ANALYSIS OF EMAIL AS A COLLECTION METHOD OF DIGITAL IMAGE EVIDENCE FROM APPLE IOS

by

ANIESHA REBEKAH JOJOLA

B.S., Regis University, 2018

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

Aniesha Rebekah Jojola

has been approved for the

Media Forensics Program

by

Catalin Grigoras, Chair

Gregory S. Wales

Cole M. Whitecotton

Date: May 13, 2023

Jojola, Aniesha Rebekah (M.S., Media Forensics Program)

Analysis of Email as a Collection Method of Digital Image Evidence from Apple iOS

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

For evidence-collection purposes, it makes sense that iPhones and email would be commonly expected to be acceptable forms of data acquisition since they are so heavily utilized in our modern society. However, sending images from iPhones is not always a forensically sound method for collecting image data, no research has been published specifically testing the validity of collecting digital evidence from Apple iOS via the native Mail application. Furthermore, because this method has not been targeted for forensic investigation, there has been a knowledge gap in this area in the scientific community.

This research was therefore conducted to fill this knowledge gap in the forensic field. Images were collected from various iPhone models and emailed via the Mail application native to Apple iOS. All image data originating on the phones were extracted for analysis, along with the emailed images that were sent from these devices.

Some analysis results were mostly inconclusive due to limiting factors, and further research is suggested. However, stream hash analysis and metadata analysis were completed so that conclusions could be made. These conclusions were that only the Actual image size email option could be relied upon as a forensically sound delivery method for images. Images sent as Actual size could be considered digital clones of the original images and can therefore be trusted when collected as evidence. This statement is contingent upon these images having the same image capture settings selected on the iPhones at the time of their capture as utilized in our testing environment. Any modifications to the camera settings could still alter images deeming

them evidentiarily useless even if still emailed as Actual size.

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

Approved: Catalin Grigoras

ACKNOWLEDGEMENTS

I would like to thank the entire NCMF Staff for their instruction and endless support throughout this entire program. Thanks to Leah Haloin for holding, it all down and making sure we were kept on track and prepared for every step along the way. Special thanks to Greg Wales for his guidance and specific influence on this thesis work, for helping me with the experiment and its progress. A very big thank you to Catalin Grigoras for being always available (does he ever sleep?) to answer any questions, provide further explanation, or calm some nerves with a pep talk, providing motivation and confidence with his endless supplies of kindness and knowledge. Also thank you to my fellow classmates, who were an inspiration and a joy to learn and collaborate with.

TABLE OF CONTENTS

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF ABBREVIATIONS

iOS – iPhone Operating System

IQA – Image Quality Analysis

NCMF – National Center for Media Forensics

PRNU – Photo Response Non-Uniformity

SHA-256 – Secure Hashing Algorithm, 256 Bits

CHAPTER I

INTRODUCTION

In today's world email as a form of communication and sharing information is the norm. It makes sense that this also applies to the legal domain. The discovery process now includes "e-discovery," which addresses the electronic aspect of collecting electronically stored information (ESI). Digital evidence is as prominent, if not more, than analog evidence. Since electronically stored information can only be shared digitally in its original format, emailing a digital image or a duplicate is equivalent to mailing an analogue image or duplicate. It should be admissible in court, given that the evidence is not damaged or corrupted in the delivery process. However, this is not always the case. Often, especially in high-profile cases, lawyers point fingers at the reporter and law enforcement for being incompetent in their data collection. Sometimes, it all comes down to one simple detail/error, the data transfer of the media files from the witness' device to the collection agency (and/or the subsequent transfers). One specific scenario reported numerous times is the situation where there were issues between what was on a witness mobile phone, the version the witness emailed the reporters, and what forensic experts found on the phone during the examination.

Not only is email now normalized as one of the most used forms of communication and information sharing, but mobile phones are also now the most common device used for image capture, as opposed to a digital or analog camera. Therefore, it only makes sense, since cameras for photography and email applications for sharing information both exist on cell phones, that it would be expected for people to use the easy option of emailing images directly from a cell phone for any reason necessary.

