NEW AND EMERGING MOBILE APPS AMONG TEENS
ARE FORENSIC TOOLS KEEPING UP?

by

Kelsey Billups

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology

West Lafayette, Indiana

May 2020

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Marcus Rogers, Chair

Department of Computer and Information Technology

Dr. Kathryn Seigfried-Spellar

Department of Computer and Information Technology

Dr. Umit Karabiyik

Department of Computer and Information Technology

Approved by:

Dr. Eric T. Matson

Head of the Graduate Program

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ADB	Android Debugging Bridge
CEM	Child Exploitation Material
CSAM	Child Sexual Abuse Material
EC3	European Cyber Crime Centre
ECPAT	End Child Prostitution and Trafficking
IACIS	International Association of Computer Investigative Specialists
ICAC	Internet Crimes Against Children
ICMEC	International Center for Missing and Exploited Children
LE	Law Enforcement
NCMEC	National Center for Missing and Exploited Children
NIST	National Institute of Standards and Technology
SHA	Secure Hash Algorithm
SQL	Structured Query Language
UFED	Universal Forensic Extraction Device

GLOSSARY

Forensic artifact: items of interest or of evidentiary value in digital investigations, including but not limited to, files, logs, activities, etc.

Forensic tool: hardware or software used to process, view, or analyze pieces of digital evidence

Mobile applications: software that is intended to run on a mobile device, cell phone, tablet, etc. that are generally downloaded from an application store from the device the application will be used on

ABSTRACT

Mobile applications are an important but fast changing piece of the digital forensics' world. For mobile forensics researchers and field analysts, it is hard to keep up with the pace of the ever-changing world of the newest and most popular applications teens are using. Mobile forensic tools are quickly becoming more and more supportive of new applications, but with how quickly apps are changing and new ones being released, it is still difficult for the tools to keep up. The research question for this project examines to what extent digital forensic tools support new and emerging applications seen recently in investigations involving teenagers? For this research, a survey was conducted asking digital forensic analysts, and others who investigate digital crimes, what applications they are coming across most frequently during investigations involving teens and whether those applications are being supported by forensic tools. The top three applications from the survey that were not supported by mobile forensic tools, Monkey, Houseparty, and Likee were populated onto a test device and then evaluated and analyzed to see what forensic artifacts were found in those applications. The mobile application artifacts were then compared on two different forensic tools to see which tool obtains the most forensic artifacts from the applications. Through the examination and analysis of the applications and data contained within the apps, it was determined that 61% of the populated forensic artifacts were recovered manually and only 45% were recovered by a forensic tool for the Monkey application. 100% of the populated forensic artifacts were recovered manually and only 29% were recovered by a forensic tool for the Houseparty application. 42% of the populated forensic artifacts were recovered manually and only 3% were recovered by a forensic tool for the Likee application. It was found that the extent of support from digital forensic tools for these types of applications depends greatly on how the application stores the artifacts, but the artifact extraction support was limited for all applications. This research benefits in helping researchers and analysts by understanding the data and artifacts contained within the applications, what forensic artifacts are recoverable, and where to find those important artifacts. This research can help in finding important evidence for future investigations.

CHAPTER 1. INTRODUCTION

1.1 Background

It is challenging to keep up with the new and upcoming social media applications teenagers are using to communicate, share their interests, post pictures, and live their lives online. With more than 91% of teens having access to the Internet and social media sites, there are more teens online than ever before (Ramdass, 2016). This, unfortunately, means more opportunity for the younger generation to be involved in and the victim of crimes involving social media applications. New social media platforms targeted for teens provide a variety of opportunities for offenders and teens to exploit those sites or applications and target adolescent individuals. (Ramdass, 2016).

