FILE STRUCTURE ANALYSIS OF MEDIA FILES SENT AND RECEIVED OVER WHATSAPP

by

HENRY LUKEN RISEMBERG

B.F.A., University of Cincinnati, 2017

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

2020

This thesis for the Master of Science degree by

Henry Luken Risemberg

has been approved for the

Recording Arts Program

by

Catalin Grigoras, Chair

Jeff M. Smith

Cole Whitecotton

Date: May 16, 2020

Risemberg, Henry Luken (M.S., Recording Arts Program)

File Structure Analysis of Media Files Sent and Received Over WhatsApp

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

This research study explores the effects of sending and downloading image and audio files through the WhatsApp platform. A better understanding of how images and audio are affected by WhatsApp is necessary because of its popularity and the prevalence of digital images and audio as evidence in digital forensic investigations.

WhatsApp is a cross-platform communication service that allows the sending of media files and is one of the most popular services of its kind used worldwide. This application can be downloaded for use on mobile phones, iOS and Windows computers. There is also a website application available. The research done here will help investigators understand the process of different uploading and downloading techniques through different devices and the effects these methods have on file structure and metadata. An examination of recompression by WhatsApp, and how the WhatsApp software behaves when interacting with original images and audio will be conducted. The resulting media file’s structure, metadata, binary data, quantization table data and other compression characteristics will be examined, and changes between files that are sent and the corresponding files that are downloaded will be analyzed.

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

Approved: Catalin Grigoras

DEDICATION

I would like to thank my parents for supporting me and guiding me to where I am today. Thank you for supporting me and motivating me to pursue an education. I would also like to especially dedicate this to my grandfather. I looked up to him more than anything, and how he lived his life further inspired me to work hard.

To those who have kept in contact with me throughout this process, Luke, Katie, Michael, Kevin, Henri, and my sisters, I am grateful.

To my co-workers and management at the Texas Department of Public Safety Crime Lab in Austin Texas who welcomed me with open arms.

And finally, a very special thank you to Bill.

ACKNOWLEDGEMENTS

I want to acknowledge everyone at the NCMF for their knowledge, support, and patience during my studies at the University of Colorado Denver. Especially Jeff and Catalin. If not for our introduction at AES conference in Los Angeles I never would have even known this was an opportunity for me. Thank you for giving me a chance in this field, and for making my time at University of Colorado Denver more than enjoyable.

Thank you, Cole, for always being there for me and for providing me with valuable input throughout the process of developing this thesis. And Leah for helping with every administrative aspect of this program.

I want to acknowledge my co-workers, Deegant, Erin, Jennifer, Marco, Melissa, Traig, and Caitlyn for their valuable input and help throughout this process.

And finally, to the NCMF 2017 – 2019 cohort. I am honored to have shared this time with such a bright group of people. We worked hard and had so much fun along the way.

TABLE OF CONTENTS

CHAPTER

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

CHAPTER I

INTRODUCTION

With the advent of computers, the internet, and cell phone technology, people in today's world can communicate with anyone anywhere in the world practically instantly at any time. As technology has evolved, social media platforms have emerged as an efficient vehicle for many people to share information and keep in touch with each other. Although instant text messaging is a common means of communication, one of the more effective ways to communicate a message is through image or audio messages. With current technology, these types of files can now be easily sent over a variety of social media platforms in virtually an instant.

Given their current popularity and the privacy that many popular social media platforms offer, social media services that offer instant messaging and file sharing are not only being used for legitimate purposes, but also for nefarious criminal activity. A significant number of cybercrimes involve the illicit distribution and possession of media files, and many other cases involve media files that have been sent and received over social media platforms in one way or another. For these types of cases, cell phones and computers are a rich source of evidence to investigators. When evidence media is discovered on these devices, it is important for investigators to understand how sending and receiving media files over social media platforms effects the data associated with those files.

For these social media platforms to facilitate the sending of media files containing image and audio information while providing users with a private and user-friendly environment, many will take original files and re-compress them so that they will work most efficiently within the platform environment. While this re-compression makes it easier for platforms to transmit, load, and store media files, data that could be important from an investigative standpoint is lost.

Depending on how re-compression takes place however, data can also be embedded into media files.

Central to the research conducted in this study is the idea that some of the embedded information, such as when and where a file was created for example, could possibly be useful to investigators who discover media files on a suspect device. The investigative research will hopefully be able to help digital forensic investigators recognize the changes that are made to media files sent and received over the WhatsApp platform. The file structure analysis of media files sent and received over WhatsApp can be added to the growing library of information collected in previous studies on how social media platforms interact with media files.

WhatsApp

WhatsApp is a free messaging service that facilitates the delivery of voice communications and multimedia sessions over internet protocol networks (VoIP). The application was created and launched in 2009 and in 2014 was acquired by Facebook for $19 Billion [2]. WhatsApp is currently the 3rd most popular social media network, and the most popular communication application worldwide with 1,600,000,000 active users [4]. Within the application, users can interact with each other one-on-one or in group messages. The service supports messaging, media file sharing, voice and video calling all while utilizing the internet via cell phone data plans or Wi-Fi. Because of this feature, users can use the application to connect to other WhatsApp users for free. The app can operate on iPhone, Android and KaiOS mobile devices. It is also available as a desktop application for Microsoft Windows and MacOS, as well as through the web application WhatsApp Web.

One important feature that has contributed to the popularity of WhatsApp is the use of end-to-end encryption with every form of communication on the service including multimedia messaging and calls. With this encryption in place, it is advertised that WhatsApp employees cannot even comply with court orders for access to information disseminated through WhatsApp. This feature is popular with users because it offers privacy. However, end to end encryption along with the large number of users creates the perfect environment for those with criminal or terroristic intentions to communicate and share files securely. WhatsApp was even used by terrorist organization ISIS to orchestrate the November 2017 Paris Attacks and the April 2017 Stockholm Attack [1] [3].

Related Works

Structure and image re-compression analysis of media file transfers over other social media and messaging platforms such as Twitter [5] and Instagram [6] have been done in recent years. There have also been more general analyses of multimedia file signatures for smart-phone forensics [7] and forensic analyses of WhatsApp messaging [8]. None of this previous research has focused on the file structure of multimedia files sent and received over WhatsApp. These papers provide a foundation for the research done in this study.

CHAPTER II

TECHNICAL OVERVIEW

JPEG Compression

The ability to capture digital images and process, store, transmit, and display them efficiently is something that we take for granted as part of our modern everyday lives. Digital image compression technology is what gives us this ability. Compression is necessary to reduce file size so that computers can handle images that would otherwise take up large amounts of storage space and processing power, ideally while maintaining the visual integrity of images. Lossy compression algorithms such as JPEG seek to discard information that is less easily noticed by the human eye and eliminate redundant information that takes up unnecessary space to achieve this. However, as the compression is applied more aggressively to save more and more space, quality is sacrificed, and compression artifacts start to become visible.

Of the different methods of image compression that are available today, JPEG is by far the most widely used and versatile. JPEG, which is an acronym for Joint Photographic Experts Group, was developed in the late 1980's and officially published in 1992 [9]. The JPEG standard was developed out of the necessity for a universal image compression specification in a time when images were starting to be shared over the internet and computers were not particularly good at processing images efficiently.

In JPEG compression, a digital image is divided into non-overlapping 8-by-8 blocks and the Discrete Cosine Transform (DCT) is computed for each block. This makes a set of 64 DCT Coefficients for each block. These coefficients are then divided by a quantization matrix and rounded off to the nearest integer. This is where data is lost. Many of these coefficients may now become zero and no longer need to be stored. Higher frequency information, which is less perceptible to the human eye, is also discarded here. Then, a compression algorithm is run on the entire set of integers [14].

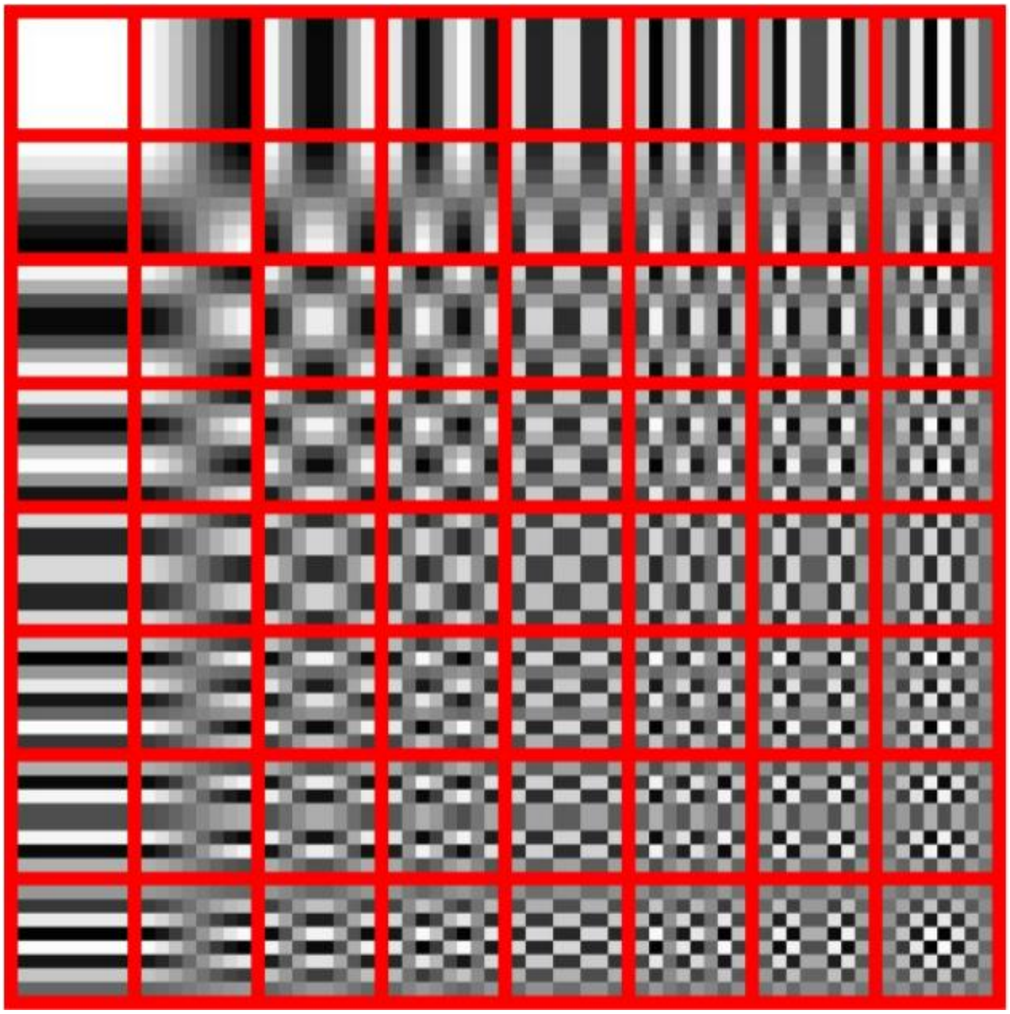


Figure 1: *Discrete Cosine Transform*

The 64 base cosine waves that can be combined to reproduce any image in 8x8 pixels for one channel

In this study, only JPEG images were analyzed. This is not only because JPEG images are so common, but also the fact that WhatsApp is primarily a mobile application, and as a default setting on most mobile devices images are captured as JPEG.

Hashing and Stream Hashing

Hash algorithms create a value of hexadecimal characters using complex mathematics based on a set of data. If any piece of that data changes, the resulting hash will also change. When two different sets of data produce the same hash value, this is called a collision. A collision can be engineered or accidental. While collisions have been engineered by computer scientist in the past, an accidental collision has never been recorded [10]. The Message Digest 5 (MD5) hash algorithm used in this study has been compromised as a result of an engineered collision before, but MD5 is still accepted as appropriate for digital signatures. Hash generation software such as the one used in this study generate hash values for given data sets very quickly and easily. The user selects a file to hash and the software calculates a hash value for that file. This is useful to identify files that are exact copies of each other as well as to identify files that may look or sound identical but have differences that are imperceptible to the human eye or ear, or have differences in metadata.

Stream hashing operates on the same concept as hashing. However, stream hashing only hashes the decoded data stream of an image file and excludes header and footer or metadata information. With this hashing method, it can be determined if the data streams of two different files are identical even if header and footer information may be different.

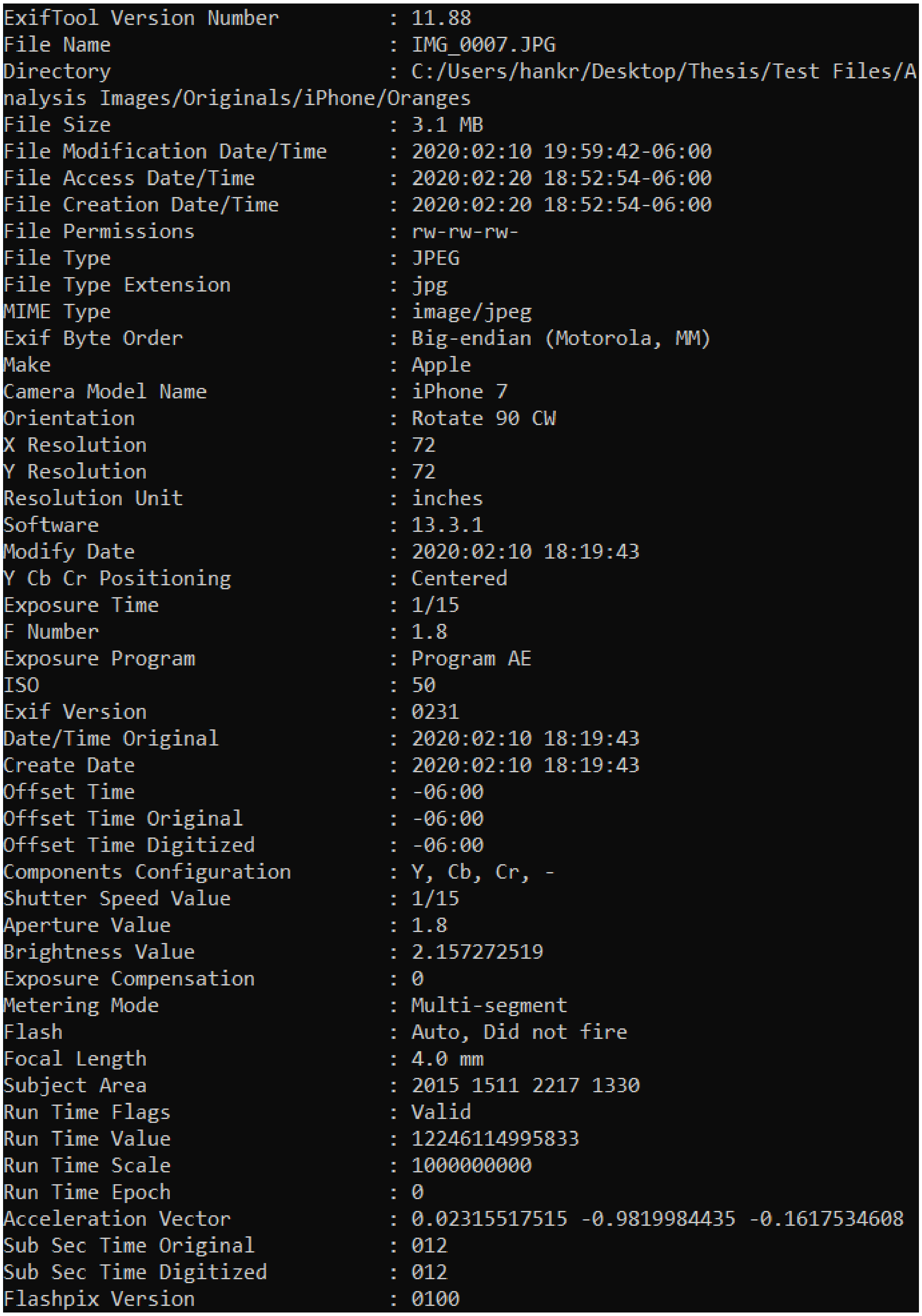
Metadata

Metadata, according to the Scientific Working Group on Digital Evidence, is “Data, frequently embedded within a file, that describes a file or directory, which can include the locations where the content is stored, dates and times, application specific information, and permissions” [18]. So, metadata is basically data that provides information about other data. In the case of this study, we are referring to metadata associated with image and audio files. This data is some of the most important data to digital forensic investigators as it can include unique identifiable information about the who, what, when, where and how associated with a media file.

Exif Data

Exchangeable Image File Format, abbreviated as “Exif”, is a form of metadata and is the format in which data associated with image files captured with digital cameras is stored. The format was developed and is maintained by the Japan Electronic Industries Development Association and was first specified in 1998 [11]. Exif data associated with media files can include, but is not limited to, the GPS coordinates of where the media file was created, time and date information, identifying information of the recording device, camera settings and much more.

The volume of Exif data entries associated with a given file depends on the device used to capture the original image and can be affected by post processing an image file. Some files may have many Exif data entries while others may have very few. Simply observing how many Exif data entries there are may give clues to how the image file was captured and processed, and the content of Exif entries provides important information to digital forensic investigators.



```
ExifTool Version Number         : 11.88
File Name                       : IMG_0007.JPG
Directory                       : C:/Users/hankr/Desktop/Thesis/Test Files/A
nalysis Images/Originals/iPhone/Oranges
File Size                       : 3.1 MB
File Modification Date/Time     : 2020:02:10 19:59:42-06:00
File Access Date/Time           : 2020:02:20 18:52:54-06:00
File Creation Date/Time         : 2020:02:20 18:52:54-06:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Make                            : Apple
Camera Model Name               : iPhone 7
Orientation                     : Rotate 90 CW
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Software                        : 13.3.1
Modify Date                     : 2020:02:10 18:19:43
Y Cb Cr Positioning             : Centered
Exposure Time                   : 1/15
F Number                        : 1.8
Exposure Program                : Program AE
ISO                             : 50
Exif Version                    : 0231
Date/Time Original              : 2020:02:10 18:19:43
Create Date                     : 2020:02:10 18:19:43
Offset Time                     : -06:00
Offset Time Original            : -06:00
Offset Time Digitized           : -06:00
Components Configuration        : Y, Cb, Cr, -
Shutter Speed Value             : 1/15
Aperture Value                  : 1.8
Brightness Value                : 2.157272519
Exposure Compensation           : 0
Metering Mode                   : Multi-segment
Flash                           : Auto, Did not fire
Focal Length                    : 4.0 mm
Subject Area                    : 2015 1511 2217 1330
Run Time Flags                  : Valid
Run Time Value                  : 12246114995833
Run Time Scale                  : 1000000000
Run Time Epoch                  : 0
Acceleration Vector             : 0.02315517515 -0.9819984435 -0.1617534608
Sub Sec Time Original           : 012
Sub Sec Time Digitized          : 012
Flashpix Version                : 0100
```

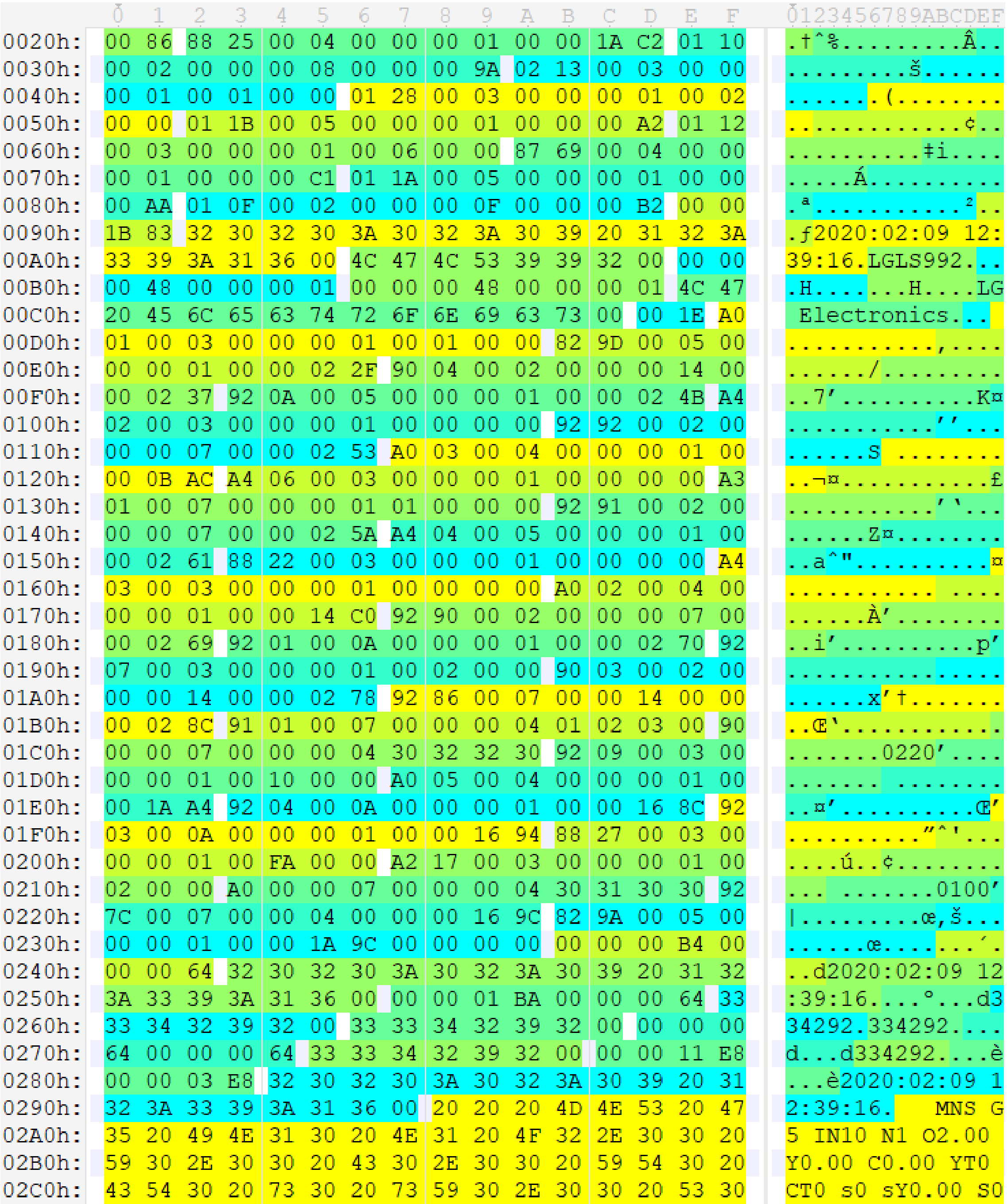
Figure 2: *Exif Data*

This figure is an example of a printout of Exif data that was obtained running the program ExifTool on a JPEG image file

Hex Data

At the most basic level, all digital information is stored, processed and represented in binary form. That is, the binary numerical system of ones and zeros. Each one or zero represents a binary digit, the smallest unit of data in a computer. Computers can take these bits and process them as instructions to perform tasks that we want the computer to perform. These ones and zeros are incomprehensible to most people, but digital forensic investigators must make sense of this data to represent what it means.

