IMAGE STRUCTURE ANALYSIS FROM X ON AN IPHONE DEVICE

by

JENNIFER F. KULAK

B.A., Temple University, 2020

A thesis submitted to the

Faculty of the College of Arts & Media of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

Media Forensics Program

2023

This thesis for the Master of Science degree by

Jennifer F. Kulak

has been approved for the

Media Forensics Program

by

Catalin Grigoras, Chair

Gregory S. Wales

Cole M. Whitecotton

Date: December 16, 2023

Kulak, Jennifer F. (M.S., Media Forensics Program)

Image Structure Analysis from X on an iPhone Device

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

Recently, Twitter underwent changes and has now been marketed as a comprehensive social media application known as X. With the alterations made to the application, it is crucial to study the changes the application can make to digital images. The purpose of analyzing this is to be able to determine an original image from an image processed through the X application. With enough research on the topic, it may be possible to recognize patterns the X application-created image files have and to easily distinguish these image files from original ones.

The methods used to determine these alterations were first comparing the data from an original image test set to a test set uploaded to X. Next, another test set was created by sending the original image test sets through X's messages feature. This message feature test set was then compared to the first two test sets, and structural and data changes were recorded. Altogether, the experimentation and analysis conducted showed that the X application does in fact make changes to an image file when it is uploaded and processed through the messages feature. Certain patterns of image data changes reveal themselves through this work, and aid in determining an original image from an altered image.

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

Approved: Catalin Grigoras

DEDICATION

I dedicate this thesis to my family. Mom, thank you for always believing in and standing by me. I could not have done this without you. Dad, thank you for always supporting my passions and helping me achieve my dreams. My dear sister Kate, thank you for always listening to me and rooting for me. Bennett, my sweet nephew, thank you for being a light for me. Tom, thank you for always caring for me and my sister like we were your own. Kelly, thank you for being a source of knowledge and inspiration and for all you have done for us. Rory, thank you for always being my big brother and the voice of reason.

Aunt Daphne and Ashley, I dedicate this thesis to you. If it were not for your encouragement and belief in me, I would not be sitting here writing this. You both have taught me so much and for that I am forever grateful. To my grandfather, Albert, thank you for inspiring me to follow my dreams and study forensics just like you.

Vik, thank you for always being my proof-reader and my best friend, you always believed in me, and I am so thankful for you.

Adam, thank you for always supporting me and standing in my corner. You have encouraged me to be and do the best that I can. I am so grateful to have you in my life.

ACKNOWLEDGEMENTS

I would like to acknowledge and thank my brilliant professors at NCMF. Jeff Smith, Catalin Grigoras, and Gregory Wales thank you for your time and dedication. Learning remotely, although sometimes challenging, never felt like a struggle because I had such attentive professors. Answering any questions and guiding us through the difficult learning curves are what set you apart from any other educator I have ever had. I have never felt more confident and excited to learn since joining our program, so thank you.

Cole, I would also like to acknowledge and thank you for the many hours you have dedicated to our cohort. You have helped me stay on track these past few years and I am beyond appreciative that you have shared your knowledge with us. Every in-person meeting you were always there checking in, helping us whenever we needed it, and answering all our questions. Thank you for everything.

I also want to acknowledge and thank Leah Haloin. When I wanted to join CU Denver's MSMF program, the first person I contacted was Leah; and she got back to me right away. From that point on she guided me through applying to this wonderful program to now completing and writing my thesis. Without her dedication I do not think any of us would be where we are. Thank you, Leah, you are awesome.

TABLE OF CONTENTS

CHAPTER

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF ABBREVIATIONS

EXIF – Exchangeable Image File Format

QT – Quantization Tables

SI – Sample Image

SP – Sample Posted Image

SM – Sample Messaged Image

FIAS – Forensic Image Analysis System

CHAPTER I

INTRODUCTION

The social media application, Twitter, has been widely used in the current digital age. Recently, the company underwent major changes and is now a new, comprehensive application said to do everything from posting live audio conversations between users to joining online communities. The rebranded application, X, still acts in the same fashion as Twitter, however there are many differences to note. Like before, this application allows users to upload and share photos with their digital networks and connect with users through other features, like messages. With the prevalent use of this social media application, it has become a growing issue that original images' data are being significantly altered once they are shared to this platform. Although this may be of minor importance to a user, this serves a great deal of controversy for digital forensic investigators. For an investigator, alterations to an image can compromise the integrity of an investigation, leaving them with little evidence or no crucial information about the image in question. Therefore, this proposal will explore how the use of X on an iPhone (iOS) device makes changes to an image's data stream and why it is critical for investigators to recognize these alterations before leading their investigation.

Attempts have been made by scholars and other scientific institutions to understand and analyze the changes made to an image file once it is uploaded to a photo-sharing application. They sought to provide practical methods for extracting necessary data from these altered images. Therefore, current knowledge on this issue lacks a set of guidelines and best practices for investigators to follow when analyzing image data changes. The goal of this paper is to demonstrate the alterations made to an image file's data when it is uploaded to X via an iPhone, how to identify these changes, and the importance these data changes have to digital forensic investigators.

Overall, this topic not only has digital forensic relevance, but also has other scientific and practical relevance. It provides more research and general knowledge to how image data files change when uploaded to different platforms. Specifically for the digital forensic community, this topic can provide more insight and give a detailed analysis of the changes X makes to image files and how this modifies an iOS-created image.

Previous Research

Studies on the ways in which social media applications alter image's file structures have been provided in prior educational and research works. Also, forensic groups and establishments provide guidelines that help an experimenter to maintain the integrity of this type of work. The National Center for Media Forensics (NCMF) has provided much knowledge on related topics from previous students and educators. For this exploration, works from Zachary Douglas and Holly Naru Arai will be reviewed as they pertain to the research questions proposed next. Other forensic and scientific working groups, like American Society for Testing and Materials (ASTM) International, Institute of Electrical and Electronics Engineering (IEEE), and the Scientific Working Group on Digital Evidence (SWGDE) provide guidelines and best practices to be followed when studying and conducting this kind of experimentation. Previous research provides pertinent background knowledge to a topic and is analyzed in the writing that follows.

The first relevant source to draw similarities to this topic came from a paper by Zachary Douglas, a former University of Colorado Denver student. His thesis, "Digital Image Recompression Analysis of Instagram," summarizes the changes made to an image file's data when uploaded to a social media application. Douglas conducted an experiment utilizing three different mobile devices, Motorola, Samsung, and iPhone and uploaded a test of original unaltered images to the Instagram mobile application. He recorded the original image's file structures and hashes and the uploaded image's same file structures and hashes. Utilizing an iPhone 6s model, he concluded that the original and uploaded images had different file hashes, thus showing that the Instagram application changed the original image. Douglas concluded that "every image recovered from Instagram comes back with the same structure" (2018, p. 86). This means that forensic investigators can determine whether the image they obtained was recovered directly from the Instagram application or if it is the original/unaltered image.

