IMAGE ANALYSIS OF IOS AND SNAPCHAT CAMERA: UNRAVELING FILE STRUCTURE AND STRUCTURAL CHANGES IN POSTED, MESSAGED, AND SAVED IMAGES

by

JENNIFER LYNN JONES

B.A., Grand Canyon University, 2021

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 Lynn Jones

has been approved for the

Media Forensics Program

by

Catalin Grigoras, Chair

Gregory S. Wales

Jeff M. Smith

Cole M. Whitecotton

Date: December 16, 2023

Jones, Jennifer Lynn (M.S., Media Forensics Program)

Image Analysis of iOS and Snapchat Camera: Unraveling File Structure and Structural Changes in Posted, Messaged, and Saved Images

Thesis directed by Associate Professor Catalin Grigoras

ABSTRACT

This thesis investigated Snapchat-generated image creation, storage, and interaction on an iOS device used to develop potential forensic artifacts to fill a knowledge gap to aid the forensic science community. The study hypothesized that iOS versions of Snapchat alter images when transferring images via chats and posting to Snapchat stories.

The quantitative research method used a quasi-experimental approach involving three iOS devices that created 80 Snapchat-generated images to compare with 20 native camera application created images used as control or reference images. The study used mobile forensic tools to locate potential forensic artifacts to contrast native camera application versus Snapchat image creation, storage, and interaction. The Snapchat interaction included direct messaging, saving to camera roll, and posting to story. The research collected and analyzed raw data related to Snapchat-generated image file structure, metadata, compression, and artifact locations within the iOS operating system.

Analysis of image data revealed noteworthy alterations to file structures, metadata, and compression within the iOS system. Most notably, Snapchat images were observed to be stored in a distinct file system subfolder, previously inaccessible to the Camera Roll application. This discovery provides crucial insights for digital forensics experts, enabling a more comprehensive understanding of image storage and retrieval mechanisms on iOS devices and potentially assisting in investigations involving social media content.

The study developed evidence to support that iOS versions of Snapchat alter images when transferring images via chats and posting to Snapchat stories.

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

Approved: Catalin Grigoras

DEDICATION

To God, for His unwavering provision and guidance, even in our most challenging moments. To my loving husband, whose tireless efforts and God-given talents ensure our family's needs are met, and whose unwavering support fuels my mission. To my incredible daughters, whose patience and understanding brighten our days. Your helpfulness and understanding teach us the true meaning of family and unity. To my mom, a shining example of tenacity and strength, who has taught me that it's never too late to reinvent yourself and has always been there. To my dad, your support and wisdom throughout my educational journey have been invaluable.

ACKNOWLEDGEMENTS

I would like to express my heartfelt gratitude to the professors who have been instrumental in my academic journey. Your support and understanding during the most challenging times have been invaluable.

I am particularly thankful to Cole Whitecotton for his unwavering dedication to keeping systems running smoothly and being readily available to provide support. To Jeff Smith, I extend my appreciation for his extraordinary patience and for working alongside me, allowing me the time and space to troubleshoot and problem-solve independently. Catalin Grigoras has been a solid rock of support, and I am deeply grateful for his guidance.

Leah Haloin deserves special recognition for her exceptional assistance in navigating the program, from class registration to deadlines and ongoing support. Gregory Wales, your availability, support, directness, honesty, forgiveness, and inspiration have had a profound impact on my journey, and for that, I am truly thankful. Your contributions have been invaluable to the successful completion of this thesis.

TABLE OF CONTENTS

CHAPTER

LIST OF TABLES

TABLE

LIST OF FIGURES

FIGURE

LIST OF ABBREVIATIONS

AR – Augmented Reality

ASTM – American Society for Testing and Materials

AVI – Audio Video Interleave

CCM – Color Correction Matrix

DCT – Discrete Cosine Transform

DAUs – Daily Active Users

EXIF – Exchangeable Image File Format

HEIF – High Efficiency Image File Format

IMEI – International Mobile Equipment Identity

iOS – iPhone Operating System

JPEG – Joint Photographic Experts Group

MSE – Mean Squared Error

MS-SSIM – Multi-Scale Structural Similarity

PSNR – Peak Signal-to-Noise Ratio

RLE – Run-Length Encoding

RQ – Research Question

SWGDE – Scientific Working Group on Digital Evidence

CHAPTER I

INTRODUCTION

In an age where digital communication and image sharing have become ubiquitous, forensic science faces an evolving challenge—unraveling the complexities of Snapchat-generated images on iOS devices. In the pursuit of unlocking the secrets hidden within Snapchat-generated images on iOS devices, this thesis sheds light on the obscure world of Snapchat and iOS, unraveling file structures and uncovering structural changes in the images shared, messaged, and saved. As we initiate this diagnostic investigation, we venture to bridge a significant knowledge gap, one that may hold the key to enhancing the capabilities of forensic experts in the digital age. However, within the encrypted confines of iOS devices and the ephemeral world of Snapchat, a clandestine metamorphosis unfolds, reshaping the images we share and the traces we leave behind.

This thesis embarks on a pioneering journey through the intricacies of image creation, storage, and interaction in the realm of Snapchat on iOS, shedding light on the previously obscured forensic artifacts that hold the power to reshape digital investigations.

Using a carefully structured quantitative research approach, this study investigates 80 Snapchat-generated images alongside 20 images created using the native camera application. We aim to uncover hidden insights within the iOS operating system. Employing mobile forensic tools, we examine file structures, metadata, compression, and artifacts. What we discovered is of great significance: Snapchat images are stored in a separate subfolder, previously inaccessible to the Camera Roll application.

This discovery provides crucial insight into how images are stored and retrieved on iOS devices and represents a significant step forward in digital forensics, especially in social media content investigations. Our research is punctuated by a transformative finding: iOS versions of Snapchat can significantly modify images as they travel through chats and stories.

Snapchat

The investigation into Snapchat-generated image manipulation on iOS devices holds significant importance in forensic science. Understanding Snapchat's iOS version’s file structure, alterations to metadata, and compression during interactions and storage is crucial for digital forensics experts. This research not only addresses a knowledge gap but also offers essential insights into image storage and retrieval mechanisms on iOS devices, enhancing the ability to uncover and analyze potential forensic artifacts. Such knowledge is invaluable for forensic investigations, particularly those involving social media content, where image authenticity and integrity are of paramount concern.

The rapid progress in camera technology and the increasing popularity of Snapchat as a primary communication tool for those aged 18-34 underscore the need for the multimedia forensic community to gain a deeper understanding of camera functionalities and the automatic processes images and videos undergo during transmission. Moreover, comprehending the file structure within the iOS system and the location of artifacts related to Snapchat is essential. Currently, the absence of research specifically focused on the Snapchat application on iPhone devices, including the image processing techniques employed, the extent of similarity or distortion between original reference images and those transmitted via Snapchat, and the file structure where these artifacts are located, creates a notable gap in image analysis research. This study aims to address and bridge this gap, as establishing the field as a meticulous, efficient, and reproducible science is crucial for its credibility in legal proceedings.

Related Works

In the modern world, digital evidence and the field of digital forensic science have become increasingly important. One crucial aspect of this discipline is media forensics, which involves the organized collection, preservation, and analysis of various media types, such as audio, video, and images. These media are obtained from a wide range of devices, including digital cameras, voice recorders, computers, and mobile phones.

Previous research in the field of mobile phone forensics, especially regarding image-based analysis, has concentrated on Android devices. This has left a significant gap in our understanding of how ephemeral messaging apps like Snapchat interact with iOS devices.