To solve this problem, we have a slightly easier way of representing binary data in the form of hexadecimal data. Hexadecimal uses a base 16 number system to represent data, using the numbers 1 through 9 to represent values zero to nine, and letters A through F to represent values ten to fifteen. Hex reader software can act as a translator to represent the data in Hexadecimal. This way data is more easily understood. Hex readers can further translate some data into meaningful ASCII information, which is an abbreviation for American Standard Code for Information Interchange [12]. ASCII information sometimes contains meaningful words and phrases that give important information about a file.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0020h: 00 86 88 25 00 04 00 00 00 01 00 00 1A C2 01 10  .†ˆ%.........Â..
0030h: 00 02 00 00 00 08 00 00 00 9A 02 13 00 03 00 00  .........š......
0040h: 00 01 00 01 00 00 01 28 00 03 00 00 00 01 00 02  .......(........
0050h: 00 00 01 1B 00 05 00 00 00 01 00 00 00 A2 01 12  .............¢..
0060h: 00 03 00 00 00 01 00 06 00 00 87 69 00 04 00 00  ..........‡i....
0070h: 00 01 00 00 00 C1 01 1A 00 05 00 00 00 01 00 00  .....Á..........
0080h: 00 AA 01 0F 00 02 00 00 00 0F 00 00 00 B2 00 00  .ª...........²..
0090h: 1B 83 32 30 32 30 3A 30 32 3A 30 39 20 31 32 3A  .ƒ2020:02:09 12:
00A0h: 33 39 3A 31 36 00 4C 47 4C 53 39 39 32 00 00 00  39:16.LGLS992...
00B0h: 00 48 00 00 00 01 00 00 00 48 00 00 00 01 4C 47  .H.......H....LG
00C0h: 20 45 6C 65 63 74 72 6F 6E 69 63 73 00 00 1E A0   Electronics... 
00D0h: 01 00 03 00 00 00 01 00 01 00 00 82 9D 00 05 00  ...........‚....
00E0h: 00 00 01 00 00 02 2F 90 04 00 02 00 00 00 14 00  ....../.........
00F0h: 00 02 37 92 0A 00 05 00 00 00 01 00 00 02 4B A4  ..7’..........K¤
0100h: 02 00 03 00 00 00 01 00 00 00 00 92 92 00 02 00  ...........’’...
0110h: 00 00 07 00 00 02 53 A0 03 00 04 00 00 00 01 00  ......S ........
0120h: 00 0B AC A4 06 00 03 00 00 00 01 00 00 00 00 A3  ..¬¤...........£
0130h: 01 00 07 00 00 00 01 01 00 00 00 92 91 00 02 00  ...........’‘...
0140h: 00 00 07 00 00 02 5A A4 04 00 05 00 00 00 01 00  ......Z¤........
0150h: 00 02 61 88 22 00 03 00 00 00 01 00 00 00 00 A4  ..aˆ"..........¤
0160h: 03 00 03 00 00 00 01 00 00 00 00 A0 02 00 04 00  ........... ....
0170h: 00 00 01 00 00 14 C0 92 90 00 02 00 00 00 07 00  ......À’........
0180h: 00 02 69 92 01 00 0A 00 00 00 01 00 00 02 70 92  ..i’..........p’
0190h: 07 00 03 00 00 00 01 00 02 00 00 90 03 00 02 00  ................
01A0h: 00 00 14 00 00 02 78 92 86 00 07 00 00 14 00 00  ......x’†.......
01B0h: 00 02 8C 91 01 00 07 00 00 00 04 01 02 03 00 90  ..Œ‘............
01C0h: 00 00 07 00 00 00 04 30 32 32 30 92 09 00 03 00  .......0220’....
01D0h: 00 00 01 00 10 00 00 A0 05 00 04 00 00 00 01 00  ....... ........
01E0h: 00 1A A4 92 04 00 0A 00 00 00 01 00 00 16 8C 92  ..¤’..........Œ’
01F0h: 03 00 0A 00 00 00 01 00 00 16 94 88 27 00 03 00  ..........”ˆ'...
0200h: 00 00 01 00 FA 00 00 A2 17 00 03 00 00 00 01 00  ....ú..¢........
0210h: 02 00 00 A0 00 00 07 00 00 00 04 30 31 30 30 92  ... .......0100’
0220h: 7C 00 07 00 00 04 00 00 00 16 9C 82 9A 00 05 00  |.........œ‚š...
0230h: 00 00 01 00 00 1A 9C 00 00 00 00 00 00 00 B4 00  ......œ.......´.
0240h: 00 00 64 32 30 32 30 3A 30 32 3A 30 39 20 31 32  ..d2020:02:09 12
0250h: 3A 33 39 3A 31 36 00 00 00 01 BA 00 00 00 64 33  :39:16....°...d3
0260h: 33 34 32 39 32 00 33 33 34 32 39 32 00 00 00 00  34292.334292....
0270h: 64 00 00 00 64 33 33 34 32 39 32 00 00 00 11 E8  d...d334292....è
0280h: 00 00 03 E8 32 30 32 30 3A 30 32 3A 30 39 20 31  ...è2020:02:09 1
0290h: 32 3A 33 39 3A 31 36 00 20 20 20 4D 4E 53 20 47  2:39:16.   MNS G
02A0h: 35 20 49 4E 31 30 20 4E 31 20 4F 32 2E 30 30 20  5 IN10 N1 O2.00 
02B0h: 59 30 2E 30 30 20 43 30 2E 30 30 20 59 54 30 20  Y0.00 C0.00 YT0 
02C0h: 43 54 30 20 73 30 20 73 59 30 2E 30 30 20 53 30  CT0 s0 sY0.00 S0
```

Figure 3: *Hex Data*

This figure is an example of Hexadecimal data as viewed in the hex viewer 010 Editor. The right most column contains addresses, the middle column contains data represented in Hexadecimal, and the right most column contains information interpreted as ASCII. Data is color coded by 010 editor to help identify meaningful chunks of data.

Baseline JPEG vs. Progressive JPEG

JPEG images can come in two different forms, Baseline or Progressive. A Baseline JPEG image uses an algorithm that starts to display image data as it becomes available, line by line from top to bottom. If you were to see a Baseline JPEG image load slowly, you could see the image showing up on your screen in this manner. Progressive JPEG on the other hand loads images in a different way. This type of image is displayed first as a blurry version of the image in its entirety, becoming clearer and clearer as more image data is made available [13].

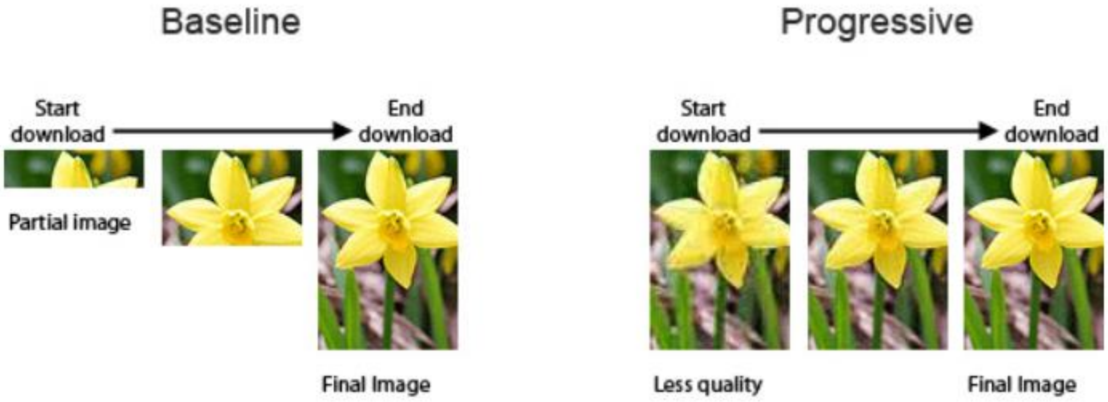
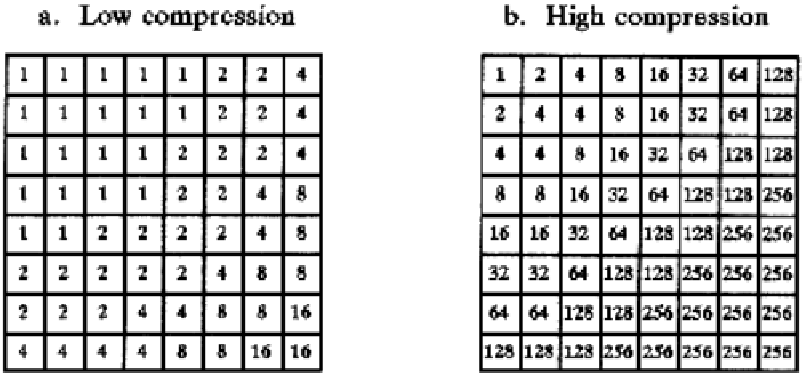


***Figure 4:** Baseline vs. Progressive Encoding*

Quantization Tables

Quantization is part of the JPEG compression process. The JPEG compression algorithm uses one or more quantization tables that dictate the degree to which images will be compressed. This in turn determines the images overall "Quality Factor". The original image is processed into coefficients, and these coefficients are rounded to the nearest integer. This is the part of jpeg compression where image data is lost and file size is reduced. The resulting integers are divided by the value in the quantization table that corresponds to that integer. If a higher level of compression is used the quantization table has higher values in it. In this case a lower quality image file with a smaller file size is created. If a lower level of compression is used the quantization table uses lower values. In this case a higher quality image file results but the file size is not reduced as much [15].



a. Low compression

1	1	1	1	1	2	2	4
1	1	1	1	1	2	2	4
1	1	1	1	2	2	2	4
1	1	1	1	2	2	4	8
1	1	2	2	2	2	4	8
2	2	2	2	2	4	8	8
2	2	2	4	4	8	8	16
4	4	4	4	8	8	16	16

b. High compression

1	2	4	8	16	32	64	128
2	4	4	8	16	32	64	128
4	4	8	16	32	64	128	128
8	8	16	32	64	128	128	256
16	16	32	64	128	128	256	256
32	32	64	128	128	256	256	256
64	64	128	128	256	256	256	256
128	128	128	256	256	256	256	256

Figure 5: *JPEG Quantization Tables*

This figure portrays two examples of quantization tables that may be used in JPEG compression. The table on the left is indicative of a lower level of compression, and the table on the right a higher level of compression.

Lossy Compression Analysis

Lossy compression analysis is a method that can be used to identify what type of software or device was used to record an audio recording by assessing the traces of lossy compression in the signal [17]. In this method, reference recordings from known phones or devices are used to configure a database of compression models for each phone or device. The compression model that is created consists of AAC decoded MDCT coefficients, the Long-Term Average Sorted Spectrum, and the Audio compression level of known audio files. Unknown audio files can be compared against the database automatically to determine if the unknown files compression characteristics match that of any of the models in the database.

Appendix 5. FDK-AAC (upper) and Nero (lower) decoded original Voice Memos iOS 11.0.2 .M4A/AAC recordings

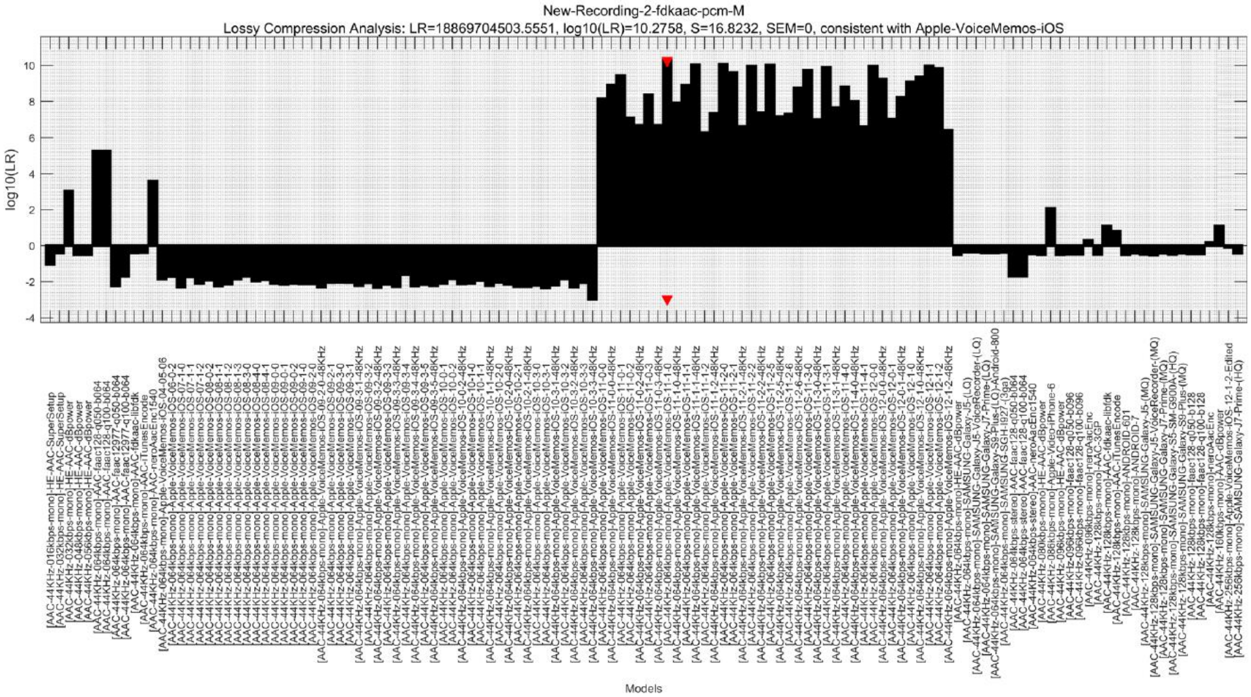


Figure 6: *Lossy Compression Analysis*

This figure shows the result of lossy compression level analysis against a curated database. The red arrow indicates which compression model the inputted file is most consistent with.

CHAPTER III

MATERIALS

Device Specifications

The research in this study was conducted with six different devices including two laptop computers and four mobile devices. It was determined that two iPhone devices and two Android devices should be used. This was because logging in and out of multiple WhatsApp accounts multiple times on mobile devices caused WhatsApp to lock out the user for increasingly long periods of time. When it came time to send images from Android to Android or iPhone to iPhone another device was employed to avoid this issue. The same issue was not experienced with desktop or web applications. The specifications of the devices used as well as the Google Chrome web application are listed below.

Table 1: *PC Laptop Specifications*

PC Laptop	
Manufacturer	MSI
Model	GF65 Thin
Processor	Intel Core i5-9300H CPU @ 2.4 GHz
RAM	8.00 GB
Operating System	Windows 10 Build 18362.719
WhatsApp Version	0.4.315

Table 2: *MacBook Pro Laptop Specifications*

MacBook Pro	
Manufacturer	Apple Inc.
Model	Mid 2015, 15-inch, Retina Display
Processor	2.8 GHz Intel Core i7
RAM	16.00 GB
Operating System	MacOS Mojave Version 10.14.4
WhatsApp Version	0.4.315

Table 3: *iPhone 6 Plus Specifications*

iPhone 6 Plus	
Manufacturer	Apple Inc.
Model Number	NGAU2LL/A
Operating System	iOS 12.4.5
Serial Number	F9CS706UG5QJ
IMEI Number	35 931906 197647 9
WhatsApp Version	2.20.21

Table 4: *iPhone 7 Specifications*

iPhone 7	
Manufacturer	Apple Inc.
Model Number	MN9D2LL/A
Operating System	iOS 13.3.1
Serial Number	F17VH2K1HG7F
IMEI Number	35 676008 911620 9
WhatsApp Version	2.20.21

Table 5: *Android G5 Specifications*

Android G5	
Manufacturer	LG
Model Number	LGLS992
Software Version	LS992ZVF
Build Number	NRD90U
IMEI Number	355602072466687
WhatsApp Version	2.20.21

Table 6: *Galaxy S9 Specifications*

Samsung Galaxy S9 Plus	
Manufacturer	Samsung
Model Number	SM-G965U
Software Version	G965USQS7DTB1
IMEI Number	356420092963925
WhatsApp Version	2.20.108
Android Version	10

Table 7: *Web Application Specifications*

In instances where the Web Application was used, it was accessed via the MSI Laptop.

Web Application	
Browser	Google Chrome
Browser Version	79.0.3945.130 (official build) (64-bit)
URL	web.whatsapp.com

Test Media Preparation

It was determined that images captured on mobile phones would be the most relevant type of images to use in this study because the WhatsApp application is primarily used on mobile devices [4]. The goal of the test media preparation in this study was to ensure that the images and audio used for testing were identical before sending regardless of the device they originated from.

A total of four images were used for testing in this study. Two images were captured on the iPhone 7, and two more images were captured on the Android G5. For each device, one image was captured in portrait orientation (with the device held upright) and one image was captured in landscape orientation (with the device held 90 degrees from upright).

- The image captured on the iPhone 7 in portrait orientation will henceforth be referred to as “iPhone Image 1”.
- The image captured on the iPhone 7 in landscape orientation will henceforth be referred to as “iPhone Image 2”
- The image captured on the Android G5 in portrait orientation will henceforth be referred to as “Android Image 1”
- The image captured on the Android G5 in landscape orientation will henceforth be referred to as “Android Image 2”

After the images were captured with each device, the original images were extracted from the iPhone and the Android devices directly to the MSI laptop computer. The hashes of these images were then calculated. Then, the images were loaded onto every other device that the images did not originate from via a data cable transfer. After the images were populated to every device, a hash verification was conducted against every corresponding image on every device to ensure that images were not altered by the process of moving them from device to device in preparation for the study. This verification was successful. At this point, there were 4 images on the MSI Laptop, MacBook Pro, iPhone 6 Plus, iPhone 7, Android G5 and Galaxy S9.

A total of twenty audio recordings were also used for this study. The twenty audio recordings with an average approximate length of one minute were recorded on the iPhone 7 using the Apple Voice Memos application. These audio recordings were only sent from the iPhone 7. Sending the audio recordings from other devices other than the iPhone 7 was determined to be beyond the scope of this study. Ten of these recordings were recorded with the “Lossless” setting enabled in the iPhone Voice Memos settings menu, and ten more recordings were recorded with the “Compressed” setting enabled.

A WhatsApp account with the name “Hank Thesis” was create solely for the purpose of this study to provide a sterile environment for testing. Since WhatsApp requires a phone number to be associated with any account, a Google Voice account was created to associate the WhatsApp account with.

CHAPTER IV

METHODOLOGY

Sending Methods

After the four original images were populated to the six devices to be used in this study, each image was sent using the ten different sending methods listed below. This list of sending methods includes every easily accessible method to send images from within the WhatsApp user interface in a chat between two users. If more than three images are sent without a text message in between, the images are grouped into a collection of images that needs to be expanded to be viewed and downloaded. To avoid the variables that this would introduce, one text message was sent between the sending of each image.

Table 7: *Image Send Methods*

Send Methods		
Device	**Reference in Hash Tables**	**Method**
iPhone	Send Method 1	'+' Icon
	Send Method 2	Camera Icon
Android	Send Method 3	Attachment Icon
	Send Method 4	Camera Icon
PC Application via MSI Laptop	Send Method 5	Drag and Drop
	Send Method 6	Attachment Icon
MacOS Application via MacBook Pro	Send Method 7	Drag and Drop
	Send Method 8	Attachment Icon
Google Chrome Application	Send Method 9	Drag and Drop
	Send Method 10	Attachment Icon

The audio files in this study were sent using the "share" function within the Apple Voice Memos application of the iPhone 7. It is possible to select audio files from within the WhatsApp application for sending, however exploring the effects of using different send methods for audio was determined to be beyond the scope of this study.

Download Methods

After the images were sent through WhatsApp, they were downloaded using the following download methods from the four different devices and web application. The list of download methods includes every easily accessible method to download images within the WhatsApp user interface in a chat between two users.

Table 8: *Image Download Methods*

Download Methods		
Device	**Reference in Hash Tables**	**Method**
iPhone	DL M 1	Automatic Download
	DL M 2	Automatic Download Disabled
Android	DL M 3	Automatic Download
	DL M 4	Automatic Download Disabled
PC Application via MSI Laptop	DL M 5	Menu Icon
	DL M 6	Download Arrow
	DL M 7	Expanded Download Arrow
MacOS Application via MacBook Pro	DL M 8	Menu Icon
	DL M 9	Download Arrow
	DL M 10	Expanded Download Arrow
Google Chrome Application	DL M 11	Download Arrow
	DL M 12	Right Click Download
	DL M 13	Expanded Download Arrow
	DL M 14	Expanded Rick Click Download

There is currently no application programming interface for WhatsApp, so images that could have otherwise been sent and downloaded automatically were sent and downloaded manually. After the images were downloaded via all the downloaded methods in table 8, they were extracted from each device to the MSI laptop for analysis.

Audio files were downloaded from the WhatsApp PC application to a device using the Windows 10 operating system for analysis.

Analysis Procedure

The sending and downloading of four images utilizing all ten send methods and all fourteen download methods resulted in the creation of a set of 560 test images to be analyzed. After the images were extracted from all devices and consolidated onto the MSI laptop, the first step in the analysis was to calculate hash values for each individual image.

Calculating the hash values of all resultant images was done to determine what sending and downloading methods produced bit stream duplicate files and if any combination of methods did not change the files at all. Patterns of combinations of sending and downloading methods that resulted in duplicate files could be observed and documented. After this step analysis could be limited to files that were not duplicates of each other. Stream hashes were calculated as a second level of further assessing files that did not have matching hash values. This was done to determine if there were images that may have identical image data and only have differences in metadata.

After unique images were identified for analysis, file characteristics and structure were observed. Analysis of Metadata, Hex data, Exif data, Quantization Tables, and how the images were encoded was conducted and conclusions drawn from this information.

Analysis of the audio files was conducted separately from the image files in this study. Audio files were downloaded from WhatsApp to a desktop computer and a Lossy Compression Analysis was conducted against the files.

Analysis Tools

The following table lists the tools and their respective versions that were used for analysis in this study.

Table 9: *Analysis Tools and Versions*

Analysis Tools	
Tool	**Version**
ExactFile	1.0.0.15
MediaInfo	19.09
ffmpeg	4.2.1
JPEG Snoop	1.7.3
ExifTool	11.88
010 Editor	10.0.1

CHAPTER V

RESULTS

File Name

The first file characteristic to be observed in this study was file name. All downloaded images had unique file names. Some useful information was able to be observed in the names of the downloaded image files.

The original images all had a file extension of ".jpg". After images were sent through WhatsApp and downloaded however, the file extension changed to ".jpeg" in all instances.

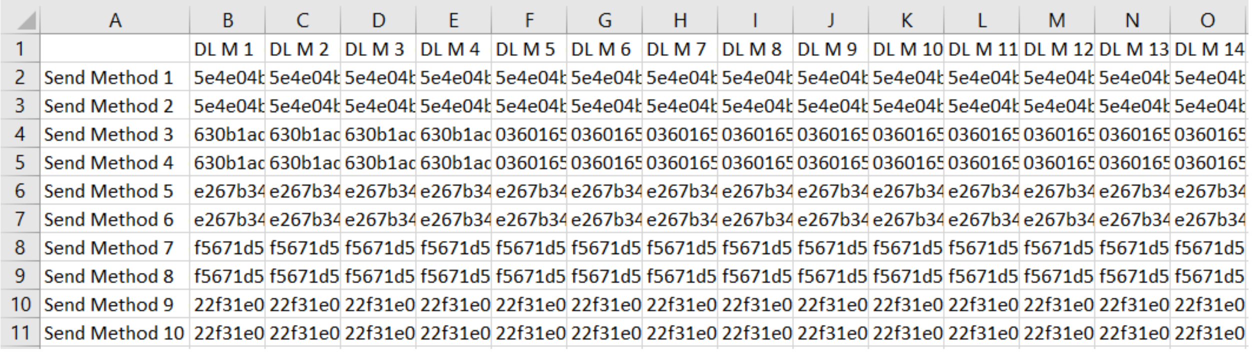
The naming convention applied to image files downloaded from WhatsApp is dictated by what type of device or web application was used to download the images. A unique naming convention is applied if the image is received on an iPhone or an Android device. If the image is downloaded through the MacOS application, Windows application, or web application (except for the right click/download method within the web application), the naming convention is the same. The naming conventions with examples are described as follows.

- Download to iPhone device
    - Four uppercase letters followed by four numbers
    - Ex.) "QOJY4018"
- Download to Android device
    - "IMG" followed by "-" followed by date arranged in "yyyymmdd", followed by "-", followed by "WA", followed by a four digit number that seems to indicate the order in which the images were downloaded to the phones file system
    - Ex.) "IMG-20200215-WA0049"

- Download via Mac Application, Windows Application, or Web Application
    - “WhatsApp Image” followed by date in the format of “yyyy-mm-dd” followed by “at”, followed by time that the message was *sent* “h.mm.ss”, followed by “AM” or “PM”
    - Ex.) “WhatsApp Image 2020-02-15 at 4.43.32 PM”
- Download using the right click / download feature within the WhatsApp Web Application
    - 8 numbers and lower-case letters, followed by 4 numbers and lowercase letters, followed by 4 more numbers and lowercase letters, followed by 12 numbers and lowercase letters. No patterns were determined in this naming convention
    - Ex.) “2d7a76ec-310b-400c-abed-7b7555699584”

Hash Analysis

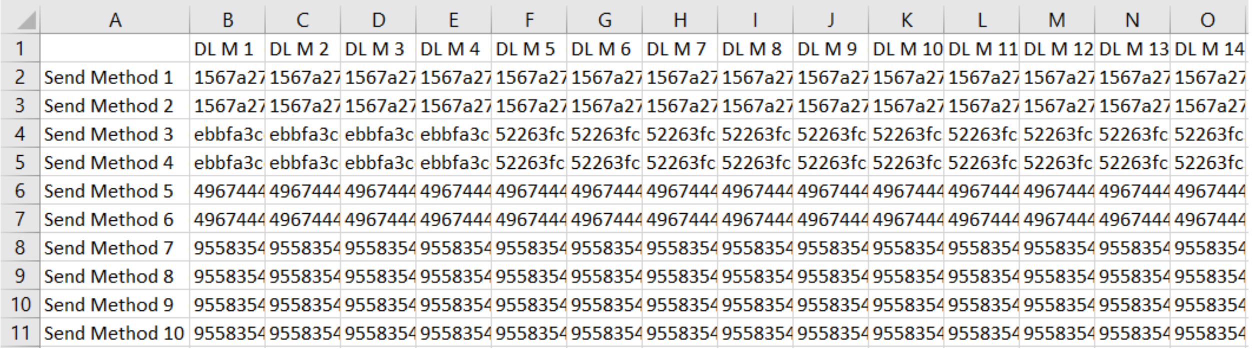
Hash values were calculated for all downloaded images. Every hash value was entered into a table with sending methods on the y-axis and download methods on the x-axis. A different table was created for each source image. This helped facilitate visually observing patterns of likeness between downloaded images dependent on the method of sending and downloading. In the tables to follow, only a portion of the hash values are shown. Reference Table 7 and 8 for what send methods and download methods are used in each row and column.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1		DL M 1	DL M 2	DL M 3	DL M 4	DL M 5	DL M 6	DL M 7	DL M 8	DL M 9	DL M 10	DL M 11	DL M 12	DL M 13	DL M 14
2	Send Method 1	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b
3	Send Method 2	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b	5e4e04b
4	Send Method 3	630b1ac	630b1ac	630b1ac	630b1ac	0360165	0360165	0360165	0360165	0360165	0360165	0360165	0360165	0360165	0360165
5	Send Method 4	630b1ac	630b1ac	630b1ac	630b1ac	0360165	0360165	0360165	0360165	0360165	0360165	0360165	0360165	0360165	0360165
6	Send Method 5	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34
7	Send Method 6	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34	e267b34
8	Send Method 7	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5
9	Send Method 8	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5	f5671d5
10	Send Method 9	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0
11	Send Method 10	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0	22f31e0

Figure 7: *Table of Hash Values for iPhone Image 1*

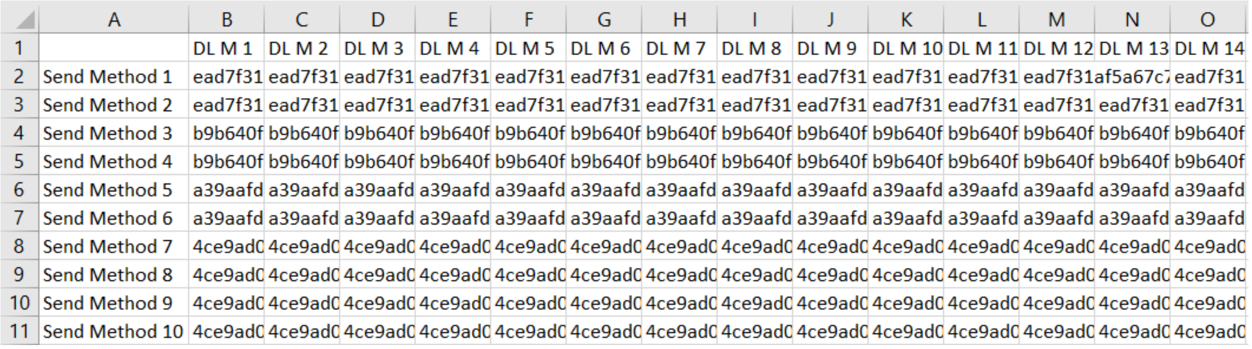
After sending and receiving "iPhone Image 1" by means of every combination of send and download methods, five different images were produced. One different image was created for each device or web application that was used to send the image.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1		DL M 1	DL M 2	DL M 3	DL M 4	DL M 5	DL M 6	DL M 7	DL M 8	DL M 9	DL M 10	DL M 11	DL M 12	DL M 13	DL M 14
2	Send Method 1	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27
3	Send Method 2	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27	1567a27
4	Send Method 3	ebbfa3c	ebbfa3c	ebbfa3c	ebbfa3c	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc
5	Send Method 4	ebbfa3c	ebbfa3c	ebbfa3c	ebbfa3c	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc	52263fc
6	Send Method 5	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444
7	Send Method 6	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444	4967444
8	Send Method 7	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354
9	Send Method 8	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354
10	Send Method 9	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354
11	Send Method 10	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354	9558354

Figure 8: *Table of Hash Values for iPhone Image 2*

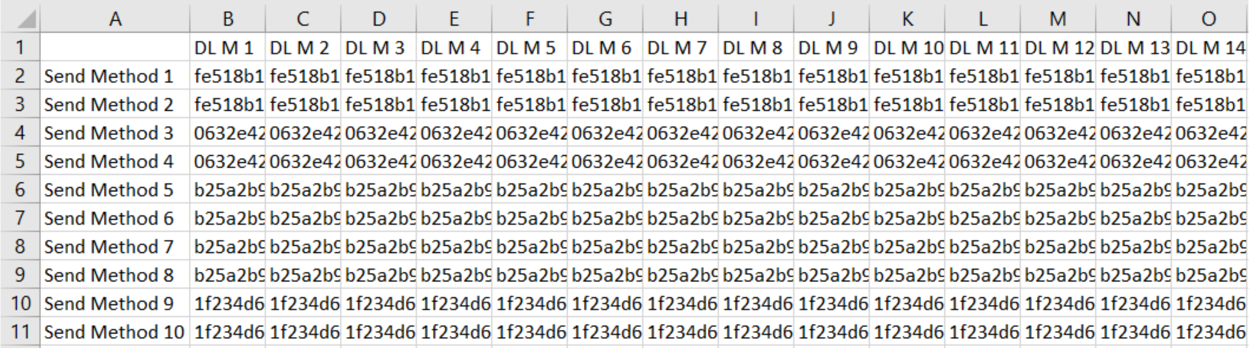
After sending and receiving "iPhone Image 2" by means of every combination of send and download methods, four different images were produced. One different image was created for each device or web application that was used to send the image. However, images sent from the WhatsApp application running on Windows 10 matched images that were sent from the WhatsApp application on the MacOS.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1		DL M 1	DL M 2	DL M 3	DL M 4	DL M 5	DL M 6	DL M 7	DL M 8	DL M 9	DL M 10	DL M 11	DL M 12	DL M 13	DL M 14
2	Send Method 1	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	af5a67c7	ead7f31
3	Send Method 2	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31	ead7f31
4	Send Method 3	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f
5	Send Method 4	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f	b9b640f
6	Send Method 5	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd
7	Send Method 6	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd	a39aafd
8	Send Method 7	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0
9	Send Method 8	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0
10	Send Method 9	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0
11	Send Method 10	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0	4ce9ad0

Figure 9: *Table of Hash Values for Android Image 1*

After sending and receiving "Android Image 1" by means of every combination of send and download methods, four different images were produced. This time, the same results were observed as with "iPhone Image 2". One different image was created for each device or web application that was used to send the image, except images sent from the WhatsApp application running on Windows 10 matched images that were sent from the WhatsApp application on the MacOS.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1		DL M 1	DL M 2	DL M 3	DL M 4	DL M 5	DL M 6	DL M 7	DL M 8	DL M 9	DL M 10	DL M 11	DL M 12	DL M 13	DL M 14
2	Send Method 1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1
3	Send Method 2	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1	fe518b1
4	Send Method 3	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42
5	Send Method 4	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42	0632e42
6	Send Method 5	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9
7	Send Method 6	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9
8	Send Method 7	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9
9	Send Method 8	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9	b25a2b9
10	Send Method 9	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6
11	Send Method 10	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6	1f234d6

Figure 10: *Table of Hash Values for Android Image 2*

After sending and receiving "Android Image 2" by means of every combination of send and download methods, four different images were produced. One different image was created for each device or web application that was used to send the image, except this time images sent from the WhatsApp application running on Windows 10 matched images that were sent from the WhatsApp Web application.

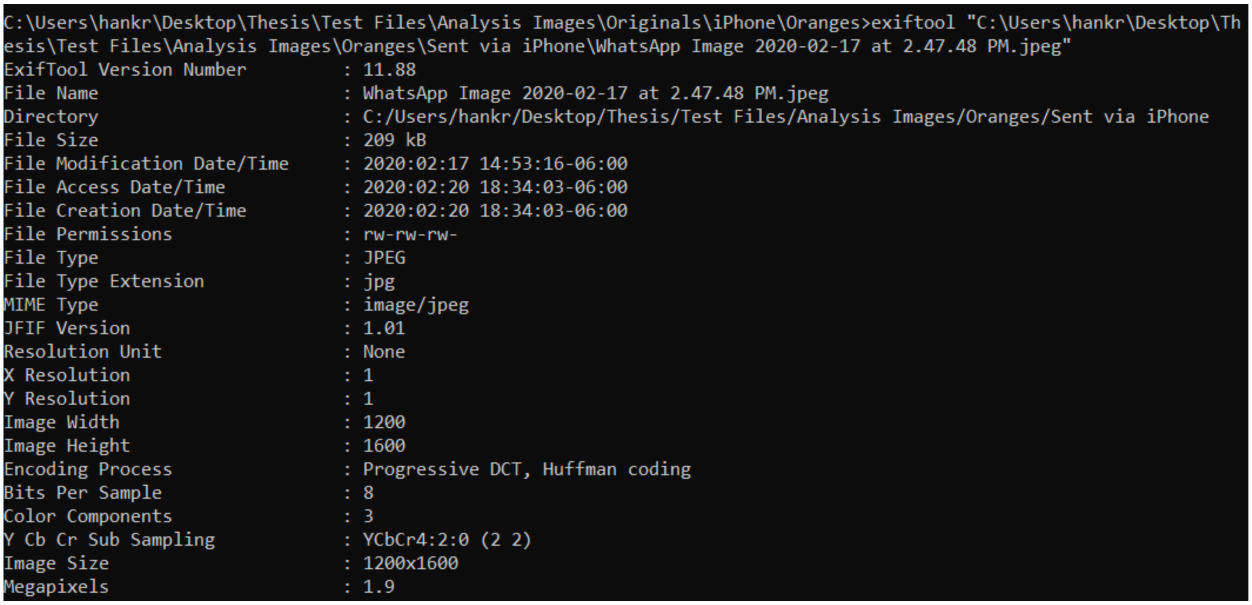
After every send and download method was used to process the four different original images, a total of seventeen different downloaded images were produced. Different images were produced dependent on the send method, and different send methods within an application on one device or web application had no effect on the downloaded images. Different download methods had no effect on the output images outside of how the files were named. In some cases, but not all, there is uniformity between images that are sent from different desktop devices or web applications.

Five different versions of "iPhone Image 1" were produced, and four different images were produced for the other three images, "iPhone Image 2", "Android Image 1", and "Android Image 2". From this point forward, analysis was conducted only on one each of those seventeen different images.

Stream hash values were calculated for each of the resulting seventeen different images and there were no matches. This shows that there are differences in the core image data of all seventeen images.

Exif Data

The four original images and seventeen images downloaded from WhatsApp were inputted into ExifTool. The volume of Exif entries observed for images was significantly reduced after those images were sent and then downloaded through WhatsApp. There were a total of 123 Exif entries for both images that were captured on the iPhone, and 79 Exif entries for both images that were captured on Android. After images were sent and then downloaded through WhatsApp however, only 22 Exif entries were observed.