Overall, Douglas' experimentation and research assist in answering a few of the later proposed research questions. Firstly, Douglas found significant structural differences between an original image and an Instagram-created image file, and uploading an original image to Instagram changes the image's data stream. Furthermore, his work displayed that once an image is uploaded to Instagram, the photo application will make significant file and structure changes to the original image. Although his research did not involve the behaviors of an image's file when the messenger feature is used, his research is a start to understanding what alterations are made and how to notice when an image is recovered from Instagram. This will help to look for patterns of changes when an image file is uploaded to a social media platform.

Critical concepts are drawn from the next piece of literature from Holly Naru Arai, another former University of Colorado Denver student. Arai's thesis, "Digital Image Recompression Analysis: Seno Wibo," will aid in providing more general information about how social media applications alter image file structures. This study centers on a social media application in China called Seno Wibo; however, Arai briefly touches on how similar this social media application is to commonly used sites in America like Twitter and Facebook. This research will provide a general basis for how social media applications manipulate an image's file structure. Like Douglas, Arai looked at recompression and metadata changes to an image once it was uploaded and downloaded from the Seno Wibo application. It was noted that images downloaded from Seno Wibo were structurally the same on a mobile device, and "the metadata was consistent based on the method of download used" (Arai, 2018, p. 42).

Looking at Arai's experimentation and results in tandem with Douglas,' one can see similarities in an image's data file once it is downloaded from a social media application. Both experiments aid in understanding how a social media application changes the properties of an image once it is uploaded and what one can look for when they are recovering an image from these sites. In addition, Arai's paper showed how social media applications act similarly in recompressing images. This consistent theory among Douglas and Arai's work helps to answer the research questions later discussed, but further research will need to be conducted into X's messages feature and changes made directly to an iOS image.

This research aims to meet the multimedia forensic standard from ASTM International. Their "Standard Guide for Forensic Digital Image Processing" outlines the process for acquiring and producing forensically sound evidence that is accepted within the courts. Their standards should be met to ensure that an investigator stays within their scope of forensic practices and that no loss or damage occurs during the acquisition and analysis of imagery. Another standard to meet during later experimentation comes from a work published by IEEE, a highly regarded journal in the forensic field. The study by Aniello Castiglione, Giuseppe Cattaneo, and Alfredo De Santis, "A Forensic Analysis of Images on Online Social Networks," will provide standards to meet in this research since it covers digital image forensic analysis on online social networks like Instagram. The main goal of this journal is to "focus on how the OSN (Online Social Networks) processes the uploaded images and what changes are made to some of the characteristics" (Castligione et al., 2011, p. 679). Their work will provide a starting point for conducting analysis and experimentation.

Best practices relevant to this research come from SWGDE's "Best Practices for Image Authentication," which will help to conduct experimentation on significant image changes after being uploaded to X on an iPhone iOS. When following their best practices, one can understand how to detect image manipulation and changes to an uploaded photo and how best to advance when analyzing an image's data file after being shared with the application. The gaps in knowledge this research aims to meet are how an X-created image file is changed when it is sent or shared between users on the application using the messenger feature, how original iOS captured images are changed when sent through messages, what overall standard should be met when investigating an iOS or X-created image, and what to look for in the future if X changes its application's functions. Overall, this project aims to cover all these missing topics from previous research and elaborate specifically on how X alters the properties of an image.

Research Questions

The following research questions include: Does the X application-created image file in the iOS device have any encoding or structural differences from the native iOS camera image file? Does the X application-created image file change the image stream when sent to another Instagram recipient?

Research Question (RQ) 1

"Does the X application-created image file in the iOS device have any encoding or structural differences from the native iOS camera image file?"

Research Question (RQ) 2

"Does the X application-created image file change the image stream when sent to another X recipient?"

CHAPTER II

MATERIALS

In the interest of answering the research questions described above, this section's experiments will entail utilizing an iOS device to capture a set of test images, upload these images to the X feed, download these images, and send them through the messages feature to record the structural changes made to the original image. 10 images were taken using a personal iPhone 12 with an iOS version of 16.3.1 *(See Figure 1).*

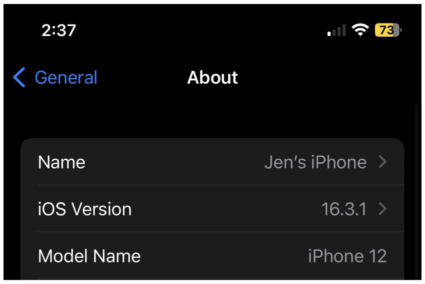

Figure 1. Test iPhone 12 General Information

The format of capture on this iPhone will be set to "Most Compatible," which uses JPEG/ H.264; 4K at 60 fps (frames per second) and 1080p 240 fps. This format was chosen since it is the iPhone's default setting and does not alter the file size of the image (*See Figure 2).*

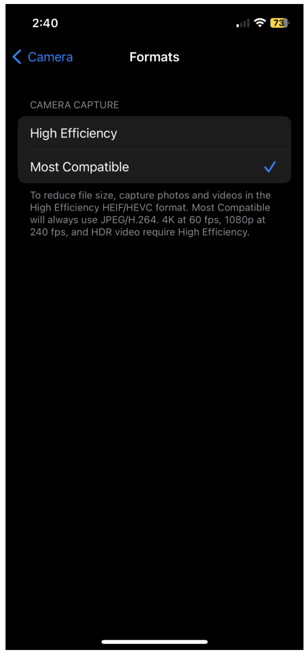

Figure 2. Test iPhone Camera Capture Format

Next, using the X application (Version 10.16) on the mobile device, a test account was created on the application that was used only for this experiment *(See Figure 3)*. Ten images were uploaded in separate posts, with no filters or changes added to the photos. The uploaded application-created photos were then downloaded from the "Save Photo" feature on the X application to the iOS device for analysis *(See Figure 4)*. The ten images downloaded came from the owner's account, or the original test account created.