Unfortunately, for legal purposes, this method of image delivery and collection might not be the best option to use, forensically.

Research Purpose

This research looked at image data collection techniques from one specific brand of mobile phone devices (Apple's iPhone/ iOS) to identify and address the challenges faced. After reviewing previous research, experiments were conducted to help fill the knowledge gap in this specific area of interest. Finally, this paper proposes a forensically sound approach to tackling these challenges for increased efficacy in the acquisition of digital images from such devices for evidentiary purposes in the future.

Research Questions

The following research questions were developed as a basis for the research and experimentation performed. The intention of our data collection and analysis was an attempt to specifically answer these questions.

- **RQ1** - What are the differences between the image created with the native iPhone camera and the various sized email attachments?
- **RQ2** - Where are the downsized images used as email attachments stored on the email originating iPhone?
- **RQ3** - Do the downsized images used as email attachments provide artifacts for attribution to the original emailing iPhone?

Answering these questions help the forensic community to determine if evidence should be collected via email from Apple devices or if these images need to be extracted directly from the device to be determined as original images. These questions and attempts to answer them are directly in support of the research intentions.

Previous Research

The Scientific Working Group on Digital Evidence (SWGDE) has created Minimum Requirements for Testing Tools used in Digital and Multimedia Forensics [5], along with Recommended Guidelines for Validation Testing [6]. These resources are the foundational references for these experiments as it was discovered through my research that there had not been any published papers on this specific research topic. Additionally, no evidence was found that attempts were made to verify image data received from the iPhone iOS native Mail application nor was there research on the validity of this tool as a forensically sound image collection method.

An investigation into previous research yielded some results indicating that papers have been published on similar or related topics. For example, analysis was performed on digital images after being processed via the Twitter application [3]. Many images are often uploaded from mobile devices to social media platforms, which could then be attempted to be collected for evidentiary purposes. Closer to the mark, some experiments have analyzed iPhone videos transmitted over various methods [2]. Even closer, research on iPhone image transfer methods was conducted by University of Colorado graduate student John Nelson in 2020 [4]. His research was closest to the research presented here. To provide a quick comparison, he used only Actual sized images, his dataset appeared to be smaller, and his intention was to compare the destructive

or nondestructive qualities between multiple image delivery methods. It is important to note that he found that the emailed versions of Actual images were non-destructive, and file hashes matched originals.

As noted in the 2019 paper, “Detection of Tampering by Image Resizing Using Local Tchebichef Moments” [8], “no matter which image resizing technique is adopted, it will destroy local texture and spatial correlations among adjacent pixels to some extent.” This is one reason image resizing is a variable worth considering when testing image collection tools. This variable was one of the variables considered in this research. Unfortunately, to date, an extensive analysis of email as a collection method of digital evidence from Apple iOS has not been conducted. This research aims to address this knowledge gap in the scientific community.

CHAPTER II

MATERIALS

The experiment required the use of multiple Apple iPhones. We chose three different iPhone models. First, we created image data on each phone. Then this data was collected and analyzed using various tools. The phones, their data, and the collection/analysis tools utilized are as follows:

Cell Phones

Table 1. iPhones

iPhone	Make	Model	Operating System
1	iPhone 12 Pro Max	13.4	15.5
2	iPhone 8	10.4	14.7.1
3	iPhone SE	8.4	14.4

Cell Phone Data

Each cell phone was used to collect 10 images for a total of 30 images created for our original source data.

Table 2. Photos Taken

iPhone	Make	Photos Taken
1	iPhone 12 Pro Max	10
2	iPhone 8	10
3	iPhone SE	10
Total		30

Each cell phone was used to email each image four times. In addition, each delivery size option available (Actual, Small, Medium, and Large) was used resulting in a total of 120 photos that were emailed.