The types of crimes that are uninhibited by new social media applications include child sexual abuse material, sexting, sextortion, as well as others. The advancement of the Internet and social media has given these crimes a new dimension, easy access to images, videos, and actual children to have direct contact with. (Dushi, 2019). When these crimes are investigated by law enforcement, forensic tools are used to view evidence on the mobile devices that were involved. The companies that are creating these forensic tools are trying to stay up to date with new applications but still fall short with the rapid advancements in technology. Law enforcement officers and digital forensic analysts who investigate these crimes are not able to stay up to date with every single application that teens are using, either. There are many challenges to combating child exploitation, cyber-bullying, and other crimes involving teens online.

The new applications that seem to be more popular among teenagers according to news articles and the media, include anonymous messaging applications like Lipsi, Tellonym, and Yolo. There are also the live video chatting apps like Houseparty, Holla, and Likee. New entertainment applications like Zepeto and BitLife include messaging features as well. New teen dating apps like Yubo and Blendr are providing ways for teens to meet strangers online, potentially unknowing if they are who they say they are. The ubiquitous messaging applications like Kik, WhatsApp, Telegram, and Discord are still being heavily used by the younger generations. Apps like TikTok, Snapchat, Instagram, and VSCO are some of the most popular applications among teens according to online resources for parents (C. Brown, 2019; Newport

Academy, 2019). The question that remains is: Are these applications being supported by forensic tools?

The prominence and wide spread adoption of cell phones use and social media accounts at such a young age has created a problem with cyber-bullying, being exposed to adult content at a young age, being lured by child predators, and other situations that did not occur before the 2000's. According to research, around 68% of parents agree 9 years old is the youngest a child should own their own devices, a third suggesting 12 as the minimum age. Around 30% of 9-year-old children own their own smart phones or devices. Over one-third of teens claim they are spending over 6 hours a day on their mobile devices in 2018 ("Connected Children," 2018). When looking at the amount of young people online, it only makes since that they might be using new applications adults either aren't using or aren't aware of, making those applications more dangerous for the children.

1.2 Problem Statement and Significance

Technology is changing faster than what law enforcement and forensic companies can keep up with. These digital forensic companies and law enforcement investigators are having a difficult time keeping up with the newest applications teens are progressing towards. It is beneficial to know and understand what these new and emerging applications are. Understanding how these applications work and where items of evidentiary value would reside, would speed up the investigation process, solving crimes faster, helping children in danger. Having forensic tools to support the gathering of this evidence would be even more beneficial for those investigating these applications. If the forensic tools that are being used by law enforcement, who are investigating crimes against children, were able to find data of evidentiary value coming from new applications that the examiner may not have heard of before, can be an extremely important ability when advancements in technology are outpacing the knowledge of investigators. Knowing what applications teens are using is beneficial for the purposes of understanding what applications researchers should be improving the ability for tools to support and to understand where important evidence might be located in the applications on a mobile device. This study is significant in many ways, including supporting the advancement in forensic tools and their support of newer applications used by teens, and supporting the research of understanding how

teens are using mobile applications, and what applications might be holding data of evidentiary value in the case of an investigation involving those popular applications.

In this study, the goal is to understand to what extent forensic tools are supporting newer applications that are becoming popular among teenagers based on the number of artifacts found. Follow-up questions that arise based on that goal are understanding what applications are becoming more popular among teenagers and in those applications, what data of evidentiary value can be found?

1.3 Research Question

This study covers the following research question:
To what extent are digital forensic tools supporting new and emerging mobile applications seen recently in investigations involving teenagers?

1.4 Hypothesis

The hypothesis for this study was:

H_1: New and emerging mobile applications are limited in the extent of support forensic tools provide, where there are incomplete or missing artifacts not recovered from the applications.