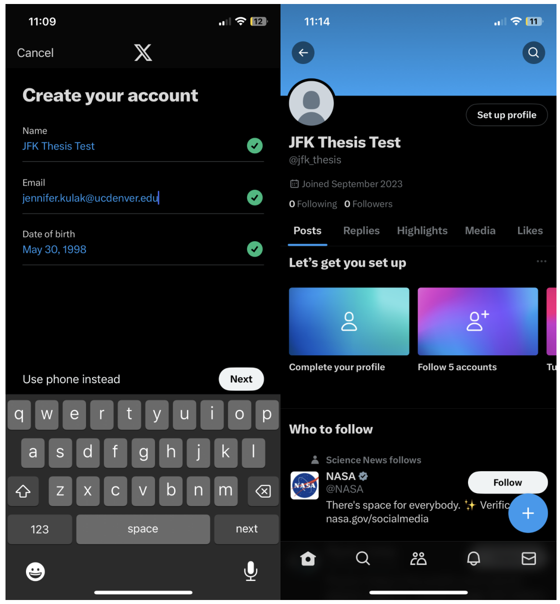

Figure 3. First X Test Account Created for Experiment

Analyzing the 10 images' file structure prior to uploading, the software FIAS (Forensic Image Analysis System; Version 2023.09.27) was used to record the original encoding and file structure of the iOS created images. After uploading Test Set 2 Images and sending Test Set 3 Images through messages *(See Table 1),* all software mentioned above will be used again to collect data on the X-created image file that was downloaded to the iOS device.

Table 1. Details of Test Images Used in Experimentation

Image Set Title	Number/Type of Images	How Set Was Created
Test Set 1 Images	10	Taken with iPhone X
Test Set 2 Images	10 (*Same 10 images were used from Test Set 1)*	Uploaded to X via a Test Account and Downloaded
Test Set 3 Images	10 (*Same 10 images were used from Test Set 1)*	Sent from one X Test Account to another Test Account and Downloaded

CHAPTER III

METHODOLOGY

Test Set 1 Transfer from iPhone to Remote Desktop Connection (RDC)

Once Test Set 1 of Images were taken with the iPhone 12, the Airdrop feature was utilized on the iPhone 12 to share them onto a MacBook Pro. Apple's Terminal Window was used to generate both the SHA256 and MD5 hashes of the first set of images. Once the images were transferred securely, those hashes were generated and documented (*See Table 2 below).*

Table 2. Sample Images and Working Copies Hash Values

File Name	SHA256 Hash	MD5 Hash	Working Copy (WC) File Name	SHA256 Hash (WC)	MD5 Hash (WC)
Kulak_Sample_1.jpg	03C6608485D21EF51A93A8C0D92EACCCD38AD172E225077117DCD0DBE8062968	A74200BC2765AFD5AC770F64CCFEA0B5	SI_001.jpg	03C6608485D21EF51A93A8C0D92EACCCD38AD172E225077117DCD0DBE8062968	A74200BC2765AFD5AC770F64CCFEA0B5
Kulak_Sample_2.jpg	8D27A4909EDE0ABE5C8F97FAE39D1E5064B04F1947014978E626BD93D7877700	85FE7A946C01D01ECB32802EA35957D0	SI_002.jpg	8D27A4909EDE0ABE5C8F97FAE39D1E5064B04F1947014978E626BD93D7877700	85FE7A946C01D01ECB32802EA35957D0
Kulak_Sample_3.jpg	00874B965EA25B09B939E678689F29723CCB7005379E7BE4AA227D03DB5FEF93	2416C23663E7FFC6847620BACA6AD83A	SI_003.jpg	00874B965EA25B09B939E678689F29723CCB7005379E7BE4AA227D03DB5FEF93	2416C23663E7FFC6847620BACA6AD83A

Table 2. Continued

File Name	SHA256 Hash	MD5 Hash	Working Copy (WC) File Name	SHA256 Hash (WC)	MD5 Hash (WC)
Kulak_Sample_4.jpg	6A231AC7FB04A7CC3658B4098AEC40F44D117027DCB0E756BA190B5CB2B35E14	B57B0A8DE80BF9CF121A6E2C43FEDFD0	SI_004.jpg	6A231AC7FB04A7CC3658B4098AEC40F44D117027DCB0E756BA190B5CB2B35E14	B57B0A8DE80BF9CF121A6E2C43FEDFD0
Kulak_Sample_5.jpg	AF231470D65E2791B6B1A33A8F7F790F9D21CC61C2C0C4431CC1867328D0EE19	21052A866F739BDF19C9A3A34396E525	SI_005.jpg	AF231470D65E2791B6B1A33A8F7F790F9D21CC61C2C0C4431CC1867328D0EE19	21052A866F739BDF19C9A3A34396E525
Kulak_Sample_6.jpg	CBAAD175AA572AA9ED3D9054B15A103C3D053973EEF0B095E4C6AF2DD5062484	F126907A85D2083E8C7E488F03792BBE	SI_006.jpg	CBAAD175AA572AA9ED3D9054B15A103C3D053973EEF0B095E4C6AF2DD5062484	F126907A85D2083E8C7E488F03792BBE
Kulak_Sample_7.jpg	A986D924A786C988054EAC362D309B02D4480E13EBECF0A031A90DBD5CAF8284	11EF1223A0626CCB3C234311220DA553	SI_007.jpg	A986D924A786C988054EAC362D309B02D4480E13EBECF0A031A90DBD5CAF8284	11EF1223A0626CCB3C234311220DA553
Kulak_Sample_8.jpg	A693FB14F737E6D108BE9CF4EA61C93705B5DA7262B4B78A2E21E53BA336A205	1A817E63B40A3172C919ED5E3E889935	SI_008.jpg	A693FB14F737E6D108BE9CF4EA61C93705B5DA7262B4B78A2E21E53BA336A205	1A817E63B40A3172C919ED5E3E889935
Kulak_Sample_9.jpg	EC2518BF8B65930B22087A6C5D1302D42450FC103B024C62B7127D32D7F197DE	4970C97D7DF138E83DBA168DED851C31	SI_009.jpg	EC2518BF8B65930B22087A6C5D1302D42450FC103B024C62B7127D32D7F197DE	4970C97D7DF138E83DBA168DED851C31
Kulak_Sample_10.jpg	080D21437EBE23DC776C9309BBC4E44B6C34D49D0AA329DB5E25AE44B4230C1A	3A33DBA72F9BC484241049D0F24B6CFE	SI_010.jpg	080D21437EBE23DC776C9309BBC4E44B6C34D49D0AA329DB5E25AE44B4230C1A	3A33DBA72F9BC484241049D0F24B6CFE

Once this was verified as a viable method for transferring the images taken, uploaded, and sent through X to my laptop, the same steps were taken above for the Test Set 2 and Test Set 3 images.

Uploading Sample Images to X

Using the first image test set and the X account created on the iPhone 12, each sample image was posted in 10 different posts with no description. After they were posted, the photos were saved directly from X using the "Save Photo" button. Each posted image was saved to the iPhone's photo library (*See figure 4*).

