Now You See Me, Now You Don’t – Snapchat Forensics

Jasmine J. Walker

Champlain College
Abstract

The intertwining of social media applications and crime has become exceedingly more entangled. As the popularity of social media applications has risen, so has the number of digital forensics investigations involving them. We have come to a point where social media applications are not only used for socializing amongst friends and family, but now are being used as primary vectors to commit crime. The correlation between crime and social media use, has stressed the need for solid forensics methodologies surrounding these social media applications. This research will primarily focus on the one of the fastest growing social media platforms in the world; Snapchat. Snapchat has a handful of application features that makes it incredibly alluring to criminals. Is Snapchat the social media application of every criminals dream? Has social media applications in general made it easier for criminals to commit crimes? How does this all affect the mobile digital forensics field? These questions and many more will be answered throughout the course of this research.

Keywords: digital forensics social media, snapchat, mobile, android, bluestacks
Now You See Me, Now You Don’t – Snapchat Forensics

According to Statista.com over 2.62 billion people accessed some type of social media platform in 2018. This number is set to soar over 3 billion by the year 2021. Within the United States the top 10 most widely used social media applications include Facebook (168 million), Instagram (116 million), Facebook Messenger (110 million), Twitter (70 million), Pinterest (58 million), Snapchat (52 million), Reddit (33 million), Tumblr (23 million), WhatsApp (20 million), and Google Hangouts (15 million) (Statista, 2018).

Introduction

In the 2013 action packed thriller movie ‘Now You See Me’, follows a group of magicians band together to carry out a series of bank heists. The movie takes the audience on a series of twists and turns where things are often not what they appear to be. This same type of ‘magic’ can be seen in the mobile phone application ‘Snapchat’.

Snapchat

Snapchat is the brain child of Evan Spiegel, Bobby Murphy, and Reggie Brown. While at Stanford the three dreamed of creating one of the most used social media applications on the planet. During the prototype phase of the application the working name of the application was called ‘Picaboo’ (Bernazzani, 2017). The unique aspect of their app, would be that any videos or pictures shared between friends on the application, would disappear after a set period of time. Fast forward to September 2011, their dream would become a reality.

Core Functionality. One of the major features that draw users to the Snapchat application is the disappearing act of any messages or videos posted on the platform. While at first glance might seem like a con rather than a pro for the app, this is the exactly the vibe of the app that Evan Spiegel and his team were searching for. In May of 2012 Spiegel explained that
they were building an “...app that doesn’t conform to unrealistic notions of beauty or perfection but rather creates a space to be funny, honest or whatever else you might feel like at the moment you take and share a Snap” (Bernazzani, 2017, ‘2012: Video arrives’, para. 1). These ‘snaps’ can be either pictures or short 10 second videos. These individual snaps join together to make one long running ‘story’ for the each user. User stories encompass all of their snap for a set 24 hours period. Once the snap has been viewed once by a user, it cannot be viewed by them again. Once a snap has been in a user’s story for 24 hours, it will also be automatically deleted. Any private Snapchat messages will automatically be deleted after 30 days if left unopened. If at any point a screenshot is taken of a snap, the author of the snap will be notified.

Another key functionality of the application is ‘Snapchat Memories’. Snapchat Memories can be used for users that want to hold onto their snaps that would otherwise be deleted after a 24 hour period of time. Users are able to save these snaps with custom keywords; this makes searching their own personal Snapchat Memory database that much easier (Howell, 2016). Snapchat Memories cannot be used on snaps that are not the users’ own. There are some marketed third party applications and workarounds that allow users to save other users’ snaps without them knowing; however often times these applications end up failing to save the snap altogether.