```
C:\Users\hankr\Desktop\Thesis\Test Files\Analysis Images\Originals\iPhone\Oranges>exiftool "C:\Users\hankr\Desktop\Th
esis\Test Files\Analysis Images\Oranges\Sent via iPhone\WhatsApp Image 2020-02-17 at 2.47.48 PM.jpeg"
ExifTool Version Number         : 11.88
File Name                       : WhatsApp Image 2020-02-17 at 2.47.48 PM.jpeg
Directory                       : C:/Users/hankr/Desktop/Thesis/Test Files/Analysis Images/Oranges/Sent via iPhone
File Size                       : 209 kB
File Modification Date/Time     : 2020:02:17 14:53:16-06:00
File Access Date/Time           : 2020:02:20 18:34:03-06:00
File Creation Date/Time         : 2020:02:20 18:34:03-06:00
File Permissions                : rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 1200
Image Height                    : 1600
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1200x1600
Megapixels                      : 1.9
```

Figure 11: *Exif Entries for Image Downloaded From WhatsApp*

Of the twenty-two Exif entries, the following entries were the same for every image.

- File Permission: rw-rw-rw
- File Type: JPEG
- File Type Extension: jpg
- MIME Type: image/jpeg
- JFIF Version: 1.01
- Resolution Unit: 1.01
- X Resolution: 1
- Y Resolution: 1
- Bits Per Sample: 8
- Color Components: 3
- Y Cb Cr Sub Sampling: YCbCr4:2:0 (2 2)

Of the twenty-two Exif entries, the following entries varied between images.

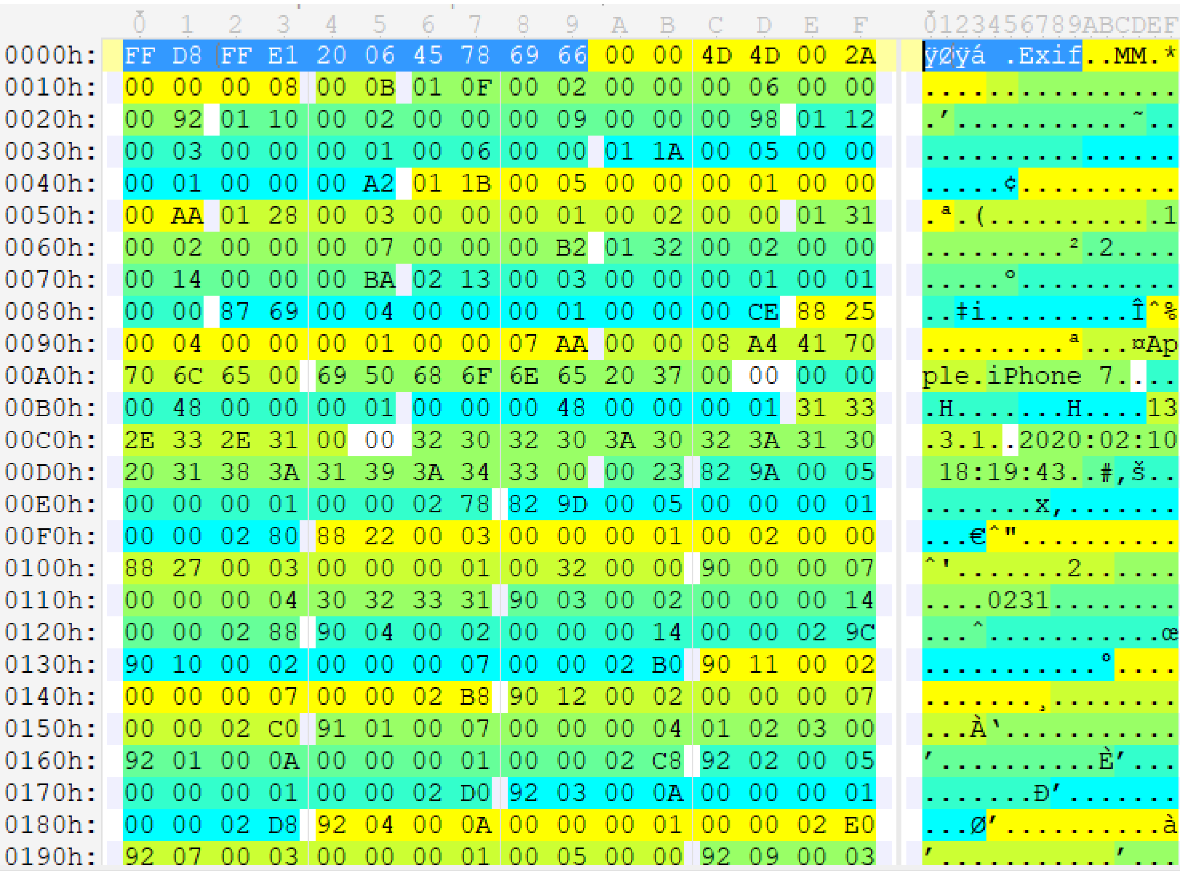
- File Name
- Directory
- File Size
- File Modified Date/Time
- File Access Date/Time
- File Creation Date/Time
- Image Width
- Image Height
- Encoding Process
- Image Size
- Megapixels

One variable that experienced some interesting and consistent changes was image size and dimensions. Images that were originally captured on an iPhone had their width and height dimensions reduced by a factor of 2.52 by the WhatsApp compression. Images that were originally captured on an Android device had their width and height dimensions reduced by a factor of 3.32 by the WhatsApp compression. Images that were captured on an Android device *and* were sent by an Android device had their width and height dimensions reduced by a factor of exactly 4 by the WhatsApp compression.

The file size of images that originated from the same source image and were sent via desktop applications were all very similar. In cases where images originating from the same source image that were sent over different desktop applications did not have matching hash values, there was only a relatively very small difference (less than a kilobyte) in their file size.

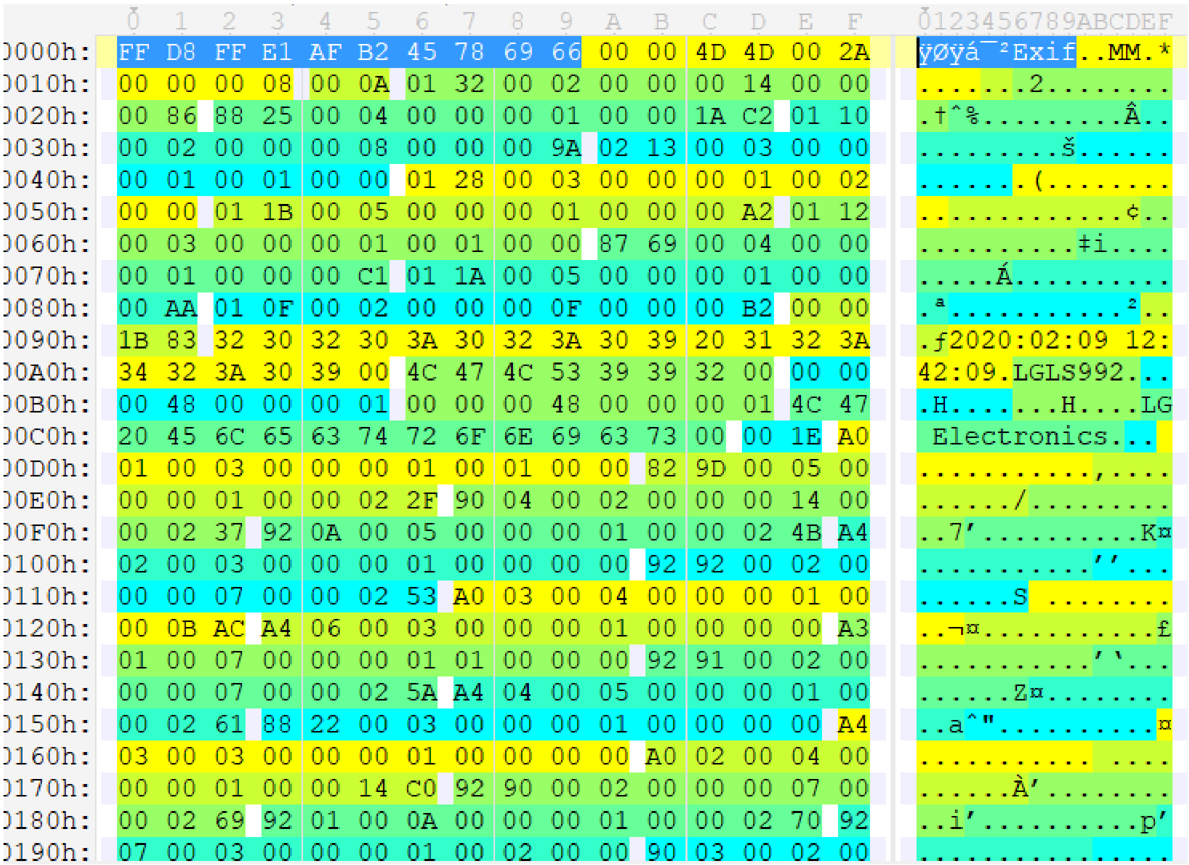
Hex Data (Image)

Hex data analysis and observations were conducted using 010 Editor. The color coding is applied by 010 Editor to highlight logical segments of data. Original images displayed the JPG EXIF file signature `FF D8 FF E1 ?? ?? 45 78 69 66 00 00`. Shown below is the beginning of the file header for one original iPhone image and one original Android image.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FF D8 FF E1 20 06 45 78 69 66 00 00 4D 4D 00 2A  ÿØÿá .Exif..MM.*
0010h: 00 00 00 08 00 0B 01 0F 00 02 00 00 00 06 00 00  ................
0020h: 00 92 01 10 00 02 00 00 00 09 00 00 00 98 01 12  .’...........˜..
0030h: 00 03 00 00 00 01 00 06 00 00 01 1A 00 05 00 00  ................
0040h: 00 01 00 00 00 A2 01 1B 00 05 00 00 00 01 00 00  .....¢..........
0050h: 00 AA 01 28 00 03 00 00 00 01 00 02 00 00 01 31  .ª.(...........1
0060h: 00 02 00 00 00 07 00 00 00 B2 01 32 00 02 00 00  .........².2....
0070h: 00 14 00 00 00 BA 02 13 00 03 00 00 00 01 00 01  .....º..........
0080h: 00 00 87 69 00 04 00 00 00 01 00 00 00 CE 88 25  ..‡i.........Îˆ%
0090h: 00 04 00 00 00 01 00 00 07 AA 00 00 08 A4 41 70  .........ª...¤Ap
00A0h: 70 6C 65 00 69 50 68 6F 6E 65 20 37 00 00 00 00  ple.iPhone 7....
00B0h: 00 48 00 00 00 01 00 00 00 48 00 00 00 01 31 33  .H.......H....13
00C0h: 2E 33 2E 31 00 00 32 30 32 30 3A 30 32 3A 31 30  .3.1..2020:02:10
00D0h: 20 31 38 3A 31 39 3A 34 33 00 00 23 82 9A 00 05   18:19:43..#‚š..
00E0h: 00 00 00 01 00 00 02 78 82 9D 00 05 00 00 00 01  .......x‚.......
00F0h: 00 00 02 80 88 22 00 03 00 00 00 01 00 02 00 00  ...€ˆ"..........
0100h: 88 27 00 03 00 00 00 01 00 32 00 00 90 00 00 07  ˆ'.......2......
0110h: 00 00 00 04 30 32 33 31 90 03 00 02 00 00 00 14  ....0231........
0120h: 00 00 02 88 90 04 00 02 00 00 00 14 00 00 02 9C  ...ˆ...........œ
0130h: 90 10 00 02 00 00 00 07 00 00 02 B0 90 11 00 02  ...........°....
0140h: 00 00 00 07 00 00 02 B8 90 12 00 02 00 00 00 07  .......¸........
0150h: 00 00 02 C0 91 01 00 07 00 00 00 04 01 02 03 00  ...À‘...........
0160h: 92 01 00 0A 00 00 00 01 00 00 02 C8 92 02 00 05  ’..........È’...
0170h: 00 00 00 01 00 00 02 D0 92 03 00 0A 00 00 00 01  .......Ð’.......
0180h: 00 00 02 D8 92 04 00 0A 00 00 00 01 00 00 02 E0  ...Ø’..........à
0190h: 92 07 00 03 00 00 00 01 00 05 00 00 92 09 00 03  ’...........’...
```