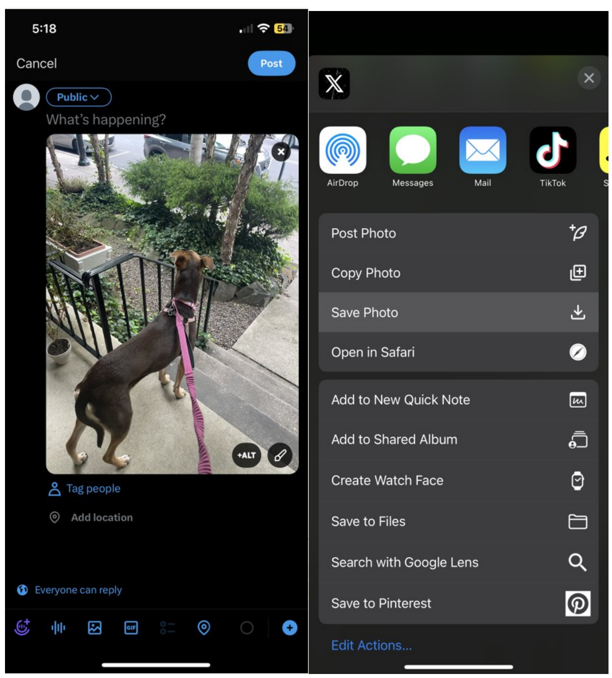

Figure 4. Test Images Uploading to X and Downloaded Back onto iPhone 12

After the 10 test images were uploaded to X and then downloaded onto the iPhone 12, the same methodology above was used to calculate the hash values of the posted Test Set 2 Images.

Airdrop was utilized to get the posted images set from the iPhone to a laptop. The hash values for Test Set 2 were then generated, which can be seen below in *Table 3*.

Table 3. Test Set 2 Posted Images Hash Values

File Name	SHA256 Hash	MD5 Hash
SP_001.jpg	1E1D7C0C10448AC26378E82B6D39E02F63B0E8BA68C098D5006F9A546D2E1E14	8F0EEDB28FED0E7446A6CD0156C9D6B8
SP_002.jpg	2FA44FC3E256EEF95768678A71ACE557C14874A7FF35F2879569AFA93E37DEDC	578357F11E0D716484BD6DC113627FF3
SP_003.jpg	A9AFADC8E71EA92505AD27F96BCB399A8C8B89D6C9AD302297C72898CADCA1F3	F8C858D510BC19A7ED73A4A7E4BD1B33
SP_004.jpg	33770811AE6AFBAE3030134A0300D7DA55541C79D45095B969775185EF85099A	660831F74BE91EF42530F8711E368066
SP_005.jpg	1DF790889D0F3193A71E833928BEFD878FF67327C889FE863C23F012401A9B0E	D60245ABC6E3F2069948653411C0CA3D
SP_006.jpg	C3BE53A709C20C1F9619960E4860D5962303ED63F123025254F9DAAB66A34AF6	9AEA837A390D1A54A5141F3187BC3924
SP_007.jpg	A411CF857BC92363B54DC56A8BC6377F23B923B7A2CBC544DE128CAAC0FF0C05	E8580BB91D47C4BDE5FCA3C7BFC46E3F
SP_008.jpg	3CEC2FD81A2746151FF551E4DBDB215BF91437C5119DB58C3C473687BC0B64DE	14F890FC0CC403C6D4451D7C217C9077
SP_009.jpg	8AE3F39EF2B980C475765DD4D37B047EA21BAF0F0C0335E52AF292138F3ECC1E	D64299A1A5468A5EC4625586377032E2
SP_010.jpg	69167DE98E0003AB16C67FDC7CCB3FE02C1072B6B590105A81187553B5E4266F	592F2083A4B71077D33129437616D1AE

Sending Sample Images Through X's Messages Feature

To answer the second RQ, "Does the X application-created image file change the image stream when sent to another X recipient?" A new Google email account was made to generate another test account on X. This second account was used solely to send images to the original X test account, "JFK Thesis Test." Below in *Figure 5*, the steps taken to create the second X account and send the test images through messages can be seen.

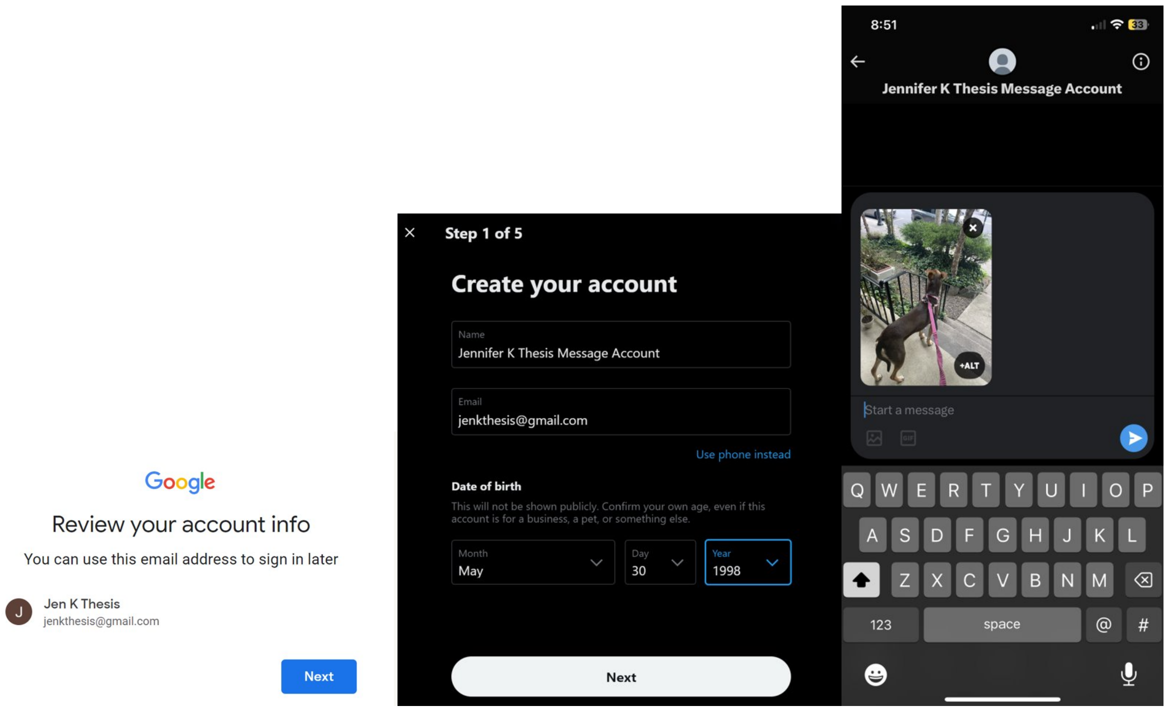

Figure 5. Creating Second Test Account for Sending Images

Once the 10 sample images were sent through X's messages feature, each of the photos were downloaded to the iPhone's library and the Airdrop method was utilized again to transfer them for analysis. The SHA256 and MD5 hash values of the sent/messaged images were created and can be seen below (*Table 4)*.

