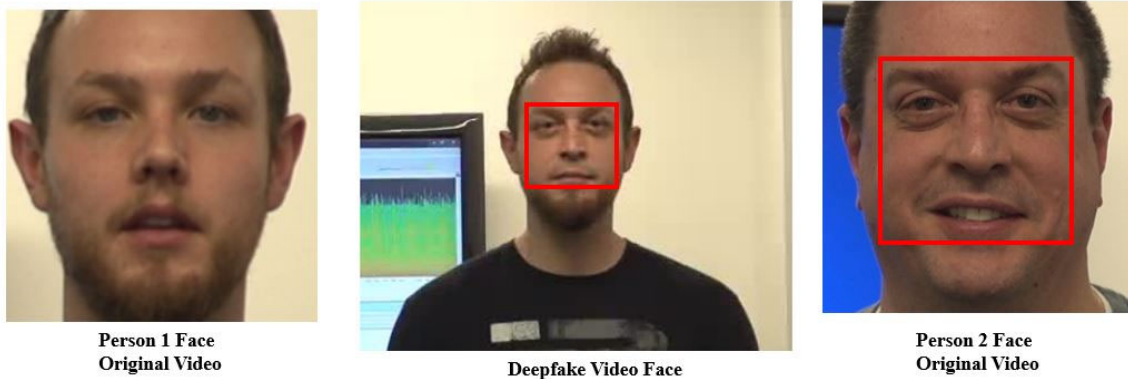


Figure 3 - Person 1 Body, Hair, Ears, & Face Combined With Person 2 Face Used To Create Deepfake Video [8]

The video frame above contains a compilation of two people. The deepfake video persona in Figure 2 and Figure 3 middle picture was created with Person 1's video and retaining their body, hair (including part of the facial hair), and voice in the deepfake video. Person 2's face was inserted, in part, into the deepfake video persona. Note the red box area on both Person 2 and deepfake video face in Figure 3 above. The contents of the red box area on Person 2 illustrates the impact of AI in video manipulation. The deepfake video persona is completely different than

either Person 1 or Person 2. Authenticating deepfake videos will present unique challenges to detect what is altered in the original video.

Challenge From Different Types of Video Recorders

Digital video recorders exist in a multitude of different shapes, sizes, manufactures, operating systems, and configurations. Some devices provide the forensic video examiner distinctive metadata for use in video authentication. The same make and model of video recorder may contain optional settings and configurations that are available to the user. These options may overlay a title or clock on a video or present an option to include or eliminate metadata in a video file upon export. These are just a few examples video recorders present as challenges in video authentication.

Challenge From Mobile Devices

Along with the ability of mobile devices to record videos, those who use mobile phones to record videos have the ability to easily edit the video with pre-loaded basic or third-party software applications while the video is on the mobile device. Mobile phone manufacturers have made it easy to synchronize mobile devices with computers to allow the user to have access to robust video editing and enhancement software. Mobile devices have become the preferred method of communications in the 21st Century. Videos or links to download videos are transferred between computers and mobile devices in Multimedia Message Systems (MMS), iPhone Messages and emails. These communications present the challenge that a video located on a mobile device may not have been created with the camera on the device containing the video. An example in actual casework involved a video of criminal activity transferred from a Motorola phone to an iPhone when the witness purchased the new iPhone and the provider transferred data to the new device from the Motorola phone. The video of interest, created on

the Motorola phone, was accessible on the new iPhone by the user to show investigators, but the video was not stored in the normal camera folder when collected using mobile forensic processing tools. The video was stored in the iPhone file system consistent with other images and videos received from outside the phone's camera system.

Challenge From Advances In Technology & New CODECs

Apple introduced Live Photo in early 2016 in its iPhone 6S and 6S Plus that uses iOS 9 and higher. In 2017, Apple implemented a new image (photograph) file type and video format with a new video codec with the introduction of iOS 11. The new video codec, High Efficiency Video Coding (HEVC), implemented the H.265 video compression standard. The HEVC codec was also available as one of the different codecs for High Efficiency Image File (HEIF) photographs in iOS 11 on iPhone 7 and later devices. Apple also included these in the OSX High Sierra. With those systems, the user has an option to change the settings of the camera and use the older Joint Photographic Experts Group (JPEG) image file format and H.264 video compression for movies or the legacy type multimedia files [9].

Apple devices have Live Photo turned on by default from iPhone 6S and 6S Plus using iOS 9 to the latest devices and iOS 12.1.2 at the time of this paper. Apple described Live Photo in their support website as the camera capturing 1.5 seconds of activity before the photo and 1.5 seconds of activity after the photograph was taken. Apple noted the photograph as the “key photo” and allows the user to change the key photo to any photograph in the approximately 3 seconds of recording [10].

Forensic analysis of an Apple iPhone using Live Photo revealed not only the key photo in both JPEG and HEIC forms, but also a video file with the same file name containing the entire recorded video (a derivative or side car video). The new Apple codecs and derivative videos

present unique challenges. The new codecs are not viewable on Windows computers without downloadable plug-ins that install updated codecs. Many forensic analysis tools at the time of this paper do not support the HEIC and HEVC files.

A video authentication framework is needed that can be adapted to changes in technology, codecs, other challenges noted above, and any challenges in the future. The proposed video authentication framework is offered with modules that may be utilized in a general workflow that facilitates the inclusion of new or updated techniques as technology advances.

Scope

This thesis proposes a framework that incorporates the analysis of the different features of a digital recording into a workflow for digital video authentication that may meet legal expectations for authentication.

The multimedia forensic science community does not have a digital video authentication framework. A framework would need to meet legal expectations for acceptance in court when used by the forensic video examiner in expert testimony. The development of a proposed framework will also need to use video and audio authentication methodology based upon a series of testing techniques / methods that are peer-reviewed and accepted in the multimedia forensic science community.

There are individual techniques / methods from peer-reviewed publications and conferences that are accepted in multimedia forensic science community, but the community does not have a structured process or system that assesses and uses the appropriate methods for inclusion / exclusion in video authentication examinations.

This thesis proposes to research, develop, and test a proposed video authentication framework that is generally reliant on three interrelated areas.

- Framework use (approach) is based upon the general analysis question posed to the forensic video examiner in the employment of the scientific method.
- The decision to include or exclude specific methods, in the video authentication methodology toolbox, to use in the execution of the framework is based upon the digital multimedia file submitted for examination.
- Development of an evaluation tool to test techniques or methods for forensic video examiner to use to validate each proposed technique or method in the methodology toolbox based upon method validation testing and legal assessment of each method.

While acceptance of the proposed framework for video authentication by the courts will always be based upon a case by case basis dependent upon each cases facts, the proposed framework offers a structured approach to assess and use forensic science community accepted video authentication techniques or methods that are evaluated for reproducibility, repeatability, accuracy, and precision while meeting the general legal requirements recognized by courts in the International community, U.S., and many countries around the world.

The proposed digital video authentication framework is not carved in stone as a rigid and low-level step-by-step protocol that must be explicitly followed by a forensic examiner. Instead, this framework is intended to be used as the basic foundation to implement the required scientific methodology using peer reviewed and community recognized video authentication methods as experiments or tests to detect video authenticity. The individual video authentication techniques employed in this thesis and noted in various scientific papers are intended to be updated as new methods are discovered, refined, or tested in the community and as technology advances in the

future. The individual techniques are considered to be modules that can be inserted or removed as appropriate depending upon the video file and circumstances of the case. The thesis also recognizes the legal aspects of video authentication. The proposed framework is intended to provide forensic examiners, who possess a solid foundation of training and education, with a structured process for use in authenticating digital video in court and other types of litigation.

CHAPTER II

LEGAL CONSIDERATIONS OF AUTHENTICATION

This thesis addresses a proposed framework for digital video authentication, based upon forensic science that may be used by the court recognized expert to aid the trier of fact in determining the authenticity of digital videos offered to the court. The use of the proposed framework is intended for use by the plaintiff or prosecution and/or the defense to scientifically illustrate that digital video has or has not been manipulated. The proposed framework is also useful to the court for recognition of the type of scientific tests that a digital video file should undergo for authentication.

It is important to understand the legal aspects of authentication and to recognize the importance of a scientific based framework for digital video authentication. Appendix A contains information concerning the following:

- 1) Authentication of Electronically Stored Information in the U.S.
- 2) Survey of 2018 U.S. Federal Cases of Questioned Video Authentication
- 3) Authentication of Electronically Stored Information in International Criminal Court
- 4) Expert Testimony

The information in Appendix A influenced the development of the proposed framework and the overall legal aspects for the framework use.

Legal Aspects For Use In Proposed Framework

This portion of the thesis clarifies the use of the scientific method in the framework development, the criteria to assess individual techniques used in the framework, and a discussion on expert testimony approach when using the proposed framework.

Scientific Method

In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993), hereafter noted as *Daubert* case, the U.S. Supreme Court specifically articulated the basis of the reliability that the trial judge should use to assess potential expert testimony when it wrote “...in order to qualify as "scientific knowledge," an inference or assertion must be derived by the scientific method” [11].

The Oxford Dictionary described the scientific method as “a method of procedure that has characterized natural science since the 17th century, consisting in systematic observation, measurement, and experiment, and the formulation, testing, and modification of hypotheses” [12].

The National Center for Media Forensics (NCMF) teaches and uses a six-step scientific method in scientific research. (See Appendix B for the scientific method and a general explanation of its use in the proposed framework development and use in video authentication.)

Criteria Used To Assess Techniques

The scientific method noted in Appendix B contains a “process” section noted as experiments /test. This section is where the examiner uses a series of smaller testing procedures or techniques to test video authenticity. The examiner subsequently analyzes the smaller testing procedures or techniques, which is then reported in the analysis section of the scientific method. The decision which specific smaller testing techniques to use should be based on the repeatability and reliability of the proposed scientific technique(s) / method(s).

The examiner who uses the framework should assess potentially new techniques / methods using criteria similar to the courts in the jurisdiction where the examiner may be expected to provide expert testimony on the results of the video authentication. The U.S. Federal

courts, ICC, and courts in many other countries have generally accepted a criteria to test forensic science, including the framework and the techniques used in the framework, based on the methodology noted in the *Daubert* case as noted above. Additionally, examiners who use the framework in the future and update the techniques in this framework should use similar criteria for assessing the use of the techniques as new methods are developed. The assessment criteria are offered below.

Has The Theory Or Technique Been Tested?

The underlying methodology may be based upon basic forensic science principles that have been previously tested. One example is device identification based upon Photo Response Non-Uniformity (PRNU) comparison methodology that is based upon the forensic science principal of individualization. The foundations of individualization in forensic science have an extensive history of testing. The examiner should review and retain the documentation to support their answers to this criteria portion.

Has The Theory Or Technique Been Subject To Peer Review & Publication?

The video forensic examiner who will use this framework should research each proposed technique in the series of smaller testing procedures or techniques to test the video's authenticity in order to validate the proper level of peer review and publication. Peer review and publication have multiple levels of acceptance, which may be inside or outside the laboratory.

Peer review and publication. The preferred peer review process should start with the submission of a paper to an entity that is associated with scientific research including multimedia forensics such as the American Academy of Forensic Sciences (AAFS) and Digital Forensic Research Workshop (DFRWS). The preference for these entities is based upon the stringent peer review process undertaken by those organizations. Papers are submitted to a double-blind

peer review, which means that both the reviewer(s) and author(s) identities are hidden from each other throughout the review process. Papers submitted to, and accepted by AAFS and DFRWS for review are subsequently published (see publication section below).

There are other less stringent peer review processes that are acceptable, such as those that are not reviewed in the double-blind process.. An example of other processes include research that is associated with thesis and dissertations which are subjected to peer review by an advisory committee.

The preferred method of publication is to use journals linked to the entities that use a stringent peer review process. AAFS publishes the Journal of Forensic Sciences ; DFRWS publishes the Journal of Digital Investigation.

What Is The Error Rate Of The Theory Or Technique?

The next criteria for assessing the theory or technique based upon the methodology noted in *Daubert* involves error rates. Error rates are used across forensic sciences to characterize the likelihood that a specific result is correct or accurate.

In 2018, The Scientific Working Group on Digital Evidence (SWGDE) published a document titled “Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis” [13] that directly addressed error rates relevant in the field of digital and multimedia forensics through the use of error mitigation.

The SWGDE analysis begins with three questions.

- Is the theory or technique based upon valid science?
- Are the implementations of the technique correct and appropriate for the environment where they are used?
- Are the results interpreted correctly? [13]

The SWGDE error mitigation approach addresses potential sources of error, takes steps to mitigate systemic errors such as those commonly arising from the implementation, and generally use a quality assurance approach of continuous human oversight and improvement process to ensure the production of reliable results. SWGDE noted that error rates should be included in the overall error mitigation analysis when those rates can be calculated [13].

Is The Theory Or Technique Accepted In The Forensic Science Community?

The next criteria for assessing the theory or technique is determining the acceptance of that theory or technique in the forensic science community. This may include searching court cases for references to the specific technique's acceptance or recognition; researching presentations at forensic science organization events where peer review of presentations occur (e.g., AAFS, DFRWS, Audio Engineering Society (AES) Technical Committee – Audio Forensics, etc.); reviewing peer reviews found in forensic science publications; and reviewing best practices published by community organizations like SWGDE and American Society for Testing and Materials (ASTM) related to digital and multimedia forensics.

What Are The Standards Controlling The Use Of The Theory Or Technique?

The last criteria for assessing the theory or technique is to determine the existence and maintenance of any standards controlling the operations or use of the theory or technique. The review of the SWGDE best practices where the theory or technique was cited may list standards controlling the use of the theory or technique.

Expert Testimony Approach Using Proposed Framework

The survey of questioned video authentication found in 2018 U.S. Federal cases revealed that the Grimm et. al. findings of 2009 can still be found in federal cases almost 10 years later. While the actual merit of the challenges to the video authentication cannot be addressed in this

thesis; the survey found that in no instance did the challenging party use any technique or method noted later in this proposed framework. It was evident from the review of the cases in the survey that the trial court expected specific scientific evidence to indicate any alteration of the video or audio consistent with the *Lorraine* case when it offered a “how to” guide related to ESI and in part discussed authentication.

The proposed framework is a process that may be used by a court recognized and properly trained forensic video expert to authenticate a video focusing on its contents, substance, and distinctive characteristics.

CHAPTER III

LIGHT TO DIGITAL VIDEO FILE

This chapter provides a quick overview of the digital video file creation chain, general description of the digital multimedia file, and a description of camera sensor noises. It is important to understand the digital video file creation chain, digital multimedia file, and sensor noises as later chapters refer to some of these concepts.

Video Creation Chain

Today's video files are created with and without audio depending upon camera configuration. It is important to understand digital video file creation chain before one can analyze videos for alterations or editing. Figure 4 below illustrates the video creation chain with an audio content and builds upon the concepts in the subsequent sections of this chapter.

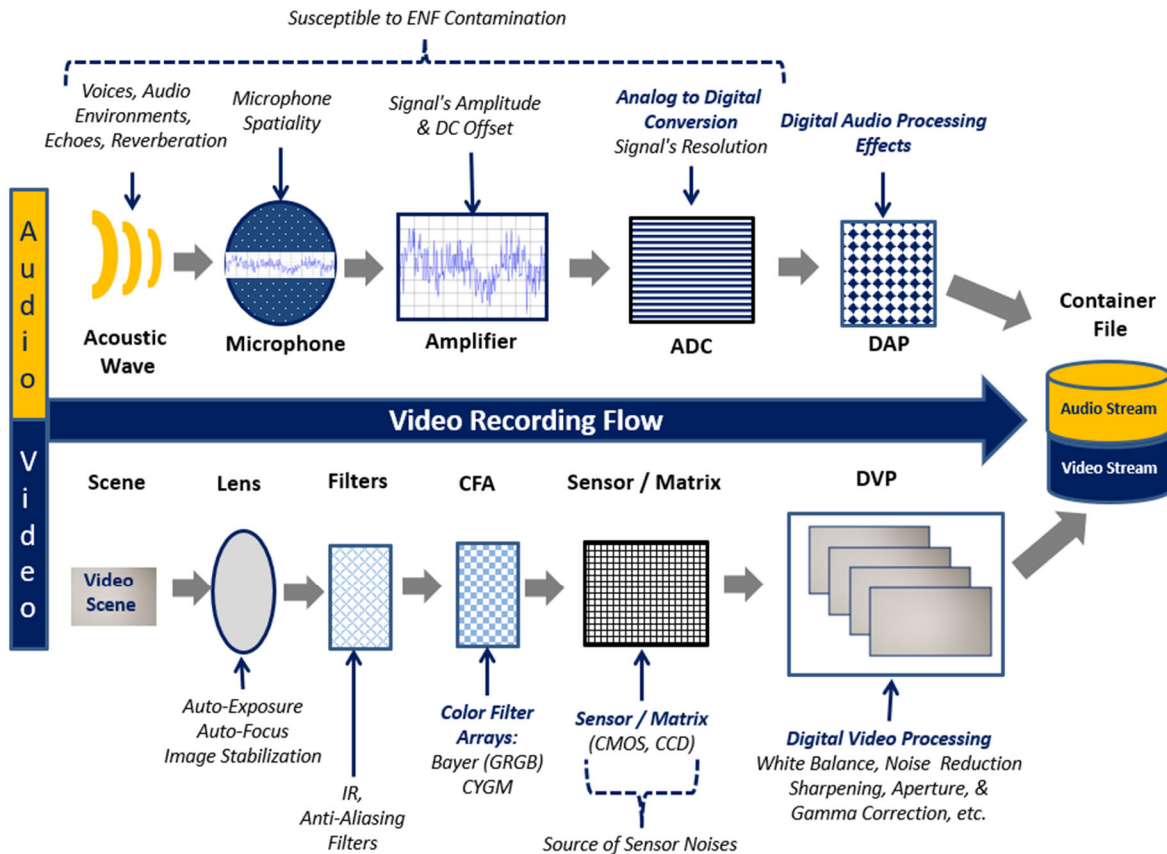


Figure 4 - Final Video Creation Chain With Influence Factors

Figure 4 illustrates the overall video creation chain as light rays reflect off an object and sound emanates from an object. The video creation chain (with audio) has the creation of both the audio and video stream recording flow noted from left to right in Figure 4 above. The illustration notes single video and audio streams in the creation of the video file. It is important to also note that a video file may contain more than one audio and video stream.

Audio Stream Creation Chain

The top half of Figure 4 addresses the audio stream creation / recording flow that produces the final audio stream. The audio stream creation flows from left to right in the top half of Figure 4. An acoustic wave originates from an object / the scene and enters the microphone of the camera to the amplifier. The acoustic wave continues through the amplifier to the analog to digital converter (ADC). The ADC passes the signal to the digital audio processing (DAP) for processing effect to the original output / container file's audio stream.

Video Stream Creation Chain

The bottom half of Figure 4 addresses the video stream creation / recording flow that produces the final video stream. The video stream creation flows from left to right in the bottom half of Figure 4. Light rays reflect off an object in the video scene and enter lens of the camera to the filters. Light rays continue through the filters to the color filter array to the sensor. The sensor digitizes the light rays reflected off an object and passes the digitized video processing (DVP) through digital processing to the original output file.

Influences on Audio Stream During Creation

There are multiple creation aspects that influence the final audio stream in the original output file that the forensic examiner should consider in the overall authentication process as part of the framework. Figure 4 addresses some, but not all, of the creation aspects that influence the

final audio stream. Figure 4 contains some of the creation aspects that influence the final audio stream noted above the overall audio stream creation chain. Figure 4 notes above the acoustic wave that voices, audio environments, echoes, and reverberations may influence the final audio stream. Spatiality has major impact on the audio streams creation. The forensic examiner should consider the signals amplitude and direct current (DC) offset associated with the amplifier. The forensic examiner should also consider the signal's resolution in the ACD process. Figure 4 also notes that all of the previous audio stream creation elements (microphone, amplifier, and ADC) are susceptible to Electronic Network Frequency (ENF) influence depending upon the camera power source. The forensic examiner should consider ENF during the authentication process.

Influences on Video Stream During Creation

There are multiple creation aspects that influence the final video stream in the original output file that the forensic examiner should consider in the overall authentication process as part of the framework. Figure 4 addresses some, but not all, of the creation aspects that influence the final video stream. Figure 4 contains some of the creation aspects that influence the final video stream noted below the overall video stream creation chain. Figure 4 notes below the lens that auto-exposure, auto-focus, and image stabilization may influence the final video stream and be of interest to the forensic examiner in the authentication process. The forensic examiner should be interested in infrared (IR) and anti-aliasing filters applied to the video stream as noted in Figure 4 under filters. The forensic examiner should consider the type of color filter array used in the video stream creation such as Bayer filter (RGBE) and CYGM (cyan, yellow, green, and magenta) filters as noted in Figure 4. A major contributor to camera identification is the Photo Response Non-Uniformity (PRNU) characters in the video stream from the sensor as noted in

Figure 4. The forensic examiner should consider white balance, noise reduction, sharpening, gamma correction digital video processing aspect of the original video stream.

Combined Audio & Video Creation Chain With Influences

Figure 4 combines all of the video creation chain aspects with the previously referenced influences as a reference for use during the video authentication process.

Digital Multimedia File

The digital multimedia file has a file header, metadata, video stream(s), and may have audio stream(s). See Figure 5 below for an example of a digital multimedia file using a book analogy.

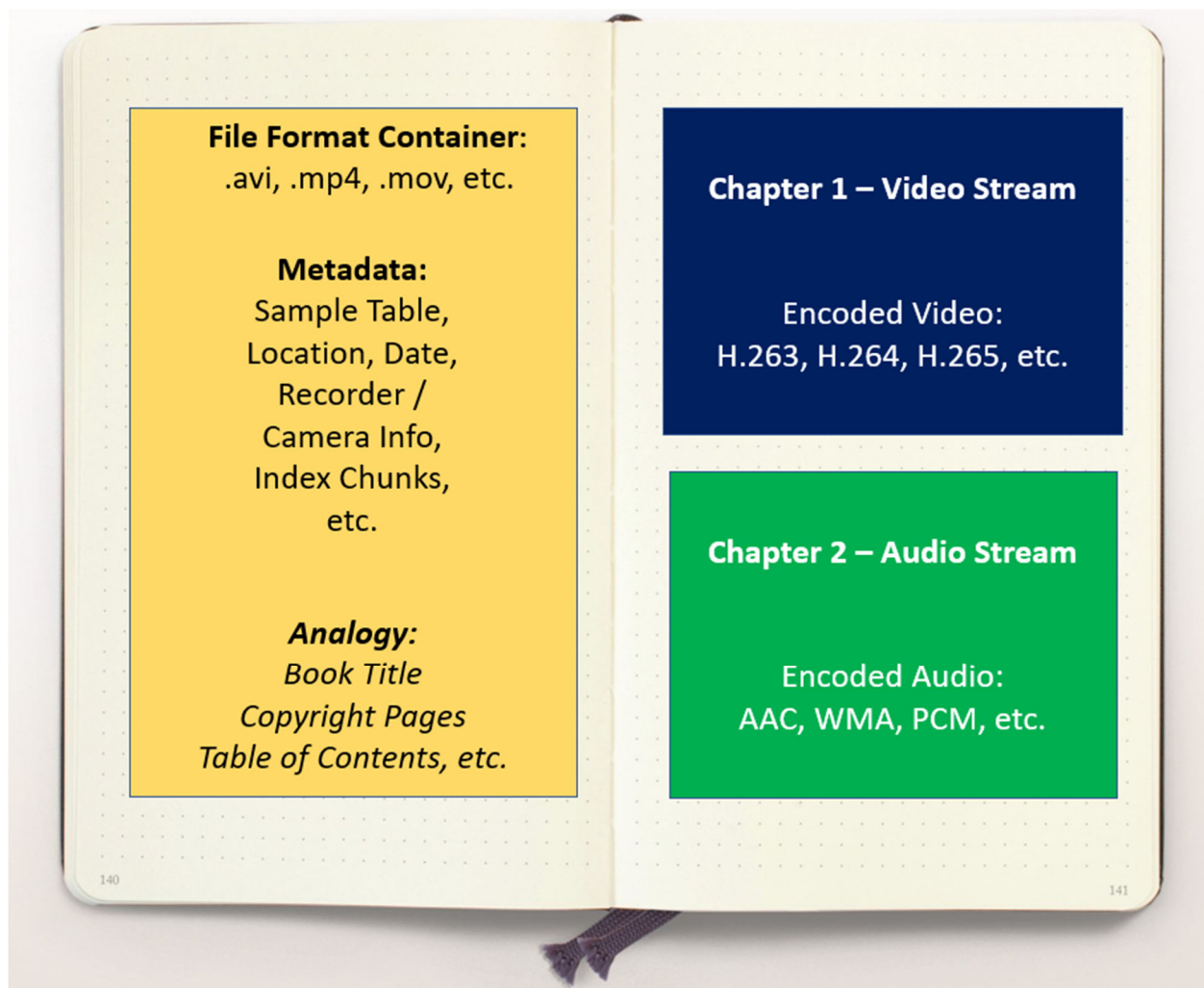


Figure 5 - Example of Digital Multimedia File Using Book Analogy

Figure 5 illustrates an example of a digital multimedia file using a book analogy. The digital multimedia file regardless of the audio or video codec or container type (lossy compression or lossless compression) have at least a file header and the relevant streams. The example in Figure 5 contains one video stream and one audio stream. The digital multimedia files frequently contains metadata. The metadata may be very small or a minimum amount of data. Additionally, metadata may reside before the audio / video streams or after or both locations. Metadata could reside between streams.

Sensor Noises

Digital video cameras today use either CMOS or CCD sensor chips. The sensor chips generate noises during the image or frame creation process as noted in Figure 4 above. It is important to understand the types of noises a sensor generates and their general origin as the forensic examiner develops their method toolbox for video authentication. Some of the recent research in video authentication methods use different noises for indicators of video alteration and camera identification. The two sensor chips have similar noise types but there are a couple of differences. This section will address each sensor chip's noise types.

CMOS Sensor

The Complementary Metal-Oxide Semiconductor (CMOS) sensor is common in older and lower end cameras as they are lower cost to produce. The following figure offers a general block diagram of the CMOS sensor noise model based upon research published by Gow, Renshaw, Findlater, Grant, McLeod, Hart, and Nicol (2007) [14].

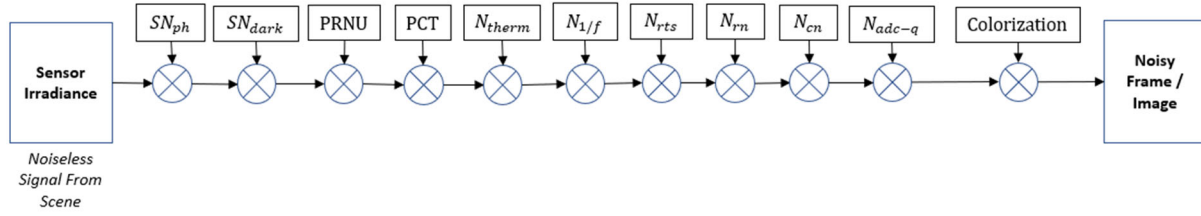


Figure 6 - General Block Diagram of CMOS Sensor Noise Model [14]

As noted in the figure above, the noiseless signal arrives at the sensor surface, the noise accrues throughout the process as the noisy frame / image leaves the sensor. The following table offers explanations of the noise types noted in the block diagram above.

Table 1 - CMOS Sensor Noise Types [14]

Noise Type	Origin	Manifestation	Description
SN_{ph} – photon shot noise.	CMOS sensor	Additive temporal variance.	Incident to pixel illumination
SN_{dark} – dark-current shot noise	CMOS sensor	Additive temporal and spatial variance. Fixed Pattern Noise	Temperature
$PRNU$ – photo response non-uniformity	CMOS sensor	Multiplicative spatial variance only. Fixed Pattern Noise	Incident to pixel illumination
PCT – Pixel cross talk	CMOS sensor	Additive temporal and spatial variance. Fixed Pattern Noise	Incident to pixel illumination
N_{therm} – Combined thermal noise	CMOS support integrated circuits	Additive temporal and spatial variance.	Temperature
$N_{1/f}$ – Low frequency flicker noise	CMOS support integrated circuits	Additive temporal variance. Fixed Pattern Noise	Temperature
N_{rts} – Random Telegraph Signal	CMOS support integrated circuits	Additive temporal variance. Fixed Pattern Noise	Temperature
N_{rm} – Row noise	CMOS sensor and CMOS support integrated circuits	Additive temporal variance.	Temperature
N_{cn} – Column noise	CMOS sensor and CMOS support integrated circuits	Additive temporal variance.	Temperature
N_{adc-q} – Analog to Digital Quantization	CMOS support integrated circuits	Additive is image content dependent	Variance of image data.
$Colorization$ – Pixel cross talk	CMOS support integrated circuits	Additive is image content dependent	Variance of image data.

CCD Sensor

The Charge Couple Device (CCD) sensor is common in newer and mid to higher end cameras as they are more expensive to produce but tend to offer better quality video. The following figure offers a general block diagram of the CCD sensor noise model based upon research published by Irie, McKinnon, Unsworth, & Woodhead, table 3008 [15] [16].

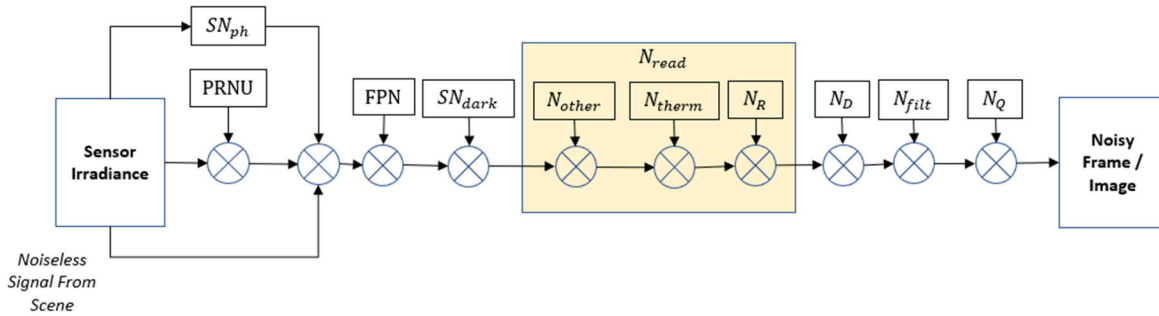


Figure 7 - General Block Diagram of CCD Sensor Noise Model [15][16]

As noted in the figure above, the noiseless signal arrives at the sensor surface, the noise accrues throughout the process as the noisy frame / image leaves the sensor. The following table offers explanations of the noise types noted in the block diagram above.

Table 2 - CCD Sensor Noise Types [15][16]

Noise Type	Origin	Manifestation	Description
SN_{ph} – photon shot noise.	CCD sensor	Additive temporal variance.	Incident to pixel illumination.
$PRNU$ – photo response non-uniformity.	CCD sensor	Multiplicative spatial variance only.	Incident to pixel illumination.
FPN – offset fixed-pattern noise.	CCD sensor	Additive spatial variance only.	Temperature, exposure time.
SN_{dark} – dark-current shot noise	CCD sensor	Additive temporal and spatial variance.	Temperature, exposure time.
N_{other} – combined flicker noise, transistor dark currents, and other minor contributors.	CCD sensor and CCD support integrated circuits	Additive temporal and spatial variance.	Temperature, CCD readout rate.
N_{therm} – Combined thermal noise.	CCD support integrated circuits	Additive temporal and spatial variance.	Temperature.

N_R – reset noise	CCD support integrated circuits	Additive temporal and spatial variance.	Temperature.
N_{read} – readout noise. Combined $N_R + N_{therm} + N_{other}$	As per N_R , N_{therm} , and N_{other}	Additive temporal variance.	Temperature, CCD readout rate.
N_D – demosaicing noise.	CCD support integrated circuits.	Multiplicative noise amplification or attenuation.	Demosaicing implementation, combined sensor noise.
N_{filt} – post image-capture effects.	CCD support integrated circuits.	Multiplicative noise effect.	Parameters for image enhancement, combined sensor noise.
N_Q – quantization noise	CCD support integrated circuits	Additive noise. Image content dependent.	Variance of image data. Sets lower noise limit for non-trivial image content.

Overview of Sensor Noise Types

The sensor noise types are briefly described below.

Photon Shot Noise

Photon shot noise is described by Gow et al, 2007, as an inescapable uncertainty in the number of photons collected in the photodiode and this is due to the quantum nature of light [14]. It indicates the variations in number of the photons detected due to the occurrence independent of each other.

Dark Current Shot Noise

Hytti (2006) described dark current shot noise as thermal generation of electrons in the silicon that is usually different from pixel to pixel [17].

Photo Response Non-Uniformity

Irie et al., 2008, described PRNU as the difference in pixel responses to uniform light sources [15].

Pixel Cross Talk

Pixel cross talk is described by Gow et al, 2007, as a phenomenon that causes mixing, image blur, and degrades the signal-to-noise ratio after color reconstruction in CMOS sensors [14].

Offset Fixed-Pattern Noise

Irie et al., 2008, described offset FPN as changes in dark currents from variations in pixel geometry which originates from fabrication of the sensor [15].

Thermal Noise

Irie et al., 2008, described thermal noise as fluctuations of an electric current inside the electrical conductor from the random thermal motion of charge carriers [15].

Flicker Noise

Van Houten and Geradts, in their 2009 research, cited flicker noise as a temporal noise where charges are trapped in surface states and subsequently released after some time in the charge to the voltage amplifier [18].

Random Telegraph Signal

Ishida, Kagawa, Komuro, Zhang, Seo, Takasawa, and Kawahito (2018) described random telegraph signal (RTS) noise as mainly generated by CMOS traps of the source follower transistor [19].

Row Noise

Gow et al, 2007, noted when a row in the photodiode is released from reset, all pixels in that row are unprotected from noise entering through the reset line, transfer gate, or read transistor. Gow et al, 2007, noted the row noise manifests in images as horizontal lines and with fixed and temporal components [14].

Column Noise

Gow et al, 2007, noted column noise is introduced by the sample and hold capacitors during reset [14].

Reset Noise

Irie et al., 2008, described reset noise as a specific type of thermal noise originating from the capacitors (kTC) when resetting the charge sensor capacitor to a reference voltage [15].

Demosaicing Noise

Irie et al., 2008, described demosaicing noise as the interpolation of the RGB color data for each pixel [15].

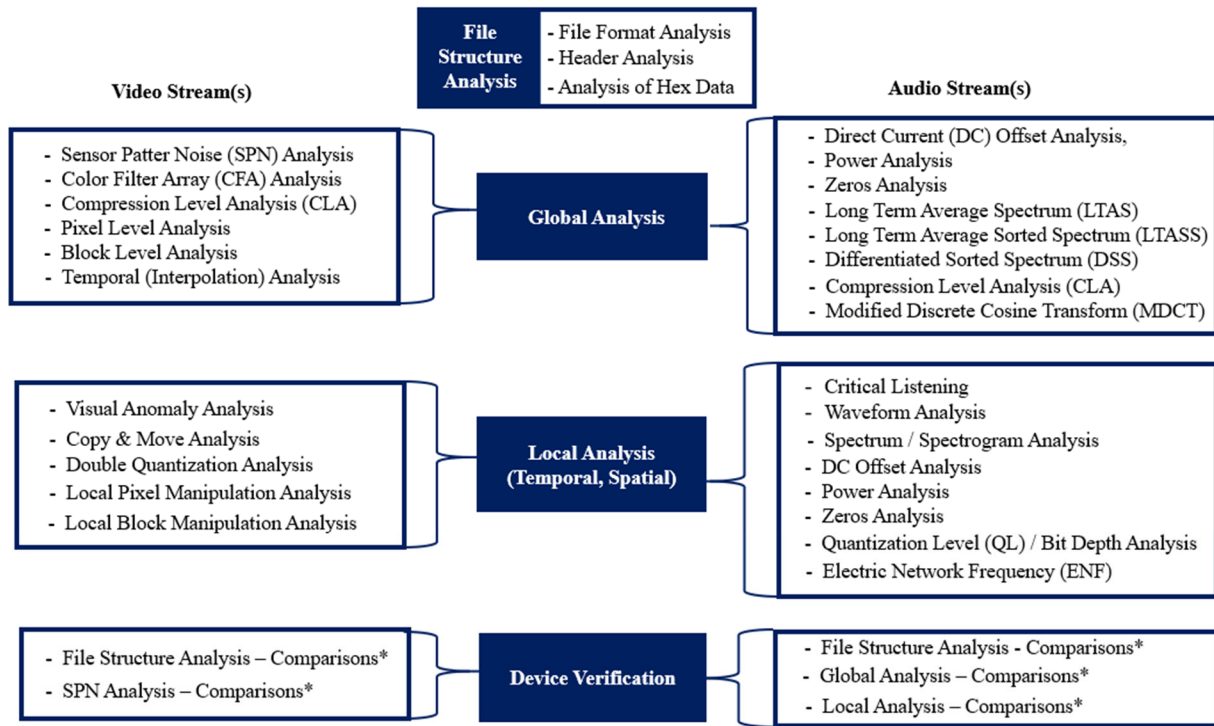
ADC Quantization Noise

Gow et al, 2007, noted the noise as a linear quantization of the input signal based upon the analog to digital conversion architecture [14].

CHAPTER IV

PROPOSED FRAMEWORK

The structure for the proposed framework uses a repeatable approach. The proposed framework analyzes the file structure, the video stream(s), the audio stream(s), and device verification (if applicable). These analysis are cumulative in their influence in reaching a conclusion about the authenticity of the questioned video file. The file structure analysis is performed on a forensic duplicate (working copy) of the submitted video file. The figure below illustrates the proposed framework.



** Note: Comparisons With Questioned Device(s), Known Device Library / Database, & Core Software Library / Database*

Figure 8 - Proposed Video Authentication Framework

File Structure Analysis

The file structure analysis includes the sub-analysis components of file format analysis, header analysis, and analysis of hex data.

Workflow Optimization

Management may wish to optimize the workflow of the forensic video examiner. A workflow optimization method in the proposed framework would be the insertion of a logic condition at this point. A decision point in the workflow is offered below.

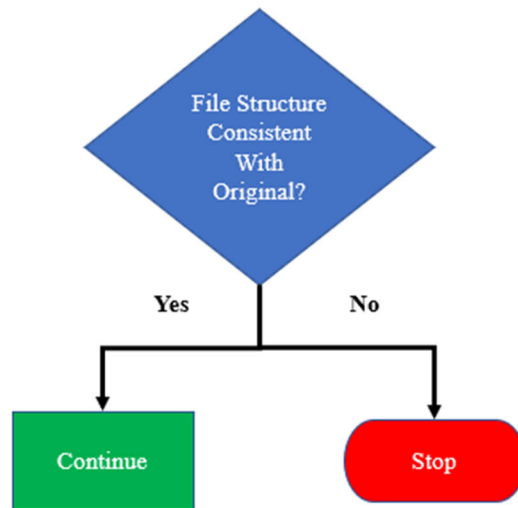


Figure 9 - Workflow Optimization Based On File Structure Analysis

The figure above illustrates the decision point that if the file structure was consistent with an original file, a workflow optimization condition would be to continue to the video and audio stream analyses. However, if the file structure was not consistent with an original file, a workflow optimization condition would be to stop the analyzes and report the findings.