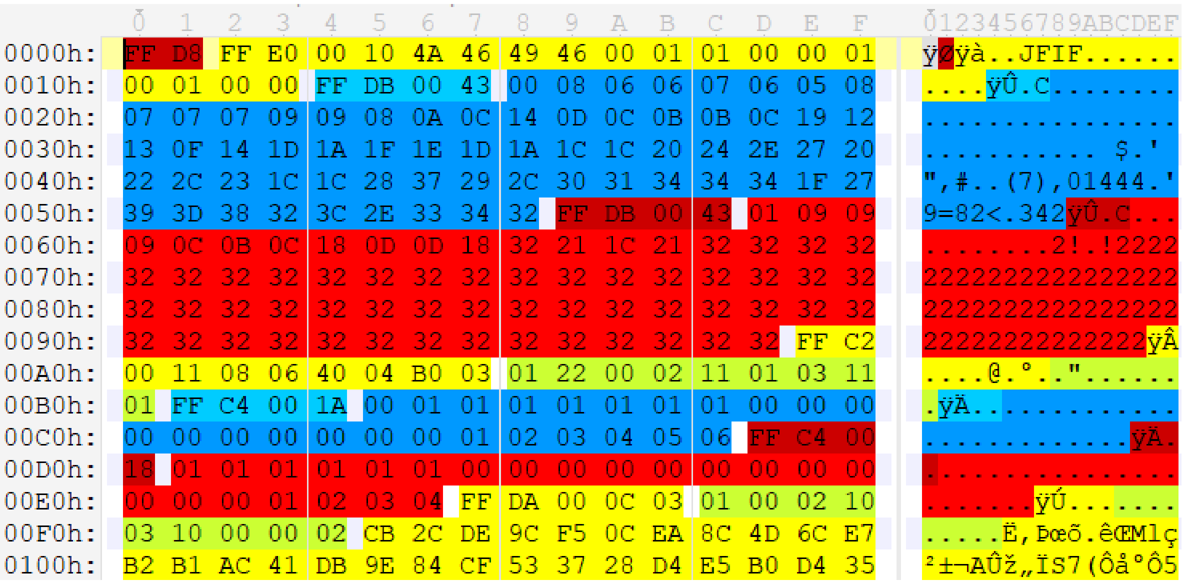
Figure 12: *File Signature for iPhone Image 1*



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FF D8 FF E1 AF B2 45 78 69 66 00 00 4D 4D 00 2A   ÿØÿá¯²Exif..MM.*
0010h: 00 00 00 08 00 0A 01 32 00 02 00 00 00 14 00 00   .......2........
0020h: 00 86 88 25 00 04 00 00 00 01 00 00 1A C2 01 10   .†ˆ%.........Â..
0030h: 00 02 00 00 00 08 00 00 00 9A 02 13 00 03 00 00   .........š......
0040h: 00 01 00 01 00 00 01 28 00 03 00 00 00 01 00 02   .......(........
0050h: 00 00 01 1B 00 05 00 00 00 01 00 00 00 A2 01 12   .............¢..
0060h: 00 03 00 00 00 01 00 01 00 00 87 69 00 04 00 00   ..........‡i....
0070h: 00 01 00 00 00 C1 01 1A 00 05 00 00 00 01 00 00   .....Á..........
0080h: 00 AA 01 0F 00 02 00 00 00 0F 00 00 00 B2 00 00   .ª...........²..
0090h: 1B 83 32 30 32 30 3A 30 32 3A 30 39 20 31 32 3A   .ƒ2020:02:09 12:
00A0h: 34 32 3A 30 39 00 4C 47 4C 53 39 39 32 00 00 00   42:09.LGLS992...
00B0h: 00 48 00 00 00 01 00 00 00 48 00 00 00 01 4C 47   .H.......H....LG
00C0h: 20 45 6C 65 63 74 72 6F 6E 69 63 73 00 00 1E A0    Electronics... 
00D0h: 01 00 03 00 00 00 01 00 01 00 00 82 9D 00 05 00   ...........‚....
00E0h: 00 00 01 00 00 02 2F 90 04 00 02 00 00 00 14 00   ....../.........
00F0h: 00 02 37 92 0A 00 05 00 00 00 01 00 00 02 4B A4   ..7’..........K¤
0100h: 02 00 03 00 00 00 01 00 00 00 00 92 92 00 02 00   ...........’’...
0110h: 00 00 07 00 00 02 53 A0 03 00 04 00 00 00 01 00   ......S ........
0120h: 00 0B AC A4 06 00 03 00 00 00 01 00 00 00 00 A3   ..¬¤...........£
0130h: 01 00 07 00 00 00 01 01 00 00 00 92 91 00 02 00   ...........’‘...
0140h: 00 00 07 00 00 02 5A A4 04 00 05 00 00 00 01 00   ......Z¤........
0150h: 00 02 61 88 22 00 03 00 00 00 01 00 00 00 00 A4   ..aˆ"..........¤
0160h: 03 00 03 00 00 00 01 00 00 00 00 A0 02 00 04 00   ........... ....
0170h: 00 00 01 00 00 14 C0 92 90 00 02 00 00 00 07 00   ......À’........
0180h: 00 02 69 92 01 00 0A 00 00 00 01 00 00 02 70 92   ..i’..........p’
0190h: 07 00 03 00 00 00 01 00 02 00 00 90 03 00 02 00   ................
```

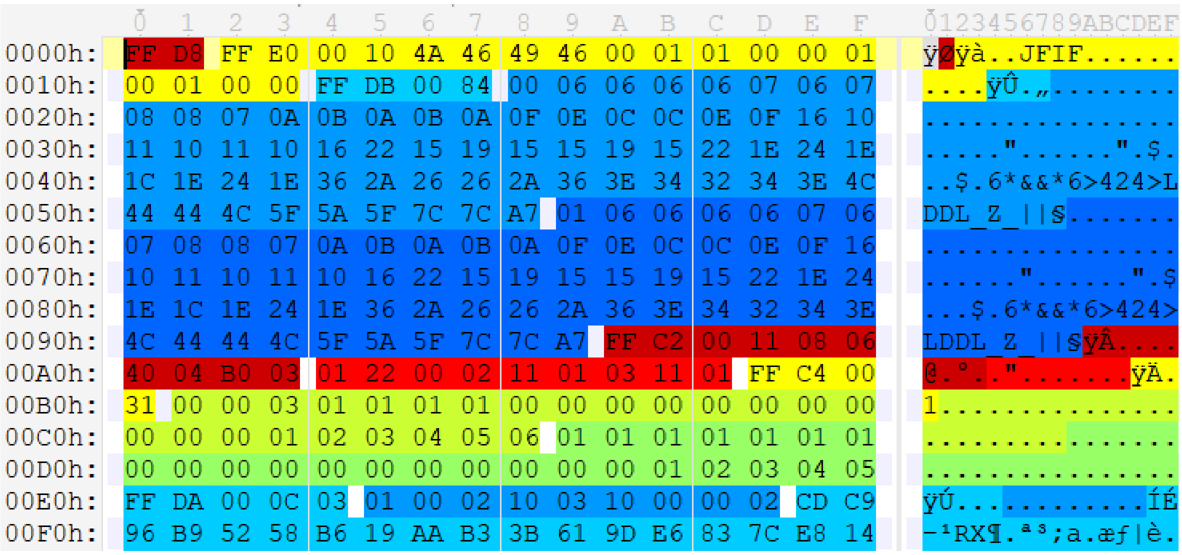
Figure 13: *File Signature for Android Image 1*

After these images were sent through WhatsApp and downloaded, the Exif tag was no longer displayed in the Hex data. Instead, images downloaded from WhatsApp Displayed the JPG JFIF file signature `FF D8 FF E0 00 10 4A 46 49 46 00 01.` Below are five examples of file headers of images downloaded from WhatsApp.



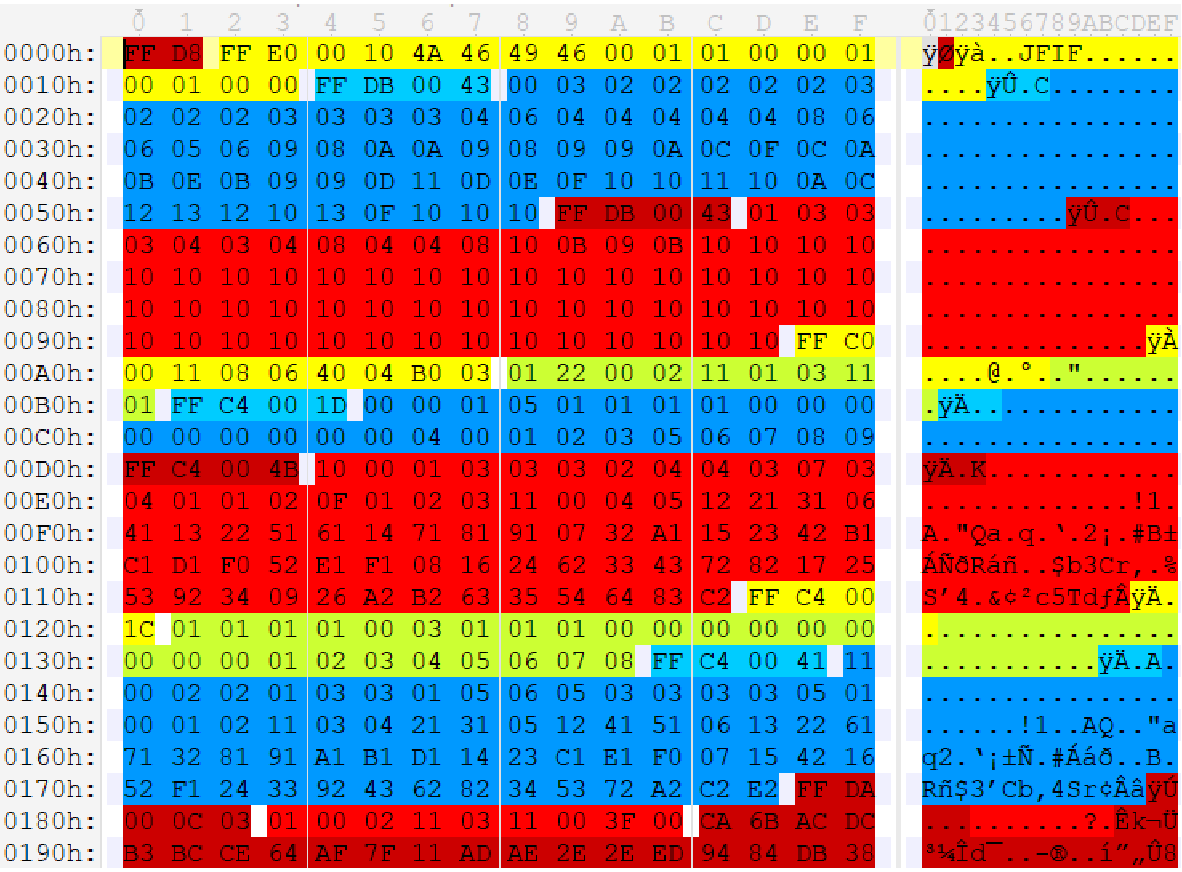
```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01   ÿØÿà..JFIF......
0010h: 00 01 00 00 FF DB 00 43 00 08 06 06 07 06 05 08   ....ÿÛ.C........
0020h: 07 07 07 09 09 08 0A 0C 14 0D 0C 0B 0B 0C 19 12   ................
0030h: 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20   ........... $.' 
0040h: 22 2C 23 1C 1C 28 37 29 2C 30 31 34 34 34 1F 27   ",#..(7),01444.'
0050h: 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09   9=82<.342ÿÛ.C...
0060h: 09 0C 0B 0C 18 0D 0D 18 32 21 1C 21 32 32 32 32   ........2!.!2222
0070h: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32   2222222222222222
0080h: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32   2222222222222222
0090h: 32 32 32 32 32 32 32 32 32 32 32 32 32 32 FF C2   22222222222222ÿÂ
00A0h: 00 11 08 06 40 04 B0 03 01 22 00 02 11 01 03 11   ....@.°.."......
00B0h: 01 FF C4 00 1A 00 01 01 01 01 01 01 01 00 00 00   .ÿÄ.............
00C0h: 00 00 00 00 00 00 00 01 02 03 04 05 06 FF C4 00   .............ÿÄ.
00D0h: 18 01 01 01 01 01 01 00 00 00 00 00 00 00 00 00   ................
00E0h: 00 00 00 01 02 03 04 FF DA 00 0C 03 01 00 02 10   .......ÿÚ.......
00F0h: 03 10 00 00 02 CB 2C DE 9C F5 0C EA 8C 4D 6C E7   .....Ë,Þœõ.êŒMlç
0100h: B2 B1 AC 41 DB 9E 84 CF 53 37 28 D4 E5 B0 D4 35   ²±¬AÛž„ÏS7(Ôå°Ô5
```

Figure 14: *File Header of .jpg File Sent Over WhatsApp via iPhone*



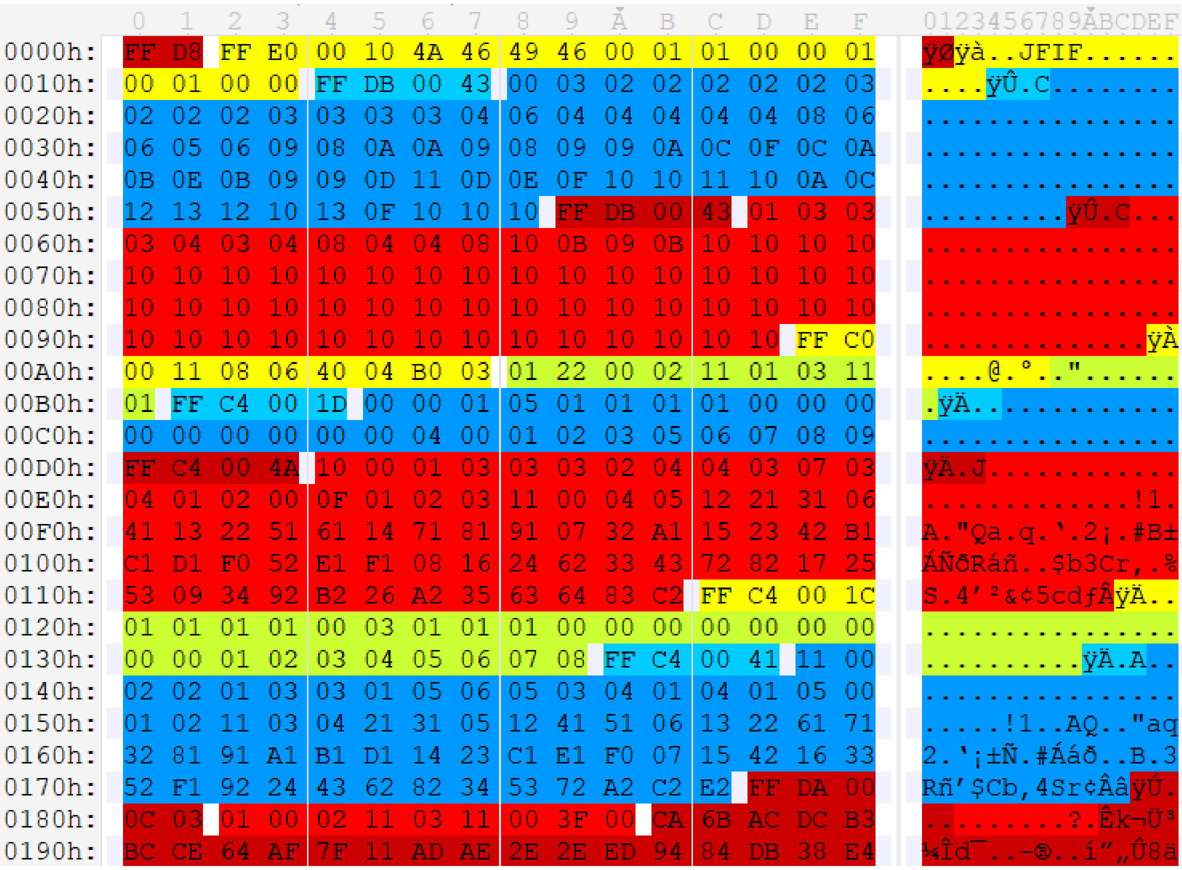
```
       0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01   ÿØÿà..JFIF......
0010h: 00 01 00 00 FF DB 00 84 00 06 06 06 06 07 06 07   ....ÿÛ.„........
0020h: 08 08 07 0A 0B 0A 0B 0A 0F 0E 0C 0C 0E 0F 16 10   ................
0030h: 11 10 11 10 16 22 15 19 15 15 19 15 22 1E 24 1E   ....."......".$.
0040h: 1C 1E 24 1E 36 2A 26 26 2A 36 3E 34 32 34 3E 4C   ..$.6*&&*6>424>L
0050h: 44 44 4C 5F 5A 5F 7C 7C A7 01 06 06 06 06 07 06   DDL_Z_||§.......
0060h: 07 08 08 07 0A 0B 0A 0B 0A 0F 0E 0C 0C 0E 0F 16   ................
0070h: 10 11 10 11 10 16 22 15 19 15 15 19 15 22 1E 24   ......"......".$
0080h: 1E 1C 1E 24 1E 36 2A 26 26 2A 36 3E 34 32 34 3E   ...$.6*&&*6>424>
0090h: 4C 44 44 4C 5F 5A 5F 7C 7C A7 FF C2 00 11 08 06   LDDL_Z_||§ÿÂ....
00A0h: 40 04 B0 03 01 22 00 02 11 01 03 11 01 FF C4 00   @.°..".......ÿÄ.
00B0h: 31 00 00 03 01 01 01 01 00 00 00 00 00 00 00 00   1...............
00C0h: 00 00 00 01 02 03 04 05 06 01 01 01 01 01 01 01   ................
00D0h: 00 00 00 00 00 00 00 00 00 00 00 01 02 03 04 05   ................
00E0h: FF DA 00 0C 03 01 00 02 10 03 10 00 00 02 CD C9   ÿÚ............ÍÉ
00F0h: 96 B9 52 58 B6 19 AA B3 3B 61 9D E6 83 7C E8 14   –¹RX¶.ª³;a.æƒ|è.
```

Figure 15: *File Header of .jpg File Sent Over WhatsApp via Android*



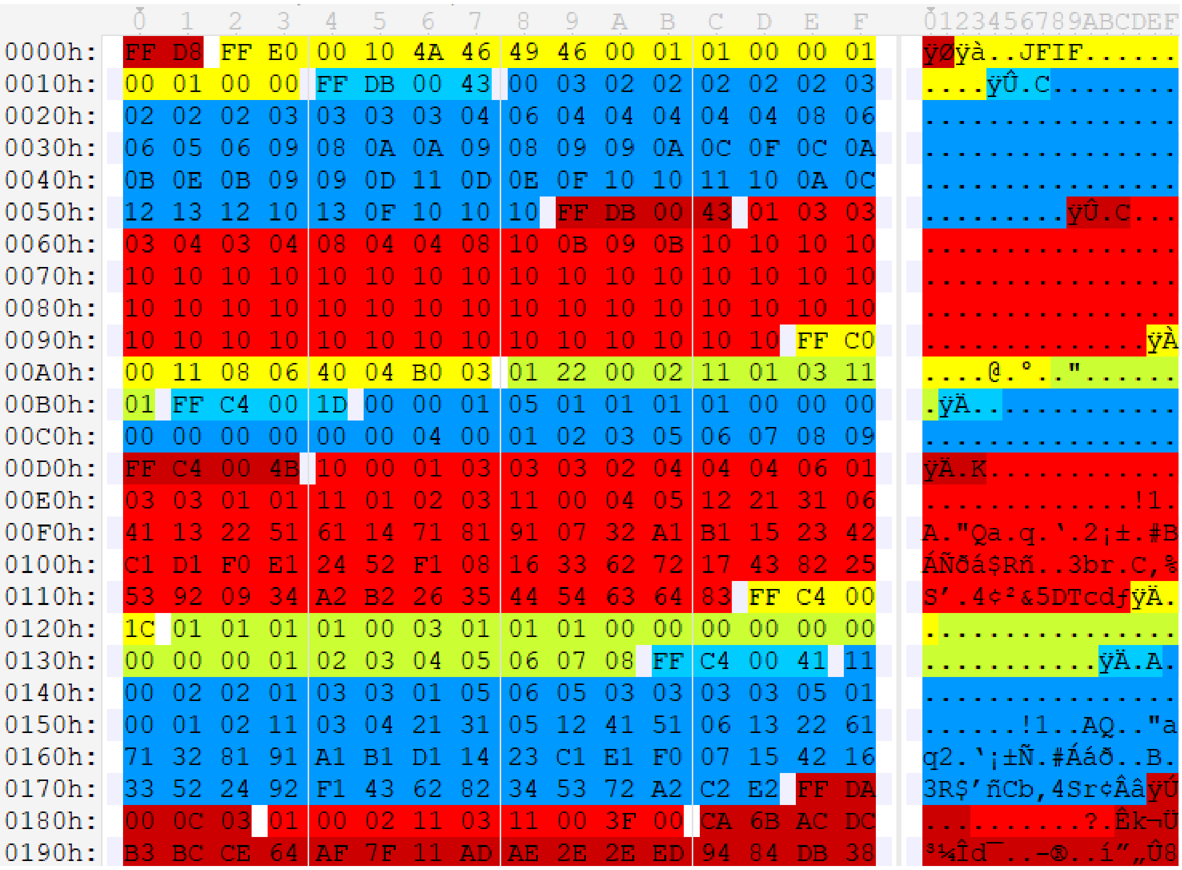
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 01  ÿØÿà..JFIF......
0010h: 00 01 00 00 FF DB 00 43 00 03 02 02 02 02 02 03  ....ÿÛ.C........
0020h: 02 02 02 03 03 03 03 04 06 04 04 04 04 04 08 06  ................
0030h: 06 05 06 09 08 0A 0A 09 08 09 09 0A 0C 0F 0C 0A  ................
0040h: 0B 0E 0B 09 09 0D 11 0D 0E 0F 10 10 11 10 0A 0C  ................
0050h: 12 13 12 10 13 0F 10 10 10 FF DB 00 43 01 03 03  .........ÿÛ.C...
0060h: 03 04 03 04 08 04 04 08 10 0B 09 0B 10 10 10 10  ................
0070h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10  ................
0080h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10  ................
0090h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 FF C0  ..............ÿÀ
00A0h: 00 11 08 06 40 04 B0 03 01 22 00 02 11 01 03 11  ....@.°.."......
00B0h: 01 FF C4 00 1D 00 00 01 05 01 01 01 01 00 00 00  .ÿÄ.............
00C0h: 00 00 00 00 00 00 04 00 01 02 03 05 06 07 08 09  ................
00D0h: FF C4 00 4B 10 00 01 03 03 03 02 04 04 03 07 03  ÿÄ.K............
00E0h: 04 01 01 02 0F 01 02 03 11 00 04 05 12 21 31 06  .............!1.
00F0h: 41 13 22 51 61 14 71 81 91 07 32 A1 15 23 42 B1  A."Qa.q.'.2¡.#B±
0100h: C1 D1 F0 52 E1 F1 08 16 24 62 33 43 72 82 17 25  ÁÑðRáñ..$b3Cr,.%
0110h: 53 92 34 09 26 A2 B2 63 35 54 64 83 C2 FF C4 00  S'4.&¢²c5TdƒÂÿÄ.
0120h: 1C 01 01 01 01 00 03 01 01 01 00 00 00 00 00 00  ................
0130h: 00 00 00 01 02 03 04 05 06 07 08 FF C4 00 41 11  ...........ÿÄ.A.
0140h: 00 02 02 01 03 03 01 05 06 05 03 03 03 03 05 01  ................
0150h: 00 01 02 11 03 04 21 31 05 12 41 51 06 13 22 61  ......!1..AQ.."a
0160h: 71 32 81 91 A1 B1 D1 14 23 C1 E1 F0 07 15 42 16  q2.'¡±Ñ.#Ááð..B.
0170h: 52 F1 24 33 92 43 62 82 34 53 72 A2 C2 E2 FF DA  Rñ$3'Cb,4Sr¢ÂâÿÚ
0180h: 00 0C 03 01 00 02 11 03 11 00 3F 00 CA 6B AC DC  ..........?.Êk¬Ü
0190h: B3 BC CE 64 AF 7F 11 AD AE 2E 2E ED 94 84 DB 38  ³¼Îd¯..-®..í",Û8
```