Table 4. Test Set 3 Messaged Images Hash Values

File Name	SHA256	MD5
SM_001.jpg	BAC34AFCFA09527CE874B91410 4F0A2540F66C3E6EC75B00A5AE DAEB07EFE0EE	9C6A61C694B300D22B2FD0B570 213571
SM_002.jpg	593CEC8FAF0DC0537AA8A1D16 D1EBCE21B06EC816459EBABB2 DBEBDC29D0EDE1	C894DB62012EDE35A6D40DC61 CA313E5
SM_003.jpg	E88CD19BBEB23629B72C9C495 CED898BC4A95B2F52ACA54857 070C8531A9B45E	A735C17AE56CD287A2677A09D 1C5FA7D
SM_004.jpg	29C75AA488C5A2A950C0064A2 B695D51554C144A4DF3E2E985C 6E0AE59A60AD4	24EB53E9255C2FF3C910A1181F B6E3AD
SM_005.jpg	EB27089050D61DDDE7796C0E47 4D7FF301CA4A6318B512BAD95 AED0448FFBD2C	811C687F208B97D10876D19681A CE544
SM_006.jpg	7F906F75E6622FAC942787AC735 AFA04AC1DC8DCD0E3E6513E6 F3C594A803DD1	B76D1D29CEB42ECAF0A63C698 D22CF2F
SM_007.jpg	2C3181DB0E3C2E3449CB4BDB7 5AA42F691F8726A6C379649503C BCD5554024C6	010F37E8A634E0ADB1C5E0670B DFB143
SM_008.jpg	095E9B5691B1DC80C905FB8C2F 747BBF5A9079DAAF00B25E7986 7D5507995FD4	8F3D3E3EF7B60AFD1B9CBFE2B CA7BB10
SM_009.jpg	3F9FEDE87B28CF71F4790A7FC8 5CF28A73B45C848241B4ADD1B 9F8296D6FA6BA	C1FD607507D343A35E013C98C1 EEC3A7
SM_010.jpg	D02E7658285D022C755DB53EB4 754D5E7755BE1E47102B925F5F D631603DD3F2	DB11BC2E2F726B50C3E34B93A F1E4B78

CHAPTER IV

RESULTS

FIAS Results

Using the software, FIAS, a Structure and EXIF (Exchangeable Image File Format) analysis, QT (Quantization Tables) analysis, and a Hex Analysis were performed. In *Figure 6* below, one can see, highlighted, the analyses ran on each of the images.

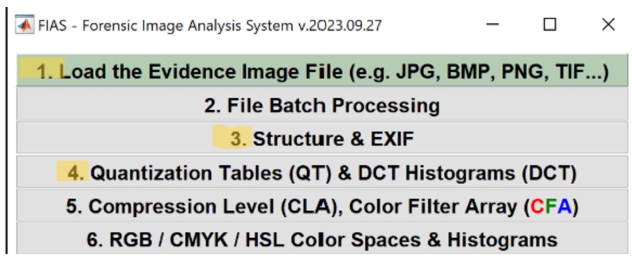

Figure 6. FIAS Menu/Analysis Steps Performed

EXIF Analysis Test Set 1 and Test Set 2 Comparison

The key differences between the EXIF analyses of Test Set 1 and Test Set 2 are that the posted images Test Set 2 EXIF analysis does not contain any specifics about the camera used to capture the photo. Test Set 1 EXIF provides information about it being taken on an iPhone 12, the software version of the iPhone 12, information about the flash, focal length, and subject area. Test Set 2 EXIF analysis did not provide any of the aforementioned characteristics. Another key difference to note is that the X application changed the image size and the megapixels of the image. For example, in SI_001.jpg the image size is 4032x3024 and the megapixels are 12.2. In SP_001.jpg (the image posted to X), the image size is 1536x2048 and the megapixels are 3.1 *(See Figure 7 below).*

Report-exif.txt - Notepad

File Name	SI-001.JPG
File Size	5.5 MB
File Modification Date/Time	2023:09:28 10:58:49-06:00
File Access Date/Time	2023:10:27 13:18:59-06:00
File Creation Date/Time	2023:10:27 13:18:51-06:00
File Permissions	-rw-rw-rw-
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
JFIF Version	1.01
Exif Byte Order	Big-endian (Motorola, MM)
Make	Apple
Camera Model Name	iPhone 12
Orientation	Rotate 90 CW
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Software	16.3.1
Modify Date	2023:09:28 12:58:48
Host Computer	iPhone 12
Y Cb Cr Positioning	Centered
Exposure Time	1/60
F Number	1.6
Exposure Program	Program AE
ISO	80
Exif Version	0232
Date/Time Original	2023:09:28 12:58:48
Create Date	2023:09:28 12:58:48
Offset Time	-04:00
Offset Time Original	-04:00
Offset Time Digitized	-04:00
Components Configuration	Y, Cb, Cr, -
Shutter Speed Value	1/60
Aperture Value	1.6
Brightness Value	3.138932496
Exposure Compensation	0
Metering Mode	Multi-segment
Flash	Off, Did not fire
Focal Length	4.2 mm
Subject Area	2015 1511 2323 1393
Maker Note Version	14
Run Time Flags	Valid
Run Time Value	397346125069125
Run Time Scale	1000000000
Run Time Epoch	0
AE Stable	Yes
AE Target	175
AE Average	166
AF Stable	Yes

Report-exif.txt - Notepad

File Name	SP-001.JPG
File Size	820 kB
File Modification Date/Time	2023:10:17 19:26:29-06:00
File Access Date/Time	2023:10:27 13:46:08-06:00
File Creation Date/Time	2023:10:27 13:46:04-06:00
File Permissions	-rw-rw-rw-
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
X Resolution	72
Y Resolution	72
Resolution Unit	inches
Modify Date	2023:09:28 17:19:31
Y Cb Cr Positioning	Centered
Exif Version	0221
Date/Time Original	2023:09:28 17:19:31
Create Date	2023:09:28 17:19:31
Offset Time	-04:00
Offset Time Original	-04:00
Offset Time Digitized	-04:00
Components Configuration	Y, Cb, Cr, -
Sub Sec Time	874
Sub Sec Time Original	874
Sub Sec Time Digitized	874
Flashpix Version	0100
Color Space	sRGB
Exif Image Width	1536
Exif Image Height	2048
Scene Capture Type	Standard
Compression	JPEG (old-style)
Thumbnail Offset	478
Thumbnail Length	13351
Profile CMM Type	Apple Computer Inc.
Profile Version	4.0.0
Profile Class	Display Device Profile
Color Space Data	RGB
Profile Connection Space	XYZ
Profile Date Time	2022:01:01 00:00:00
Profile File Signature	acsp
Primary Platform	Apple Computer Inc.
CMM Flags	Not Embedded, Independent
Device Manufacturer	Apple Computer Inc.
Device Model	
Device Attributes	Reflective, Glossy, Positive, Col
Rendering Intent	Perceptual
Connection Space Illuminant	0.9642 1 0.82491
Profile Creator	Apple Computer Inc.
Profile ID	ecfda38e388547c36db4bd4f7ada182f