Table 3. Photos Emailed

iPhone	Make	Actual	Small	Medium	Large	Phone Total
1	iPhone 12 Pro Max	10	10	10	10	40
2	iPhone 8	10	10	10	10	40
3	iPhone SE	10	10	10	10	40
Total		30	30	30	30	120

Cellebrite Software was utilized to extract the original photos and the emailed versions from the phones. The emailed versions were not detected on the phones. Only the original photos were found on the phones and were able to be extracted.

Table 4. Photos Extracted for Analysis

iPhone	Make	Original	Actual	Small	Medium	Large	Phone Total
1	iPhone 12 Pro Max	10	0	0	0	0	10
2	iPhone 8	10	0	0	0	0	10
3	iPhone SE	10	0	0	0	0	10
Total		30	0	0	0	0	30

Data Collection and Analysis Tools

The following tools were utilized in the collection and analysis of the phone data.

Apple's Mail Application

Apple Mail is an application that is native to all of Apple's iOS devices. This application was used for the transmission of image data via email.

Cellebrite Physical Analyzer Version 7.55.2.2

Cellebrite is a forensic tool used to collect, review, analyze, and manage digital data. For our purposes, we used the Physical Analyzer tool to attempt to collect and analyze the original photos that were taken with the phones along with the alternative versions (actual, small, medium, large) that were emailed from the phones.

Cellebrite UFED 4 PC

Cellebrite UFED stands for "Universal Forensics Extraction Device". This tool from the Cellebrite suite of software applications was used to extract all image data from each of the phones tested. The extraction via this tool is necessary before loading it into the Physical Analyzer software.

Ffmpeg

Ffmpeg is an open-source software program that can handle multimedia data for multiple uses. For this experiment, this tool was utilized to calculate the SHA-256 Stream Hashes of the image files tested.

MediaInfo

MediaInfo is another opensource tool that displays technical information about media files. It was used in this case to view the metadata of the image files tested.

Data for Analysis

The original photos collected from the Cellebrite extraction were used for analysis. There were 30 total original images extracted.

The intention was to collect 120-150 images from the Cellebrite extraction (the 30 original images plus a possible 90-120 images identified as the actual, small, medium, and large email image options), but only the originals were found on the phone.

Table 5. Photos Extracted and Analyzed

iPhone	Make	Original	Phone Total
1	iPhone 12 Pro Max	10	10
2	iPhone 8	10	10
3	iPhone SE	10	10
Total		30	30

The images received from the iPhones after being emailed via the Mail app were safely downloaded and used for comparison to the original image files extracted directly from the iPhones. A total of 120 emailed images of various delivery options were analyzed and compared to their respective image files originating from the iPhones.

Table 6. Photos Emailed and Analyzed

iPhone	Make	Actual	Small	Medium	Large	Phone Total
1	iPhone 12 Pro Max	10	10	10	10	40
2	iPhone 8	10	10	10	10	40
3	iPhone SE	10	10	10	10	40
Total		30	30	30	30	120

CHAPTER III

METHODOLOGY

The procedures for developing, collecting, and analyzing the test data are below. These procedures were applied to our experiments to answer Research Questions #1 and #2. Unfortunately, there were no procedures developed for Research Question #3 since RQ3 was dependent upon the findings from RQ2 and locating downsized photos on the phones, which did not occur. There were also limitations further testing for RQ3, which will be readdressed in the conclusions chapter of this paper.

Development of Test Data Procedure

1. Step 1 - Evaluate Phones and Consider Testing Options

- Evaluate each model phone camera capture format options and email options. Consider image test options:
- High Efficiency
- Most Compatible
- Apple ProRAW

- Consider email test options:
- Actual Size
- Large
- Medium
- Small

2. Step 2 - Camera Settings - *See Figure 1.*

- Turn off:
- Scene Detection
- Prioritize Faster Shooting
- Lens Correction
- Smart HDR
- Live Photo
- Photographic Styles

- Camera Zoom Settings:
- 0.5 (Do Not Use)
- 1 (Only Camera Zoom Setting)

