THE VIABILITY OF EVIDENCE RETRIEVED FROM COUNTERFEIT AND UNBRANDED TECHNOLOGY

by

CHRISTOPHER L.M. WHEELER

A.A., Macon State College, 2005

B.S., Macon State College, 2007

M.S., Mercer University, 2013

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 Program

2019

This thesis for the Master of Science degree by

Christopher L.M. Wheeler

has been approved for the

Recording Arts Program

by

Catalin Grigoras

Jeff Smith

Cole Whitecotton

Date: May 18, 2019

Wheeler, Christopher L.M. (M.S., Recording Arts Program)

The Viability of Evidence Retrieved from Counterfeit and Unbranded Technology

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

Since the iPhone hit the market in 2007, there has been a large increase in the amount of recording devices of various sorts that become easily accessible and cost effective to the population at large. There is a great deal of information available on the mainstream devices for forensic professionals to review, and research is always ongoing to add to that information. Along with these well-known devices, we are also now able to get any number of cheap, cloned, and counterfeit devices that can do many of the same functions. Chapter 1 reviews devices that are commonly available at low cost and summarizes the possible problems with their use and the recovery of data to use as evidence in criminal and civil cases. Chapter 2 is a list of the devices and software used in this study, along with the basic information that is being reviewed for each type of media and device and the framework for the research done. Chapter 3 contains the data explored from each device, along with the findings from each item found. Finally, Chapter 4 is the conclusions drawn from the data found.

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

Approved: Catalin Grigoras

I dedicate this work to my wife Amy and my daughters Audrey and Darla.

You make me want to be the best “me” I can be.

ACKNOWLEDGEMENTS

It is hard to single out any one person at the NCMF, as you have all been great over the last couple of years. Catalin and Jeff, you have both been good friends during this time, and I am a better person for having known you both. Leah, without you I would never remember to finish anything, so you have been a blessing a thousand time over. Thank you all for everything.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF ABBREVIATIONS

EXIF - Exchangeable Image File Format

FTK - AccessData Forensic Tool Kit

Hex - Hexadecimal

JPEG - Joint Photographic Experts Group

SIM - Subscriber Identity Module

UFED - Universal Forensic Extraction Device

USB - Universal Serial Bus

CHAPTER I

INTRODUCTION

With the advent of the personal computer in the 1970s, the need for forensic professionals to follow developing technological trends has become not only good practice, but a necessity in the fluid landscape of computer science. Items that were considered science fiction 20 years ago have become common household items today. Many of the consumer electronics that were popular in the 1980s and 90s have all been replaced with a single item, the smart phone. With the proliferation of computer and media technology in the world today, it has also become cheaper to produce. Consumers can get decent quality recording and computer equipment at a nominal cost.

Along with this boom in technology there has also been a growing market for low end, or "unbranded" technology. To explain further, unbranded products can be seen predominantly in online markets such as eBay, Amazon, and numerous "click-bait" stores that advertise throughout social media. To identify likely unbranded technology, one need only to look at the unbelievable price something is being offered at. A Samsung Gear smartwatch or Apple Watch can cost anywhere from $150.00 to $400.00 dollars depending on the model, but an unbranded smartwatch can be found for as little as $0.75 cents as seen in the figure below. The old saying that you get what you pay for does come in to play here, as these devices are of a far inferior quality to their branded counterparts. Even so, it does not mean that there is not valid and useful forensic evidence to be found on them.

Figure 1.1 eBay Auction Screenshot, March 2019

Exploring Unbranded Technology

When looking at lower cost technology, there are distinctions that can be made for different types or classes of items. Unbranded is defined as a product that is sold under the name of a shop rather than the company that made it [4]. An example of this would be a Staples brand USB drive that is bought at Staples Office Supplies. It may have been made by SanDisk, but there are no outside markings to let us know. Because these items are commonly made by the same companies that make their own branded items, they tend to function in a predictable manner much like their brand name counterparts. For the purposes of this study, these items will not be used, as they have known manufacturers and specifications. Another type of unbranded technology could also be defined as technology that is not cloned or counterfeit but has no specific manufacturer [3]. An example of this is the U8 smart watch depicted in figure 1-1. Searches for a source for this device show that there are numerous manufacturers and no specific company or designer named.

Unbranded technology runs the gambit between decent store brands and cheap technology that may not work, but counterfeit technology is slightly different. In this case items may be marketed as a branded item, yet once purchased for a very low price, the consumer finds that they have purchased a substandard product of much lower quality [1]. Another version of this is using cloned software on a different device. An example would be using the program code from an Olympus audio recorder to run a low-quality audio recorder. While this is an economic and intellectual property theft problem [2], that is not the focus of this study. What is important here is the evidence created.

As time goes on, forensic professionals are going to encounter more of this technology rather than less. When faced with these lower quality items we must ask: Does the low quality or unethical creation of these items make the data any less valid or viable than other digital devices? When looking at the files created, can the devices used for creation be identified, and are the files that are created in a recognizable format that can be easily accessed and used?

Another area of note is the multi-functionality of many of these devices. The common unbranded smartwatch not only functions as an add on to a smartphone but can often be fitted with a SIM card to

make the watch a stand-alone phone. Does this mean that evidence can be collected from these devices in the same manner that we already collect data from cell phones? On the web base article “China Phone Hacking”, there is a great deal of information about how to possibly access the file structure of these watches to obtain the data they contain [7], but identifying the exact hardware and firmware on the devices is not always easy or even possible.

CHAPTER II

PREPARATIONS

This is an exploratory test on various types of multimedia created on a variety of unbranded/counterfeit devices. The original concept was to test several smart watches and find what data could be collected from them, however; after receiving many watches they were found to have arrived damaged or became inoperable shortly after arrival and before data could be retrieved. Due to this, two unbranded watches were selected due to the fact they reliably continued to function throughout testing. Added to this study were two unbranded hidden cameras and two unbranded audio recorders. All devices will be used to create native files for the device type and the data will be collected in a forensically sound manner for analysis in appropriate programs. The goal of this study is not to judge the quality of the respective file type, but rather to find if the files can be authenticated based on the device that created them, and in the case of the smart watches, if they leave evidence on the phone they are paired with.

Materials

The software programs used in this study were: Cellebrite version 7.15.1, FTK Imager, iZotope RX 6, JPEGSnoop, Media Info, FFMPEG, HXD and 010 Hex Editors and USBDview. The two smart watches selected are unbranded. One contains a model number of yay-q18, and the other, R306. They are depicted as follows:

Figure 2.1 yay-Q18 Smart Watch

Figure 2.2 R306 Smart Watch

The first audio recorder used in this study is a USB voice recorder, no known brand, and is depicted below.

Figure 2.3 USB Voice Recorder

The second audio recorder used was an unbranded, standalone recorder like a small Olympus voice recorder and depicted below

Figure 2.4 Stand-Alone Voice Recorder

The final two devices were two “hidden” cameras. The first was in the shape of a lighter (Figure 2.5) and the other was in the shape of a pen (Figure 2.6).

Figure 2.5 Lighter Hidden Camera *Figure 2.6 Pen Hidden Camera*

Micro SD cards were the storage required by all devices that did not have built-in memory. Micro Center brand 16 GB Micro SDHC cards were used in this study. The final item used was a Samsung Galaxy S5 smartphone, model number SM-G900T. For the duration of this study the phone was activated on the T-Mobile network. The phone and memory card type are depicted in figures 2.7 and 2.8.

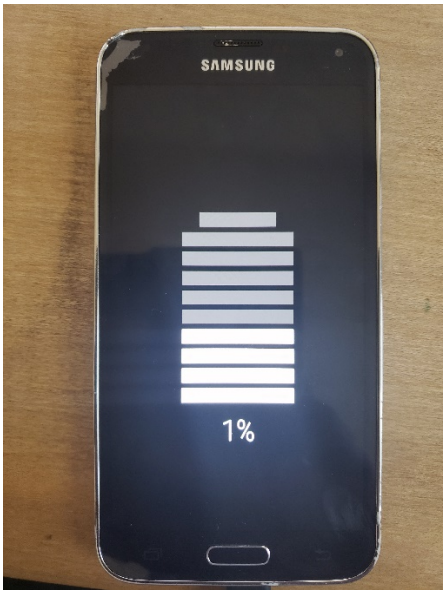


Figure 2.7 Micro SD Card *Figure 2.8 Samsung Galaxy S5*

Methods

This study did not focus on audio, video, or image files that were created by the phone, so no recordings were made with it. The rest of the items were used to create various files based on the type of device. The following table indicates the files that were created with each device, and the software used to retrieve the data from the device storage while employing USB write-blocking software:

Table 2.1 Device Data Retrieval

Device	Files Created	Data Acquistion Method	USB Identifier
Smart Watch 1 yayq18	IMG001A.jpg 010100052900.amr	FTK Imager	No Identifier found
Smart Watch 2 R306	IMG0002A.jpg 010100162400.amr	FTK Imager	VID_0E8D&PID_0002\530271807000700
Audio recorder	REC001.wav	FTK Imager	VID_10D6&PID_1101\7&2a24e7ed&0&1
USB Audio Recorder	rec00000.mp3 rec00001.mp3	FTK Imager	VID_E0B6&PID_0811\7&2a24e7ed&0&1
Lighter Camera	SUNP0000.avi SUNP0001.avi SUNP0002.avi SUNP0003.avi SUNP0004.avi SUNP0005.avi SUNP0006.avi SUNP0007.avi SUNP0008.avi PICT0000.jpg PICT0001.jpg	FTK Imager	VID_1B3F&PID_0C52
Pen Camera	PICT0000.jpg RECO0000.wav	FTK Imager	VID_046D&PID_C537\6&31465cb8&0&10

As shown, each device was used to create media files in one, or more when applicable, media types. Also shown is the USB identification of each device when available. Regarding the smartwatches, the data retrieved was from the microSD card only.

Utilizing both HxD and 010 Hex editors, I will be checking the hex data of the created multimedia files to look for unique and identifiable features to help with authentication of the files, and to check if any device specific information is embedded in that hex data. IZotope RX 6 will be used to check the spectrographs of all audio data to look for any visual indication of inconsistencies within the sound data produced and to verify that sound data does exist within the file if playback fails.

During this study, attempts were made using Cellebrite to try and retrieve all available data from the watches using generic phone profiles. All attempts to acquire images of the watches in this manner failed. Further attempts to mount the file system of each watch as a readable drive also failed in both Windows and Linux operating system. To attempt to gather further data on the devices, each smartwatch was paired with the Galaxy S5 phone and used to send and receive at least one text message. The phone was then forensically acquired following standard Cellebrite procedures. The phone was wiped and reset for each watch pairing. The data retrieved from the phone was consolidated in a UFED Reader report from Cellebrite to be used as reference for this report.