Researchers such as Mahajan et al. (2013) and Alyahya & Kausar (2017) have made substantial contributions to this area, focusing exclusively on artifacts found on Android devices. However, their work offers limited insights into the correlation with iOS devices. In contrast, preliminary studies by Barrios and Lehrfeld (2011) provided an initial glimpse into the wealth of forensic information available on iOS devices. Furthermore, Faklaris and Hook (2016) emphasized the importance of including social media content in litigation-hold notices, underlining the need to preserve valuable evidence. Understanding the structure and capabilities of these devices is crucial for effectively preserving and extracting forensic data, thereby bridging the knowledge gap in mobile phone forensics.

A review of the literature for changes in the iPhone Snapchat application regarding the quality of images yielded no prior research or data highlighting a specific research gap. Previous research has discussed the development of multiple media formats for encoding photos for high or low bandwidth internet streaming (Ravikumar & Arulmozhi, 2019). However, due to the high volume of traffic on social media platforms, it has become customary practice to automatically compress images to optimize bandwidth usage and reduce load times (Flynn et al., 2013). Handling substantial amounts of image and video data is not feasible without employing compression algorithms like JPEG, H.264, and AVI, among others. These algorithms aim to perform lossy compression of images and videos to significantly reduce file sizes and bandwidth consumption while incurring minimal or acceptable reductions in visual quality (Venkataramanan et al., 2021).

Snapchat is not renowned for its exceptional image quality; in fact, it is known for its inconsistent scoring algorithm. Nevertheless, Snapchat's swift information transmission is a significant advantage for its users. Unfortunately, the lossy compression employed by Snapchat results in lower-quality videos and images after compression and upload, degrading image and video quality. Moreover, the way people perceive the quality of images varies significantly, with a tendency to favor certain operating systems, such as iOS, over others like Android.

While various researchers have explored related subjects, prior research has not directly investigated the relationship between iPhone and Snapchat, leaving a gap in this area of research. (Arias, 2021) examines the differences in audio files when sending and receiving Snapchat snaps on devices with various operating systems. The study involved testing Snapchat on four different devices, each with a different operating system. Results showed that when an Android device sent a snap to another device, it produced an identical copy, regardless of the recipient's OS. However, when an iOS device sent a snap, it resulted in variations, including changes in file duration. These differences seem to occur during uploading and downloading from the Snapchat server, specifically for iOS devices.

Closely related to metadata and compression analysis is (Malley, 2012) investigation into the distinction between video files saved through Snapchat on Android and Apple iPhones, aiming to enhance the future authentication of such files. The study compares Snapchat video files transferred through various methods between Android and iPhones. Notable findings include that Android Snapchat videos transferred via Dropbox and Gmail remain unchanged, while those sent via MMS message show heavy recompression, including audio and video stream hash value mismatches. iPhone Snapchat videos transferred via Dropbox exhibit no changes, while those sent via Gmail and MMS message to Android experience recompression, with audio stream hash value matches and video stream hash mismatches. Metadata distinctions are observed, linking the files to their respective platforms, but not always directly to Snapchat. Audio samples vary depending on the transfer method and platform.

Tso et al. discuss iPhone and social networking in the context of evidence investigations, but they do not address Snapchat specifically. They provide valuable information on the iPhone backup process to iTunes, backup files of social media applications, and the extraction of digital evidence, which is vital for digital media forensics. However, their work does not explicitly cover specifics related to Snapchat. The five social media sites they address are Facebook, Skype, Viber, Windows Live Media, and WhatsApp Messenger. Central to the Snapchat application is its primary communication feature, involving images and videos, and its distinctive augmented reality (AR) technology.

Azfar et al. focused their study on Android mobile phones and five popular social apps, including Twitter, POF Dating, Snapchat, Fling, and Pinterest. This case study contributed to research and adversary capabilities within the forensic community. The information gained from this study related to Snapchat provided directory information on where Snapchat database data is stored, including Images, Sent Images, Received Videos, Received Snaps, and Sent Snaps. All of this is of forensic value in recovering data from an Android device and relates to Snapchat version 9.8.0.0. However, their study did not address image analysis specifically related to Snapchat.

Scope and Limitations

This thesis will investigate the file structure of images captured on three separate iOS devices, examining images taken with the iOS native camera and the Snapchat application camera. Furthermore, the study will provide a comprehensive analysis of metadata within images from the iOS native camera and Snapchat's camera. Additionally, it will assess compression rates during various Snapchat interactions, such as messaging and posting to user stories, to establish a foundational framework for future research in this field.

Research Questions Addressed

This is not a solution-based study. This is a ground-level study gathering the following information:

1. What is the file structure of images generated on the iOS native camera?
2. What is the file structure of images generated via the Snapchat application camera?
3. Does a Snapchat application-created image file in the iOS device have any encoding or structural differences from the native iOS camera image file?
4. What modifications, if any, occur to iOS native camera images when they are uploaded and sent via direct message to another Snapchat user?
5. What modifications, if any, occur to saved Snapchat application images when they are uploaded and sent via direct message to another Snapchat user?
6. What modifications occur to iOS native camera images when they are uploaded and posted to the users Snapchat story?

7. What modifications occur to saved Snapchat application images when they are uploaded and posted to the users Snapchat story?
8. What are the differences in metadata between iOS native camera images and Snapchat application camera images?
9. What is the extent of image compression in the Snapchat application, particularly in direct messaging and posting to a Snapchat story?

CHAPTER II

TECHNICAL OVERVIEW

iPhone Camera Basics (Front vs. Rear)

In the realm of mobile photography and video recording, an iPhone is equipped with two distinct camera units: the front camera and the back camera. These cameras are strategically positioned to serve different purposes.

Front Camera

- The front camera is on the side of the device intended for user interaction, typically above the display.
- It is commonly referred to as the "front-facing camera."
- The primary function of the front camera is to capture self-portraits, commonly known as "selfies," and facilitate video calls.
- The front camera is optimized for capturing photos and videos of the user, making it suitable for various communication and social media purposes.

Back Camera (Rear Camera)

- The back camera, conversely, is on the opposite side of the iPhone, usually at the back of the device.
- It is the primary imaging unit of the iPhone, boasting higher quality, multiple lenses, and advanced features.
- The back camera is designed for capturing photos and videos of the external environment, making it the preferred choice for general photography and videography tasks.

- The rear camera system typically includes multiple lenses and sensors, allowing for a wide range of creative and functional possibilities in photography and video recording.

In summary, the front camera is intended for user-facing content, including selfies and video calls, while the back camera is optimized for capturing the world in front of the device, offering a more versatile and high-quality imaging experience.

JPEG Image Compression

JPEG image compression consists of a series of ordered technical stages, each executed in sequence, with the goal of reducing the file size of a digital image while maintaining an acceptable level of visual quality (Rabbani & Joshi, 2002). Here is a sequential breakdown of the JPEG image compression process, introduced to set the stage for the concepts explored within this study.

Color Space Conversion

The process typically begins by converting the image from the RGB color space to the YCbCr color space. Y represents the luminance (brightness) information, while Cb and Cr represent the chrominance (color) information (Gopinathan & Gayathri, 2016). This conversion separates the color information from the brightness information, allowing for more efficient compression of each component.

Subsampling

In the YCbCr color space, the Cb and Cr components are often subsampled. This means that some of the color information is discarded or averaged, reducing the amount of data that needs to be encoded. Common subsampling ratios are 4:4:4, 4:2:2, and 4:2:0, with the latter being the most aggressive in terms of chrominance compression (Rodrigues, 2015).

Block Division

The image is divided into non-overlapping blocks, typically 8x8 pixels in size. Each block is processed independently (Subramanya, 2001).