1.5 Assumptions

The assumptions for this study are five-fold, based on the phases of this research, and include:

- Phase 1
  - Teenagers are using applications that are new and emerging
  - Mobile applications are being used in crimes
  - Law enforcement investigators understand what mobile applications are being used in crimes involving teenagers
  - Law enforcement investigator views reflect actual teen application use

- Phase 2

- There are applications that are not supported by forensic tools
- Populating a test phone reflects actual use of the application

• Phase 3

- Forensic tools extract 3rd party mobile application data
- Forensic tools could be missing data that is located in mobile applications
- Forensic software is capable of extracting the application data
- Forensic software is capable of reading files extracted from mobile applications

• Phase 4

- Data is located in databases, and other files located in the mobile application
- Forensic tools miss locating and finding 3rd party application data
- Application data includes database files and other files containing important data

• Phase 5

- Findings include data missed by forensic tools

1.6 Limitations

The limitations for this study are five-fold, based on the phases of this research, and include:

• Phase 1

- Results and answers may not directly reflect what the results would have been if the study surveyed teenagers.
- Results are be based on the opinion of law enforcement investigator's perception of teen application usage.
- Results of the survey are be based on opinions and knowledge of only IACIS and ICAC members
- All respondents are be 18 years old or older

• Phase 2

- Only using Android phone to populate test data

- Using an older device to populate test data
- Only using 1 test device

• Phase 3
- Only using two forensic software programs
- Relying on forensic extractions from 1 software program

• Phase 4
- Only relying on two software programs

• Phase 5
- Unable to collaborate with others on findings

1.7 Delimitations

The delimitations for this study are five-fold, based on the phases of this research, and include:

• Phase 1
- The restrictions for surveying teenagers directly and the time considerations for doing so was the cause for this research to survey the investigators who investigate crimes involving teens.
- The choice of only including participants that are residents of the U.S. was chosen to simplify the study and focus on results based on U.S. views

• Phase 2
- Only the three most frequently mentioned applications that were not supported by forensic tools were populated and analyzed further because of time constraints.

• Phase 3
- The use of only two forensic tool suites was be used in the analysis portion of the study, due to what was available at no cost

- The use of Cellebrite to perform the forensic extractions was chosen because the tool supports more extraction types than Magnet AXIOM

• Phase 4

- The use of the two chosen software programs for the analysis was chosen because of their features and ability to use at no costs

• Phase 5

- Due to this type of research project, unavoidable circumstances, and time, collaboration with others on findings was not an option.

1.8 Summary

In this chapter, an overview was provided describing the background, problem statement, significance, research questions, assumptions, limitations and delimitations. The main purpose of this study was to provide insight on what new applications teens are using and are becoming more common in law enforcement investigations, so forensic tools can support those applications. This study was focused on understanding to what extent applications are not supported by forensic tools and to shine a light into the gap of research on these applications and their potential evidentiary value to law enforcement investigations. This study consists of a survey intended to provide understanding into what mobile applications law enforcement investigators are seeing more frequently among teens, and what applications are not being supported by forensic tools.

The next chapter gives some understanding to why this issue is important and outlines relevant literature. A background of online crimes against children is covered, along with teen use of social media, the challenges law enforcement face, privacy and safety challenges, and the history of the top social media applications among teens.

CHAPTER 2. LITERATURE REVIEW

2.1 Understanding Online Crimes Against Children

There are many forms of crimes against children, but the Internet has created place for child sexual offenders to thrive. When speaking about crimes against children, the most common mentioned are child sexual exploitation, online enticement, and sextortion (Ramdass, 2016).

Sexual exploitation has been defined as "a practice by which a person(s) achieve sexual gratification or financial gain or advancement through the abuse of a person's sexuality by abrogating that person's human right to dignity, equality, autonomy and physical and mental well-being" (Hughes, 1999, p. 4), and is considered child sexual exploitation when it involves someone under the age of 18, in the United States (Edwards, 2009). A significant time in history regarding child sexual abuse material (CSAM), commonly referred as child exploitation material (CEM) or child pornography, started in the 1982 when New York V. Ferber was decided (White, B.R. & Supreme Court of the United States., 1982). This Supreme Court case stated that the right to free speech, the First Amendment, did not forbid states from banning and prosecuting the sale, distribution, and creation of material related to children engaged in sexual activity. The efforts of cracking down on individuals doing this, led to the government believing CSAM was becoming a solved problem towards the mid 1990's. However, with the rise, prominence, and wide use of the Internet, growth of CSAM was substantial. Government officials were worried by the exponential growth of this problem and met with tech companies, proposing solutions on handling the problem and getting the material offline. By 2008, PhotoDNA and other computerized algorithms were being used to combat CSAM online. With advancing technology, the Internet, and the presence of many social media platforms, this new social communication model provides many ways for children to encounter different types of sexual exploitation (Ramdass, 2016). Online sexual predators are taking advantage of today's youth and their availability on social media applications.