The simple detection of an altered or edited video may be sufficient for a case and the workflow optimization is a useful tool for management in an effort to manage resource and personnel. Nevertheless, there are incidents where it is important to know the location of tampering and the general methodology to determine if the alteration or editing was consistent with intent to manipulate the viewers perspective.

File Preparation For Audio & Video Stream Analysis

The file may be prepared for the analyzes of both the audio stream analysis and video stream analysis through bifurcation. The audio stream may be copied to a Wave PCM file for subsequent authentication. The stream copy is accomplished while not changing the sample rate. The video stream may need to be transcoded out of a proprietary file to a lossless format for subsequent authentication processing. However, the frames per second (FPS), dimension, or other important properties should not be changed. The most advisable way to transcode the video or audio streams is by using multimedia stream hashing method [20]. Using this method a stream hash can be calculated prior to transcoding and compared with the bifurcated file's stream hash to verify no modifications have been made to the target signals.

Audio Authentication

Each audio stream should be subjected to a series of smaller testing methods or techniques using a previously published and forensic community recognized framework [22] [24] [25]. The series of testing should include methods for global and local analysis areas.

Video Authentication

Each video stream in the video file should by subjected to a series of smaller testing methods or techniques as part of the authentication framework. The series of testing should include methods for global and local analysis areas.

Device Identification / Verification

Device verification analyses are useful in corroborating a questioned video file originated / created by an alleged camera / recorder or attributing the video to an unknown recording device (specifically excluding submitted camera / recorder). These analyses involve various techniques

that could be used for just one analyses area (e.g., global, etc.) or span all three areas (global, local, and device verification).

The analysis of the each section in the framework should be documented. Appendix E may be used to document the digital video authentication framework analysis.

CHAPTER V

FRAMEWORK JUSTIFICATION – RESEARCH, TESTING, & RESULTS

This chapter addresses the overall development and use of the proposed framework, previous research on analysis methods / techniques, testing of techniques, and a general overview of the testing results.

Framework Development & Use

The development and use of the proposed video authentication framework is reliant on three interrelated issues. The first issue is the general analysis question, based upon the scientific method (reference Appendix - A). The second issue is based upon the digital multimedia file that is submitted for examination. The third issue is an assessment of the tools available in our toolbox.

Analysis Questions

The scientific method begins with the analysis question (reference Appendix-A). The requestor for authentication of questioned video submits the following question to the forensic examiner.

Analysis Question #1 (AQ-1) - Has the video stream, video stream and audio stream, or audio stream been processed or manipulated?

The request for video authentication usually involves this analysis question (AQ-1). It is important to make a key distinction in this analysis question. The distinction is the difference between “processed” and “manipulated” when the forensic examiner analyzes data (step #5 of scientific method) from the experiment / test results (involved in step #4 of scientific method). [21] described a processed video and / or audio stream involves recompression and transcoding that does not involve media manipulation. Media manipulation is the application of different

editing techniques to audios, photographs, videos, or electronic data in order to create an illusion or deception, through analogue or digital means. A manipulated video and / or audio stream involves media manipulation. The editing (media manipulation) may involve deleting video and / or audio, adding video and / or audio, enhancement of either or both with intent to deceive the viewer / listener, or the creation of deepfake video and / or audio.

A second, and related, question may also be asked of the forensic examiner if a questioned camera / recorder is available for experiments / testing. The second question posed to the forensic examiner follows.

Analysis Question #2 (AQ-2) – Did the submitted camera / recorder create the questioned video?

The two analysis questions influence the general components involved in the authentication framework. Another aspect of the framework depends upon the questioned file's container and it's contents.

Digital Multimedia File

The digital multimedia file may consist of the file header, metadata, video stream(s), and audio stream(s). The digital multimedia file may use lossy compression or lossless compression. The digital multimedia file format may be open source or proprietary. All of these factors influence the video authentication process. However, there are some common digital multimedia file components that influence analysis areas in the development of the framework. See figure below for a graphic of the general analysis areas for the proposed framework.

Framework Development

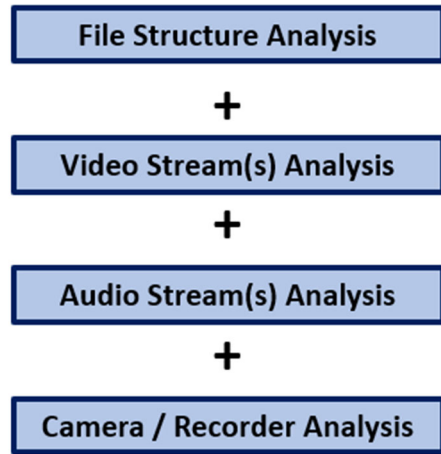


Figure 10 - Framework Development General Areas of Analysis

The figure above illustrates the development and areas of the proposed video authentication framework. The proposed general analysis areas include File Structure Analysis, Video Stream(s) Analysis, Audio Stream(s), and Camera / Recorder Analysis. The general areas are included depending upon the analytical question(s) and the digital multimedia file contents. These analyses may be global, local, or device verification.

Global analyses are conducted on the questioned video file as a whole and produce results relevant to authenticity without focusing on specific portions or segments of the multimedia streams. Local analyses are conducted on specific portions or segments of the questioned video file to detect the file's authenticity. Device verification analyses are useful in corroborating whether a questioned video file originated / created by an alleged camera / recorder or attributing the video to an unknown recording device (excluding submitted camera / recorder). These analyses involve various techniques that could be used for just one analyses area (e.g., global, etc.,) or span all three areas (global, local, and device verification). An example of a technique that spans all three areas would be sensor pattern noise (SPN) analysis.

SPN analysis may be used for global analyses test, local analyses test, and detecting individual characteristics within the device verification analysis.

File Structure Analysis

The file structure analysis involves a comprehensive examination of the file format, the file header, and the hex data within the digital multimedia file. The file structure examination involves a non-exhaustive list of areas to review including the file extension, file header, various metadata components, various video and audio recorded contents, and possible footer. Much of this data may be in hex and some recognizable information in American Standard Code for Information Interchange (ASCII). The forensic examiner observes the file structure information to identify the number of videos streams and audio streams (if audio is present) as well as the camera / recorder information and any software used to create the recorded contents.

Video Stream(s) Analysis

The video stream(s) analysis examines all videos streams present within the digital multimedia file for evidence of global and local alterations or edits. The specific techniques used for testing the video stream(s) are noted in the research section of this chapter. The forensic examiner compiles the collected findings data relative to each tests for subsequent development of a conclusion.

Audio Stream Analysis

The audio stream(s) analysis examines all audio streams present within the digital multimedia file for evidence of global and local alterations or edits. The specific techniques used for testing the audio stream(s) are noted in the research section of this chapter. The forensic examiner compiles the collected findings data relative to each tests for subsequent development of a conclusion.

Camera / Recorder Analysis

The camera / recorder analysis uses questioned device(s) to create exemplars under similar recording environments as those of the questioned video digital multimedia file to conduct comparison of exemplars and the questioned video file for video authentication including device verification. The specific techniques used for camera / recorder testing are noted in the research section of this chapter. The forensic examiner compiles the collected findings data relative to each test for subsequent development of a conclusion.

Data Interpretation & Conclusion Development

The findings from the individual analysis areas above are combined to develop the conclusion. Each test result should be scientifically interpreted and technical descriptions should be articulated in an unbiased way. Authenticity conclusions should be factually documented and thoroughly supported by the analyses conducted.

Grigoros, Rappaport, and Smith (2012), noted in their paper “Analytical Framework for Digital Audio Authentication” at the Audio Engineering Society’s 46th International Conference, that no scientific inquiry, including those in forensics, produce a result of absolute certainty. Therefore, conclusions in digital audio examinations related to an audio recording’s authenticity should not be stated in terms of absolutes. Language implying 100% certainty should be avoided unless speaking about known alterations or deletions [22]. This approach also applies to digital video authentication.

An authentication examination may have the following conclusions:

- Consistent with an original recording.
- Inconclusive.
- In-consistent / not consistent with an original recording.

However, the same results above should be used as a grading scale for each analysis results or finding.

Tools For Video Authentication Toolbox

The third issue in the framework development and use process is a discussion of the tools (methods / techniques) available for the video authentication framework. Each method or technique the examiner uses in the authentication framework should be subjected to testing / evaluations as to their viability for use in the framework.

The video authentication framework, as noted in the introduction chapter's scope, is proposed for use by the forensic examiner to authenticate digital videos and support their conclusion in court testimony as an expert. The forensic examiner will need to continuously update the methods / techniques in video authentication framework. Additionally, some methods / techniques are not relevant to every use of the authentication framework depending upon the analysis question(s) and files contents. The forensic examiner should conduct two overall evaluations of the tools in their toolbox for video authentication. The evaluations are a Tool Validation Testing and a Admissibility Assessment.

Tool Validation Testing

Validation testing is defined by SWGDE as “an evaluation to determine if a tool, technique, or procedure functions correctly and as intended” [23]. The first part of the test is whether the technique functions correctly. As previously noted in Chapter 1, there are multiple published articles and papers on various digital video authentication techniques, but many of them involved techniques in laboratory-controlled environments that subject the videos to a specific video authentication technique that is not reproduceable. The technique's reproducibility is critical to use for forensic science. Additionally, it is important that the

forensic examiner validate a technique for its intended use and that the technique performs as expected.

Admissibility Assessment

The admissibility assessment is used to ensure the forensic examiner can support the technique or method in court. The Daubert case is the guiding precedent for the admissibility assessment. As previously stated in the legal aspects chapter of this thesis, the assessment should ask the following questions.

- Has the theory or technique been tested?
- Has the theory or technique been subject to peer review and publication?
- What is the error rate of the theory or technique or is error mitigation implemented?
- Is the theory or technique accepted in the forensic science community?
- What are the standards controlling the use of the theory or technique?

Refer to the Legal Aspects chapters of this document for a detailed discussion of these topics.

Updating Analyses Tools

The forensic examiner should continuously research new methods or techniques in the analyses of digital multimedia file analysis, audio stream analysis, video stream analysis, and camera / recorder device verification analysis for new or updated authentication methods.

Research For Analysis Tools

The following section covers a non-exclusive list of researched methods / techniques for use in the digital video authentication framework.

File Structure Analysis Techniques

All digital cameras create files with unique file structures and contents. The file structure is important to investigate as it is interpreted by the computer, mobile device, or camera as to how to process the contents of the file.

The file structure analysis, for the forensic examiner conducting video authentication, involves a comprehensive examination of the file format, the file header, and hex data within the digital multimedia file. The file structure analysis technique involves analysis of the questioned file format for inconsistencies observed in this area that may lead the forensic examiner to more conclusive analyses. The file header and hex analysis inconsistencies may provide the forensic examiner more conclusive results [22] [24] [25] [26] [27].

The forensic examiner may want to use one of two in-depth approaches to the file structure analysis based upon the published standard or, if the suspected originating recorder is available, use exemplars from suspected originating recorder for comparison with the questioned file.

File Format

There are many different types of video files in use today. Video files have chunks of data organized based upon file format and encoding applied to some chunks of data based upon the video codec used and if audio is present the audio codec used. The different digital multimedia files each have a standardized format that defines how data is stored within the file. Examples of these digital multimedia files are 3GP, AVI, MOV, MKV, and MP4. Examples of various video codecs include H.263, H.264, H.265, and MJPEG. Examples of various audio codecs include AAC, WMA, and PCM.

A technical review of the file format should be made to document information for subsequent analyses. Part of the file format analysis may involve reverse engineering the file format in order to explain how the file could attain the current state. The main areas of the file format analysis include format, codecs, sample rates, bit depth, etc. [22][24][25].

A video file today does not just contain video streams and audio streams. The forensic examiner may also find closed caption data. Caption data may use the following non-inclusive listing of formats:

- Web Video Text Track (WEBVTT),
- Consumer Electronics Associations (CEA) 608 / 708,
- Distribution Format Exchange Profile (DFXP),
- Timed Text Markup Language (TTML),
- Synchronized Accessible Media Interchange (SAMI).

The video files today also contains metadata.

Metadata written by cameras / recorders today may write metadata in Exchangeable Image Format (EXIF) or Adobe's Extensible Metadata Platform (XMP) format. Metadata tags may contain information about the recording date, time, camera, and location of recordings. It is important to understand that metadata may be easily changed or deleted. Research has revealed that some social media websites and video sharing websites (e.g., YouTube, etc.) typically remove the original camera metadata from videos and images [28] [29] [30].

Header Analysis

Metadata analysis tools extract and interpret file header data and file properties into human readable information. A forensic examiner should compare metadata analysis information to the actual hex data. However, it is more important to overcome tool error or

completeness by using 2 or more tools to cross-verify metadata information. File headers may contain recorder device information such as make, model, firmware version, serial number, and the date, time, and length of the recording.

Hex Analysis

Hex analysis of a video file is important for file structure analysis of the file to locate post-processing artifacts and understanding the presentation of the video, audio, and closed capture information. Additionally, metadata tags not normally recognized by metadata analysis tools may be discovered deep in the hex of a video stream in a digital multimedia file.

As previously noted, the file structure analysis, for the forensic examiner conducting video authentication, involves a comprehensive examination of the file format, the file header, and hex data within the digital multimedia file. Jake Hall (2015) authored an MPEG-4 file format and metadata analysis methodology for video authentication in his graduate thesis at University of Colorado Denver [31]. In addition, Scott Anderson (2011) offered a detailed file structure authentication methodology in his graduate thesis also at University of Colorado Denver [26].

The file structure analysis method / technique has potential application for the entire analysis perspective of the file. See Table 3 below for the relevant analyses areas.

Table 3 - File Structure Analysis Authentication Method / Technique Relevance

Method / Technique	Global Analysis	Local Analysis	Device Identification (Characteristics)		References
			Class	Individual	
File Structure Analysis	Yes	Yes	Yes	Yes	[22] [24] [25] [26] [27] [31]

Audio Stream(s) & Video Stream(s) Bifurcated Approach

A video file containing both audio stream(s) and video stream(s) should be bifurcated for further analysis. This approach facilitates the forensic examiner separating the file into smaller data sets while leveraging a previous forensic community recognized framework for audio authentication.

Audio Authentication Analysis Tools

The audio stream(s) in the video file should be subjected to a series of smaller testing methods or techniques using a previously published and forensic community recognized framework [22] [24] [25]. This framework may use the methods or techniques noted in the following table to test the audio stream(s) authentication.

Table 4 - Audio Stream Authentication Methods / Techniques Relevance

Method / Technique	Global Analysis	Local Analysis	Device Identification (Characteristics)		References
			Class	Individual	
Critical Listening	Yes	Yes	No	No	[22] [24] [25]
High Resolution Waveform Analysis	Yes	Yes	No	No	[22] [24] [25]
Signal Power Analysis	Yes	Yes	No	No	[24] [25]
DC Offset	Yes	Yes	Yes	Yes	[22] [24] [25]
Long Term Average Spectrum (LTAS)	Yes	Yes	Yes	Yes	[22] [24] [25]
LTAS Sorted Spectrum	Yes	Yes	Yes	Yes	[22] [24] [25]
Differentiated Sorted Spectrum	Yes	No	No	No	[22] [24] [25] [32]
Butt-Splice Detection Analysis	No	Yes	No	No	[22] [24] [25]
Interpolation Analysis (Transitions)	No	Yes	No	No	[22] [24] [25]
Compression Level Analysis	Yes	No	No	No	[22] [24] [25]
Electronic Network Frequency	Yes	Yes	No	Yes	[22] [24] [25]
Phase Continuity (Mono & Stereo)	No	Yes	No	No	[22] [24] [25]

Table 4 methods / techniques are not discussed in this paper since they have been covered in-depth in other papers noted in references.

Video Authentication Analysis Tools

The framework breaks down the tools into device identification, global analysis, and local analysis. Global analysis are format / structure as well as analysis that produces a plot representing the video as a whole. Local analysis is broken down into temporal and spatial analyzes. Temporal analysis compares one frame to the next or a series of frames to another series of frames. Spatial analysis localizes edits or manipulations accomplished within a frame on the pixel level to reveal removal, clone, or spliced (from a different source) areas.

The video stream(s) in the video file should be subjected to a series of smaller testing methods or techniques as part of the authentication framework. A non-exclusive listing of potential test methods or techniques are offered in no specific order below.

Video Copy / Paste / Editing Detection

Today's society has many free and low cost video editing software tools. Additionally, many cameras' have built in video editing capabilities and mobile devices have several 3rd party applications that allow the user to edit videos easily. The following methods / techniques are potential tools in the forensic examiner's video authentication tool box.

Detection of cloning / duplicating frames. Wang and Farid (2007) offered a method to detect a common video manipulation technique of cloning or duplication of frames [33]. These video manipulation techniques are commonly used for removing people or objects from a video. Wang and Farid's (2007) detection method involved two techniques. The first technique detected entire frame duplication while the second technique detected portions of a frame duplicated across one or more frames. The method also discusses the use of the technique across blocks or segments of a video to be more efficient. Wang and Farid's (2007) detection method

could also detect duplicates in both high and low quality compressed video with few false positives [33].

The clone and duplicate frame detection analysis method / technique has potential application for both global and local analysis perspective of the file. See Table 5 below for the relevant analyses areas.

Table 5 - Clone / Duplicate Frame Detection Analysis Authentication Method / Technique

Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
Clone / Duplicate Frame Detection	No	Yes	Yes	No	No	[33]

Directional lighting inconsistency detection. Hany Farid's (2006) Significance magazine article discussed how to detect fake digital images. The article presented information about detecting directional lighting inconsistency and presented some published digital images as illustrations [34]. The directional lighting detection methodology was based upon research Farid and Micah Johnson published in 2005 paper titled "Exposing Digital Forgeries by Detected Inconsistencies in Lighting." The Farid and Johnson (2005) paper offered an example of a digital image where two people standing next to each other was created with different light source directions revealing inconsistencies that may be used to reveal traces of digital tampering [35].

The directional lighting inconsistency analysis may be detected by visual content review or by using algorithms noted in Farid and Johnson (2005) papers. The overall methodology / technique has potential application for both global and local analysis perspective of the file. See Table 6 below for the relevant analyses areas.

*Table 6 - Directional Lighting Inconsistency Detection Analysis Authentication Method /
Technique Relevance*

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
Directional Lighting Inconsistency Detection	Yes	Yes	Yes	No	No	[34] [35]

Local (spatio-temporal) tampering detection. Bestagini, Milani, Tagliasacchi, and Tubaro (2013) offered a method / technique using an algorithm that is able to detect a spatio-temporal region of frames that were replaced with frames or a series of frames from a different time interval where the video contains duplicate blocks of data. The algorithm detects duplicated blocks of data after correlation analysis of the frames. This method has worked with videos with high and low level compression. Bestagini et al., (2013) noted testing correctly detected duplicate blocks in 90% of the sequences when the video was not re-compressed and correctly detected duplicate blocks in 87% of the re-compressed videos. They further noted the incorrect detection activity was not the detection of duplicate blocks, but rather duplicate blocks were not detected [36].

The overall methodology / technique has potential application for both global and local analysis perspective of the file. See Table 7 below for the relevant analyses areas.

*Table 7 - Local (Spatio-Temporal) Tampering Detection Analysis Authentication Method /
Technique Relevance*

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
Local (Spatio-Temporal) Tampering Detection	No	Yes	Yes	No	No	[36]

Interlaced & Deinterlaced Video Inconsistency Detection

Wang and Farid (2007) proposed two methods for detecting inconsistencies in interlaced and deinterlaced videos for detecting altered or edited videos. An interlaced video is an interlaced signal that contains two fields of a video frame at different times. The video camera records first half the video lines at the initial scan ($t = 1^{\text{st}}$ time scan). The video camera records the second half of the video lines at the second scan ($t+I = 2^{\text{nd}}$ time scan). The interlaced video combines the two scan results and produces the frame [37].

Wang and Farid (2007) noted the motion between the two fields of a single frame and in the surrounding frames should be equal in an interlaced video. They noted if the video was tampered with the motion between fields of a single frame and across fields of neighboring frames will reveal inconsistencies [37].

They also offered a model to illustrate the correlation that is introduced by deinterlacing algorithms when software is used on an interlaced video. Wang and Farid (2007) noted tampering can alter these correlations. They also made it a point to note that compression artifacts make it difficult to estimate these deinterlacing correlations. Wang and Farid (2007) recommended the deinterlacing correlation estimate approach be used for high to medium quality videos [37].

In addition, Wang and Farid (2007) suggested the algorithms for the previous techniques could be adapted to detect frame rate conversions that may have occurred post video manipulation. They noted the standard approach to reducing the frame rate is remove the number of frames to meet the expected frame ratio. Wang and Farid (2007) noted this action alters the inter-field and inter-frame motion ratio [37].

The overall methodology / technique has potential application for both global and local analysis perspective of the file. See Table 8 below for the relevant analyses areas.

Table 8 - Interlaced & Deinterlaced Video Inconsistency Detection Analysis Authentication

Method / Technique Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
Interlaced & Deinterlaced Video Inconsistency Detection	Yes	Yes	No	No	No	[37]

Video Double-Compression Detection

Detection of double compression MPEG video. The MPEG video standard uses a Group of Pictures (GOP) with I (intra) – frame (usually the highest quality), P (predictive) – frame, and B (bi-directional) – frame. The I-frame is a full inter-coded frame. The P-frame contains only changes from the previous frame. B-frames contain differences between the previous and following frame.

Global analysis technique. Wang and Farid (2006) offered a method to detect doubly compressed MPEG video sequences as they introduce static and temporal statistical deviations in the video stream whose presence indicate evidence of tampering. Wang and Farid (2006) noted that their method using statistical artifacts made the detection of tampering in doubly-compressed MPEG videos likely [37]. The method they offered approached the detection of the double compression from a global analysis perspective by detecting frame insertion or deletion points. The doubly-compressed I-frame (a double JPEG compression) prior to the frame insertion or deletion point, presents a statistical pattern that is observable in the distribution of discrete cosine transform (DCT) coefficients that may be plotted on a histogram. Additionally, Wang and Farid (2006) revealed that when a P-frame is predicted from a frame that belonged to

a different GOP there was an increase in the total prediction error that may be observed. Wang and Farid (2006) proposed detecting frame deletion or addition by visually inspecting the sequence for a periodic fingerprint. They proposed using a Discrete Fourier Transform (DFT) of the sequence to detect peaks in the periodic fingerprint displayed in a histogram [37].

Local analysis technique. Wang and Farid (2009) offered another double compression detection method of MPEG video sequences that focused on localized analysis that may detect alterations in 16x16 pixel macroblocks [39]. A key limitation in the localized analysis method is that the second compression must be higher than the original video's compression for detection. In addition, the higher the difference in compression the higher the detection performance rate (lower false positives). Wang and Farid (2009) noted this method is particularly useful in detecting the fairly common digital effect of green-screening (a process of combining two videos into one) [39].

Wang and Farid (2009) acknowledge that both the global analysis and local analysis techniques of MPEG double compression detection are vulnerable to countermeasure that can hide traces of tampering [38][39]. However, this is why a series of tests are used in the authentication framework. The MPEG double compression detection analysis method / technique has potential application for both global and local analysis perspective of the file. See Table 9 below for the relevant analyses areas.

Table 9 - MPEG Double Compression Detection Analysis Authentication Method / Technique

Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
MPEG Double Compression Detection	Yes [37]	No	Yes [38][39]	No	No	[37][38][39]

Sensor Noises Detection Methods

Overview. The camera sensor introduces imperfections and noise in images and videos that are not part of the original scene. There is a large body of research in this area that is applicable to video authentication.

Color filter array inconsistency detection. Popescu and Farid (2005) noted in their research on color filter array (CFA) inconsistency detection, that a single color sample is captured by the camera sensor and the other two colors are estimated from neighboring samples. Their research offered a methodology to detect tampering as it creates inconsistencies in the correlations across the image / frame [40].

The CFA interpolation may be based upon several demosaicing approaches. The interpolation may use one of the following:

- Bilinear
- Bicubic
- Smooth Hue Transition
- Median Filter
- Gradient Based
- Adaptive Color Plan
- Threshold Based Variable Number of Gradients [40]

Detection of CFA interpolation uses an expectation / maximization (E/M) algorithm which was a two step iterative algorithm. The E-step calculates the estimated probability each sample belongs to each interpolation approach. This step produces a two dimensional array (probability map) with each entry indicating similarity of each image pixel to one of the two groups of samples (the ones correlated to their neighbors). The E-step iteration of the algorithm

will detect if the interpolation was a linear approach and a region of the image / frame was altered (typically requiring up-sampling). Then the M-step estimates each specific form of correlations between samples. The M-step estimates the weight (interpolation coefficients) which tell the amount of input each pixel has in the interpolation kernel [40].

Popescu and Farid (2005) noted their results for detection of inconsistencies in all CFA interpolation techniques had accuracies (with 0% false positives) with either 100% or 98% (with 1 in 50 misclassified) [40].

Table 10 - Color Filter Array Analysis Authentication Method / Technique Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
Color Filter Array Analysis	No	No	Yes	No	No	[40]

Source camera identification. The general technique used to perform source camera identification is based upon extracting sensor pattern noise from images or frames left behind in the video by the source camera. The specific pattern noise of interest is PRNU.

Van Houten and Geradts (2009) research that these sensor pattern noises are unique to each sensor or camera. The sensor pattern noise may be compared to reference patterns from a database of cameras or a suspect camera. Van Houten and Geradts (2009) also noted PRNU is present in all images / videos created by CCD or CMOS active pixel sensors and cannot be removed by a layman. Furthermore, CCD and CMOS image sensors are present in a wide range of electronic devices including:

- mobile phones,
- webcams,
- photo camera,
- video cameras, and

- image scanners [18].

Sensor pattern noise approach for camera identification. Multiple researchers have conducted studies into sensor pattern noise. However, Lukas, Fridrich, and Goljan (2006) offered a sensor pattern noise extraction filter and approach that has illustrated a high degree of reliability in detecting forged images based upon PRNU. Lukas et al., (2006) research also looked at the stability of sensor pattern noise over the course of a short period of time (one to two years) and noted it to be fairly stable [41][42].

Sensor pattern noise in videos from YouTube for camera identification. Other researchers have continued to build upon the concepts of sensor pattern noise for camera identification. Van Houten and Geradts (2009) used Lukas et al., (2006) approach to expand on source camera identification while focusing on identification of video cameras from multiple compressed videos collected from YouTube. Van Houten and Geradts (2009) noted by extracting and comparing the sensor noise patterns they could identify the source camera even after the video was uploaded to YouTube where the added layer of compression further degraded the sensor noise. Their research indicated they were able to correctly identify the source camera even after two or three layers of compression was applied. Van Houten and Geradts (2009) also identified limitations to their approach. The limitations included changing aspect ratio or resizing the input video was detrimental to sensor noise and this could prevent accurate identification [18].

Table 11 - Source Video Camera Identification Using PRNU Detection Method For Authentication Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
PRNU Detection Method For Camera ID	No	No	No	Yes	Yes	[18][41][42]

G-PRNU & Resizing Images For Camera Identification.

Al-Athamneh, Kurugollu, Crookes, and Farid (2018) noted in their research that after an exposure time of 0.15 seconds the green channel is the noisiest channel among the three colors of RGB. As a result of their research, they proposed a new method for digital video source identification focusing on the green channel of PRNU [43].

Al-Athamneh et al., (2018) research included resizing the images to 512x512 as a standard size. However, they also conducted research into the best interpolation method and resize dimension for use in their proposed method [43]. Their research results in this area are presented in the following table.

Table 12 - Source Camera Successful Identification Rates Using Different Interpolations & Dimensions [43]

Interpolation	Dimension				
	64x64	128x128	256x256	512x512	640x640
Bicubic	76.51	82.53	88.55	92.77	92.17
Bilinear	72.29	82.53	87.35	99.15	93.37
Nearest	71.69	80.72	85.96	88.55	79.52

Al-Athamneh et al., (2018) research indicated bilinear at 512x512 offered the most optimal settings for use of their proposed method [43].

Al-Athamneh et al., (2018) also tested using 2-D correlation coefficient detection to identify the source of each of the 236 test videos versus matching with six video references using PRNU, Green-PRNU (G-PRNU) only, and using G-PRNU interpolated by resized 512x512 bilinear interpolations. They used six different cameras with both CMOS and CCD sensors with movies in .MOV, .AVI, and .MP4 formats [43]. The results of the source camera identification rates reported by Al-Athamneh et al., (2018) are presented in the following table.

Table 13 - Source Camera Identification Rates [43]

Camera	PRNU	G-PRNU	G-PRNU With Bilinear Interpolation
C1	15%	97.5%	100%
C2	36.58%	95.12%	97.56%
C3	25.8%	96.77%	97.56%
C4	37.83%	100%	100%
C5	26.47%	100%	100%
C6	95.34%	97.67%	100%
Total Average	41.15%	97.79%	99.15%

Al-Athamneh et al., (2018) research indicated using G-PRNU with bilinear interpolation could correctly determine the source of 234 videos with a correct detection rate of 99.15% [43].

Al-Athamneh et al., (2018) proposed method is noted below:

1. Extract the green channel frames from the video (350 frames per video).
2. Resize the extracted frames to 512x512 using bilinear interpolation.
3. Perform wavelet-based de-noising on the green channel frames.
4. Create the G-PRNU map for the video by averaging the results of step 3.
5. Create a reference by performing steps 1-4 on 9 videos captured by the same camera.
6. Use 2-D correlation coefficient as the camera detection test [43].

Table 14 - G-PRNU & Image Resize For Camera Identification Detection Method For Authentication Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
G-PRNU & Image Resize For Camera ID	No	No	No	Yes	Yes	[43]

Block Level Manipulation Detection Method

Hsu, Hung, Lin, and Hsu (2008) proposed in their research the use a temporal correlation of block level pattern noise to locate tampered regions of videos. Their method used models

based upon the distribution of temporal sensor noise correlation values of video blocks in tampered regions and normal regions by using a Gaussian mixture model (GMM). Hsu et al., (2008) initially subtract the original frame from the noise-free version, using a wavelet denoising filter, to obtain the sensor pattern noise of each frame. Their method subsequently partitions each video frame into non-overlapping blocks of size $N \times N$. Hsu et al., (2008) then correlate the noise residuals between the same spatially indexed block of two successive frames. Their method then locates the tampered blocks by analyzing the statistical properties of block-level PRNU correlations [44].

Table 15 - Block Level Manipulation Detection Method For Authentication Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
Block Level Manipulation Detection	No	No	Yes	No	No	[44]

Pixel Level Manipulation Detection Method

Li, Wang, and Xu (2018) proposed in their research to use a 2D phase congruency with correlation coefficient analysis of adjacent frames to detect pixel tampering. Li et al., (2018) proposed method measures the inter-frame continuity of the content of each frame. This method may be applied in a global analysis and local analysis [45].

Table 16 - 2D Phase Congruency CC Detection Method For Authentication Relevance

Method / Technique	Global Analysis	Local Analysis		Device Identification (Characteristics)		References
		Temporal	Spatial	Class	Individual	
2D Phase Congruency Correlation Coefficient Analysis	Yes	Yes	No	No	No	[45]

Testing of Methods & Proposed Framework

The following section offers case studies of use of the proposed digital video authentication framework.

Adding New Method To Video Authentication Toolbox – Case Study 1

Case Study 1 illustrates the use of the proposed method evaluation tool for the forensic video examiner to validate a new method for their methodology toolbox. The process includes examiner validation of the proposed method.

The method evaluation tool report addressed the potential use of multimedia stream hash validation method [20][65]. The evaluation contained two tests or assessments. The first test was a validation test using SWGDE tool validation testing guidance [23]. The second test or assessment was a admissibility assessment of the proposed method.

The method validation testing assessed the proposed multimedia stream hash validation method for the following:

- 1) reproducibility, repeatability, accuracy, and precision.
- 2) use for intended purpose, and
- 3) method performance as expected.

The test involved to test scenarios. The specific tests involved the following steps.

- 1) Hash multimedia streams (both audio and video) in test data set. This is test preparation and establishes the original hashes for subsequent comparison.
- 2) Forensically copy each test data set's audio stream to a wave PCM audio digital multimedia file. Test scenario #1.
- 3) Hash the audio stream in each derivative wave PCM audio digital multimedia file. Test scenario #1.

- 4) Analyze results of test scenario #1.
- 5) Forensically copy each test data set's video stream to a lossless MP4 digital multimedia file. Test scenario #2
- 6) Hash the video stream in each derivative lossless MP4 digital multimedia file. Test scenario #2.
- 7) Analyze results of test scenario #2.

The admissibility assessment evaluated the following:

- 1) Has the method been tested?
- 2) Has the technique / method been subjected to peer review & publication?
- 3) What is the error rate of the theory or is an error mitigation method implemented?
- 4) Is the technique / method accepted in the forensic science community?
- 5) What are the standards controlling the use of the technique / method?

The test results demonstrated that multimedia stream hash validation method, as it relates to video and audio streams, was a viable method for use in video authentication process when transcoding video and audio streams for further authentication. The method was added to the video authentication method toolbox of the author for use within the limitations noted in the method validation testing report. See Appendix B for case study 1.

Clone Alteration Test Videos – Case Study 2

Clone alterations, or copy and pasting one region of a frame to another to the same or different region across multiple frames, is a very popular method to add or remove people or objects to a video with the intent to manipulate the viewer perspective. This cases study focuses on this type of manipulation where the goal is to change how the viewer would interpret imaged events from how they actually happened. See Appendix C for case study 2.

Case study #2 involved testing the proposed video authentication framework against four videos known to have local clone alterations. The test videos were the same videos used by Hsu et al., (2008) in their block level manipulation detection paper. All four videos had local clone alterations. One video also used an example-based texture synthesis technique along with the clone technique. In addition, one of the videos involved a panning camera while using the clone technique to remove a person walking in one direction and a car passing in the background in the opposite direction [44].

Examination of all four test videos (known to have tampered regions) using the proposed video authentication framework revealed the file structure analysis detected the alteration of the videos with a known video processing tool. The framework would have allowed the forensic video examiner to opt out of detecting the precise tampering regions by using the workflow optimization option. However, the tests were designed to continue without using the workflow optimization options. Further examination of all four video streams resulted in accurate and precise detection of the regions within each frame of all four videos.

Text Video #1 Frame Tampering Summary

See figure below for test video #1 validation of test results.

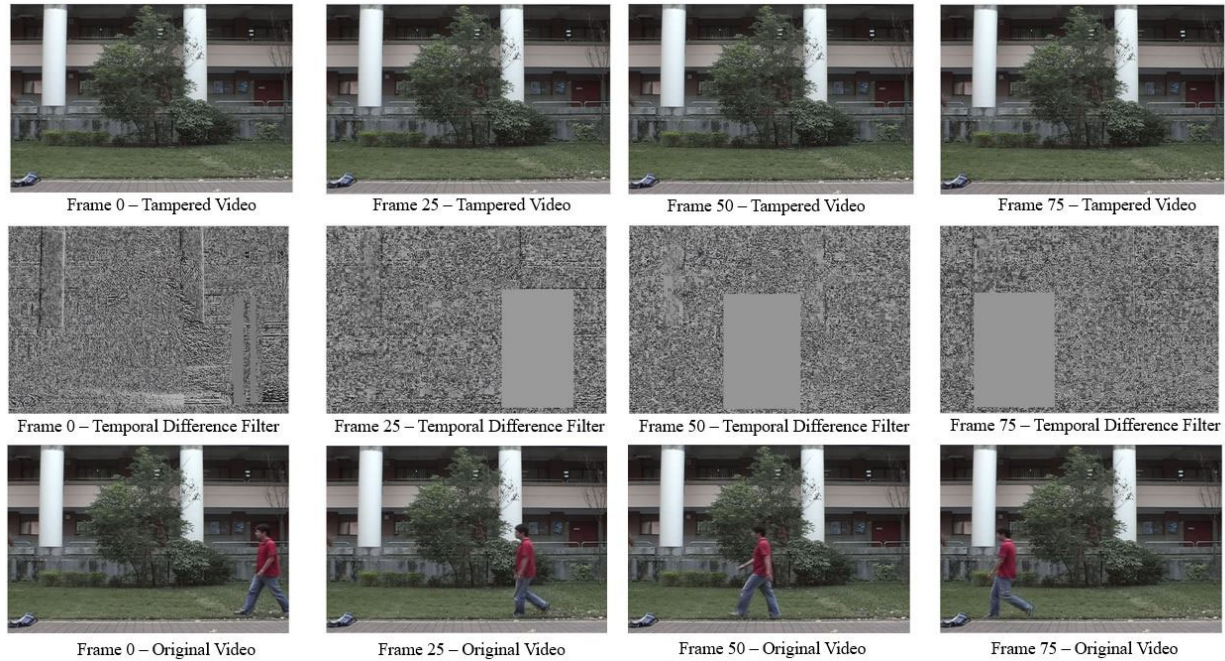


Figure 11 - Case Study 2 Test 1 Test Validation Results

Figure above provides a summary of Frames 0, 25, 50, & 100 from test video 1. The top row presents the respective frame contents visually for the tampered video. The middle row contains the respective frames after a temporal difference filter was applied to each video. Each of the middle row frames contain greyish boxes for the clone altered regions. The bottom row of the figure offers the respective frame contents from the original video and shows the person walking who was removed from the video frames in the tampered video in the top row. The middle row detected tampered regions directly correlates to the original video frames of the person walking.

Text Video #2 Frame Tampering Summary

See figure below for test video #2 validation of test results.