Figure 16: *File Header of .jpg File Sent Over WhatsApp via Windows Application*



```
        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 01 00 00 01  ÿØÿà..JFIF......
0010h: 00 01 00 00 FF DB 00 43 00 03 02 02 02 02 02 03  ....ÿÛ.C........
0020h: 02 02 02 03 03 03 03 04 06 04 04 04 04 04 08 06  ................
0030h: 06 05 06 09 08 0A 0A 09 08 09 09 0A 0C 0F 0C 0A  ................
0040h: 0B 0E 0B 09 09 0D 11 0D 0E 0F 10 10 11 10 0A 0C  ................
0050h: 12 13 12 10 13 0F 10 10 10 FF DB 00 43 01 03 03  .........ÿÛ.C...
0060h: 03 04 03 04 08 04 04 08 10 0B 09 0B 10 10 10 10  ................
0070h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10  ................
0080h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10  ................
0090h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 FF C0  ..............ÿÀ
00A0h: 00 11 08 06 40 04 B0 03 01 22 00 02 11 01 03 11  ....@.°.."......
00B0h: 01 FF C4 00 1D 00 00 01 05 01 01 01 01 00 00 00  .ÿÄ.............
00C0h: 00 00 00 00 00 00 04 00 01 02 03 05 06 07 08 09  ................
00D0h: FF C4 00 4A 10 00 01 03 03 03 02 04 04 03 07 03  ÿÄ.J............
00E0h: 04 01 02 00 0F 01 02 03 11 00 04 05 12 21 31 06  .............!1.
00F0h: 41 13 22 51 61 14 71 81 91 07 32 A1 15 23 42 B1  A."Qa.q.‘.2¡.#B±
0100h: C1 D1 F0 52 E1 F1 08 16 24 62 33 43 72 82 17 25  ÁÑðRáñ..$b3Cr,.%
0110h: 53 09 34 92 B2 26 A2 35 63 64 83 C2 FF C4 00 1C  S.4’²&¢5cdƒÂÿÄ..
0120h: 01 01 01 01 00 03 01 01 01 00 00 00 00 00 00 00  ................
0130h: 00 00 01 02 03 04 05 06 07 08 FF C4 00 41 11 00  ..........ÿÄ.A..
0140h: 02 02 01 03 03 01 05 06 05 03 04 01 04 01 05 00  ................
0150h: 01 02 11 03 04 21 31 05 12 41 51 06 13 22 61 71  .....!1..AQ.."aq
0160h: 32 81 91 A1 B1 D1 14 23 C1 E1 F0 07 15 42 16 33  2.‘¡±Ñ.#Ááð..B.3
0170h: 52 F1 92 24 43 62 82 34 53 72 A2 C2 E2 FF DA 00  Rñ’$Cb,4Sr¢ÂâÿÚ.
0180h: 0C 03 01 00 02 11 03 11 00 3F 00 CA 6B AC DC B3  ..........?.Êk¬Ü³
0190h: BC CE 64 AF 7F 11 AD AE 2E 2E ED 94 84 DB 38 E4  ¼Îd¯..-®..í”„Û8ä
```

Figure 17: *File Header of .jpg File Sent Over WhatsApp via MacOS Application*



```
        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 01 00 00 01   ÿØÿà..JFIF......
0010h: 00 01 00 00 FF DB 00 43 00 03 02 02 02 02 02 03   ....ÿÛ.C........
0020h: 02 02 02 03 03 03 03 04 06 04 04 04 04 04 08 06   ................
0030h: 06 05 06 09 08 0A 0A 09 08 09 09 0A 0C 0F 0C 0A   ................
0040h: 0B 0E 0B 09 09 0D 11 0D 0E 0F 10 10 11 10 0A 0C   ................
0050h: 12 13 12 10 13 0F 10 10 10 FF DB 00 43 01 03 03   .........ÿÛ.C...
0060h: 03 04 03 04 08 04 04 08 10 0B 09 0B 10 10 10 10   ................
0070h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10   ................
0080h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10   ................
0090h: 10 10 10 10 10 10 10 10 10 10 10 10 10 10 FF C0   ..............ÿÀ
00A0h: 00 11 08 06 40 04 B0 03 01 22 00 02 11 01 03 11   ....@.°.."......
00B0h: 01 FF C4 00 1D 00 00 01 05 01 01 01 01 00 00 00   .ÿÄ.............
00C0h: 00 00 00 00 00 00 04 00 01 02 03 05 06 07 08 09   ................
00D0h: FF C4 00 4B 10 00 01 03 03 03 02 04 04 04 06 01   ÿÄ.K............
00E0h: 03 03 01 01 11 01 02 03 11 00 04 05 12 21 31 06   .............!1.
00F0h: 41 13 22 51 61 14 71 81 91 07 32 A1 B1 15 23 42   A."Qa.q.‘.2¡±.#B
0100h: C1 D1 F0 E1 24 52 F1 08 16 33 62 72 17 43 82 25   ÁÑðá$Rñ..3br.C‚%
0110h: 53 92 09 34 A2 B2 26 35 44 54 63 64 83 FF C4 00   S’.4¢²&5DTcdƒÿÄ.
0120h: 1C 01 01 01 01 00 03 01 01 01 00 00 00 00 00 00   ................
0130h: 00 00 00 01 02 03 04 05 06 07 08 FF C4 00 41 11   ...........ÿÄ.A.
0140h: 00 02 02 01 03 03 01 05 06 05 03 03 03 03 05 01   ................
0150h: 00 01 02 11 03 04 21 31 05 12 41 51 06 13 22 61   ......!1..AQ.."a
0160h: 71 32 81 91 A1 B1 D1 14 23 C1 E1 F0 07 15 42 16   q2.‘¡±Ñ.#Ááð..B.
0170h: 33 52 24 92 F1 43 62 82 34 53 72 A2 C2 E2 FF DA   3R$’ñCb‚4Sr¢ÂâÿÚ
0180h: 00 0C 03 01 00 02 11 03 11 00 3F 00 CA 6B AC DC   ..........?.Êk¬Ü
0190h: B3 BC CE 64 AF 7F 11 AD AE 2E 2E ED 94 84 DB 38   ³¼Îd¯..-®..í”„Û8
```

Figure 18: *File Header of .jpg File Sent Over WhatsApp via Web Application*

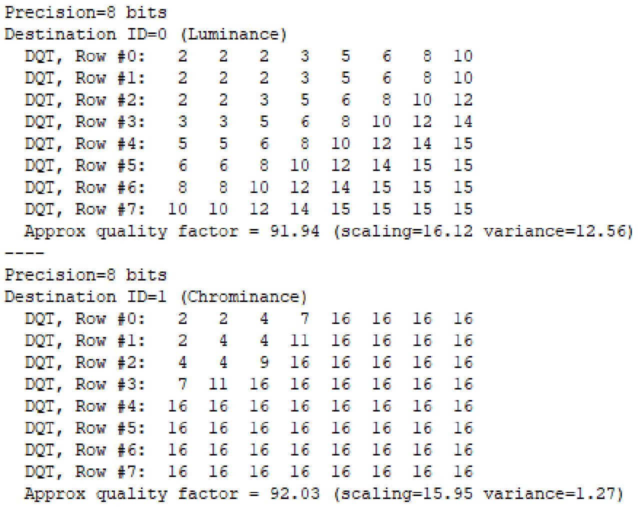
As visualized, header information is different for images sent via iPhone as opposed to images sent via Android. However, images sent via the WhatsApp application on Windows 10, MacOS, or the WhatsApp web applications have extremely similar header information with practically all the differences between those files residing in the actual image data stream.

Baseline JPEG vs. Progressive JPEG

Images were inputted into ExifTool to observe if they were compressed with Baseline or Progressive encoding. Original images captured on iPhone or Android mobile devices were compressed with Baseline DCT encoding. Images sent over WhatsApp via an iPhone or Android device were compressed and displayed with Progressive DCT encoding. This was apparent in the WhatsApp application. As these images downloaded and were being decoded, a blurry version of the image was displayed in its entirety before the download was completed. When images were sent via the Windows 10, MacOS, or WhatsApp Web Application, the images were compressed with Baseline DCT encoding.

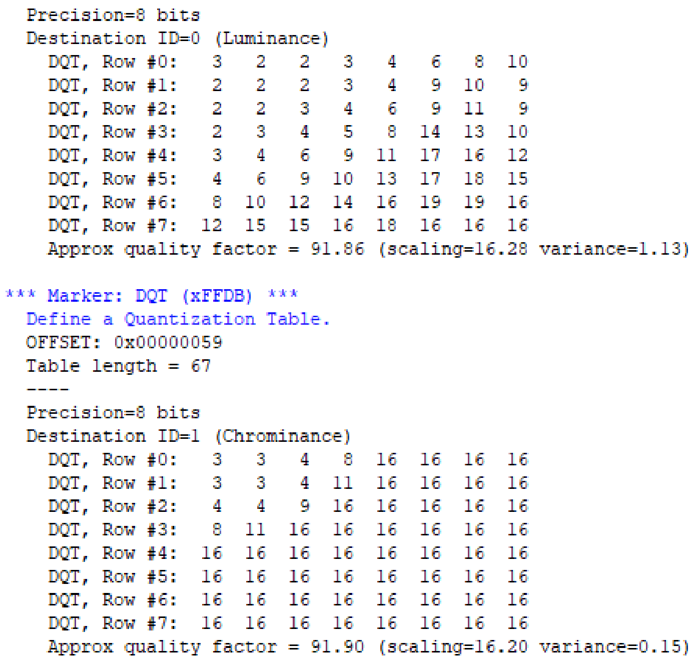
Quantization Tables

Images were inputted into JPEG Snoop to observe quantization tables and quality factors. Images sent via the Windows, MacOS, or WhatsApp Web Applications all had the same quality factor identified. The level of compression applied by WhatsApp when images were sent using a desktop application is similar to the level of compression applied to the original iPhone images and is a relatively low level of compression when compared to images downloaded from WhatsApp that were sent over mobile devices.



```
Precision=8 bits
Destination ID=0 (Luminance)
  DQT, Row #0:   2   2   2   3   5   6   8  10
  DQT, Row #1:   2   2   2   3   5   6   8  10
  DQT, Row #2:   2   2   3   5   6   8  10  12
  DQT, Row #3:   3   3   5   6   8  10  12  14
  DQT, Row #4:   5   5   6   8  10  12  14  15
  DQT, Row #5:   6   6   8  10  12  14  15  15
  DQT, Row #6:   8   8  10  12  14  15  15  15
  DQT, Row #7:  10  10  12  14  15  15  15  15
  Approx quality factor = 91.94 (scaling=16.12 variance=12.56)
----
Precision=8 bits
Destination ID=1 (Chrominance)
  DQT, Row #0:   2   2   4   7  16  16  16  16
  DQT, Row #1:   2   4   4  11  16  16  16  16
  DQT, Row #2:   4   4   9  16  16  16  16  16
  DQT, Row #3:   7  11  16  16  16  16  16  16
  DQT, Row #4:  16  16  16  16  16  16  16  16
  DQT, Row #5:  16  16  16  16  16  16  16  16
  DQT, Row #6:  16  16  16  16  16  16  16  16
  DQT, Row #7:  16  16  16  16  16  16  16  16
  Approx quality factor = 92.03 (scaling=15.95 variance=1.27)
```

Figure 19: *Quantization Tables and Quality Factor of Original iPhone Image*

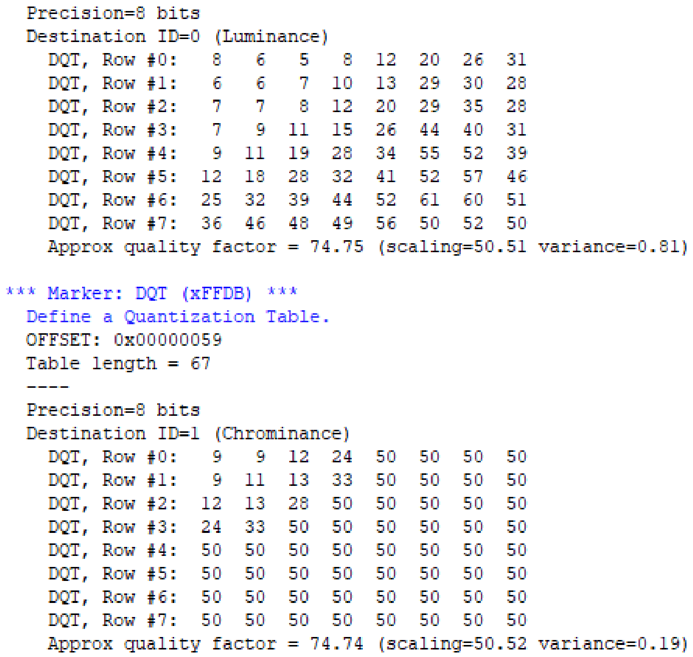


```
  Precision=8 bits
  Destination ID=0 (Luminance)
    DQT, Row #0:   3   2   2   3   4   6   8  10
    DQT, Row #1:   2   2   2   3   4   9  10   9
    DQT, Row #2:   2   2   3   4   6   9  11   9
    DQT, Row #3:   2   3   4   5   8  14  13  10
    DQT, Row #4:   3   4   6   9  11  17  16  12
    DQT, Row #5:   4   6   9  10  13  17  18  15
    DQT, Row #6:   8  10  12  14  16  19  19  16
    DQT, Row #7:  12  15  15  16  18  16  16  16
    Approx quality factor = 91.86 (scaling=16.28 variance=1.13)

*** Marker: DQT (xFFDB) ***
  Define a Quantization Table.
  OFFSET: 0x00000059
  Table length = 67
  ----
  Precision=8 bits
  Destination ID=1 (Chrominance)
    DQT, Row #0:   3   3   4   8  16  16  16  16
    DQT, Row #1:   3   3   4  11  16  16  16  16
    DQT, Row #2:   4   4   9  16  16  16  16  16
    DQT, Row #3:   8  11  16  16  16  16  16  16
    DQT, Row #4:  16  16  16  16  16  16  16  16
    DQT, Row #5:  16  16  16  16  16  16  16  16
    DQT, Row #6:  16  16  16  16  16  16  16  16
    DQT, Row #7:  16  16  16  16  16  16  16  16
    Approx quality factor = 91.90 (scaling=16.20 variance=0.15)
```

Figure 20: *Quantization Tables and Quality Factor of Image Sent Over WhatsApp via Windows Application*

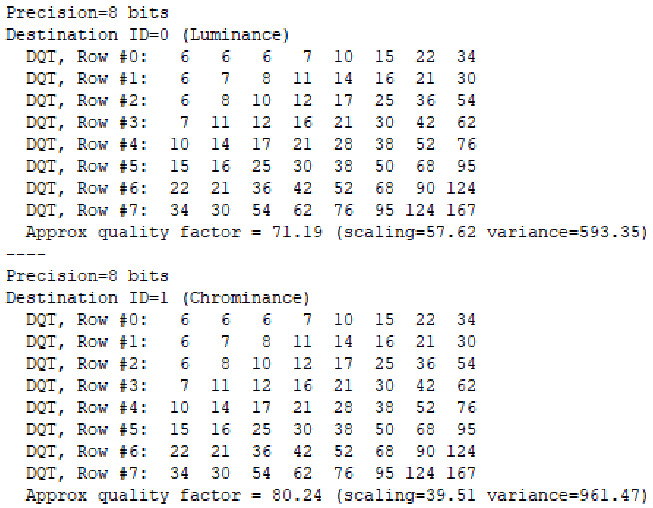
Images sent over the mobile WhatsApp application had more aggressive compression applied to them as indicated by higher numbers in the quantization tables and lower quality factors identified.



```
  Precision=8 bits
  Destination ID=0 (Luminance)
    DQT, Row #0:   8   6   5   8  12  20  26  31
    DQT, Row #1:   6   6   7  10  13  29  30  28
    DQT, Row #2:   7   7   8  12  20  29  35  28
    DQT, Row #3:   7   9  11  15  26  44  40  31
    DQT, Row #4:   9  11  19  28  34  55  52  39
    DQT, Row #5:  12  18  28  32  41  52  57  46
    DQT, Row #6:  25  32  39  44  52  61  60  51
    DQT, Row #7:  36  46  48  49  56  50  52  50
    Approx quality factor = 74.75 (scaling=50.51 variance=0.81)

*** Marker: DQT (xFFDB) ***
  Define a Quantization Table.
  OFFSET: 0x00000059
  Table length = 67
  ----
  Precision=8 bits
  Destination ID=1 (Chrominance)
    DQT, Row #0:   9   9  12  24  50  50  50  50
    DQT, Row #1:   9  11  13  33  50  50  50  50
    DQT, Row #2:  12  13  28  50  50  50  50  50
    DQT, Row #3:  24  33  50  50  50  50  50  50
    DQT, Row #4:  50  50  50  50  50  50  50  50
    DQT, Row #5:  50  50  50  50  50  50  50  50
    DQT, Row #6:  50  50  50  50  50  50  50  50
    DQT, Row #7:  50  50  50  50  50  50  50  50
    Approx quality factor = 74.74 (scaling=50.52 variance=0.19)
```

Figure 21: *Quantization Tables and Quality Factor of Image Sent Over the iPhone WhatsApp Application*



```
Precision=8 bits
Destination ID=0 (Luminance)
  DQT, Row #0:   6   6   6   7  10  15  22  34
  DQT, Row #1:   6   7   8  11  14  16  21  30
  DQT, Row #2:   6   8  10  12  17  25  36  54
  DQT, Row #3:   7  11  12  16  21  30  42  62
  DQT, Row #4:  10  14  17  21  28  38  52  76
  DQT, Row #5:  15  16  25  30  38  50  68  95
  DQT, Row #6:  22  21  36  42  52  68  90 124
  DQT, Row #7:  34  30  54  62  76  95 124 167
  Approx quality factor = 71.19 (scaling=57.62 variance=593.35)
----
Precision=8 bits
Destination ID=1 (Chrominance)
  DQT, Row #0:   6   6   6   7  10  15  22  34
  DQT, Row #1:   6   7   8  11  14  16  21  30
  DQT, Row #2:   6   8  10  12  17  25  36  54
  DQT, Row #3:   7  11  12  16  21  30  42  62
  DQT, Row #4:  10  14  17  21  28  38  52  76
  DQT, Row #5:  15  16  25  30  38  50  68  95
  DQT, Row #6:  22  21  36  42  52  68  90 124
  DQT, Row #7:  34  30  54  62  76  95 124 167
  Approx quality factor = 80.24 (scaling=39.51 variance=961.47)
```

Figure 22: *Quantization Tables and Quality Factor of Image Sent Over the Android WhatsApp Application*

Lossy Compression Analysis

For the audio portion of this study, the 20 recordings previously mentioned were sent through WhatsApp. After the audio recordings were sent through WhatsApp and then downloaded, a Lossy Compression Analysis was conducted, and the recordings compression levels were compared to a database of compression profiles of other devices.

For the recordings that were recorded with the "Compressed" setting enabled, the Apple Voice Memos compression profile was detected.

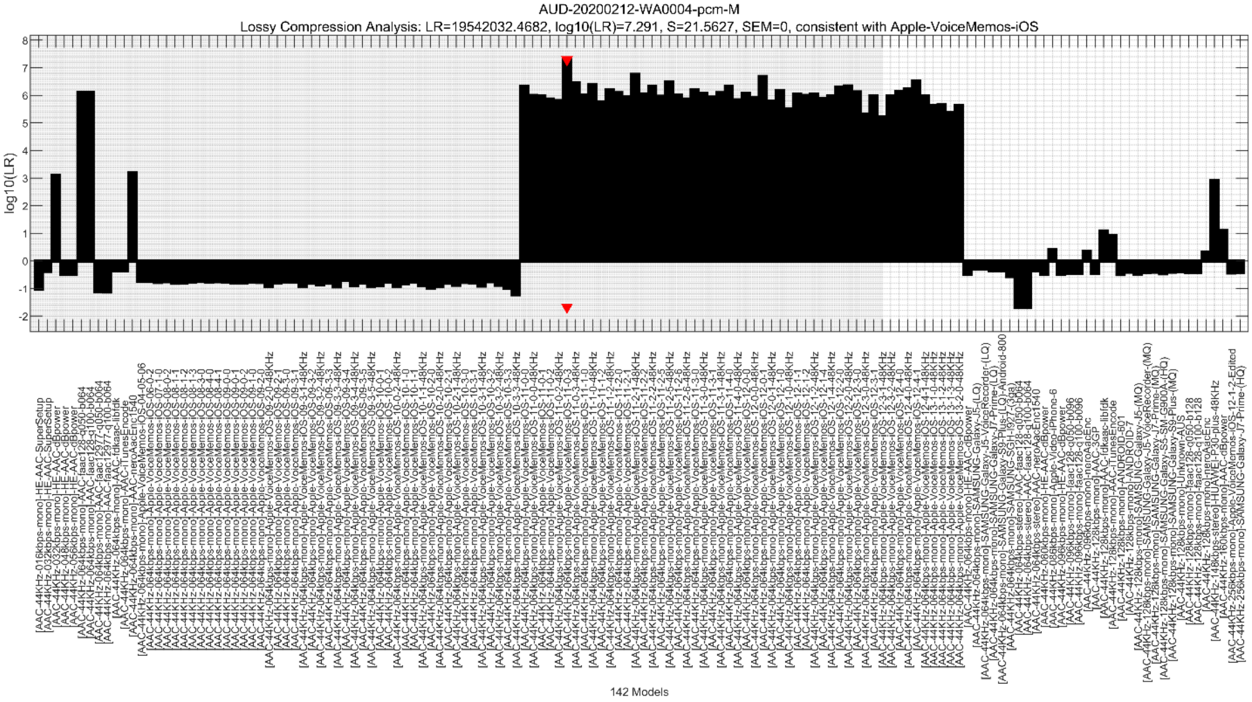


Figure 23: *Lossy Compression Analysis Results of an Audio File Recorded With the "Compressed" Setting in the Apple Voice Memos Application Enabled and Sent Through WhatsApp*

For recordings that were recorded with the "Lossless" setting enabled, the initial results of Lossy Compression Analysis were inconclusive. It was determined that longer recordings with an approximate length of between fifteen and twenty minutes should be sent through WhatsApp and downloaded to configure the database. Ten new audio recordings were recorded in the Apple Voice Memos application with the "Lossless" setting enabled and sent through WhatsApp. These recordings were downloaded from WhatsApp and used to create a WhatsApp audio compression profile.

After configuring the Lossy Compression Analysis database with the longer files initially recorded with lossless compression and then sent through WhatsApp, the lossy compression applied by WhatsApp was able to be observed and verified. When the ten shorter recordings recorded with the lossless setting in Apple Voice memos enabled were compared to the database, the WhatsApp compression was detected.