Discrete Cosine Transform (DCT)

For each 8x8 block, a mathematical transformation called the c is applied. The DCT transforms spatial pixel data into the frequency domain, representing the image as a sum of cosine functions at different frequencies and amplitudes. The result is a set of 64 DCT coefficients for each block (Saha, 2000).

Quantization

The DCT coefficients are divided by a quantization matrix. This is a crucial step in the compression process, as it reduces the precision of the coefficients and introduces loss (Saha, 2000). Higher-frequency DCT coefficients, which represent minute details and are less perceptible to the human eye, are quantized more aggressively (divided by larger values), resulting in significant data reduction.

Lossless Huffman Encoding

After quantization, the DCT coefficients are processed using lossless compression techniques, such as Huffman coding. This encoding reduces the bit depth of the coefficients and optimally represents them using shorter codes for more frequent values (Hussain, et al., 2018).

Entropy Encoding

Additional entropy encoding methods may be applied to further compress the data. Run-length encoding (RLE) is often used to represent sequences of zeros efficiently, which are common after quantization (Vijayvargiya et al., 2013).

Storage or Transmission

The compressed data, along with metadata describing the quantization matrix and subsampling scheme, is stored as a JPEG file or transmitted over a network. The compressed file is significantly smaller in size compared to the original image (Rabbani & Joshi, 2002).

The degree of compression can be adjusted by varying the quantization matrix and other parameters. More aggressive compression reduces file size but may result in noticeable loss of image quality and the introduction of compression artifacts. The challenge in JPEG compression is to find a balance between file size reduction and acceptable visual quality.JPEG, created by the Joint Photographic Experts Group, is the predominant image compression technique, originally designed to address the internet's early need for universal image compression. It efficiently reduces file sizes while preserving satisfactory image quality, thus becoming a standard choice, especially for mobile devices (Rabbani & Joshi, 2002). In this study, we exclusively examined JPEG images, primarily because of their widespread use and the fact that Snapchat, as a mobile application, typically captures images in the JPEG format by default on most mobile devices.

Lossy Compression

In forensic image analysis, lossy compression is a technique used to reduce the file sizes of digital images by permanently discarding some image data. This process involves the removal of less critical image details and subtle nuances, resulting in smaller file sizes. However, in the context of forensic image analysis, this reduction in file size can be a critical concern, as it may lead to the loss of potentially important image information (Popa, 2016). Therefore, forensic professionals often carefully consider the impact of lossy compression on image quality and the potential loss of valuable forensic details when working with compressed images.

Metadata

Metadata, as defined by the Scientific Working Group on Digital Evidence, is "information frequently found within a file that describes a file or directory. This information can encompass details such as storage locations, timestamps, application-specific data, and permissions" [18]. Metadata serves as data that imparts information about other data. In the context of this study, we specifically refer to metadata associated with image files. This information holds significant value for digital forensic investigators, as it can contain distinctive, identifying details about the individuals involved, the content, timestamps, locations, and the methods related to an image file.

EXIF Data (Exchangeable Image File Format)

EXIF data is integrated into image files, such as JPEGs, as a discrete section or metadata header. It is structured as a collection of key-value pairs, where each tag represents a specific attribute of the image or the image-capturing process. These tags encompass a wide range of information, including the following structural data (Roberts & Haggerty, 2013).

Structure of EXIF Data:

- Technical Data: Details about the camera, such as make and model, lens specifications, and sensor type.
- Capture Parameters: Information on exposure settings (shutter speed, aperture, ISO), white balance, and focus.
- Geographic Data: GPS coordinates and location information, which are especially important for geotagging images.
- Date and Time: Timestamps indicating when the image was captured.

- Copyright and Authorship: Copyright notices, author information, and intellectual property details.
- Camera Settings: Information on image compression, resolution, and color profiles.
- Thumbnail Images: A smaller, lower-resolution version of the image for quick previews.
- Software Information: Details about the software used for image processing.

Significance of EXIF Data:

- Digital Forensics: EXIF data plays a crucial role in digital forensics, enabling investigators to verify the authenticity of images, trace their origins, and establish their integrity as evidence.
- Photographic Analysis: Photographers and professionals use EXIF data to understand how an image was captured, helping in post-processing, and improving photography techniques.
- Geotagging: GPS data within EXIF facilitates the geotagging of images, allowing users to organize and visualize photos based on their geographical locations.
- Archiving and Organizing: EXIF data assists in categorizing and cataloging image collections by date, location, or camera settings.
- Quality Control: It aids in quality control processes for image-based industries, ensuring that images adhere to specific standards and requirements.
- Copyright Protection: EXIF data can include copyright information, helping photographers and artists protect their intellectual property.

In summary, EXIF data, encapsulated within the Exchangeable Image File Format, serves as a vital repository of information related to digital images. This structured metadata empowers a wide range of applications, from digital forensics to photography enhancement and geospatial analysis, making it an indispensable component of the digital imaging ecosystem.

Hexadecimal Data (HEX Data)

Hexadecimal data, often referred to as HEX data, is a numerical representation system commonly used in the field of computer science and digital technology. This technical description outlines the fundamental aspects of HEX data, its structure, and its significance in the context of digital systems and data representation.

Structure of HEX Data:

Hexadecimal (HEX) is a base-16 numbering system, as opposed to the decimal system, which is base-10. In HEX, digits represent values from 0 to 15, and they are typically expressed using the numbers 0-9 and the letters A-F, where 'A' represents 10, 'B' is 11, and so on up to 'F' for 15. HEX digits are often grouped into pairs to represent a byte (8 bits) of data. For example, the HEX value "1A" corresponds to 26 in decimal (Cox, 2006).

Significance of HEX Data:

HEX data plays a pivotal role in forensic image analysis by providing essential insights into the composition and structure of digital images. Within this context, HEX data is a valuable tool for deciphering color profiles and pixel information, aiding in the identification of potential image manipulations or alterations. It allows forensic investigators to examine the image at a granular level, uncovering hidden details, metadata, and potential anomalies that may be critical to a forensic examination. Moreover, HEX data assists in the verification of image authenticity and integrity, which is essential in legal proceedings. Its utility extends to the analysis of image file formats and can reveal hidden information within digital images, making it an indispensable asset in the field of forensic image analysis.

CHAPTER III

MATERIALS

In this study, the research was done using three mobile devices, utilizing both their front and rear cameras. Additionally, the Snapchat application was employed to capture images, which were saved, sent in messages, and posted to stories, using both its front and rear camera functionality.

Device Specifications

Table 1*. iPhone Specifications*

Device #1	
Manufacturer	Apple Inc.
Model Number	iPhone 13 Pro Max
Operating System	iOS 15.5
Serial Number	QD91067X1G
IMEI Number	353282624359573
Snapchat Version	v. 11.83.0

Device #2	
Manufacturer	Apple Inc.
Model Number	iPhone 13 Pro
Operating System	iOS 15.5
Serial Number	NW3VVM96J2
IMEI Number	356133314071365
Snapchat Version	v. 11.83.0

Device #3	
Manufacturer	Apple Inc.
Model Number	iPhone 13 Pro
Operating System	iOS 15.5
Serial Number	M47166D06H
IMEI Number	356514414626051
Snapchat Version	v. 11.83.0

Table 2. *PCs Used for Data Retrieval*

JLJMedia Workstation	
Processor	AMD Ryzen 9 3900X 12-Core Processor 3.79 GHz
Installed RAM	32.0 GB
Device ID	5489CEA7-8A05-4028-9814-721CEF492A08
Product ID	00330-52716-57452-AAOEM
System Type	64-bit operating system, x64-based processor
Windows Specifications	
Edition	Windows 11 Pro
Version	22H2
Installed on	12/8/2022
OS Build	22621.2428
Experience	Windows Feature Experience Pack 1000.22674.1000.0

NCMF-CLSRM-102	
Processor	12th Gen Intel(R) Core (TM) i7-12700 2.10 GHz
Installed RAM	64.0 GB
Device ID	A668F867-B351-4A96-9E66-D3B719740A8F
Product ID	00329-00000-00003-AA795
System Type	64-bit operating system, x64-based processor
Windows Specifications	
Edition	Windows 10 Enterprise
Version	22H2
Installed on	9/2/2022
OS Build	19045.3570
Experience	Windows Feature Experience Pack 1000.19052.1000.0

Data

The data collected consists of images captured on the above-listed mobile devices using the iOS native front and rear cameras and the Snapchat application front and rear cameras. Images were subjected to various actions, including posting to Snapchat stories, direct messaging to other Snapchat users, and saving to the camera roll.