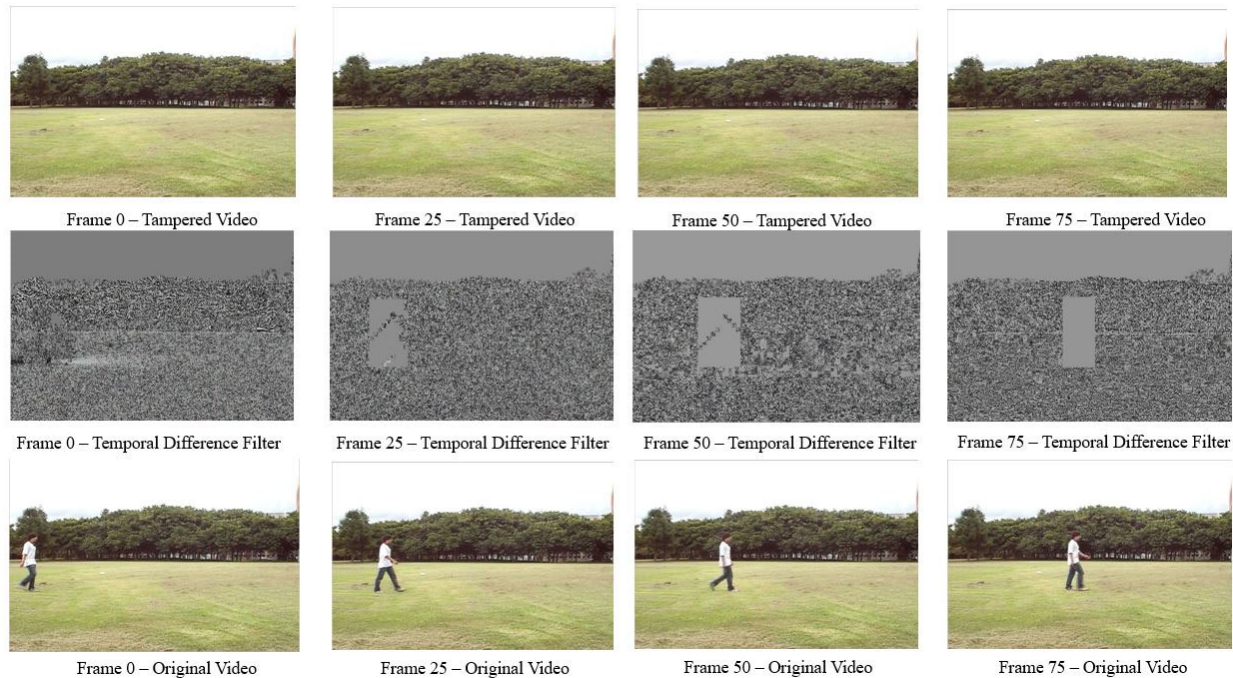


Figure 12 - Case Study 2 Test 2 Test Validation Results

Figure above provides a summary of Frames 0, 25, 50, & 100 from test video 2. The top row presents the respective frame contents visually for the tampered video. The middle row contains the respective frames after a temporal difference filter was applied to each video. Each of the middle row frames contain greyish boxes for the clone altered regions. The bottom row of the figure offers the respective frame contents from the original video and shows the person walking who was removed from the video frames in the tampered video in the top row. The middle row detected tampered regions directly correlates to the original video frames of the person walking.

Text Video #3 Frame Tampering Summary

See figure below for test video #3 validation of test results.

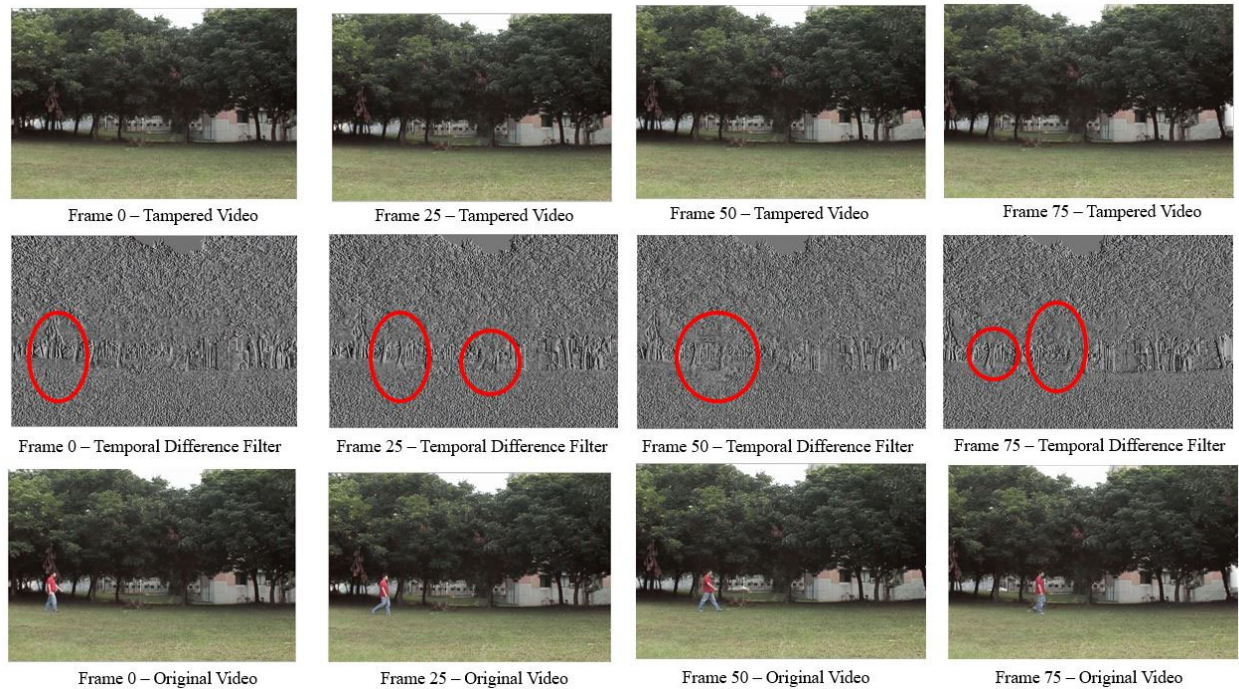


Figure 13 - Case Study 2 Test 3 Test Validation Results

Figure above provides a summary of Frames 0, 25, 50, & 100 from test video 3. The top row presents the respective frame contents visually for the tampered video. The middle row contains the respective frames after a temporal difference filter was applied to each video. Each of the middle row frames contain red circles highlighting differences in the greyish areas for the clone altered regions. The bottom row of the figure offers the respective frame contents from the original video and shows the person walking who was removed from the video frames in the tampered video in the top row. The middle row tampered regions directly correlates to the original video frames of the person walking. A major difference in this test from the other tests in case study #2 was that the camera was panning right while one tampered region of interest moved with the camera panning right and a smaller background entity moved across the screen to the left. The camera movement caused the temporal differences filter to present the examiner much less contrast in the detected tampered regions than found in fixed camera positioning text videos (1, 2, & 4).

Text Video #4 Frame Tampering Summary

See figure below for test video #4 validation of test results.

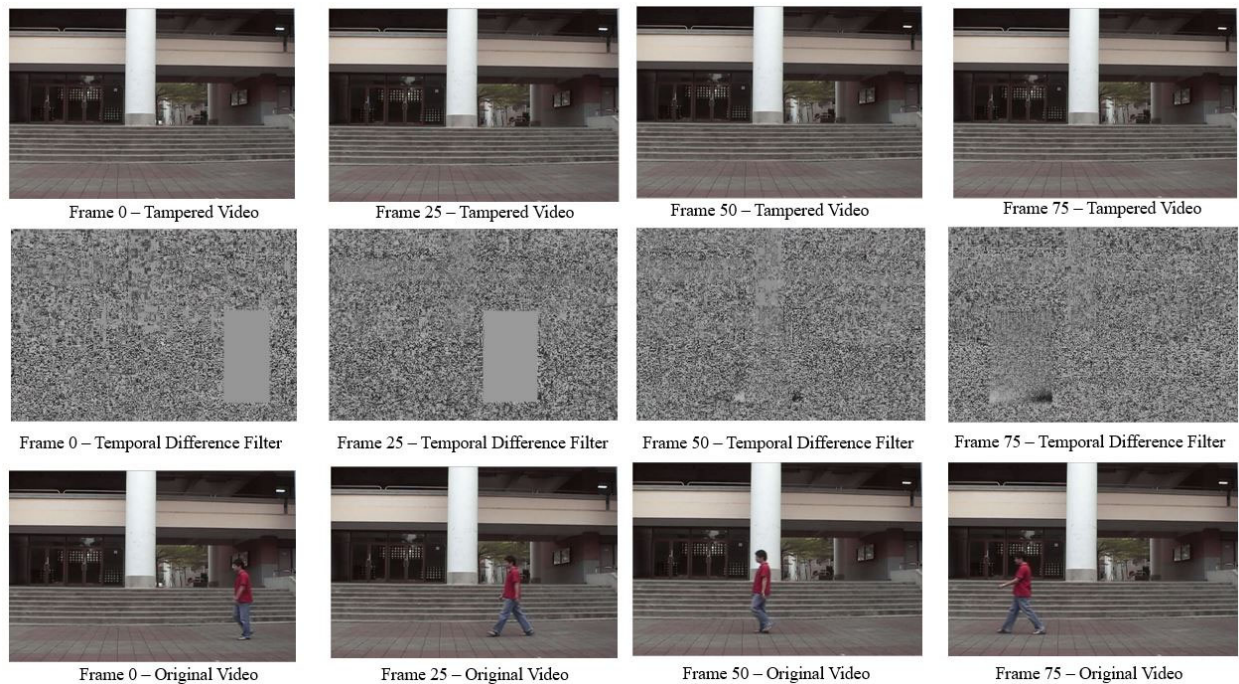


Figure 14 - Case Study 2 Test 4 Test Validation Results

Figure above provides a summary of Frames 0, 25, 50, & 100 from test video 2. The top row presents the respective frame contents visually for the tampered video. The middle row contains the respective frames after a temporal difference filter was applied to each video. Each of the middle row frames contain greyish boxes for the clone altered regions. The bottom row of the figure offers the respective frame contents from the original video and shows the person walking who was removed from the video frames in the tampered video in the top row. The middle row detected tampered regions directly correlates to the original video frames of the person walking.

Case Study #2 illustrates the framework may be used as a structured process for executing video authentication methods from a forensic video examiner's methodology toolbox for accurate and precise detection of video manipulation.

Axon Fleet 2 Camera Video – Case Study 3

Law enforcement today uses body cameras and video cameras mounted in their patrol vehicles to document events. Axon is a major provider of law enforcement video cameras. The cameras may be activated by the law enforcement officer to record an event, but Axon video cameras also have a pre-event buffer video recording of 30 seconds by default. The event recording and the pre-event recording are important to document all events at the scene. Both the pre-event buffer portion and the event portion of the video's integrity is important to the legal system to protect all parties. See Appendix D for case study 3.

Case study #3 tests the proposed video authentication framework against an Axon Fleet 2 camera video. Working copies of the video were edited to remove both a large amount of frames and a small amount of frames. The video editing occurred in both the pre-event buffer recording area and the event recording area to simulate someone tampering with the video to hide part of the overall event. Three test videos were created for case study #3.

Examination of the three test videos (known to have tampered / spliced regions) using the proposed video authentication framework revealed the file structure analysis detected the alteration of the videos with a known video processing tool. The framework would have allowed the forensic video examiner to opt out of detecting the precise tampered regions by using the workflow optimization option. However, the tests were designed to continue without using the workflow optimization options. Further examination of all three test video streams resulted in accurate and precise detection of the spliced areas of all three videos.

Test Video #1 Frame Tampering Summary

The first video had frames 600-700 deleted from the video using Adobe Premiere software. This area of tampering was the pre-event buffer area of the recording. The file structure analysis detected artifacts of Adobe Premiere software use.

Global analysis. A global analysis of the overall video file did not reveal any inconsistencies.

Local analysis. A temporal analysis of the video file revealed pixel level inconsistencies. See figure below for the results of the local analysis findings of pixel level irregularities.

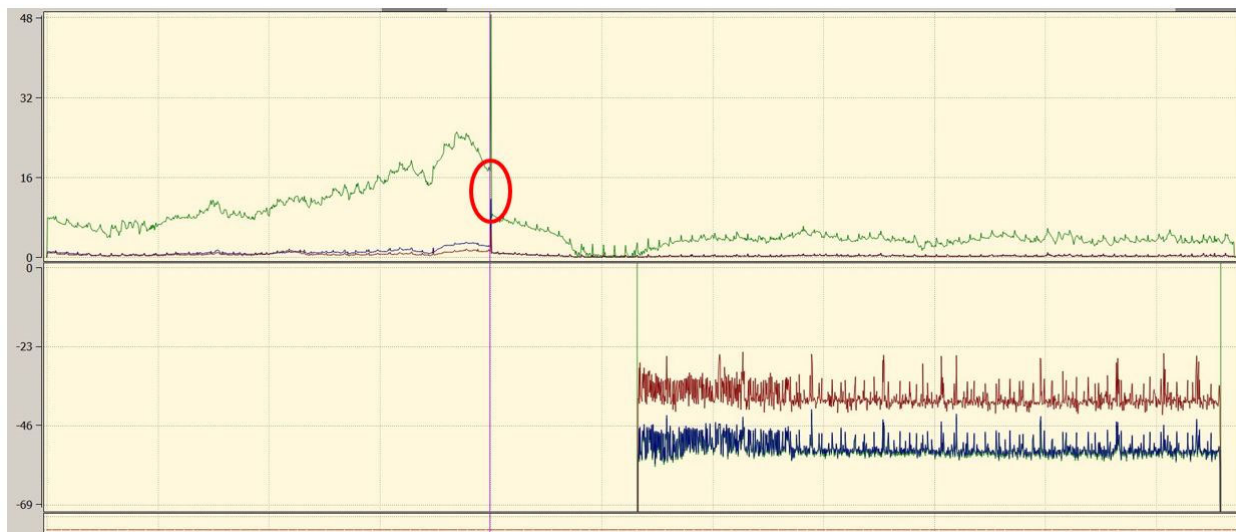


Figure 15 - Temporal Analysis of Y Plane Revealing Current Frame Versus Preceding Frame Differences

The figure above illustrates a temporal analysis of the Y plane of each current frame and the preceding frame which revealed a major visual change from one frame to the next between frame 598 and frame 600.

The local analysis also included a visual content analysis. See figure below for the results of the local analysis's visual content analysis.

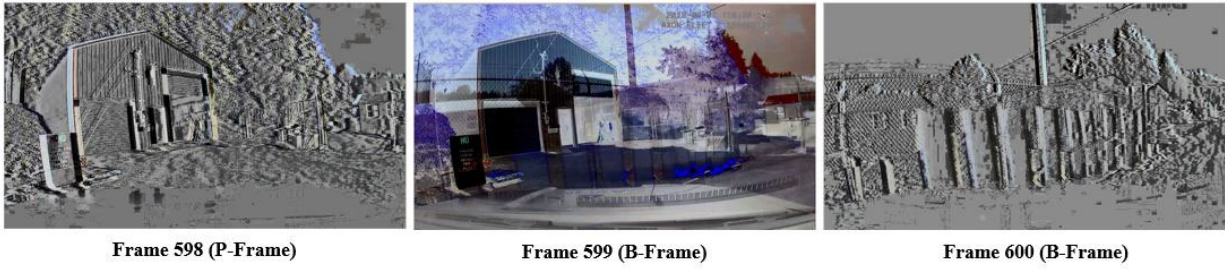


Figure 16 - Comparison of Frame 598, 599, & 600 Visual Content Using Temporal Difference Filter

Visual analysis of frames 598, 599, & 600 using a temporal difference filter between frames revealed a significant visual change at frame 599 as noted above.

In addition, see figure below for local pixel analysis results.

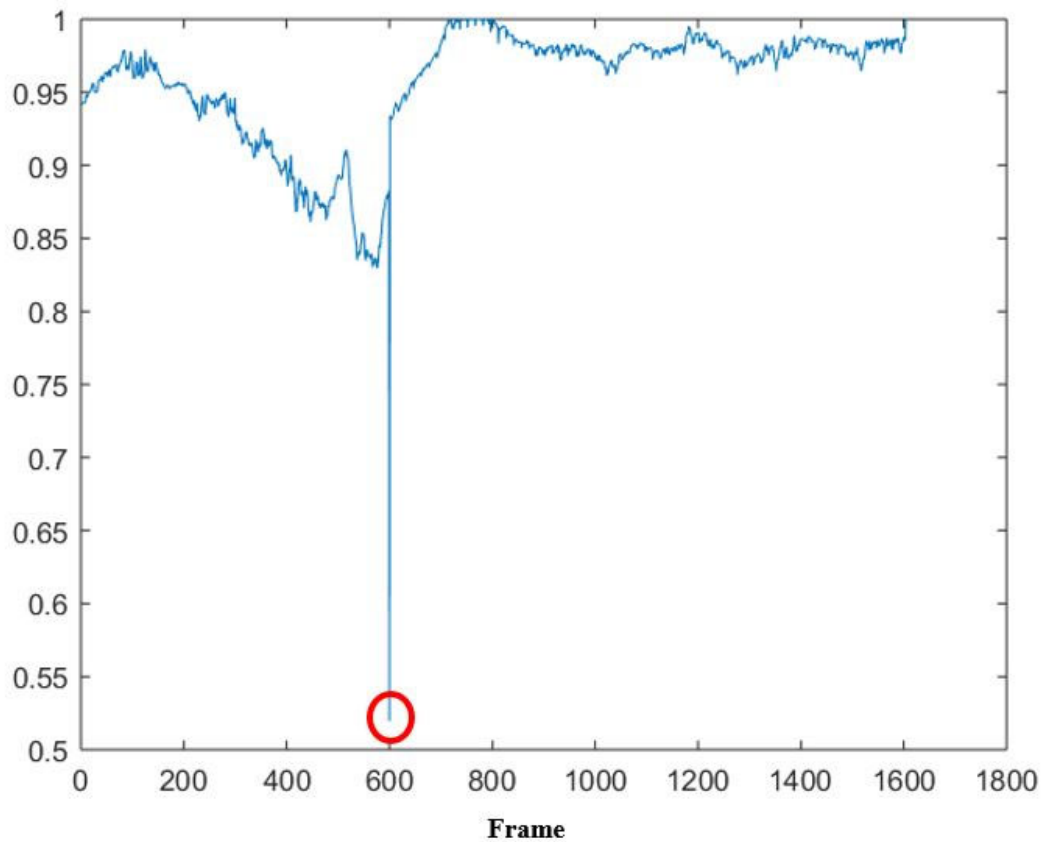


Figure 17 - 2D Phase Congruency With Correlation Coefficient of Adjacent Frames

Figure above illustrates the results of using 2D phase congruency with correlation coefficient on adjacent frames of the video. The noted spike in the histogram at frame 599 in the

video was the same location as noted in the local pixel level analysis and visual anomaly analysis noted above.

Test Video #2 Frame Tampering Summary

Test video #2 had only two frames deleted from the video using Adobe Premiere software. This area of tampering was in the event area of the recording. Frames 1075 and 1076 were removed from the video stream. A file structure analysis of the edited video detected artifacts of Adobe Premiere software use.

Global analysis. A global analysis of the overall video file did not reveal any inconsistencies.

Local analysis. A temporal analysis of the video file did not revealed pixel level inconsistencies. See figure below for the results of the local analysis findings of pixel level irregularities.



Figure 18 - Temporal Analysis of Y Plane Revealing Current Frame Versus Preceding Frame

Differences

The figure above illustrates a temporal analysis of the Y plane of each current frame and the preceding frame. The subtle differences in the video between frame 1074 and 1076 were not detected in this analysis as noted in Figure 16 above.

Local analysis. A local analysis included visual content analysis. See figure below for the results of the local analysis' visual content analysis.



Frame 1074



Frame 1075

Figure 19 - Comparison of Frame 1074 & 1075 Visual Content

Visual inconsistencies were very minor when comparing frame 1074 to 1075. Two frames were removed, but without the local pixel manipulation analysis in Figure 18 below the subtle inconsistency would probably be undetected. See figure below for local pixel analysis results.

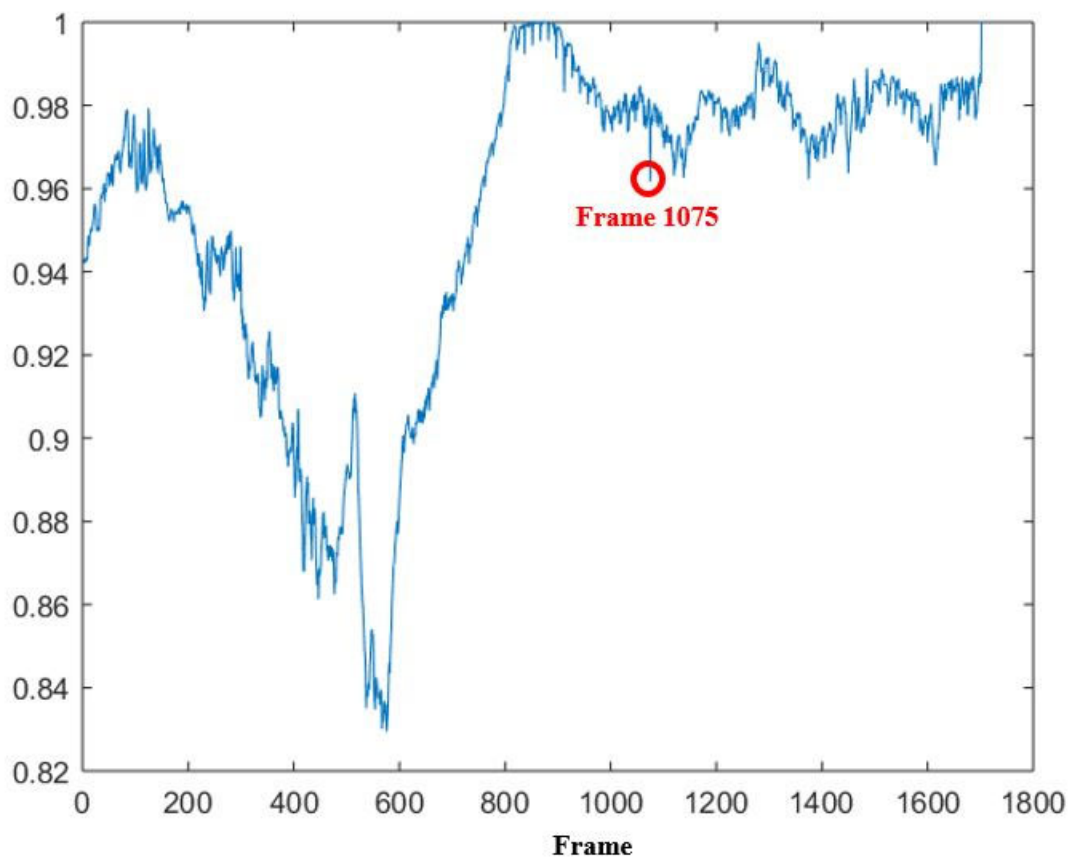


Figure 20 - 2D Phase Congruency With Correlation Coefficient of Adjacent Frames

Figure above illustrates the results of using 2D phase congruency with correlation coefficient on adjacent frames of the video. The analysis detected a spike in the histogram at frame 1075 consistent with the tampered area of the video.

Test Video #3 Frame Tampering Summary

Test video #3 had the entire pre-event buffer recording deleted from the video using Shortcut, an open source video editing software. This resulted in only the event area of the recording present in the tampered video. The file structure analysis revealed the presence of Lavf58.20.100 encoder rather than the Ambarella Advanced Video Coding noted in original video from Axon fleet 2 cameras.

Global analysis. A global analysis of the overall video file did not reveal any inconsistencies.

Local analysis. A local analysis included visual content analysis. The visual content analysis revealed no inconsistencies in the frames, but noticeably absent was the pre-event buffer video stream that contains 30 seconds of default video content prior to law enforcement officer activating the camera to record the event. In addition, 2D phase congruency with correlation coefficient on adjacent frames of the video revealed no alterations.

Case Study #3 illustrates the framework may be used as a structured process for executing video authentication methods from a forensic video examiner's methodology toolbox for accurate and precise detection of video manipulation.

Proposed Framework Overall Test Results

Testing of the proposed framework in video authentication of known data sets has produced results consistent with test hypotheses. Testing has illustrated the framework may be used as a structured process for executing video authentication methods from a forensic video examiner's methodology toolbox for accurate and precise detection of video manipulation.

CHAPTER VI

CONCLUSION

The proposed framework offers a structured approach to assess and use forensic science community accepted video and audio authentication methods. The proposed framework incorporates methods or techniques that are evaluated for reproducibility, repeatability, accuracy, and precision while meeting the general legal requirements recognized by courts in the International community, U.S., and many countries around the world.

The framework has a built in methodology evaluation tool. The methodology evaluation tool includes a methodology validation assessment and a legal assessment to aid the user in determining if a proposed method should be included or excluded from use as part of the specific framework protocol for each video file considered for authentication. Testing of the proposed framework assessment processes and use in video authentication of known data sets has produced results consistent with test hypotheses. And the proposed framework offers the forensic video examiner a methodology to assess published video and audio authentication techniques recognized in the forensic science community while using generally accepted criteria to test and evaluate the techniques as expected by the courts.

However, there are limitations. Acceptance of the proposed framework for video authentication by the courts will always be based upon a case by case basis dependent upon each cases facts, proper use of the scientific methods, and the overall experience, training, and knowledge of the forensic video examiner who testifies as an expert. The proposed framework is intended for digital video and not applicable to analog video. New methods that are developed in the deep learning and computer vision communities may be incorporated into new methods.

REFERENCES

- [1] Saferstein, R. (2007). *Criminalistics: an introduction to forensic science* (9th ed.). Upper Saddle River, NJ: Prentice Hall.
- [2] Casey, E. (2000). *Digital Evidence and Computer Crime* (1st ed.). London: Academic Press.
- [3] Legal Information Institute Staff - Cornell Law School. (2011, December 01). Rule 401. Test for Relevant Evidence. Retrieved December 5, 2018, from https://www.law.cornell.edu/rules/fre/rule_401
- [4] Legal Information Institute Staff - Cornell Law School. (2011, December 05). Rule 901. Authenticating or Identifying Evidence. Retrieved December 5, 2018, from https://www.law.cornell.edu/rules/fre/rule_901
- [5] Scientific Working Group on Digital Evidence (SWGDE). (2016, June 3). *SWGDE Digital & Multimedia Evidence Glossary*, v 3. Retrieved January 8, 2019, from <https://www.swgde.org/documents/Current Documents/SWGDE Digital and Multimedia Evidence Glossary>.
- [6] Fowler, G. A. (2018, October 18). *I fell for Facebook fake news. Here's why millions of you did, too*. Retrieved January 8, 2019, from https://www.washingtonpost.com/technology/2018/10/18/i-fell-facebook-fake-news-heres-why-millions-you-did-too/?utm_term=.464a38303f84
- [7] YouTube Video From MeniThings. (2017, June 14). *Extreme Crosswind | Airliner spins 360*. Retrieved January 8, 2019, from <https://youtu.be/AgvzhJpyn10>
- [8] YouTube Video From Jeff Smith. (2018, December 23). *No Title*. Retrieved January 9, 2019, from <https://youtu.be/B0ZG9IUCD3k>
- [9] Apple Inc. (2018, November 08). Using HEIF or HEVC media on Apple devices. Retrieved January 10, 2019, from <https://support.apple.com/en-us/HT207022>
- [10] Apple Inc. (2018, September 19). Take and edit Live Photos. Retrieved January 9, 2019, from <https://support.apple.com/en-us/HT207310>
- [11] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993).
- [12] Oxford University Press. (n.d.). Scientific method | Definition of scientific method in English by Oxford Dictionaries. Retrieved January 13, 2019, from https://en.oxforddictionaries.com/definition/scientific_method

- [13] Scientific Working Group Digital Evidence. (2018, November 20). SWGDE Establishing Confidence in Digital and Multimedia Evidence Forensic Results by Error Mitigation Analysis. Retrieved January 19, 2019, from <https://swgde.org/documents/Current Documents/SWGDE Establishing Confidence in Digital Forensic Results by Error Mitigation Analysis>
- [14] Gow, R. D., Renshaw, D., Findlater, K., Grant, L., McLeod, S. J., Hart, J., & Nicol, R. L. (2007). A comprehensive tool for modeling CMOS image-sensor-noise performance. *IEEE Transactions on Electron Devices*, 54(6), 1321-1329. doi:10.1109/TED.2007.896718.
- [15] Irie, K., McKinnon, A. E., Unsworth, K., & Woodhead, I. M. (2008). A model for measurement of noise in CCD digital-video cameras. *Measurement Science and Technology*, 19(4), 045207. doi:10.1088/0957-0233/19/4/045207.
- [16] Irie, K., McKinnon, A. E., Unsworth, K., & Woodhead, I. M. (2008). A technique for evaluation of CCD video-camera noise. *IEEE Transactions on Circuits and Systems for Video Technology*, 18(2), 280-284.
- [17] Hytti, H. T. (2006, January). Characterization of digital image noise properties based on RAW data. In *Image Quality and System Performance III* (Vol. 6059, p. 60590A). International Society for Optics and Photonics.
- [18] Van Houten, W., & Geradts, Z. (2009). Source video camera identification for multiply compressed videos originating from YouTube. *Digital Investigation*, 6(1), 48-60. doi:10.1016/j.diin.2009.05.003
- [19] Ishida, H., Kagawa, K., Komuro, T., Zhang, B., Seo, M., Takasawa, T., Kawahito, S. (2018). Multi-aperture-based probabilistic noise reduction of random telegraph signal noise and photon shot noise in semi-photon-counting complementary-metal-oxide-semiconductor image sensor. *Sensors (Basel, Switzerland)*, 18(4), 977. doi:10.3390/s18040977
- [20] Whitecotton, C. M. (2017). *YouTube: Recompression Effects*. University of Colorado at Denver.
- [21] Grigoros, C. (2017). *Forensic Audio Authentication*. Retrieved from University of Colorado Denver Canvas - Forensic Audio Analysis course material.
- [22] Grigoros, C., Rappaport, D., and Smith, J. (2012). *Analytical Framework for Digital Audio Authentication*. Presented at AES 46th International Conference.
- [23] Scientific Working Group Digital Evidence. (2014, September 5). SWGDE Recommended Guidelines for Validation Testing, V2. Retrieved February 5, 2019, from <https://www.swgde.org/documents/Current Documents/SWGDE Recommended Guidelines for Validation Testing>

- [24] Rappaport, D. L. (2012). *Establishing a standard for digital audio authenticity: A critical analysis of tools, methodologies, and challenges*. University of Colorado at Denver.
- [25] Scientific Working Group Digital Evidence. (2018, September 20). SWGDE Best Practices for Digital Audio Authentication v 1.3. Retrieved February 8, 2019, from <https://www.swgde.org/documents/Current Documents/SWGDE Best Practices for Digital Audio Authentication>
- [26] Anderson, S. D. (2011). *Digital image analysis: Analytical framework for authenticating digital images* (University of Colorado Denver).
- [27] Grigoros, C., & Smith, J. (2013, February 21). Digital Imaging: Enhancement and Authentication. Retrieved from <https://www.sciencedirect.com/science/article/pii/B9780123821652001276>
- [28] Wolanin, J. E. (2018). *ANALYSIS OF FACEBOOK'S VIDEO ENCODERS* (University of Colorado at Denver).
- [29] Lawson, M. (2017). *A Forensic Analysis of Digital Image Characteristics Associated to Flickr and Google Plus* (University of Colorado Denver).
- [30] Giammarrusco, Z. P. (2014). *Source identification of high definition videos: A forensic analysis of downloaders and YouTube video compression using a group of action cameras*. University of Colorado at Denver.
- [31] Hall, J. R. (2015). *MPEG-4 video authentication using file structure and metadata* (University of Colorado Denver).
- [32] B.E. Koenig and D.S. Lacey, "Forensic Authentication of Digital Audio Recordings." J. Audio Eng. Soc., Vol 57, No. 9, 2009 Sept.
- [33] Wang, W., & Farid, H. (2007, September). Exposing digital forgeries in video by detecting duplication. In *Proceedings of the 9th workshop on Multimedia & security* (pp. 35-42). ACM.
- [34] Farid, H. (2006). Digital doctoring: How to tell the real from the fake. *Significance*, 3(4), 162-166. doi:10.1111/j.1740-9713.2006.00197.
- [35] Johnson, M., & Farid, H. (2005). Exposing digital forgeries by detecting inconsistencies in lighting. Paper presented at the 1-10. doi:10.1145/1073170.1073171
- [36] Bestagini, P., Milani, S., Tagliasacchi, M., & Tubaro, S. (2013). Local tampering detection in video sequences. Paper presented at the 488-493. doi:10.1109/MMSP.2013.6659337

- [37] Wang, W., & Farid, H. (2007). Exposing digital forgeries in interlaced and deinterlaced video. *IEEE Transactions on Information Forensics and Security*, 2(3), 438-449. doi:10.1109/TIFS.2007.902661
- [38] Wang, W., & Farid, H. (2006, September). Exposing digital forgeries in video by detecting double MPEG compression. In *Proceedings of the 8th workshop on Multimedia and security*(pp. 37-47). ACM.
- [39] Wang, W., & Farid, H. (2009, September). Exposing digital forgeries in video by detecting double quantization. In *Proceedings of the 11th ACM workshop on Multimedia and security* (pp. 39-48). ACM.
- [40] Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, 53(10), 3948-3959. doi:10.1109/TSP.2005.855406
- [41] Lukáš, J., Fridrich, J., & Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2), 205-214. doi:10.1109/TIFS.2006.873602
- [42] Lukáš, J., Fridrich, J., & Goljan, M. (2006). Detecting digital image forgeries using sensor pattern noise. Paper presented at the , 6072(1) 60720Y-60720Y-11. doi:10.1117/12.640109
- [43] Al-Athamneh, M., Kurugollu, F., Crookes, D., & Farid, M. (2016). Digital video source identification based on green-channel photo response non-uniformity (G-PRNU).
- [44] Hsu, C. C., Hung, T.Y., Lin, C. W., & Hsu, C. T. Video forgery detection using sensor pattern noise. In 2008 21th Conference on Computer Vision, Graphics and Image Processing.
- [45] Li, Q., Wang, R., & Xu, D. (2018). An Inter-Frame Forgery Detection Algorithm for Surveillance Video. *Information*, 9(12), 301.
- [46] *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534 (D.Md. May 4, 2007)
- [47] Grimm, P. W., Ziccardi, M. V., & Major, A. W. (2009). Back to the future: *Lorraine v. Markel American Insurance Co.* and new findings on the admissibility of electronically stored information. *Akron L. Rev.*, 42, 357.
- [48] UNITED STATES OF AMERICA, v. KENNETH PETTWAY, JR., Defendant., 2018 U.S. Dist. LEXIS 176848, 2018 WL 4958962 (United States District Court for the Western District of New York October 15, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5TGW-F2W1-FGCG-S01B-00000-00&context=1516831>.

- [49] UNITED STATES OF AMERICA, Plaintiff - Appellee, v. MATTHEW LANE DURHAM, Defendant - Appellant., 902 F.3d 1180, 2018 U.S. App. LEXIS 24546 (United States Court of Appeals for the Tenth Circuit August 29, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5T4V-BCT1-JFDC-X4XW-00000-00&context=1516831>.
- [50] VIRGINIA NESTER, Individually and As Next Friend of C.N. and S.N., minors; ROBERT SCOTT NESTER, Individually and As Next Friend of C.N. and S.N., minors, Plaintiffs - Appellees v. TEXTRON, INCORPORATED, doing business as E-Z-GO, Defendant - Appellant, 888 F.3d 151, 2018 U.S. App. LEXIS 9783, CCH Prod. Liab. Rep. P20,339, 2018 WL 1835816 (United States Court of Appeals for the Fifth Circuit April 18, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5SAK-8MM1-JJSF-20C2-00000-00&context=1516831>.
- [51] MARIO COSTELLO, Petitioner, -against- THOMAS GRIFFIN, Superintendent, Greenhaven Correctional Facility, Respondent., 2018 U.S. Dist. LEXIS 202412 (United States District Court for the Eastern District of New York November 28, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5TVD-5YY1-JFDC-X4M1-00000-00&context=1516831>.
- [52] JOSE RAYMOND COLON, Petitioner, v. SECRETARY, DEPARTMENT OF CORRECTIONS, Respondent., 2018 U.S. Dist. LEXIS 152747, 2018 WL 4281466 (United States District Court for the Middle District of Florida, Tampa Division September 7, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5TS-RTM1-JFSV-G391-00000-00&context=1516831>.
- [53] MARY A. GILMORE VERSUS SPRINGHILL MEDICAL CENTER, 2018 U.S. Dist. LEXIS 75327, 2018 WL 2069728 (United States District Court for the Western District of Louisiana, Shreveport Division May 3, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5SP-FW21-JP9P-G4NY-00000-00&context=1516831>.
- [54] UNITED STATES OF AMERICA v. JOSHUA MOSES, 2018 U.S. Dist. LEXIS 12030 (United States District Court for the Eastern District of Pennsylvania January 25, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5RGT-8PG1-JWJ0-G20K-00000-00&context=1516831>.
- [55] STEVEN KLEIN, Petitioner, v. NEIL MCDOWELL, warden, Respondent., 2018 U.S. Dist. LEXIS 196069, 2018 WL 6018208 (United States District Court for the Southern

- District of California November 16, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5T-RT-BWM1-JT42-S12G-00000-00&context=1516831>.
- [56] MARCUS SIMPSON, Plaintiff, and MICHAEL GLOVER, Plaintiff-Appellant, v. VILLAGE OF LINCOLN HEIGHTS, et al., Defendants-Appellees., 2018 U.S. App. LEXIS 13240 (United States Court of Appeals for the Sixth Circuit May 21, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5S-CP-1J61-FFMK-M0M6-00000-00&context=1516831>.
 - [57] UNITED STATES OF AMERICA v. CHARLES STAGNER, Defendant., 2018 U.S. Dist. LEXIS 105617 (United States District Court for the Southern District of Alabama, Southern Division June 25, 2018, Filed). Retrieved from <https://advance-lexis-com.aurarialibrary.idm.oclc.org/api/document?collection=cases&id=urn:contentItem:5S-N0-Y0D1-F900-G0CT-00000-00&context=1516831>.
 - [58] Laurel E. Fletcher, Chris Jay Hoofnagle, Eric Stover, Jennifer Urban, et al.. "Working Paper: An Overview of the Use of Digital Evidence in International Criminal Courts, Salzburg Workshop on Cyber Investigations" *Salzburg Workshop on Cyberinvestigations* (2013) Available at: http://works.bepress.com/laurel_fletcher/41/
 - [59] Laurel E. Fletcher, Chris Jay Hoofnagle, Eric Stover, Jennifer Urban, et al.. "Working Paper: Digital Evidence: Investigatory Protocols" *Salzburg Workshop on Cyberinvestigations* (2013) Available at: http://works.bepress.com/laurel_fletcher/43/
 - [60] National Forensic Science Technology Center. (n.d.). Forensic Evidence Admissibility & Expert Witnesses. Retrieved January 10, 2019, from <http://www.forensicsciencesimplified.org/legal/702.html>
 - [61] *General Electric Co. v. Joiner*, 522 U.S. 136, 118 S. Ct. 512, 139 L. Ed. 2d 508 (1997).
 - [62] *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 119 S. Ct. 1167, 143 L. Ed. 2d 238 (1999).
 - [63] Legal Information Institute Staff - Cornell Law School. (2011, December 01). Rule 702. Testimony by Expert Witnesses. Retrieved January 12, 2019, from https://www.law.cornell.edu/rules/fre/rule_702
 - [64] Knoops, G. J. A. (2009). The Proliferation of Forensic Sciences and Evidence before International Criminal Tribunals from a Defence Perspective. In *Criminal Law Forum* (pp. 1-28). Springer Netherlands.
 - [65] Warren, J., Clear, M., & McGoldrick, C. (2012, October). Metadata Independent Hashing for Media Identification & P2P Transfer Optimisation. In *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery* (pp. 58-65). IEEE.