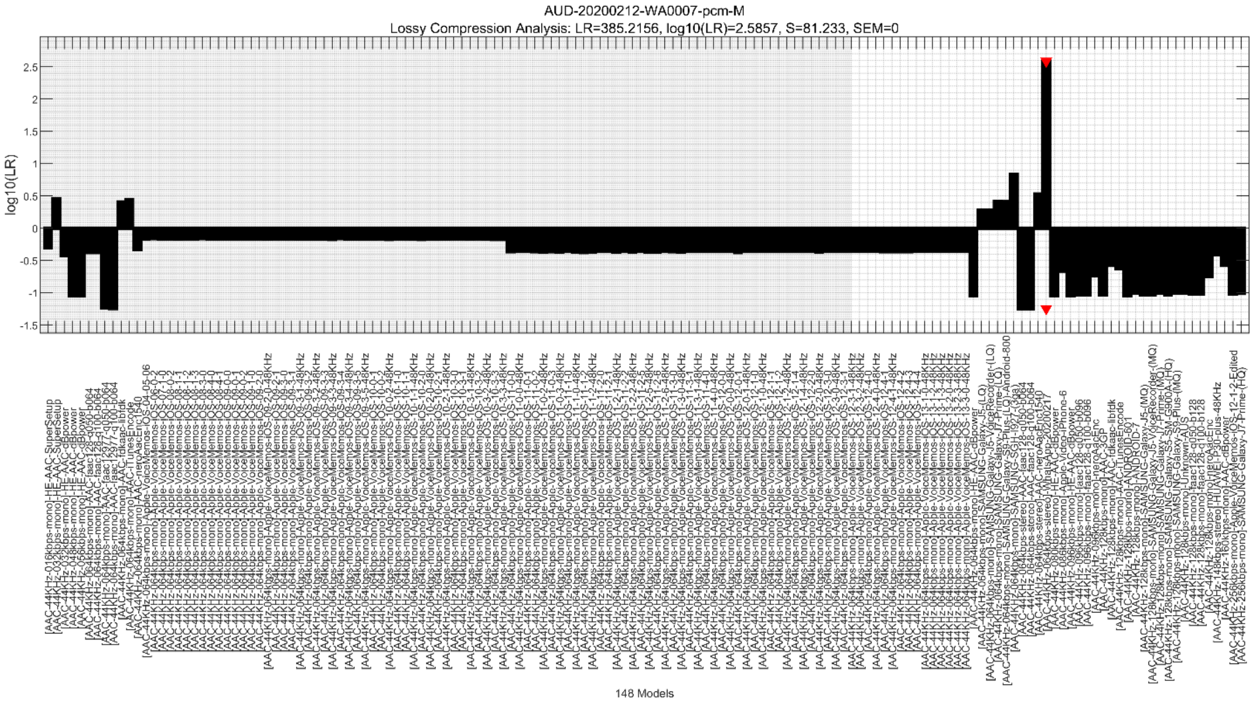
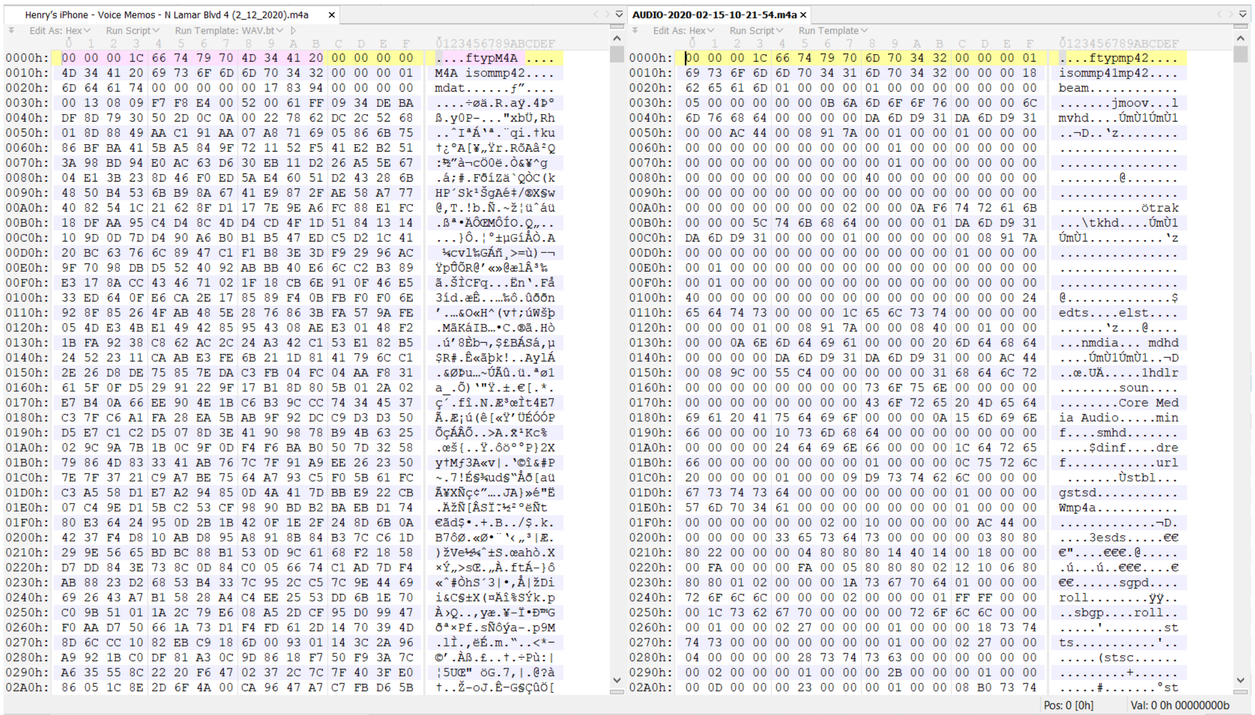


Figure 24: *Lossy Compression Analysis Results of an Audio File Recorded With the "Lossless" Setting in the Apple Voice Memos Application Enabled and Sent Through WhatsApp*

Hex Data (Audio)

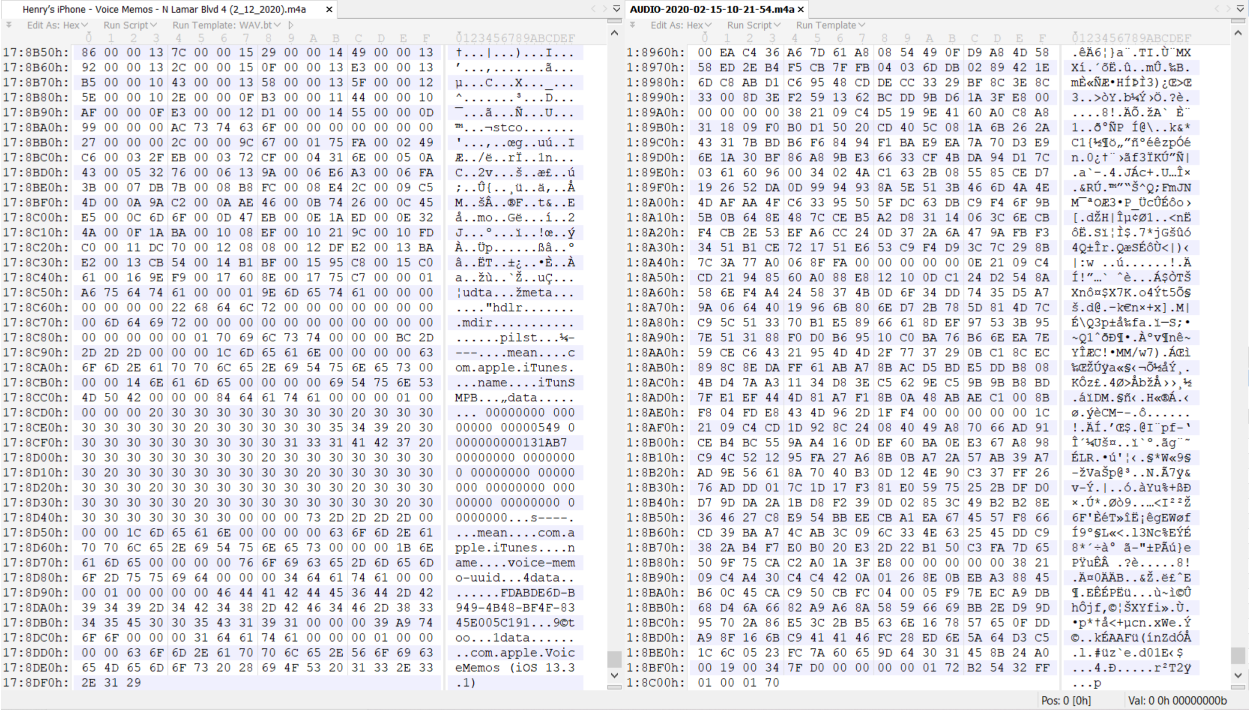
Hex data analysis and observations of the audio files examined in this study was conducted using 010 Editor. Original audio recordings were recorded with the lossless setting enabled. In the original recordings, file metadata is mainly contained in the footer of the file after the core audio data. After the WhatsApp compression, metadata is no longer seen in the footer of the file, but rather written in the header of the file before the core audio data. After the WhatsApp compression, ASCII strings associated with the iPhone are no longer seen. When viewed in ExifTool, metadata identifying Apple and iPhone as the encoder is also no longer visible after the WhatsApp compression.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 00 00 00 1C 66 74 79 70 4D 34 41 20 00 00 00 00  ....ftypM4A ....
0010h: 4D 34 41 20 69 73 6F 6D 6D 70 34 32 00 00 00 01  M4A isommp42....
0020h: 6D 64 61 74 00 00 00 00 00 17 83 94 00 00 00 00  mdat......ƒ”....
0030h: 00 13 08 09 F7 F8 E4 00 52 00 61 FF 09 34 DE BA  ....÷øä.R.aÿ.4Þº
0040h: DF 8D 79 30 50 2D 0C 0A 00 22 78 62 DC 2C 52 68  ß.y0P-..."xbÜ,Rh
0050h: 01 8D 88 49 AA C1 91 AA 07 A8 71 69 05 86 6B 75  ..ˆIªÁ‘ª.¨qi.†ku
0060h: 86 BF BA 41 5B A5 84 9F 72 11 52 F5 41 E2 B2 51  †¿ºA[¥„Ÿr.RõAâ²Q
0070h: 3A 98 BD 94 E0 AC 63 D6 30 EB 11 D2 26 A5 5E 67  :˜½”à¬cÖ0ë.Ò&¥^g
0080h: 04 E1 3B 23 8D 46 F0 ED 5A E4 60 51 D2 43 28 6B  .á;#.FðíZä`QÒC(k
0090h: 48 50 B4 53 6B B9 8A 67 41 E9 87 2F AE 58 A7 77  HP´Sk¹ŠgAé‡/®X§w
00A0h: 40 82 54 1C 21 62 8F D1 17 7E 9E A6 FC 88 E1 FC  @‚T.!b.Ñ.~ž¦üˆáü
00B0h: 18 DF AA 95 C4 D4 8C 4D D4 CD 4F 1D 51 84 13 14  .ßª•ÄÔŒMÔÍO.Q„..
00C0h: 10 9D 0D 7D D4 90 A6 B0 B1 B5 47 ED C5 D2 1C 41  ...}Ô.¦°±µGíÅÒ.A
00D0h: 20 BC 63 76 6C 89 47 C1 F1 B8 3E 3D F9 29 96 AC   ¼cvl‰GÁñ¸>=ù)–¬
00E0h: 9F 70 98 DB D5 52 40 92 AB BB 40 E6 6C C2 B3 89  Ÿp˜ÛÕR@’«»@ælÂ³‰
00F0h: E3 17 8A CC 43 46 71 02 1F 18 CB 6E 91 0F 46 E5  ã.ŠÌCFq...Ën‘.Få
0100h: 33 ED 64 0F E6 CA 2E 17 85 89 F4 0B FB F0 F0 6E  3íd.æÊ..…‰ô.ûððn
0110h: 92 8F 85 26 4F AB 48 5E 28 76 86 3B FA 57 9A FE  ’.…&O«H^(v†;úWšþ
0120h: 05 4D E3 4B E1 49 42 85 95 43 08 AE E3 01 48 F2  .MãKáIB…•C.®ã.Hò
0130h: 1B FA 92 38 C8 62 AC 2C 24 A3 42 C1 53 E1 82 B5  .ú’8Èb¬,$£BÁSá‚µ
0140h: 24 52 23 11 CA AB E3 FE 6B 21 1D 81 41 79 6C C1  $R#.Ê«ãþk!..AylÁ
0150h: 2E 26 D8 DE 75 85 7E DA C3 FB 04 FC 04 AA F8 31  .&ØÞu…~ÚÃû.ü.ªø1
0160h: 61 5F 0F D5 29 91 22 9F 17 B1 8D 80 5B 01 2A 02  a_.Õ)‘"Ÿ.±.€[.*.
0170h: E7 B4 0A 66 EE 90 4E 1B C6 B3 9C CC 74 34 45 37  ç´.fî.N.Æ³œÌt4E7
0180h: C3 7F C6 A1 FA 28 EA 5B AB 9F 92 DC C9 D3 D3 50  Ã.Æ¡ú(ê[«Ÿ’ÜÉÓÓP
0190h: D5 E7 C1 C2 D5 07 8D 3E 41 90 98 78 B9 4B 63 25  ÕçÁÂÕ..>A.˜x¹Kc%
01A0h: 02 9C 9A 7B 1B 0C 9F 0D F4 F6 BA B0 50 7D 32 58  .œš{..Ÿ.ôöº°P}2X
01B0h: 79 86 4D 83 33 41 AB 76 7C 7F 91 A9 EE 26 23 50  y†Mƒ3A«v|.‘©î&#P
01C0h: 7E 7F 37 21 C9 A7 BE 75 64 A7 93 C5 F0 5B 61 FC  ~.7!É§¾ud§“Åð[aü
01D0h: C3 A5 58 D1 E7 A2 94 85 0D 4A 41 7D BB E9 22 CB  Ã¥XÑç¢”….JA}»é"Ë
01E0h: 07 C4 9E D1 5B C2 53 CF 98 90 BD B2 BA EB D1 74  .ÄžÑ[ÂSÏ˜.½²ºëÑt
01F0h: 80 E3 64 24 95 0D 2B 1B 42 0F 1E 2F 24 8D 6B 0A  €ãd$•.+.B../$.k.
0200h: 42 37 F4 D8 10 AB D8 95 A8 91 8B 84 B3 7C C6 1D  B7ôØ.«Ø•¨‘‹„³|Æ.
0210h: 29 9E 56 65 BD BC 88 B1 53 0D 9C 61 68 F2 18 58  )žVe½¼ˆ±S.œahò.X
0220h: D7 DD 84 3E 73 8C 0D 84 C0 05 66 74 C1 AD 7D F4  ×Ý„>sŒ.„À.ftÁ-}ô
0230h: AB 88 23 D2 68 53 B4 33 7C 95 2C C5 7C 9E 44 69  «ˆ#ÒhS´3|•,Å|žDi
0240h: 69 26 43 A7 B1 58 28 A4 C4 EE 25 53 DD 6B 1E 70  i&C§±X(¤Äî%SÝk.p
0250h: C0 9B 51 01 1A 2C 79 E6 08 A5 2D CF 95 D0 99 47  À›Q..,yæ.¥-Ï•Ð™G
0260h: F0 AA D7 50 66 1A 73 D1 F4 FD 61 2D 14 70 39 4D  ðª×Pf.sÑôýa-.p9M
0270h: 8D 6C CC 10 82 EB C9 18 6D 00 93 01 14 3C 2A 96  .lÌ.‚ëÉ.m.“..<*–
0280h: A9 92 1B C0 DF 81 A3 0C 9D 86 18 F7 50 F9 3A 7C  ©’.Àß.£..†.÷Pù:|
0290h: A6 35 55 8C 22 20 F6 47 02 37 2C 7C 7F 40 3F E0  ¦5UŒ" öG.7,|.@?à
02A0h: 86 05 1C 8E 2D 6F 4A 00 CA 96 47 A7 C7 FB D6 5B  †..Ž-oJ.Ê–G§ÇûÖ[
```

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 00 00 00 1C 66 74 79 70 6D 70 34 32 00 00 00 01  ....ftypmp42....
0010h: 69 73 6F 6D 6D 70 34 31 6D 70 34 32 00 00 00 18  isommp41mp42....
0020h: 62 65 61 6D 01 00 00 00 01 00 00 00 00 00 00 00  beam............
0030h: 05 00 00 00 00 00 0B 6A 6D 6F 6F 76 00 00 00 6C  .......jmoov...l
0040h: 6D 76 68 64 00 00 00 00 DA 6D D9 31 DA 6D D9 31  mvhd....ÚmÙ1ÚmÙ1
0050h: 00 00 AC 44 00 08 91 7A 00 01 00 00 01 00 00 00  ..¬D..‘z........
0060h: 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00  ................
0070h: 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
0090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00A0h: 00 00 00 00 00 00 00 02 00 00 0A F6 74 72 61 6B  ..........ötrak
00B0h: 00 00 00 5C 74 6B 68 64 00 00 00 01 DA 6D D9 31  ...\tkhd....ÚmÙ1
00C0h: DA 6D D9 31 00 00 00 01 00 00 00 00 00 08 91 7A  ÚmÙ1..........‘z
00D0h: 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00E0h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0100h: 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 24  @..............$
0110h: 65 64 74 73 00 00 00 1C 65 6C 73 74 00 00 00 00  edts....elst....
0120h: 00 00 00 01 00 08 91 7A 00 00 08 40 00 01 00 00  ......‘z...@....
0130h: 00 00 0A 6E 6D 64 69 61 00 00 00 20 6D 64 68 64  ...nmdia... mdhd
0140h: 00 00 00 00 DA 6D D9 31 DA 6D D9 31 00 00 AC 44  ....ÚmÙ1ÚmÙ1..¬D
0150h: 00 08 9C 00 55 C4 00 00 00 00 00 31 68 64 6C 72  ..œ.UÄ.....1hdlr
0160h: 00 00 00 00 00 00 00 00 73 6F 75 6E 00 00 00 00  ........soun....
0170h: 00 00 00 00 00 00 00 00 43 6F 72 65 20 4D 65 64  ........Core Med
0180h: 69 61 20 41 75 64 69 6F 00 00 00 0A 15 6D 69 6E  ia Audio.....min
0190h: 66 00 00 00 10 73 6D 68 64 00 00 00 00 00 00 00  f....smhd.......
01A0h: 00 00 00 00 24 64 69 6E 66 00 00 00 1C 64 72 65  ....$dinf....dre
01B0h: 66 00 00 00 00 00 00 00 01 00 00 00 0C 75 72 6C  f............url
01C0h: 20 00 00 00 01 00 00 09 D9 73 74 62 6C 00 00 00   .......Ùstbl...
01D0h: 67 73 74 73 64 00 00 00 00 00 00 00 01 00 00 00  gstsd...........
01E0h: 57 6D 70 34 61 00 00 00 00 00 00 00 01 00 00 00  Wmp4a...........
01F0h: 00 00 00 00 00 00 02 00 10 00 00 00 00 AC 44 00  .............¬D.
0200h: 00 00 00 00 33 65 73 64 73 00 00 00 00 03 80 80  ....3esds.....€€
0210h: 80 22 00 00 00 04 80 80 80 14 40 14 00 18 00 00  €"....€€€.@.....
0220h: 00 FA 00 00 00 FA 00 05 80 80 80 02 12 10 06 80  .ú...ú..€€€....€
0230h: 80 80 01 02 00 00 00 1A 73 67 70 64 01 00 00 00  €€......sgpd....
0240h: 72 6F 6C 6C 00 00 00 02 00 00 00 01 FF FF 00 00  roll........ÿÿ..
0250h: 00 1C 73 62 67 70 00 00 00 00 72 6F 6C 6C 00 00  ..sbgp....roll..
0260h: 00 01 00 00 02 27 00 00 00 01 00 00 00 18 73 74  .....'........st
0270h: 74 73 00 00 00 00 00 00 00 01 00 00 02 27 00 00  ts...........'..
0280h: 04 00 00 00 00 28 73 74 73 63 00 00 00 00 00 00  .....(stsc......
0290h: 00 02 00 00 00 01 00 00 00 2B 00 00 00 01 00 00  .........+......
02A0h: 00 0D 00 00 00 23 00 00 00 01 00 00 08 B0 73 74  .....#.......°st
```

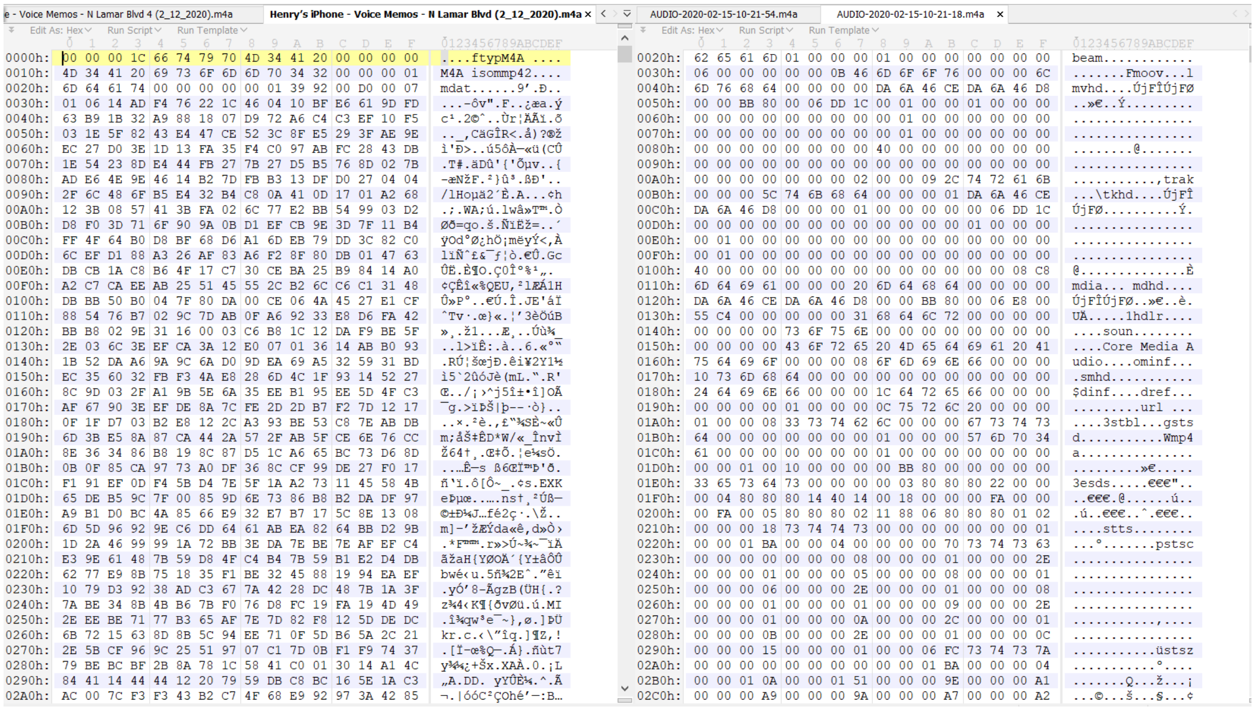
Figure 25: *File Header of Original Lossless Recording on Left, and That Same Audio Recording Compressed by WhatsApp on Right*



```
           0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
17:8B50h: 86 00 00 13 7C 00 00 15 29 00 00 14 49 00 00 13   †...|...)...I...
17:8B60h: 92 00 00 13 2C 00 00 15 0F 00 00 13 E3 00 00 13   ’...,.......ã...
17:8B70h: B5 00 00 10 43 00 00 13 58 00 00 13 5F 00 00 12   µ...C...X..._...
17:8B80h: 5E 00 00 10 2E 00 00 0F B3 00 00 11 44 00 00 10   ^.......³...D...
17:8B90h: AF 00 00 0F E3 00 00 12 D1 00 00 14 55 00 00 0D   ¯...ã...Ñ...U...
17:8BA0h: 99 00 00 00 AC 73 74 63 6F 00 00 00 00 00 00 00   ™...¬stco.......
17:8BB0h: 27 00 00 00 2C 00 00 9C 67 00 01 75 FA 00 02 49   '...,..œg..uú..I
17:8BC0h: C6 00 03 2F EB 00 03 72 CF 00 04 31 6E 00 05 0A   Æ../ë..rÏ..1n...
17:8BD0h: 43 00 05 32 76 00 06 13 9A 00 06 E6 A3 00 06 FA   C..2v...š..æ£..ú
17:8BE0h: 3B 00 07 DB 7B 00 08 B8 FC 00 08 E4 2C 00 09 C5   ;..Û{..¸ü..ä,..Å
17:8BF0h: 4D 00 0A 9A C2 00 0A AE 46 00 0B 74 26 00 0C 45   M..šÂ..®F..t&..E
17:8C00h: E5 00 0C 6D 6F 00 0D 47 EB 00 0E 1A ED 00 0E 32   å..mo..Gë...í..2
17:8C10h: 4A 00 0F 1A BA 00 10 08 EF 00 10 21 9C 00 10 FD   J...º...ï..!œ..ý
17:8C20h: C0 00 11 DC 70 00 12 08 08 00 12 DF E2 00 13 BA   À..Üp......ßâ..º
17:8C30h: E2 00 13 CB 54 00 14 B1 BF 00 15 95 C8 00 15 C0   â..ËT..±¿..•È..À
17:8C40h: 61 00 16 9E F9 00 17 60 8E 00 17 75 C7 00 00 01   a..žù..`Ž..uÇ...
17:8C50h: A6 75 64 74 61 00 00 01 9E 6D 65 74 61 00 00 00   ¦udta...žmeta...
17:8C60h: 00 00 00 00 22 68 64 6C 72 00 00 00 00 00 00 00   ...."hdlr.......
17:8C70h: 00 6D 64 69 72 00 00 00 00 00 00 00 00 00 00 00   .mdir...........
17:8C80h: 00 00 00 00 00 01 70 69 6C 73 74 00 00 00 BC 2D   ......pilst...¼-
17:8C90h: 2D 2D 2D 00 00 00 1C 6D 65 61 6E 00 00 00 00 63   ---....mean....c
17:8CA0h: 6F 6D 2E 61 70 70 6C 65 2E 69 54 75 6E 65 73 00   om.apple.iTunes.
17:8CB0h: 00 00 14 6E 61 6D 65 00 00 00 00 69 54 75 6E 53   ...name....iTunS
17:8CC0h: 4D 50 42 00 00 00 84 64 61 74 61 00 00 00 01 00   MPB...„data.....
17:8CD0h: 00 00 00 20 30 30 30 30 30 30 30 30 20 30 30 30   ... 00000000 000
17:8CE0h: 30 30 30 30 30 20 30 30 30 30 30 35 34 39 20 30   00000 00000549 0
17:8CF0h: 30 30 30 30 30 30 30 30 30 31 33 31 41 42 37 20   000000000131AB7 
17:8D00h: 30 30 30 30 30 30 30 30 20 30 30 30 30 30 30 30   00000000 0000000
17:8D10h: 30 20 30 30 30 30 30 30 30 30 20 30 30 30 30 30   0 00000000 00000
17:8D20h: 30 30 30 20 30 30 30 30 30 30 30 30 20 30 30 30   000 00000000 000
17:8D30h: 30 30 30 30 30 20 30 30 30 30 30 30 30 30 20 30   00000 00000000 0
17:8D40h: 30 30 30 30 30 30 30 00 00 00 73 2D 2D 2D 2D 00   0000000...s----.
17:8D50h: 00 00 1C 6D 65 61 6E 00 00 00 00 63 6F 6D 2E 61   ...mean....com.a
17:8D60h: 70 70 6C 65 2E 69 54 75 6E 65 73 00 00 00 1B 6E   pple.iTunes....n
17:8D70h: 61 6D 65 00 00 00 00 76 6F 69 63 65 2D 6D 65 6D   ame....voice-mem
17:8D80h: 6F 2D 75 75 69 64 00 00 00 34 64 61 74 61 00 00   o-uuid...4data..
17:8D90h: 00 01 00 00 00 00 46 44 41 42 44 45 36 44 2D 42   ......FDABDE6D-B
17:8DA0h: 39 34 39 2D 34 42 34 38 2D 42 46 34 46 2D 38 33   949-4B48-BF4F-83
17:8DB0h: 34 35 45 30 30 35 43 31 39 31 00 00 00 39 A9 74   45E005C191...9©t
17:8DC0h: 6F 6F 00 00 00 31 64 61 74 61 00 00 00 01 00 00   oo...1data......
17:8DD0h: 00 00 63 6F 6D 2E 61 70 70 6C 65 2E 56 6F 69 63   ..com.apple.Voic
17:8DE0h: 65 4D 65 6D 6F 73 20 28 69 4F 53 20 31 33 2E 33   eMemos (iOS 13.3
17:8DF0h: 2E 31 29                                          .1)
```