Image Collection Breakdown

300 images were captured using three different devices, each contributing 100. All these images were taken under precisely controlled conditions within a controlled environment.

Factors such as lighting, distance from the subject, and other variables were consistent across all captures. The subsequent discussion pertains to the specific attributes of these images and the gathered data that will undergo examination.

Image Attributes and Data Collected

Table 3. *Data Collected from Image Files*

File Location	Image Data / Content (pixel data)
File Format	GPS Location Data
File Name and Extension	Device Information Data
File Size	Camera Settings
File Creation and Modification Timestamps	Software Information
Image Orientation	EXIF Data
Thumbnail	Exposure Time
Fstop	ISO
Focal Length	Signal to Noise Ratio
Colorspace	Height and Width
Encoding Process	Bit Depth
Compression	Profile CCM Type

Scope of Analysis

File Format and Compression:

- Evaluate the variances in image file formats employed by iOS devices and Snapchat.
- Assess the extent of image compression in both scenarios.
- Contrast the file formats of Snapchat-captured images with those stored in the camera roll.

Metadata:

- Scrutinize the metadata contained in images captured by iOS devices and those received via Snapchat.
- Investigate whether Snapchat modifies or reduces metadata for privacy enhancement.

Table 4. *Analysis Tools and Versions*

Software	Version	Usage
ExactFile	1.0.0.15	Hash Comparison
EXIFTool	12.67	Extract Metadata
Cellebrite		Identify File Structure
MediaInfo	22.09	Gather Preliminary Data

Image Processing and Filters:

- Examine the application of image processing techniques and filters in various contexts.
- Distinguish original Snapchat-captured images from the versions posted in stories or sent as direct messages to identify potential alterations due to image processing.

CHAPTER IV

METHODOLOGY

Meticulously structured methodology to investigate the Snapchat experience across its core platforms, namely Camera, Communications, and Stories was designed. Our focus is on understanding how images are captured, transmitted, and stored on iOS devices.

Reference Sample Collection

To initiate the research, we gathered reference samples. These samples were collected to establish a baseline dataset, enabling us to have a representative set of images with their respective structures, EXIF data, and other attributes. This baseline dataset will serve as a point of comparison for assessing Snapchat interactions.

For reference in this section, the term "iOS native camera" refers to the built-in camera app that comes with Apple's iOS operating system, which is used on devices like iPhones and iPads. This camera app is the default and primary tool for taking photos and recording videos on iOS devices. It is often referred to as the "native camera" because it is an integral part of the iOS ecosystem, as opposed to third-party camera apps that users can install from the App Store.

A "Snapchat application created image" refers to an image that is captured or generated using the camera feature within the Snapchat mobile application. Snapchat allows users to take photos and record videos directly within the app and are typically created and edited within the Snapchat platform and shared with other users through Snapchat's messaging and story-sharing features. These images may have unique characteristics and metadata associated with them, distinct from images captured using the device's native camera app.

iOS Native Camera Settings

In this preliminary study, the reference samples were obtained using the fundamental camera settings. The device was configured to capture images in the "most compatible" format, which defaults to the JPEG image format. It is important to note that this study did not consider HEIC and Apple ProRaw formats, nor did it evaluate Live Photos.

Furthermore, the front camera images will exhibit a noticeable reversal in orientation compared to the rear camera images. This is because the option to mirror the front camera was deliberately disabled to eliminate any additional interference related to camera effects. Additionally, lens correction for distortion and all photographic style options were also disabled. All camera settings were turned off to ensure that the reference samples were captured in their most basic form, free from any enhancements or alterations.

Table 5. *Reference Image Acquisition*

Device	**Camera Used**	**# of Images Taken**
iPhone 13 Pro Max (Device #1)	iOS Native Rear Camera	10
	iOS Native Front camera	10
	Snapchat Application Rear Camera	10
	Snapchat Application Front Camera	10
iPhone 13 Pro (Device #2)	iOS Native Rear Camera	10
	iOS Native Front camera	10
	Snapchat Application Rear Camera	10
	Snapchat Application Front Camera	10
iPhone 13 Pro Max (Device #3)	iOS Native Rear Camera	10
	iOS Native Front camera	10
	Snapchat Application Rear Camera	10
	Snapchat Application Front Camera	10

Snapchat Application Captured Images

Research questions 1 to 3 aim to address three key aspects. Firstly, they investigate the file structure of images created using the iOS native camera. Secondly, they explore the file structure of images generated through the Snapchat application's camera. Lastly, these questions involve a comparative analysis of the encoding and structural distinctions between images produced by these two methods.

To collect this data, we created Snapchat accounts on each mobile device and linked their profiles together. Device #1 was used to capture ten images using the Snapchat application's front and rear camera, with these images being saved directly to the device's camera roll. The primary aim here is to examine the structural distinctions between images created through Snapchat and those generated using the native iOS camera, which are then stored on the device. This same process was repeated on both device #2 and device #3 to ensure consistency in the analysis.

Images Transmitted Via Direct Message

Research questions 4 and 5 are focused on investigating whether any alterations occur in images generated by the iOS native camera and images saved from the Snapchat application when these images are uploaded and transmitted through direct messages to another Snapchat user.

To collect this data, we used the set of 20 reference images previously captured via the iOS native camera and the 20 reference images taken with the Snapchat application camera, all of which had been saved to the camera roll of device #1. Subsequently, each of these 40 reference images was individually sent, one by one, using Snapchat's "upload image" feature, and sent via direct message to another Snapchat user. On the receiving end, the 40 reference images were opened and saved to the camera roll. This identical process was then repeated on both device #2 and device #3.

Images Posted to Snapchat Story

Research questions 6 and 7 are focused on examining whether any alterations or changes take place in images produced by the iOS native camera and images saved from the Snapchat application when these images are uploaded and shared on the user's Snapchat story.