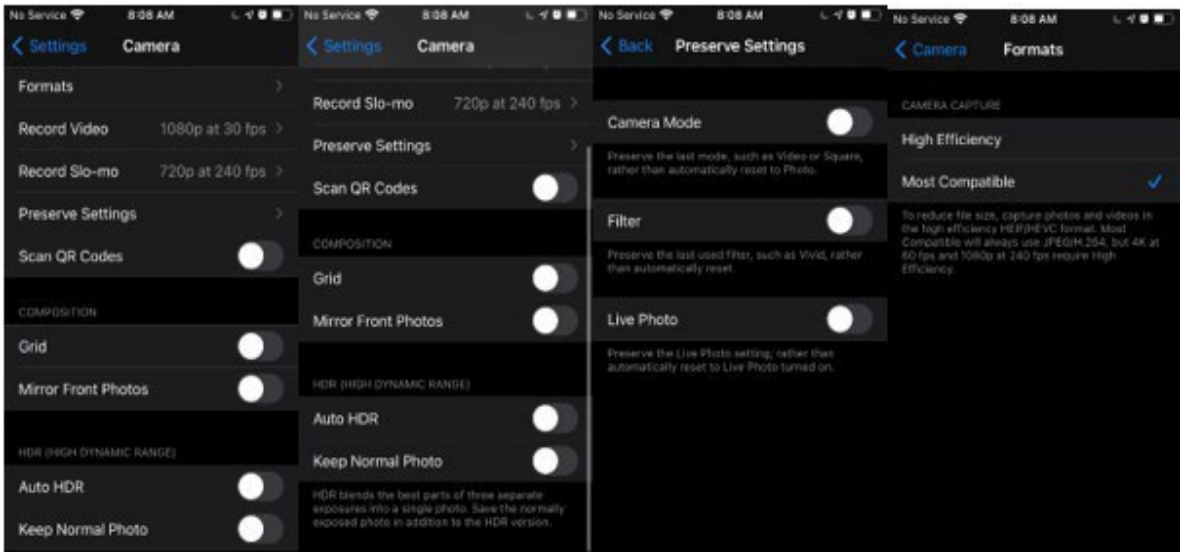

Figure 1. Camera Settings Example from iPhone8 15.4.1

- 2.5 (Do Not Use)

- Camera Mode Settings:
- Photo (Only Camera Mode Setting Used)
- Portrait (Do Not Use)
- Panorama (Do Not Use)
- Flash (Do Not Use)

- Camera Aspect Ratio Settings:
- Square
- 4:3
- 16:9

3. Step 3 – Create Photos

- Create photos per device:

- iPhone 12 Pro Max (Phone1)
    - High Efficiency (HE) x 10 (do not use)
    - Most Compatible (MC) x 10 (use)
    - Apple ProRAW (APR) x 10 (do not use)

- iPhone8 (Phone2)
    - High Efficiency (HE) x 10 (do not use)
    - Most Compatible (MC) x 10 (use)

- iPhoneSE (Phone1)
    - Most Compatible (MC) x 10 (use) – there are no other capture format setting options on this phone.

4. Step 4 – Email images as attachments for each size option for each photo on each phone

- Create per device, attach each photo, and mail each attachment per setting:

- Actual Size
- Large
- Medium
- Small

Collect Phone Test Data Procedure

1. Step 1

   Collect each device logical + advanced logical + file system (if available) Cellebrite UFED 4 PC capture of all relevant test data (images, email, and logs/file system data).

2. Step 2

   Load each device capture into Cellebrite PA and examine for relevant test data.

Collect Email Test Data Procedure

1. Step 1

   Access destination email account on a computer using a standardized application and configuration (e.g., Chrome with Gmail via web-based email).

2. Step 2

   Downloaded image attachment and .zip without accessing (opening) the image.