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
1:8960h: 00 EA C4 36 A6 7D 61 A8 08 54 49 0F D9 A8 4D 58   .êÄ6¦}a¨.TI.Ù¨MX
1:8970h: 58 ED 2E B4 F5 CB 7F FB 04 03 6D DB 02 89 42 1E   Xí.´õË.û..mÛ.‰B.
1:8980h: 6D C8 AB D1 C6 95 48 CD DE CC 33 29 BF 8C 3E 8C   mÈ«ÑÆ•HÍÞÌ3)¿Œ>Œ
1:8990h: 33 00 8D 3E F2 59 13 62 BC DD 9B D6 1A 3F E8 00   3..>òY.b¼Ý›Ö.?è.
1:89A0h: 00 00 00 00 38 21 09 C4 D5 19 9E 41 60 A0 C8 A8   ....8!.ÄÕ.žA` È¨
1:89B0h: 31 18 09 F0 B0 D1 50 20 CD 40 5C 08 1A 6B 26 2A   1..ð°ÑP Í@\..k&*
1:89C0h: 43 31 7B BD B6 F6 84 94 F1 BA E9 EA 7A 70 D3 E9   C1{½¶ö„”ñºéêzpÓé
1:89D0h: 6E 1A 30 BF 86 A8 9B E3 66 33 CF 4B DA 94 D1 7C   n.0¿†¨›ãf3ÏKÚ”Ñ|
1:89E0h: 03 61 60 96 00 34 02 4A C1 63 2B 08 55 85 CE D7   .a`–.4.JÁc+.U…Î×
1:89F0h: 19 26 52 DA 0D 99 94 93 8A 5E 51 3B 46 6D 4A 4E   .&RÚ.™”“Š^Q;FmJN
1:8A00h: 4D AF AA 4F C6 33 95 50 5F DC 63 DB C9 F4 6F 9B   M¯ªOÆ3•P_ÜcÛÉôo›
1:8A10h: 5B 0B 64 8E 48 7C CE B5 A2 D8 31 14 06 3C 6E CB   [.dŽH|Îµ¢Ø1..<nË
1:8A20h: F4 CB 2E 53 EF A6 CC 24 0D 37 2A 6A 47 9A FB F3   ôË.Sï¦Ì$.7*jGšûó
1:8A30h: 34 51 B1 CE 72 17 51 E6 53 C9 F4 D9 3C 7C 29 8B   4Q±Îr.QæSÉôÙ<|)‹
1:8A40h: 7C 3A 77 A0 06 8F FA 00 00 00 00 00 0E 21 09 C4   |:w ..ú......!.Ä
1:8A50h: CD 21 94 85 60 A0 88 E8 12 10 0D C1 24 D2 54 8A   Í!”…` ˆè...Á$ÒTŠ
1:8A60h: 58 6E F4 A4 24 58 37 4B 0D 6F 34 DD 74 35 D5 A7   Xnô¤$X7K.o4Ýt5Õ§
1:8A70h: 9A 06 64 40 19 96 6B 80 6E D7 2B 78 5D 81 4D 7C   š.d@.–k€n×+x].M|
1:8A80h: C9 5C 51 33 70 B1 E5 89 66 61 8D EF 97 53 3B 95   É\Q3p±å‰fa.ï—S;•
1:8A90h: 7E 51 31 88 F0 D0 B6 95 10 C0 BA 76 B6 6E EA 7E   ~Q1ˆðÐ¶•.Àºv¶nê~
1:8AA0h: 59 CE C6 43 21 95 4D 4D 2F 77 37 29 0B C1 8C EC   YÎÆC!•MM/w7).ÁŒì
1:8AB0h: 89 8C 8E DA FF 61 AB A7 8B AC D5 BD E5 DD B8 08   ‰ŒŽÚÿa«§‹¬Õ½åÝ¸.
1:8AC0h: 4B D4 7A A3 11 34 D8 3E C5 62 9E C5 9B 9B B8 BD   KÔz£.4Ø>ÅbžÅ››¸½
1:8AD0h: 7F E1 EF 44 4D 81 A7 F1 8B 0A 48 AB AE C1 00 8B   .áïDM.§ñ‹.H«®Á.‹
1:8AE0h: F8 04 FD E8 43 4D 96 2D 1F F4 00 00 00 00 00 1C   ø.ýèCM–-.ô......
1:8AF0h: 21 09 C4 CD 1D 92 8C 24 08 40 49 A8 70 66 AD 91   !.ÄÍ.’Œ$.@I¨pf-‘
1:8B00h: CE B4 BC 55 9A A4 16 0D EF 60 BA 0E E3 67 A8 98   Î´¼Uš¤..ï`º.ãg¨˜
1:8B10h: C9 4C 52 12 95 FA 27 A6 8B 0B A7 2A 57 AB 39 A7   ÉLR.•ú'¦‹.§*W«9§
1:8B20h: AD 9E 56 61 8A 70 40 B3 0D 12 4E 90 C3 37 FF 26   -žVaŠp@³..N.Ã7ÿ&
1:8B30h: 76 AD DD 01 7C 1D 17 F3 81 E0 59 75 25 2B DF D0   v-Ý.|..ó.àYu%+ßÐ
1:8B40h: D7 9D DA 2A 1B D8 F2 39 0D 02 85 3C 49 B2 B2 8E   ×.Ú*.Øò9..…<I²²Ž
1:8B50h: 36 46 27 C8 E9 54 BB EE CB A1 EA 67 45 57 F8 66   6F'ÈéT»îË¡êgEWøf
1:8B60h: CD 39 BA A7 4C AB 3C 09 6C 33 4E 63 25 45 DD C9   Í9º§L«<.l3Nc%EÝÉ
1:8B70h: 38 2A B4 F7 E0 B0 20 E3 2D 22 B1 50 C3 FA 7D 65   8*´÷à° ã-"±PÃú}e
1:8B80h: 50 9F 75 CA C2 A0 1A 3F E8 00 00 00 00 00 38 21   PŸuÊÂ .?è.....8!
1:8B90h: 09 C4 A4 30 C4 C4 42 0A 01 26 8E 0B EB A3 88 45   .Ä¤0ÄÄB..&Ž.ë£ˆE
1:8BA0h: B6 0C 45 CA C9 50 CB FC 04 00 05 F9 7E EC A9 DB   ¶.EÊÉPËü...ù~ì©Û
1:8BB0h: 68 D4 6A 66 82 A9 A6 8A 58 59 66 69 BB 2E D9 9D   hÔjf‚©¦ŠXYfi».Ù.
1:8BC0h: 95 70 2A 86 E5 3C 2B B5 63 6E 16 78 57 65 0F DD   •p*†å<+µcn.xWe.Ý
1:8BD0h: A9 8F 16 6B C9 41 41 46 FC 28 ED 6E 5A 64 D3 C5   ©..kÉAAFü(ínZdÓÅ
1:8BE0h: 1C 6C 05 23 FC 7A 60 65 9D 64 30 31 45 8B 24 A0   .l.#üz`e.d01E‹$ 
1:8BF0h: 00 19 00 34 7F D0 00 00 00 00 01 72 B2 54 32 FF   ...4.Ð.....r²T2ÿ
1:8C00h: 01 00 01 70                                       ...p
```

Figure 26: *File Footer of Original Lossless Recording on Left, and That Same Audio Recording Re-Compressed by WhatsApp on Right*

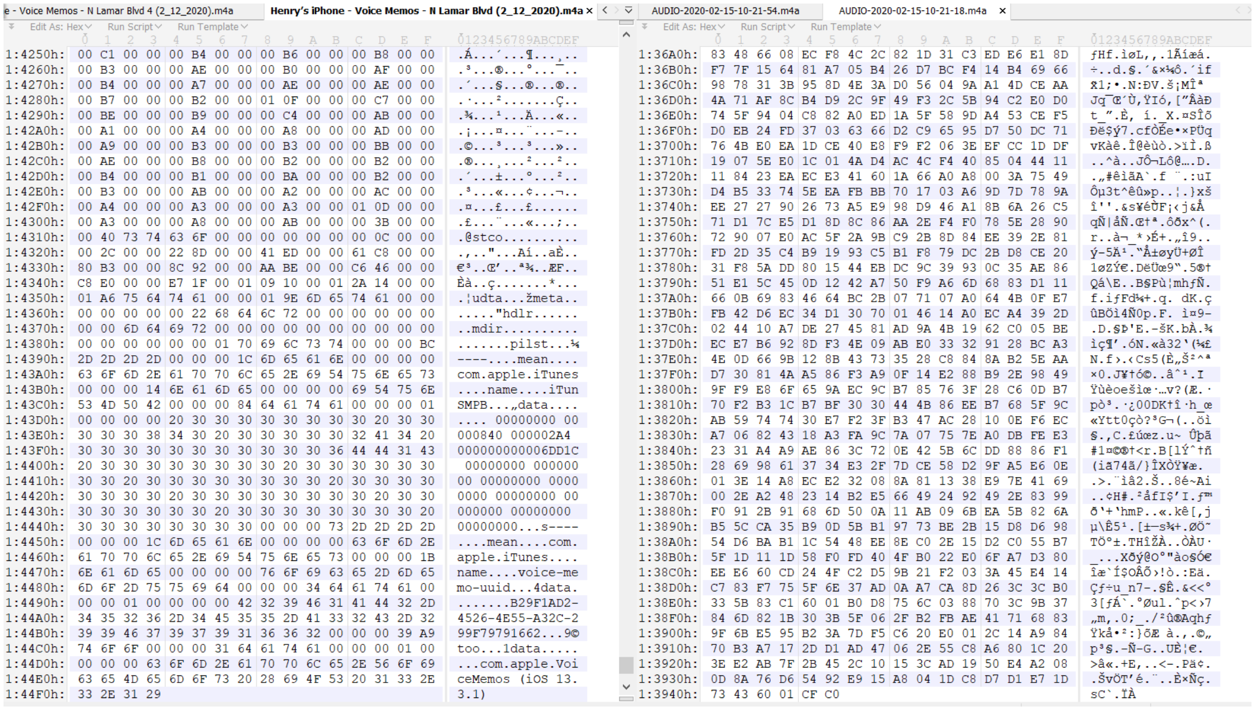


e - Voice Memos - N Lamar Blvd 4 (2_12_2020).m4a
Henry's iPhone - Voice Memos - N Lamar Blvd (2_12_2020).m4a ×
Edit As: Hex
Run Script
Run Template
AUDIO-2020-02-15-10-21-54.m4a
AUDIO-2020-02-15-10-21-18.m4a ×
Edit As: Hex
Run Script
Run Template

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 00 00 00 1C 66 74 79 70 4D 34 41 20 00 00 00 00  ....ftypM4A ....
0010h: 4D 34 41 20 69 73 6F 6D 6D 70 34 32 00 00 00 01  M4A isommp42....
0020h: 6D 64 61 74 00 00 00 00 00 01 39 92 00 D0 00 07  mdat......9’.Ð..
0030h: 01 06 14 AD F4 76 22 1C 46 04 10 BF E6 61 9D FD  ...-ôv".F..¿æa.ý
0040h: 63 B9 1B 32 A9 88 18 07 D9 72 A6 C4 C3 EF 10 F5  c¹.2©ˆ..Ùr¦ÄÃï.õ
0050h: 03 1E 5F 82 43 E4 47 CE 52 3C 8F E5 29 3F AE 9E  .._‚CäGÎR<.å)?®ž
0060h: EC 27 D0 3E 1D 13 FA 35 F4 C0 97 AB FC 28 43 DB  ì'Ð>..ú5ôÀ—«ü(CÛ
0070h: 1E 54 23 8D E4 44 FB 27 7B 27 D5 B5 76 8D 02 7B  .T#.äDû'{'Õµv..{
0080h: AD E6 4E 9E 46 14 B2 7D FB B3 13 DF D0 27 04 04  -æNžF.²}û³.ßÐ'..
0090h: 2F 6C 48 6F B5 E4 32 B4 C8 0A 41 0D 17 01 A2 68  /lHoµä2´È.A...¢h
00A0h: 12 3B 08 57 41 3B FA 02 6C 77 E2 BB 54 99 03 D2  .;.WA;ú.lwâ»T™.Ò
00B0h: D8 F0 3D 71 6F 90 9A 0B D1 EF CB 9E 3D 7F 11 B4  Øð=qo.š.ÑïËž=..´
00C0h: FF 4F 64 B0 D8 BF 68 D6 A1 6D EB 79 DD 3C 82 C0  ÿOd°Ø¿hÖ¡mëyÝ<‚À
00D0h: 6C EF D1 88 A3 26 AF 83 A6 F2 8F 80 DB 01 47 63  lïÑˆ£&¯ƒ¦ò.€Û.Gc
00E0h: DB CB 1A C8 B6 4F 17 C7 30 CE BA 25 B9 84 14 A0  ÛË.È¶O.Ç0Îº%¹„..
00F0h: A2 C7 CA EE AB 25 51 45 55 2C B2 6C C6 C1 31 48  ¢ÇÊî«%QEU,²lÆÁ1H
0100h: DB BB 50 B0 04 7F 80 DA 00 CE 06 4A 45 27 E1 CF  Û»P°..€Ú.Î.JE'áÏ
0110h: 88 54 76 B7 02 9C 7D AB 0F A6 92 33 E8 D6 FA 42  ˆTv·.œ}«.¦’3èÖúB
0120h: BB B8 02 9E 31 16 00 03 C6 B8 1C 12 DA F9 BE 5F  »¸.ž1...Æ¸..Úù¾_
0130h: 2E 03 6C 3E EF CA 3A 12 E0 07 01 36 14 AB B0 93  ..l>ïÊ:.à..6.«°“
0140h: 1B 52 DA A6 9A 9C 6A D0 9D EA 69 A5 32 59 31 BD  .RÚ¦šœjÐ.êi¥2Y1½
0150h: EC 35 60 32 FB F3 4A E8 28 6D 4C 1F 93 14 52 27  ì5`2ûóJè(mL.“.R'
0160h: 8C 9D 03 2F A1 9B 5E 6A 35 EE B1 95 EE 5D 4F C3  Œ../¡›^j5î±•î]OÃ
0170h: AF 67 90 3E EF DE 8A 7C FE 2D 2D B7 F2 7D 12 17  ¯g.>ïÞŠ|þ--·ò}..
0180h: 0F 1F D7 03 B2 E8 12 2C A3 93 BE 53 C8 7E AB DB  ..×.²è.,£“¾SÈ~«Û
0190h: 6D 3B E5 8A 87 CA 44 2A 57 2F AB 5F CE 6E 76 CC  m;åŠ‡ÊD*W/«_ÎnvÌ
01A0h: 8E 36 34 86 B8 19 8C 87 D5 1C A6 65 BC 73 D6 8D  Ž64†¸.Œ‡Õ.¦e¼sÖ.
01B0h: 0B 0F 85 CA 97 73 A0 DF 36 8C CF 99 DE 27 F0 17  ..…Ê—s ß6ŒÏ™Þ'ð.
01C0h: F1 91 EF 0D F4 5B D4 7E 5F 1A A2 73 11 45 58 4B  ñ‘ï.ô[Ô~_.¢s.EXK
01D0h: 65 DE B5 9C 7F 00 85 9D 6E 73 86 B8 B2 DA DF 97  eÞµœ..….ns†¸²Úß—
01E0h: A9 B1 D0 BC 4A 85 66 E9 32 E7 B7 17 5C 8E 13 08  ©±Ð¼J…fé2ç·.\Ž..
01F0h: 6D 5D 96 92 9E C6 DD 64 61 AB EA 82 64 BB D2 9B  m]–’žÆÝda«ê‚d»Ò›
0200h: 1D 2A 46 99 99 1A 72 BB 3E DA 7E BE 7E AF EF C4  .*F™™.r»>Ú~¾~¯ïÄ
0210h: E3 9E 61 48 7B 59 D8 4F C4 B4 7B 59 B1 E2 D4 DB  ãžaH{YØOÄ´{Y±âÔÛ
0220h: 62 77 E9 8B 75 18 35 F1 BE 32 45 88 19 94 EA EF  bwé‹u.5ñ¾2Eˆ.”êï
0230h: 10 79 D3 92 38 AD C3 67 7A 42 28 DC 48 7B 1A 3F  .yÓ’8-ÃgzB(ÜH{.?
0240h: 7A BE 34 8B 4B B6 7B F0 76 D8 FC 19 FA 19 4D 49  z¾4‹K¶{ðvØü.ú.MI
0250h: 2E EE BE 71 77 B3 65 AF 7E 7D 82 F8 12 5D DE DC  .î¾qw³e¯~}‚ø.]ÞÜ
0260h: 6B 72 15 63 8D 8B 5C 94 EE 71 0F 5D B6 5A 2C 21  kr.c.‹\”îq.]¶Z,!
0270h: 2E 5B CF 96 9C 25 51 97 07 C1 7D 0B F1 F9 74 37  .[Ï–œ%Q—.Á}.ñùt7
0280h: 79 BE BC BF 2B 8A 78 1C 58 41 C0 01 30 14 A1 4C  y¾¼¿+Šx.XAÀ.0.¡L
0290h: 84 41 14 44 44 12 20 79 59 DB C8 BC 16 5E 1A C3  „A.DD. yYÛÈ¼.^.Ã
02A0h: AC 00 7C F3 F3 43 B2 C7 4F 68 E9 92 97 3A 42 85  ¬.|óóC²ÇOhé’—:B…
```

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0020h: 62 65 61 6D 01 00 00 00 01 00 00 00 00 00 00 00  beam............
0030h: 06 00 00 00 00 00 0B 46 6D 6F 6F 76 00 00 00 6C  .......Fmoov...l
0040h: 6D 76 68 64 00 00 00 00 DA 6A 46 CE DA 6A 46 D8  mvhd....ÚjFÎÚjFØ
0050h: 00 00 BB 80 00 06 DD 1C 00 01 00 00 01 00 00 00  ..»€..Ý.........
0060h: 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00  ................
0070h: 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00  ................
0080h: 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
0090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00A0h: 00 00 00 00 00 00 00 02 00 00 09 2C 74 72 61 6B  ...........,trak
00B0h: 00 00 00 5C 74 6B 68 64 00 00 00 01 DA 6A 46 CE  ...\tkhd....ÚjFÎ
00C0h: DA 6A 46 D8 00 00 00 01 00 00 00 00 00 06 DD 1C  ÚjFØ..........Ý.
00D0h: 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
00E0h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0h: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0100h: 40 00 00 00 00 00 00 00 00 00 00 00 00 00 08 C8  @..............È
0110h: 6D 64 69 61 00 00 00 20 6D 64 68 64 00 00 00 00  mdia... mdhd....
0120h: DA 6A 46 CE DA 6A 46 D8 00 00 BB 80 00 06 E8 00  ÚjFÎÚjFØ..»€..è.
0130h: 55 C4 00 00 00 00 00 31 68 64 6C 72 00 00 00 00  UÄ.....1hdlr....
0140h: 00 00 00 00 73 6F 75 6E 00 00 00 00 00 00 00 00  ....soun........
0150h: 00 00 00 00 43 6F 72 65 20 4D 65 64 69 61 20 41  ....Core Media A
0160h: 75 64 69 6F 00 00 00 08 6F 6D 69 6E 66 00 00 00  udio....ominf...
0170h: 10 73 6D 68 64 00 00 00 00 00 00 00 00 00 00 00  .smhd...........
0180h: 24 64 69 6E 66 00 00 00 1C 64 72 65 66 00 00 00  $dinf....dref...
0190h: 00 00 00 00 01 00 00 00 0C 75 72 6C 20 00 00 00  .........url ...
01A0h: 01 00 00 08 33 73 74 62 6C 00 00 00 67 73 74 73  ....3stbl...gsts
01B0h: 64 00 00 00 00 00 00 00 01 00 00 00 57 6D 70 34  d...........Wmp4
01C0h: 61 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  a...............
01D0h: 00 00 01 00 10 00 00 00 00 BB 80 00 00 00 00 00  .........»€.....
01E0h: 33 65 73 64 73 00 00 00 00 03 80 80 80 22 00 00  3esds.....€€€"..
01F0h: 00 04 80 80 80 14 40 14 00 18 00 00 00 FA 00 00  ..€€€.@......ú..
0200h: 00 FA 00 05 80 80 80 02 11 88 06 80 80 80 01 02  .ú..€€€..ˆ.€€€..
0210h: 00 00 00 18 73 74 74 73 00 00 00 00 00 00 00 01  ....stts........
0220h: 00 00 01 BA 00 00 04 00 00 00 00 70 73 74 73 63  ...º.......pstsc
0230h: 00 00 00 00 00 00 00 08 00 00 00 01 00 00 00 2E  ................
0240h: 00 00 00 01 00 00 00 05 00 00 00 08 00 00 00 01  ................
0250h: 00 00 00 06 00 00 00 2E 00 00 00 01 00 00 00 08  ................
0260h: 00 00 00 01 00 00 00 01 00 00 00 09 00 00 00 2E  ................
0270h: 00 00 00 01 00 00 00 0A 00 00 00 2C 00 00 00 01  ...........,....
0280h: 00 00 00 0B 00 00 00 2E 00 00 00 01 00 00 00 0C  ................
0290h: 00 00 00 15 00 00 00 01 00 00 06 FC 73 74 73 7A  ...........üstsz
02A0h: 00 00 00 00 00 00 00 00 00 00 01 BA 00 00 00 04  ...........º....
02B0h: 00 00 01 0A 00 00 01 51 00 00 00 9E 00 00 00 A1  .......Q...ž...¡
02C0h: 00 00 00 A9 00 00 00 9A 00 00 00 A7 00 00 00 A2  ...©...š...§...¢
```

Figure 27: *File Header of Original Recording Compressed by Apple Voice Memos on Left, and That Same Recording Compressed by WhatsApp on Right*



e - Voice Memos - N Lamar Blvd 4 (2_12_2020).m4a | Henry’s iPhone - Voice Memos - N Lamar Blvd (2_12_2020).m4a ×

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
1:4250h:  00 C1 00 00 00 B4 00 00 00 B6 00 00 00 B8 00 00  .Á...´...¶...¸..
1:4260h:  00 B3 00 00 00 AE 00 00 00 B0 00 00 00 AF 00 00  .³...®...°...¯..
1:4270h:  00 B4 00 00 00 A7 00 00 00 AE 00 00 00 AE 00 00  .´...§...®...®..
1:4280h:  00 B7 00 00 00 B2 00 00 01 0F 00 00 00 C7 00 00  .·...².......Ç..
1:4290h:  00 BE 00 00 00 B9 00 00 00 C4 00 00 00 AB 00 00  .¾...¹...Ä...«..
1:42A0h:  00 A1 00 00 00 A4 00 00 00 A8 00 00 00 AD 00 00  .¡...¤...¨...-..
1:42B0h:  00 A9 00 00 00 B3 00 00 00 B3 00 00 00 BB 00 00  .©...³...³...»..
1:42C0h:  00 AE 00 00 00 B8 00 00 00 B2 00 00 00 B2 00 00  .®...¸...²...²..
1:42D0h:  00 B4 00 00 00 B1 00 00 00 BA 00 00 00 B2 00 00  .´...±...°...²..
1:42E0h:  00 B3 00 00 00 AB 00 00 00 A2 00 00 00 AC 00 00  .³...«...¢...¬..
1:42F0h:  00 A4 00 00 00 A3 00 00 00 A3 00 00 01 0D 00 00  .¤...£...£......
1:4300h:  00 A3 00 00 00 A8 00 00 00 AB 00 00 00 3B 00 00  .£...¨...«...;..
1:4310h:  00 40 73 74 63 6F 00 00 00 00 00 00 00 0C 00 00  .@stco..........
1:4320h:  00 2C 00 00 22 8D 00 00 41 ED 00 00 61 C8 00 00  .,.."...Aí..aÈ..
1:4330h:  80 B3 00 00 8C 92 00 00 AA BE 00 00 C6 46 00 00  €³..Œ’..ª¾..ÆF..
1:4340h:  C8 E0 00 00 E7 1F 00 01 09 10 00 01 2A 14 00 00  Èà..ç.......*...
1:4350h:  01 A6 75 64 74 61 00 00 01 9E 6D 65 74 61 00 00  .¦udta...žmeta..
1:4360h:  00 00 00 00 00 22 68 64 6C 72 00 00 00 00 00 00  ....."hdlr......
1:4370h:  00 00 6D 64 69 72 00 00 00 00 00 00 00 00 00 00  ..mdir..........
1:4380h:  00 00 00 00 00 00 01 70 69 6C 73 74 00 00 00 BC  .......pilst...¼
1:4390h:  2D 2D 2D 2D 00 00 00 1C 6D 65 61 6E 00 00 00 00  ----....mean....
1:43A0h:  63 6F 6D 2E 61 70 70 6C 65 2E 69 54 75 6E 65 73  com.apple.iTunes
1:43B0h:  00 00 00 14 6E 61 6D 65 00 00 00 00 69 54 75 6E  ....name....iTun
1:43C0h:  53 4D 50 42 00 00 00 84 64 61 74 61 00 00 00 01  SMPB...„data....
1:43D0h:  00 00 00 00 20 30 30 30 30 30 30 30 30 20 30 30  .... 00000000 00
1:43E0h:  30 30 30 38 34 30 20 30 30 30 30 30 32 41 34 20  000840 000002A4
1:43F0h:  30 30 30 30 30 30 30 30 30 30 30 36 44 44 31 43  000000000006DD1C
1:4400h:  20 30 30 30 30 30 30 30 30 20 30 30 30 30 30 30   00000000 000000
1:4410h:  30 30 20 30 30 30 30 30 30 30 30 20 30 30 30 30  00 00000000 0000
1:4420h:  30 30 30 30 20 30 30 30 30 30 30 30 30 20 30 30  0000 00000000 00
1:4430h:  30 30 30 30 30 30 20 30 30 30 30 30 30 30 30 20  000000 00000000
1:4440h:  30 30 30 30 30 30 30 30 00 00 00 73 2D 2D 2D 2D  00000000...s----
1:4450h:  00 00 00 1C 6D 65 61 6E 00 00 00 00 63 6F 6D 2E  ....mean....com.
1:4460h:  61 70 70 6C 65 2E 69 54 75 6E 65 73 00 00 00 1B  apple.iTunes....
1:4470h:  6E 61 6D 65 00 00 00 00 76 6F 69 63 65 2D 6D 65  name....voice-me
1:4480h:  6D 6F 2D 75 75 69 64 00 00 00 34 64 61 74 61 00  mo-uuid...4data.
1:4490h:  00 00 01 00 00 00 00 42 32 39 46 31 41 44 32 2D  .......B29F1AD2-
1:44A0h:  34 35 32 36 2D 34 45 35 35 2D 41 33 32 43 2D 32  4526-4E55-A32C-2
1:44B0h:  39 39 46 37 39 37 39 31 36 36 32 00 00 00 39 A9  99F79791662...9©
1:44C0h:  74 6F 6F 00 00 00 31 64 61 74 61 00 00 00 01 00  too...1data.....
1:44D0h:  00 00 00 63 6F 6D 2E 61 70 70 6C 65 2E 56 6F 69  ...com.apple.Voi
1:44E0h:  63 65 4D 65 6D 6F 73 20 28 69 4F 53 20 31 33 2E  ceMemos (iOS 13.
1:44F0h:  33 2E 31 29                                      3.1)
```