Figure 7. EXIF Analysis of Test Set 1 and Test Set 2

```
Thumbnail Offset                : 2544
Thumbnail Length                : 12949
MPF Version                     : 0100
Number Of Images                : 2
MP Image Flags                  : (none)
MP Image Format                 : JPEG
MP Image Type                   : Undefined
MP Image Length                 : 290600
MP Image Start                  : 5234132
Dependent Image 1 Entry Number  : 0
Dependent Image 2 Entry Number  : 0
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Col
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ecfda38e388547c36db4bd4f7ada182f
Profile Description             : Display P3
Profile Copyright               : Copyright Apple Inc., 2022
Media White Point               : 0.96419 1 0.82489
Red Matrix Column               : 0.51512 0.2412 -0.00105
Green Matrix Column             : 0.29198 0.69225 0.04189
Blue Matrix Column              : 0.1571 0.06657 0.78407
Chromatic Adaptation            : 1.04788 0.02292 -0.0502 0.02959 0
Image Width                     : 4032
Image Height                    : 3024
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Run Time Since Power Up         : 4 days 14:22:26
Aperture                        : 1.6
Image Size                      : 4032x3024
Megapixels                      : 12.2
Scale Factor To 35 mm Equivalent: 6.2
Shutter Speed                   : 1/60
Create Date                     : 2023:09:28 12:58:48.882-04:00
Date/Time Original              : 2023:09:28 12:58:48.882-04:00
Modify Date                     : 2023:09:28 12:58:48-04:00
```

```
Offset Time Digitized           : -04:00
Components Configuration        : Y, Cb, Cr, -
Sub Sec Time                    : 874
Sub Sec Time Original           : 874
Sub Sec Time Digitized          : 874
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 1536
Exif Image Height               : 2048
Scene Capture Type              : Standard
Compression                     : JPEG (old-style)
Thumbnail Offset                : 478
Thumbnail Length                : 13351
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Col
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ecfda38e388547c36db4bd4f7ada182f
Profile Description             : Display P3
Profile Copyright               : Copyright Apple Inc., 2022
Media White Point               : 0.96419 1 0.82489
Red Matrix Column               : 0.51512 0.2412 -0.00105
Green Matrix Column             : 0.29198 0.69225 0.04189
Blue Matrix Column              : 0.1571 0.06657 0.78407
Chromatic Adaptation            : 1.04788 0.02292 -0.0502 0.02959 0
Image Width                     : 1536
Image Height                    : 2048
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                      : 1536x2048
Megapixels                      : 3.1
Create Date                     : 2023:09:28 17:19:31.874-04:00
Date/Time Original              : 2023:09:28 17:19:31.874-04:00
Modify Date                     : 2023:09:28 17:19:31.874-04:00
```

Figure 7. Continued

EXIF Analysis Test Set 2 and Test Set 3 Comparison

In the interest of answering RQ2, the comparison of Test Set 2 (Posted images) and Test Set 3 (Sent images) shows the application, X, makes similar changes to an image's data when it is uploaded to the application and sent through the messages feature. The reason for comparing these two is that they are almost identical to one another, except that the Sub Sec Time, Sub Sec Time Original, and Sub Sec Time Digitized are different *(Figure 8*). However, the analyses of the Test Set 2 and Test Set 3 differ from Test Set 1, as discussed in the previous section.

```
File Name                       : SP-001.JPG
File Size                       : 820 kB
File Modification Date/Time     : 2023:10:17 19:26:29-06:00
File Access Date/Time           : 2023:10:27 13:46:08-06:00
File Creation Date/Time         : 2023:10:27 13:46:04-06:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2023:09:28 17:19:31
Y Cb Cr Positioning             : Centered
Exif Version                    : 0221
Date/Time Original              : 2023:09:28 17:19:31
Create Date                     : 2023:09:28 17:19:31
Offset Time                     : -04:00
Offset Time Original            : -04:00
Offset Time Digitized           : -04:00
Components Configuration        : Y, Cb, Cr, -
Sub Sec Time                    : 874
Sub Sec Time Original           : 874
Sub Sec Time Digitized          : 874
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 1536
Exif Image Height               : 2048
Scene Capture Type              : Standard
Compression                     : JPEG (old-style)
Thumbnail Offset                : 478
Thumbnail Length                : 13351
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Col
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ecfda38e388547c36db4bd4f7ada182f
```

```
File Name                       : SM-001.JPG
File Size                       : 820 kB
File Modification Date/Time     : 2023:10:17 19:29:47-06:00
File Access Date/Time           : 2023:10:27 14:11:29-06:00
File Creation Date/Time         : 2023:10:27 14:11:27-06:00
File Permissions                : -rw-rw-rw-
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Modify Date                     : 2023:09:28 21:09:51
Y Cb Cr Positioning             : Centered
Exif Version                    : 0221
Date/Time Original              : 2023:09:28 21:09:51
Create Date                     : 2023:09:28 21:09:51
Offset Time                     : -04:00
Offset Time Original            : -04:00
Offset Time Digitized           : -04:00
Components Configuration        : Y, Cb, Cr, -
Sub Sec Time                    : 178
Sub Sec Time Original           : 178
Sub Sec Time Digitized          : 178
Flashpix Version                : 0100
Color Space                     : sRGB
Exif Image Width                : 1536
Exif Image Height               : 2048
Scene Capture Type              : Standard
Compression                     : JPEG (old-style)
Thumbnail Offset                : 478
Thumbnail Length                : 13351
Profile CMM Type                : Apple Computer Inc.
Profile Version                 : 4.0.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2022:01:01 00:00:00
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Apple Computer Inc.
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Col
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Apple Computer Inc.
Profile ID                      : ecfda38e388547c36db4bd4f7ada182f
```

Figure 8. EXIF Analysis of Test Set 2 and Test Set 3

QT Analysis Test Set 1, 2, and 3 Comparison

The analysis of Quantization Tables allows one to see the changes in quality of an image. The tables shown on the left reveal the sample image's quantization table and the right shows the images that were posted to X. "Using JPEG quantization tables to identify imagery processed by software," by Jesse D. Kornblum explains how Quantization Tables can show whether an image has been processed through software. Within this work, Kornblum explains that the lower the numerical value, the less data that is removed from the compression, which results in a higher-quality image (2008, p. S22). Examining the images from Test Set 1 against the images in Test Set 2, one can see the numerical values of Test Set 2 are doubled/higher than the Test Set on the left-handed side *(Figure 9)*.