**Marketing & Revenue.** Boasting over 300 million active monthly users, it should be no surprise that Snapchat’s ad revenue in 2017 was over 500 million dollars (Sterling, 2018). One of the primary ways in which Snapchat generates add revenue is through their ‘Geofilters’. Geofilters are filters that can only be accessed when a Snapchat user is within a specific geolocation. Geofilters are regularly used by companies to advertise for special promotions and events that are going on at the time.
Another key way Snapchat integrates ads within their application are through their ‘Snap Ads’, Snap Ad are advertisements that are placed in the middle of users’ snap stories. Snapchat first started allowing advertisers to buy these Snap Ads in 2014. (Sloane, 2016) This advertisement generally last not more than 15 seconds and can be skipped instantly if the user chooses to do so. If a user wants more information about the product or company that’s being advertised, they can swipe up to be taken to their website. This same ‘swipe up’ ad functionally can be seen within Instagram stories as well. These interactive Snap Adds generally cost $55 for every 1,000 snap user views.

**Embroidment.** Though Snapchat has been largely successful since its founding in 2011, it has gone through its fair share of hardships. One of these hardships came about in 2014 when the Federal Trade Commission (FTC) accused Snapchat of not being completely honest with its users. According to the FTC Snapchat “deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure” (FTC, 2014, para. 1). The FTC’s main gripe with Snapchat is they felt that the company needed to be more transparent with regards to the actual ‘disappearing’ nature of user’s Snaps. Snapchat could not give an exact time as to when Snaps would be deleted from their servers. Even in the cases where Snaps were delated from the main servers, Snapchat explained that they could possibly be recovered from their backup servers.

Another controversy came about when Snapchat introduced one of their new features ‘Snap Map’. This questionable new feature was introduced in 2017 and allowed Snap users to share their locations with their Snap friends. While Snap Maps was by default turned off, many Snapchat users still raised privacy concerns over the new feature. The most problematic part of the Snap Map feature is that it updated the location of a Snap user as soon as they opened the
app; even if they were not posting any new Snaps. For example, if a Snap user happened to home at night and opened up one of their friends Snap messages their location would instantly be broadcast to all of their Snap friends. This location would also not just be the general location of the Snap user but within an exact block of where they were. Though the functionality was never disabled by Snapchat, many Snap users now only operate in ‘ghost mode’. With this enabled Snap users’ locations is never broadcasts to anymore, not even their Snap friends.

Social Media & Crime

Has social media applications made it easier for criminals to commit various crimes?

Snapchat. The most unique feature about Snapchat, makes it especially freighting for digital forensic examiners. As Jeremy Hobson points out “Snapchat has become a haven for child predators to be able to both exchange child pornography with each other, and to be able to induce children to send pictures of them to the predator” (Wandt, 2018, ‘Interview Highlights’ para. 1). In most cases once wrongdoing is reported to the authorities, it is often too late to manually recover any of the data from the device. This unfortunately makes Snapchat especially alluring to child predators.

Along with child predators, other criminals are using Snapchat in an attempt to better conceal their crimes. A prime example of this can be seen through Kemia Hassel. She along with Jeremy Cuellar plotted for months to kill her husband U.S. Sergeant Tyron Hassel III. The main communication between Mrs. Hassell and Mr. Cuellar where done on Snapchat. Mrs. Hassell explained that they through the “temporary messages would be untraceable by police” (Miller, 2019, para. 11). The two planned to kill Sergeant Hassel for financial gain, and to continued their romantic relationship. They both have been charged with first degree murder. It’s currently
unknown if the police department is working with Snapchat to recover any of the snaps from their servers.

*Other Social Media Applications.* Like Snapchat, other Social media applications have also made it easier for criminals to lure in unsuspecting victims. One of these gruesome examples was the murder of 17 year old Ashleigh Hall. Ashleigh Hall was a student in the UK at she befriended who she thought be a teenage boy on the social media website Facebook. Sadly, this ‘boy’ turned out to be a 32 year old man. Peter Chapman had created a fake Facebook account to lure in young girls. He has already been to prison several times and was classified as a ‘serial sex offended’. Ms. Hall was raped and murdered, and he body was eventually recovered from a ditch (Milivojwvic, 2010).

Unfortunately, stories like this continue to plague the news. Just last year Danueal Drayton was arrested by the Los Angeles Police department for the rapping and killing of Samantha Stewart (Arnold, 2018). Like Peter Chapman, Drayton also used social media to select his victims. In Drayton’s case, he used the popular social media dating application Tinder. Drayton is linked to seven other murders all involving the social media application Tinder. During his initial interrogation by the LAPD, Drayton told them that he himself was the victim. He claimed that voices within his head told him to commit the murders.