3. Step 3

   Print and save emails with zip file. (optional)

Analyze Test Data Procedure

1. Step 1 – Stream Hash analysis using ffmpeeg

- Using the following command in ffmpeg, obtain the stream hash for all data files:

  Ffmpeg -i "filename.jpg" -f streamhash - > "filename.txt"

- Compare Original stream hashes to the Actual, Small, Medium, and Large stream hashes.

2. Step 2 – Metadata Analysis using MediaInfo.

- Using MediaInfo, individually load all files to obtain pertinent metadata, specifically aspect ratio and bit depth file data. *See Figure 2.*

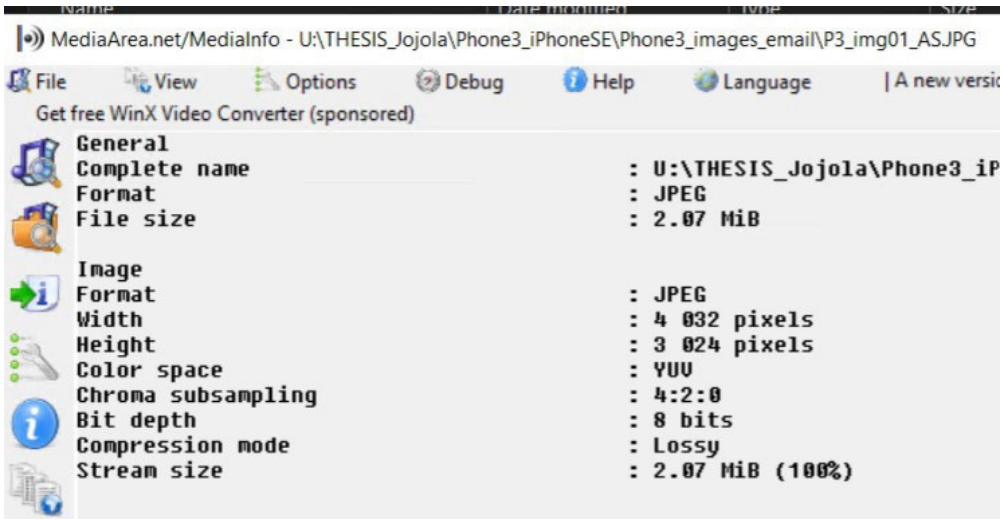

Figure 2. Metadata Capture Example from P3_img01_AS.JPG

- Compare metadata of Original files to the metadata of the Actual, Small, Medium, and Large files.

Methodology Summary

For our research, three iPhones were used to collect image data. It was determined that we wanted to control the variables of image capture as much as possible and limit any filters or image manipulation to the original image captures. For each phone, we made sure all default settings were "off," such as Flash, Live, and HDR, and we used the "most compatible" setting as compared to "high efficiency" or "Apple ProRAW", and others. These images were then emailed via Apple's native iOS Mail

application to an email account, where the files were then downloaded unaltered. Using Cellebrite software, data extractions were performed to find the original and downsized email versions of each photo taken. All of the relevant image files found on the phones and the emailed downloads of the images were analyzed using three analysis tools to compare the files forensically.

CHAPTER IV

RESULTS

Analysis was performed on the original 30 phone image files and on the 120 emailed image files. The emailed files were compared to the respective original files to determine the level of image manipulation or file modification, if any.

Stream Hash Results

The results of the stream hashing analysis via FFMpeg are below. The tables included in the results do not represent the entire data set of results obtained from the experiments. Instead, the tables are meant to provide a visual aid as an example of the results found for all of the findings regarding the comparison of the originally extracted files to the emailed files.

Phone 1

The stream hashing indicates that the Original and Actual file images are a match for Phone 1, the iPhone 12 Pro Max. The Small, Medium, and Large files did not match the original files. Please note that the table below only depicts the results of comparing one original photo to its corresponding various-sized emailed options for one photo that was taken on this phone. The results were similar for all 10 of the original photos taken. The Originals and Actual sized images resulted in matching stream hashes for all 10 photos. In contrast, the respective Small, Medium, and Large stream hashes did not match the originals.