CHAPTER III

BREAKDOWN OF RETRIEVED DATA

Analysis of Smartwatch 1

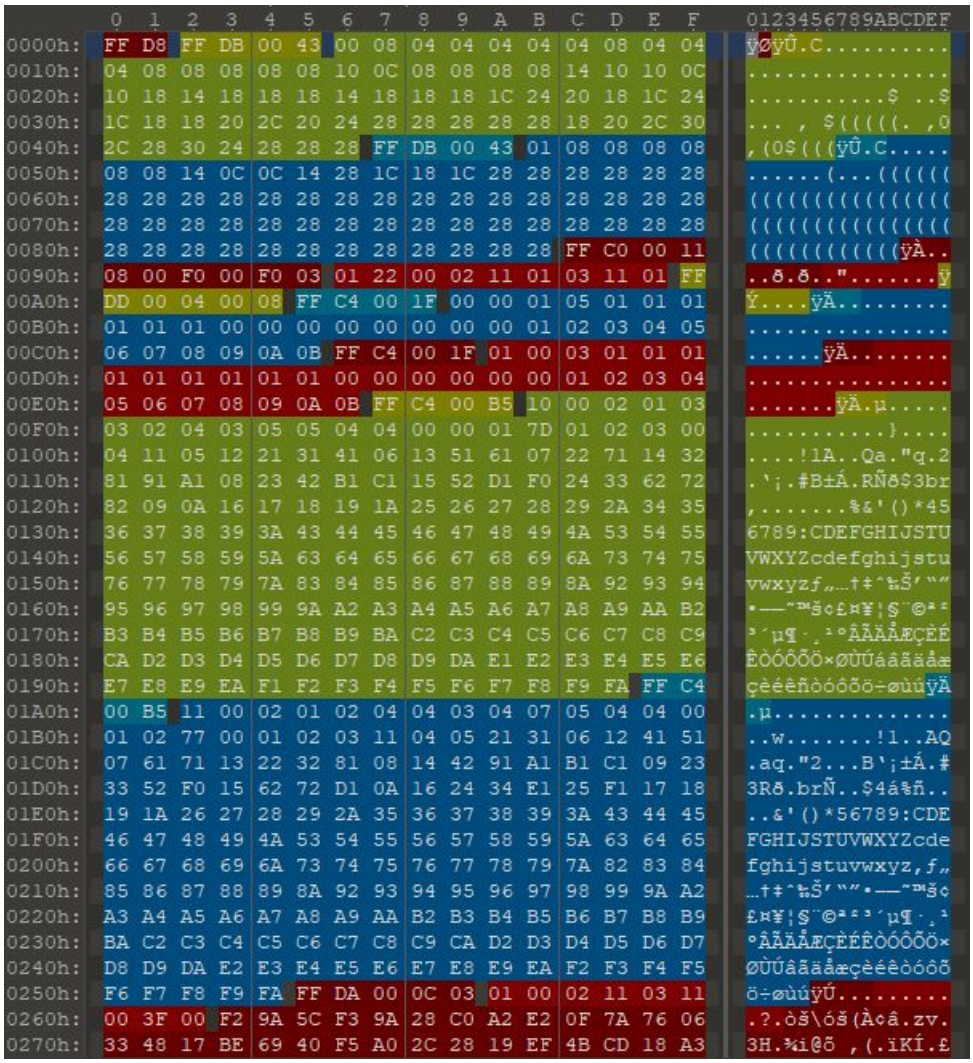
Smartwatch one contains both a camera and a microphone and can create audio and visual media. Attempts to create test media originally failed due to the need to have a memory card placed in the device for storage. Once a microSD card was placed in the device, a photo was taken, and an audio file was recorded using the built-in camera and microphone. The device was set for a date of 12/31/2016 at around 11:00 pm when these tests were conducted. The test files were retrieved using FTK Imager and the watch as an external USB drive. The files retrieved were IMG001A.jpg and 010100052900.amr.

Device Analysis

While this device was connected to the computer, a check of USB devices was made. No identifying data was retrieved, and the device was listed simply as a USB Mass Storage Device. While attached, only the microSD card was accessible, no connection to the watch file structure was made.

File Analysis

The first item checked was the time stamps of the retrieved files. Both the image and audio file were seen to have time stamps consistent with the time displayed on the watch at the time of creation. The next item checked was the file information in HxD and 010 hex editors for the file structure information. The hex data found for IMG001A.jpg is as follows in Figure 3.1.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	FF	D8	FF	DB	00	43	00	08	04	04	04	04	04	08	04	04	ÿØÿÛ.C.....
0010h:	04	08	08	08	08	08	10	0C	08	08	08	08	14	10	10	0C	.....
0020h:	10	18	14	18	18	18	14	18	18	18	1C	24	20	18	1C	24	.....$ ..$
0030h:	1C	18	18	20	2C	20	24	28	28	28	28	28	18	20	2C	30	... , $(((((. ,0
0040h:	2C	28	30	24	28	28	28	FF	DB	00	43	01	08	08	08	08	,(0$(((ÿÛ.C.....
0050h:	08	08	14	0C	0C	14	28	1C	18	1C	28	28	28	28	28	28	......(...((((((
0060h:	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	((((((((((((((((
0070h:	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	28	((((((((((((((((
0080h:	28	28	28	28	28	28	28	28	28	28	28	28	FF	C0	00	11	((((((((((((ÿÀ..
0090h:	08	00	F0	00	F0	03	01	22	00	02	11	01	03	11	01	FF	..ð.ð.."......ÿ
00A0h:	DD	00	04	00	08	FF	C4	00	1F	00	00	01	05	01	01	01	Ý....ÿÄ.....
00B0h:	01	01	01	00	00	00	00	00	00	00	00	01	02	03	04	05	.....
00C0h:	06	07	08	09	0A	0B	FF	C4	00	1F	01	00	03	01	01	01	......ÿÄ.....
00D0h:	01	01	01	01	01	01	00	00	00	00	00	00	01	02	03	04	.....
00E0h:	05	06	07	08	09	0A	0B	FF	C4	00	B5	10	00	02	01	03	.....ÿÄ.µ.....
00F0h:	03	02	04	03	05	05	04	04	00	00	01	7D	01	02	03	00	.....}....
0100h:	04	11	05	12	21	31	41	06	13	51	61	07	22	71	14	32	....!1A..Qa."q.2
0110h:	81	91	A1	08	23	42	B1	C1	15	52	D1	F0	24	33	62	72	.'¡.#B±Á.RÑð$3br
0120h:	82	09	0A	16	17	18	19	1A	25	26	27	28	29	2A	34	35	,.....%&'()*45
0130h:	36	37	38	39	3A	43	44	45	46	47	48	49	4A	53	54	55	6789:CDEFGHIJSTU
0140h:	56	57	58	59	5A	63	64	65	66	67	68	69	6A	73	74	75	VWXYZcdefghijstu
0150h:	76	77	78	79	7A	83	84	85	86	87	88	89	8A	92	93	94	vwxyzƒ„…†‡ˆ‰Š'""
0160h:	95	96	97	98	99	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	•—˜™š¢£¤¥¦§¨©ª²
0170h:	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	³´µ¶·¸¹ºÂÃÄÅÆÇÈÉ
0180h:	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	E1	E2	E3	E4	E5	E6	ÊÒÓÔÕÖ×ØÙÚáâãäåæ
0190h:	E7	E8	E9	EA	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4	çèéêñòóôõö÷øùúÿÄ
01A0h:	00	B5	11	00	02	01	02	04	04	03	04	07	05	04	04	00	.µ.....
01B0h:	01	02	77	00	01	02	03	11	04	05	21	31	06	12	41	51	..w.....!1..AQ
01C0h:	07	61	71	13	22	32	81	08	14	42	91	A1	B1	C1	09	23	.aq."2...B'¡±Á.#
01D0h:	33	52	F0	15	62	72	D1	0A	16	24	34	E1	25	F1	17	18	3Rð.brÑ..$4á%ñ..
01E0h:	19	1A	26	27	28	29	2A	35	36	37	38	39	3A	43	44	45	..&'()*56789:CDE
01F0h:	46	47	48	49	4A	53	54	55	56	57	58	59	5A	63	64	65	FGHIJSTUVWXYZcde
0200h:	66	67	68	69	6A	73	74	75	76	77	78	79	7A	82	83	84	fghijstuvwxyz,ƒ„
0210h:	85	86	87	88	89	8A	92	93	94	95	96	97	98	99	9A	A2	…†‡ˆ‰Š'"•—˜™šc
0220h:	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	B9	£¤¥¦§¨©ª²³´µ¶·¸¹
0230h:	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×
0240h:	D8	D9	DA	E2	E3	E4	E5	E6	E7	E8	E9	EA	F2	F3	F4	F5	ØÙÚâãäåæçèéêòóôõ
0250h:	F6	F7	F8	F9	FA	FF	DA	00	0C	03	01	00	02	11	03	11	ö÷øùúÿÚ.....
0260h:	00	3F	00	F2	9A	5C	F3	9A	28	C0	A2	E2	0F	7A	76	06	.?.òš\óš(À¢â.zv.
0270h:	33	48	17	BE	69	40	F5	A0	2C	28	19	EF	4B	CD	18	A3	3H.¾i@õ ,(.ïKÍ.£

Figure 3.1 IMG001A.jpg Header Hex Data

00000B60	34	B4	ED	A0	83	14	BC	D1	46	4E	28	B5	C6	21	CF	5A	4´í ƒ.¼ÑFN(µÆ!ÏZ
00000B70	28	39	A4	39	A7	60	03	D6	8A	3B	D1	45	AE	01	9A	0D	(9¤9§`.ÖŠ;ÑE®.š.
00000B80	04	D2	13	48	03	22	83	C7	7A	3F	0A	43	40	80	7A	E6	.Ò.H."ƒÇz?.C@€zæ
00000B90	83	F5	A4	EF	46	70	28	EA	1D	40	93	9A	52	73	49	9A	ƒõ¤ïFp(ê.@"šRsIš
00000BA0	4E	33	4E	C0	CF	FF	D3	F2	BA	4A	52	41	ED	49	9A	15	N3NÀÏÿÓò°JRAíIš.
00000BB0	C4	7F	FF	D9													Ä.ÿÙ

Figure 3.2 IMG001A.jpg Footer Hex Data

The data shows that the file has the correct information to indicate that this is an image file as denoted by the FF D8 at the start of the file, and the FF D9 at the end. Outside of the basic and common JPEG data, there is no other identifiable hex data to give any indication of hardware or software used. While there is little to authenticate within this file, the image file does properly open, and is consistent with a JPEG

image file. This is a known original photo, but it should be noted that when the EXIF data of the file was checked using JPEGSnoop, it was reported as an altered or processed image.

The second file from this device is the audio file labeled 010100052900.amr. This type of file is a compressed audio file optimized for storing spoken audio data and is commonly used by cell phones for that purpose [5]. The relevant hex data for this file is as follows in Figure 3.3.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	23	21	41	4D	52	0A	3C	47	01	1F	B9	80	77	A5	C0	49	#!AMR.<G..¹€w¥ÀI
00000010	80	AA	E9	E0	8D	CC	A5	8A	B8	DC	6D	E1	A3	20	93	07	€ªéà.Ì¥Š¸Ümá£ ".
00000020	82	10	25	AA	B1	E0	3C	47	01	1F	B9	80	77	A5	C0	49	,.%ª±à<G..¹€w¥ÀI
00000030	80	AA	E9	E0	8D	CC	A5	8A	B8	DC	6D	E1	A3	20	93	07	€ªéà.Ì¥Š¸Ümá£ ".
00000040	82	10	25	AA	B1	E0	3C	47	01	1F	B9	80	77	A5	C0	49	,.%ª±à<G..¹€w¥ÀI
00000050	80	AA	E9	E0	8D	CC	A5	8A	B8	DC	6D	E1	A3	20	93	07	€ªéà.Ì¥Š¸Ümá£ ".
00000060	82	10	25	AA	B1	E0	3C	F8	64	64	40	48	70	02	00	34	,.%ª±à<ødd@Hp..4

Figure 3.3 01010052900.amr Hex Data

In Figure 3.3, Offset 00000000-00000005 indicate the proper file header information to indicate that this is an amr audio file. There is no further identifying information contained within the file to denote software or hardware used in the creation of the file. As with the previous file tested, this file opens properly and shows nothing unexpected for the file type. This file was also opened with iZotope RX 6 Audio Editor to view the spectrograph of the audio data to look for obvious inconsistencies as indicated in Figure 3.4. Based on the test recording made, no inconsistencies were found.