- [66] Scientific Working Group Digital Evidence. (2018, November 20). SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics v 1.0. Retrieved March 22, 2019, from <https://swgde.org/documents/Released%20For%20Public%20Comment/SWGDE%20Best%20Practices%20for%20Mobile%20Device%20Evidence%20and%20Collection,%20Preservation,%20and%20Acquisition>.
- [67] Scientific Working Group Digital Evidence. (2018, November 20). SWGDE Technical Notes on FFmpeg v 2.0. Retrieved March 22, 2019, from <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Technical%20Notes%20on%20FFmpeg>

APPENDIX A

ADDITIONAL LEGAL INFORMATION

This appendix reviews the expectations for authentication of digital video found in case precedent and rules in both the U.S. federal and International courts. This chapter also provided a discussion of what is expected of expert witnesses who testify in U.S. federal and International courts. The information from these areas was then used to develop certain features of the proposed framework.

Authentication of Electronically Stored Information In U.S.

U.S. federal courts have addressed various areas of authentication of electronically stored information (ESI) that includes digital video. The *Lorraine v. Markel American Insurance Company* (241 F. R. D. 534 (D. Md. 2007)) (*Lorraine*) case is one of the leading comprehensive cases that address the complex aspects of evidential law and its applicability in ESI [46].

Lorraine v. Markel American Insurance Company

In *Lorraine* the court addressed the admission of ESI based upon the following:

- Relevance
- Authenticating Evidence
- Hearsay Evidence
- Evidence should be original or admissible duplicate
- Admissibility of Evidence (Probative Value).

The *Lorraine* court provided guidance on authenticating ESI. The court noted that in order for ESI to be admissible, the party offering the evidence “must produce evidence sufficient to support a finding that the item is what the proponent claims it is” as noted in U.S. Federal Rules of Evidence (FRE) 901(a).

The *Lorraine* case noted several precedent cases where courts excluded ESI because the proffering party did not properly offer sufficient evidence to support a finding that the ESI was what its proponents claimed. Although FRE 901(a) addresses the requirement for authentication, it does not address how to authenticate the evidence.

The *Lorraine* court noted that FRE 901(b) offered a non-exclusive list of methods for authentication. The *Lorraine* court offered additional guidance on how to authenticate ESI under FRE 901(b) that are directly relevant to this thesis and are discussed below.

It is important for the forensic scientist to understand how authentication methodology testimony may be offered to the court under the FRE. The forensic scientist may offer testimony to the trier of fact as an expert witness (FRE 901(b)(3)) based upon contents, substance and distinctive characteristics (FRE 901(b)(4)), or a description of the process to produce results (FRE 901(b)(9)).

This thesis focuses on the *Lorraine* decision as it relates to authenticating evidence; the requirement that evidence be original or an admissible duplicate; and the case guidance as it relates to a contested authenticity of proffered evidence.

Witness With knowledge

FRE 901(b)(1) allows “[t]estimony that a matter is what it is claimed to be” [4]. The *Lorraine* court clarified that this means a witness may testify with knowledge through “having participated in or observed the event reflected by the exhibit” [46].

Expert Witness

FRE 901(b)(3) allows “... comparison with an authenticated specimen by an expert witness or the trier of fact” [4]. The *Lorraine* court noted the “authenticated specimen” used by the expert witness may be authenticated by any means allowable under FRE 901 and FRE 902 and that

authentication is permitted based upon knowledge that an item is what it claimed to be as stated in FRE 901(b) (1) [46].

The court also clarified that the “knowledge” of the specimen (exemplar) may be obtained based upon first hand data (creating the specimen or observing the creation) and provide the forensic scientist a judicious approach to obtaining authenticated specimens (exemplars) [46].

Contents, Substance, & Distinctive Characteristics.

FRE 901(b)(4) allows exhibits to be authenticated by “... appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances” [4]. The *Lorraine* court provided three general areas of characteristics for authentication under FRE 901(b)(4): hash values, metadata, and other distinctive characteristics [46].

Hashing. Hashing is the application of a mathematical algorithm to digital data that results in a unique alpha numeric value that is a unique identifier of the digital data [46]. The recognition of hash values for authentication in the *Lorraine* case as it related to digital data hashes includes the hash of stream data found in digital video or audio files.

Metadata. Metadata is generally data, frequently embedded within a file, that may include file creation and /or modification dates and times, specific applications and hardware used to create the file, and specific storage locations. Many, but not all, multimedia files contain metadata that may be used for authentication.

The *Lorraine* court noted a third method of authenticating electronic evidence under FRE 901(b)(4) included other distinctive characteristics linked to email, text messages, and web pages [46]. The examples noted in *Lorraine* are analogous to file structure and format analysis, global and local analysis, and device identification of digital multimedia files. Specific illustrations of those examples are found in Chapter IV of this document.

Description of Process to Produce Results.

FRE 901(b)(9) allows authentication based upon “evidence describing a process or system and showing that it produces an accurate result” [4]. The *Lorraine* court noted this authentication method was specifically useful in authenticating electronically stored information created or generated by a computer [46].

Applicable Elements of FRE 1001 (Definitions That Apply to This Article) and FRE 1003 (Admissibility of Duplicates)

The *Lorraine* court restated the following definitions found in FRE 1001:

- Photographs – included still photographs, X-ray film, video tapes, and motion pictures.
- Original – An original of a photograph, if data stored in a computer or similar device, includes any printout or other output readable by sight and shown to reflect the data accurately.
- Duplicate – A counterpart product by the same impression as original or by same means as photography, including enlargements and miniatures, or by electronic re-recording, or by other equivalent techniques which accurately reproduces the original [46].

The *Lorraine* court also noted that FRE 1003 essentially allowed duplicates to be admissible unless there was an issue as to the authenticity of the original [46].

Survey of 2018 U.S. Federal Cases of Questioned Video Authentication

The court decided the *Lorraine*, case in 2007. The presiding judge, the Honorable Paul W. Grimm, along with attorneys Michael V. Ziccardi and Alexander W. Major, reviewed the impact of *Lorraine* in recent decisions in their 2009 Akron Law Review article titled “Back to the future: *Lorraine v. Markel American Insurance Co.* and new findings on the admissibility of electronically stored information.” Grimm et al., noted:

“... in the two years since *Lorraine* was issued, courts and counsel still seem to struggle with the basic principles of authentication as it applies to electronic evidence. Some courts are still permitting only rudimentary admissibility standards and counsel are still, at times, failing to meet that low bar. As electronic evidence becomes more ubiquitous at trial, it is critical for courts to start demanding that counsel give more in terms of authentication—and counsel who fail to meet courts’ expectations will do so at their own peril” [47].

In addition to understanding how digital video is best admitted into evidence, it is also important to understand how opposing counsel can challenge the authentication of digital video offered into evidence and how courts have responded to those challenges.

Survey of Federal Court Decisions

In light of information noted in the Grimm et al., *Akron Law Review* article, a search of the Nexis Uni® database for federal cases with the search terms “video” and “authentication” within 150 words of each other for the period between January 1, 2018 and December 31, 2018, resulted in 102 court case publications. This search resulted in the identification of 102 court cases. A review 10 of those cases as a representative sample where the admission of the video, with or without audio, was challenged on the basis of authentication. This survey conducted a further analysis of those 10 cases to determine the origin of the video (mobile phone, surveillance system, etc.), authentication approach (witness with knowledge, expert witness, etc.), a summary of the argument made by the challenging party, and the court’s decision on the challenge to the authentication of the video evidence.

Survey Results

An analysis of the 10 cases involved the courts' decision denying challenges related to the "witness with knowledge" of the authentication. The analysis found:

- All 10 cases involved the authentication approach of "witness with knowledge" pursuant to FRE 901(b)(1).
- Two of the cases involved courts permitting only rudimentary admissibility standards.
- Three of the cases involved the challenging party offering specific indicators of video / audio alteration, but not based upon forensic science.

[48][49][50][51][52][53][54][55][56][57]

Authentication of Electronically Stored Information In International Criminal Court

Methods of authenticating ESI take many forms in countries around the world. While several international courts address various cross border and international issues, I selected the International Criminal Court (ICC), an intergovernmental organization and international tribunal located in The Hague, Netherlands, to compare authentication of digital videos with the Federal Rules of Evidence and one of the leading cases in this area from the Federal Courts in the U.S.

International Criminal Court e-Court Protocol

Fletcher, Hoofnagle, Stover, and Urban (2018) provided insight into digital evidence authentication by the International Criminal Court (ICC) in their "Working Paper: An Overview of the Use of Digital Evidence in International Criminal Courts, Salzburg Workshop on Cyber Investigations." Fletcher et al., noted the ICC rarely admitted digital information as direct evidence, but usually admitted it as corroborating evidence to corroborate oral testimony. Fletcher et al., specifically cited video evidence as an example of digital evidence of concern and

further noted courts in general were concerned that video footage could be manipulated and metadata could be changed [58].

In addition, Fletcher et al., revealed that the ICC had developed standards specifically addressing digital evidence which were identified as the “e-Court Protocol.” They noted the ICC designed this protocol to “ensure authenticity, accuracy, confidentiality and preservation of the record of proceedings.” Fletcher et al., disclosed the “e-Court Protocol” required that digital evidence submissions include metadata to be attached, including the chain of custody in chronological order, the identity of the source, the original author and recipient information, and the author and recipient’s respective organizations [58].

It is important to note that the ICC practice of admitting digital information as corroborating evidence to support testimony has similarities to the U.S. Federal court system relating to the admission of video and audio evidence. Specifically, digital video and audio are not recognized by U.S. Federal courts as self-authenticating; instead, admission of digital video and audio evidence requires a witness with knowledge or recognized expertise to testify to the authenticity of the evidence. The survey of 2018 cases noted earlier in this chapter revealed that the testimony was offered by a knowledgeable witness.

Digital Evidence – Investigatory Protocol Overview

Fletcher et al., (2013) also provided insight into ICC’s digital evidence authentication in another Salzburg Workshop on Cyber Investigations paper titled “Working Paper: Digital Evidence: Investigatory Protocols.” Fletcher et al., broke down the authentication in to different scenarios. The first scenario involved authentication when the device was available to the investigator; the second involved authentication without the device being available [59].

Device Available

Fletcher et al., generally described that the investigator should use the digital forensic best practice of creating a forensic image or duplicate of the digital media with the use of pre- and post hashing of the media to illustrate the integrity of the forensic image or duplicate [59]. Fletcher et al., seemed to infer that a video found on a hard drive or on a mobile phone was authentic; however, the inference was based on no additional authentication methodology description for devices that were available.

This perception did not account for video and audio editing software on mobile phones or even freeware software that is available to the average user for download to their computer.

Device Not Available

Fletcher et al., provided examples of a scenarios where devices were not available, such as a video that was emailed to the investigator or downloaded from a public website. Fletcher et al., focused on authentication techniques such as witness testimony, internal factors such as metadata, and comparison with other independently authenticated evidence. They also offered an example approach related to videos downloaded from YouTube where a request is made to YouTube to identify the information of the subscriber who uploaded the video to YouTube. Fletcher et al., offered the Sri Lanka case example noted below for comparison with other independently authenticated evidence [59].

Sri Lanka case. In the Sri Lanka case example, Fletcher et al., noted that video of the Sri Lankan army's battle against the Liberation Tigers of Tamil Eelam in August 2009 showed the execution of prisoners. They also revealed that there were no witnesses who were willing to verify the video and any ancillary evidence to corroborate the video's authenticity. Fletcher et al., also pointed out that the Sri Lankan Government denied the allegations and labeled the video as unreliable.

Fletcher et al., described the authentication of the suspect video by a “digital editing forensic expert” as containing no breaks in the continuity and indicating that the footage had not been edited or manipulated. They further described the video authentication process by combining the video expert’s conclusions with the findings of a ballistic expert and a forensic pathologist related to their video content analysis of the same video. Although Fletcher et al., noted that none of the experts’ findings independently proved the video was authentic, the combination of their findings served as compelling evidence of the video’s authenticity [59].

It is evident from cases reviewed from the U.S. Federal Court system and the Sri Lanka case example from the ICC that the approach to video authentication presented in the two court systems are very different. However, the review of the court cases revealed that the use of a scientific based method or framework for digital video authentication was seldom, if ever, mentioned.

Expert Testimony

The authentication approaches presented in the *Lorraine* case specifically noted the use of the expert witness as an option for authenticating digital evidence. The forensic video examiner who authenticates videos using the proposed framework in this paper must be prepared to testify in court as an expert. The expert testimony should be based upon forensic science regardless if the testimony is offered by the prosecution, defense, or if the expert is engaged by the court itself. This section of the thesis addresses the U.S. Federal Rules of Evidence (FRE) 702 (including updates in 2000 & 2011) and specific case precedents at a high level for special consideration when developing and using various techniques within the proposed framework. In addition, this section looks at ICC expert testimony.

U.S. Federal Rules of Evidence 702

The U.S. Congress enacted the Federal Rules of Evidence (FRE) in 1975 which provided new guidelines for U.S. Federal courts to admit expert testimony and scientific evidence.

According to the National Forensic Science Technology Center website, the first version of FRE 702 (Testimony by Expert Witnesses) provided that a witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- the testimony is based on sufficient facts or data;
- the testimony is the product of reliable principles and methods; and,
- the expert has reliably applied the principles and methods to the facts of the case [63].

The Daubert Trilogy

The Daubert Trilogy is comprised of three U.S. Supreme Court decisions that form the foundation of expert testimony in the U.S. Federal court system and many U.S. state courts. The trilogy begins with the case known as *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993) (Daubert)[11] .

Daubert v Merrell Dow.

The U.S. Supreme Court decided the *Daubert* case in 1993. It became the standard for U.S. Federal court system to use to interpret the FRE as it relates to expert testimony.

Specifically, the trial judge is assigned the role of “gatekeeper” to ensure that the expert’s testimony:

- is based upon sufficient facts or data;

- the product of reliable principals and methods; and,
- has applied the principals and methods reliably to the facts of the case [11].

The Court further described the basis of reliability that the trial judge should use to assess potential expert testimony by noting:

“...in order to qualify as "scientific knowledge," an inference or assertion must be derived by the scientific method. Proposed testimony must be supported by appropriate validation—*i. e.*, "good grounds," based on what is known. In short, the requirement that an expert's testimony pertain to "scientific knowledge" establishes a standard of evidentiary reliability” [11].

In addition, the Court noted that when an expert is proposed for testimony, the trial judge determines if the expert will testify to scientific knowledge that can assist the trier of fact in determining a fact at issue. The Court provided guidance to the trial judge when they wrote:

“... This entails a preliminary assessment of whether the reasoning or methodology underlying the testimony is scientifically valid and of whether that reasoning or methodology properly can be applied to the facts in issue. We are confident that federal judges possess the capacity to undertake this review. Many factors will bear on the inquiry, and we do not presume to set out a definitive checklist or test. But some general observations are appropriate” [11].

In its decision, the Court listed the non-exclusive checklist for the trial judge to use in the preliminary assessment as follows:

- Whether a theory or technique is scientific knowledge that will assist the trier of fact will be whether it can be (and has been) tested;
- Whether the theory or technique has been subjected to peer review and publication;

- Whether a particular scientific technique or theory produce results with a known error rate;
- Whether a particular scientific technique or theory has the existence and maintenance of standards controlling the technique's operations; and
- Whether a particular scientific technique or theory has attracted a widespread acceptance within a relevant scientific community [11].

General Electric v. Joiner.

The second case in the trilogy continued with *General Electric Co. v. Joiner*, 522 U.S. 136, 118 S. Ct. 512, 139 L. Ed. 2d 508 (1997) which involved the review of a lower court decision to exclude scientific evidence and the appeals court's opinion that *Daubert* removed the abuse of discretion standard ordinarily applied to a review of evidence by the lower court. The Supreme Court opined that *Daubert* did not change the "abuse of discretion standard" ordinarily applied to review of evidence rulings [61].

Kumho Tire Co. v. Carmichael, et al.

The trilogy concluded with *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 119 S. Ct. 1167, 143 L. Ed. 2d 238 (1999). In this case, the Court opined that the *Daubert* standard applied to "technical" and "other specialized knowledge" even though *Daubert* ruling was limited to "scientific knowledge" [62].

Amendments to U.S. Federal Rules of Evidence 702

The U.S. Congress amended FRE 702 in 2000 to include information from the cases related to the *Daubert* Trilogy and again in 2011 to adopt a language style for ease of understanding. The amended Rule 702 notes:

“A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

- the expert’s scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
- the testimony is based on sufficient facts or data;
- the testimony is the product of reliable principles and methods; and
- the expert has reliably applied the principles and methods to the facts of the case” [30].

International Criminal Courts Forensic Science Expert Competence

In 2009, the Dutch lawyer Geert-Jan Alexander Knoops, who practices both in the Netherlands and internationally, published “The Proliferation of Forensic Sciences and Evidence before International Criminal Tribunals from a Defence [sic] Perspective” in *Criminal Law Forum*. Knoops discussed the generally accepted criteria to test forensic science in the international community based upon the *Daubert* case . He noted the reliability and credibility of the forensic evidence the expert may present is assessed by the following criteria:

- Has the theory or technique used been tested?
- Was it subject to peer review?
- What is the error rate?
- Do scientific standards exist and were they maintained?
- Was this standard widely accepted in scientific community?
- Does an internationally accepted norm exist?
- Was the norm applied properly? [64]

Knoops noted the criteria above has been adapted and applied by various domestic and international jurisdictions [64].

APPENDIX B

SCIENTIFIC METHOD (Framework General Process)

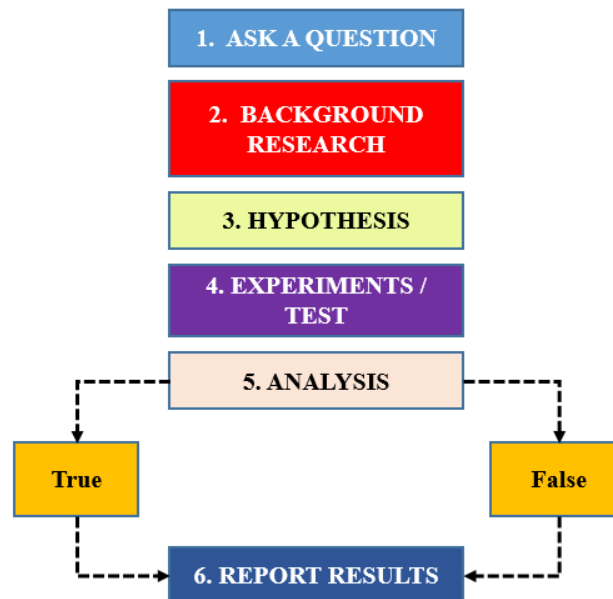


Figure 21 - Diagram of Scientific Method Used In Proposed Framework

Step 1 – Ask A Question: *Analysis Question – Is Video Altered / Real / Edited?*

Step 2 – Background Research: The examiner conducts any background research necessary to conduct examination. Research on file structure, codecs, recording device, etc.

Step 3 – Hypothesis: The examiner develops a hypothesis or multiple hypotheses based upon Step 1.

Step 4 – Experiments: The examiner conducts tests/experiments (e.g., file format analysis, hex analysis, etc.). This is where multiple individual techniques are used to test the hypothesis.

Step 5 – Analysis: Examiner analyzed test/experiment data relative to the hypothesis to determine if the data collected supports (true) or does not support (false) the hypothesis.

Step 6 – Report Results: The examiner documented the findings of each experiment / test (each technique results from examiner analysis) and ultimately the examiner's conclusion.

Note: Steps 3 – 6 may be cyclic and require adjustments to the hypothesis if the examiner only detects inconclusive results.

APPENDIX C Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses	
Hypothesis	

Questioned File Information	
File Name:	
File Size:	
MD5 Hash:	
SHA1 Hash:	
SHA256 Hash:	

HYPOTHESIS ANALYSIS				
#	Analytical Area	Type of Analysis	Data	Observations / Comments
1	File Structure Analysis	File Format Analysis		
2		Header Analysis		
3		Hex Data Analysis		
4	Workflow Optimization Decision		<div> <pre> graph TD A{File Structure Consistent With Original?} -- Yes --> B[Continue] A -- No --> C[Stop] </pre> </div>	
5	Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.			

6	Video File Bifurcation Process - File Preparation Decision	Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.			
7	AUDIO STREAM ANALYSIS				
8	Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis				
9	Global Analysis	DC Offset Analysis			
10		Power Analysis			
11		Zero Analysis			
12		LTAS Analysis			
13		LTASS Analysis			
14		DSS			
15		CLA			
16		MDCT			
17					
18	Local Analysis	Critical Listening	Waveform:		
			Spectrogram		
19		Waveform Analysis			

20	Spectrum / Spectrogram Analysis				
21		DC Offset Analysis			
22		Power Analysis			
23		Zero Analysis			
24		QL / Bit Depth Analysis			
25		ENF Analysis			
26					
27	VIDEO STREAM ANALYSIS				
28	Repeat This Analysis Area For Each Video Stream Analyzed				
29	Global Analysis	SPN Analysis			
30		CFA Analysis			
31		CLA			
32		Pixel Level Analysis			
33		Block Level Analysis			
34		Temporal (Interpolation) Analysis			
35					
36	Local Analysis	Visual Anomaly Analysis			

37	<div></div>	Copy & Move Analysis			
38		Double Quantization Analysis			
39		Local Pixel Manipulation Analysis			
40		Local Block Manipulation Analysis			
41					
42	Overall Decision For Hypothesis				

- 97
- ☒ Consistent with an original recording.
 ☒ Not Consistent with an original recording.
 ☐ Inconclusive / cannot run.

Conclusion:

The evidence file and video / audio stream are CONSISTENT / NOT CONSISTENT with an original recording.

APPENDIX D CASE STUDY 1

Methodology Evaluation Tool Report

The method evaluation tool report addressed the potential use of multimedia stream hash validation method [20]. This evaluation contains two tests or assessments. The first test is validation testing using SWGDE tool / method validation testing guidance [23]. The second test or assessment is a admissibility assessment of the proposed method.

Method Validation Testing

The method validation testing answered the following questions.

Are the results of method reproducible, repeatable, accurate, and precise?

The method validation testing produced:

- 1) Hashes of respective audio streams in original file and audio streams in transcoded derivative digital multimedia files that matched 100% (100 files out of 100).
- 2) Hashes of respective video streams in original file and video streams in transcoded derivative digital multimedia files that matched 100% (100 files out of 100).

This demonstrated reproducibility as noted by Whitecotton (2017) and Warren et al., (2012) as generally discussed in their research [20][65]. The method validation testing demonstrated repeatability. The test demonstrated accuracy and precision by the exactness of the hash used. The numerical probability of a random collision for MD5 hash is 1 in 2^{64} (about 1 in 1.84×10^{19}) [66].

Is the method used for its intended purpose?

The method validation testing was limited to the intended purpose of validating the technique of hashing the multimedia streams (original audio streams and videos stream transcoded to new derivative files).

Does the method perform as expected?

The multimedia hash validation method performed as expected. A noted limitation is the use of the method is also dependent upon using proper transcoding software and an understanding of transcoding multimedia files.

Admissibility Assessment of Proposed Method

Has the method been tested?

The method was tested as noted by Warren et al., [65] and offered by Whitecotton [20]. Completed personal validation testing as noted in Appendix D-1, D-2, D-3, & D-4 for method validation testing.

Has the technique / method been subjected to peer review & publication?

Yes. The concept of multimedia stream hashing for identification was published in scientific paper that was submitted under IEEE technical peer review standards using at least single blind peer review in 2012. The paper was published as [65]. Additionally, the published paper was presented as part of 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery proceedings. In addition, Whitecotton's thesis was published as [20].

What is the error rate of the theory or is an error mitigation method implemented?

See Appendix D-1, D-2, D-3, & D-4 for method validation testing. The testing resulted in no known error rate. The use of this method should be used in conjunction with an error mitigation methodology that includes technical peer review [13].

Is the technique / method accepted in the forensic science community?

Hashing and use of MD5 hash in the forensic science community is accepted in the community as noted in by SWGDE document titled "SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics" Volume 1.0 [66]. In addition, the reference to the use of hashing of digital media, files, or various data is accepted in the forensic community as noted in the SWGDE Digital & Multimedia Evidence Glossary volume 3 [5].

What are the standards controlling the use of the technique / method?

The use of multimedia stream hashing is noted in SWGDE technical notes on FFmpeg. The tested method used the underlying standard noted in the SWGDE technical notes on FFmpeg [67].

Decision To Include / Exclude Method In Video Authentication Method Toolbox

The test results have demonstrated that multimedia stream hash validation method, as it relates to video and audio streams, is a viable method for use in video authentication process when transcoding video and audio streams for further authentication. The method is added to the author's video authentication method toolbox for use within the limitations noted in the method validation testing report.

APPENDIX D-1

Method Validation Test Summary Report

Test Title: Multimedia Stream Hash Validation Method

Test Date: 3/22/2019

Test Description:

This report documents the method validation assessment of multimedia stream hashing an audio stream or video stream when they are transcoded from a video digital multimedia file for subsequent authentication. The use of the method under validation testing is frequently needed for transcoding a digital multimedia file's audio and video stream to digital multimedia files more suited for authentication during the proposed forensic video authentication bifurcation step. The method validation test consisted of two test scenarios. Multimedia stream hashing was noted in research by Warren, Clear, and McGoldrick (2012). Their research focused more on metadata, but addressed audio stream and video stream hashing instead of digital multimedia file [65]. In addition, the specific method was noted by Whitecotton (2017) [20].

Test Results:

Table 17 -Test Results For Method Validation

Test Number	Environment	Requirement 1	Requirement 2	Requirement 3	Requirement 4
1	Audio	Pass	Pass	Pass	Pass
2	Video	Pass	Pass	Pass	Pass

Requirements:

1. Successfully extract a forensic duplicate of the multimedia stream from one video digital multimedia file to another audio or video digital multimedia file;
2. Hash method uses cryptographic hashing algorithm to verify that the multimedia stream was unchanged in the forensic duplication process;
3. Hash is tested by comparison (original multimedia stream versus copied multimedia stream); and
4. Use of at least MD5 algorithm for hashing.

Observations/Concerns:

The test had no errors.

Limitations:

The method validation test was limited to the intended purpose of validating the technique of hashing the multimedia streams (original audio streams and videos stream transcoded to new derivative files). The use of the method is also dependent upon using proper transcoding software and an understanding of transcoding multimedia files.

Recommendations:

The test results have demonstrated that multimedia stream hash validation method, as it relates to video and audio streams, is a viable method for use in video authentication process when

transcoding video and audio streams for further authentication. The method is recommended for use within the limitations noted.

APPENDIX D-2

METHOD VALIDATION TEST PLAN

Test Title: Multimedia Stream Hash Validation Method

Purpose and Scope:

This test plan will evaluate the technique of multimedia stream hash validation when an audio stream or video stream is forensically copied from a video digital multimedia file for subsequent authentication. The use of the method under validation testing is frequently needed for transcoding a digital multimedia file's audio and video stream to digital multimedia files more suited for authentication during the proposed forensic video authentication bifurcation step. This plan will consist of two test scenarios. One test scenario is the extraction of audio stream from a video digital multimedia file and the second test scenario is the extraction of video stream from a video digital multimedia file. Multimedia stream hashing was noted in research by Warren, Clear, and McGoldrick (2012). Their research focused more on metadata, but addressed audio stream and video stream hashing instead of digital multimedia file [65]. In addition, the specific method was noted by Whitecotton (2017) [20].

There are two purposes of the test. They are as follows:

- *Test results of the multimedia stream hash validation method for reproducibility, repeatability, accuracy, and precision?*
- *Test results of the multimedia stream hash validation method to determine if it performs as expected?*

Requirements:

1. Successfully extract a forensic duplicate of the multimedia stream from one video digital multimedia file to another audio or video digital multimedia file;
2. Hash method uses cryptographic hashing algorithm to verify that the multimedia stream was unchanged in the forensic duplication process;
3. Hash is tested by comparison (original multimedia stream versus copied multimedia stream); and
4. Use of at least MD5 algorithm for hashing.

Description of Methodology:

- 1) Hash multimedia streams (both audio and video) in test data set. This is test preparation and establishes the original hashes for subsequent comparison.
- 2) Forensically copy each test data set's audio stream to a wave PCM audio digital multimedia file. Test scenario #1.
- 3) Hash the audio stream in each derivative wave PCM audio digital multimedia file. Test scenario #1.
- 4) Analyze results of test scenario #1.

- 5) Forensically copy each test data set's video stream to a lossless MP4 digital multimedia file. Test scenario #2
- 6) Hash the video stream in each derivative lossless MP4 digital multimedia file. Test scenario #2.
- 7) Analyze results of test scenario #2.

Expected Results:

1. Hashes of respective multimedia streams in original file and multimedia streams in new digital multimedia files match.
2. Demonstrate reproducibility by Warren et al., (2012) as generally discussed in their research [65].
3. Demonstrate repeatability by tester.
4. Demonstrate accuracy and precision by the exactness of the hashes used.

Test Scenarios:

Table 18 - Planned Test Scenarios

Test Number	Environment:	Actions:	Assigned Reqt's:	Expected Results:
1	Audio Stream	Forensic Copy Audio Stream To New Wave PCM File, Hash Audio Stream In New Wave PCM, & Compare Derivative File's Audio Hash With Original Audio Stream	All	All
2	Video Stream	Forensic Copy Video Stream To New Lossless MP4 File, Hash Video Stream In New MP4, & Compare Derivative File's Video Hash With Original Video Stream	All	All

Test Data Description:

Test Data Set:

The test data set is made up of 100 video files created with an iPhone 8Plus with iOS 11.2.6 using Live Photo to create photographs. The 100 video files were side car / derivative of the Live Photo process. The movie files contain both video and audio streams. The video codec of each file was High Efficiency Video Coding (HEVC) and the audio codec of each file was Linear Pulse Code Modulation (LPCM).

The following are the test data file hashes.

Filename: IMG_0229.MOV
Filesize: 3052636 bytes
MD5: 5ab7abec7424f6cc17e0783183b313e3
SHA1: b0e9ae59d74bd21ba1ad648f35892712e61720cb
SHA256: d8a6329b915bf349bbf62bb55da7a17e4cf0d2d97a0841c196cab8508fe9583f

Filename: IMG_0230.MOV
Filesize: 3130388 bytes
MD5: 7d9280811899d0b0b048d30accd22c61
SHA1: 7103913bd5b7e4c1e8ca0d7daf60b11e30236500
SHA256: 9ed104bda2e43d4c531118d021eddce4879b0226627275cdb8c65404985bfbbf

Filename: IMG_0231.MOV
Filesize: 3302243 bytes
MD5: 3813a68ea095196f8392ee732c1db1ea
SHA1: 989ba7afbb8fbabf4d1742da275c3dacf1db0740
SHA256: f253a29357aa1566875009be2086481a4ccff8cc9904b31e96f5936c236111ba

Filename: IMG_0232.MOV
Filesize: 3070881 bytes
MD5: e5510c3251c7f8c9b01d39987d04efbf
SHA1: a5ba73cbda7c23fbc5abc9b5289ae1b09f0edcd6
SHA256: 8a7d61b0267b662d4d214baead7e600d6ce7f44b5e836308af8efcc797406954

Filename: IMG_0233.MOV
Filesize: 3208412 bytes
MD5: ad348ddebc6db5e4028c65512c55be7f
SHA1: 192e3f8b120e00beb919c5a8ace591b8914cae45
SHA256: 0557d9b348c57bbf44d569b1de4e3bdfb3d7a112ece08da8c10d2ed6c2bbf188

Filename: IMG_0234.MOV
Filesize: 3502974 bytes
MD5: 67453057742a7845be3d5053b5f1860a
SHA1: ed61cbaf375e13ecbc71f5d1a363d97e0a99a9f3
SHA256: 81eaae13a37f29c46b07b847c75a8a64863aa102aba648df54eb137fc66ef257

Filename: IMG_0235.MOV
Filesize: 3641120 bytes

MD5: d017cb2c559057dfcb5c98e3d77b4adb
SHA1: 790e59600502c005185e084bc53eb812ae8be902
SHA256: 88454b6b64560070f51697796aa12784a65a1f3537b40e425bea1b0af4a7a495

Filename: IMG_0236.MOV
Filesize: 3302658 bytes
MD5: f9c3b124d5376fd167b88be798a1943d
SHA1: 6b52ba634985ff67538f4b71cbe8b918eb80a7cf
SHA256: 545238e5f4ac8a9679cfd259b274315cfa2a86e57d8a081a8b1961c3b2e886ca

Filename: IMG_0237.MOV
Filesize: 3434964 bytes
MD5: ca45c3ae6d43ce488543769e2a23d4f0
SHA1: e65e102698a7fe6082401e1aba4c910fa2f1eb24
SHA256: e5bbc86d6bed03007e5d0a53aa995cb989f9d73e19f6c7320481c8c78c6a6fe3

Filename: IMG_0238.MOV
Filesize: 3648426 bytes
MD5: e3dc4e25e0f56df2aa7b696f16e7772f
SHA1: 6af81fd21bec8b1cd7c1ebe8b567bd10c9f4eeac
SHA256: 34fb5a9900f381ffe8b3085a747ea39aa49668bff4f686c4ff90aa3ea66c325a

Filename: IMG_0239.MOV
Filesize: 2967772 bytes
MD5: 4282e63107d30ced86d889ca2dc2dc08
SHA1: ca65fadbb81716be049a76157c8b94bc8ff673fb6
SHA256: e57646ab6909b781ba02ec460e87a2d4fda1197ec75a8ebf52e97b46b1318490

Filename: IMG_0240.MOV
Filesize: 2457755 bytes
MD5: 700e5f18a4f9b520fc21190c5a5b34a6
SHA1: c11c5a33a6b3cb4e9f036442a033a0e64e878ee8
SHA256: 557201edc1252dac08f8e8805f8a32476b25a2825a9962f513669f1c0a35b5de

Filename: IMG_0241.MOV
Filesize: 2839241 bytes
MD5: 50f97bccd6b072ef63475cbd4a3de1b8
SHA1: d5cbefd27a97f56da7db3d5776ac7580937f7ef2
SHA256: 0e9eedbefc8be47ed6d56675a2c8f1fa1bbb5b5514d7ec51883bf5640a5b5321

Filename: IMG_0242.MOV
Filesize: 2825243 bytes
MD5: 82074f1bc95d8b4936117d6665c7ad26
SHA1: cd0e9091f22326666a5b197c2153165a3b95cffb
SHA256: 274331cf3e5861ae270ced7ba85348a6a6eeeb3280248a0d61a0978ced737324

Filename: IMG_0243.MOV
Filesize: 2696997 bytes
MD5: 4dd74cd4241b67041689ecce26a68b90
SHA1: 0727a90c62b22387c00e996c37c530a14164a391
SHA256: aa92526f1f7077223dc37f9d2dde7b44afab39bb625f751b96aa220ad314a2f0

Filename: IMG_0244.MOV
Filesize: 2931704 bytes
MD5: a5e0bef5ad9e5468f6e4d3b626205e32
SHA1: a6a84308a7b43a4a6a4a4fa14eb954cc8df7c026
SHA256: c1d0718a767850a7af7963a72869332c78a965b77bd9ad69a91cae024a229e2d

Filename: IMG_0245.MOV
Filesize: 2858671 bytes
MD5: fa0376c8afc0364acb36dc868da92236
SHA1: 1cd06f3c5608f13f961648b1b193a75b0e33bb4e
SHA256: ce91e4f3eae4ebcfda342ee2a362dd93bd84999c84666dfd4029dc02c4dca687

Filename: IMG_0246.MOV
Filesize: 2148979 bytes
MD5: fbb488a9850e0842216a6971dce63229
SHA1: 5cf866261e98d5472a90498b5b7f0f4cb9cfa5a6
SHA256: 558fb5901d7c049650be9da2a286293dbfba0306c1973404c18d211b474f582e

Filename: IMG_0247.MOV
Filesize: 3231455 bytes
MD5: 623bc7a52744ac15565e4e1ebbe6e6eb
SHA1: dcd3a4a1949df4c51edb1976a318f719a280653d
SHA256: 8360902faa573427f05af1898befe482a6d8b0782907978637c4590caaa2344d

Filename: IMG_0248.MOV
Filesize: 2856570 bytes
MD5: 7fd4db067bbfe7148d7462c2f0f56d96
SHA1: ca1905fcb11b3d94730cead85567afa49bf6b4f5
SHA256: b7bed7c820cc8701c8430ef5965b525b9b77991178c52315365ce4c1da0f72e4

Filename: IMG_0252.MOV
Filesize: 2637002 bytes
MD5: 09e1bbc73057f53b17da95debb1f7f21
SHA1: ef1a8094f944105f29aa3f73229bd294281b1b1e
SHA256: e0bc9811e4f58e4be7f0a1baa944d84e06920238dd5f8bac4866c7379003af22

Filename: IMG_0253.MOV
Filesize: 2659292 bytes
MD5: 4f2dc9a8eab6eb4840bc52182788e508
SHA1: 83128aafd868745eedc5f4f24166b3bc79f9ffc6

SHA256: 4b9140d87320d6ec80f673a99c87d0cdc95b0d836501fe2c2cbefbf494f9ad3e

Filename: IMG_0254.MOV

Filesize: 2633994 bytes

MD5: 7c76d5ce41f67b48a01b54d4928be359

SHA1: 08d08aeb8c3017c50e539062c26f5aadcae21151

SHA256: c4aab8991b1f57e35f12b55d20ac5a849a9f5e18034d8553cd67e1b2a97f1049

Filename: IMG_0255.MOV

Filesize: 2816902 bytes

MD5: d782c06cad933e4aa91a2500902f0633

SHA1: 7b15740eca1e967af2db00e37c3ec41a7d2bc370

SHA256: 672b798c0910c5065bfd7a9521990cc09eda93d56501d410203dd445e53cfe64

Filename: IMG_0256.MOV

Filesize: 2676768 bytes

MD5: d9d056b0ffba3ca9885a229b80a57d48

SHA1: 875c36ae1e49c99e9ab7a330179933273091f6ad

SHA256: dafbf61d68df7e04e9ee4bf0ed7cc97ba9a1aee07f9491e96c4ff3a3812ff4fd

Filename: IMG_0257.MOV

Filesize: 2685411 bytes

MD5: fcfd718e4beb908fc72bdc669bf4a50a

SHA1: feb484eba681cdf7b4b3c04bb74d514b0f1ae2ac

SHA256: fb484bef6f60d0a57a979226f9f81312ded7fda9fe2d98c840d45d47346b9205

Filename: IMG_0258.MOV

Filesize: 2751184 bytes

MD5: 6a56fb83b3f88fcdf727132c69896b40

SHA1: 5455d2f7b525282f7c1e01672ed0a96f32afb2c8

SHA256: 974db58b8fd4ce414844d2da0d72620c76f0af483dbba62699ac8a0316c71d75

Filename: IMG_0259.MOV

Filesize: 2667810 bytes

MD5: 19f57e62fb319d01a7d35fdf735fcdc8

SHA1: 398039d60d0242f001add31f2f7d4ddd5498f589

SHA256: d5059845ff208bd6a4960ea4ab3cc7c2bce5e7481683dbae9d1d9d5bc6813208

Filename: IMG_0260.MOV

Filesize: 2677297 bytes

MD5: 14133b733e0fbbecb1e223c26e1dcdbd9

SHA1: f5176d4cc0ee9daab362840336aa1a14ee5bd5fa

SHA256: df660d4347669baec86a54f1627731b6381929d83cfa9ff4bb229c555a0bd88e

Filename: IMG_0261.MOV

Filesize: 2629407 bytes

MD5: 5dfe03b7e03790db3c7d0e4731db06f2
SHA1: cc025e3beb59f4015e4223a6a1906a8edaf5f7de
SHA256: 397a24704489ca848849d34eae7bc3266b6757614f3d5f3423a452a82f82ce32