SI-001-QT.txt - Notepad

1	1	1	2	3	4	5	6
1	1	1	2	3	4	5	6
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	8
3	3	4	5	6	7	8	9
4	4	5	6	7	8	9	9
5	5	6	7	8	9	9	9
6	6	7	8	9	9	9	9
1	1	2	4	9	9	9	9
1	2	2	6	9	9	9	9
2	2	5	9	9	9	9	9
4	6	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9
9	9	9	9	9	9	9	9

SP-001-QT.txt - Notepad

4	4	4	7	10	13	16	20
4	4	4	7	10	13	16	20
4	4	7	10	13	16	20	24
7	7	10	13	16	20	24	28
10	10	13	16	20	24	28	31
13	13	16	20	24	28	31	31
16	16	20	24	28	31	31	31
20	20	24	28	31	31	31	31
5	5	8	14	32	32	32	32
5	7	7	22	32	32	32	32
8	7	18	32	32	32	32	32
14	22	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32

Figure 9. QT Analysis of Test Set 1 and Test Set 2

Comparison of Test Set 2 (Posted images) and Test Set 3 (Messaged images) showed that the quantization tables were the same for each of the images in the sets. In the examples below, one can see SP_002.jpg, SP_003.jpg, SM_002.jpg, and SM_003.jpg have the same table *(Figure 10 and 11).*

SM-002-QT.txt - Notepad

4	4	4	7	10	13	16	20
4	4	4	7	10	13	16	20
4	4	7	10	13	16	20	24
7	7	10	13	16	20	24	28
10	10	13	16	20	24	28	31
13	13	16	20	24	28	31	31
16	16	20	24	28	31	31	31
20	20	24	28	31	31	31	31
5	5	8	14	32	32	32	32
5	7	7	22	32	32	32	32
8	7	18	32	32	32	32	32
14	22	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32

SP-002-QT.txt - Notepad

4	4	4	7	10	13	16	20
4	4	4	7	10	13	16	20
4	4	7	10	13	16	20	24
7	7	10	13	16	20	24	28
10	10	13	16	20	24	28	31
13	13	16	20	24	28	31	31
16	16	20	24	28	31	31	31
20	20	24	28	31	31	31	31
5	5	8	14	32	32	32	32
5	7	7	22	32	32	32	32
8	7	18	32	32	32	32	32
14	22	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32

SP-003-QT.txt - Notepad

4	4	4	7	10	13	16	20
4	4	4	7	10	13	16	20
4	4	7	10	13	16	20	24
7	7	10	13	16	20	24	28
10	10	13	16	20	24	28	31
13	13	16	20	24	28	31	31
16	16	20	24	28	31	31	31
20	20	24	28	31	31	31	31
5	5	8	14	32	32	32	32
5	7	7	22	32	32	32	32
8	7	18	32	32	32	32	32
14	22	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32

SM-003-QT.txt - Notepad

4	4	4	7	10	13	16	20
4	4	4	7	10	13	16	20
4	4	7	10	13	16	20	24
7	7	10	13	16	20	24	28
10	10	13	16	20	24	28	31
13	13	16	20	24	28	31	31
16	16	20	24	28	31	31	31
20	20	24	28	31	31	31	31
5	5	8	14	32	32	32	32
5	7	7	22	32	32	32	32
8	7	18	32	32	32	32	32
14	22	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32
32	32	32	32	32	32	32	32

Figure 10 and 11. QT Analysis of Test Set 2 and 3

Hex Analysis Test Set 1, 2, and 3 Comparison

When comparing the Hex data of the same image of each separate set (SI_001.jpg, SP_001.jpg, etc.) one can see that the images from Test Set 1 have Hex data that provides more information about the image, camera used, and the device used to capture the image.

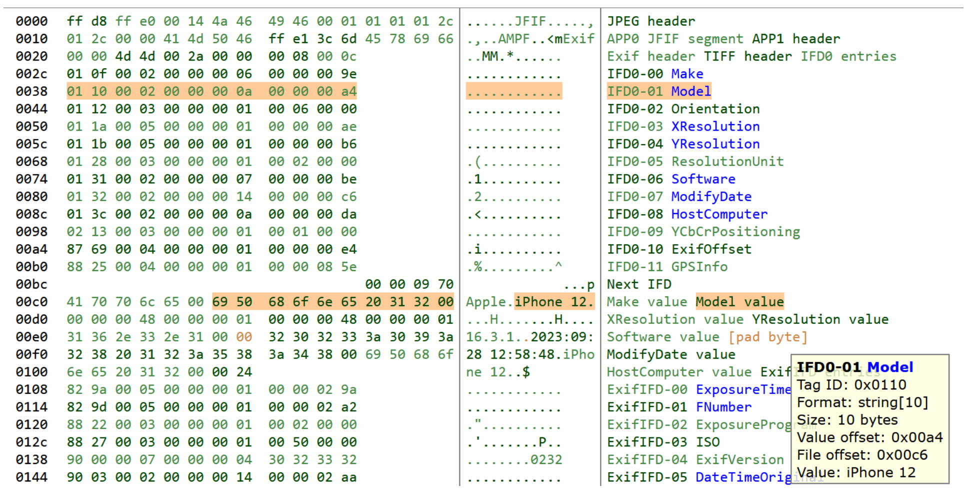

Figure 12. Beginning Hex Data for SI_001.jpg

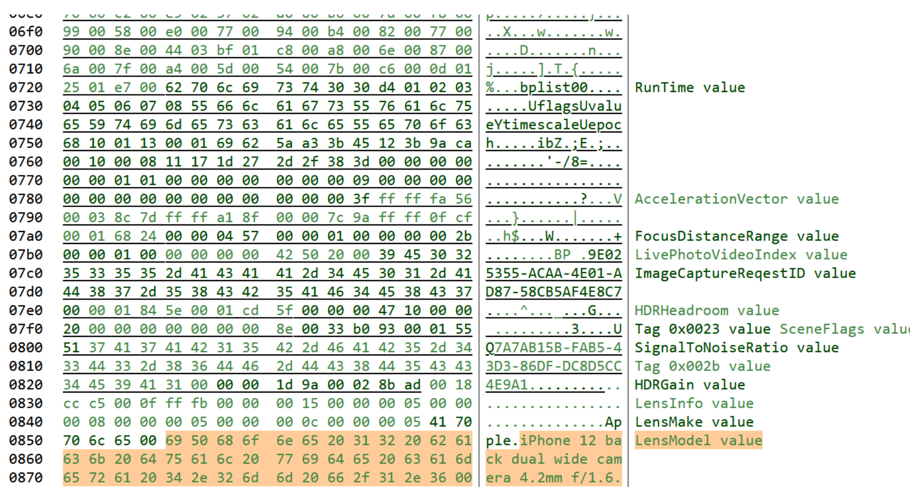

Figure 13. Hex Data for SI_001.jpg

When looking at *Figure 12* and *Figure 13* above, one can see that the images taken with the iPhone 12 have more data in the file and provide more information about the device that was used to capture the image. However, when looking at the Hex data provided from the images that were uploaded and messaged through the X application, one sees that the information about where and what the picture came from is not provided (*See Figure 14 and Figure 15)*.