There are signs that laws are not stopping predators from getting their hands on CSAM because of the rise in the number of arrests of adults who are producing the illegal material. Unfortunately, there is no known number to how many children have been a victim of online sexual exploitation. In the US, between 2000 and 2009, the number of individuals arrested for

producing CSAM practically doubled. 37% of those arrested, had taken the images of the children themselves (Seto et al., 2018). The National Center for Missing and Exploited Children (NCMEC) is a clearinghouse that centralizes and investigates reports of suspected child exploitation. Just in 2017, NCMEC reported over 10.2 million reports of child exploitation, with number growing substantially each year (National Center for Missing & Exploited Children, 2017a). To put that number into perspective, since the start of NCMEC's CyberTipline in 1998, as of 2018, they had received over 42.9 million reports though their CyberTipline of child exploitation (National Center for Missing & Exploited Children, n.d.). 2017 alone was almost one fourth of all the CyberTips reported.

Online enticement can be defined as "an individual communicating with someone believed to be a child via the Internet with the intent to commit a sexual offense or abduction" (National Center for Missing & Exploited Children, n.d., p. 1). This can be a form of child sexual exploitation and sextortion. Online enticement can occur when a child is being persuaded or groomed to take sexually explicit images or potentially meet face-to-face with the offender for sexual purposes. This type of victimization is occurring every day and happening on every type of social media that a child can be found on (National Center for Missing & Exploited Children, n.d.).

According to NCMEC, in 2015, the majority of online enticement child victims are girls (78%) and 13% were boys, where 9% could not be determined. The mean age of victims being 15 years old. When categorizing by younger and older children, older girls were victims 48% of the time compared to younger girl (24%), older boys (8%) and younger boys (4%). It was found that in 23% of the online enticement reports in 2015, it was indicated that the offender had additional child victims, but this number is likely to be underrepresented. The offenders were found to be male 82% of the time and female 9%, where the other 9% could not be determined, due to lack of evidence or data. In 98% of the reports, the offenders did not know the children in real life, where only 2% of offenders knew their victims. 91% of the time, the offenders are the ones who are initiating attempt to communicate with the child. The goals of the offenders are mostly to receive sexually explicit images of the children (60%), meeting up with the child to have sexual contact (32%), engage in a sexual, role play like, conversation with the child (8%), or to get some type of financial gain from the child (2%). Of the reports looked at, 24% of the time, the offender received photos of the child victim, and 32% of the time the child received

photos of the offender. This communication is happening on more than just one platform. Many times, the offenders are using more than one type of communication or social media application to communicate with their victims. It is common for the offenders to start communication on a well-known platform, then move the conversation to an anonymous or encrypted chat application to receive the explicit images. This is so they can try to evade detection from those social media applications that do report when finding users trading child exploitation material (National Center for Missing & Exploited Children, 2017a).