Filename: IMG_0262.MOV
Filesize: 2489416 bytes
MD5: cea84e58d95d578c6d47a878018f5634
SHA1: e85407882f7e794808598212b8025c0174339126
SHA256: 20922d8368f7f5d1211e52c279e716b1390e9b531dc2c301d79d2962c675f476

Filename: IMG_0263.MOV
Filesize: 2484359 bytes
MD5: 208c68b4cb05688f1c6fc7df23b8745d
SHA1: 734dd2ff0324a0e51741a3054a799779020490a6
SHA256: 7129d0cf422b6bd9ff78a8b4d50157b2c07a4c2499074d953d26642ec695705a

Filename: IMG_0264.MOV
Filesize: 2406707 bytes
MD5: 3e884c825560932c25e2cba60403c954
SHA1: 16b6ef1c54765730d93933434e3cf9a003a01f4b
SHA256: ac945c84b116615ada59db153543cd5a94df27463bfe1f064a5a58eb0263179f

Filename: IMG_0265.MOV
Filesize: 1899152 bytes
MD5: 73317ffbcc8da3aef164a0fee6527d9b
SHA1: fced7ed4acbb25dcecd9a43d6b7739f110d51f87
SHA256: a15cf83059b8e86f7edc76dd81b6ed84311eb432b897c83d8f859fe62b9c998a

Filename: IMG_0266.MOV
Filesize: 2473549 bytes
MD5: 9ad057a65b9bb2403581384ab899e76e
SHA1: 4303f9629f160eba2bfbcddc17832a4f59abddc6a
SHA256: 570dd76cdc2b97f128cfa521ee7a4b42ed6b0f593447ba56d98f5243ab41c2d6

Filename: IMG_0267.MOV
Filesize: 2154174 bytes
MD5: 9adfce24315c25bad77804036fa1ff78
SHA1: 55281073ac2d7b20fcaea6986b577512d6fb0b34
SHA256: 80ef9ea983f8b144914161c4ca76231d7fccc9b58ef7a0f7308ae431788b63a5

Filename: IMG_0268.MOV
Filesize: 2189425 bytes
MD5: bd26f8e9761b4516252e7697df5f16a9
SHA1: 3a72b56b6f1a00f95ab7cca63fabdaf4199563c2
SHA256: 7374ecca2ebab890de0df85939b8c44a4d0a6d0341936928a716f408f0ac2bde

Filename: IMG_0269.MOV
 Filesize: 2986278 bytes
 MD5: e3f02b976e1afc2097f69e1905c5e631
 SHA1: dc81fbf5de51b332d755276c803c6a9d21f3fcf7
 SHA256: 8538cdff1ff40237f0b58b49fbb48a9cb3516b5f3ac86f5e23589bb7a4504f7b

Filename: IMG_0270.MOV
 Filesize: 2635249 bytes
 MD5: bd902162eb987587d32307d8b521a31c
 SHA1: c44ce22a50d244394f606c6a1b885bfeca4a6e36
 SHA256: 6c1e686036183ae1d626bf462798b6862bd9e1ec029bf7748b14209e247b5bcf

Filename: IMG_0271.MOV
 Filesize: 2914899 bytes
 MD5: 06d4692b52ea70f25fc1c8297a692320
 SHA1: 2dcc16e8f6c97cae8c3ceb8f4f3aa3b56c65c8f7
 SHA256: 409148d03c01ff791aa33651bb22232dc408687f2670ea3fa5bf8e9f1cc7749b

Filename: IMG_0272.MOV
 Filesize: 3547734 bytes
 MD5: 3f88626ae8329ea65e533e112f7e4006
 SHA1: af0dbcaed6041ca918feb18166787c0f3d65cdbc
 SHA256: 274c51c81b981777445b43167c056b344746017986ac34f3b2ac13fb28e489e0

Filename: IMG_0273.MOV
 Filesize: 3393457 bytes
 MD5: 2d86267b2fdf356d708dd935cd5da4c5
 SHA1: 5ce664a66aa83e9cee8e0aa7075dabc79692e8b6
 SHA256: 37b8c489e68f0f97e190181103a5ce273dff304339253cdcb7d66a80448eadc0

Filename: IMG_0274.MOV
 Filesize: 3467523 bytes
 MD5: c3756337b36f94b3e2f25b3a075eed94
 SHA1: efea2ba98db8e6572454a3b53fea8646bd49e510
 SHA256: 2bf969ad9e39f37c76471a7eb181fcba95ad10f5d6b3553d44f5d98fa216b27d

Filename: IMG_0275.MOV
 Filesize: 3683847 bytes
 MD5: a87e1ea7ddfa624e6a087c1b8ad5f821
 SHA1: 71bdeb8cf461d474f09a257bcb361a265e93dc13
 SHA256: fa4a0aac4f423a0677e5ea073a5a29574806d403d4e21f7897888e3f449f8677

Filename: IMG_0276.MOV
 Filesize: 2915740 bytes
 MD5: bee757461d2b286db0ccc12a0aa201ba
 SHA1: 4d96b2f62a05b2d72b337a2f2f9d96831a618622

SHA256: 41b08c7d2d60a911025cb2338a49ef7a43e44bb942aa455fd8a289ad525d8f0b

Filename: IMG_0277.MOV

Filesize: 3070376 bytes

MD5: 3b95e3abd6b1d73eee441273d88d6071

SHA1: 7dc44b985408d8eeb930aeb2b89e7bd5791a6f5e

SHA256: 7442c206099ee7ef6a8cfe69e18c46c2733a89c6df01cd8698c1563f743294d1

Filename: IMG_0278.MOV

Filesize: 3257661 bytes

MD5: 7384981eeb49e1fad49282a912789330

SHA1: c7375a535a4c00135478918f8b2e33b4d34841e1

SHA256: ba8cc875539d4e719e0fbdd77163aa45b440d83eb1c987d2359c13a53da8e3f5

Filename: IMG_0279.MOV

Filesize: 3078844 bytes

MD5: 6e59b3ee6a3558552964da36612a7299

SHA1: 9c111a52d3d9a49a883d5e441797d5115be30b40

SHA256: 88fa75375ffa0f13cb0e3c193631f8ecc973b1b04f6f5978070217d387bd81f9

Filename: IMG_0280.MOV

Filesize: 3158292 bytes

MD5: 63c8d1ab0ca0e381893b96f135e93177

SHA1: ff35ce05025462a15c1c5010ec4fab292e3adb10

SHA256: 911b2e99bfd1596c2fd4b3fe906e982770c780c1c4d48a71205861e0b6d10e90

Filename: IMG_0281.MOV

Filesize: 2579832 bytes

MD5: 7bc5761311b704c1e7eb9bddcb966f0c

SHA1: 3649df8f8b539fb18a2fe37b6fe1ec0cc13616e1

SHA256: 4acf710b81770bfc6afe685c24b7d7d6391974876db3ab6524793f86530b0914

Filename: IMG_0282.MOV

Filesize: 2413564 bytes

MD5: 2abd838568225300e46a5cb5d099dfb5

SHA1: 4ba6cbdbcceaf266536e374ae4d9f5500ac3191c

SHA256: 6106811f992f538621ef3da5fd2700c8bd2983cd44db0bfc6b1b96799f9181ef

Filename: IMG_0283.MOV

Filesize: 2492310 bytes

MD5: 5a3982bee771d3f3548c120e5ccba43c

SHA1: 1aebf08c20a647cb6c422cfd6b67ebc76337a94a

SHA256: 869dfefc05c2a20b12dea9ac8c77efbb92e36dd417a26eb412105b23b97dd144

Filename: IMG_0284.MOV

Filesize: 2556945 bytes

MD5: ded47595c6d62ad8f3fc63b5e4146b63
SHA1: 1230622ab5fd2841eeefd87ea2d73d1ca1d6f565
SHA256: 4c33e966278ad5475d432230d0d851a8c87139ff6ebdde6bca581b9d899c9ac0

Filename: IMG_0285.MOV
Filesize: 1901224 bytes
MD5: e3d86eb28a14b7cae64110bb8e4518db
SHA1: bde450ffaf2ef13d79e2d26a94efb266f6dcb3a5
SHA256: c6e6a88f4c417130ec9460b96981012ac81a2f05c9cca2e09c6e1879a37bf1b0

Filename: IMG_0286.MOV
Filesize: 2718963 bytes
MD5: ca5d4e4bd15de0f9e4adba0618234847
SHA1: a59dbba9e861ddef513c725d8c7171ba209f1639
SHA256: a045696ff0c1d5f45e703f7e3eb12fba2d46bc2745de692e316780f7ae138bb0

Filename: IMG_0287.MOV
Filesize: 2759510 bytes
MD5: 95dd87683d8513f4f7c9be7ba4f97ed3
SHA1: 03b6196babd67ed1a419963d92e31b30999c5b5c
SHA256: 36da5299ebf5a4b39a76edd701c8ba71c65fb9268451a1b6d125dbfbde4d9980

Filename: IMG_0288.MOV
Filesize: 2831431 bytes
MD5: 3ccd551384ccce31fb73b4453a64b9c0
SHA1: 41c0302be0cae1d02b179d3e2bd1f8334ed8b65a
SHA256: cde8b45191120b84dcdb64ed6acbb114d7479111b17d3991bde6d3eb7660e73a

Filename: IMG_0289.MOV
Filesize: 2569357 bytes
MD5: 1dac9e21ae4ca2bacf792314278d5655
SHA1: 44c1ef30d6cc9b543c5c0673bdc01aa4136b80ec
SHA256: 4d4c61dcead75a392f52e5b6f53f1d9729595e767d0f8b010dc13bbaceb28784

Filename: IMG_0290.MOV
Filesize: 2498775 bytes
MD5: 2c505668ffd21b25748658f309e8a7b7
SHA1: c4572d264f7a422ad208184332d27e633a541fa7
SHA256: 4cad406f5d5785cf8c33d8e3fa1bec133b7ca618992606eaa6c3762770ac515d

Filename: IMG_0291.MOV
Filesize: 3083395 bytes
MD5: 5395d546433a18ab48a3d4f8f31ead17
SHA1: dcee53c2d856306e7a7d9748873515849f455670
SHA256: da92611d0675d34fb1669d33a5b9eb941785eaf0143204fcb052a31b99ddd914

Filename: IMG_0292.MOV
Filesize: 2738319 bytes
MD5: 2c3fd5f4ff3ed3317a35704cc239c1e0
SHA1: b1f0cebee8f8fc7f05859e6f53a7b92dcb3c3422
SHA256: 70ca7ecd998df88931e9094d64cd499ddc8d1c6c1f2278f5a7b8ad10953a48b8

Filename: IMG_0293.MOV
Filesize: 2719992 bytes
MD5: c47f00fdcd6f2b9b4ad1960fd11ec47c
SHA1: e0fd5bb68154205295756a97ce968284dc054d35
SHA256: 066d8ae6833232725599ab1b374d564a80b2e7cdfcfaf322fa07983f7f6470e0

Filename: IMG_0294.MOV
Filesize: 2759513 bytes
MD5: 3801cdfc846a2b2493c9c036dbcf20a8
SHA1: eea0225212c616b338be3298212e9d4b7aba4e8d
SHA256: e2dc03f2ece0ce05773ef9cfdc282c664b0235b9e9192456e234b1baf18cd000

Filename: IMG_0295.MOV
Filesize: 2599686 bytes
MD5: e6daf28b0e4d23efedbf368d31a00ca9
SHA1: 4f7145f68309e412defdd87c744ce2ddc19e3b63
SHA256: bd060863813462b563a464855b6fe4fd182460ee19f9985ad7c0a361f5328878

Filename: IMG_0296.MOV
Filesize: 2750381 bytes
MD5: c50931b382407741ec1bd337f668b17e
SHA1: d8c101f37a694657c5cf055864400c655e96d0c3
SHA256: d0fda20e1250e26db1a5796f149a741f83b028012be2b50fa1cd82d8a246a948

Filename: IMG_0297.MOV
Filesize: 2766554 bytes
MD5: 2e517718f6c5ee569d3a753ea4089083
SHA1: 21a5d78c4bd6c00af2391111f7c621e53d31d93b
SHA256: 9c1ebadc16ed01de40914e3932d494865ca495bb3c322a8f8e69e8abe940798a

Filename: IMG_0298.MOV
Filesize: 2880233 bytes
MD5: 820748dd78fb388690d5936de1d0e36e
SHA1: 5a7d4f15b3547b15fc61960fbeb6aa7a33c4625d
SHA256: 8db198c7965c9349d0ae87e7ae89e0246c75ff09792893cc573f233d8311ac9c

Filename: IMG_0299.MOV
Filesize: 2773127 bytes
MD5: 22f33cf23f743dd22e5f95c3ec3568e
SHA1: b460be08e22cd9dfa474dda91a904796afb20af6

SHA256: 9e5dfd6fd6b602ab8885602881df842a5e1996b8ed614a56f28a26184e985eea

Filename: IMG_0300.MOV

Filesize: 2861337 bytes

MD5: adf633bc0c789bdcaaa06f2273608d2d

SHA1: 1f169fc3f641b4cab3f81262b127c0263c57b5ce

SHA256: bd124367c04ec2e35f549d673708a2fb7b68dc926d35b0e8eab19bdf0f46be68

Filename: IMG_0301.MOV

Filesize: 2825665 bytes

MD5: 62739b66828918b5b4570e6e0525e97e

SHA1: 302ebea178b36bf82c82da2bc294b5dc99adac53

SHA256: 5f9ccaeb31c10d305adfdb304dfbe837613ab95f2a3b0b19acda1cab19e9ae4

Filename: IMG_0302.MOV

Filesize: 2462816 bytes

MD5: 179215a12db3ad7d8ae82308ebf39c41

SHA1: b0cf3ba37bab497af76f68c28d9a184a4227b15c

SHA256: 07d430c05a1cccef27cfda49218c3e3873a20fa5d936d539ca25ffa514dfa9b8

Filename: IMG_0303.MOV

Filesize: 2455343 bytes

MD5: 25318710a92a9244df81c0de86de4311

SHA1: 2c1c3e61925f072a86f2467cf5808cf5990316a0

SHA256: 73d193474271ff6d3be0f8c87581437f16f82b14a45410e82e044c5747498d80

Filename: IMG_0304.MOV

Filesize: 2456561 bytes

MD5: a28a75eae8c283c023947265a6a4a762

SHA1: e9831ad3ebcab2694f485fc620871db3dcf48b3c

SHA256: 5d5425000e51da776e62dde8c0da47d1872000a9749b03eef8ece0460e32fb4c

Filename: IMG_0305.MOV

Filesize: 2467493 bytes

MD5: ded16cc6679d729a177a9bc69d81b96e

SHA1: 15751311f70cf968211127d80912679d3d67320a

SHA256: 5d1b0e3c1308426d5c391ee9fce6c1d0d5aaca23738defe7c69c85f41190143e

Filename: IMG_0306.MOV

Filesize: 2136429 bytes

MD5: db35339f2213205a27656d5c642f6f3a

SHA1: 6dc8084762d50ce38379fc4acb39d49987aeeb59

SHA256: d7e7bc2cbcaac02fa7d9259997c5903f9eea094ff752674e4977ede66c336128

Filename: IMG_0307.MOV

Filesize: 2451278 bytes

MD5: bc20e2931ff271116b78ff5f127f6b5f
SHA1: 7199c489aa76d2efbbdbcbcb58d119d42ba264e
SHA256: 5f17e3c1c12daed746e971e49edc63d2a064613fbfd0fa5681651cbdb03aaed

Filename: IMG_0308.MOV
Filesize: 2497958 bytes
MD5: c6e5a1ab98e6e001f66dadb73acc5eff
SHA1: d6d3d1f74c63543d8513fe9d322a938f85ad5590
SHA256: 49e3f4b96bda8671e4e771737c3422a7bb11078e735190593697f88b41859e4c

Filename: IMG_0309.MOV
Filesize: 2441856 bytes
MD5: 57a54ffe3c5f61cc8b1ad9bcdd056b29
SHA1: 68d168c884e87abda60a360881d7b15de5badec8
SHA256: 994865fdbd1352ce2621d4b1d554fbd2c86f6970fc811d18f3b2fdef25d0571b

Filename: IMG_0310.MOV
Filesize: 2435438 bytes
MD5: 9f206ee2ac1fa1176b306c63d481fa24
SHA1: d562afec90c04f9bb634f0848004213eaf1735a7
SHA256: 3c054338c95e37497a8f9cc43578044f08522517a78f596cde1a32a1fd2feee1

Filename: IMG_0311.MOV
Filesize: 2452305 bytes
MD5: 7b917232d2eefa0d31ddb942505c531f
SHA1: 21fcca90f57e4d2333ecee1ac720e1b8eeee24a9
SHA256: d5336d7b6ffd48cbe988b4ecdd12a191801931f675ad096046abcca8a939e542

Filename: IMG_0312.MOV
Filesize: 2631683 bytes
MD5: 8d9c0b2af3923d0de6bc199c64117a73
SHA1: 2a25f55abe17e8a3c27359dd3745a4a60eff8213
SHA256: 82a7e3ee2dd5030453e06f3d9515a485e9cd1b19399f86060cb672a6e3bb074b

Filename: IMG_0313.MOV
Filesize: 2736789 bytes
MD5: 95b205636e4a721d7d72dc7a0a5a8f8e
SHA1: a058988fb4b5f3dca5aff9891b3f9685b9da39a8
SHA256: b531160b7a38575436aab631116d133bbb0f3ad9c61456fb14b239d4ea86f76a

Filename: IMG_0314.MOV
Filesize: 2725759 bytes
MD5: c1c5785783744a4ae2b790cfc49b795a
SHA1: 429e2e6270e77f804f87c238ae1929e7b13a12b6
SHA256: 292dfc119bd035b94e118931fdf714cf4c4a1360bb986bcf1e76590add3ea088

Filename: IMG_0315.MOV
Filesize: 2901421 bytes
MD5: 549e37349582eee128bf5bcae4347731
SHA1: b5691b31f8b5c66e00c68d8dc79a57a8b60040d6
SHA256: 64500963719df45601d73bcb7d39d92961e06683797625d9be58813cccff65d8

Filename: IMG_0316.MOV
Filesize: 2938237 bytes
MD5: abad676b5b13ed178cc59b46eb703d5
SHA1: faec1d3a03b376041d5b63cda2fee48c8e08868c
SHA256: 099db288c968d33a78f6e109751bb7dc9e932d7f9d7c5c05e1a6578b3c1507f4

Filename: IMG_0317.MOV
Filesize: 2920275 bytes
MD5: f368137375d34999f792ea23014c82a7
SHA1: 1022fd918db74482c1bf78b727f8937a5f7e16dd
SHA256: c9ee35c2a6f04d5e157732d48e05f2fb41dd38cdadfd7ea67e87b3342de3180b

Filename: IMG_0318.MOV
Filesize: 2983658 bytes
MD5: bed03ff76ac91519bf4b0af50c07a6dc
SHA1: a9fa038d24d0351d1d4fa4650830e67e89c58ba1
SHA256: 4368670278e9722a43ce9fe96a9577790400ae642905204d4ee65cd28a8fe5e4

Filename: IMG_0319.MOV
Filesize: 2894092 bytes
MD5: 071e6ad3e4713ffa6969b31e546443fb
SHA1: 10d2ec5bd990baa1d86fe462a2c516ef982365d7
SHA256: 9a444bc0107d2bb7d5a81af57db846a20b9faa6f86eea7d422e095846b57a13f

Filename: IMG_0320.MOV
Filesize: 2871712 bytes
MD5: 05a4633da977adeb23b580829efde0a9
SHA1: 3f6fcb338582ef5d6b9257efbb018f404d1976fc
SHA256: 5094387a254bf9d737cde854286f22526c2c7a1133a843dcb1f3abd4f7d47930

Filename: IMG_0321.MOV
Filesize: 2881056 bytes
MD5: 46dc06d99786aa24601cede835b2b44b
SHA1: fabcd7014e03fabf48b9698cd3fa4ee64a2fa71f
SHA256: e7ac6eb0adcdd875fb26b79853bf30ad1b31839170cb4f22c5c65d15553f92ef

Filename: IMG_0322.MOV
Filesize: 2449563 bytes
MD5: e8f0fcb0c16da403968bfff829955181
SHA1: 469dbe32198e1eedded510180c91fe5396ca868

SHA256: 22458b1a66a563e2838c5888eb1723799b1c64bd57966872dcbc7ca199bfd4af

Filename: IMG_0323.MOV

Filesize: 2447465 bytes

MD5: 90fe24656af928f0e7ba70ccf9b20f30

SHA1: 990db09b8191ccf7da4d21670e9f6483a0563caa

SHA256: c5c0487516bdb69671823b4fd6668528c61bd62febbf1b377deca673d4463ccb

Filename: IMG_0324.MOV

Filesize: 2430121 bytes

MD5: bf44f3fbfd9ebe6e709090bc8dfbd93c

SHA1: b557dbf1d2b7a24e879c09f205f4692da0df79bf

SHA256: 08f63c5050adaf0d1955a6ff97143a64cc6bd527fee0052d2d3ced99eea5dd1d

Filename: IMG_0325.MOV

Filesize: 2442257 bytes

MD5: 4ac8eefe31f9496c36d281367e65fe27

SHA1: 08a54be8856b0eeb6a41822e9a6a2175220e9b44

SHA256: bf9619dd8cd9e9ed1f4f62d9dcc4857214804874b0a126bdc3578395f90ffedd

Filename: IMG_0326.MOV

Filesize: 2405645 bytes

MD5: 3c5ebd3b85979f472b506fc52d71b8c7

SHA1: 49db2ce29aa999ea0be29662ff3f68347afda18c

SHA256: 897b43e2aa65b631d1ae04dc3e757b5e46a2c4a7160a457300525140450b163c

Filename: IMG_0327.MOV

Filesize: 2451196 bytes

MD5: 210ba1e00c3f0555d41c336dd224e5b7

SHA1: 3c416ae9dd87637a2989e9048c33ffcd3301b0a

SHA256: 64ef6b410e1f76b59d3d67ec4a23f28896c473830951caa859526f8a643df854

Filename: IMG_0328.MOV

Filesize: 2414906 bytes

MD5: ba339bc15413eafb6200c3d3423beed6

SHA1: 73fa022b1cf446624c0120d851c8dbc5950596a5

SHA256: 446bbc70ae74a237d1b68ea5d29201fb12d66b5d09a40e3f0f32959fff3eef34

Filename: IMG_0329.MOV

Filesize: 2449232 bytes

MD5: 80d0b0948fb49988936b778b4e0259a2

SHA1: b7219505da76a7112feb15d59b7db1de45c006bd

SHA256: 30a293d5c674342ecdc85af0d5a1a13b767d26a678819fe309a8ea90e37842f3

Filename: IMG_0330.MOV

Filesize: 2454590 bytes

MD5: a1a03eaf251e67e2eefc587a4a91bb78
 SHA1: d8d859dff5f8c7498ab0bb9c3d3e2f06b27cfa9f
 SHA256: b403ad736045445eda173d6c501072ca05193b0d291133f2b8162584da447a49

Filename: IMG_0331.MOV
 Filesize: 2423935 bytes
 MD5: 4a94325d602d4e52f0b3d504545bd5cc
 SHA1: d706427b91bb69ff54bd9726773c590de9872b0c
 SHA256: c2a10d910438b7b7195316227b59bfd929e2a1d839cd0c639d6af1e3f1a0611e

The test data set original audio stream hashes are below:

Table 19 - Original Audio Stream Hash Listing

Digital Multimedia File Name	Audio Stream Hash
IMG_0229.MOV	a01e10fe0a6a296544cbe23e4c97bbf9
IMG_0230.MOV	d2b5e9763320431cf87d1e22c0b68f9e
IMG_0231.MOV	62eb4dc19399c95224168645bae06f64
IMG_0232.MOV	25e426033c91cd6e5ca5fac1f062e1b1
IMG_0233.MOV	7d809c4606eb5082f743c4cafb2c2c3c
IMG_0234.MOV	dcbd06f3fcd6596605494585a6bd3ac1
IMG_0235.MOV	91636f45a4d29b485e33702bd9b2efc7
IMG_0236.MOV	bcedcf6894670e4a9d5a83575320febe
IMG_0237.MOV	0c4689a614c640e1720e3f6abfa7af5c
IMG_0238.MOV	b7aae9490ff10a2ace2cc5c0a1f0c6c1
IMG_0239.MOV	a399da2d290f0e1d7634829bbdb8b736
IMG_0240.MOV	c00b879771728b4cf02ed7b79d960667
IMG_0241.MOV	0e1062a461f30885df2138282444e7d4
IMG_0242.MOV	182389a2804d80aa0087c90ccd83617c
IMG_0243.MOV	085a04edb3040647c610cc2ec84572e7
IMG_0244.MOV	9a7c8f537f0f0f189818bd7ae9aeb562
IMG_0245.MOV	eecca3bde508d5a9aa3f93a67c525a6ca
IMG_0246.MOV	fd6ac88eac58b9b542f552ec4b9a2a02
IMG_0247.MOV	29fafa1d3146fc384d8bbd7a248fd540
IMG_0248.MOV	ba4715fe0634e84d49a6486fc4693727
IMG_0252.MOV	32cb9b34018a776e59f7c8cf87c9f392
IMG_0253.MOV	0489ad4d616e0011ef5b047110ab4c98
IMG_0254.MOV	f8144bce1542758c601213df8236d4a6
IMG_0255.MOV	576add4c10e109bb9305cc9a2ef13632
IMG_0256.MOV	0d1526e49f94f886d3300afca611c5b3
IMG_0257.MOV	7eab5e8b7c6f8290c8145e822559b0d3
IMG_0258.MOV	c3839ab70d98d32be87805be154f8e0c
IMG_0259.MOV	6235502843875198766eaaaf7282ce761
IMG_0260.MOV	64092081a5e7d71e0073701fdaeed1ea

IMG_0261.MOV	0a9e645c6eaf492555c248720798edc5
IMG_0262.MOV	2ce48597463fd5eb9374f98b7f9a2074
IMG_0263.MOV	9f0d8a6b1c452d5f376b6ac175261581
IMG_0264.MOV	0aa2b295709a05b0760c83026b3399bc
IMG_0265.MOV	dbc0a4895ef4800ba7883af7f2897e81
IMG_0266.MOV	963b00e33ec492810b208dbc85f9a2a2
IMG_0267.MOV	9b5294ad8787566fef8a7c82edbe18a8
IMG_0268.MOV	7c7abaf848e6552a2b10c1927be174a9
IMG_0269.MOV	54af5a642071c36edc28d5a093a5a61a
IMG_0270.MOV	c3e863ba40d2c146b004845fbf6b170f
IMG_0271.MOV	43ada8ebe7e2ce82f9e79a091998f92b
IMG_0272.MOV	5fadaa2e49463a3a2d48b1e27623fbd3
IMG_0273.MOV	b03fcba7ed7072514f25f7f3e2ca7494
IMG_0274.MOV	0d3b686101fe43ca2fab853e21f29f74
IMG_0275.MOV	f23418bd6b899188a4fd8cdaa962f206
IMG_0276.MOV	d89caafebe448a12da60335ea2c1e348
IMG_0277.MOV	1d018d290de1f39b47ad4b21ab9451a6
IMG_0278.MOV	5f9bc1403f4b43d41f33f9c895aef144
IMG_0279.MOV	01de9dec69f70b52db7aa0c26d70722f
IMG_0280.MOV	08b40e1fbd1b61a676409648bf014c1e
IMG_0281.MOV	6d52b9d35a6c480ac0de5a656b08a636
IMG_0282.MOV	1bba8842b7b29ea1be73b5fb44cce1c0
IMG_0283.MOV	0550c70f67601c6dfddf6454c56987ad
IMG_0284.MOV	1b74524ebe31db54cfcbf4e034cc69c5
IMG_0285.MOV	c54d25c3b7c79b3d34708a71b5678f22
IMG_0286.MOV	2b01a416a429cfd9cba4ac34917d8677
IMG_0287.MOV	2faf46f539aeb9e89de1ab57b147cdda
IMG_0288.MOV	debc302b921cc6227fb7cf11c3b1e18a
IMG_0289.MOV	e9520165ce82131078e4faadb86a3dad
IMG_0290.MOV	472f6229650fc5f6e88011c9fbae547a
IMG_0291.MOV	853371620fbb23e8007ece1638e59a2a
IMG_0292.MOV	e568da62daf277f8a24358c5b8dfd895
IMG_0293.MOV	55ddd1ba9b04c8c5732464262804826e
IMG_0294.MOV	64d0bdf1d078d2f564803cd1006a5339
IMG_0295.MOV	6e9866efcd104d71956b7c2686fb15d0
IMG_0296.MOV	2b6867ceac45488ba39b826dbbaca421
IMG_0297.MOV	94b2fe005aa0c0353d503583efb1ee2d
IMG_0298.MOV	7d63c94f5da7f79b190c9d1921986195
IMG_0299.MOV	2075d5f030ce484887d7c9cc5f6c3184
IMG_0300.MOV	c54fa2bfd97ad4d0f9580c3e14f37194
IMG_0301.MOV	a5c4f6c0798e20986c5b75af1e6516c7
IMG_0302.MOV	108b89e3c146ed5fe3bee546e9ee5c44
IMG_0303.MOV	26865740c15627e76e913cf5828446b7

IMG_0304.MOV	a22c70614677f9003e4afbd802154240
IMG_0305.MOV	0d70756b6adbf4c4563599e4548004ed
IMG_0306.MOV	238f9bd68c884202cde94ef84f0e7da3
IMG_0307.MOV	310fa26b2a025bb3413d47700960a7da
IMG_0308.MOV	c2f35a9e7a31ce4b565602bcc73779a5
IMG_0309.MOV	179ff72ea22fa337e2385aa2f184b8b7
IMG_0310.MOV	f619b567c15d8781646b7bb2643a2ed8
IMG_0311.MOV	f6770c39b62ee76f6855694ed96791e6
IMG_0312.MOV	e472522b21748ad961b528237503137f
IMG_0313.MOV	468cd2195f3e97e757b018a5475a888f
IMG_0314.MOV	8ca7fa831d1e27e4f22143962af239e3
IMG_0315.MOV	566b56c18857a3b8d5e794e06f4fe584
IMG_0316.MOV	263b1fae5f3f3ccf32b605467a0e55a1
IMG_0317.MOV	a2b9996e7e4aed588b5b868988ae249d
IMG_0318.MOV	816b2f74b91823c55f838a639eb70b3e
IMG_0319.MOV	9f980d3db923c0f0a88786ea63ea9d06
IMG_0320.MOV	6b07b2457c3bf9bd90564fe168702734
IMG_0321.MOV	d4b6ecb21bd5a06d93c54ab131fd61d0
IMG_0322.MOV	bc842776bfeca535c9529c9e81180122
IMG_0323.MOV	bd9d223f1ef34afbcced4fe0ca10f68b
IMG_0324.MOV	58aa3135ba0dc9e1615d85b818f52476
IMG_0325.MOV	c14e987df3f550daf548196db26ad4b9
IMG_0326.MOV	04eb9dee03096457a11a2373b20ab1c2
IMG_0327.MOV	535408e8f23786378cfa71c476b1a941
IMG_0328.MOV	493b399762169d88030191adc4730f58
IMG_0329.MOV	55569c71f226ee26abdda1df2d69310e
IMG_0330.MOV	fedff0cbff0b83e62bb17c2584eaa2a9
IMG_0331.MOV	843328998495b7f6071b69c57a52cf69
IMG_0332.MOV	e75f5cb015921b0deb12be00347f493a
IMG_0333.MOV	2acdbce48c2de1808bd0aa81e80808b8
IMG_0334.MOV	58966e7841efb5d04515516bd980ae38
IMG_0335.MOV	d8df70dc01fbb02d628fab7879af3ce9
IMG_0336.MOV	67c3c69ea73a69194f26f10fa7d85322
IMG_0337.MOV	50c6deaa1b7d2f77b0a3870500787f4f
IMG_0338.MOV	5f3db2b82e6b7c7e848d4f314d19fb14
IMG_0339.MOV	36eeb8f593dea654caa2fa8bb77d2f4b
IMG_0340.MOV	1406245affd45a1833c89c761d3489bc
IMG_0341.MOV	423e7e9e054465cf8fcb5c4821934ab
IMG_0342.MOV	95a7f59e966656c53a4d13adebaa0944
IMG_0343.MOV	77dae41a5d73cfa9c7eeac1659ddf256
IMG_0344.MOV	89b97b114c20d835c62a25e2e9f9ad9c
IMG_0345.MOV	0910cfc669e27cd72f7a96b4c89150bd
IMG_0346.MOV	b2f248532883e0b8b63175ea9b87746c

IMG_0347.MOV	e5ddefd7075e73f5898d4c47dab31bca
IMG_0348.MOV	7e42dabac1de4ba3072cf07ef763a726
IMG_0349.MOV	9c8c11756d0a7dcfe849527cb60d985f
IMG_0350.MOV	35c0ea2ce61887d2d5be35324ed0e2e7
IMG_0351.MOV	c4f373aadd8ad40d74b698e25b2dcdbd7

The test data set original video stream hashes are below:

Table 20 - Original Video Stream Hash Listing

Digital Multimedia File Name	Video Stream Hash
IMG_0229.MOV	e9aa6b620854165be45da111afe3bf78
IMG_0230.MOV	b9c0c89929929b08ba19cd0551d8d577
IMG_0231.MOV	642517d772b6b523fe787775fd0accf0
IMG_0232.MOV	eb8721c7541521ca4f6b0f18da58f2d4
IMG_0233.MOV	e3d5e05f6208faaa26f5695612964b23
IMG_0234.MOV	2c76584373d9b955ddc9f1601bd8593f
IMG_0235.MOV	d13bc4583273c53c108c22f519cfc62a
IMG_0236.MOV	2da4e08a4e467d009b8b4d6e022d3ab9
IMG_0237.MOV	265e5c807c85c238ae9399cca13c54b5
IMG_0238.MOV	e6fe6ed4f9ac233bb4a594d6890220ec
IMG_0239.MOV	52834d5c0b2155a5da6e17370ebca56c
IMG_0240.MOV	6c4c9c547e7808e3330856d3c4e3f3ce
IMG_0241.MOV	661dcd186a1e247255d0d4f4a78b4ed5
IMG_0242.MOV	486cf3c7cfc33ed0f2fa6a7889a74a5c
IMG_0243.MOV	12e6c7240184edd07398865e114af12b
IMG_0244.MOV	ea5f4aba94507ced49979f102ed7f657
IMG_0245.MOV	16926b15a9cfac3bc1dd791fdf28159f
IMG_0246.MOV	9d241b58a71ddeb591b3dd2448294eda
IMG_0247.MOV	3dfc068055fe9fd2e17623a834a95cef
IMG_0248.MOV	a2a041475ff9eddbca8149c54c2d5988
IMG_0252.MOV	bdde00517240ee054ff77902b298b734
IMG_0253.MOV	36d1ce3dfd0ce96f1356c81d6462a8c9
IMG_0254.MOV	505213e44cc70474da39b5a100dc2088
IMG_0255.MOV	586f751a5e1cedc2649181fde1324ffc
IMG_0256.MOV	43fbb9bae47bba6907c596279f9cd33c
IMG_0257.MOV	5e845fcd8d2da053f2a0638ec7f1d8fe
IMG_0258.MOV	b87bd46a722ada54549efb60e41b88c5
IMG_0259.MOV	45f5c0b4f3335e1aa8b0ffeee8ef38c0
IMG_0260.MOV	400737c63f8895fdb97603401fd968c4
IMG_0261.MOV	7122ec4145ec22cada64cf5fe17a075b
IMG_0262.MOV	ea9720c91000eadc82bea884b9914f70
IMG_0263.MOV	673d77c7957c5d87fb5fdc5f941f7b34

IMG_0264.MOV	d884b2c302d6ad65c974d73b21b35b98
IMG_0265.MOV	b018eb41deb914b2bd5fb3c85216400b
IMG_0266.MOV	951aeeb9ec053de592bbeff5dd1b4d83
IMG_0267.MOV	39abfdcf854b5ac4f9f611db0e1033eb
IMG_0268.MOV	fe395f07f8012c713777215965cca929
IMG_0269.MOV	b292ed63753cd0c3a32fd95b9ec16e74
IMG_0270.MOV	flc4891f2842d4d2758097c76fae4995
IMG_0271.MOV	453bfb44fb8d15c15df81d578c453627
IMG_0272.MOV	199babe9a13eb67cddb0f5f46c665609
IMG_0273.MOV	a4eddfc8052c6b512155aca9313d3326
IMG_0274.MOV	a303ea48304b99289529f9a619e900b6
IMG_0275.MOV	60ab627cb090e2fcee122858ff14f240
IMG_0276.MOV	a65d5f2c95e640a997a74e6b10a6f34d
IMG_0277.MOV	185416b1aeecf87a3282b111cb1c5b08
IMG_0278.MOV	dad03ad588a5f76033a87d68759a63f2
IMG_0279.MOV	c6730264d5fadb45394cd56a3d2178e0
IMG_0280.MOV	87b97b493232305bc7a652e94208e1f3
IMG_0281.MOV	91a9eccee83826ccf8dcb8f0dc23c3f3
IMG_0282.MOV	016b00a338882f4a9526265efd027c84
IMG_0283.MOV	f55a600b4223fcf481d670a379eef0f0
IMG_0284.MOV	8bf095f3ec474a5fb6e7c3c92dc700ef
IMG_0285.MOV	38261b482498a54cb56e475f854025f8
IMG_0286.MOV	573c0dd9c98b7c0d0a7136bcb2a5da8
IMG_0287.MOV	fd0ea1a5d96d57311455f2df5c94fac1
IMG_0288.MOV	b11ab853f48c59bf7f426c5521f3a25c
IMG_0289.MOV	b4d102c3f26c619bfa73b34319cb8877
IMG_0290.MOV	bc09399c0e34945e7f6af114bd3c75a5
IMG_0291.MOV	4304de6ccc44ac15aca2c57f2f89c0f5
IMG_0292.MOV	55daa2af20299b909bdc51b3a2e93a67
IMG_0293.MOV	de4a12f2c037da6c80b04d65698afdf4
IMG_0294.MOV	a5b30589ccb5319e4f594be3346039de
IMG_0295.MOV	c35072457f64f7584a69f29a9b7c5d49
IMG_0296.MOV	9fb1f245d4b86e7d272041892baaa92a
IMG_0297.MOV	1d458aec0d671e178358098c8da8902
IMG_0298.MOV	8e98c3c75b92386f55f16d3fdead00b0
IMG_0299.MOV	77ef0b6697186c3b556fa87b1e53836c
IMG_0300.MOV	2f42fabab17e3e87b86a4c2dc34a6e17
IMG_0301.MOV	5d237e1bc2838e0b80f35caa01967926
IMG_0302.MOV	e111543f19f4d8589b8091699282b175
IMG_0303.MOV	bb796495eb6151b794a6ffa38f5e727c
IMG_0304.MOV	8e660c54af834f983a5e0cafdcbd2a21
IMG_0305.MOV	fcc60b29bde6423a377002cbc70ada03
IMG_0306.MOV	32a4ec283654c7be993b4098beaa0640

IMG_0307.MOV	90e2c6908ecbcbfcb7610c4475061ec7
IMG_0308.MOV	9f24f356315b984871c44635e08f1b9e
IMG_0309.MOV	6b92925a37fed496653604c83d121c0b
IMG_0310.MOV	bcd4448dafa28d39f06da6b7e073a82
IMG_0311.MOV	964b0a9c365d95f2a5887222e0387b8a
IMG_0312.MOV	3cfafeb8cee58da800c28b83d7a60167
IMG_0313.MOV	4b73530e9739fab93669b79660510495
IMG_0314.MOV	271ea44d50b766e009083104123d1f85
IMG_0315.MOV	393f3701824e6f5b4e6cc48a16626225
IMG_0316.MOV	d61eee9810735fed7ec3d3d3e9d9fa3e
IMG_0317.MOV	e19b73e587aaadadd4d192e08825e470
IMG_0318.MOV	cc75205ccae8cf6eda2f764103856911
IMG_0319.MOV	469e60c5b1a2d120ba072fd50d05402e
IMG_0320.MOV	b84432607eeb5670d336013b4c44cd00
IMG_0321.MOV	b8944f7583753ac8cd37a40c297ac415
IMG_0322.MOV	c53eddae41eb07299686fc811df27c31
IMG_0323.MOV	bec0cd11cbfad8141e83c50bced46d
IMG_0324.MOV	b413c065df5524a921d37f80f06f7b72
IMG_0325.MOV	7ba0c4c312bd4658e5f4d4bd69631a31
IMG_0326.MOV	12722df242daa3a4e76856084a9b3e2f
IMG_0327.MOV	ad68a1f0a4e5573dd7a958d26f6a5033
IMG_0328.MOV	071402624011cc2948949e349c484713
IMG_0329.MOV	375b3ceeadd0b91e5c56c1b770372439
IMG_0330.MOV	cb302a3676ea177c3b9258093e9f525a
IMG_0331.MOV	1a29798fd548fcaa03fca116e69fabdc
IMG_0332.MOV	3b3bcd3fb7972560ce8287e6889b353
IMG_0333.MOV	bab7bc20bb5b6c71d9c51fa741476676
IMG_0334.MOV	7a3c0068864730a7c24919f4e26a88ef
IMG_0335.MOV	c91b181e199d256283e03b72646d34da
IMG_0336.MOV	f8ac923aee44c53f9ea4a66156e84f58
IMG_0337.MOV	c22f7bc51eed4cb9c4eab3b59f1d5d1b
IMG_0338.MOV	7aab922d74a0e81db39366161630a907
IMG_0339.MOV	c028bcfa11a7af93135671d20970a755
IMG_0340.MOV	f6402abc91b6bb755ec1d4616b5a006c
IMG_0341.MOV	40a119ca092624da5d7ddd0fc910f1a6
IMG_0342.MOV	34bfb5362164455ccaf3f04b3fb32123
IMG_0343.MOV	a2aa112c049b2e44513a196b2b044656
IMG_0344.MOV	d80dac76f6f828a1d6e3a211f9afa537
IMG_0345.MOV	edc6111dae978d1b08c8217e87e7a7c5
IMG_0346.MOV	a4aa4b34fb2599459df37b5c26a1fab6
IMG_0347.MOV	9922be7e400e446ed7ba6ec112d0beef
IMG_0348.MOV	09220163a91b2bbefd77b26bdb8f8b8f
IMG_0349.MOV	bdf70e16eb7109325b1b7e83c5afc2f8

IMG 0350.MOV	fadeb87719725fea952188a7b4fd35d2
IMG 0351.MOV	ae8f06744a7b9ff08dbd22d90d3ec1f2

APPENDIX D-3

METHOD VALIDATION TEST SCENARIO

Test # 1

Test Title: Multimedia Stream Hash Validation Method

Test Date: 3/12/2019

Test Description

This test will evaluate the technique of audio stream hash validation when an audio stream is bifurcated from a video digital multimedia file for subsequent authentication.