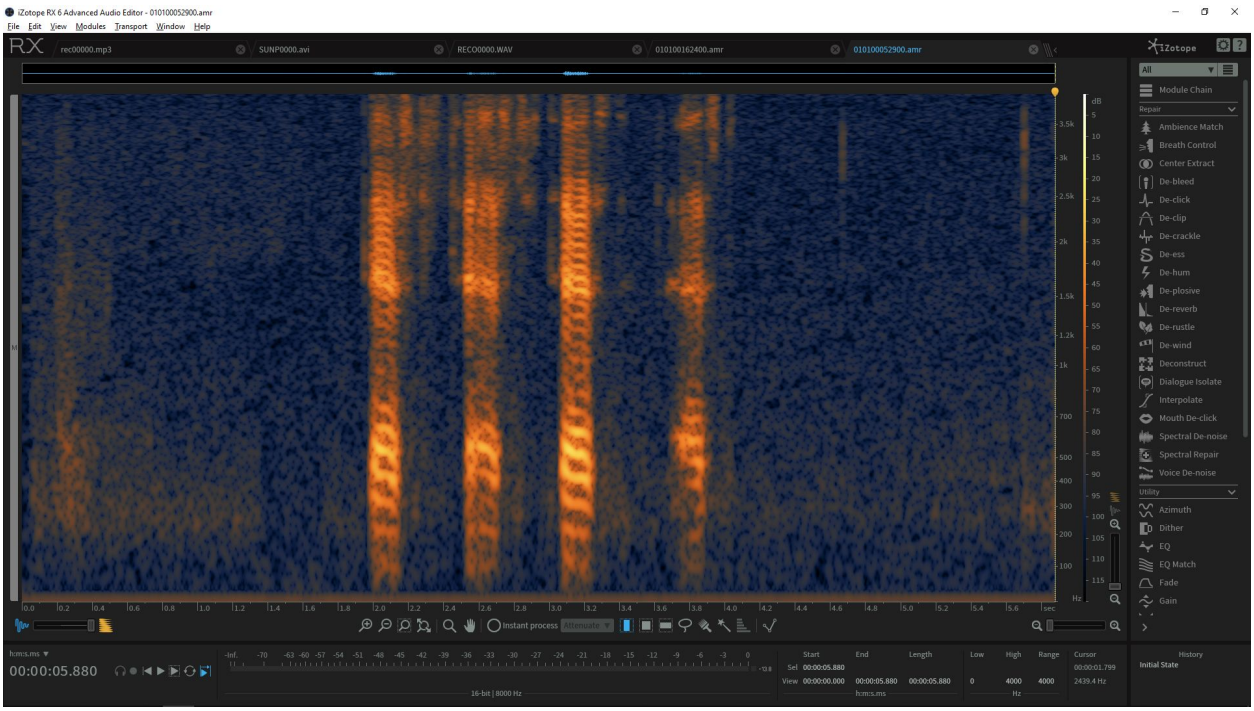


Figure 3.4 010100052900.amr Spectrograph View

The final stage of testing with this device was to attempt to connect the watch to the Samsung Galaxy S5 cell phone and attempt to send and receive information with the watch. Attempts to pair the watch as a Bluetooth device natively to the phone failed. Several third-party applications were used to attempt to sync the watch to the phone. BT Notify was found to be somewhat successful in that it could identify the watch as a device, but no text message information would share between the devices.

Analysis of Smartwatch 2

Smartwatch two contains both a camera and a microphone and can create audio and visual media. Attempts to create test media originally failed due to the need to have a memory card placed in the device for storage. Once a microSD card was placed in the device, a photo was taken, and an audio file was recorded using the built-in camera and microphone. The device was set for a date of 12/31/2016 at around 11:15 pm when these tests were conducted. The test files were retrieved using FTK Imager and the watch as an external USB drive. The files retrieved were IMG002A.jpg and 010100162400.amr.

Device Analysis

While this device was connected to the computer, a check of USB devices was made. The identifier \VID_0E8D&PID_0002\ was retrieved from the device. This is a known identifier for several USB mass storage devices. While attached, only the microSD card was accessible, no connection to the watch file structure was made.

File Analysis

The first item checked was the time stamps of the retrieved files. Both the image and audio file were seen to have time stamps consistent with the time displayed on the watch at the time of creation. The next item checked was the file information in HxD and 010 editors for their file structure information. The hex data found for IMG002A.jpg is as follows in figure 3.5 and 3.6.

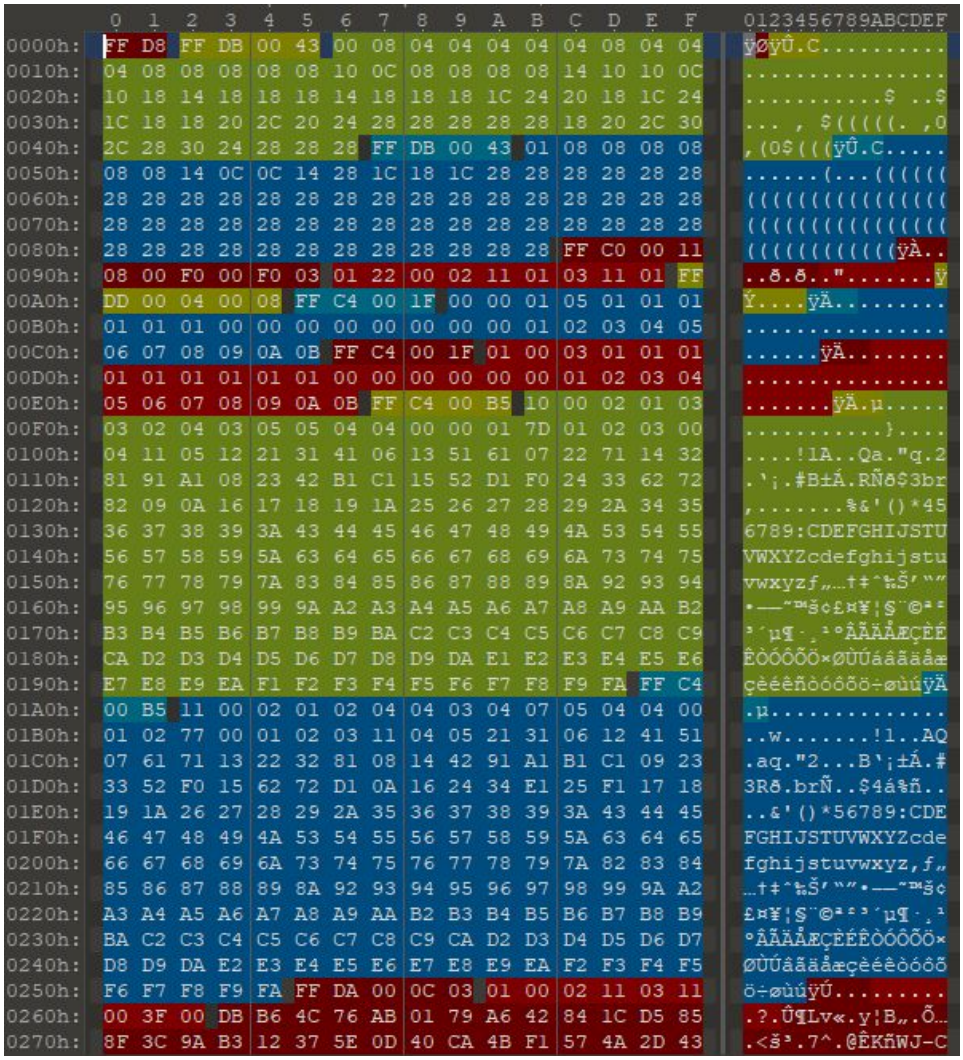


Figure 3.5 IMG002A.jpg Header Hex Data

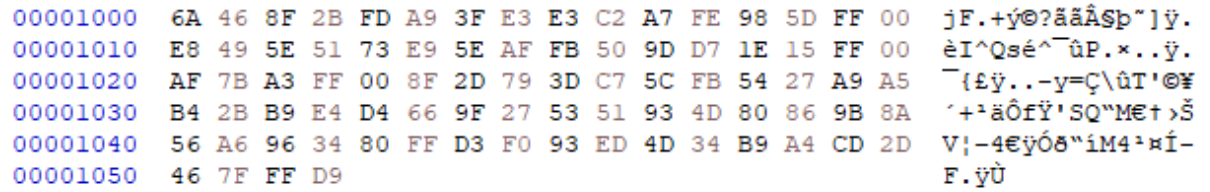


Figure 3.6 IMG002A.jpg Footer Hex Data

The data shows that the file has the correct information to indicate that this is an image file as denoted by the FF D8 at the start of the file, and the FF D9 at the end. Outside of the basic and common JPEG data, there is no other identifiable hex data to give any indication of hardware or software used. While there is little to authenticate within this file, the image file does properly open, and is consistent with a JPEG image file. This is a known original photo, but it should be noted that when the EXIF data of the file was checked using JPEGSnoop, it was reported as an altered or processed image.

The second file from this device is the audio file labeled 010100162400.amr. The relevant hex data for this file is as follows in Figure 3.7

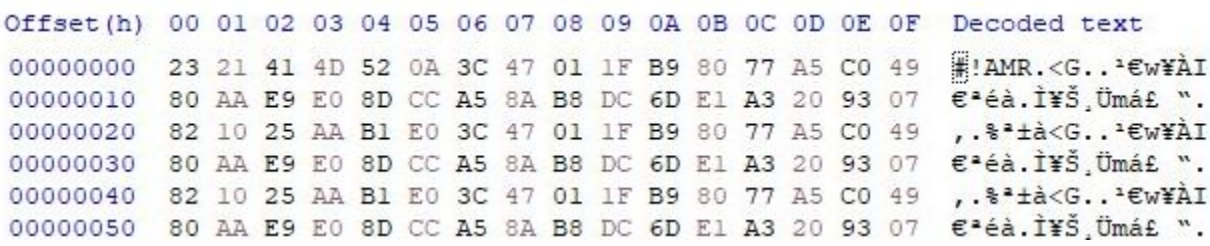


Figure 3.7 010100162400.amr Hex Data

In Figure 3.7, Offset 00000000-00000005 indicate the proper file header information to indicate that this is an amr audio file. There is no further identifying information contained within the file to denote software or hardware used in the creation of the file. As with the previous file tested, this file opens properly and shows nothing unexpected for the file type. This file was also opened with iZotope RX 6 Audio Editor to view the spectrograph of the audio data to look for obvious inconsistencies as indicated in Figure 3.8. Based on the test recording made, no inconsistencies were found.