Another type of crime against children is sextortion. According to (National Center for Missing & Exploited Children, 2017b), sextortion is defined as a type of online sexual exploitation where a non-physical form of coercion is used, such as blackmail, to receive sexual images or videos from a child, obtain money from the child, or engage in sex with the child. When NCMEC began tracking sextortion reports in 2014, in just the first 2 full years, they saw a 90% increase in the total number of sextortion reports. This pattern has continued through the years. For sextortion statistics collected by NCMEC, they found that 78% of reports involved female children and 15% male children, where 8% could not be determined. There was a similar mean age of 15 years old, seen in online enticement reports as well. It was mentioned in 24% of reports that the reporter suspected the offender to be targeting other children. Sextortion occurs through phones and messaging applications, social networking sites, and other types of video chatting. Again, about half the reports indicate that more than one platform is being used for this type of crime. The most common tactics used in sextortion are offenders threatening to post previously acquired sexual images or videos of the victim online, on a social media platform (67%), or specifically threatening to post the sexual content to a place or social media network where family or friends could see (29%), if the child does not comply with requests from the offender. NCMEC states that when victims reported a negative outcome because of the sextortion, 1 in 3 victims reported to have engaged in self-harm, threatening suicide, or attempted suicide as a result of the victimization (National Center for Missing & Exploited Children, 2017b)

These types of crimes are not rarities and are happening every day online, across the globe. Europe's Europol European Cybercrime Center (EC3) collaborates with NCMEC and other international organizations in establishing international databases and helping others from around the world (Europol, n.d.). An international organization that is based in Thailand, ECPAT,

combats and researches child sexual exploitation. Their research has shown that the ages of children who are victims of CSAM are getting younger and younger, with experts saying they have seen infants, days old, victimized by child sexual exploitation (ECPAT International, 2018b). Police in the UK are experiencing the same problems, reporting that offences for creating, possessing, and distributing CSAM have doubled in both 2010-2011 and 2014-2015 (ECPAT International, 2018a). In an International Center for Missing and Exploited Children (ICMEC) report from 2016, 82 out of 196 countries have sufficient laws and regulations against child sexual exploitation, 35 of those countries having absolutely no laws (Westlake, 2019).

With these statistics and facts, it is hard not to take notice in the rise of crimes against children. The internet has made it less difficult for offenders to commit crimes, but with a less chance of being caught by authorities. With the rapid advancements in technology, there will be more ways than ever to commit these kinds of crimes.

2.2 Understanding Teen Use of Social Media

Social media platforms have given child predators a way to get personal information from targets such as age, sex, name, photos, friends, and much more, by just looking at their profiles. It was found that 82% of online sex crimes against children started with the predator utilizing social media networks to gather personal information about their targets (Ramdass, 2016). It also gives the sexual predators a means of hiding behind a fake profile. Most times, on social networking sites, legitimacy of the person's identity is not checked thoroughly. This can allow predators to pretend to be whoever they want and act younger to appeal to their targets. There are new trends in social networks that are contributing to cyber exploitation (Ramdass, 2016). Social networking sites have facilitated the production and dissemination of child exploitation material, given online enticement a means to grow and sextortion a place to stay, and it all can be done in the matter of a second (Dushi, 2019).

Research examining the newest forms of social media teens are using is limited, and the increase of cybercrimes involving teens is significantly rising (Ramdass, 2016). A national study in 2010 showed that social networking sites were involved in an estimated 2,322 arrests involving online sex crimes against children, 503 arrests involved identified child victims (Mitchell et al., 2010). With these figures in 2010, the prominence and availability of social media sites, now, projects a growth in that number of arrests. Online sexual exploitation can be

more likely when teens display certain digital behaviors (Wurtele & Kenny, 2016). 75% of teens in the United States have access to or own a mobile device. 91% of teens are accessing the Internet and social networking sites daily (Lenhart, 2015) The need for self-actualization, validation, and the desire to belong has brought teens to these social networking sites. This potential support they seek has 43% of adolescents spending more than 4 hours a day on these applications (Ramdass, 2016). The social media application, Skout, removed all accounts of users under 18 years of age due to several reported sexual assaults being carried out by adults against underage victims in 2012 (Perlroth, 2012).

Today, the different social media applications teens use are changing so rapidly, it is difficult to stay on top of what's trending (Bentley et al., 2015). In a study, teens used, on average, 37 different types of applications on their phones per day, social networking and other communication applications contributing to more than half of those. They also found that those 37 applications didn't stay consistent over time. Teens changed which applications they communicated or socialized with from day to day and there was a rapid migration to new apps during the 14-day study.