Table 7. Phone 1: iPhone12 Pro Max Stream Hashes

Image	SHA-256 Stream Hash	Match ?
Original	d946e689fec8575d09884c57fc1f6b13716d5642da4f790d01bdad6b6d3a0cbd	n/a
Actual	d946e689fec8575d09884c57fc1f6b13716d5642da4f790d01bdad6b6d3a0cbd	Yes
Small	42b842201bccd1a8a31beabd22bf574a820d26a8cab7571ec1aa7a5c54591aa1	No
Medium	6c68c70e4d736622ac45597954285ca148a767350bae57baaa76276ebe0d680b	No
Large	fff2f549ae3896bdb50d66cfadccc3658ace9f80d4498e4d95cc21c0c377db17	No

Phone 2

Same changes as Phone 1 above.

Table 8. Phone 2: iPhone8 Stream Hashes

Image	SHA-256 Stream Hash	Match?
Original	b00e0e7b6840dc62160ac1d6b3a0208011e2b9ffd70d14d54931d6852069033b	n/a
Actual	b00e0e7b6840dc62160ac1d6b3a0208011e2b9ffd70d14d54931d6852069033b	Yes
Small	84034fb2567fbacdbd707cbaf801a0e9fa5f4066324d02abb291ee31e8c99489	No
Medium	ab48a090bd6048b30d88c8f61979f5289e4fbd542961bf4ed2d2ac9d34dc595e	No
Large	d904e6e312d648293e491d2ea1a9b9b89e7cad56a5a81cd279bcd336347631b9	No

Phone 3

Same changes as Phone 1 above.

Table 9. Phone 3: iPhoneSE Stream Hashes

Image	SHA-256 Stream Hash	Match ?
Original	4cd3500c05d82febb454e85e3cbfaaad99301d0d776e0af58f77f1bd69ec5be1	n/a
Actual	4cd3500c05d82febb454e85e3cbfaaad99301d0d776e0af58f77f1bd69ec5be1	Yes
Small	a05b155d1ca3dae16e69229b3d631cb832e438e4ddfcb4917076cf363a8c259c	No
Medium	878234a422c1c45cf8302bfdd074ad5006fa512ccc64d8764c08518044415811	No
Large	46fbd767691a3b72c2c1b5a90d23222b252528a79a6445002625ee1b5fb18ea2	No

Stream Hash Summary

The results of the stream hashing indicate that for all three phones tested, only the emailed Actual image stream hashes matched the Original images stream hashes. The Small, Medium, and Large stream hashes did not match the Original images stream hashes.

Metadata Results

The results of the Metadata analysis via MediaInfo are below. The tables included in the results do not represent the entire data set of results obtained from the experiments. Instead, the tables are meant to provide a visual aid as an example of the results found for all of the findings regarding the comparison of the originally extracted files to the emailed files.

Phone 1

Same changes as Phone 1 in stream hashing.

Table 10. Phone 1: iPhone12 Pro Max Metadata

Image	W:H	Bit Depth	Match?
Original	4032:3024	8	n/a
Actual	3024:4032	8	Yes
Small	240:320	8	No
Medium	480:640	8	No
Large	1512:2016	8	No

Phone 2

Same changes as Phone 1 in stream hashing.

Table 11. Phone 2: iPhone8 Metadata

Image	W:H	Bit Depth	Match?
Original	4032:3024	8	n/a
Actual	4032:3024	8	Yes
Small	320:240	8	No
Medium	640:480	8	No
Large	2016:1512	8	No

Phone 3

Same changes as Phone 1 in stream hashing.

Table 12. Phone 3: iPhoneSE Metadata

Image	WxH	Bit Depth	Match?
Original	4032:3024	8	n/a
Actual	4032:3024	8	Yes
Small	320:240	8	No
Medium	640:480	8	No
Large	2016:1512	8	No

Metadata Summary

The results of the metadata analysis indicate that for all three phones tested, only the emailed Actual images matched the Original images in regard to the bit depth and aspect ratio. In addition, the Small, Medium, and Large images did not match the Original images in these areas.