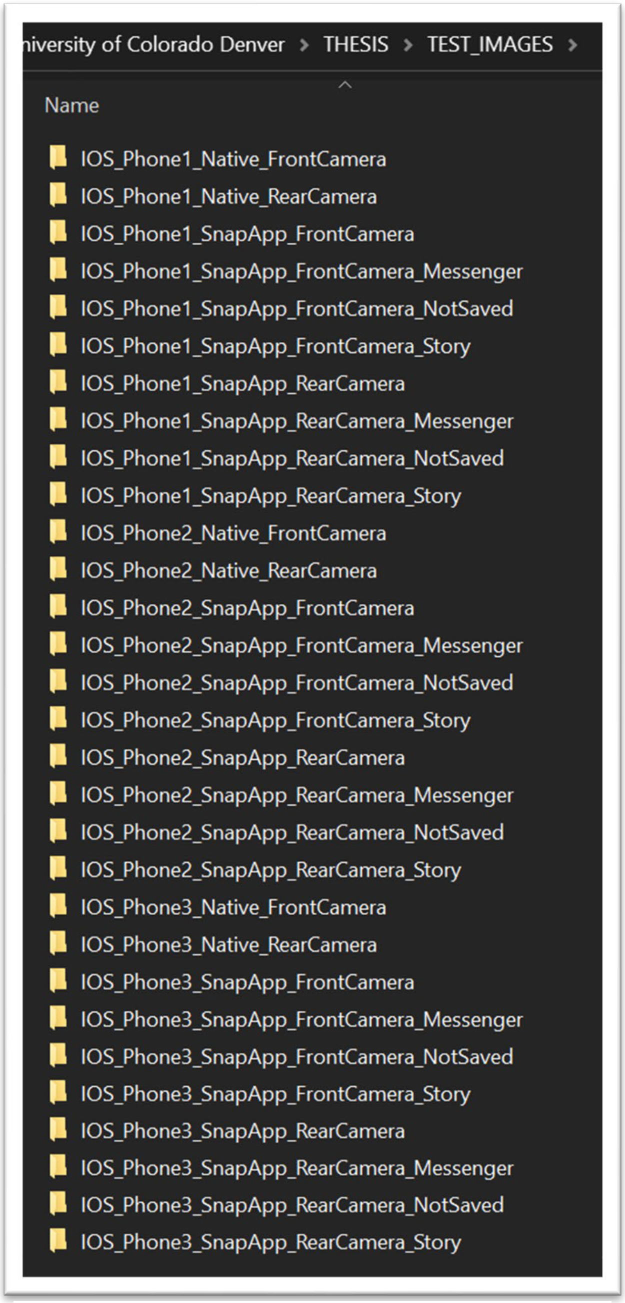
To gather this data, we utilized the same set of 20 native camera and 20 Snapchat app images referenced. Each of the 40 reference images were again individually uploaded using Snapchat's "upload image" feature and posted to the user's Snapchat story. On the receiving end, the 40 reference images were opened and saved to the camera roll. This exact procedure was again replicated on both device #2 and device #3.

Metadata and Compression Levels

Research questions 8 and 9 focus on two key aspects: the examination of metadata in both iOS native camera and Snapchat application camera images, and the comparison of this metadata after these images have undergone interactions like direct messaging and posting to Snapchat stories. Furthermore, these questions assess the level of compression applied to images when used within the Snapchat application, with a specific emphasis on images from the native camera and those saved within the Snapchat application. This analysis extends to both direct messaging and posting images to a user's Snapchat story.

Image Download Process

Following the image collection on the devices, a direct connection using a lightning cable was established between the iPhone devices and PC while Cellebrite was used to facilitate the collection, review, and analysis of the images. The transferred images were then methodically sorted into distinct folders. Each folder was designated with a systematic naming convention, incorporating information such as the device, camera source, camera location, and interaction associated with the images.



niversity of Colorado Denver > THESIS > TEST_IMAGES >

Name

IOS_Phone1_Native_FrontCamera
IOS_Phone1_Native_RearCamera
IOS_Phone1_SnapApp_FrontCamera
IOS_Phone1_SnapApp_FrontCamera_Messenger
IOS_Phone1_SnapApp_FrontCamera_NotSaved
IOS_Phone1_SnapApp_FrontCamera_Story
IOS_Phone1_SnapApp_RearCamera
IOS_Phone1_SnapApp_RearCamera_Messenger
IOS_Phone1_SnapApp_RearCamera_NotSaved
IOS_Phone1_SnapApp_RearCamera_Story
IOS_Phone2_Native_FrontCamera
IOS_Phone2_Native_RearCamera
IOS_Phone2_SnapApp_FrontCamera
IOS_Phone2_SnapApp_FrontCamera_Messenger
IOS_Phone2_SnapApp_FrontCamera_NotSaved
IOS_Phone2_SnapApp_FrontCamera_Story
IOS_Phone2_SnapApp_RearCamera
IOS_Phone2_SnapApp_RearCamera_Messenger
IOS_Phone2_SnapApp_RearCamera_NotSaved
IOS_Phone2_SnapApp_RearCamera_Story
IOS_Phone3_Native_FrontCamera
IOS_Phone3_Native_RearCamera
IOS_Phone3_SnapApp_FrontCamera
IOS_Phone3_SnapApp_FrontCamera_Messenger
IOS_Phone3_SnapApp_FrontCamera_NotSaved
IOS_Phone3_SnapApp_FrontCamera_Story
IOS_Phone3_SnapApp_RearCamera
IOS_Phone3_SnapApp_RearCamera_Messenger
IOS_Phone3_SnapApp_RearCamera_NotSaved
IOS_Phone3_SnapApp_RearCamera_Story

Figure 1. *Organization of Reference and Test Images*

Analysis

The process encompassed the comprehensive analysis of a dataset containing 300 test images that were captured, transmitted, and posted using three different iOS devices. These images were collected, consolidated on the JLJMedia Workstation, and subjected to a series of analytical procedures.

The initial step involved the calculation of hash values for each image, a method used to detect any potential alterations that might have occurred during the processes of sending, posting, and downloading these image files.

Subsequently, a detailed examination of the image files was conducted. This examination included an in-depth review of various aspects, such as metadata, Hex data, EXIF data, and the encoding techniques employed for these images. Conclusions and insights were derived from this thorough analysis of the data, contributing to the study's overall findings.

CHAPTER V

RESULTS

File Structure

Images captured using the iOS native camera follow a standardized file structure. This structure includes the use of file formats such as JPEG or HEIC, with corresponding file extensions (.jpg for JPEG and .heic for HEIC). The file names are often auto-assigned and reflect the date and time of capture, while file sizes vary based on factors like resolution and compression. These images also contain metadata containing information about capture details, device specifications, and GPS data. They are typically organized within the device's file system, following a structure based on date, location, or user-defined albums. The storage location for these images is typically the device's internal memory or external storage.