A newer, more dangerous trend in social networking is the anonymous sites and applications. The main principle for these types of applications is the ability to share and interact with others, without fear of judgement that name may bring (Ramdass, 2016). These act as safety nets for predators because no one else can see the conversations between the predator and their target (George, 2016). Teens seem to be aware of the risks these anonymous sites bring but are still using them. There are many of these anonymous applications on the market now with the success of Ask.fm, Whisper, Sarahah, After School, and others (Farrugia et al., 2018) . The ability to stay anonymous is appealing to teens because of the freedoms the find and the ability to express themselves in different ways on these applications (Boyd, 2014). The opportunity that these types of application bring has already began to present itself in the investigations of online child solicitation, enticement, and exploitation by predators.

There are many cases that have come of teens using social media and interacting with child predators. According to a 2019 report from the U.S. Immigration and Customs Enforcement's Homeland Security Investigations department, the number of sexual predators arrested in the fiscal year rose by 18%, with 3,771 sexual predators arrested. Homeland Security initiated over 4,224 child exploitation cases in 2019 that resulted in 3,771 criminal arrests. Over 1,066 child

victims were identified or rescued in parts of Homeland Security's efforts (ICE HSI, 2019). A quick search online presents thousands of news articles that are updated almost every day with new cases and new instances of children being targeted and taken advantage of online, predators trying to entice them, meet up with them, and other attempts to sexually exploit them. In 2019, some headlining cases included a child sexual abuse material (child pornography) sting in Florida that led to the arrest of 17 people, including two Disney World employees (Acevedo, 2019).

Another CSAM sting in Oregon led to nine men arrested, all facing several felony charges (Roberts, 2019). In Washington state, the latest 'Net Nanny' undercover operation led to the total of 287 arrests, since 2015, of individuals trying to meet up with whom they think are underage girls and boys, as young as six (MyNorthwest, 2019). A man was accused of walking from Indiana to Wisconsin, a total of 351 miles, to try and meet up with an underage girl to have sex with the child (WBAY, 2019). One of the largest stings in recent history led to over 300 being arrested in a worldwide Dark Web child abuse marketplace investigation. The marketplace hosted over 200,000 unique videos of CSAM, including videos and images toddlers and infants involved in sex acts with adults and was being bought with Bitcoin. The sale transactions on the site totaled over $730,000 worth of Bitcoin. The arrests from this sting included individuals from 38 different countries (Mindock, 2019). As long as teens and predators have access to social networking applications, the exploitation will continue.

2.3 Understanding Law Enforcement Challenges

The law enforcement officers or analysts who investigate these types of crimes have a difficult time keeping up with the fast-paced migration to new applications and understanding how these new application work. As mentioned before, teens do not stay on one application for very long. As new applications or social media platforms come into the spotlight, they leave the old ones behind in favor of the newer forms of communication. Predators know and understand this and are able to find ways to stay up to date with the current trends in social media that their targets are using.

One issue law enforcement is facing, is the lack of research for these new applications (Ramdass, 2016). When a new platform becomes popular, besides the teens using it, law enforcement are usually one of the first to encounter it because of the crimes or investigations

involving the apps. Mobile forensic companies are trying to keep up, but with the rapid migration of social media, they are struggling as well. Cellebrite, one of the top mobile forensic tools, releases a document with every new update, detailing what applications they support and are working on supporting (Cellebrite, 2019d). Although these top mobile forensic tools support a lot of the newer social media applications, it takes time for researchers to understand the layouts of the data inside of the applications and how to process it.