**Methodology**

**Objective & Scope**

The main objective of this research is to develop a simple digital forensics methodology for Snapchat in order to better familiarize digital forensics examiners with forensic artifacts of the application. Having this familiarity with the mobile application Snapchat is critical for digital forensics examiners, as many of the Snapchat artifacts can disappear forever within a matter of
Knowing what artifacts can be recovered and what cannot be recovered is crucial when time is of the essence for these particular digital forensic investigations.

**iPhone 6s Plus.** The device that was used to conduct this research was an iPhone 6s Plus cellular phone. The Apple device utilized the iOS 11.4.1 (15G77) operating system. The device was not actively connected to any mobile network; it is only active connection was to a Wi-Fi network.

**Forensic Toolkit 6.0.** The primary application used during this research was the AccessData Forensic Toolkit Version 6.0.3.5. This is the version that is currently installed within the Champlain Forensics VDI.

**EnCase v.8.05.** The secondary application used during this research was EnCase v.8.05. This is the version that is currently installed within the Champlain Forensics VDI.

**Experiment**

**Setup**

The Snapchat (ver. 10.50.1.1) application was installed on the iPhone 6s plus via the Apple App Store. Once the application was installed on the iPhone, a Snapchat account was created. The Snapchat user name that was created for this experiment was Groot Tree ‘iamgroot8907’.
Snapchat Forensics

What's New

Version 10.50.1.1

- Tap on a friend's Bitmoji to view your Friendship Profile! You'll find the images, videos, messages, links, and more that you and your friends have saved.

Create Account

FIRST NAME: Groot
LAST NAME: Tree

BIRTHDAY: January 1, 2000

By tapping Sign Up & Accept, you acknowledge that you have read the Privacy Policy and agree to the Terms of Service.

Sign Up & Accept
Data

Once the account was successfully setup, various Snaps were created. These Snaps were added to was Groot Tree’s ‘iamgroot8907’ Snap Story. All but two of the snaps Snap Memories. The above screenshots we take with the iPhone screen capture functionality.
The above screenshots we take with the iPhone screen capture functionality

**Artifacts**

In order to extract the application data from the iPhone 6s WinSCP needed to be used. WinSCP (Windows Secure Copy) is an open source SCP client that allows the transfer of files between two devices. This application needed to be used because for the ‘/private/var’ section of the Apple file system to be viewed root access was needed. Once the WinSCP client was downloaded the ‘Host name’, ‘Port number’, ‘user name’, and ‘password’ needed to be entered. The host name was the IP address of the iPhone. By default, Apple makes the user name ‘root’ and the password ‘alpine’. Before connecting via WinSCP the root password of the iPhone was changed for security purposes. It is also important to note that both the Apple iPhone and laptop computer that I was using WinSCP with, needed to be logged on to the same network. For this experiment, both devices were connected to the ‘IAMGROOT – 5G’ wireless network.
Once remotely logged into the iPhones filesystem, the ‘var’ folder was copied to my locals pc’s Desktop. The folder was then zipped and added to Dropbox. After being uploaded to Dropbox, the ‘var.zip’ was then downloaded from a Chrome web browser within the Champlain HTML Forensics VDI.
Analysis – Forensics Tool Kit 6.0

Once successfully downloaded from Dropbox, the ‘var.zip’ file was then unzipped and placed on the Desktop of the Champlain Forensic VDI. The Forensic Toolkit 6.0 was then opened. A new case was created titled ‘Snapchat Forensics Final Project (Jasmine Walker). Once we load the ‘var’ folder of the iPhone 6s, we can see the break down of the folder’s contents with the ‘Case Overview’ tab.
One of the first files of interest is found within the Multimedia section of the ‘Case Overview’.