AUDIO-2020-02-15-10-21-54.m4a | AUDIO-2020-02-15-10-21-18.m4a ×

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
1:36A0h:  83 48 66 08 EC F8 4C 2C 82 1D 31 C3 ED E6 E1 8D  ƒHf.ìøL,‚.1Ãíæá.
1:36B0h:  F7 7F 15 64 81 A7 05 B4 26 D7 BC F4 14 B4 69 66  ÷..d.§.´&×¼ô.´if
1:36C0h:  98 78 31 3B 95 8D 4E 3A D0 56 04 9A A1 4D CE AA  ˜x1;•.N:ÐV.š¡MÎª
1:36D0h:  4A 71 AF 8C B4 D9 2C 9F 49 F3 2C 5B 94 C2 E0 D0  Jq¯Œ´Ù,ŸIó,[”ÂàÐ
1:36E0h:  74 5F 94 04 C8 82 A0 ED 1A 5F 58 9D A4 53 CE F5  t_”.È‚ í._X.¤SÎõ
1:36F0h:  D0 EB 24 FD 37 03 63 66 D2 C9 65 95 D7 50 DC 71  Ðë$ý7.cfÒÉe•×PÜq
1:3700h:  76 4B E0 EA 1D CE 40 E8 F9 F2 06 3E EF CC 1D DF  vKàê.Î@èùò.>ïÌ.ß
1:3710h:  19 07 5E E0 1C 01 4A D4 AC 4C F4 40 85 04 44 11  ..^à..JÔ¬Lô@….D.
1:3720h:  11 84 23 EA EC E3 41 60 1A 66 A0 A8 00 3A 75 49  .„#êìãA`.f ¨.:uI
1:3730h:  D4 B5 33 74 5E EA FB BB 70 17 03 A6 9D 7D 78 9A  Ôµ3t^êû»p..¦.}xš
1:3740h:  EE 27 27 90 26 73 A5 E9 98 D9 46 A1 8B 6A 26 C5  î''.&s¥é˜ÙF¡‹j&Å
1:3750h:  71 D1 7C E5 D1 8D 8C 86 AA 2E F4 F0 78 5E 28 90  qÑ|åÑ.Œ†ª.ôðx^(.
1:3760h:  72 90 07 E0 AC 5F 2A 9B C9 2B 8D 84 EE 39 2E 81  r..à¬_*›É+.„î9..
1:3770h:  FD 2D 35 C4 B9 19 93 C5 B1 F8 79 DC 2B D8 CE 20  ý-5Ä¹.“Å±øyÜ+ØÎ
1:3780h:  31 F8 5A DD 80 15 44 EB DC 9C 39 93 0C 35 AE 86  1øZÝ€.DëÜœ9“.5®†
1:3790h:  51 E1 5C 45 0D 12 42 A7 50 F9 A6 6D 68 83 D1 11  Qá\E..B§Pù¦mhƒÑ.
1:37A0h:  66 0B 69 83 46 64 BC 2B 07 71 07 A0 64 4B 0F E7  f.iƒFd¼+.q. dK.ç
1:37B0h:  FB 42 D6 EC 34 D1 30 70 01 46 14 A0 EC A4 39 2D  ûBÖì4Ñ0p.F. ì¤9-
1:37C0h:  02 44 10 A7 DE 27 45 81 AD 9A 4B 19 62 C0 05 BE  .D.§Þ'E.-šK.bÀ.¾
1:37D0h:  EC E7 B6 92 8D F3 4E 09 AB E0 33 32 91 28 BC A3  ìç¶’.óN.«à32‘(¼£
1:37E0h:  4E 0D 66 9B 12 8B 43 73 35 28 C8 84 8A B2 5E AA  N.f›.‹Cs5(È„Š²^ª
1:37F0h:  D7 30 81 4A A5 86 F3 A9 0F 14 E2 88 B9 2E 98 49  ×0.J¥†ó©..âˆ¹.˜I
1:3800h:  9F F9 E8 6F 65 9A EC 9C B7 85 76 3F 28 C6 0D B7  Ÿùèoešìœ·…v?(Æ.·
1:3810h:  70 F2 B3 1C B7 BF 30 30 44 4B 86 EE B7 68 5F 9C  pò³.·¿00DK†î·h_œ
1:3820h:  AB 59 74 74 30 E7 F2 3F B3 47 AC 28 10 0E F6 EC  «Ytt0çò?³G¬(..öì
1:3830h:  A7 06 82 43 18 A3 FA 9C 7A 07 75 7E A0 DB FE E3  §.‚C.£úœz.u~ Ûþã
1:3840h:  23 31 A4 A9 AE 86 3C 72 0E 42 5B 6C DD 88 86 F1  #1¤©®†<r.B[lÝˆ†ñ
1:3850h:  28 69 98 61 37 34 E3 2F 7D CE 58 D2 9F A5 E6 0E  (i˜a74ã/}ÎXÒŸ¥æ.
1:3860h:  01 3E 14 A8 EC E2 32 08 8A 81 13 38 E9 7E 41 69  .>.¨ìâ2.Š..8é~Ai
1:3870h:  00 2E A2 48 23 14 B2 E5 66 49 24 92 49 2E 83 99  ..¢H#.²åfI$’I.ƒ™
1:3880h:  F0 91 2B 91 68 6D 50 0A 11 AB 09 6B EA 5B 82 6A  ð‘+‘hmP..«.kê[‚j
1:3890h:  B5 5C CA 35 B9 0D 5B B1 97 73 BE 2B 15 D8 D6 98  µ\Ê5¹.[±—s¾+.ØÖ˜
1:38A0h:  54 D6 BA B1 1C 54 48 EE 8E C0 2E 15 D2 C0 55 B7  TÖº±.THîŽÀ..ÒÀU·
1:38B0h:  5F 1D 11 1D 58 F0 FD 40 4F B0 22 E0 6F A7 D3 80  _...Xðý@O°"ào§Ó€
1:38C0h:  EE E6 60 CD 24 4F C2 D5 9B 21 F2 03 3A 45 E4 14  îæ`Í$OÂÕ›!ò.:Eä.
1:38D0h:  C7 83 F7 75 5F 6E 37 AD 0A A7 CA 8D 26 3C 3C B0  Çƒ÷u_n7-.§Ê.&<<°
1:38E0h:  33 5B 83 C1 60 01 B0 D8 75 6C 03 88 70 3C 9B 37  3[ƒÁ`.°Øul.ˆp<›7
1:38F0h:  84 6D 82 1B 30 3B 5F 06 2F B2 FB AE 41 71 68 83  „m‚.0;_./²û®Aqhƒ
1:3900h:  9F 6B E5 95 B2 3A 7D F5 C6 20 E0 01 2C 14 A9 84  Ÿkå•²:}õÆ à.,.©„
1:3910h:  70 B3 A7 17 2D D1 AD 47 06 2E 55 C8 A6 80 1C 20  p³§.-Ñ-G..UÈ¦€.
1:3920h:  3E E2 AB 7F 2B 45 2C 10 15 3C AD 19 50 E4 A2 08  >â«.+E,..<-.Pä¢.
1:3930h:  0D 8A 76 D6 54 92 E9 15 A8 04 1D C8 D7 D1 E7 1D  .ŠvÖT’é.¨..È×Ñç.
1:3940h:  73 43 60 01 CF C0                                sC`.ÏÀ
```

Figure 28: *File Footer of Original Recording Compressed by Apple Voice Memos on Left, and That Same Recording Compressed by WhatsApp on Right*

CHAPTER VI

DISCUSSION

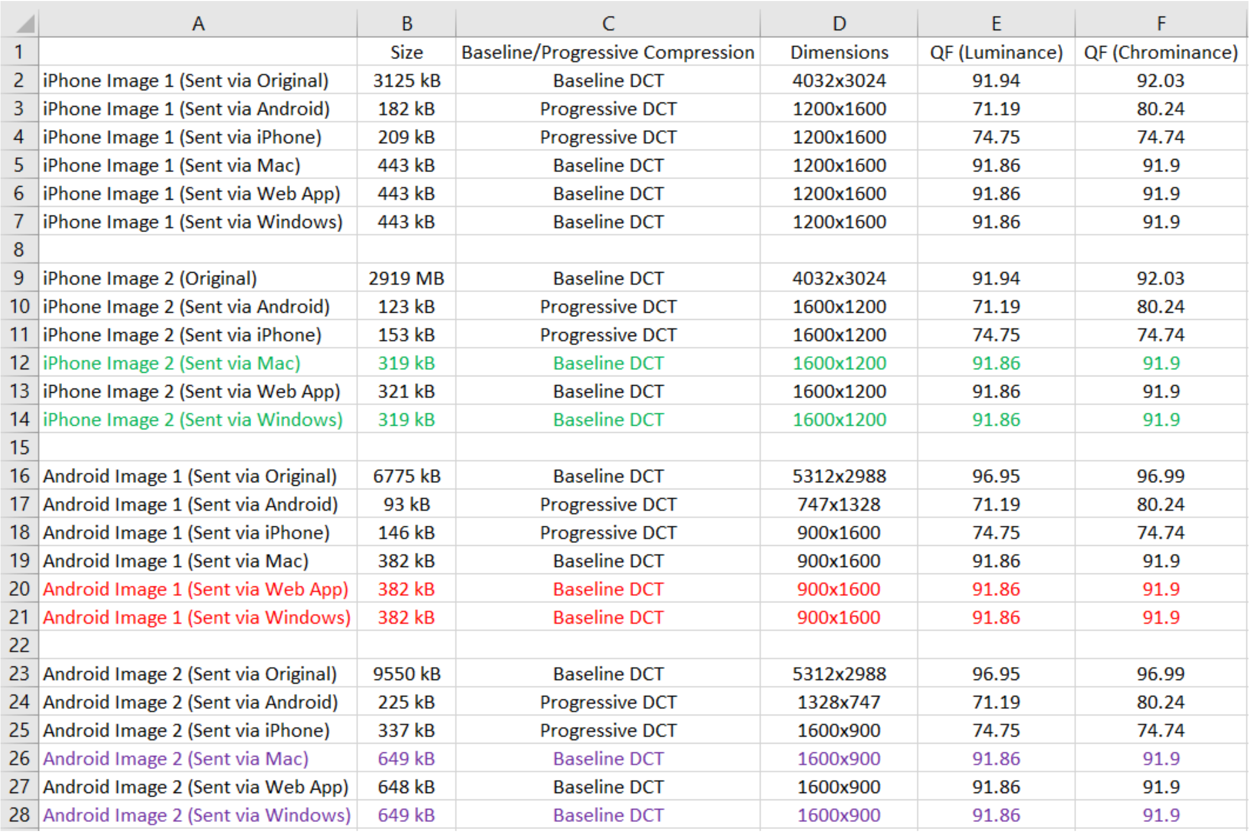
Conclusions

Based on the results of the analysis, it appears as though different compression schemes are applied to images that are sent over WhatsApp depending on which of three broad methods are used to send them. Those methods being over iPhone, Android, or desktop applications. Although this study explored many different methods of sending media files, only these broader categories of methods influenced how the media files were changed. None of the more specific sending methods within those broader methods or the download methods used influenced how the files were compressed. The first observation made was that the naming convention applied to the downloaded images was dictated by the type of device or web application that was used to download them. The most striking differences in images downloaded from WhatsApp were observed between images sent via cellular devices and those sent via desktop applications. Images that were sent via mobile devices had more aggressive compression applied to them based on observing the quantization tables and quality factors identified, and these images were compressed with Progressive DCT encoding. This is compared to images that were sent via desktop devices that had much less aggressive compression applied to them and were compressed with Baseline DCT encoding.

There were also some commonalities among all images that were sent and then downloaded from WhatsApp compared to their original counterparts. After the transmission, the volume of Exif entries identified was significantly reduced to 22 entries no matter how many entries were observed in the original images. The Exif tag was lost, and instead the JFIF file signature was identified.

An interesting finding was that in some cases, but not all, there is uniformity between images that are sent from different desktop applications. However, based on the Exif data, Hex data, and quantization tables, we can see that the same compression is used by all desktop applications examined in this study. The information gathered here can be used to help identify images that have been sent over the WhatsApp application and the type of device that was used to send them.

Below is a table visualizing the variable data associated with each different downloaded image. Color coded rows indicate images that have matching hash values.



	A	B	C	D	E	F
1		Size	Baseline/Progressive Compression	Dimensions	QF (Luminance)	QF (Chrominance)
2	iPhone Image 1 (Sent via Original)	3125 kB	Baseline DCT	4032x3024	91.94	92.03
3	iPhone Image 1 (Sent via Android)	182 kB	Progressive DCT	1200x1600	71.19	80.24
4	iPhone Image 1 (Sent via iPhone)	209 kB	Progressive DCT	1200x1600	74.75	74.74
5	iPhone Image 1 (Sent via Mac)	443 kB	Baseline DCT	1200x1600	91.86	91.9
6	iPhone Image 1 (Sent via Web App)	443 kB	Baseline DCT	1200x1600	91.86	91.9
7	iPhone Image 1 (Sent via Windows)	443 kB	Baseline DCT	1200x1600	91.86	91.9
8						
9	iPhone Image 2 (Original)	2919 MB	Baseline DCT	4032x3024	91.94	92.03
10	iPhone Image 2 (Sent via Android)	123 kB	Progressive DCT	1600x1200	71.19	80.24
11	iPhone Image 2 (Sent via iPhone)	153 kB	Progressive DCT	1600x1200	74.75	74.74
12	iPhone Image 2 (Sent via Mac)	319 kB	Baseline DCT	1600x1200	91.86	91.9
13	iPhone Image 2 (Sent via Web App)	321 kB	Baseline DCT	1600x1200	91.86	91.9
14	iPhone Image 2 (Sent via Windows)	319 kB	Baseline DCT	1600x1200	91.86	91.9
15						
16	Android Image 1 (Sent via Original)	6775 kB	Baseline DCT	5312x2988	96.95	96.99
17	Android Image 1 (Sent via Android)	93 kB	Progressive DCT	747x1328	71.19	80.24
18	Android Image 1 (Sent via iPhone)	146 kB	Progressive DCT	900x1600	74.75	74.74
19	Android Image 1 (Sent via Mac)	382 kB	Baseline DCT	900x1600	91.86	91.9
20	Android Image 1 (Sent via Web App)	382 kB	Baseline DCT	900x1600	91.86	91.9
21	Android Image 1 (Sent via Windows)	382 kB	Baseline DCT	900x1600	91.86	91.9
22						
23	Android Image 2 (Sent via Original)	9550 kB	Baseline DCT	5312x2988	96.95	96.99
24	Android Image 2 (Sent via Android)	225 kB	Progressive DCT	1328x747	71.19	80.24
25	Android Image 2 (Sent via iPhone)	337 kB	Progressive DCT	1600x900	74.75	74.74
26	Android Image 2 (Sent via Mac)	649 kB	Baseline DCT	1600x900	91.86	91.9
27	Android Image 2 (Sent via Web App)	648 kB	Baseline DCT	1600x900	91.86	91.9
28	Android Image 2 (Sent via Windows)	649 kB	Baseline DCT	1600x900	91.86	91.9

Figure 29: *Variable Data Table*

For the audio portion of this study, observations of the hex data associated with the audio files that were sent and then downloaded from WhatsApp were recorded. A model of the WhatsApp audio compression was then detected and configured for a Lossy Compression

Analysis database. This information can be used to help identify audio recordings that have been sent over the WhatsApp application.

Further Research

WhatsApp has more capabilities for sending and receiving media files that were not explored in this study. Some of the upload and download methods available within WhatsApp were excluded from this study because they were only available in group chat communications. Some additional downloading methods were also available for images when more than three were sent without a text message in between. However, based on the research done in this study it would seem unlikely that these methods would create different images.

Another capability that was excluded from this study is the ability to send and receive videos. Videos can be recorded within the WhatsApp application, or videos that are stored on a device can be selected and sent through WhatsApp. Within WhatsApp, audio messages and images can also be captured without leaving the app and then immediately sent. How the WhatsApp application captures images, video and audio could most definitely also be an interesting avenue for further research.

In this study, only 4 source images were used. Those images were taken using only two mobile devices, and the image capture settings were not changed. Those two mobile devices were the only mobile devices used in this study. This opens the door for further research utilizing images of different sizes, dimensions, and file types. Using different mobile devices as well as desktop devices to send and receive images could be a valuable topic for further research considering the plethora of different devices available to the consumer that are supported by WhatsApp.

REFERENCES

[1] Osborne, Samuel. “Stockholm suspect Rakhmat Akilov 'exchanged Whatsapp messages with Isis supporter before and after attack'” *The Independent.* 10 Apr. 2017.

[2] “WhatsApp.” *Wikipedia.* Wikimedia Foundation, 2020.

[3] Graham, Robert. “How Terrorists Use Encryption” *Combating Terrorism at West Point*, 15 Nov. 2017.

[4] Clement, J. “Social Media – Statistics and Facts.” *Statista*, 4 Sep. 2019.

[5] Lomboy, Gretchel. "Digital Image Recompression Analysis: Twitter." Thesis. University of Colorado, Denver, 2018. *Research Theses from the Master of Science in Recording Arts Emphasis in Media Forensics Program*. National Center for Media Forensics.

[6] Douglas, Zachary. "Digital Image Recompression Analysis of Instagram." Thesis. University of Colorado, Denver, 2015. *Research Theses from the Master of Science in Recording Arts Emphasis in Media Forensics Program*. National Center for Media Forensics.

[7] D. Hamdi, F. Iqbal, T. Baker and B. Shah, "Multimedia File Signature Analysis for Smartphone Forensics," *2016 9th International Conference on Developments in eSystems Engineering (DeSE)*, Liverpool, 2016, pp. 130-137.

[8] Anglano, Cosimo. “Forensic Analysis of WhatsApp Messenger on Android Smartphones,” *Digital Investigation Journal,* Alessandria, Italy. Vol 11. Sep. 2014.

[9] Hudson, Graham, et al. “JPEG-1 Standard 25 Years: Past, Present, and Future Reasons for a Success.” *Journal of Electronic Imaging*, International Society for Optics and Photonics, 2018

[10] “SWGDE Position on the Use of MD5 and SHA1 Hash Algorithms in Digital and Multimedia Forensics” Version: 1.0. *SWGDE.* Nov 20, 2018.

[11] AV&IT Standardization Committee. “ JEITA CP-3451C Exchangeable image file format for digital still cameras: Exif Version 2.3”. *Standards of Japan Electronics and Information and Technology Industries Association.* April, 2010.

[12] Mackenzie, Charles E. *Coded Character Sets, History and Development*. Reading: Addison-Wesley, 1980. *The Systems Programming Series*.

[13] "Image Format - Baseline JPEG vs. Progressive JPEG." *Tourwriter Knowledge Base*. N.p., 09 Aug. 2017.

[14] Rajwade, Ajit. “Image Compression”. *CSE, IIT Bombay.* Fall, 2014. Lecture.

[15] Smith, Steven W., “Chapter 27: Data Compression” The Scientist and Engineer’s Guide to

Digital Signal Processing (2002).

[16] Craig, William. “JPEG 101: A Crash Course Guide on JPEG.” *WebFX Blog*, 21 Dec. 2018,

[17] Grigoras, Catalin. Smith, Jeff. “ Forensic Analysis of AAC Encoding on Apple iPhone Voice Memos Recordings. *The Audio Engineering Society.* Conference on Audio Forensics. 2019.

[18] "SWGDE Digital & Multimedia Evidence Glossary Version 3.0." *Scientific Working Group on Digital Evidence*. SWGDE, 23 June 2016.