With the new security and privacy features that are being implemented into applications, it gets even more difficult to find relevant data or evidence with forensic tools (Horsman, 2018). Security focused platforms are now not leaving behind data on the phones that accounts were connected to, making it impossible to find evidence for investigations without serving the social media companies with legal warrants. Encryption is another issue when it comes to finding evidence on these types of applications. When the messages or communication has been encrypted on the sender and receiver's ends, it is likely not possible to find any data of evidentiary value on those devices (Judge, 2018). More about encryption is discussed further in the next section. In a survey by Cellebrite, investigators and law enforcement officers said that the inability to extract data from encrypted apps is one if the biggest challenges they are facing currently (Cellebrite, 2019a). There are also the anonymous social media platforms that hide the identities of its users, making the chase to find the predators much more difficult (Farrugia et al., 2018). Professor Adam Wandt was interviewed about the significance of applications like Snapchat and their ability to hide data. Professor Wandt stated:

> "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. And we're also seeing difficulty in law enforcement being able to investigate due to the safeguards Snapchat has in deleting both snaps and 'stories' after certain amounts of time." (Hobson, 2018, p. 1)

Overall, one of the biggest challenges law enforcement are facing are the number of online offending cases are exceeding the resources they have available to them. They are faced with more cases than ever before with growing amounts of data to look through and more applications and devices to be familiar with (Dwyer et al., 2016). The other big challenge to LE is the encryption, safeguards, and masking abilities of these newer applications, hiding

communications, the sharing and storage of pictures, of potential evidence for a crime (Hobson, 2018).

2.4 Understanding Privacy and Safety Challenges

The current discussion and arguments about internet privacy and encryption are of concern for those protecting children and fighting against child exploitation and other crimes committed against children online. The National Center for Missing and Exploited Children (NCMEC) posted a statement discussing their concerns for end-to-end encryption on the big social media platforms that harbor these child crimes. They discuss how if tech companies "shutter the visibility to this dehumanizing abuse of children by adopting end-to-end encryption without a solution in place to safeguard children, those who are sexually exploited will be invisible and left as collateral damage while offenders will continue to create, share, and collect child sexual abuse images without detection" (National Center for Missing & Exploited Children, 2019, p. 1). The FBI Director, Christopher Wray, has said that end-to-end encryption would make Facebook and other social media networks, a "dream come true" for child predators without the fear of consequences (CNN, 2019).

Law enforcement agencies say encryption is a major obstacle when investigating child sex abuse, terrorism, and other types of crimes involving encrypted sites or applications. Law enforcement entities, such as the Justice Department, have argued this topic for many years saying that encryption is a tool that protects the personal data of users from malicious groups, but also lets child predators, as well as other criminals, hide their online criminal activity. Sujit Raman, an associate Deputy General in the Justice Department, says there has been a consensus among law enforcement officials that end-to-end encryption is a serious problem. (Valentino-DeVries & Dance, 2019). End-to-end encryption on these social media applications would be risking the safety of children everywhere (Farid, 2019).

In 2018, NCMEC received over 18 million reports of online child abuse. If encryption was implemented on the social networking platforms that predators are using, these reports would likely be cut in half. NCMEC pleads for a way for tech companies to "see" the online abuse and be able to report it to the authorities so then law enforcement can investigate and rescue a child from abuse. Encryption will not stop offenders from abusing children, sexually exploiting innocent victims, or attempting to meet up with children. End-to-end encryption will only close

the curtain on what is happening online (National Center for Missing & Exploited Children, 2019).

Government entities across the globe are arguing for tech companies, like Facebook and Apple, to think twice about fully implementing end-to-end encryption. They argue encryption is making it impossible to track child predators, terrorists, and other criminals (Perlroth, 2019). The international police organization, Interpol, condemns the implementation of end-to-end encryption, saying it protects child sexual predators (Menn, 2019). Australian lawmakers, in 2018, passed a bill requiring tech companies to provide Australian security agencies with access to encrypted data from secured and encrypted communications. This bill was based on a 2016 act from Britain where the British government can now compel Britain companies to provide an encryption key to secured information. India has also implemented similar laws with Facebook where Indian laws requires the decryption of messages and for them to supply the Indian government with the unencrypted information upon request (Perlroth, 2019).