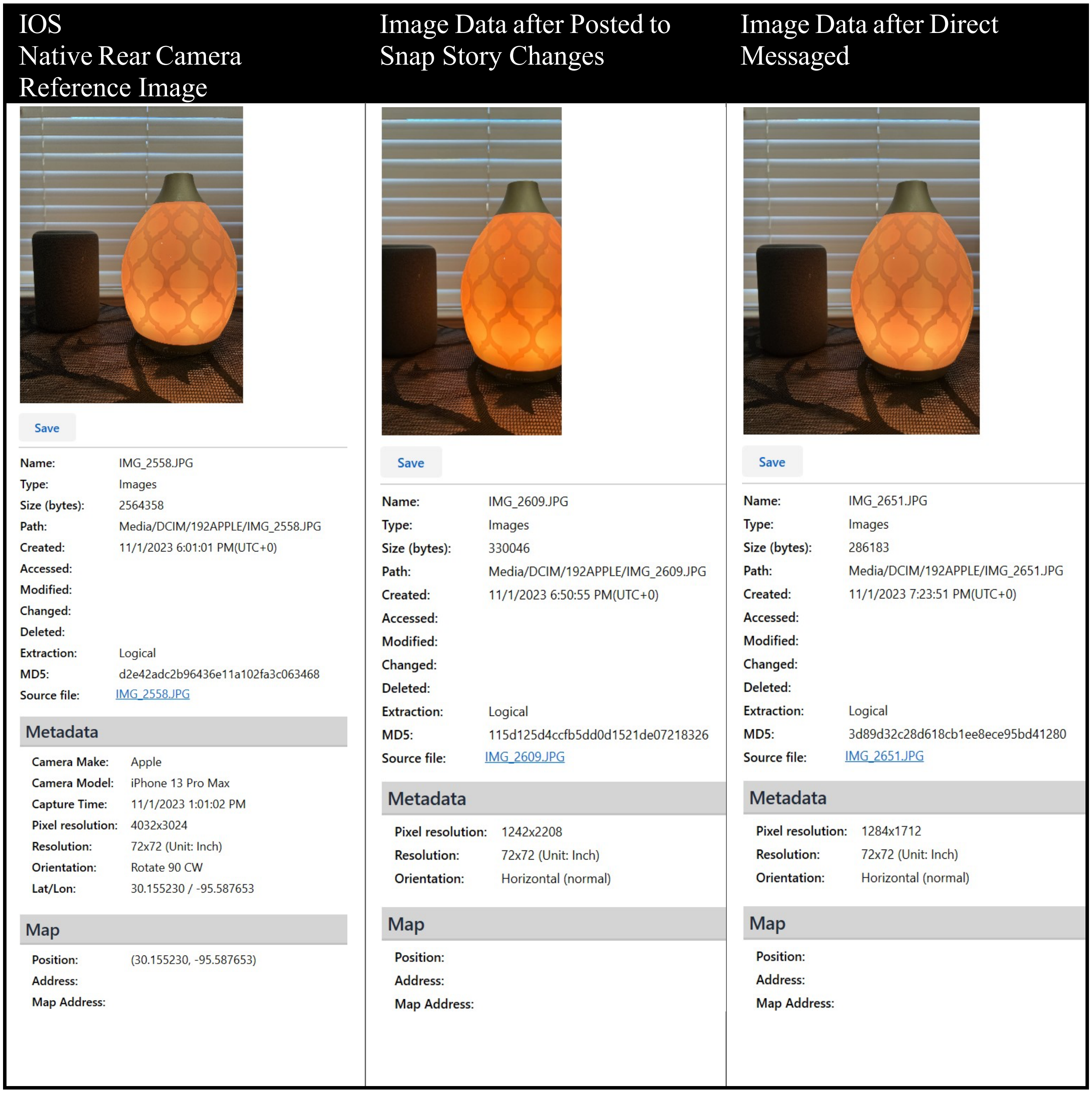
The exact file structure may show minor variations depending on the iOS version and device configurations, but this description provides a broad understanding of how images are typically organized on iOS devices. The images captured by the iOS native cameras in our study were found within the iOS device's *media/DCIM* folder, a common location in the iOS operating system.

Notably, the Snapchat images were not stored in the iOS system's DCIM folder. Tagged with a ".nomedia" extension, these files were stored in the cache/SCMediaCache folder. These folders and material in them are not accessible without the proper forensic software. Other novice software is available to access iOS file systems, however, there is a level of protection guarding privacy information from being accessible.

In pursuit of answering Research Question 3 (RQ3), which sought to investigate whether there were any encoding or structural distinctions between image files created by the Snapchat application on iOS devices and those generated by the native iOS camera, we conducted a comparative analysis. Our examination revealed that images captured by the iOS native front and rear cameras displayed more extensive metadata within the image files. In contrast, the Snapchat application-generated images lacked this metadata present in the native camera-captured images. Notable examples of the absent data in the initial reference images taken by the two separate camera applications encompassed details like the camera's make and model, GPS information, and camera settings, including exposure time, F-stop, ISO, focal length, and signal-to-noise ratio.

Structural Changes

Research Questions 4 and 6 focused on changes to iOS native camera images when sent through Snapchat. These images, regardless of whether transmitted as direct messages or stories, experienced significant metadata loss, aligning with Snapchat's privacy standards, which involve stripping most metadata from shared images.



IOS
Native Rear Camera
Reference Image

Name: IMG_2558.JPG
Type: Images
Size (bytes): 2564358
Path: Media/DCIM/192APPLE/IMG_2558.JPG
Created: 11/1/2023 6:01:01 PM(UTC+0)
Accessed:
Modified:
Changed:
Deleted:
Extraction: Logical
MD5: d2e42adc2b96436e11a102fa3c063468
Source file: IMG_2558.JPG

Metadata

Camera Make: Apple
Camera Model: iPhone 13 Pro Max
Capture Time: 11/1/2023 1:01:02 PM
Pixel resolution: 4032x3024
Resolution: 72x72 (Unit: Inch)
Orientation: Rotate 90 CW
Lat/Lon: 30.155230 / -95.587653

Map

Position: (30.155230, -95.587653)
Address:
Map Address:

Image Data after Posted to
Snap Story Changes

Name: IMG_2609.JPG
Type: Images
Size (bytes): 330046
Path: Media/DCIM/192APPLE/IMG_2609.JPG
Created: 11/1/2023 6:50:55 PM(UTC+0)
Accessed:
Modified:
Changed:
Deleted:
Extraction: Logical
MD5: 115d125d4ccfb5dd0d1521de07218326
Source file: IMG_2609.JPG

Metadata

Pixel resolution: 1242x2208
Resolution: 72x72 (Unit: Inch)
Orientation: Horizontal (normal)

Map

Position:
Address:
Map Address:

Image Data after Direct
Messaged

Name: IMG_2651.JPG
Type: Images
Size (bytes): 286183
Path: Media/DCIM/192APPLE/IMG_2651.JPG
Created: 11/1/2023 7:23:51 PM(UTC+0)
Accessed:
Modified:
Changed:
Deleted:
Extraction: Logical
MD5: 3d89d32c28d618cb1ee8ece95bd41280
Source file: IMG_2651.JPG

Metadata

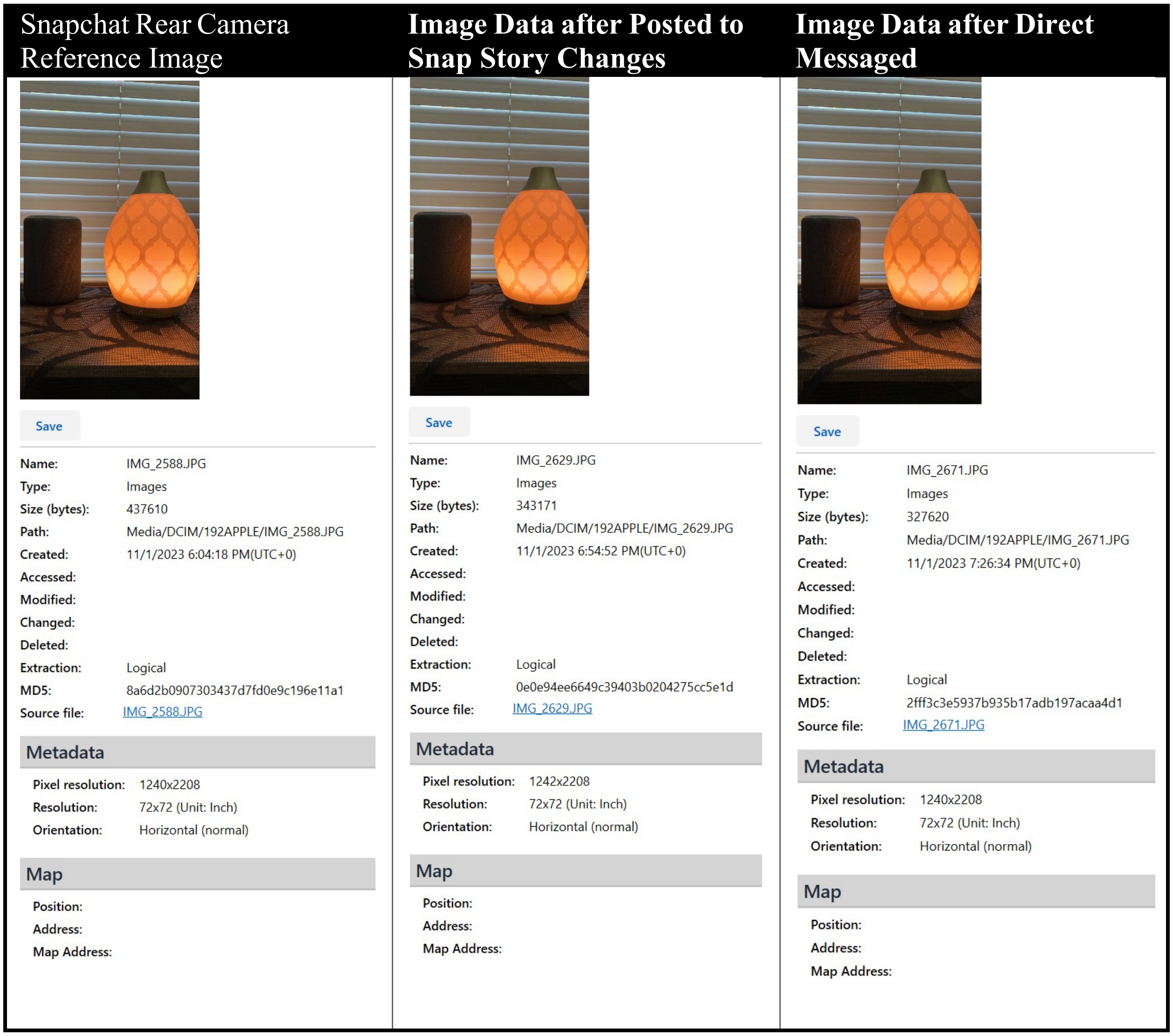
Pixel resolution: 1284x1712
Resolution: 72x72 (Unit: Inch)
Orientation: Horizontal (normal)