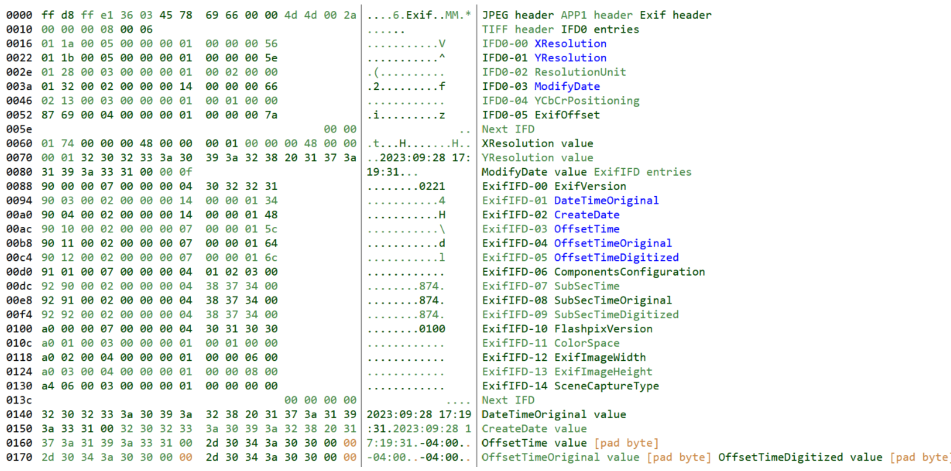

Figure 14. Beginning Hex Data for SP_001.jpg

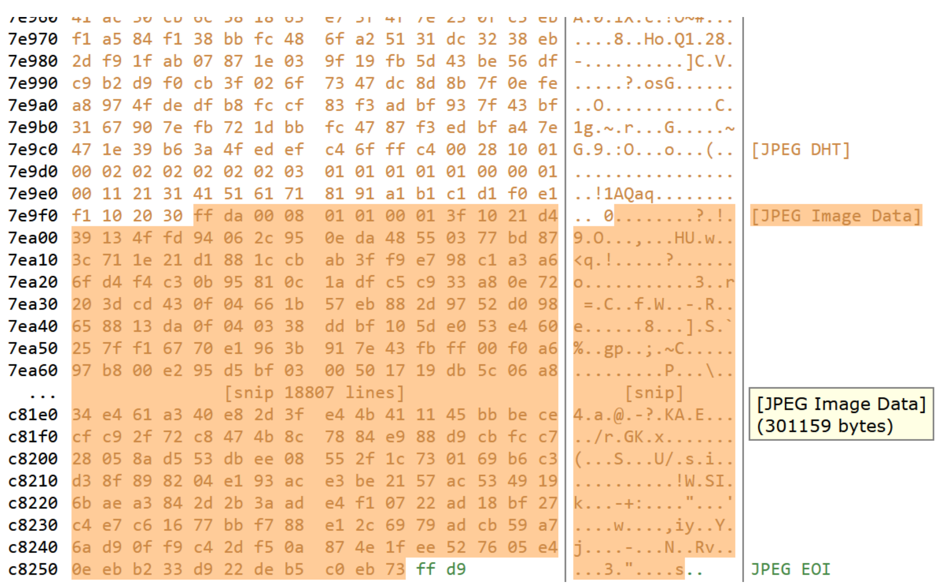

Figure 15. Ending Hex Data for SP_001.jpg

CHAPTER V

CONCLUSIONS

In closing, after capturing 10 images with my iPhone 12, uploading them to the social media application X, and messaging them to another recipient on X, one can conclude that X does make changes to an image's data stream. First with ensuring that the method of transfer from the iPhone device to a laptop for analysis, the method of using Airdrop and creating a zip file kept the integrity of the original image taken with the phone. The hash values of the original 10 images and their working copies were a match, and comparing those values to the values of the Test Sets that were uploaded to the app and messaged, I concluded that the hash values were different.

Not only this, the EXIF information for the original image Test Set (Test Set 1) was different from Test Set 2 and 3. The EXIF analysis showed that the X-created image files did not provide much or any information about what device/camera the photo was taken on. The QT analysis also showed that the X-created image files were different than the original iOS image files. It appears through all the analysis conducted that the application X does make some structural changes to an image's data. When comparing these Test Sets between one another, one can infer which of the images came directly from the iOS device and which came from X.

Implications and Contributions to Knowledge

Overall, this proposal provides for knowledge gaps in analyzing metadata and file structure changes made to an image using X. These findings are intended to create more guidelines for forensic investigators when they need to analyze an image uploaded to the X application. Changes to these images are crucial to investigators, as it can help them to detect changes and decipher an original image from an X-created image. This proposal's purpose is to contribute more research into this issue and assist in creating new digital forensic guidelines.

This work will help to strengthen other research and experimentation on this specific topic. If more research on the matter of X-created images becomes known, it will spark a need to understand similar implications that may occur in the future, as technology and social media applications change. Overall, investigators and the digital forensic community can highly benefit from this research, and other research on this topic. Not only does this research serve the digital forensic community, but it may also assist other scientific communities in understanding social media application changes to images and other digital files.

REFERENCES

1. American Society for Testing and Materials (ASTM) International. (2022, May 12). Standard Guide for Forensic Digital Image Processing. ASTM International. Retrieved July 16, 2022, from https://www.astm.org/e2825-21.html

2. Arai, H. N. (2018, December 15). Digital Image Recompression Analysis: Sino Weibo. ProQuest. Retrieved June 14, 2022, from https://www.proquest.com/docview/2158384292/D7F2696D61754A06PQ/3accountid=14506

3. Castiglione, A., Cattaneo, G., & de Santis, A. (2011). A Forensic Analysis of Images on Online Social Networks. 2011 Third International Conference on Intelligent Networking and Collaborative Systems. https://doi.org/10.1109/incos.2011.17

4. Douglas, Z. (2018, May 12). Digital Image Recompression Analysis of Instagram. ProQuest. Retrieved June 14, 2022, from https://www.proquest.com/docview/2061630572?pq-origsite=gscholar&fromopenview=true

5. Kornblum, J. D. (2008, May 26). Using JPEG quantization tables to identify imagery processed by software. ScienceDirect. Retrieved November 14, 2023, from https://www.sciencedirect.com/science/article/pii/S1742287608000285

6. SWGDE. (2018, July 11). SWGDE - Imaging - Best Practices for Image Authentication. Retrieved June 14, 2022, from https://www.swgde.org/documents/swgit-document-archive