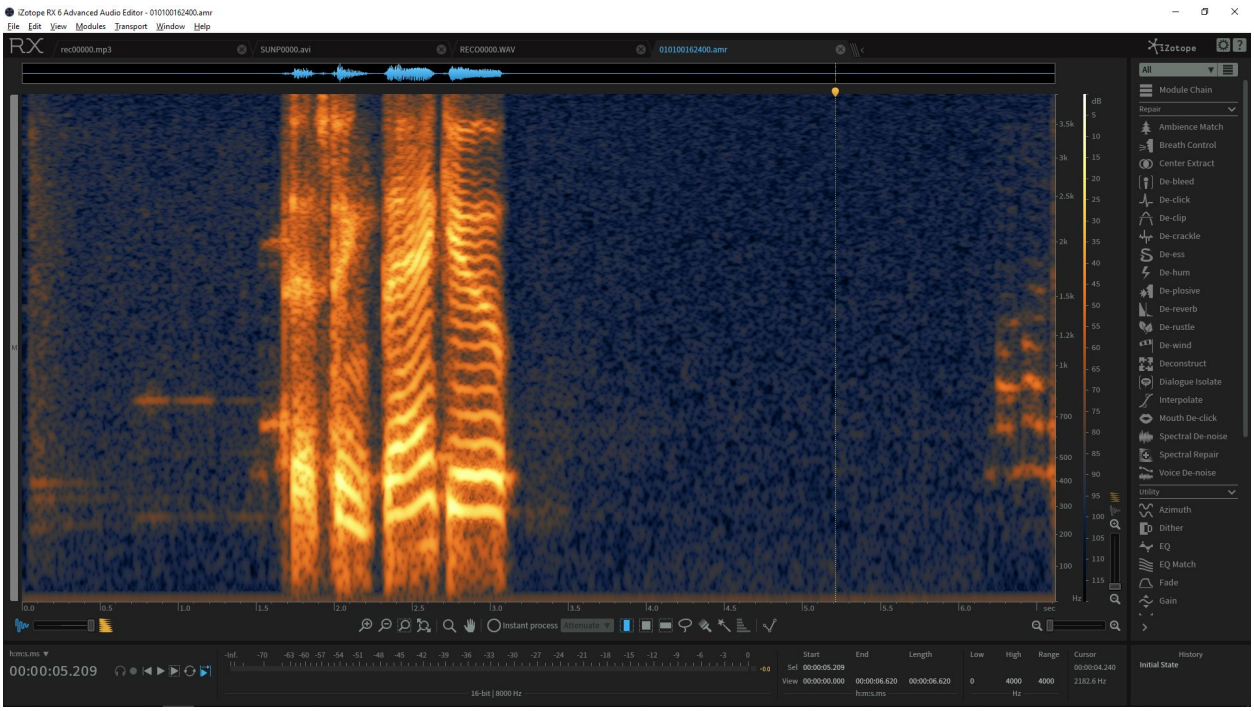


Figure 3.8 010100162400.amr Spectrograph View

The final stage of testing with this device was to attempt to connect the watch to the Samsung Galaxy S5 cell phone and attempt to send and receive information with the watch. Due to the limited success with Smartwatch One, BT Notify was used to sync this watch with the Galaxy S5 phone. In this case, the watch was able to communicate with the phone and send and receive text messages. It is unknown if the data was stored anywhere on the watch, as no connection to the operating system file was able to be made, the Cellebrite acquisition was able to see the text message as shown in Figure 3.9.

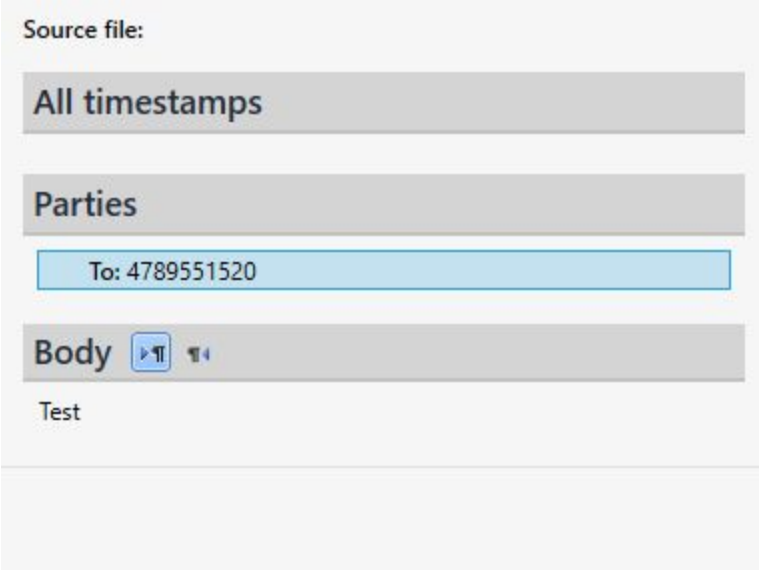


Figure 3.9 Cellebrite Message From Smartwatch 2

Further searching into the data recovered by Cellebrite did show that the various syncing apps used for unbranded smartwatches was installed on the phone as seen in figure 3.10. While the apps did connect to the BT Notifier application, there did not appear to be a log in the Bluetooth database on the phone for the connection to the phone.

Figure 3.10 Cellebrite Bluetooth Application Installation

Analysis of USB Voice Recorder

The USB Voice recorder contains a microphone and an internal battery that is charged via USB port directly. Two test audio files were recorded with the device, rec00000.mp3 and rec00001.mp3, with the first file being used for analysis.

Device Analysis

While this device was connected to the computer, a check of USB devices was made. The identifier \ VID_E0B6&PID_081\ was retrieved from the device. This is a known identifier for several USB human interface devices and is consistent with a generic USB microphone. The device model is listed as AC309N with no brand. A search for this model number returns several USB voice recorders of various styles and no specific manufacturer. There also appears to be no way to set a date and time for this device.

File Analysis

The first item checked was the timestamp of the retrieved file. The file was seen to have a date stamp of 1/1/1601 with no time. Since there is no timestamp, the first date of the Gregorian Calendar appears to be attached to files created with this device [6]. The next item checked was the file information in HxD hex editor for file structure information. The hex data found for rec00000.mp3 is as follows in figure 3.11.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	FF	FD	88	04	33	33	33	55	55	44	44	44	33	33	33	6D	ÿý^.333UUDDD333m
00000010	24	89	24	90	00	00	00	00	00	00	00	00	00	00	00	00	$‰$..............
00000020	00	00	00	C3	0C	30	C3	29	EA	4A	7A	93	26	9C	C9	A7	...Ã.0Ã)êJz"&œÉ§
00000030	3E	39	CF	8E	73	A8	9C	EA	27	4A	6A	92	9A	A4	26	9D	>9ÏŽs¨œê'Jj'š¤&.
00000040	09	A7	4E	59	53	96	54	65	95	19	65	52	89	94	A2	64	.§NYS–Te•.eR‰"¢d
00000050	66	A1	19	A8	52	89	94	A2	64	A7	A5	29	E9	56	7A	D5	f¡.¨R‰"¢d§¥)éVzÕ
00000060	9E	B4	A8	A5	2A	29	5A	69	96	9A	64	E6	A1	39	A8	77	ž´¨¥*)Zi–šdæ¡9¨w
00000070	77	77	77	77	77	77	77	77	77	77	77	77	77	77	5B	16	wwwwwwwwwwwwwwww[

Figure 3.11 rec00000.mp3 Header Information

The file header does not conform to standard mp3 file containers, and when it was opened with common audio player software, it was unable to play. However, when the file was opened with iZotope, the audio information was available as seen in figure 3.12.

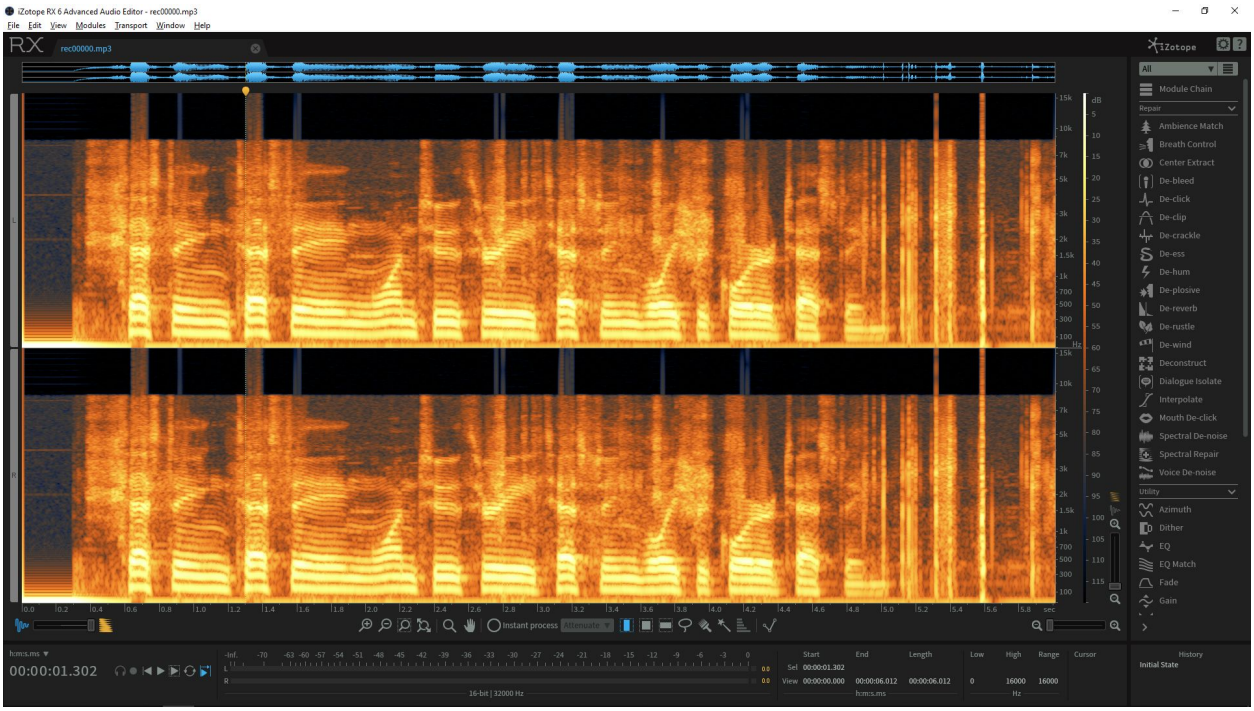


Figure 3.12 Spectrograph of rec00000.mp3

The audio file was successfully played from iZotope and was able to be exported as a different file type that could be used with common audio player software.

Analysis of Stand-Alone Audio Recorder

The stand-alone audio recorder contains 8 gigabytes of internal storage, stereo microphones, and is powered by an internal, USB port rechargeable battery. This device also has external controls for recording and playback on a built-in speaker. A test audio file named REC001.wav was created with this device.

Device Analysis

While this device was connected to the computer, a check of USB devices was made. The identifier \ VID_E0B6&PID_081\ was retrieved from the device. This is a known identifier for several mp3/mp4 recorders and players made by Actions Semiconductor Co., Ltd. It is unknown if this device

was manufactured by this company or if the technology was cloned. The date and time of this device was not set to current time due to virus concerns that are mentioned in the device documentation. The default date of December 31, 2015 was left in place for testing.

File Analysis

The first item checked was the timestamp. The file was consistent with the device time of December 31st, 2015 at 11:00 pm. The next item checked was the file header and is shown in figure 3.13 below.