Map

Position:
Address:
Map Address:

Figure 2. *Metadata of Reference Image 2558 from Native Camera*

Research Questions 5 and 7 addressed alterations in saved Snapchat application images when sent as direct messages. In this case, there were no additional modifications, and the size and metadata from the initial capture were retained throughout the transmission process.



	Snapchat Rear Camera Reference Image	Image Data after Posted to Snap Story Changes	Image Data after Direct Messaged
Name:	IMG_2588.JPG	IMG_2629.JPG	IMG_2671.JPG
Type:	Images	Images	Images
Size (bytes):	437610	343171	327620
Path:	Media/DCIM/192APPLE/IMG_2588.JPG	Media/DCIM/192APPLE/IMG_2629.JPG	Media/DCIM/192APPLE/IMG_2671.JPG
Created:	11/1/2023 6:04:18 PM(UTC+0)	11/1/2023 6:54:52 PM(UTC+0)	11/1/2023 7:26:34 PM(UTC+0)
Accessed:			
Modified:			
Changed:			
Deleted:			
Extraction:	Logical	Logical	Logical
MD5:	8a6d2b0907303437d7fd0e9c196e11a1	0e0e94ee6649c39403b0204275cc5e1d	2fff3c3e5937b935b17adb197acaa4d1
Source file:	IMG_2588.JPG	IMG_2629.JPG	IMG_2671.JPG
Metadata			
Pixel resolution:	1240x2208	1242x2208	1240x2208
Resolution:	72x72 (Unit: Inch)	72x72 (Unit: Inch)	72x72 (Unit: Inch)
Orientation:	Horizontal (normal)	Horizontal (normal)	Horizontal (normal)
Map			
Position:			
Address:			
Map Address:			

Figure 3. *Metadata of Reference Image 2588 from Snapchat Application Camera*

Metadata

In Research Question 8, we delve into the distinctions in metadata between iOS native camera images and those captured through the Snapchat application. These disparities encompass:

Location Information: iOS native camera images often contain GPS coordinates that indicate where the photo was taken, while Snapchat images may not include this data.

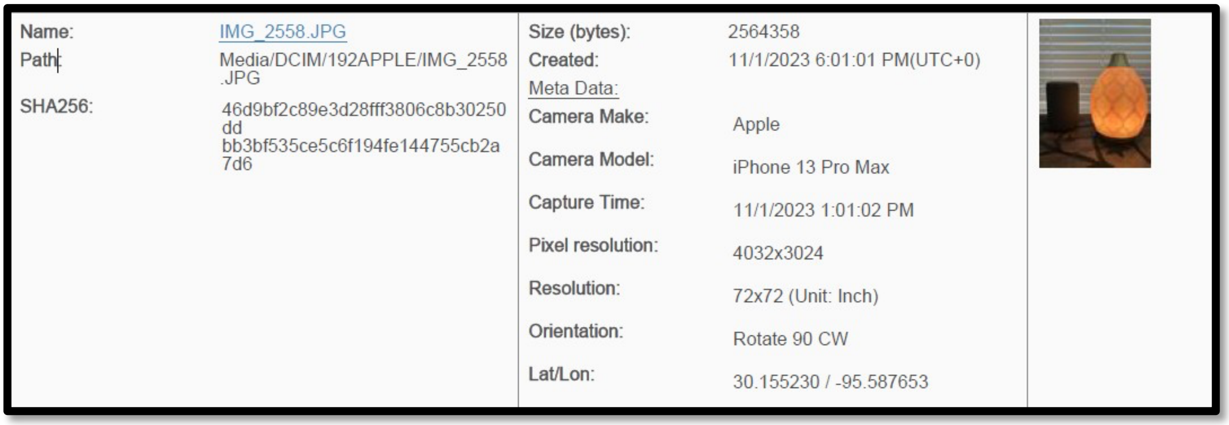
Device Information: Metadata from iOS native camera images may include details about the make and model of the device used to capture the photo, which Snapchat images may lack.

Camera Settings: Information about camera settings such as exposure time, F-stop, ISO, focal length, and signal-to-noise ratio may be present in metadata from iOS native camera images but not in Snapchat images.

Timestamps: Both types of images usually include timestamps, but the format and precision may vary.

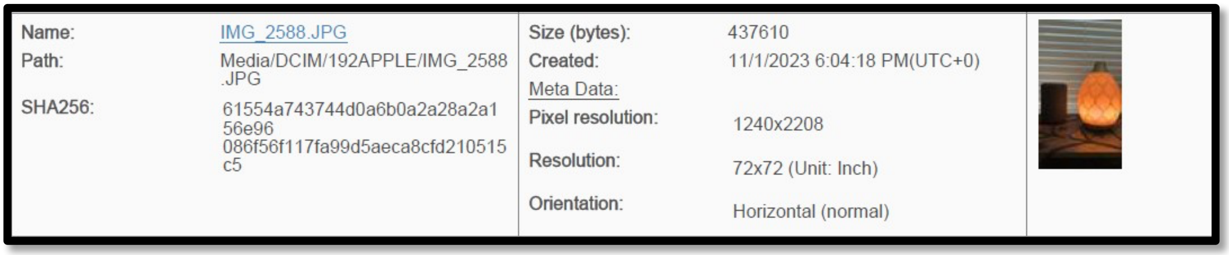
Compression: Snapchat images might undergo compression that affects metadata, potentially reducing the file size and altering metadata related to image quality.

These differences in metadata reflect the contrast between the privacy-focused, ephemeral nature of Snapchat and the more detailed metadata often associated with photos taken using the iOS native camera.