The very first Snap that was take, can actually be seen in the
‘/mobile/Containers/Data/Application/*name*/Library/Caches/tmp/IAMGROOT8907~name*’ folder. While this is great artifact to recover, this is the only one of the videos that can be seen in the folder.
Moving along to the graphics portion of the ‘var’ file system there is another Snapchat artifacts that is identified. Instead of a video this time, it is one of the Snap pictures that was taken. The picture has a ‘.tiff’ file extension and was found in the ‘var/mobile/Media/PhotoData/MISC/PreviewWellImage’ folder. Again, this was the only image file that was found in .tiff image graphics section.
Analysis – EnCase v.8.05

Along with analyzing the ‘var.zip’ file in the Forensics Tool Kit, the Apple iPhone root var zip was also examined in EnCase v.8.05. A new case titled ‘Snapchat Forensics (Jasmine Walker) was created and stored within the ‘Documents’ folder. The ‘var.zip’ file was then extracted and dragged/dropped into the case file.

The main folder that was targeted once the var file was loaded, was the ‘/var/mobile’ folder. Immediately upon accessing this folder two of the Snapchat artifacts can be observed. What was
interesting about these two artifacts, is that they are neither a Snap picture or Snap video. The two .png picture files that were found were previews of one of the snap videos that was taken.

Snapchat & Warrants

As observed in both the Forensics Toolkit & EnCase digital forensics applications, neither of the Snaps that were not saved to Groot Tree’s ‘iamgroot8907’ memories were able to be recovered. If Snaps cannot be manually recovered, the next step would be to see work directly with Snapchat to possibly recover this data. Per Snapchat’s own documentation, ‘delete is our default’. They stress that in ‘most cases’ all snaps are deleted after 30 days. They explain on their ‘Request a Copy of a Snap’ support page “…if you feel a crime has been committed, we encourage you to contact your local law enforcement” (Snapchat Support, 2019, para. 3). In these cases, it’s up to the local law enforcement agencies to request this information from Snapchat. Snapchat follows the Electronic Communications Privacy Act when determining when user data can be turned over to law enforcement agencies. In almost all cases either a subpoena, court order, or search warrant would need to be presented to Snapchat.
In addition to working with local law enforcement agencies, Snapchat also puts out ‘Transparency Reports’ twice a year. These reports detail all requests made by government agencies for Snapchat user data. The two main tables with the transparency report included the ‘United States Criminal Legal Requests’ table, and the ‘International Government Information Requests’ table. It’s also important to note here that Snapchat does notify users when there has been a legal request for their information. This is done for all user data, unless Snapchat is “legally prohibited from doing so, or when we believe there are exceptional circumstances (like child exploitation or an imminent risk of death or bodily injury)” (Snapchat Support, 2018, para. 2).

### United States Criminal Legal Requests
Requests for User Information pursuant to U.S. legal process.

<table>
<thead>
<tr>
<th>Category</th>
<th>Requests</th>
<th>Account Identifiers</th>
<th>Percentage of requests where some data was produced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>7235</td>
<td>12308</td>
<td>85%</td>
</tr>
<tr>
<td>Subpoena</td>
<td>1944</td>
<td>4103</td>
<td>82%</td>
</tr>
<tr>
<td>PRTT</td>
<td>68</td>
<td>97</td>
<td>96%</td>
</tr>
<tr>
<td>Court Order</td>
<td>219</td>
<td>441</td>
<td>85%</td>
</tr>
<tr>
<td>Search Warrant</td>
<td>4241</td>
<td>6766</td>
<td>88%</td>
</tr>
<tr>
<td>EDR</td>
<td>755</td>
<td>885</td>
<td>77%</td>
</tr>
<tr>
<td>Wiretap Order</td>
<td>8</td>
<td>16</td>
<td>100%</td>
</tr>
<tr>
<td>Summons</td>
<td>73</td>
<td>337</td>
<td>89%</td>
</tr>
</tbody>
</table>

Conclusion

WILL ADD CONCLUSION IN FINAL DRAFT OF PAPER.
References


(ICRIIS), 2011th ser., 1-6. Retrieved from

https://pdfs.semanticscholar.org/f55c/23932b7aaacaeb918c4998515311c08e6ba0.pdf.