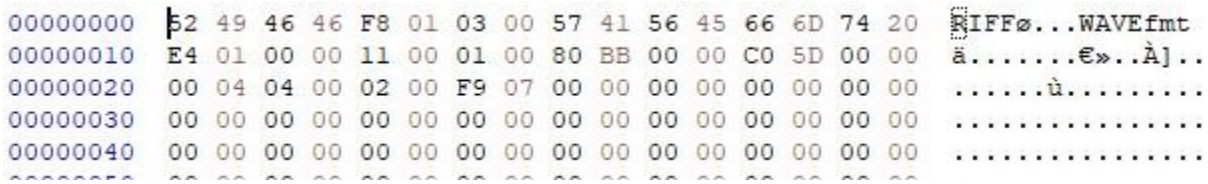


Figure 3.13 REC001.wav Header Hex Data

As shown, the header information identifies this file as a .wav file. This file did playback properly on the device itself, but once the file was transferred to a desktop computer, no common audio programs would play the file, citing corrupt file errors. An attempt to open the file with iZotope also failed. A final attempt to open the file in VLC Media Player did allow the file to be played. VLC Media player was then used to export the audio file in a lossless compression .flac format. The exported file was able to be opened in iZotope as seen in figure 3.14.

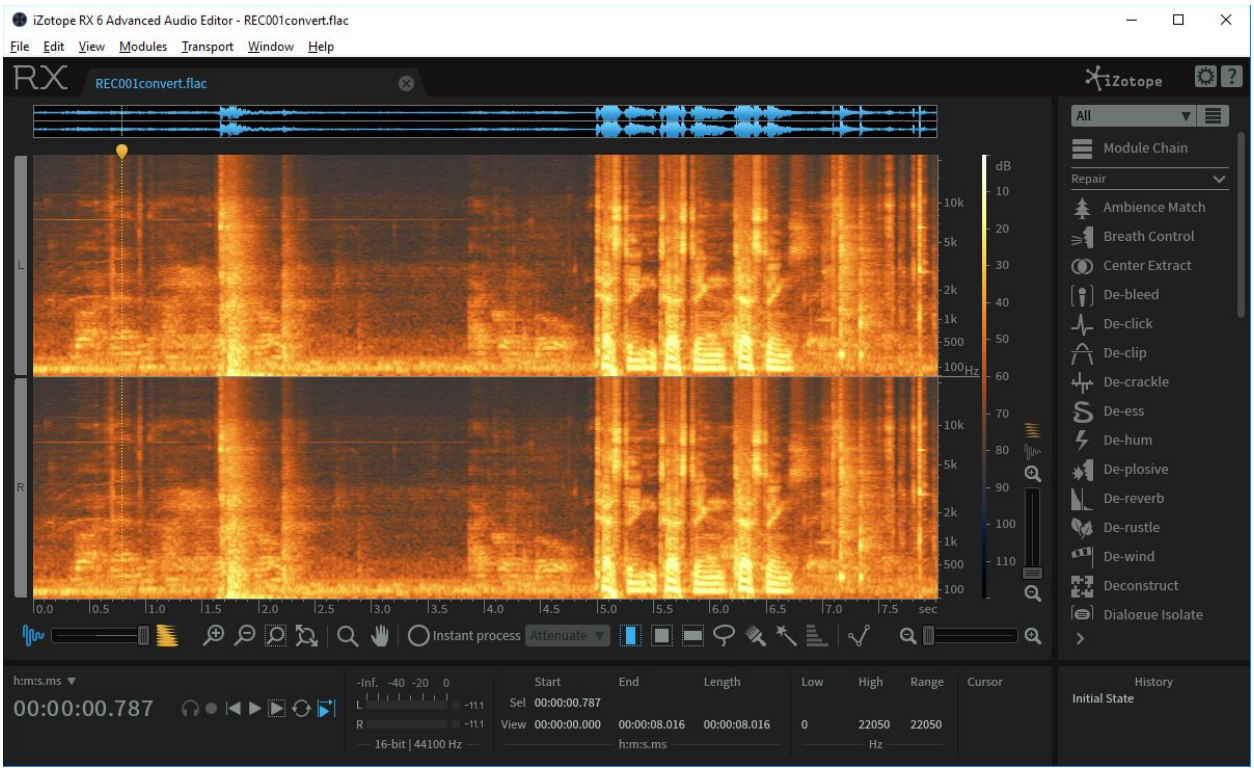


Figure 3.14 REC001.wav Spectrograph After Format Conversion

Analysis of Lighter Camera

This camera is designed to be a hidden camera that resembles a cigarette lighter. It contains a pinhole camera and microphone and is powered by an internal USB port rechargeable battery. This device has an external button to start recording. Several test files were made, but only the files labeled SUNP0000.avi and pict0000.jpg were used for analysis.

Device Analysis

While this device was connected to the computer, a check of USB devices was made. The identifier \ VID_1B3F&PID_0C52\ was retrieved from the device. This is a known identifier for cameras manufactured by Generalplus Technology Inc. It is unknown if this device was manufactured by this company or if the technology was cloned as there are no identifying labels on the device itself. The date and time of this device is set based on a text file on the root of the microSD card named tag.txt. The default date of May 1st, 2016 was left in place for testing.

File Analysis

The first items checked were the timestamps. The device has initially been charged to full power 22 days before the tests were conducted. The internal clock, when the device had power, did keep time from the initial date and time stamp mentioned previously. Given this information, the date and time of the test files of May 23rd, 2016 at 9:24 am was consistent with the device time. The next item checked was the file information in HxD and 010 hex editors for the file structure information. The hex data found for pict0000.jpg is as follows in figure 3.15 and 3.16.

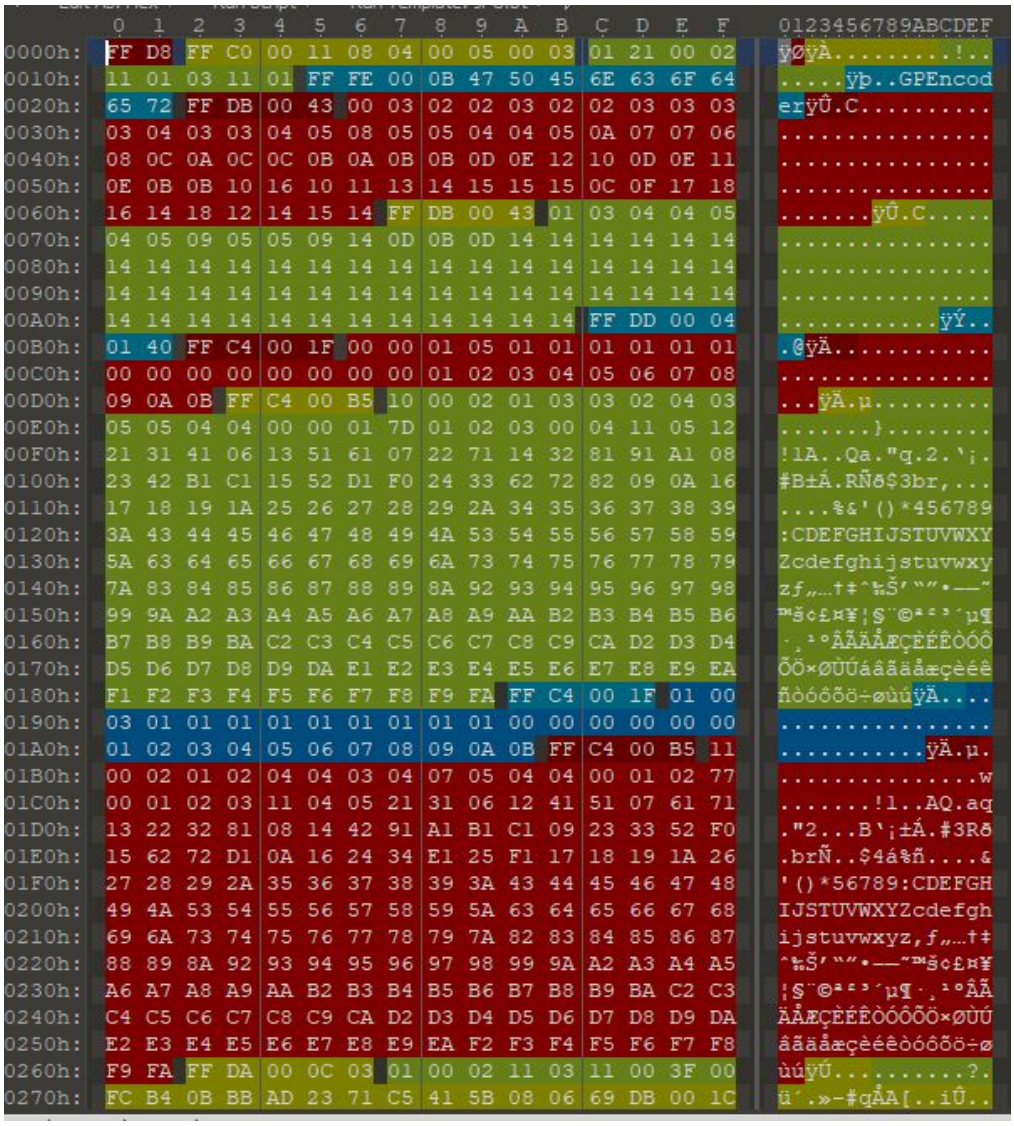
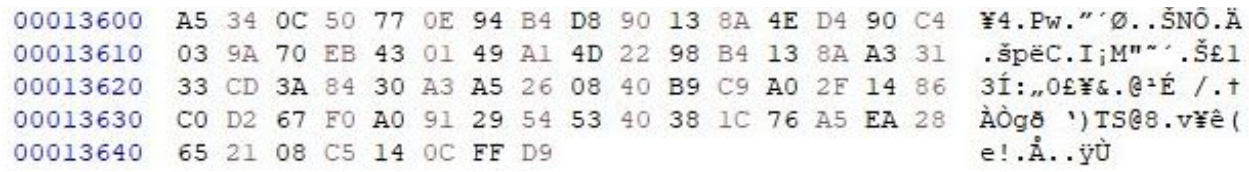


Figure 3.15 pict0000.jpg Header Hex Data

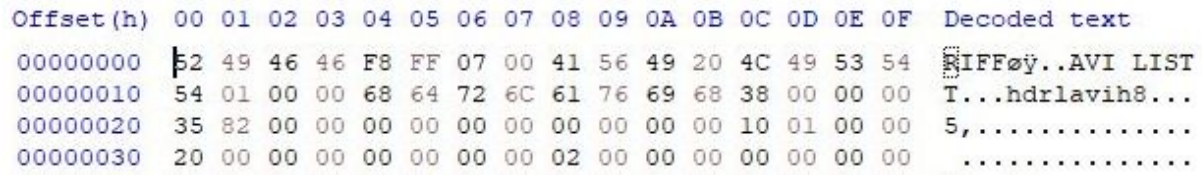


00013600	A5	34	0C	50	77	0E	94	B4	D8	90	13	8A	4E	D4	90	C4	¥4.Pw.”´Ø..ŠNÔ.Ä
00013610	03	9A	70	EB	43	01	49	A1	4D	22	98	B4	13	8A	A3	31	.špëC.I¡M"˜´.Š£1
00013620	33	CD	3A	84	30	A3	A5	26	08	40	B9	C9	A0	2F	14	86	3Í:„0£¥&.@¹É /.†
00013630	C0	D2	67	F0	A0	91	29	54	53	40	38	1C	76	A5	EA	28	ÀÒgð ‘)TS@8.v¥ê(
00013640	65	21	08	C5	14	0C	FF	D9									e!.Å..ÿÙ

Figure 3.16 pict0000.jpg Footer Hex Data

The data shows that the file has the correct information to indicate that this is an image file as denoted by the FF D8 at the start of the file, and the FF D9 at the end. A search was conducted for GPEncoder since it is displayed in the file information, but no information was found. Even though no information was found, it is likely that GPEncoder stands for General Plus Encoder based on the manufacturer of the device. There is no other identifiable hex data to give any indication of hardware or software used. While there is little to authenticate within this file, the image file does properly open, and is consistent with a JPEG image file. This is a known original photo, but it should be noted that when the EXIF data of the file was checked using JPEGSnoop, it was reported as an altered or processed image.