Name:	IMG_2558.JPG	Size (bytes):	2564358
Path:	Media/DCIM/192APPLE/IMG_2558.JPG	Created:	11/1/2023 6:01:01 PM(UTC+0)
		Meta Data:	
SHA256:	46d9bf2c89e3d28fff3806c8b30250ddbb3bf535ce5c6f194fe144755cb2a7d6	Camera Make:	Apple
		Camera Model:	iPhone 13 Pro Max
		Capture Time:	11/1/2023 1:01:02 PM
		Pixel resolution:	4032x3024
		Resolution:	72x72 (Unit: Inch)
		Orientation:	Rotate 90 CW
		Lat/Lon:	30.155230 / -95.587653

Figure 4. *Reference Native Rear Camera Cellebrite Report*



Name:	IMG_2588.JPG	Size (bytes):	437610
Path:	Media/DCIM/192APPLE/IMG_2588.JPG	Created:	11/1/2023 6:04:18 PM(UTC+0)
SHA256:	61554a743744d0a6b0a2a28a2a156e96086f56f117fa99d5aeca8cfd210515c5	Meta Data:	
		Pixel resolution:	1240x2208
		Resolution:	72x72 (Unit: Inch)
		Orientation:	Horizontal (normal)

Figure 5. *Reference Snapchat Rear Camera Cellebrite Report*

Compression

The extent of image compression in the Snapchat application, particularly when sending direct messages and posting to a Snapchat story, is notable. Snapchat employs aggressive image compression to reduce file sizes and enhance data transfer speed. This compression is designed to align with Snapchat's focus on efficiency and fast sharing of content.

When you send an image via direct message or post it to your story on Snapchat, the app compresses the image to a significant degree. This compression can result in a reduction in image quality, often leading to some loss of detail and clarity. The extent of compression may vary depending on factors such as the device you're using, your network connection, and the specific image content.

Snapchat's image compression aims to strike a balance between maintaining reasonable image quality while ensuring swift sharing and efficient data usage. As a result, images on Snapchat may not match the original image's quality and resolution.

It's important to keep in mind that this compression is intentional and is a part of Snapchat's design to prioritize quick sharing and efficient data transfer over the highest image quality. Users should be aware of this when using Snapchat to share images, particularly if image quality is a critical concern.

CHAPTER VI

CONCLUSIONS

In conclusion, this study employed a meticulous methodology to investigate the Snapchat experience across its core platforms: Camera, Communications, and Stories, with a particular focus on iOS devices. Reference sample collection was the initial step, aimed at establishing a baseline dataset for comparison of Snapchat interactions. The study included research questions that addressed various aspects, such as file structure, encoding, metadata, and compression levels, when images were captured, transmitted, and posted using iOS devices.

The results of this investigation revealed significant insights into the Snapchat experience on iOS devices. Notably, images captured using the iOS native camera followed a standardized file structure, while Snapchat images exhibited distinct storage and organizational characteristics. These findings provide valuable knowledge for forensic examination and data retrieval from Snapchat.

Furthermore, the study illuminated the differences in metadata between images captured with the iOS native camera and those created with the Snapchat application. The contrast in metadata content reflects the privacy-focused and ephemeral nature of Snapchat compared to the more detailed metadata often associated with photos taken using the iOS native camera.

The extent of image compression applied within the Snapchat application was also a key finding. Snapchat utilizes aggressive image compression to prioritize efficiency and fast content sharing. This compression, while enhancing data transfer speed, can result in a reduction in image quality. It is essential for Snapchat users to be aware of this intentional compression when sharing images.

In summary, this study contributes to a deeper understanding of how Snapchat functions on iOS devices, shedding light on the intricate processes involved in capturing, transmitting, and storing images, as well as the implications for metadata and image quality. These findings have implications for both forensic analysis and user awareness when using the Snapchat platform.

Future Research

A potential future research idea stemming from the findings of this study could be to explore the forensic implications of Snapchat's image compression on digital investigations and data recovery. Specifically, this research could focus on the challenges and opportunities presented by Snapchat's intentional image compression during the transmission and storage of images.

The study could investigate how image compression impacts the ability of digital forensics experts to retrieve meaningful data from Snapchat interactions on iOS devices. It could delve into the extent to which compression affects metadata preservation, image quality, and the ability to recover contextual information related to images.

Furthermore, this future research could aim to develop and test forensic tools and techniques tailored to address the unique characteristics of Snapchat images, including the challenges posed by compression. It could also explore the differences in forensic examination between images captured using the iOS native camera and those generated within the Snapchat application.

By delving deeper into the forensic implications of Snapchat's image compression, this research would not only enhance our understanding of digital forensics but also provide valuable insights for law enforcement agencies, cybersecurity experts, and forensic investigators dealing with cases involving Snapchat data. This research could contribute to the development of more effective forensic methodologies and tools for handling Snapchat evidence in legal and investigative contexts.

REFERENCES

Aji, M. P., Riadi, I., & LUTFHI, A. (2017). The Digital Forensic Analysis of Snapchat Application Using XML Records. *Journal of Theoretical & Applied Information Technology*, 95(19).

Alyahya, T., Tadani, & Kausar, F. (2017). Snapchat Analysis to Discover Digital Forensic Artifacts on Android Smartphone. *Procedia Computer Science*, 109, 1035-1040. Elsevier.

Barrios, R. M., & Lehrfeld, M. R. (2011). iOS Mobile Device Forensics: Initial Analysis.

Cox, N. J. (2006). Stata tip 33: Sweet sixteen: Hexadecimal formats and precision problems. Stata Journal, 6(199-2016-2590), 282-283.

Dixon, S. (2022). Most used social media 2021 | Statista. *Statista*. [Link: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/]

Faklaris, C., & Hook, S. A. (2016). Oh, Snap! The State of Electronic Discovery amid the Rise of Snapchat, WhatsApp, Kik, and Other Mobile Messaging Apps.

Gopinathan, S., Mashiane, T., & Shozi, N. A. (2015). Snapchat Media Retrieval for Novice Device Users. In *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 162-169).

Hussain, A. J., Al-Fayadh, A., & Radi, N. (2018). Image compression techniques: A survey in lossless and lossy algorithms. Neurocomputing, 300, 44-69.

Khan, Z. C., Mashiane, T., & Shozi, N. A. (2015). Snapchat Media Retrieval for Novice Device Users. In *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 162-169).

Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic Analysis of Instant Messenger Applications on Android Devices. *arXiv preprint* arXiv:1304.4915.

Popa, B. (2016, November). Algorithms for lossless compression in image processing systems. In Proceedings of the 20th Pan-Hellenic Conference on Informatics (pp. 1-4).

Rabbani, M., & Joshi, R. (2002). An overview of the JPEG 2000 still image compression standard. *Signal Processing: Image Communication*, 17(1), 3-48. [DOI: 10.1016/S0923-5965(01)00024-8]

Ravikumar, R., & Arulmozhi, D. (2019). Digital Image Processing-A Quick Review. [Link: https://ijict.com/V2I2/V2I2P03.pdf]

Roberts, M., & Haggerty, J. (2013). MetaFor: Metadata Signatures for Automated Remote File Identification in Forensic Investigations. In EISMC (pp. 123-132).

Rodrigues, C. A. M. (2015). Color space conversion in hardware for multimedia applications.

Saha, S. (2000). Image compression—from DCT to wavelets: a review. XRDS: Crossroads, The ACM Magazine for Students, 6(3), 12-21.

Subramanya, A. (2001). Image compression technique. *IEEE Potentials*, 20(1), 19-23. [DOI: 10.1109/45.913206]

Vijayvargiya, G., Silakari, S., & Pandey, R. (2013). A survey: various techniques of image compression. arXiv preprint arXiv:1311.6877.