Test Materials

Test System Software

OS Name & Version: Microsoft Windows 10 Home

Test System Hardware:

System Manufacturer: Hewlett Packard

System Model: Envy

Processor: Intel Core i5 7200U CPU @ 2.50 GHz

Test Data Set:

The test data set is made up of 100 video files created with an iPhone 8Plus with iOS 11.2.6 using Live Photo to create photographs. The 100 video files were side car / derivative of the Live Photo process. The movie files contain both video and audio streams. The video codec of each file was High Efficiency Video Coding (HEVC) and the audio codec of each file was Linear Pulse Code Modulation (LPCM). Refer to test plan for details of test data set.

Test Method

Test Notes:

The test preparation established the original hashes of the audio streams of the respective files for subsequent comparison.

Test Procedures:

1. Forensically copy each test data set's audio stream to a wave PCM audio digital multimedia file.
2. Hash the audio stream in each derivative wave PCM audio digital multimedia file.
3. Analyze results of transcoding process.

Test Data

Expected Test Results:

1. Hashes of respective multimedia streams in original file and multimedia streams in new digital multimedia files match.
2. Demonstrate reproducibility by Warren et al., (2012) as generally discussed in their research [65] and Whitecotton (2017) [20].
3. Demonstrate repeatability by tester.
4. Demonstrate accuracy and precision by the exactness of the hashes used.

Actual Test Results:

1. Forensically copy each test data set's audio stream to a wave PCM audio digital multimedia file.

Wrote a script to use FFmpeg version N-90908-g0807a77160 to transcode the all (100) original test data set files' audio streams to derivative wave PCM audio digital multimedia files with similar names. Executed without issues.

2. Hash the audio stream in each derivative wave PCM audio digital multimedia file.

Wrote a script to use FFmpeg to hash audio streams of all 100 derivative wave PCM audio digital multimedia files. Executed without issues.

Validation of Test Data:

Validation is tested by comparison (original multimedia stream versus copied multimedia stream).

Table 21 - Validation Test Comparison Of Original Versus Copied Audio Stream Hashes

Digital multimedia file Name	Original Audio Stream Hash	Analysis	Audio Stream Hash Of Extract File	Transcoded File
IMG 0229.MOV	a01e10fe0a6a296544cbe23e4c97bbf9	Matched	a01e10fe0a6a296544cbe23e4c97bbf9	IMG 0229 audio.wav
IMG 0230.MOV	d2b5e9763320431cf87d1e22c0b68f9e	Matched	d2b5e9763320431cf87d1e22c0b68f9e	IMG 0230 audio.wav
IMG 0231.MOV	62eb4dc19399c95224168645bae06f64	Matched	62eb4dc19399c95224168645bae06f64	IMG 0231 audio.wav
IMG 0232.MOV	25e426033c91cd6e5ca5fac1f062e1b1	Matched	25e426033c91cd6e5ca5fac1f062e1b1	IMG 0232 audio.wav
IMG 0233.MOV	7d809c4606eb5082f743c4afb2c2c3c	Matched	7d809c4606eb5082f743c4afb2c2c3c	IMG 0233 audio.wav
IMG 0234.MOV	dcdb06f3fcd6596605494585a6bd3ac1	Matched	dcdb06f3fcd6596605494585a6bd3ac1	IMG 0234 audio.wav
IMG 0235.MOV	91636f45a4d29b485e33702bd9b2efc7	Matched	91636f45a4d29b485e33702bd9b2efc7	IMG 0235 audio.wav
IMG 0236.MOV	bcedcf6894670e4a9d5a83575320febe	Matched	bcedcf6894670e4a9d5a83575320febe	IMG 0236 audio.wav
IMG 0237.MOV	0c4689a614c640e1720e3f6abfa7af5c	Matched	0c4689a614c640e1720e3f6abfa7af5c	IMG 0237 audio.wav
IMG 0238.MOV	b7aae9490ff10a2ace2cc5c0a1f0c6c1	Matched	b7aae9490ff10a2ace2cc5c0a1f0c6c1	IMG 0238 audio.wav
IMG 0239.MOV	a399da2d290f0e1d7634829b8db8b736	Matched	a399da2d290f0e1d7634829b8db8b736	IMG 0239 audio.wav
IMG 0240.MOV	c00b879771728b4cf02ed7b79d960667	Matched	c00b879771728b4cf02ed7b79d960667	IMG 0240 audio.wav
IMG 0241.MOV	0e1062a461f30885df2138282444e7d4	Matched	0e1062a461f30885df2138282444e7d4	IMG 0241 audio.wav
IMG 0242.MOV	182389a2804d80aa0087c90ccd83617c	Matched	182389a2804d80aa0087c90ccd83617c	IMG 0242 audio.wav
IMG 0243.MOV	085a04edb3040647c610cc2ec84572e7	Matched	085a04edb3040647c610cc2ec84572e7	IMG 0243 audio.wav
IMG 0244.MOV	9a7c8f537f0f0f189818bd7ae9aeb562	Matched	9a7c8f537f0f0f189818bd7ae9aeb562	IMG 0244 audio.wav

IMG_0245.MOV	eeca3bde508d5a9aa3f93a67c525a6ca	Matched	eeca3bde508d5a9aa3f93a67c525a6ca	IMG_0245 audio.wav
IMG_0246.MOV	fd6ac88eac58b9b542f552ec4b9a2a02	Matched	fd6ac88eac58b9b542f552ec4b9a2a02	IMG_0246 audio.wav
IMG_0247.MOV	29fafa1d3146fc384d8bbd7a248fd540	Matched	29fafa1d3146fc384d8bbd7a248fd540	IMG_0247 audio.wav
IMG_0248.MOV	ba4715fe0634e84d49a6486fc4693727	Matched	ba4715fe0634e84d49a6486fc4693727	IMG_0248 audio.wav
IMG_0252.MOV	32cb9b34018a776e59f7c8cf87c9f392	Matched	32cb9b34018a776e59f7c8cf87c9f392	IMG_0252 audio.wav
IMG_0253.MOV	0489ad4d616e0011ef5b047110ab4c98	Matched	0489ad4d616e0011ef5b047110ab4c98	IMG_0253 audio.wav
IMG_0254.MOV	f8144bce1542758c601213df8236d4a6	Matched	f8144bce1542758c601213df8236d4a6	IMG_0254 audio.wav
IMG_0255.MOV	576add4c10e109bb9305cc9a2ef13632	Matched	576add4c10e109bb9305cc9a2ef13632	IMG_0255 audio.wav
IMG_0256.MOV	0d1526e49f94f886d3300afca611c5b3	Matched	0d1526e49f94f886d3300afca611c5b3	IMG_0256 audio.wav
IMG_0257.MOV	7eab5e8b7c6f8290c8145e822559b0d3	Matched	7eab5e8b7c6f8290c8145e822559b0d3	IMG_0257 audio.wav
IMG_0258.MOV	c3839ab70d98d32be87805be154f8e0c	Matched	c3839ab70d98d32be87805be154f8e0c	IMG_0258 audio.wav
IMG_0259.MOV	6235502843875198766eaf7282ce761	Matched	6235502843875198766eaf7282ce761	IMG_0259 audio.wav
IMG_0260.MOV	64092081a5e7d71e0073701fdae1ea	Matched	64092081a5e7d71e0073701fdae1ea	IMG_0260 audio.wav
IMG_0261.MOV	0a9e645c6eaf492555c248720798ede5	Matched	0a9e645c6eaf492555c248720798ede5	IMG_0261 audio.wav
IMG_0262.MOV	2ce48597463fd5eb9374f98b7f9a2074	Matched	2ce48597463fd5eb9374f98b7f9a2074	IMG_0262 audio.wav
IMG_0263.MOV	9f0d8a6b1c452d5f376b6ac175261581	Matched	9f0d8a6b1c452d5f376b6ac175261581	IMG_0263 audio.wav
IMG_0264.MOV	0aa2b295709a05b0760c83026b3399bc	Matched	0aa2b295709a05b0760c83026b3399bc	IMG_0264 audio.wav
IMG_0265.MOV	dbc0a4895ef4800ba7883af7f2897e81	Matched	dbc0a4895ef4800ba7883af7f2897e81	IMG_0265 audio.wav
IMG_0266.MOV	963b00e33ec492810b208dbc85f9a2a2	Matched	963b00e33ec492810b208dbc85f9a2a2	IMG_0266 audio.wav
IMG_0267.MOV	9b5294ad8787566fef8a7c82edbe18a8	Matched	9b5294ad8787566fef8a7c82edbe18a8	IMG_0267 audio.wav
IMG_0268.MOV	7c7abaf848e6552a2b10c1927be174a9	Matched	7c7abaf848e6552a2b10c1927be174a9	IMG_0268 audio.wav
IMG_0269.MOV	54af5a642071c36edc28d5a093a5a61a	Matched	54af5a642071c36edc28d5a093a5a61a	IMG_0269 audio.wav
IMG_0270.MOV	c3e863ba40d2c146b004845fbf6b170f	Matched	c3e863ba40d2c146b004845fbf6b170f	IMG_0270 audio.wav
IMG_0271.MOV	43ada8ebe7e2ce82f9e79a091998f92b	Matched	43ada8ebe7e2ce82f9e79a091998f92b	IMG_0271 audio.wav
IMG_0272.MOV	5fadaa2e49463a3a2d48b1e27623bd3	Matched	5fadaa2e49463a3a2d48b1e27623bd3	IMG_0272 audio.wav
IMG_0273.MOV	b03fcb7ed7072514f25f7f3e2ca7494	Matched	b03fcb7ed7072514f25f7f3e2ca7494	IMG_0273 audio.wav
IMG_0274.MOV	0d3b686101fe43ca2fab853e21f29f74	Matched	0d3b686101fe43ca2fab853e21f29f74	IMG_0274 audio.wav
IMG_0275.MOV	f23418bd6b899188a4fd8cdad962f206	Matched	f23418bd6b899188a4fd8cdad962f206	IMG_0275 audio.wav
IMG_0276.MOV	d89caafebe448a12da60335ea2c1e348	Matched	d89caafebe448a12da60335ea2c1e348	IMG_0276 audio.wav
IMG_0277.MOV	1d018d290de1f39b47ad4b21ab9451a6	Matched	1d018d290de1f39b47ad4b21ab9451a6	IMG_0277 audio.wav
IMG_0278.MOV	5f9bc1403f4b43d41f33f9c895aef144	Matched	5f9bc1403f4b43d41f33f9c895aef144	IMG_0278 audio.wav
IMG_0279.MOV	01de9dec69f70b52db7aa0c26d70722f	Matched	01de9dec69f70b52db7aa0c26d70722f	IMG_0279 audio.wav
IMG_0280.MOV	08b40e1fbd1b61a676409648bf014c1e	Matched	08b40e1fbd1b61a676409648bf014c1e	IMG_0280 audio.wav
IMG_0281.MOV	6d52b9d35a6c480ac0de5a656b08a636	Matched	6d52b9d35a6c480ac0de5a656b08a636	IMG_0281 audio.wav
IMG_0282.MOV	1bba8842b7b29ea1be73b5fb44cce1c0	Matched	1bba8842b7b29ea1be73b5fb44cce1c0	IMG_0282 audio.wav
IMG_0283.MOV	0550c70f67601c6dfdd6454c56987ad	Matched	0550c70f67601c6dfdd6454c56987ad	IMG_0283 audio.wav
IMG_0284.MOV	1b74524ebe31db54cfbf4e034cc69c5	Matched	1b74524ebe31db54cfbf4e034cc69c5	IMG_0284 audio.wav
IMG_0285.MOV	c54d25c3b7c79b3d34708a71b5678f22	Matched	c54d25c3b7c79b3d34708a71b5678f22	IMG_0285 audio.wav
IMG_0286.MOV	2b01a416a429cfd9cba4ac34917d8677	Matched	2b01a416a429cfd9cba4ac34917d8677	IMG_0286 audio.wav
IMG_0287.MOV	2faf46f539aeb9e89de1ab57b147cdda	Matched	2faf46f539aeb9e89de1ab57b147cdda	IMG_0287 audio.wav
IMG_0288.MOV	debc302b921cc6227fb7cf1c3b1e18a	Matched	debc302b921cc6227fb7cf1c3b1e18a	IMG_0288 audio.wav
IMG_0289.MOV	e9520165ce82131078e4faadb86a3dad	Matched	e9520165ce82131078e4faadb86a3dad	IMG_0289 audio.wav
IMG_0290.MOV	472f6229650fe5f6e88011c9fbae547a	Matched	472f6229650fe5f6e88011c9fbae547a	IMG_0290 audio.wav

IMG 0291.MOV	853371620fbb23e8007ece1638e59a2a	Matched	853371620fbb23e8007ece1638e59a2a	IMG 0291 audio.wav
IMG 0292.MOV	e568da62daf277f8a24358c5b8dfd895	Matched	e568da62daf277f8a24358c5b8dfd895	IMG 0292 audio.wav
IMG 0293.MOV	55ddd1ba9b04c8c5732464262804826e	Matched	55ddd1ba9b04c8c5732464262804826e	IMG 0293 audio.wav
IMG 0294.MOV	64d0bdf1d078d2f564803cd1006a5339	Matched	64d0bdf1d078d2f564803cd1006a5339	IMG 0294 audio.wav
IMG 0295.MOV	6e9866efcd104d71956b7c2686fb15d0	Matched	6e9866efcd104d71956b7c2686fb15d0	IMG 0295 audio.wav
IMG 0296.MOV	2b6867ceac45488ba39b826dbbaca421	Matched	2b6867ceac45488ba39b826dbbaca421	IMG 0296 audio.wav
IMG 0297.MOV	94b2fe005aa0c0353d503583efb1ee2d	Matched	94b2fe005aa0c0353d503583efb1ee2d	IMG 0297 audio.wav
IMG 0298.MOV	7d63c94f5da7f79b190c9d1921986195	Matched	7d63c94f5da7f79b190c9d1921986195	IMG 0298 audio.wav
IMG 0299.MOV	2075d5f030ce484887d7c9cc5f6c3184	Matched	2075d5f030ce484887d7c9cc5f6c3184	IMG 0299 audio.wav
IMG 0300.MOV	c54fa2bfd97ad4d0f9580c3e14f37194	Matched	c54fa2bfd97ad4d0f9580c3e14f37194	IMG 0300 audio.wav
IMG 0301.MOV	a5c4f6c0798e20986c5b75af1e6516c7	Matched	a5c4f6c0798e20986c5b75af1e6516c7	IMG 0301 audio.wav
IMG 0302.MOV	108b89e3c146ed5fe3bee546e9ee5c44	Matched	108b89e3c146ed5fe3bee546e9ee5c44	IMG 0302 audio.wav
IMG 0303.MOV	26865740c15627e76e913cf5828446b7	Matched	26865740c15627e76e913cf5828446b7	IMG 0303 audio.wav
IMG 0304.MOV	a22c70614677f9003e4afbd802154240	Matched	a22c70614677f9003e4afbd802154240	IMG 0304 audio.wav
IMG 0305.MOV	0d70756b6adbf4c4563599e4548004ed	Matched	0d70756b6adbf4c4563599e4548004ed	IMG 0305 audio.wav
IMG 0306.MOV	238f9bd68c884202cde94ef84f0e7da3	Matched	238f9bd68c884202cde94ef84f0e7da3	IMG 0306 audio.wav
IMG 0307.MOV	310fa26b2a025bb3413d47700960a7da	Matched	310fa26b2a025bb3413d47700960a7da	IMG 0307 audio.wav
IMG 0308.MOV	c2f35a9e7a31ce4b565602bcc73779a5	Matched	c2f35a9e7a31ce4b565602bcc73779a5	IMG 0308 audio.wav
IMG 0309.MOV	179ff72ea22fa337e2385aa2f184b8b7	Matched	179ff72ea22fa337e2385aa2f184b8b7	IMG 0309 audio.wav
IMG 0310.MOV	f619b567c15d8781646b7bb2643a2ed8	Matched	f619b567c15d8781646b7bb2643a2ed8	IMG 0310 audio.wav
IMG 0311.MOV	f6770c39b62ee76f6855694ed96791e6	Matched	f6770c39b62ee76f6855694ed96791e6	IMG 0311 audio.wav
IMG 0312.MOV	e472522b21748ad961b528237503137f	Matched	e472522b21748ad961b528237503137f	IMG 0312 audio.wav
IMG 0313.MOV	468cd2195f3e97e757b018a5475a888f	Matched	468cd2195f3e97e757b018a5475a888f	IMG 0313 audio.wav
IMG 0314.MOV	8ca7fa831d1e27e4f22143962af239e3	Matched	8ca7fa831d1e27e4f22143962af239e3	IMG 0314 audio.wav
IMG 0315.MOV	566b56c18857a3b8d5e794e06f4fe584	Matched	566b56c18857a3b8d5e794e06f4fe584	IMG 0315 audio.wav
IMG 0316.MOV	263b1fae5f3f3ccf32b605467a0e55a1	Matched	263b1fae5f3f3ccf32b605467a0e55a1	IMG 0316 audio.wav
IMG 0317.MOV	a2b9996e7e4aed588b5b868988ae249d	Matched	a2b9996e7e4aed588b5b868988ae249d	IMG 0317 audio.wav
IMG 0318.MOV	816b2f74b91823c55f838a639eb70b3e	Matched	816b2f74b91823c55f838a639eb70b3e	IMG 0318 audio.wav
IMG 0319.MOV	9f980d3db923c0f0a88786ea63ea9d06	Matched	9f980d3db923c0f0a88786ea63ea9d06	IMG 0319 audio.wav
IMG 0320.MOV	6b07b2457c3bf9bd90564fe168702734	Matched	6b07b2457c3bf9bd90564fe168702734	IMG 0320 audio.wav
IMG 0321.MOV	d4b6ecb21bd5a06d93c54ab131fd61d0	Matched	d4b6ecb21bd5a06d93c54ab131fd61d0	IMG 0321 audio.wav
IMG 0322.MOV	bc842776bfeea535c9529c9e81180122	Matched	bc842776bfeea535c9529c9e81180122	IMG 0322 audio.wav
IMG 0323.MOV	bd9d223f1ef34afbcced4fe0ca10f68b	Matched	bd9d223f1ef34afbcced4fe0ca10f68b	IMG 0323 audio.wav
IMG 0324.MOV	58aa3135ba0dc9e1615d85b818f52476	Matched	58aa3135ba0dc9e1615d85b818f52476	IMG 0324 audio.wav
IMG 0325.MOV	c14e987df3f550daf548196db26ad4b9	Matched	c14e987df3f550daf548196db26ad4b9	IMG 0325 audio.wav
IMG 0326.MOV	04eb9dee03096457a11a2373b20ab1c2	Matched	04eb9dee03096457a11a2373b20ab1c2	IMG 0326 audio.wav
IMG 0327.MOV	535408e8f23786378cfa71c476b1a941	Matched	535408e8f23786378cfa71c476b1a941	IMG 0327 audio.wav
IMG 0328.MOV	493b399762169d88030191adc4730f58	Matched	493b399762169d88030191adc4730f58	IMG 0328 audio.wav
IMG 0329.MOV	55569c71f226ee26abdda1df2d69310e	Matched	55569c71f226ee26abdda1df2d69310e	IMG 0329 audio.wav
IMG 0330.MOV	fedff0cbff0b83e62bb17c2584eaa2a9	Matched	fedff0cbff0b83e62bb17c2584eaa2a9	IMG 0330 audio.wav
IMG 0331.MOV	843328998495b7f6071b69c57a52cf69	Matched	843328998495b7f6071b69c57a52cf69	IMG 0331 audio.wav

Analysis & Discussion of Test Data

The hashes of respective audio streams in original file and audio streams in transcoded derivative digital multimedia files matched 100% (100 files out of 100). This demonstrated reproducibility as noted by Warren et al., (2012) as generally discussed in their research [65] and Whitecotton (2017) [20]. This demonstrated repeatability. The test demonstrated accuracy and precision by the exactness of the hash used. The numerical probability of a random collision for MD5 hash is 1 in 2^{64} (about 1 in 1.84×10^{19}) [66].

Test Results

This test has demonstrated that multimedia stream hash validation method, as it relates to audio streams, is a viable method for consideration for use in the video authentication process when transcoding the audio stream for further authentication.

APPENDIX D-4

METHOD VALIDATION TEST SCENARIO

Test # 2

Test Title: Multimedia (Video) Stream Hash Validation Method

Test Date: 3/12/2019

Test Description

This test will evaluate the technique of video stream hash validation when an video stream is bifurcated from a video digital multimedia file for subsequent authentication.

Test Materials

Test System Software

OS Name & Version: Microsoft Windows 10 Home

Test System Hardware:

System Manufacturer: Hewlett Packard

System Model: Envy

Processor: Intel Core i5 7200U CPU @ 2.50 GHz

Test Data Set:

The test data set is made up of 100 video files created with an iPhone 8Plus with iOS 11.2.6 using Live Photo to create photographs. The 100 video files were side car / derivative of the Live Photo process. The movie files contain both video and audio streams. The video codec of each file was High Efficiency Video Coding (HEVC) and the audio codec of each file was Linear Pulse Code Modulation (LPCM). Refer to test plan for details of test data set.

Test Method

Test Notes:

The test preparation established the original hashes of the video streams of the respective files for subsequent comparison.

Test Procedures:

1. Forensically copy each test data set's video stream to an MP4 digital multimedia file.
2. Hash the video stream in each derivative MP4 video digital multimedia file.
3. Analyze results of transcoding process.

Test Data

Expected Test Results:

1. Hashes of respective multimedia streams in original file and multimedia streams in new digital multimedia files match.

2. Demonstrate reproducibility by Warren et al., (2012) as generally discussed in their research [65] and Whitecotton (2017) [20].
3. Demonstrate repeatability by tester.
4. Demonstrate accuracy and precision by the exactness of the hashes used.

Actual Test Results:

1. Forensically copy each test data set's video stream to an MP4 video digital multimedia file.

Wrote a script to use FFmpeg version N-90908-g0807a77160 to transcode the all (100) original test data set files' video streams to derivative MP4 video digital multimedia files with similar names. Executed without issues.

2. Hash the video stream in each derivative MP4 video digital multimedia file.

Wrote a script to use FFmpeg to hash video streams of all 100 derivative MP4 video digital multimedia files. Executed without issues.

Validation of Test Data:

Validation is tested by comparison (original multimedia stream versus copied multimedia stream).

Table 22 - Validation Test Comparison Of Original Versus Copied Video Stream Hashes

Original File	Original Video Stream Hash	Analysis	Video Stream Hash Of Extracted File	Transcoded File
IMG_0229.MOV	e9aa6b620854165be45da111afe3bf78	Matched	e9aa6b620854165be45da111afe3bf78	IMG_0229_video.mp4
IMG_0230.MOV	b9c0c89929929b08ba19cd0551d8d577	Matched	b9c0c89929929b08ba19cd0551d8d577	IMG_0230_video.mp4
IMG_0231.MOV	642517d772b6b523fe787775fd0accf0	Matched	642517d772b6b523fe787775fd0accf0	IMG_0231_video.mp4
IMG_0232.MOV	eb8721c7541521ca4f6b0f18da58f2d4	Matched	eb8721c7541521ca4f6b0f18da58f2d4	IMG_0232_video.mp4
IMG_0233.MOV	e3d5e05f6208faaa26f5695612964b23	Matched	e3d5e05f6208faaa26f5695612964b23	IMG_0233_video.mp4
IMG_0234.MOV	2c76584373d9b955ddc9f1601bd8593f	Matched	2c76584373d9b955ddc9f1601bd8593f	IMG_0234_video.mp4
IMG_0235.MOV	d13bc4583273c53c108c22f519cfc62a	Matched	d13bc4583273c53c108c22f519cfc62a	IMG_0235_video.mp4
IMG_0236.MOV	2da4e08a4e467d009b8b4d6e022d3ab9	Matched	2da4e08a4e467d009b8b4d6e022d3ab9	IMG_0236_video.mp4
IMG_0237.MOV	265e5c807c85c238ae9399cca13c54b5	Matched	265e5c807c85c238ae9399cca13c54b5	IMG_0237_video.mp4
IMG_0238.MOV	e6fe6ed4f9ac233bb4a594d6890220ec	Matched	e6fe6ed4f9ac233bb4a594d6890220ec	IMG_0238_video.mp4
IMG_0239.MOV	52834d5c0b2155a5da6e17370ebca56c	Matched	52834d5c0b2155a5da6e17370ebca56c	IMG_0239_video.mp4
IMG_0240.MOV	6c4c9c547e7808e3330856d3c4e3f3ce	Matched	6c4c9c547e7808e3330856d3c4e3f3ce	IMG_0240_video.mp4
IMG_0241.MOV	661dcd186a1e247255d0d4f4a78b4ed5	Matched	661dcd186a1e247255d0d4f4a78b4ed5	IMG_0241_video.mp4
IMG_0242.MOV	486cf3c7cfc33ed0f2fa6a7889a74a5c	Matched	486cf3c7cfc33ed0f2fa6a7889a74a5c	IMG_0242_video.mp4
IMG_0243.MOV	12e6c7240184edd07398865e114af12b	Matched	12e6c7240184edd07398865e114af12b	IMG_0243_video.mp4
IMG_0244.MOV	ea5f4aba94507ced49979f102ed7f657	Matched	ea5f4aba94507ced49979f102ed7f657	IMG_0244_video.mp4
IMG_0245.MOV	16926b15a9cfac3bc1dd791fd28159f	Matched	16926b15a9cfac3bc1dd791fd28159f	IMG_0245_video.mp4
IMG_0246.MOV	9d241b58a71ddeb591b3dd2448294eda	Matched	9d241b58a71ddeb591b3dd2448294eda	IMG_0246_video.mp4
IMG_0247.MOV	3dfc068055fe9fd2e17623a834a95cef	Matched	3dfc068055fe9fd2e17623a834a95cef	IMG_0247_video.mp4
IMG_0248.MOV	a2a041475ff9eddbca8149c54c2d5988	Matched	a2a041475ff9eddbca8149c54c2d5988	IMG_0248_video.mp4

IMG_0252.MOV	bdde00517240ee054ff77902b298b734	Matched	bdde00517240ee054ff77902b298b734	IMG_0252 video.mp4
IMG_0253.MOV	36d1ce3dfd0ce96f1356c81d6462a8c9	Matched	36d1ce3dfd0ce96f1356c81d6462a8c9	IMG_0253 video.mp4
IMG_0254.MOV	505213e44cc70474da39b5a100dc2088	Matched	505213e44cc70474da39b5a100dc2088	IMG_0254 video.mp4
IMG_0255.MOV	586f751a5e1cedc2649181fde1324ffc	Matched	586f751a5e1cedc2649181fde1324ffc	IMG_0255 video.mp4
IMG_0256.MOV	43fbb9bae47bba6907c596279f9cd33c	Matched	43fbb9bae47bba6907c596279f9cd33c	IMG_0256 video.mp4
IMG_0257.MOV	5e845fcd8d2da053f2a0638ec7f1d8fe	Matched	5e845fcd8d2da053f2a0638ec7f1d8fe	IMG_0257 video.mp4
IMG_0258.MOV	b87bd46a722ada54549efb60e41b88c5	Matched	b87bd46a722ada54549efb60e41b88c5	IMG_0258 video.mp4
IMG_0259.MOV	45f5c0b4f3335e1aa8b0ffeee8ef38c0	Matched	45f5c0b4f3335e1aa8b0ffeee8ef38c0	IMG_0259 video.mp4
IMG_0260.MOV	400737c63f8895fdb97603401fd968c4	Matched	400737c63f8895fdb97603401fd968c4	IMG_0260 video.mp4
IMG_0261.MOV	7122ec4145ec22cada64cf5fe17a075b	Matched	7122ec4145ec22cada64cf5fe17a075b	IMG_0261 video.mp4
IMG_0262.MOV	ea9720c91000eadc82bea884b9914f70	Matched	ea9720c91000eadc82bea884b9914f70	IMG_0262 video.mp4
IMG_0263.MOV	673d77c7957c5d87fb5fde5f941f7b34	Matched	673d77c7957c5d87fb5fde5f941f7b34	IMG_0263 video.mp4
IMG_0264.MOV	d884b2c302d6ad65c974d73b21b35b98	Matched	d884b2c302d6ad65c974d73b21b35b98	IMG_0264 video.mp4
IMG_0265.MOV	b018eb41deb914b2bd5fb3c85216400b	Matched	b018eb41deb914b2bd5fb3c85216400b	IMG_0265 video.mp4
IMG_0266.MOV	951aeeb9ec053de592bbef5dd1b4d83	Matched	951aeeb9ec053de592bbef5dd1b4d83	IMG_0266 video.mp4
IMG_0267.MOV	39abfdcf854b5ac4f9f611db0e1033eb	Matched	39abfdcf854b5ac4f9f611db0e1033eb	IMG_0267 video.mp4
IMG_0268.MOV	fe395f07f8012c713777215965cca929	Matched	fe395f07f8012c713777215965cca929	IMG_0268 video.mp4
IMG_0269.MOV	b292ed63753cd0c3a32fd95b9ec16e74	Matched	b292ed63753cd0c3a32fd95b9ec16e74	IMG_0269 video.mp4
IMG_0270.MOV	f1c4891f2842d4d2758097c76fae4995	Matched	f1c4891f2842d4d2758097c76fae4995	IMG_0270 video.mp4
IMG_0271.MOV	453bfb44fb8d15c15df81d578c453627	Matched	453bfb44fb8d15c15df81d578c453627	IMG_0271 video.mp4
IMG_0272.MOV	199babe9a13eb67cddb0f5f46c665609	Matched	199babe9a13eb67cddb0f5f46c665609	IMG_0272 video.mp4
IMG_0273.MOV	a4eddfc8052c6b512155aca9313d3326	Matched	a4eddfc8052c6b512155aca9313d3326	IMG_0273 video.mp4
IMG_0274.MOV	a303ea48304b99289529f9a619e900b6	Matched	a303ea48304b99289529f9a619e900b6	IMG_0274 video.mp4
IMG_0275.MOV	60ab627cb090e2fcee122858ff14f240	Matched	60ab627cb090e2fcee122858ff14f240	IMG_0275 video.mp4
IMG_0276.MOV	a65d5f2c95e640a997a74e6b10a6f34d	Matched	a65d5f2c95e640a997a74e6b10a6f34d	IMG_0276 video.mp4
IMG_0277.MOV	185416b1aeeccf87a3282b111cb1c5b08	Matched	185416b1aeeccf87a3282b111cb1c5b08	IMG_0277 video.mp4
IMG_0278.MOV	dad03ad588a5f76033a87d68759a63f2	Matched	dad03ad588a5f76033a87d68759a63f2	IMG_0278 video.mp4
IMG_0279.MOV	c6730264d5fad645394cd56a3d2178e0	Matched	c6730264d5fad645394cd56a3d2178e0	IMG_0279 video.mp4
IMG_0280.MOV	87b97b493232305bc7a652e94208e1f3	Matched	87b97b493232305bc7a652e94208e1f3	IMG_0280 video.mp4
IMG_0281.MOV	91a9eccee83826ccf8deb8f0dc23c3f3	Matched	91a9eccee83826ccf8deb8f0dc23c3f3	IMG_0281 video.mp4
IMG_0282.MOV	016b00a338882f4a9526265efd027c84	Matched	016b00a338882f4a9526265efd027c84	IMG_0282 video.mp4
IMG_0283.MOV	f55a600b4223fcf481d670a379eef0f0	Matched	f55a600b4223fcf481d670a379eef0f0	IMG_0283 video.mp4
IMG_0284.MOV	8bf095f3ec474a5fb6e7c3c92dc700ef	Matched	8bf095f3ec474a5fb6e7c3c92dc700ef	IMG_0284 video.mp4
IMG_0285.MOV	38261b482498a54cb56e475f854025f8	Matched	38261b482498a54cb56e475f854025f8	IMG_0285 video.mp4
IMG_0286.MOV	573c0dd9c98b7c0d0a7136bcbb2a5da8	Matched	573c0dd9c98b7c0d0a7136bcbb2a5da8	IMG_0286 video.mp4
IMG_0287.MOV	fd0ea1a5d96d57311455f2df5c94fac1	Matched	fd0ea1a5d96d57311455f2df5c94fac1	IMG_0287 video.mp4
IMG_0288.MOV	b11ab853f48c59bf7f426c5521f3a25c	Matched	b11ab853f48c59bf7f426c5521f3a25c	IMG_0288 video.mp4
IMG_0289.MOV	b4d102c3f26c619bfa73b34319cb8877	Matched	b4d102c3f26c619bfa73b34319cb8877	IMG_0289 video.mp4
IMG_0290.MOV	bc09399e0e34945e7f6af114bd3c75a5	Matched	bc09399e0e34945e7f6af114bd3c75a5	IMG_0290 video.mp4
IMG_0291.MOV	4304de6ccc44ac15aca2c57f2f89c0f5	Matched	4304de6ccc44ac15aca2c57f2f89c0f5	IMG_0291 video.mp4
IMG_0292.MOV	55daa2af20299b909bdc51b3a2e93a67	Matched	55daa2af20299b909bdc51b3a2e93a67	IMG_0292 video.mp4
IMG_0293.MOV	de4a12f2c037da6c80b04d65698afd4	Matched	de4a12f2c037da6c80b04d65698afd4	IMG_0293 video.mp4
IMG_0294.MOV	a5b30589ccb5319e4f594be3346039de	Matched	a5b30589ccb5319e4f594be3346039de	IMG_0294 video.mp4

IMG_0295.MOV	c35072457f64f7584a69f29a9b7c5d49	Matched	c35072457f64f7584a69f29a9b7c5d49	IMG_0295 video.mp4
IMG_0296.MOV	9fb1f245d4b86e7d272041892baaa92a	Matched	9fb1f245d4b86e7d272041892baaa92a	IMG_0296 video.mp4
IMG_0297.MOV	1d458aec0d671e178358098c8da8902	Matched	1d458aec0d671e178358098c8da8902	IMG_0297 video.mp4
IMG_0298.MOV	8e98c3c75b92386f55f16d3fdead00b0	Matched	8e98c3c75b92386f55f16d3fdead00b0	IMG_0298 video.mp4
IMG_0299.MOV	77ef0b6697186c3b556fa87b1e53836c	Matched	77ef0b6697186c3b556fa87b1e53836c	IMG_0299 video.mp4
IMG_0300.MOV	2f42fabab17e3e87b86a4c2dc34a6e17	Matched	2f42fabab17e3e87b86a4c2dc34a6e17	IMG_0300 video.mp4
IMG_0301.MOV	5d237e1bc2838e0b80f35caa01967926	Matched	5d237e1bc2838e0b80f35caa01967926	IMG_0301 video.mp4
IMG_0302.MOV	e111543f19f4d8589b8091699282b175	Matched	e111543f19f4d8589b8091699282b175	IMG_0302 video.mp4
IMG_0303.MOV	bb796495eb6151b794a6ffa38f5e727c	Matched	bb796495eb6151b794a6ffa38f5e727c	IMG_0303 video.mp4
IMG_0304.MOV	8e660c54af834f983a5e0cafdbcdb2a21	Matched	8e660c54af834f983a5e0cafdbcdb2a21	IMG_0304 video.mp4
IMG_0305.MOV	fcc60b29bde6423a377002cbc70ada03	Matched	fcc60b29bde6423a377002cbc70ada03	IMG_0305 video.mp4
IMG_0306.MOV	32a4ec283654c7be993b4098beaa0640	Matched	32a4ec283654c7be993b4098beaa0640	IMG_0306 video.mp4
IMG_0307.MOV	90e2c6908ecbcbfcb7610c4475061ec7	Matched	90e2c6908ecbcbfcb7610c4475061ec7	IMG_0307 video.mp4
IMG_0308.MOV	9f24f356315b984871c44635e08f1b9e	Matched	9f24f356315b984871c44635e08f1b9e	IMG_0308 video.mp4
IMG_0309.MOV	6b92925a37fed496653604c83d121c0b	Matched	6b92925a37fed496653604c83d121c0b	IMG_0309 video.mp4
IMG_0310.MOV	bcd4448dafa28d39f06da6b7e073a82	Matched	bcd4448dafa28d39f06da6b7e073a82	IMG_0310 video.mp4
IMG_0311.MOV	964b0a9c365d95f2a5887222e0387b8a	Matched	964b0a9c365d95f2a5887222e0387b8a	IMG_0311 video.mp4
IMG_0312.MOV	3cfafeb8cee58da800c28b83d7a60167	Matched	3cfafeb8cee58da800c28b83d7a60167	IMG_0312 video.mp4
IMG_0313.MOV	4b73530e9739fab93669b79660510495	Matched	4b73530e9739fab93669b79660510495	IMG_0313 video.mp4
IMG_0314.MOV	271ea44d50b766e009083104123d1f85	Matched	271ea44d50b766e009083104123d1f85	IMG_0314 video.mp4
IMG_0315.MOV	393f3701824e6f5b4e6cc48a16626225	Matched	393f3701824e6f5b4e6cc48a16626225	IMG_0315 video.mp4
IMG_0316.MOV	d61eee9810735fed7ec3d3d3e9d9fa3e	Matched	d61eee9810735fed7ec3d3d3e9d9fa3e	IMG_0316 video.mp4
IMG_0317.MOV	e19b73e587aaadadd4d192e08825e470	Matched	e19b73e587aaadadd4d192e08825e470	IMG_0317 video.mp4
IMG_0318.MOV	cc75205ccae8cf6eda2f764103856911	Matched	cc75205ccae8cf6eda2f764103856911	IMG_0318 video.mp4
IMG_0319.MOV	469e60c5b1a2d120ba072fd50d05402e	Matched	469e60c5b1a2d120ba072fd50d05402e	IMG_0319 video.mp4
IMG_0320.MOV	b84432607eeb5670d336013b4c44cd00	Matched	b84432607eeb5670d336013b4c44cd00	IMG_0320 video.mp4
IMG_0321.MOV	b8944f7583753ac8cd37a40c297ac415	Matched	b8944f7583753ac8cd37a40c297ac415	IMG_0321 video.mp4
IMG_0322.MOV	c53eddae41eb07299686fc811df27c31	Matched	c53eddae41eb07299686fc811df27c31	IMG_0322 video.mp4
IMG_0323.MOV	bececd0cd11cbfad8141e83c50bcd46d	Matched	bececd0cd11cbfad8141e83c50bcd46d	IMG_0323 video.mp4
IMG_0324.MOV	b413c065df5524a921d37f80f06f7b72	Matched	b413c065df5524a921d37f80f06f7b72	IMG_0324 video.mp4
IMG_0325.MOV	7ba0c4c312bd4658e5f4d4bd69631a31	Matched	7ba0c4c312bd4658e5f4d4bd69631a31	IMG_0325 video.mp4
IMG_0326.MOV	12722df242daa3a4e76856084a9b3e2f	Matched	12722df242daa3a4e76856084a9b3e2f	IMG_0326 video.mp4
IMG_0327.MOV	ad68a1f0a4e5573dd7a958d26f6a5033	Matched	ad68a1f0a4e5573dd7a958d26f6a5033	IMG_0327 video.mp4
IMG_0328.MOV	071402624011cc2948949e349c484713	Matched	071402624011cc2948949e349c484713	IMG_0328 video.mp4
IMG_0329.MOV	375b3ceeadd0b91e5c56c1b770372439	Matched	375b3ceeadd0b91e5c56c1b770372439	IMG_0329 video.mp4
IMG_0330.MOV	cb302a3676ea177c3b9258093e9f525a	Matched	cb302a3676ea177c3b9258093e9f525a	IMG_0330 video.mp4
IMG_0331.MOV	1a29798fd548fcaa03fca116e69fabdc	Matched	1a29798fd548fcaa03fca116e69fabdc	IMG_0331 video.mp4

Analysis & Discussion of Test Data

The hashes of respective video streams in original file and video streams in transcoded derivative digital multimedia files matched 100% (100 out of 100). This demonstrated reproducibility as noted by Warren et al., (2012) as generally discussed in their research [65] and Whitecotton

(2017) [20]. This demonstrated repeatability. The test demonstrated accuracy and precision by the exactness of the hash used. The numerical probability of a random collision for MD5 hash is 1 in 2^{64} (about 1 in 1.84×10^{19}) [66].