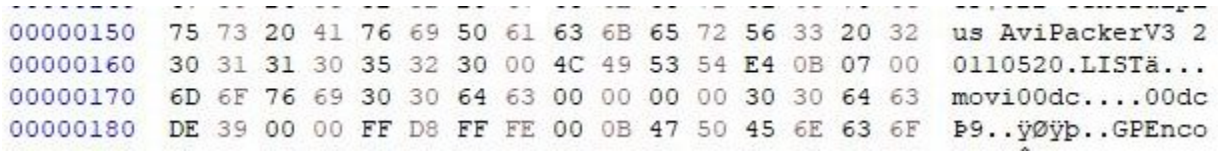
The second file from this device is the video file labeled SUNP0000.avi. The relevant hex data for this file is as follows in Figure 3.17



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	52	49	46	46	F8	FF	07	00	41	56	49	20	4C	49	53	54	RIFFøÿ..AVI LIST
00000010	54	01	00	00	68	64	72	6C	61	76	69	68	38	00	00	00	T...hdrlavih8...
00000020	35	82	00	00	00	00	00	00	00	00	00	00	10	01	00	00	5,..............
00000030	20	00	00	00	00	00	00	00	02	00	00	00	00	00	00	00	.....

Figure 3.17 SUNP0000.avi Header Hex Data

In Figure 3.17, the hex data indicates the proper file header information to indicate the video file information. Further information about the video file can be seen later in the hex data as shown in Figure 3.18 below. The rest of the file structure was consistent with a motion JPEG video.



00000150	75	73	20	41	76	69	50	61	63	6B	65	72	56	33	20	32	us AviPackerV3 2
00000160	30	31	31	30	35	32	30	00	4C	49	53	54	E4	0B	07	00	0110520.LISTä...
00000170	6D	6F	76	69	30	30	64	63	00	00	00	00	30	30	64	63	movi00dc....00dc
00000180	DE	39	00	00	FF	D8	FF	FE	00	0B	47	50	45	6E	63	6F	Þ9..ÿØÿþ..GPEnco

Figure 3.18 SUNP000.avi AviPacker Hex Data

As with the previous file tested, this file opens properly and is consistent with the file type. The item shown in Figure 3.18 labeled AviPackerV3 was found to be the General Plus video encoder and is available as an open source download. One flaw with the video was due to the camera itself. The camera lens was blocked and recorded only black frames, but it also recorded audio. This file was also opened with iZotope RX 6 Audio Editor to view the spectrograph of the audio data to look for obvious inconsistencies as indicated in Figure 3.19. Based on the test recording made, no inconsistencies in the audio were found.

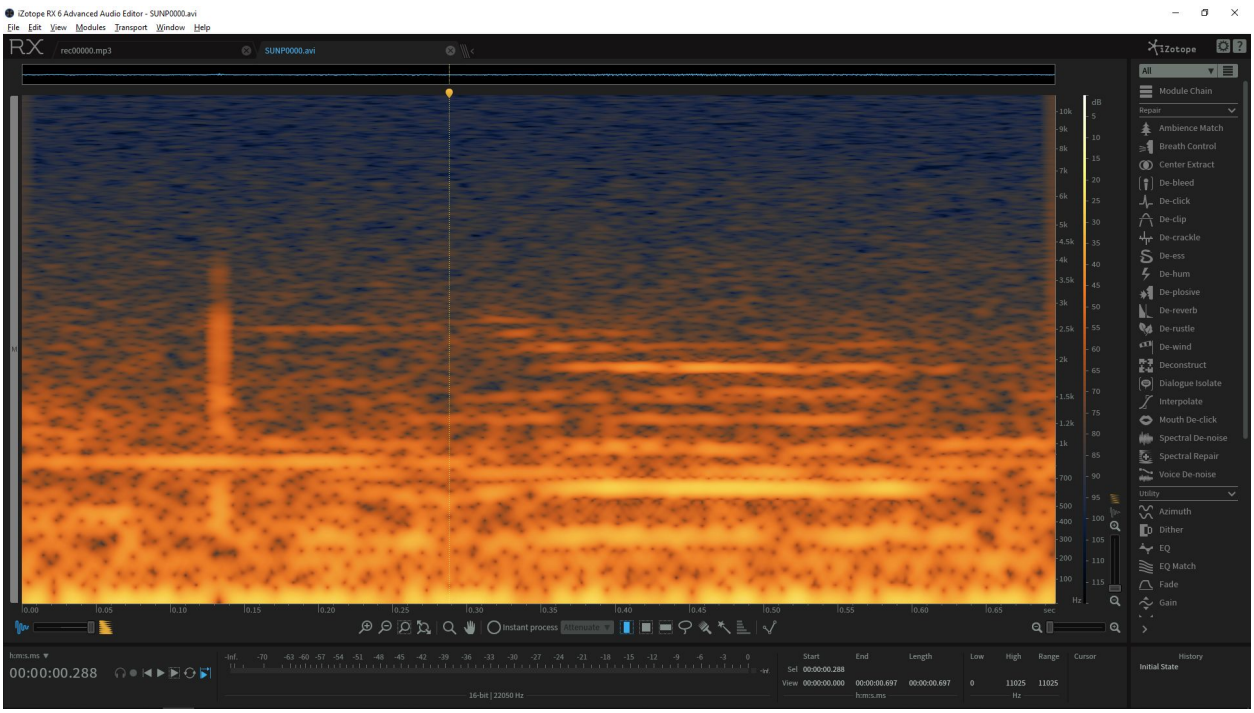


Figure 3.19 SUNP0000.avi Spectrograph View

Analysis of Pen Camera

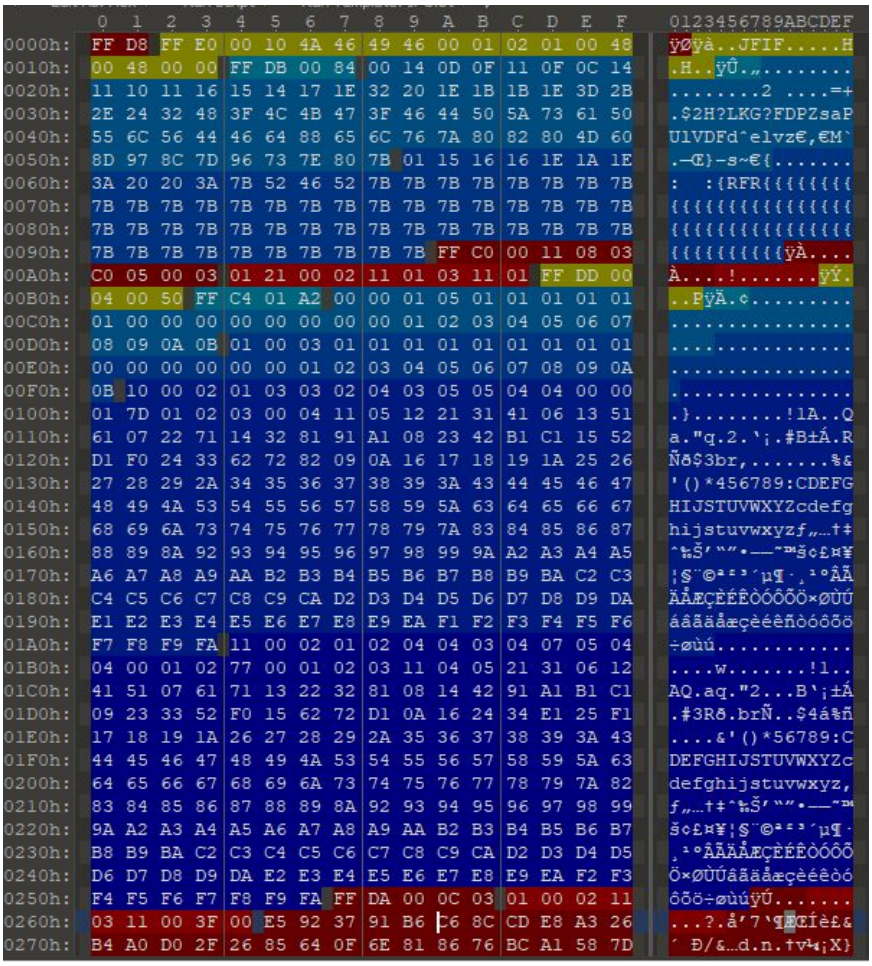
The final device tested in this study was a hidden camera built in to a writing pen.. It contains a pinhole camera and microphone and is powered by an internal USB port rechargeable battery. This device has an external button to start recording. All attempts to record video with the device failed, but image file PICT000.jpg and audio file RECO0000.wav were created.

Device Analysis

While this device was connected to the computer, a check of USB devices was made. The identifier \ VID_046D&PID_C537\ was retrieved from the device. The vendor id for this device is identified as being from Logitech, but the device id did not return results. There is no data to support that this device was manufactured by Logitech. The date and time of this device is set based on a text file on the root of the microSD card named time.txt. The default date of March 8, 2017 was left in place for testing.