Results Summary

The results of the stream hashing and the metadata analysis are consistent with each other. Both analyses indicate that for all three phones tested, only the emailed Actual images matched the Original images regarding their stream hashes, bit depth, and aspect ratios. In addition, the Small, Medium, and Large images did not match the Original images stream hashes or aspect ratios.

CHAPTER V

CONCLUSIONS

The results of the stream hashing and the metadata analysis indicate that for all three phones tested, only the emailed Actual images matched the Original images regarding their stream hashes, bit depth, and aspect ratios. The Small, Medium, and Large images did not match the Original image stream hashes or aspect ratios. The Small images were consistently resized to 320:240, the Medium were resized to 640:480, and the Large to 2016:1512, and the stream hashes did not match the originals. These alterations are not forensically acceptable as clones of original files.

As a result of this research, it is recommended that iPhone email attachments should not be used as an evidence collection technique unless the actual image size option is selected. It is concluded that this email attachment method can **only be trusted in specific circumstances**, or when a specific **order of operations** or process is followed. From our research, it is known that only when the files are sent as Actual Size are they forensically acceptable as clones of original files, given that all of the image capture settings are also identical to the settings used in our testing procedure.

Limiting Factors

One of the biggest limitations to this research was time restrictions and coordination of time between me, the student, and professors assisting with data analysis. Matching availability was a struggle at times and although communication was always excellent between all participants, I learned that I would not want to rely so much on email in the future for sharing data and their analysis results throughout the course of an extensive experimentation process.

Keeping emails and downloads organized without corrupting data was a limitation when it was being handled by multiple people in various ways. Additionally, based upon different resolutions, we could not perform pixel level analysis, which was also an initial plan.

Future Research

The research study experienced a very high-level observation of unusual phenomena which occurred when transferring working copies of original images between the researcher and committee members. The initial email activity phenomena involved some images received in the email transfers experienced approximately 20% quality factor degradation from the original images. Still, other images transferred via email experienced no changes in the quality factor. The researchers also noted that initial PRNU testing revealed that the degraded email image attachments PRNU did not match the original images. These initial emails and attachments were not used in this research as the transfers introduced a confounding variable not part of the planned experiments.

For future research it is suggested that the incomplete analysis that was begun with this research be completed or used as a starting point for future research. Performing an Image Quality Analysis on all of the data along with PRNU testing is recommended.

Additionally, we discovered that the downsized emailed images provided some metadata associating it back to make and model of the phones used to capture the images. It is worth looking into whether enough data is there to allow these images in some cases to be used evidentiarily even if not forensic clones of originals.

Lastly, similar testing is suggested taking into consideration all of the various capture settings that could be modified and used in various combinations to capture images on iPhones.

REFERENCES

1. de Roos L, Geradts Z. Factors that Influence PRNU-Based Camera-Identification via Videos. *Journal of Imaging*. 2021; 7(1):8. https://doi.org/10.3390/jimaging7010008

2. Epstein, B. (2020). Source and Generational Analysis of Transmitted Video Files to an Apple iPhone (dissertation).

3. Lomboy, G., Grigoras, C., & Smith, J. M. (2018). American Academy of Forensic Sciences 70th Annual Scientific Meeting. In *Digital Image Recompression Analysis: Twitter*.

4. Nelson, J. O. (2020). Comparative Analysis of iPhone Image Data Across Various Transfer Methods (dissertation).

5. Wales, G. S., Smith, J. M., Lacey, D. S., & Grigoras, C. (2022). Multimedia Stream Hashing: A Forensic Method for Content Verification. *Journal of Forensic Sciences*.

6. Zhang D, Wang S, Wang J, Sangaiah AK, Li F, Sheng VS. Detection of Tampering by Image Resizing Using Local Tchebichef Moments. *Applied Sciences*. 2019; 9(15):3007. https://doi.org/10.3390/app9153007