Test Results

This test has demonstrated that multimedia stream hash validation method, as it relates to video streams, is a viable method for consideration for use in the video authentication process when transcoding the video stream for further authentication.

APPENDIX E

CASE STUDY 2

Summary Report

Test Title: Case Study 2

Test Date: 3/31/2019

Test Description:

This report documents the case study 2 test of the proposed video authentication framework against four videos that had local copy and paste tampering. One video also used an Example-Based Texture Synthesis technique along with the copy and paste. In addition, one of the videos involved a panning camera while using copy and paste to remove a person walking in one direction and a car passing in the background in the opposite direction. A total of four test videos were analyzed.

Test Results:

Table 23 - Test Results

Test Number	Environment	Requirement 1	Requirement 2	Requirement 3	Requirement 4
1	Taiwan-1 videos (Copy & Paste and Example-Based Texture Synthesis)	Pass	Pass	Pass	Pass
2	Taiwan-2 videos (Copy & Paste)	Pass	Pass	Pass	Pass
3	Taiwan-3 videos (Copy & Paste w/Panning Camera)	Pass	Pass	Pass	Pass
4	Taiwan-4 videos (Copy & Paste)	Pass	Pass	Pass	Pass

Requirements:

1. Use proposed video authentication methodology to conduct authentication work.
2. Replace normal test scenario documentation with a video authentication framework workflow document created for the proposed framework.
3. Perform file structure analysis, audio stream analysis (if applicable), and video stream analysis on each test scenario questioned video file.
4. Ignore workflow optimization and continue to do at least copy & paste analysis if file structure analysis detects video file editing.

Observations/Concerns:

The tests had no errors. However, the panning camera movement had less contrast in the temporal differences as their were more differences from frame to frame as the camera panned.

Limitations:

None

Results:

The use of the video authentication framework permitted a structured and organized workflow for the video authentication process of the four video files known to have cut and paste tampering. The workflow permitted for repeatable, accurate, and precise detection of the tampering. The framework also would have allowed the forensic video examiner to opt out of detecting the precise tampering regions by using the workflow optimization option. In each of the four videos the conclusion was that the video stream was inconsistent with an original recording. Additionally, the precise areas of the copy and paste regions within each identified frame were noted for accurate and precise tampering identification.

APPENDIX E-1

TEST PLAN

Test Title: Case Study 2

Purpose and Scope:

This test plan will evaluate the proposed video authentication framework against four videos associated with a block level manipulation testing paper from Taiwan [44]. The test will contain four scenarios based upon the four block level manipulated videos used in the Taiwan paper. According to Hsu, Hung, Lin, and Hsu (2008) paper, the videos were created as follows:

Table 24 - Test Video Tampering Method

Test Video #	Tamper Method
1	Copy & Paste and Example-Based Texture Synthesis
2	Copy & Paste
3	Copy & Paste (Camera pans to right with moving tampered / removed subject area moving with camera while a small moving area in back ground moves from camera right to left).
4	Copy & Paste [44]

Each test will have the same video authentication analysis question (AQ). The AQ is as follows:

Has the video stream, video stream and audio stream, or audio stream been altered or edited?

Note: AQ-2 not used.

Requirements:

1. Use proposed video authentication methodology to conduct authentication work.
2. Replace normal test scenario documentation with a video authentication framework workflow document created for the proposed framework.
3. Perform file structure analysis, audio stream analysis (if applicable), and video stream analysis on each test scenario questioned video file.
4. Ignore workflow optimization and continue to do at least copy & paste analysis if file structure analysis detects video file editing.

Description of Methodology:

1. Hash multimedia prior to comparisons.
2. Execute File structure analysis on files and document, including multimedia stream content.
3. Bifurcate any audio streams to PCM wave file using multimedia stream sash validation method (if applicable) and document.
4. Conduct audio stream analysis (if applicable) and document.

5. Conduct video stream analysis (focus on copy & paste analysis using temporal difference method) and document.
6. Analyze results of test scenario.
7. Validate the test results for precision and accuracy by comparing the temporal difference filter frames with original videos frames before tampering.

Expected Results:

1. Video authentication framework will detect tampered video and audio (if applicable) streams in file structure analysis.
2. Video authentication framework using local copy and paste temporal difference method will detect specific area of alteration in tampered videos.

Test Scenarios:

Table 25 - Planned Test Scenarios

Test Number	Environment:	Actions:	Assigned Req't's:	Expected Results:
1	Taiwan-1 videos (Copy & Paste and Example-Based Texture Synthesis)	Execute Proposed Video Authentication Framework Using Workflow Document	All	All
2	Taiwan-2 videos (Copy & Paste)	Execute Proposed Video Authentication Framework Using Workflow Document	All	All
3	Taiwan-3 videos (Copy & Paste w/Panning Camera)	Execute Proposed Video Authentication Framework Using Workflow Document	All	All
4	Taiwan-4 videos (Copy & Paste)	Execute Proposed Video Authentication Framework Using Workflow Document	All	All

Test Data Description:

Test Data Set:

The following are the test data digital multimedia file hashes.

Filename: Taiwan-1-Tampered.avi
Filesize: 177305116 bytes
MD5: 52e941862c3dd247faef18f775388808
SHA1: fcea0873153899141ebedcd1de6c0ec8e3170dcc
SHA256: cf967a00beabaf5e0e03e54f8d9d52693b025ce77dedea086f7e885ab07bb0d7

Filename: Taiwan-1-Original.avi
Filesize: 262324684 bytes
MD5: d224c3303bb477783e9dbf7fd73bc18f
SHA1: 859c020ebb1875f98b46de2d0af95b5edb7f3f50
SHA256: 15c83638fc659e03b9790b38f68d8575f2e42fae65ae427603a7ec1766861a

Filename: Taiwan-2-Original.avi
Filesize: 398148628 bytes
MD5: c7e177748b97bbf6c2bf9a8b966d3c53
SHA1: 4db4d909fbd50a59892c044c7d871c339ba7a779
SHA256: 20d340b1b0c332f7c5b73fef31c322b9782c1a5442d3d9b403580270e9bf8ce6

Filename: Taiwan-2-Tampered.avi
Filesize: 175231468 bytes
MD5: b2dc54e8c345784200a0bd39a5d27b2f
SHA1: bb700e53c086dd629dec6996d76455131773ca12
SHA256: c00ce61d5ca8e579ad0bf45740d1258b7bc7135a5caflceddb9c35a732495af0

Filename: Taiwan-3-Original.avi
Filesize: 207373012 bytes
MD5: b34d40237c7b390366253850675a6c0a
SHA1: 67d1d852310d0fb0395a3d7697a6e2e5fcd17303
SHA256: b27bf8359d92ca59e0d26146f7b30cb5a783119d257d6f835cc11ed43d3cc604

Filename: Taiwan-3-Tampered.avi
Filesize: 207373012 bytes
MD5: c398677bf45efda0b75a5e289ac2d6d6
SHA1: e7ec7eb206445247064c50a37a3c680245daef83
SHA256: 60cc8864214273927d0e9698b9020f2761f99144737fe7256541fc27c3321ca3

Filename: Taiwan-4-Original.avi
Filesize: 308981764 bytes
MD5: cd74f53a2ca02b6edf76868730c5357a
SHA1: 39409c2d535ecc1aa5509ddb728a476afb558337

SHA256: 6afd97581dd864236107ec9ed2422d6c13409097db4b940050a66572e72f3621

Filename: Taiwan-4-Tampered.avi

Filesize: 207373012 bytes

MD5: 6b9a5fbfa0dc7d95af353a29c3b759ca

SHA1: 5c8fa0641bc7498b459150bc3afc92017e0f4db7

SHA256: 740702207794d527cf0d7b1a47323831158cdc9e7613102b29d1d54ab1394921

APPENDIX E-2 Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses

Hypothesis	<i>Has the video stream, video stream and audio stream, or audio stream been altered or edited?</i>
------------	---

Questioned File Information



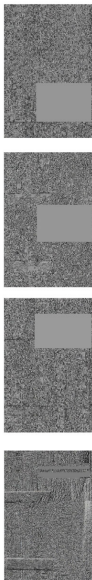


File Name:	Taiwan-1-Tampered.avi
File Size:	177305116 bytes
MD5 Hash:	52e941862c3dd247faef18f775388808
SHA1 Hash:	fcea0873153899141ebedcd1de6c0ec8e3170dcc
SHA256 Hash:	c967a00beabaf5e0e03c54f8d9d52693b025ce77dedea086f7e885ab07bb0d7

HYPOTHESIS ANALYSIS


#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

			<div>offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</div> <div>00001200 4A 55 4E 4B F8 0D 00 00 56 69 72 74 75 61 6C 44 JUNKs...VirtualD</div> <div>00001210 75 62 20 62 75 69 6C 64 20 33 32 38 34 32 2F 72 00 build 32842/F</div> <div>00001220 65 6C 65 61 73 65 00 00 00 00 00 00 00 00 00 00 release.....</div> <div>00001230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</div> <div>00001240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</div>		
4	Workflow Optimization Decision		Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication and video authentication framework.	Continue	
5	Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.				
6	Video File Bifurcation Process - File Preparation Decision	Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.	Video stream only	No bifurcation required. No transcoding required. N/A	
7	AUDIO STREAM ANALYSIS				
8	Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis				
9	Global Analysis	DC Offset Analysis		○	
10		Power Analysis		○	
11		Zero Analysis		○	
12		LTAS Analysis		○	
13		LTASS Analysis		○	

14		DSS																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			</
----	--	-----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

33	Block Level Analysis				NR
34	Temporal (Interpolation) Analysis				NR
35					
36	Visual Anomaly Analysis	 Visual inconsistencies in pixels in grass and edge of walkway as video runs in playback	Visual inconsistencies in pixels in grass and edge of walkway as video runs in playback.		
37	Copy & Move Analysis	 Frame 0 - Temporal Difference Filter Frame 24 - Temporal Difference Filter Frame 50 - Temporal Difference Filter Frame 75 - Temporal Difference Filter	Temporal difference filter revealed evidence of tampering.		
38	Local Analysis	Double Quantization Analysis			NR
39		Local Pixel Manipulation Analysis			NR
40		Local Block Manipulation Analysis			NR
41					
42	Overall Decision For Hypothesis				

 Consistent with an original recording.

 Not Consistent with an original recording.

 Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.

APPENDIX E-3 Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses




Hypothesis 1	Has the video stream, video stream and audio stream, or audio stream been altered or edited?
--------------	--

Questioned File Information

File Name:	Taiwan-2-Tampered.avi
File Size:	175231468 bytes
MD5 Hash:	b2dc54e8c345784200a0bd39a5d27b2f
SHA1 Hash:	bb700e53c086dd629dec6996d76455131773ca12
SHA256 Hash:	c00ce61d5ca8e579ad0bf45740d1258b7bc7135a5caf1eeddb9c35a732495af0



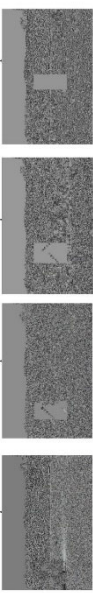


HYPOTHESIS #1 ANALYSIS

#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

1	<p>File Format Analysis</p>	<p>General</p> <p>Complete name : Taiwan-2-Tampered.avi</p> <p>Format : AVI</p> <p>Format/Info : Audio Video Interleave</p> <p>File size : 167 MiB</p> <p>Duration : 6 s 760 ms</p> <p>Overall bit rate : 207 Mb/s</p> <p>Writing library : VirtualDub build 32842/release</p> <p>Video</p> <p>ID : 0</p> <p>Format : RGB</p> <p>Codec ID : 0x00000000</p> <p>Codec ID/Info : Basic Windows bitmap format, 1, 4 and 8 bpp versions are palettised. 16, 24 and 32bpp contain raw RGB samples</p> <p>Duration : 6 s 760 ms</p> <p>Bit rate : 207 Mb/s</p> <p>Width : 720 pixels</p> <p>Height : 480 pixels</p> <p>Display aspect ratio : 3:2</p> <p>Frame rate : 25.000 FPS</p> <p>Bit depth : 8 bits</p> <p>Bits/(Pixel*Frame) : 24.000</p> <p>Stream size : 167 MiB (100%)</p>	<p>Did not observe any camera entries in the ASCII area, but did note the presence of Virtual Dub entry. Virtual Dub is free and open-source video processing utility.</p>	
2	<p>Header Analysis</p>	<p>Offset (b) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</p> <p>00000000 52 49 46 45 84 D1 71 0A 41 56 49 20 4C 49 53 54 RIFF&R.AVI LIST</p> <p>00000010 8C 11 00 00 68 64 72 6C 61 76 69 69 38 00 00 00listavib...</p> <p>00000020 40 9C 00 00 17 89 88 01 00 00 00 00 10 00 00 00 @.....</p> <p>00000030 A9 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 @.....</p> <p>00000040 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00LISTW...</p> <p>00000050 73 74 72 6C 73 74 72 68 38 00 00 00 00 00 00 00strlsth.....vids</p> <p>00000060 44 49 42 20 00 00 00 00 00 00 00 00 00 00 00 00DIB.....</p> <p>00000070 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00@.....</p> <p>00000080 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00 000.....</p> <p>00000090 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 000.....</p> <p>000000A0 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 000.....</p> <p>000000B0 00 02 0F 00 00 00 00 00 00 00 00 00 00 00 000.....</p> <p>000000C0 00 02 0F 00 00 00 00 00 00 00 00 00 00 00 000.....</p> <p>000000D0 00 00 00 00 4A 55 4E 4B 18 10 00 00 00 00 00JUNK.....</p>	<p>The file's header was a RIFF AVI file.</p>	
3	<p>Hex Data Analysis</p>	<p>Offset (b) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</p> <p>00000000 52 49 46 45 84 D1 71 0A 41 56 49 20 4C 49 53 54 RIFF&R.AVI LIST</p> <p>00000010 8C 11 00 00 68 64 72 6C 61 76 69 69 38 00 00 00listavib...</p> <p>00000020 40 9C 00 00 17 89 88 01 00 00 00 00 10 00 00 00 @.....</p> <p>00000030 A9 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 @.....</p> <p>00000040 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00LISTW...</p> <p>00000050 73 74 72 6C 73 74 72 68 38 00 00 00 00 00 00 00strlsth.....vids</p> <p>00000060 44 49 42 20 00 00 00 00 00 00 00 00 00 00 00 00DIB.....</p> <p>00000070 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00@.....</p> <p>00000080 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00 000.....</p> <p>00000090 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 000.....</p> <p>000000A0 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 000.....</p> <p>000000B0 00 02 0F 00 00 00 00 00 00 00 00 00 00 00 000.....</p> <p>000000C0 00 02 0F 00 00 00 00 00 00 00 00 00 00 00 000.....</p> <p>000000D0 00 00 00 00 4A 55 4E 4B 18 10 00 00 00 00 00JUNK.....</p> <p>offset (d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15</p> <p>000004608 4A 55 4E 4B 0D 00 00 56 69 72 74 75 61 6C 44 JUNK.....VirtualD</p> <p>000004624 75 62 20 62 75 69 6C 64 20 33 32 38 34 32 2F 72ub build 32842/r</p> <p>000004640 65 6C 65 61 73 65 00 00 00 00 00 00 00 00 00 00elease.....</p> <p>000004656 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</p>	<p>The hex entry A9 00 00 00 = 169 frames. Hex entry 01 00 00 00 = 1 stream. Hex entry D0 02 00 00 = 720 Width. Hex entry E0 01 00 00 = 480 Height. The second screen shot to the left for hex offset 46 16 to offset 46 45 – contained an entry for Virtual Dub software</p>	

4	Workflow Optimization Decision			Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication framework.	Continue
5	Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.				
6	Video File Bifurcation Process - File Preparation Decision	Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.	Video stream only	No bifurcation required. No transcoding required.	N/A
7	AUDIO STREAM ANALYSIS				
8	Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis				
9	Global Analysis	DC Offset Analysis			○
10		Power Analysis			○
11		Zero Analysis			○
12		LTAS Analysis			○
13		LTASS Analysis			○

14		DSS																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
----	--	-----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

33	Block Level Analysis				NR
34	Temporal (Interpolation) Analysis				NR
35					
36	Visual Anomaly Analysis		Visual inconsistencies in pixels in grass and edge of walkway as video runs in playback.		
37	Copy & Move Analysis		Temporal difference revealed evidence of tampering.		
38	Double Quantization Analysis			NR	
39	Local Pixel Manipulation Analysis			NR	
40	Local Block Manipulation Analysis			NR	
41					
42	Overall Decision For Hypothesis				

- ☒ Consistent with an original recording.
- ☒ Not Consistent with an original recording.
- ☐ Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.

APPENDIX E-4 Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses



Hypothesis 1	Has the video stream, video stream and audio stream, or audio stream been altered or edited?
--------------	--

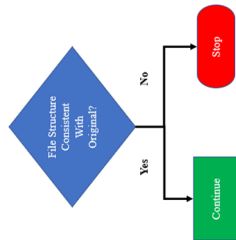
Questioned File Information

File Name:	Taiwan-3-Tampered.avi
File Size:	207373012 bytes
MD5 Hash:	c398677bf45efda0b75a5e289ac2d6d6
SHA1 Hash:	e7ec7eb206445247064c50a37a3c680245dae83
SHA256 Hash:	60cc8864214273927d0e9698b9020f2761f99144737fe7256541fc27c3321ca3






HYPOTHESIS #1 ANALYSIS

#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

1	File Format Analysis	<p>General</p> <p>Complete name : Taiwan-3-Tampered.avi</p> <p>Format : AVI</p> <p>Format/Info : Audio Video Interleave</p> <p>File size : 198 MiB</p> <p>Duration : 8 s 0 ms</p> <p>Overall bit rate : 207 Mb/s</p> <p>Writing library : VirtualDub build 32842/release</p> <p>Video</p> <p>ID : 0</p> <p>Format : RGB</p> <p>Codec ID : 0x00000000</p> <p>Codec ID/Info : Basic Windows bitmap format, 1, 4 and 8 bpp versions are palettised. 16, 24 and 32bpp contain raw RGB samples</p> <p>Duration : 8 s 0 ms</p> <p>Bit rate : 207 Mb/s</p> <p>Width : 720 pixels</p> <p>Height : 480 pixels</p> <p>Display aspect ratio : 3:2</p> <p>Frame rate : 25.000 FPS</p> <p>Bit depth : 8 bits</p> <p>Bits/(Pixel*Frame) : 24.000</p> <p>Stream size : 198 MiB (100%)</p>	Did not observe any camera entries in the ASCII area, but did note the presence of Virtual Dub entry. Virtual Dub is free and open-source video processing utility.	
2	Header Analysis	<p>Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</p> <p>00000000 52 49 46 45 84 D1 71 0A 41 56 49 20 4C 49 53 54 RIFF&RIFF.AVI LIST</p> <p>00000010 8C 11 00 00 68 64 72 6C 61 76 69 69 38 00 00 00list.....</p> <p>00000020 40 9C 00 00 17 89 88 01 00 00 00 00 10 00 00 00list.....</p> <p>00000030 A9 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00list.....</p> <p>00000040 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000060 73 74 72 6C 73 74 72 68 38 00 00 00 00 00 00 00list.....</p> <p>00000070 44 49 42 20 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000080 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000090 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00 00list.....</p> <p>000000A0 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 00list.....</p> <p>000000B0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>000000C0 00 02 0F 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>000000D0 00 00 00 00 4A 55 4E 4B 18 10 00 00 00 00 00 00JUNK.....</p>	The file's header was a RIFF AVI file.	
3	Hex Data Analysis	<p>Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</p> <p>00000000 52 49 46 45 84 D1 71 0A 41 56 49 20 4C 49 53 54 RIFF&RIFF.AVI LIST</p> <p>00000010 8C 11 00 00 68 64 72 6C 61 76 69 69 38 00 00 00list.....</p> <p>00000020 40 9C 00 00 17 89 88 01 00 00 00 00 10 00 00 00list.....</p> <p>00000030 A9 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00list.....</p> <p>00000040 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000060 73 74 72 6C 73 74 72 68 38 00 00 00 00 00 00 00list.....</p> <p>00000070 44 49 42 20 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000080 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>00000090 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00list.....</p> <p>000000A0 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 00list.....</p> <p>000000B0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>000000C0 00 02 0F 00 00 00 00 00 00 00 00 00 00 00 00list.....</p> <p>000000D0 00 00 00 00 4A 55 4E 4B 18 10 00 00 00 00 00 00JUNK.....</p> <p>offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15</p> <p>000004608 4A 55 4E 4B F8 0D 00 00 56 69 72 74 75 61 6C 44 JUNKs...VirtualD</p> <p>000004624 75 62 20 62 75 69 6C 64 20 33 32 38 34 32 2F 72 ..build 32842/r</p> <p>000004640 65 6C 65 61 73 65 00 00 00 00 00 00 00 00 00 00elease.....</p> <p>000004656 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</p>	The hex entry A9 00 00 00 = 169 frames. Hex entry 01 00 00 00 = 1 stream. Hex entry D0 02 00 00 = 720 Width. Hex entry E0 01 00 00 = 480 Height. The second screen shot to the left for hex offset 46 16 to offset 46 45 – contained an entry for Virtual Dub software	

4	Workflow Optimization Decision			Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication framework.	Continue
5	Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.				
6	Video File Bifurcation Process - File Preparation Decision	Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.	Video stream only	No bifurcation required. No transcoding required.	N/A
7	AUDIO STREAM ANALYSIS				
8	Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis				
9	Global Analysis	DC Offset Analysis			○
10		Power Analysis			○
11		Zero Analysis			○
12		LTAS Analysis			○
13		LTASS Analysis			○

14		DSS																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																		
----	--	-----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

33	Block Level Analysis				NR
34	Temporal (Interpolation) Analysis				NR
35					
36	Local Analysis	Visual Anomaly Analysis		Visual inconsistencies in pixels in grass and edge of walkway as video runs in playback.	
37		Copy & Move Analysis		Temporal difference revealed evidence of tampering.	
38		Double Quantization Analysis			NR
39		Local Pixel Manipulation Analysis			NR
40		Local Block Manipulation Analysis			NR
41					
42	Overall Decision For Hypothesis				

- ☒ Consistent with an original recording.
- ☒ Not Consistent with an original recording.
- ☐ Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.

APPENDIX E-5 Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses




Hypothesis 1	<i>Has the video stream, video stream and audio stream, or audio stream been altered or edited?</i>
--------------	---

Questioned File Information

File Name:	Taiwan-4-Tampered.avi
File Size:	207373012 bytes
MD5 Hash:	6b9a5fbfa0dc7d95af353a29c3b759ca
SHA1 Hash:	5c8fa0641bc7498b459150bc3afc92017e0f4db7
SHA256 Hash:	740702207794d527cf0d7b1a47323831158cdc9e7613102b29d1d54ab1394921

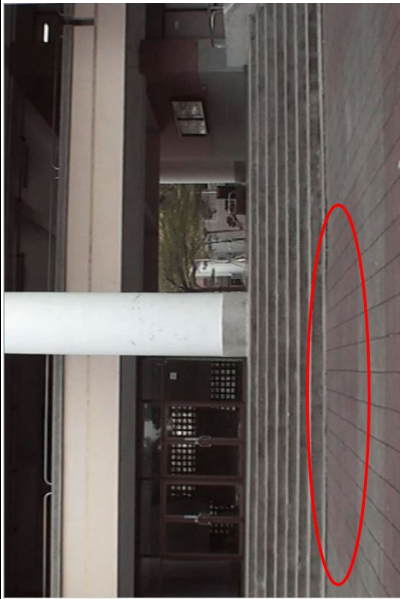

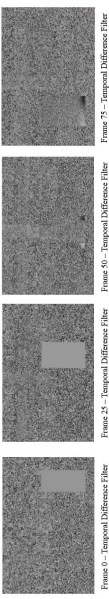


HYPOTHESIS #1 ANALYSIS

#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

1	File Format Analysis	<p>General Complete name : C:\Users\Greg\Documents\UC Denver\Thesis Research\Case Studies\CS-2 (Taiwan Videos)\Taiwan Paper Info\test4\Taiwan-4--Tampered.avi</p> <p>Format : AVI</p> <p>Format/Info : Audio Video Interleave</p> <p>File size : 198 MiB</p> <p>Duration : 8 s 0 ms</p> <p>Overall bit rate : 207 Mb/s</p> <p>Writing library : VirtualDub build 32842/release</p> <p>Video ID : 0</p> <p>Format : RGB</p> <p>Codec ID : 0x00000000</p> <p>Codec ID/Info : Basic Windows bitmap</p> <p>format. 1, 4 and 8 bpp versions are palettised. 16, 24 and 32bpp contain raw RGB samples</p> <p>Duration : 8 s 0 ms</p> <p>Bit rate : 207 Mb/s</p> <p>Width : 720 pixels</p> <p>Height : 480 pixels</p> <p>Display aspect ratio : 3:2</p> <p>Frame rate : 25.000 FPS</p> <p>Bit depth : 8 bits</p> <p>Bits/(Pixel*Frame) : 24.000</p> <p>Stream size : 198 MiB (100%)</p>	<p>Did not observe any camera entries in the ASCII area, but did note the presence of Virtual Dub entry. Virtual Dub is free and open-source video processing utility.</p>	
2	Header Analysis	<p>Offset(b) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</p> <p>00000000 52 49 46 45 64 D1 71 0A 41 56 49 20 4C 49 53 54 RIFF&AVI LIST</p> <p>00000010 8C 11 00 00 68 64 72 6C 61 76 69 69 38 00 00 00listavib...</p> <p>00000020 40 9C 00 00 17 89 88 01 00 00 00 10 00 00 00 00&.....&.....</p> <p>00000030 A9 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00&.....&.....</p> <p>00000040 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00LISTW...</p> <p>00000050 73 74 72 6C 73 74 72 68 38 00 00 00 00 00 00 00strlsth&..vids</p> <p>00000060 44 49 42 20 00 00 00 00 00 00 00 00 00 00 00 00DIB.....</p> <p>00000070 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00&.....&.....</p> <p>00000080 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00 00&.....&.....</p> <p>00000090 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 00&.....&.....</p> <p>000000A0 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 00&.....&.....</p> <p>000000B0 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00&.....&.....</p> <p>000000C0 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00&.....&.....</p> <p>000000D0 00 00 00 00 4A 55 4E 4B 18 10 00 00 00 00 00JUNK.....</p>	<p>The file's header was a RIFF AVI file.</p>	
3	Hex Data Analysis	<p>Offset(b) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F</p> <p>00000000 52 49 46 45 64 D1 71 0A 41 56 49 20 4C 49 53 54 RIFF&AVI LIST</p> <p>00000010 8C 11 00 00 68 64 72 6C 61 76 69 69 38 00 00 00listavib...</p> <p>00000020 40 9C 00 00 17 89 88 01 00 00 00 10 00 00 00 00&.....&.....</p> <p>00000030 A9 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00&.....&.....</p> <p>00000040 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00LISTW...</p> <p>00000050 73 74 72 6C 73 74 72 68 38 00 00 00 00 00 00 00strlsth&..vids</p> <p>00000060 44 49 42 20 00 00 00 00 00 00 00 00 00 00 00 00DIB.....</p> <p>00000070 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00&.....&.....</p> <p>00000080 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00&.....&.....</p> <p>00000090 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 00&.....&.....</p> <p>000000A0 00 02 80 01 73 74 72 66 28 00 00 00 00 00 00 00&.....&.....</p> <p>000000B0 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00&.....&.....</p> <p>000000C0 00 02 0F 00 FF FF FF 00 00 00 00 00 00 00 00&.....&.....</p> <p>000000D0 00 00 00 00 4A 55 4E 4B 18 10 00 00 00 00 00JUNK.....</p> <p>offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15</p> <p>000004608 4A 55 4E 4B F8 0D 00 00 56 69 72 74 75 61 6C 44 JUNK...VirtualD</p> <p>000004624 75 62 20 62 75 69 6C 64 20 33 32 38 34 32 3F 72 ..& build 32842/r</p> <p>000004640 65 6C 65 61 73 65 00 00 00 00 00 00 00 00 00 00elease.....</p> <p>000004656 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</p>	<p>The hex entry A9 00 00 00 = 169 frames. Hex entry 01 00 00 00 = 1 stream. Hex entry D0 02 00 00 = 720 Width. Hex entry E0 01 00 00 = 480 Height.</p> <p>The second screen shot to the left for hex offset 46 16 to offset 46 45 – contained an entry for Virtual Dub software</p>	

4	Workflow Optimization Decision		Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication framework.	Continue	
5	Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.				
6	Video File Bifurcation Process - File Preparation Decision	Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.	Video stream only	No bifurcation required. No transcoding required.	N/A
7	AUDIO STREAM ANALYSIS				
8	Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis				
9	Global Analysis	DC Offset Analysis			○
10		Power Analysis			○
11		Zero Analysis			○
12		LTAS Analysis			○
13		LTASS Analysis			○

14		DSS																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			</
----	--	-----	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

33	Block Level Analysis				NR
34	Temporal (Interpolation) Analysis				
35					
36	Local Analysis	Visual Anomaly Analysis		Visual inconsistencies in pixels in lower left side walk area.	
37		Copy & Move Analysis		Temporal difference revealed evidence of tampering.	
38		Double Quantization Analysis			NR
39		Local Pixel Manipulation Analysis			NR
40		Local Block Manipulation Analysis			NR
41					
42	Overall Decision For Hypothesis				

- ☒ Consistent with an original recording.
- ☒ Not Consistent with an original recording.
- ☐ Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.

APPENDIX F

CASE STUDY 3

Summary Report

Test Title: Case Study 3

Test Date: 4/10/2019

Test Description:

This report documents the case study 3 test of the proposed video authentication framework against three videos that had frames removed. The original video was created with Axon Fleet camera recorded and provided by Seattle Police Department Forensic Digital Imaging Section in a moving vehicle. The tests attempted to detect small sections of editing of video streams. A total of three test videos were analyzed.

Test Results:

Test Number	Environment	Requirement 1	Requirement 2	Requirement 3	Requirement 4
1	Pre-Event Buffering Video	Pass	Pass	Pass	Pass
2	Event Video Stream	Pass	Pass	Pass	Pass
3	Delete Pre-Event Buffering Video	Pass	Pass	Pass	Pass

Requirements:

1. Use proposed video authentication methodology to conduct authentication work.
2. Replace normal test scenario documentation with a video authentication framework workflow document created for the proposed framework.
3. Perform file structure analysis, audio stream analysis (if applicable), and video stream analysis on each test scenario questioned video file.
4. Ignore workflow optimization and continue to detect video file editing.

Observations/Concerns:

The tests had no errors. However, the pre-event buffer video removal would not be detected if the examiner is not familiar with Axon body or fleet cameras.

Limitations:

None

Results:

The use of the video authentication framework permitted a structured and organized workflow for the video authentication process of the three video files known to have frame deletions. The workflow permitted for repeatable, accurate, and precise detection of the tampering. The framework also would have allowed the forensic video examiner to opt out of detecting the precise tampering regions of the video by using the workflow optimization option. In each of the three videos the conclusion was that the video stream was inconsistent with an original

recording. Additionally, the precise areas of the video frame deletion within each video were noted for accurate and precise tampering identification.

APPENDIX F-1

TEST PLAN

Test Title: Case Study 3

Purpose and Scope:

This test plan will evaluate the proposed video authentication framework used against video created with Axon camera recorded and provided by Seattle Police Department Forensic Digital Imaging Section. The video was created with Axon Fleet camera in a moving vehicle. The test will attempt to detect small sections of editing of video streams.

The test will have the following video authentication analysis question (AQ).

AQ-1: Has the video stream, video stream and audio stream, or audio stream been altered or edited?

Note: AQ-2 (device identification) not used.

Requirements:

1. Use proposed video authentication methodology to conduct authentication work.
2. Replace normal test scenario documentation with a video authentication framework workflow document created for the proposed framework.
3. Perform file structure analysis, audio stream analysis (if applicable), and video stream analysis on each test scenario questioned video file.
4. Ignore workflow optimization and continue to detect video file editing.

Description of Methodology:

1. Execute File structure analysis on files and document, including multimedia stream content.
2. Bifurcate any audio streams to PCM wave file using multimedia stream sash validation method (if applicable) and document.
3. Conduct audio stream analysis and document.
4. Conduct video stream analysis and document.
5. Analyze results of test scenarios.
6. Validate the test results for precision and accuracy by comparing test scenario results with original videos before tampering.

Expected Results:

1. Video authentication framework will detect tampered video stream in file structure analysis.
2. Video authentication framework using video authentication method to detect video stream splicing will detect specific area of alteration in tampered videos.

Test Scenarios:

Test Number	Environment:	Actions:	Assigned Reqt's:	Expected Results:
1-1	Pre-Event Buffering Video	Execute Proposed Video Authentication Framework Using Workflow Document	All	All
1-2	Event Video Stream	Execute Proposed Video Authentication Framework Using Workflow Document	All	All
1-3	Delete Pre-Event Buffering Video	Execute Proposed Video Authentication Framework Using Workflow Document	All	All

Test Data Description:Original Data Set:

The following are the original video digital multimedia file hashes as reported by Jacksum 1.7.0.