File Analysis

The first items checked were timestamps. The device has initially been charged to full power 3 days before the tests were conducted. The date and time stamp of both files was February 8th, 2015. This would indicate that the date and time stamps of this device are not valid. The next item checked was the file information in HxD and 010 hex editors for their file structure information. The hex data found for pict0000.jpg is as follows in figure 3.20 and 3.21.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	02	01	00	48	ÿØÿà..JFIF.....H
0010h:	00	48	00	00	FF	DB	00	84	00	14	0D	0F	11	0F	0C	14	.H..ÿÛ.„.....
0020h:	11	10	11	16	15	14	17	1E	32	20	1E	1B	1B	1E	3D	2B	........2 ....=+
0030h:	2E	24	32	48	3F	4C	4B	47	3F	46	44	50	5A	73	61	50	.$2H?LKG?FDPZsaP
0040h:	55	6C	56	44	46	64	88	65	6C	76	7A	80	82	80	4D	60	UlVDFdˆelvz€‚€M`
0050h:	8D	97	8C	7D	96	73	7E	80	7B	01	15	16	16	1E	1A	1E	.—Œ}–s~€{.....
0060h:	3A	20	20	3A	7B	52	46	52	7B	7B	7B	7B	7B	7B	7B	7B	: :{RFR{{{{{{{
0070h:	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	{{{{{{{{{{{{{{{
0080h:	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	{{{{{{{{{{{{{{{
0090h:	7B	7B	7B	7B	7B	7B	7B	7B	7B	7B	FF	C0	00	11	08	03	{{{{{{{{{{ÿÀ....
00A0h:	C0	05	00	03	01	21	00	02	11	01	03	11	01	FF	DD	00	À....!.....ÿÝ.
00B0h:	04	00	50	FF	C4	01	A2	00	00	01	05	01	01	01	01	01	..PÿÄ.¢.....
00C0h:	01	00	00	00	00	00	00	00	00	01	02	03	04	05	06	07	.....
00D0h:	08	09	0A	0B	01	00	03	01	01	01	01	01	01	01	01	01	.....
00E0h:	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	0A	.....
00F0h:	0B	10	00	02	01	03	03	02	04	03	05	05	04	04	00	00	.....
0100h:	01	7D	01	02	03	00	04	11	05	12	21	31	41	06	13	51	.}.....!1A..Q
0110h:	61	07	22	71	14	32	81	91	A1	08	23	42	B1	C1	15	52	a."q.2.‘¡.#B±Á.R
0120h:	D1	F0	24	33	62	72	82	09	0A	16	17	18	19	1A	25	26	Ñð$3br,.....%&
0130h:	27	28	29	2A	34	35	36	37	38	39	3A	43	44	45	46	47	'()*456789:CDEFG
0140h:	48	49	4A	53	54	55	56	57	58	59	5A	63	64	65	66	67	HIJSTUVWXYZcdefg
0150h:	68	69	6A	73	74	75	76	77	78	79	7A	83	84	85	86	87	hijstuvwxyzƒ„…†‡
0160h:	88	89	8A	92	93	94	95	96	97	98	99	9A	A2	A3	A4	A5	ˆ‰Š’“”•–—™š¢£¤¥
0170h:	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	B8	B9	BA	C2	C3	¦§¨©ª²³´µ¶·¸¹ºÂÃ
0180h:	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	D6	D7	D8	D9	DA	ÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚ
0190h:	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	F1	F2	F3	F4	F5	F6	áâãäåæçèéêñòóôõö
01A0h:	F7	F8	F9	FA	11	00	02	01	02	04	04	03	04	07	05	04	÷øùú.....
01B0h:	04	00	01	02	77	00	01	02	03	11	04	05	21	31	06	12	....w.....!1..
01C0h:	41	51	07	61	71	13	22	32	81	08	14	42	91	A1	B1	C1	AQ.aq."2...B‘¡±Á
01D0h:	09	23	33	52	F0	15	62	72	D1	0A	16	24	34	E1	25	F1	.#3Rð.brÑ..$4á%ñ
01E0h:	17	18	19	1A	26	27	28	29	2A	35	36	37	38	39	3A	43	....&'()*56789:C
01F0h:	44	45	46	47	48	49	4A	53	54	55	56	57	58	59	5A	63	DEFGHIJSTUVWXYZc
0200h:	64	65	66	67	68	69	6A	73	74	75	76	77	78	79	7A	82	defghijstuvwxyz,
0210h:	83	84	85	86	87	88	89	8A	92	93	94	95	96	97	98	99	ƒ„…†‡ˆ‰Š’“”•–—™
0220h:	9A	A2	A3	A4	A5	A6	A7	A8	A9	AA	B2	B3	B4	B5	B6	B7	š¢£¤¥¦§¨©ª²³´µ¶·
0230h:	B8	B9	BA	C2	C3	C4	C5	C6	C7	C8	C9	CA	D2	D3	D4	D5	¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕ
0240h:	D6	D7	D8	D9	DA	E2	E3	E4	E5	E6	E7	E8	E9	EA	F2	F3	Ö×ØÙÚâãäåæçèéêòó
0250h:	F4	F5	F6	F7	F8	F9	FA	FF	DA	00	0C	03	01	00	02	11	ôõö÷øùúÿÚ.....
0260h:	03	11	00	3F	00	E5	92	37	91	B6	C6	8C	CD	E8	A3	26	...?.å’7‘¶ÆŒÍè£&
0270h:	B4	A0	D0	2F	26	85	64	0F	6E	81	86	76	BC	A1	58	7D	´ Ð/&…d.n.†v¼¡X}

Figure 3.20 PICT0000.jpg Header Hex Data

000083B0	14	5C	96	19	A3	34	0E	E1	49	4C	02	8A	04	14	52	00	.\–.£4.áIL.S..R.
000083C0	A0	D3	00	A2	80	41	45	02	0A	28	00	A4	A4	01	45	00	Ó.¢€AE..(.¤¤.E.
000083D0	14	53	04	14	50	30	A2	98	90	52	50	26	14	B4	0C	4A	.S..P0¢˜.RP&.´.J
000083E0	29	00	B4	94	08	28	A0	02	8A	00	28	A0	02	8A	00	28	).´”.(.Š.(.Š.(
000083F0	A0	02	8A	00	28	A0	61	4B	40	05	14	08	28	A0	61	4B	.Š.(aK@...(aK

Figure 3.21 PICT0000.jpg Footer Hex Data

The data shows that the file has the correct information to indicate that this is an image file as denoted by the FF D8 at the start of the file, and the FF D9 at the end. Outside of the basic and common JPEG data, there is no other identifiable hex data to give any indication of hardware or software used. While there is little to authenticate within this file, the image file does properly open, and is consistent with a JPEG image file. This is a known original photo, but it should be noted that when the EXIF data of the file was checked using JPEGSnoop, it was reported as an altered or processed image.

The second file from this device is the video file labeled RECO0000.wav. The relevant hex data for this file is as follows in Figure 3.22

```
00000000  52 49 46 46 30 D4 01 00 57 41 56 45 66 6D 74 20  RIFF0Ô..WAVEfmt
00000010  10 00 00 00 01 00 01 00 40 1F 00 00 80 3E 00 00  ........@...€>..
00000020  02 00 10 00 66 61 63 74 04 00 00 00 00 BE 00 00  ....fact.....¾..
00000030  64 61 74 61 00 D4 01 00 51 00 3D 00 F3 FF B7 FF  data.Ô..Q.=.óÿ·ÿ
00000040  C5 FF 06 00 2D 00 34 00 21 00 F3 FF C6 FF C3 FF  Åÿ..-.4.!.óÿÆÿÃÿ
```

Figure 3.22 RECO0000.wav Header Hex Data

In Figure 3.22, the hex data indicates the proper file header information to indicate the audio file information. There is no further identifying information in the hex data of the file. As with the previous file tested, this file opens properly and is consistent with the file type. This file was also opened with iZotope RX 6 Audio Editor to view the spectrograph of the audio data to look for obvious inconsistencies as indicated in Figure 3.23. Based on the test recording made, no inconsistencies in the audio were found.

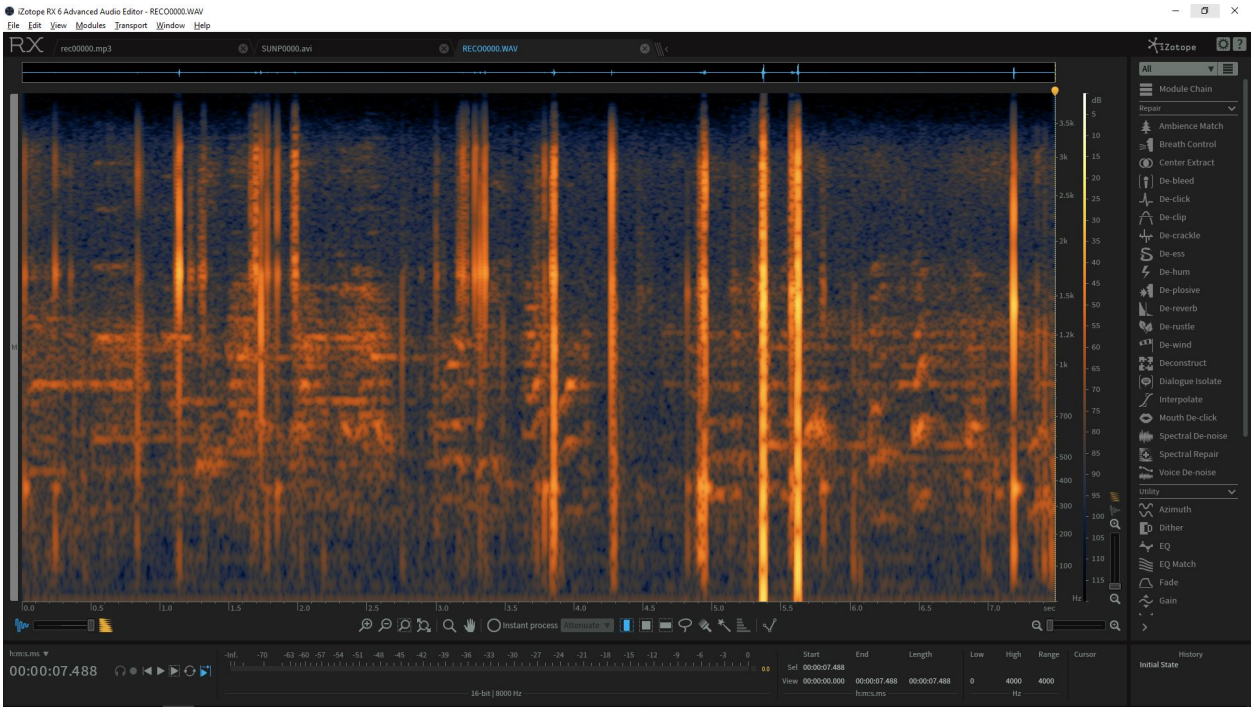


Figure 3.23 RECO0000.wav Spectrograph View

Overall Results

Smartwatches

Both smartwatches tested were of similar style and functionality. During testing it was also noted that the operating system of both watches, while looking different visually, had almost identical controls. When coupled with the similar file structures and naming conventions seen when saving files, it is fair to say that the same base programming might well be operating both devices.

During the initial stages of this study, it was planned to retrieve data from the file system of the smartwatch operating system, but based on the limited data available, no instructions were available to discover a process to accomplish this. A secondary attempt to retrieve the data was made using Cellebrite mobile phone forensic acquisition software. The basis for this attempt is that the watches are also functioning cell phones as stand-alone devices. Various settings within Cellebrite were tried for all generic devices, but no attempts to connect in this manner were successful.

The final attempt to obtain possible evidence from the watches was made by paring them with a cell phone that had been set up as a new device. Once paired, attempts were made to send and receive data through the Bluetooth connection in the form of text messages, and anything else available once the devices were paired. As discussed previously, there was limited success in pairing the watches to the phone, and what success there was depended heavily on third party applications that did not seem to store much data of value on the phone itself.

Audio Recorders

The two audio recorders that were used for this study were the same in that they both are audio recording devices, but both have significantly different operating parameters. The USB audio recorder was designed to be a covert recording device made to look like a USB Flash drive with no accessible internal operating system. In contrast, the stand-alone recorder is a device that can be powered on and controlled by various buttons available for recording and playback on the device itself. Regardless of the different purpose each device was designed for, they both successfully recorded audio data.

There were problems found with both devices with their ability to record the date and time to the files that they created. The USB recorder had no mechanism in place for notating the time on any file that it creates, defaulting instead to the first day of the Gregorian Calendar. The problem with the stand-alone recorder was more volatile. When reading the instructions for setting the time and date, it was stated to use the SetTimeTool.zip file that was included on the recorder. It was further advised, in the instructions, that this program might cause a threat to be found by virus detection software and that the user should disregard that warning. Because this device has an unknown manufacturer, this was deemed an unnecessary risk during the testing process. While the time was not updated for that reason, the timestamp placed on the created file was true to the time the device was set for.

Both audio devices did successfully audio data, but it was data that could have easily been overlooked due to encoding errors on the created files. In both cases, trying to play the files in native audio player programs failed. The file created by the USB audio recorder was able to be opened in iZotope, and the data exported to a different format. The file created by the stand-alone audio player was able to play on the device, but did not work on native players in Windows, and could not be opened in iZotope. The final attempt to play the file in VLC media player was successful and did allow for the audio data to be exported in a different format that was then playable in all programs. It is likely that this was successful due to the fact VLC Media Player is based on software that can play most media based on the media data in the file rather than the file container it is in.

Audio/Video Devices

In the case of the audio/video devices tested, both were designed to be covert recording devices. The first is designed to look like a cigarette lighter and the second as a writing pen. On both devices the cameras and microphones were operational, though the design of the lighter caused the lens to be blocked. While this problem did cause the video taken to be black frames, it did record a usable video file of what was in the camera's line of sight. The audio data from the lighter was unaffected by the blocked lens. Due to a lack of included instructions, it was difficult to properly operate the pen camera, and a video was not

created. Audio and photographic data was able to be created with the pen camera. The files created with both devices were able to be used in native programs with no issues arising.

USB Identifiers

The program USBDeview was used to check the information from each device to attempt to identify the manufacturer of each device. As noted previously, the only device that had what appears to be valid identification information is the lighter camera. The id information VID_1B3F&PID_0C52 is known to be used by Generalplus Technology Inc. for cameras that it manufactures, and a search of this company shows that they have created several pinhole cameras for a variety of devices in the past. All other devices either show as generic storage devices or have id codes that result in multiple possible devices.

Hex Data

Aside from the files created by the lighter, all files displayed what appeared to be appropriate file information for the data contained but had no further identification data for the devices that created them. In the case of the lighter, there were other markers that can be traced back to Generalplus Technology Inc. It should also be noted, as discussed previously, the audio files created by both audio recorders would not play natively until converted to a different file format. Given that the file headers indicated that the files were in a .wav format, they may not be correct due to the problems encountered during the testing.

CHAPTER IV

CONCLUSIONS

The basic question of this study is can we rely media files from unbranded technology as evidence? Overall the answer is yes, we can, but we must also be cautious when doing so. One problem that is encountered with these devices is that authenticating them is problematic as there is little to no identifying data encoded into most of the files. Even so, we can use many other techniques to validate that the files are original and unaltered in the same way that we would with any media file that we encounter. One advantage to these devices is that, for the most part, they use microSD storage for all recording activities. Because of this, it would be forensically sound to place a wiped microSD card in the suspect device to create test files for comparison if that device is available.

Another area of concern is possibly missing data that is contained in some files created. Because there is little documentation for many of these devices, their operation and file creation may not be consistent with other, better known devices. When attempting to use files created by these devices, a forensic analyst does need to look further into the data contained in files that cause errors when attempting to open them.

One last determining factor in verifying data from these devices is the totality of the circumstances in which the data was created. Many known devices have incorrect time stamps when the data is collected, and several known brands record data with no identifying information within the files. If the data comes from a reliable source it does not become invalid, it simply means all of the available information needs to be taken into account when deciding if the evidence is reliable.

Future Research

The reality of many of these devices is they are like any number of inexpensive technologies that are available in almost every aspect of life. Attempting to catalogue every unbranded device on the market would be a monumental, if not impossible, task. What could be of use would be further research into a simple, possibly universal way to access the data stored on the variety of unbranded smartwatches that are on the market. Many of them seem to work on similar operating software, but the instructions on

accessing and modifying the data on these watches are limited, and in the case of this study, completely inaccurate. There are several Russian based companies that offer programs that are advertised as allowing the user to access and change the data on these types of smartwatches, but no information on how this access is obtained was available. More in depth study on these watches and the software that can access the data may shed more light on the data that can be retrieved.

REFERENCES

[1] M. Pecht and S. Tiku, "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics," in IEEE Spectrum, vol. 43, no. 5, pp. 37-46, May 2006. doi: 10.1109/MSPEC.2006.1628506

[2] YAO, Vincent W.. An Economic Analysis of Counterfeit Goods: the Case of China. Journal of the Washington Institute of China Studies, [S.l.], v. 1, n. 1, p. 116, mar. 2014. ISSN 2373-0005. Available at: <https://www.bpastudies.org/bpastudies/article/view/15/35>. Date accessed: 12 Apr. 2019.

[3] Staff. (2011, May 27). Analysis: Counterfeit consumer electronics and brand authentication systems. Retrieved from https://www.electronicsweekly.com/news/business/distribution/analysis-counterfeit-consumer-electronics-and-brand-authentication-systems-2011-05/

[4] Unbranded | Definition in the Cambridge English Dictionary https://dictionary.cambridge.org/us/dictionary/english/unbranded

[5] Adaptive Multi-Rate Codec File. (n.d.). Retrieved from https://fileinfo.com/extension/amr

[6] Archiveddocs. (n.d.). FILETIME. Retrieved from https://docs.microsoft.com/en-us/previous-versions/aa915351(v=msdn.10)

[7] Thomas, A. (n.d.). How to Hack Chinese (Watch) Phone Firmware. Retrieved from https://www.dr-lex.be/hardware/china_phone_flashing.html

APPENDIX A

MEDIAINFO DETAILS FOR ALL FILES

SMART WATCH 1	
General	
Complete name	I:\Audio\010100052900.amr
Format	AMR
Format/Info	Adaptive Multi-Rate
File size	9.22 KiB
Duration	5 s 900 ms
Overall bit rate mode	Constant
Overall bit rate	12.8 kb/s
Audio	
Format	AMR
Format/Info	Adaptive Multi-Rate
Format profile	Narrow band
Duration	5 s 900 ms
Bit rate mode	Constant
Bit rate	12.8 kb/s
Channel(s)	1 channel
Sampling rate	8 000 Hz
Bit depth	13 bits
Stream size	9.22 KiB (100%)
Created Time 12/31/2016 11:05 PM (Consistant with Device Time)	
General	
Complete name	I:\Photos\IMG0001A.jpg
Format	JPEG
File size	2.93 KiB
Image	
Format	JPEG
Width	240 pixels
Height	240 pixels
Color space	YUV
Chroma subsampling	0.168055556
Bit depth	8 bits

Compression mode	Lossy
Stream size	2.93 KiB (100%)
Created Time 12/31/2016 11:03 PM (Consistant with Device Time)	
SMARTWATCH 2	
General	
Complete name	I:\Audio\010100162400.amr
Format	AMR
Format/Info	Adaptive Multi-Rate
File size	10.4 KiB
Duration	6 s 640 ms
Overall bit rate mode	Constant
Overall bit rate	12.8 kb/s
Audio	
Format	AMR
Format/Info	Adaptive Multi-Rate
Format profile	Narrow band
Duration	6 s 640 ms
Bit rate mode	Constant
Bit rate	12.8 kb/s
Channel(s)	1 channel
Sampling rate	8 000 Hz
Bit depth	13 bits
Stream size	10.4 KiB (100%)
Created Time 12/31/2016 11:16 PM (Consistant with Device Time)	
General	
Complete name	I:\Photos\IMG0002A.jpg
Format	JPEG
File size	4.08 KiB
Image	
Format	JPEG
Width	240 pixels
Height	240 pixels
Color space	YUV

Chroma subsampling	0.168055556
Bit depth	8 bits
Compression mode	Lossy
Stream size	4.08 KiB (100%)
Created Time 12/31/2016 11:15 PM (Consistant with Device Time)	
LIGHTER CAMERA	
General	
Complete name	I:\DCIM\100MEDIA\SUNP0000.avi
Format	AVI
Format/Info	Audio Video Interleave
File size	512 KiB
Duration	1 s 67 ms
Overall bit rate	3 931 kb/s
Director	Generplus
Original source form/Distributed by	Generplus
Recorded date	40358
Copyright	Generplus
Video	
ID	-6.944444444
Format	JPEG
Codec ID	MJPG
Duration	1 s 67 ms
Bit rate	3 865 kb/s
Width	720 pixels
Height	480 pixels
Display aspect ratio	0.010648148
Frame rate	30.000 FPS
Color space	YUV
Chroma subsampling	0.168078704
Bit depth	8 bits
Compression mode	Lossy
Bits/(Pixel*Frame)	0.00431713
Stream size	503 KiB (98%)
Audio	
ID	-6.902777778
Format	PCM

Format settings	Little / Signed
Codec ID	-6.902777778
Duration	1 s 45 ms
Bit rate mode	Constant
Bit rate	352.8 kb/s
Channel(s)	1 channel
Sampling rate	22.05 kHz
Bit depth	16 bits
Stream size	45.0 KiB (9%)
Alignment	Aligned on interleaves
Interleave duration	356 ms (10.67 video frames)
Timestamp Monday May 23 2016 3:24:32 AM (Consistant with time file after device charged)	
General	
Complete name	I:\DCIM\PHOTO\PICT0000.jpg
Format	JPEG
File size	77.6 KiB
Image	
Format	JPEG
Width	1 280 pixels
Height	1 024 pixels
Color space	YUV
Chroma subsampling	: 4:2:2
Bit depth	8 bits
Compression mode	Lossy
Stream size	77.6 KiB (100%)
Time Stamp Monday May 23 2016 3:25:08 AM	
PEN RECORDER	
General	
Complete name	I:\AUDIO\RECO0000.WAV
Format	Wave
File size	117 KiB
Duration	7 s 488 ms
Overall bit rate mode	Constant
Overall bit rate	128 kb/s

Audio	
Format	PCM
Format settings	Little / Signed
Codec ID	-6.902777778
Duration	7 s 488 ms
Bit rate mode	Constant
Bit rate	128 kb/s
Channel(s)	1 channel
Sampling rate	8 000 Hz
Bit depth	16 bits
Stream size	117 KiB (100%)
Timestamp Wednesday Feburary 8 2015 5:22:10 AM (Not Consistant with time file on device)	
General	
Complete name	I:\PHOTO\PICT0000.JPG
Format	JPEG
File size	33.0 KiB
Image	
Format	JPEG
Width	1 280 pixels
Height	960 pixels
Color space	YUV
Chroma subsampling	: 4:2:2
Bit depth	8 bits
Compression mode	Lossy
Stream size	33.0 KiB (100%)
Timestamp Wednesday February 8 2051 5:22:00 AM (Not Consistant with time file on device)	
AUDIO RECORDER	
General	
Complete name	I:\Test 1.mp3
Format	MPEG Audio
File size	8.32 MiB
Duration	3 min 38 s
Overall bit rate mode	Constant
Overall bit rate	320 kb/s
Album	Now That's What I Call Music! 85

Track name	Let Her Go (Radio Edit)
Writing library	LAME3.99.5
Audio	
Format	MPEG Audio
Format version	Version 1
Format profile	Layer 3
Format settings	Joint stereo
Duration	3 min 38 s
Bit rate mode	Constant
Bit rate	320 kb/s
Channel(s)	2 channels
Sampling rate	44.1 kHz
Frame rate	38.281 FPS (1152 SPF)
Compression mode	Lossy
Stream size	8.32 MiB (100%)
Writing library	LAME3.99.5
Timestamp Wednesday December 27 2017 4:53:14 (possible virus when trying to reset the time)	
USB AUDIO RECORDER	
General	
Complete name	I:\recode\rec00000.mp3
Format	MPEG Audio
File size	95.0 KiB
Duration	6 s 48 ms
Overall bit rate mode	Constant
Overall bit rate	128 kb/s
Audio	
Format	MPEG Audio
Format version	Version 1
Format profile	Layer 2
Duration	6 s 48 ms
Bit rate mode	Constant
Bit rate	128 kb/s
Channel(s)	2 channels
Sampling rate	32.0 kHz
Frame rate	27.778 FPS (1152 SPF)
Compression mode	Lossy

Stream size	94.5 KiB (99%)
No Time Stamps Available	