Filename: 9.mp4
Filesize: 34838122 bytes
MD5: c3a628dc47ab71e01f0fbfce4982a170
SHA1: 2c2067a9ecb6218f86a0f56a1720c75ee55e125b
SHA256: fd8f7da1a0e8f224a1747aa3ca3bf2a5d3abcb33a0c95abd78d47b24cac490e6

APPENDIX F-2

Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses

Hypothesis	<i>Has the video stream, video stream and audio stream, or audio stream been altered or edited?</i>
------------	---

Questioned File Information

File Name:	9-Spliced-600-700-Removed.mp4
File Size:	70044820 bytes
MD5 Hash:	1f8d371f9f8fac422f384337c22e2bec
SHA1 Hash:	3ed36d1ea26761a06d3d49ab81626d9a60834e24
SHA256 Hash:	d2372f558742db917495d033eac2a5e9e765348f3495d7dbb67fe14ea8e17a75

167

HYPOTHESIS ANALYSIS

#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

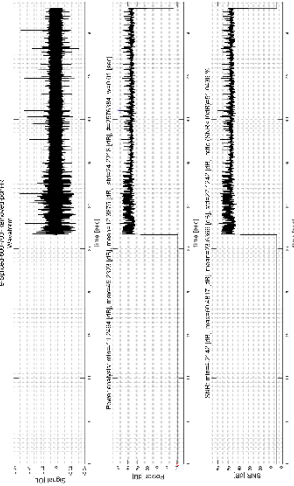

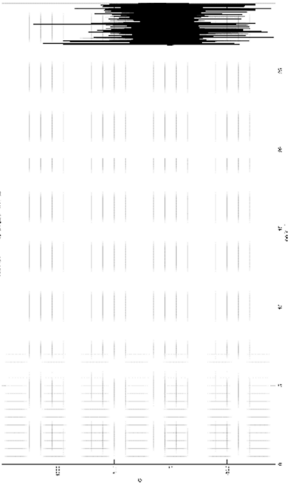

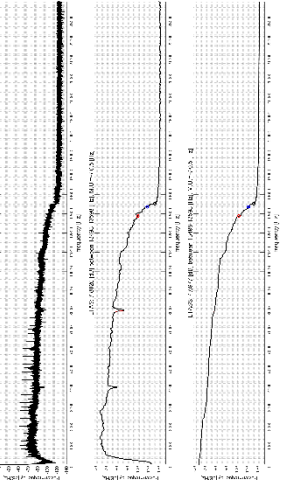

<div> <div>File Structure Analysis</div> <div>1</div> </div>	<div> <div>File Format Analysis</div> <div> <div>File Name</div> <div>File Size</div> <div>File Modification Date/Time</div> <div>File Access Date/Time</div> <div>File Creation Date/Time</div> <div>File Permissions</div> <div>File Type</div> <div>MIME Type</div> <div>Major Brand</div> <div>Minor Version</div> <div>Compatible Brands</div> <div>Movie Header Version</div> <div>Create Date</div> <div>Modify Date</div> <div>Time Scale</div> <div>Duration</div> <div>Preferred Rate</div> <div>Preferred Volume</div> <div>Preview Time</div> <div>Preview Duration</div> <div>Poster Time</div> <div>Selection Time</div> <div>Current Time</div> <div>Next Track ID</div> <div>Track Header Version</div> <div>Track Create Date</div> <div>Track Modify Date</div> <div>Track ID</div> <div>Track Duration</div> <div>Track Layer</div> <div>Track Volume</div> <div>Image Width</div> <div>Image Height</div> <div>Graphics Mode</div> <div>Op Color</div> <div>Compressor ID</div> <div>Source Image Width</div> <div>Source Image Height</div> <div>X Resolution</div> <div>Y Resolution</div> <div>Compressor Name</div> <div>Bit Depth</div> <div>Matrix Structure</div> <div>Media Header Version</div> <div>Media Create Date</div> <div>Media Modify Date</div> <div>Media Time Scale</div> <div>Media Duration</div> <div>Media Language Code</div> <div>Balance</div> <div>Handler Type</div> </div> <div> <div> <div>9-Spliced-600-700-Removed.mp4</div> <div>67 MB</div> <div>2019:04:04 05:51:50-04:00</div> <div>2019:04:05 14:06:44-04:00</div> <div>2019:04:05 14:04:41-04:00</div> <div>rw-rw-rw-</div> <div>MP4</div> <div>video/mp4</div> <div>MP4 v2 [ISO 14496-14]</div> <div>0.0.0</div> <div>mp42, mp41</div> <div>0</div> <div>2019:04:04 09:51:47</div> <div>2019:04:04 09:51:49</div> <div>90000</div> <div>0:00:53</div> <div>1</div> <div>100.00%</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>3</div> <div>0</div> <div>2019:04:04 09:51:48</div> <div>2019:04:04 09:51:48</div> <div>1</div> <div>0:00:53</div> <div>0</div> <div>0.00%</div> <div>1280</div> <div>720</div> <div>srcCopy</div> <div>0 0 0</div> <div>avc1</div> <div>1280</div> <div>720</div> <div>72</div> <div>AVC Coding</div> <div>24</div> <div>1 0 0 1 0 0 1</div> <div>0</div> <div>2019:04:04 09:51:48</div> <div>2019:04:04 09:51:48</div> <div>48000</div> <div>0:00:53</div> <div>eng</div> <div>0</div> <div>Alias Data</div> </div> </div> <div> <div>Did not observe any camera entries in the ascii area, but did note the presence of Adobe Premiere video editing software indications.</div> <div> <div></div> </div> </div> </div>
--	---

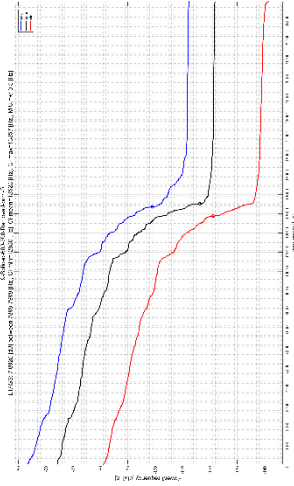
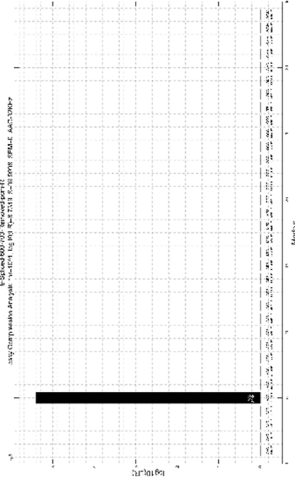
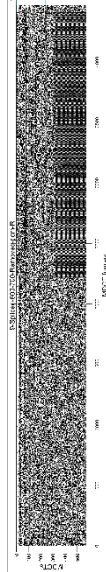
		<p>Handler Description : Alias Data Handler</p> <p>Audio Format : mp4a</p> <p>Audio Channels : 2</p> <p>Audio Bits Per Sample : 16</p> <p>User Data TIM : 00:00:00:00</p> <p>User Data TSC : 30000</p> <p>User Data TSZ : 1001</p> <p>XMP Toolkit : Adobe XMP Core 5.6-c148</p> <p>79.163765, 2019/01/24-18:11:46</p> <p>Metadata Date : 2019:04:04 03:51:49-06:00</p> <p>Creator Tool : Adobe Premiere Pro 2019.1 (Windows)</p> <p>Video Frame Rate : 29.970030</p> <p>Video Field Order : Progressive</p> <p>Video Pixel Aspect Ratio : 1</p> <p>Audio Sample Rate : 48000</p> <p>Audio Sample Type : 16-bit integer</p> <p>Audio Channel Type : Stereo</p> <p>Start Time Scale : 30000</p> <p>Start Time Sample Size : 1001</p> <p>Orientation : Horizontal (normal)</p> <p>Instance ID : xmp.iid:69cd4756-0890-e741-9bea-d0b9a1e59366</p> <p>Document ID : 20b51f75-72d3-8fa3-78bb-882b00000065</p> <p>Original Document ID : xmp.did:51701fde-e342-4243-9e89-1673bc8a6486</p> <p>Format : H.264</p> <p>Duration Value : 4830720</p> <p>Duration Scale : 1.1111111111111111e-005</p> <p>Project Ref Type : Movie</p> <p>Video Frame Size W : 1280</p> <p>Video Frame Size H : 720</p> <p>Video Frame Size Unit : pixel</p> <p>Start Timecode Time Format : 29.97 fps (non-drop)</p> <p>Start Timecode Time Value : 00:00:00:00</p> <p>Alt Timecode Time Value : 00:00:00:00</p> <p>Alt Timecode Time Format : 29.97 fps (non-drop)</p> <p>History Action : saved, created, saved</p> <p>History Instance ID : 45bf5236-f40f-150f-d190-e4a300000092, xmp.iid:fbbabd26-6c68-e740-93ea-7f1c6d64edc, xmp.iid:8442e554-89c5-dd45-aa31-9f7787d694ce, xmp.iid:69cd4756-0890-e741-9bea-d0b9a1e59366</p> <p>History When : 2019:04:04 03:51:21-06:00, 2019:04:04 03:51:49-06:00, 2019:04:04 03:51:49-06:00, 2019:04:04 03:51:49-06:00</p> <p>History Software Agent : Adobe Premiere Pro 2019.1 (Windows), Adobe Premiere Pro 2019.1 (Windows), Adobe Premiere Pro 2019.1 (Windows)</p> <p>History Changed : /, /, /metadata</p> <p>Ingredients Instance ID : xmp.iid:085a4b06-fc9f-b34b-9938-f89d37bd6ba1, xmp.iid:085a4b06-fc9f-b34b-9938-f89d37bd6ba1,</p>	
--	--	--	--

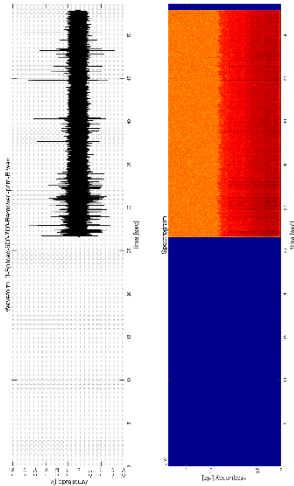

		<pre> xmp.iid:085a4b06-fc9f-b34b-9938-f89d37bd6ba1, xmp.iid:085a4b06-fc9f-b34b-9938-f89d37bd6ba1 Ingredients Document ID : 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035 Ingredients From Part : time:0d5085400320000f254016000000, time:0d5085400320000f254016000000, time:5932967040000f254016000000d8534996870400f254016000000, time:5932967040000f254016000000d8534996870400f254016000000 Ingredients To Part : time:0d5085400320000f254016000000, time:0d5085400320000f254016000000, time:5085400320000f254016000000d8534996870400f254016000000, time:5085400320000f254016000000d8534996870400f254016000000 Ingredients File Path : 9.mp4, 9.mp4, 9.mp4, 9.mp4 Ingredients Mask Markers : None, None, None, None Pantry Create Date : 2018:08:07 18:30:24Z Pantry Modify Date : 2019:04:03 13:02:50Z Pantry Metadata Date : 2019:04:04 03:51:49-06:00 Pantry Orientation : Horizontal (normal) Pantry Instance ID : xmp.iid:085a4b06-fc9f-b34b-9938-f89d37bd6ba1 Pantry Document ID : 951272b3-acfc-d9dd-503e-c38700000035 Pantry Original Document ID : xmp.did:95aebf18-0e6c-0e43-b22b-62d097d1c9e0 Pantry History Action : saved Pantry History Instance ID : xmp.iid:45b0a3d8-c2fa-e44e-9619-1328fdb1af2d Pantry History When : 2019:04:04 03:51:49-06:00 Pantry History Software Agent : Adobe Premiere Pro 2019.1 (Windows) Pantry History Changed : /metadata Pantry Duration Value : 27387360 Pantry Duration Scale : 2.083333333333333e-006 Pantry Tracks Track Name : Comment Pantry Tracks Track Type : Comment Pantry Tracks Frame Rate : f30000s1001 Pantry Tracks Markers Start Time: 700 Pantry Tracks Markers Guid : 1fad9e70-e74f-41a4-8d26-de1fd08906eb Pantry Tracks Markers Cue Point Params Key: marker_guid Pantry Tracks Markers Cue Point Params Value: 1fad9e70-e74f-41a4-8d26-de1fd08906eb Derived From Instance ID : xmp.iid:fbabd26-6c68-e740-93ea-7f1c6d464edc Derived From Document ID : xmp.did:fbabd26-6c68-e740-93ea-7f1c6d464edc Derived From Original Document ID: xmp.did:fbabd26-6c68-e740-93ea-7f1c6d464edc Windows Atom Extension : .prproj </pre>	
--	--	---	--

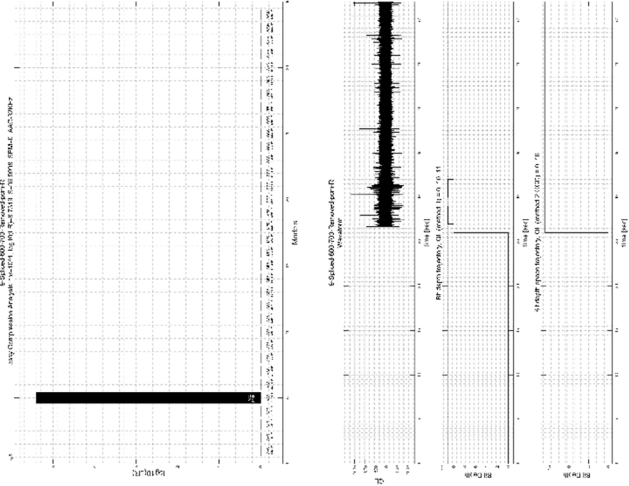

		<p>Windows Atom Invocation Flags : /L</p> <p>Mac Atom Application Code : 1347449455</p> <p>Mac Atom Invocation Apple Event : 1129468018</p> <p>Movie Data Size : 70003722</p> <p>Movie Data Offset : 41098</p> <p>Avg Bitrate : 10.4 Mbps</p> <p>Image Size : 1280x720</p> <p>Rotation : 0</p>		
2	Header Analysis		The file's header was a RIFF AVI file.	
3	Hex Data Analysis		The hex entry AB 00 00 00 = 171 frames. Hex entry 01 00 00 00 = 1 stream. The second screen shot to the left for hex offset 12 08 – offset 12 0F contained an entry for Virtual Dub software	

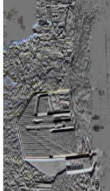

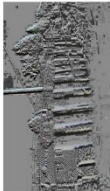

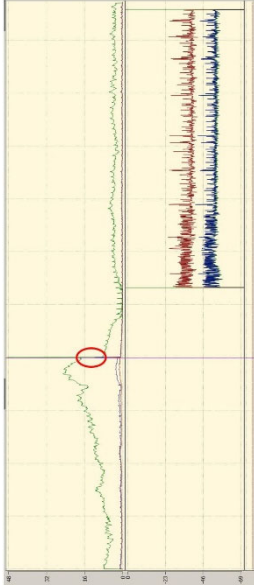

4	Workflow Optimization Decision	<pre> graph TD A{File Structure Consistent With Original?} -- Yes --> B[Continue] A -- No --> C[Stop] </pre>	Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication and video authentication framework.	Continue
5	Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.			
6	Video File Bifurcation Process - File Preparation Decision Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.	Split two stereo audio streams into two wave files	Used right audio stream for audio analysis	O
7	AUDIO STREAM ANALYSIS			
8	Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis			
9	Global Analysis	DC Offset Analysis		

10	Power Analysis		
11	Zero Analysis		
12	LTAS Analysis		

13	LTASS Analysis		<input checked="" type="checkbox"/>	
14	DSS	NR		
15	CLA		<input checked="" type="checkbox"/>	
16	MDCT		<input checked="" type="checkbox"/>	
17				
18	Local Analysis	Critical Listening	Waveform: Spectrogram	
19		Waveform Analysis		<input checked="" type="checkbox"/>

20	Spectrum / Spectrogram Analysis			
21	DC Offset Analysis		NR	
22	Power Analysis		NR	
23	Zero Analysis		NR	

24	QL / Bit Depth Analysis			
25	ENF Analysis			NR
26				
27	VIDEO STREAM ANALYSIS			
28	Repeat This Analysis Area For Each Video Stream Analyzed			
29	SPN Analysis			NR
30	CFA Analysis			NR
31	CLA			NR
32	Pixel Level Analysis			NR

33	Block Level Analysis				NR
34	Temporal (Interpolation) Analysis				NR
35					
36	Visual Anomaly Analysis	  	Visual analysis of frames 598, 599, & 600 using a temporal difference filter between frames.		
37	Copy & Move Analysis				NR
38	Double Quantization Analysis				NR
39	Local Analysis		Temporal analysis of the Y plane of the current frame and the preceding one indicates a major visual change from one frame to the next between frame 598 and frame 600. Ran 2D Phase Congruency with correlation coefficient of adjacent frames and noted a spike in the video at the same location as noted in the global pixel level analysis and visual anomaly analysis noted above.		

40	Local Block Manipulation Analysis			NR
41				
42	Overall Decision For Hypothesis			

- ☒ Consistent with an original recording.
- ☒ Not Consistent with an original recording.
- ☐ Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.

APPENDIX F-3 Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses

Hypothesis	<i>Has the video stream, video stream and audio stream, or audio stream been altered or edited?</i>
------------	---

Questioned File Information

File Name:	9-spliced-1075-1076-removed.mp4
File Size:	74734195 bytes
MD5 Hash:	b9eace9715fed4c64252894e423180e
SHA1 Hash:	f9e8ee09c729ef69a35dad3d4230b5ff87fl ea6
SHA256 Hash:	f736ff0c3e12322e169d09a6e58f3c32e1e8186d2777ee2addc73352ddb30930

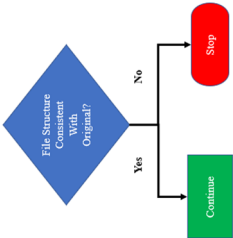
HYPOTHESIS ANALYSIS

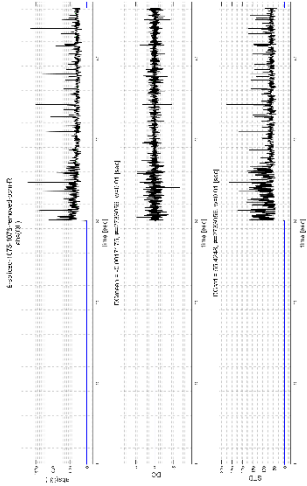

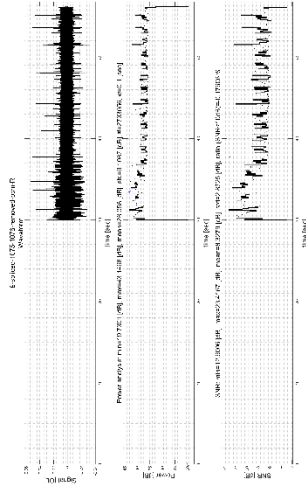

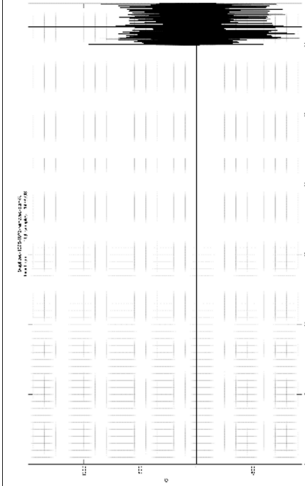

#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

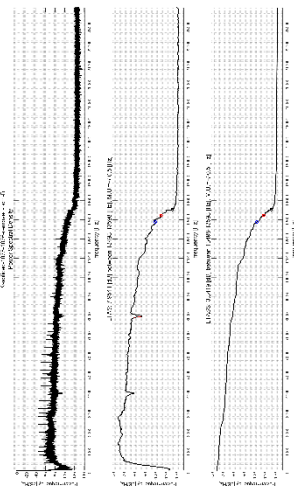

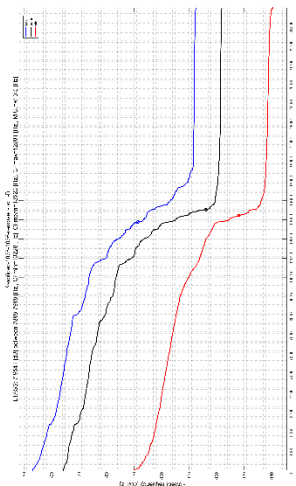

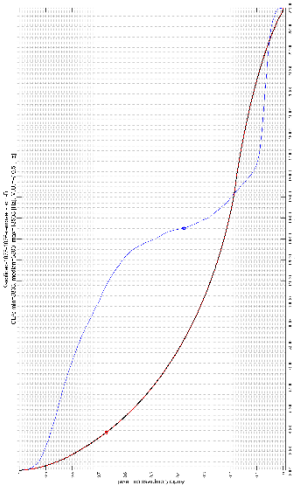

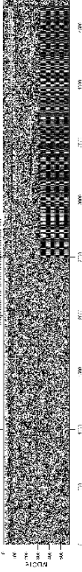

1	<div> <div>File Structure Analysis</div> <div>File Format Analysis</div> </div>	<div> <div>File Name</div> <div>File Size</div> <div>File Modification Date/Time</div> <div>File Access Date/Time</div> <div>File Creation Date/Time</div> <div>File Permissions</div> <div>File Type</div> <div>MIME Type</div> <div>Major Brand</div> <div>Minor Version</div> <div>Compatible Brands</div> <div>Movie Header Version</div> <div>Create Date</div> <div>Modify Date</div> <div>Time Scale</div> <div>Duration</div> <div>Preferred Rate</div> <div>Preferred Volume</div> <div>Preview Time</div> <div>Preview Duration</div> <div>Poster Time</div> <div>Selection Time</div> <div>Current Time</div> <div>Next Track ID</div> <div>Track Header Version</div> <div>Track Create Date</div> <div>Track Modify Date</div> <div>Track ID</div> <div>Track Duration</div> <div>Track Layer</div> <div>Track Volume</div> <div>Image Width</div> <div>Image Height</div> <div>Graphics Mode</div> <div>Op Color</div> <div>Compressor ID</div> <div>Source Image Width</div> <div>Source Image Height</div> <div>X Resolution</div> <div>Y Resolution</div> <div>Compressor Name</div> <div>Bit Depth</div> <div>Matrix Structure</div> <div>Media Header Version</div> <div>Media Create Date</div> <div>Media Modify Date</div> <div>Media Time Scale</div> <div>Media Duration</div> <div>Media Language Code</div> <div>Balance</div> <div>Handler Type</div> </div> <div> <div>: 9-spliced-1075-1076-removed.mp4</div> <div>: 71 MB</div> <div>: 2019:04:04 06:23:40-04:00</div> <div>: 2019:04:05 14:52:08-04:00</div> <div>: 2019:04:05 14:51:55-04:00</div> <div>: rw-rw-rw-</div> <div>: MP4</div> <div>: video/mp4</div> <div>: MP4 v2 [ISO 14496-14]</div> <div>: 0.0.0</div> <div>: mp42, mp41</div> <div>: 0</div> <div>: 2019:04:04 10:23:38</div> <div>: 2019:04:04 10:23:39</div> <div>: 90000</div> <div>: 0:00:56</div> <div>: 1</div> <div>: 100.00%</div> <div>: 0 s</div> <div>: 0 s</div> <div>: 0 s</div> <div>: 0 s</div> <div>: 0 s</div> <div>: 0 s</div> <div>: 0 s</div> <div>: 3</div> <div>: 0</div> <div>: 2019:04:04 10:23:38</div> <div>: 2019:04:04 10:23:38</div> <div>: 1</div> <div>: 0:00:56</div> <div>: 0</div> <div>: 0.00%</div> <div>: 1280</div> <div>: 720</div> <div>: srcCopy</div> <div>: 0 0 0</div> <div>: avc1</div> <div>: 1280</div> <div>: 720</div> <div>: 72</div> <div>: AVC Coding</div> <div>: 24</div> <div>: 1 0 0 1 0 0 1</div> <div>: 0</div> <div>: 2019:04:04 10:23:38</div> <div>: 2019:04:04 10:23:38</div> <div>: 48000</div> <div>: 0:00:56</div> <div>: eng</div> <div>: 0</div> <div>: Alias Data</div> </div>	<div> <div>Did not observe any camera entries in the ascii area, but did note the presence of Adobe Premiere.</div> <div></div> </div>	
---	---	--	--	--

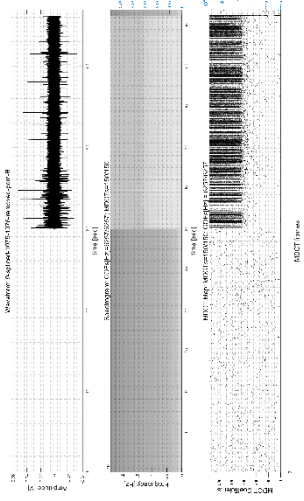
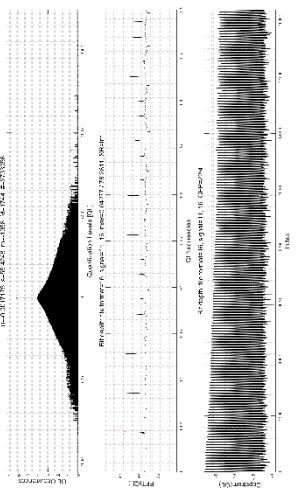
[illegible]


		<p>xmp.iid:c460e422-4f45-254d-819a-a661bd96971a, xmp.iid:c460e422-4f45-254d-819a-a661bd96971a, xmp.iid:c460e422-4f45-254d-819a-a661bd96971a, xmp.iid:c460e422-4f45-254d-819a-a661bd96971a, xmp.iid:c460e422-4f45-254d-819a-a661bd96971a, xmp.iid:c460e422-4f45-254d-819a-a661bd96971a, xmp.iid:c460e422-4f45-254d-819a-a661bd96971a</p> <p>Ingredients Document ID : 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035, 951272b3-acfc-d9dd-503e-c38700000035</p> <p>Ingredients From Part :</p> <p>time:0d5085400320000f254016000000, time:0d5085400320000f254016000000, time:0d5085400320000f254016000000, time:5085400320000f254016000000d847566720000f254016000000, time:5085400320000f254016000000d847566720000f254016000000, time:5932967040000f254016000000d3178375200000f254016000000, time:5932967040000f254016000000d3178375200000f254016000000, time:9128293574400f254016000000d5339670336000f254016000000, time:9128293574400f254016000000d5339670336000f254016000000</p> <p>Ingredients To Part :</p> <p>time:0d5085400320000f254016000000, time:0d5085400320000f254016000000, time:5085400320000f254016000000d847566720000f254016000000, time:5085400320000f254016000000d847566720000f254016000000, time:5932967040000f254016000000d3178375200000f254016000000, time:5932967040000f254016000000d3178375200000f254016000000, time:9111342240000f254016000000d5339670336000f254016000000, time:9111342240000f254016000000d5339670336000f254016000000</p> <p>Ingredients File Path : 9.mp4, 9.mp4, 9.mp4, 9.mp4, 9.mp4, 9.mp4, 9.mp4, 9.mp4, 9.mp4, 9.mp4</p> <p>Ingredients Mask Markers : None, None, None, None, None, None, None, None, None, None</p> <p>Pantry Create Date : 2018:08:07 18:30:24Z</p> <p>Pantry Modify Date : 2019:04:03 13:02:50Z</p> <p>Pantry Metadata Date : 2019:04:04 04:23:39-06:00</p> <p>Pantry Orientation : Horizontal (normal)</p> <p>Pantry Instance ID : xmp.iid:c460e422-4f45-254d-819a-a661bd96971a</p> <p>Pantry Document ID : 951272b3-acfc-d9dd-503e-c38700000035</p> <p>Pantry Original Document ID : xmp.did:95aebf18-0e6c-0e43-b22b-62d097d1c960</p> <p>Pantry History Action : saved</p> <p>Pantry History Instance ID : xmp.iid:765a3698-d792-5746-bf83-2143898d16b4</p> <p>Pantry History When : 2019:04:04 04:23:39-06:00</p> <p>Pantry History Software Agent : Adobe Premiere Pro 2019.1 (Windows)</p> <p>Pantry History Changed : /metadata</p>	
--	--	---	--

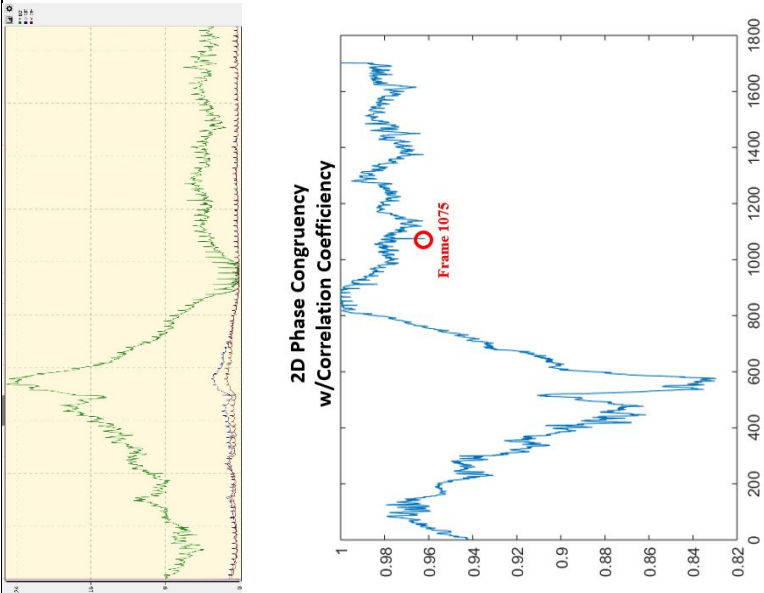
2		Header Analysis				
3		Hex Data Analysis				
4		Workflow Optimization Decision			Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication framework.	Continue
5		Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.				
6	Video File Bifurcation Process - File Preparation Decision	Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.	Split two stereo audio streams into two wave files	Used right audio stream for audio analysis		O
7		AUDIO STREAM ANALYSIS				
8		Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis				

9	DC Offset Analysis			
10	Global Analysis Power Analysis			
11	Zero Analysis			

12	LTAS Analysis			
13	LTASS Analysis			
14	DSS		NR	
15	CLA			
16	MDCT			
17				

18	Critical Listening	Waveform: Spectrogram			NR
19	Waveform Analysis				<input checked="" type="checkbox"/>
20	Spectrum / Spectrogram Analysis				<input checked="" type="checkbox"/>
21	DC Offset Analysis				NR
22	Power Analysis				NR
23	Zero Analysis				NR
24	QL / Bit Depth Analysis				<input checked="" type="checkbox"/>
25	ENF Analysis				NR
26					
27	VIDEO STREAM ANALYSIS				
28	Repeat This Analysis Area For Each Video Stream Analyzed				

29	Global Analysis	SPN Analysis			NR
30		CFA Analysis			NR
31		CLA			NR
32		Pixel Level Analysis			NR
33		Block Level Analysis			NR
34		Temporal (Interpolation) Analysis			NR
35					
36	Local Analysis	Visual Anomaly Analysis		Visual inconsistencies are very minor at comparing 1074 to 1075. Two frames were removed, but without the local pixel manipulation analysis of 2d Phase Congruency with CC, the subtle inconsistency would probably be overlooked.	O
37		Copy & Move Analysis			NR
38		Double Quantization Analysis			NR

39	Local Pixel Manipulation Analysis	 <p>Temporal analysis of the Y plane of the current frame and the preceding one indicated no major visual changes. The subtle removal of two frames were not detected.</p> <p>2d Phase Congruency with correlation coefficient of adjacent frames resulted in subtle spike in the histogram at frame 1075.</p>	<div>✗</div>
40	Local Block Manipulation Analysis		NR
41			
42			<div>✗</div>
Overall Decision For Hypothesis			

✔

Consistent with an original recording.

✗

Not Consistent with an original recording.

O Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.

APPENDIX F-4 Digital Video Authentication Framework Workflow Analysis Form

Analysis Questions As Hypotheses


Hypothesis	<i>Has the video stream, video stream and audio stream, or audio stream been altered or edited?</i>
------------	---

Questioned File Information

File Name:	9-pre-event-buffering-removed.mp4
File Size:	24628701 bytes
MD5 Hash:	e12459cc100f7ada406f2d2be84fb573
SHA1 Hash:	62597ffce55ca79b0dc8617ae3de34e211295b8b
SHA256 Hash:	3dde4fabffe8f18961efbee52ca1fd9dd428aeee63da695d39e2ecf0b8223c61a

HYPOTHESIS ANALYSIS


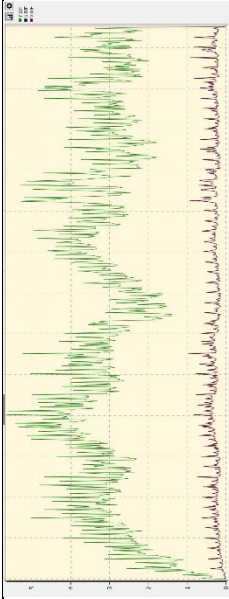
#	Analytical Area	Type of Analysis	Data	Observations / Comments	Decision
---	-----------------	------------------	------	-------------------------	----------

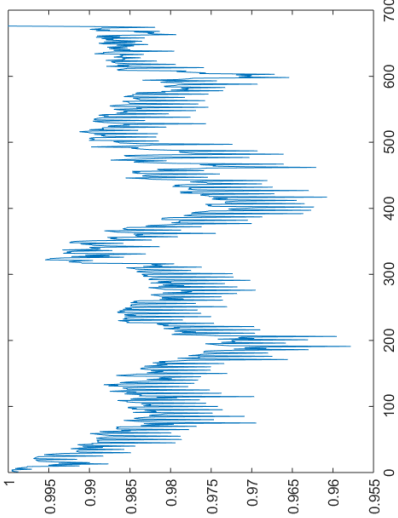
<div> <div>File Structure Analysis</div> <div>1</div> </div>	<div>File Format Analysis</div>	<div> <div>File Name</div> <div>File Size</div> <div>File Modification Date/Time</div> <div>File Access Date/Time</div> <div>File Creation Date/Time</div> <div>File Permissions</div> <div>File Type</div> <div>MIME Type</div> <div>Major Brand</div> <div>Minor Version</div> <div>Compatible Brands</div> <div>Movie Header Version</div> <div>Create Date</div> <div>Modify Date</div> <div>Time Scale</div> <div>Duration</div> <div>Preferred Rate</div> <div>Preferred Volume</div> <div>Preview Time</div> <div>Preview Duration</div> <div>Poster Time</div> <div>Selection Time</div> <div>Selection Duration</div> <div>Current Time</div> <div>Next Track ID</div> <div>Track Header Version</div> <div>Track Create Date</div> <div>Track Modify Date</div> <div>Track ID</div> <div>Track Duration</div> <div>Track Layer</div> <div>Track Volume</div> <div>Image Width</div> <div>Image Height</div> <div>Graphics Mode</div> <div>Op Color</div> <div>Compressor ID</div> <div>Source Image Width</div> <div>Source Image Height</div> <div>X Resolution</div> <div>Y Resolution</div> <div>Bit Depth</div> <div>Pixel Aspect Ratio</div> <div>Video Frame Rate</div> <div>Matrix Structure</div> <div>Media Header Version</div> <div>Media Create Date</div> <div>Media Modify Date</div> <div>Media Time Scale</div> <div>Media Duration</div> <div>Media Language Code</div> </div> <div> <div>9-pre-event-buffering-removed.mp4</div> <div>23 MB</div> <div>2019:04:06 10:18:32-04:00</div> <div>2019:04:06 20:13:15-04:00</div> <div>2019:04:06 20:13:05-04:00</div> <div>rw-rw-rw-</div> <div>MP4</div> <div>video/mp4</div> <div>MP4 Base Media v1 [ISO 14496-12:2003]</div> <div>0.2.0</div> <div>isom, iso2, avc1, mp41</div> <div>0</div> <div>0000:00:00 00:00:00</div> <div>0000:00:00 00:00:00</div> <div>1000</div> <div>27.16 s</div> <div>1</div> <div>100.00%</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>0 s</div> <div>3</div> <div>0</div> <div>0000:00:00 00:00:00</div> <div>0000:00:00 00:00:00</div> <div>1</div> <div>27.12 s</div> <div>0</div> <div>0.00%</div> <div>1920</div> <div>1080</div> <div>srcCopy</div> <div>0 0 0</div> <div>avc1</div> <div>1920</div> <div>1080</div> <div>72</div> <div>72</div> <div>24</div> <div>1:1</div> <div>25</div> <div>1 0 0 1 0 0 1</div> <div>0</div> <div>0000:00:00 00:00:00</div> <div>0000:00:00 00:00:00</div> <div>48000</div> <div>27.16 s</div> <div>und</div> </div>
	<div>Did not observe any camera entries in the ascii area, but did note the presence of Apple and Lavf58.20.100 encoder. Axon Fleet Camera uses an Ambrella AVC encoder.</div>	<div>  </div>

		<p>Handler Description</p> <p>Balance : 0</p> <p>Audio Format : mp4a</p> <p>Audio Channels : 2</p> <p>Audio Bits Per Sample : 16</p> <p>Audio Sample Rate : 48000</p> <p>Handler Type : Metadata</p> <p>Handler Vendor ID : Apple</p> <p>Encoder : Lavf58.20.100</p> <p>Movie Data Size : 24606612</p> <p>Movie Data Offset : 22089</p> <p>Avg Bitrate : 7.25 Mbps</p> <p>Image Size : 1920x1080</p> <p>Rotation : 0</p>			
2	Header Analysis			The file's header was a RIFF AVI file.	
3	Hex Data Analysis			The hex entry AB 00 00 00 = 171 frames. Hex entry 01 00 00 00 = 1 stream. The second screen shot to the left for hex offset 12 08 – offset 12 0F contained an entry for Virtual Dub software	

4	<i>Workflow Optimization Decision</i>	<pre> graph TD A{File Structure Consistent With Original?} -- Yes --> B[Continue] A -- No --> C[Stop] </pre>	Normally, optimization decision would be to stop. However, examiner will continue to illustrate more of the workflow and video authentication and video authentication framework.	Continue To Video Only
5	<i>Go To Block 6 For File Preparation Decision If Workflow Optimization Decision Is Continue Analysis.</i>			
6	Video File Bifurcation Process - File Preparation Decision Document To Right If Audio And / Or Video Streams Require Transcoding In Bifurcation Process.			N/A
7	AUDIO STREAM ANALYSIS			
8	<i>Repeat This Analysis Area For Each Audio Stream If Audio Stream Is Analyzed Or Go To Block 27 For Video Stream Analysis</i>			
9	Global Analysis	DC Offset Analysis		
10		Power Analysis		
11		Zero Analysis		
12		LTAS Analysis		
13		LTASS Analysis		

14		DSS				
15		CLA				
16		MDCT				
17						
18		Critical Listening	Waveform:			
19		Waveform Analysis	Spectrogram			
20		Spectrum / Spectrogram Analysis				
21		DC Offset Analysis				
22		Power Analysis				
23		Zero Analysis				
24		QL / Bit Depth Analysis				
25		ENF Analysis				
26						
27						
28						
29		SPN Analysis				NR
30		CFA Analysis				NR
31		CLA				NR

32	Pixel Level Analysis			NR
33	Block Level Analysis			NR
34	Temporal (Interpolation) Analysis			NR
35				
36	Visual Anomaly Analysis		No visual inconsistencies, but noticeably absent is pre-event buffering.	
37	Local Analysis	Copy & Move Analysis		
38		Double Quantization Analysis		NR
39		Local Pixel Manipulation Analysis		O

				
40	Local Block Manipulation Analysis			NR
41	Overall Decision For Hypothesis			
42				

- ☒ Consistent with an original recording.
- ☒ Not Consistent with an original recording.
- ☐ Inconclusive / cannot run.

Conclusion:

The evidence file and video stream is NOT CONSISTENT with an original recording.