2.5 Understanding the History of Top Social Networking Applications Teen are Using

In a report from 2013, the teen social media usage between 2006-2012 was a little different than what is present today. It was found that 94% of teens had a Facebook profile, 75% had a Twitter profile, 11% had an Instagram profile, and 7% had a Myspace profile (Madden et al., 2013). In a 2015 study, 71% of teens used Facebook, 52% used Instagram, 41% used Snapchat, 33% used Twitter, 33% used Google+, 24% used Vine, and 14% used Tumblr (Lenhart, 2015). In these trends, you see a shift from using some apps more or less than others, with newcomers becoming more popular. In a more recent study from 2018, it was found that Instagram (26.64%), YouTube (24.96%), and Snapchat (24.62%) were found to be the most popularly used applications in middle school student, with Facebook (7.59%), Twitter (2.19%), Pinterest (2.02%), Vine (1.52%), and Google+ (1.18%), being less popular but still used (Martin et al., 2018) .

Investigators see these applications being used by teens, and forensic companies can then research how the data in these applications are stored, so the forensic tools can then support these apps. Cellebrite and Magnet Forensics both post a reference document displaying what applications their tools support. These are updated with each release and version update of their tools and display what content within the applications that they are able to find (Magnet

Forensics, 2019; Cellebrite, 2019b; Cellebrite, 2019c). This can help researchers with knowing what applications to focus more on, with regards to what is popular and what is not supported yet.

News agencies are constantly posting articles online about the newest dangerous applications teens are using and for parents to know about. A local new station in Phoenix states that popular apps like Messenger, Snapchat, Instagram are hotspots for predators, but also mention MocoSpace, Kik, Omegle, Ask.fm, Telegram, and Whisper are less known by parents but just as dangerous (KNXV-TV, 2019). A news station in Nebraska tells parents to check their teens phones for apps like MeetMe, Grinder, Skout, Whatsapp, TikTok, Badoo, and more because they could be putting their children in dangerous situations (Naspretto, 2019). Authorities in Florida spread information from a news site, warning parents about 21 different applications parents should look out for on their kids' phones, including, Monkey, Bumble. Live.Me, Holla, Hot or Not, and many more (10News Staff, 2019). Even internationally, news sites are warning about the potential danger of certain apps targeted for teens. Metro News from the UK warns parents about the dangers of Kik, Tellonym, Yubo, Monkey, Chatous, and more (F. Brown, 2019). Discord has made headlines several times, one where a teen boy was lured to a house where he was confined and made into a sex slave for six men and one woman (Sederstorm, 2019). Kik also making several headlines, was involved in the premeditation and kidnapping of a 13-year-old girl, as well as the murder of an 18 year old female (Stolberg & Pérez-Peña, 2016). All these warnings and articles are telling of what social media applications teens are tending to use more frequently.

2.6 Understanding Previous Research on Social Media Application Forensics

In the last decade, there has been a social media revolution within mobile devices (Al Mutawa et al., 2012). The previous research for this area has covered well known applications like Facebook, Twitter, LinkedIn, Instagram, Google Hangouts, as well as others. With the constant changing and the evolution of social media applications, there are new applications needing to be analyzed every day. Mutawa et al. (2012), discuss that the increased uses of social media on mobile devices, makes these devices a "goldmine" for forensic evidence (Al Mutawa et al., 2012). The head of the UK College of Policing has said that complaints originating from social media has taken up at least half of the front-line police officer's workload. There are many

different purposes that a forensic investigation of social media may be required, for criminal matters, to internal investigations of a corporate company (Taylor et al., 2014).

There has been plenty of previous research on social media applications, most all have been focused on applications with an overall popularity among all users and not dissecting what applications are most popular among teenagers. In a 2015 study by Awan, the applications that were forensically examined were Facebook, Twitter, and LinkedIn. The author used four different smartphone brands, Apple, Android, Windows, and Blackberry, and populated each phone with these applications and user data. The author found various forensic artifacts among these applications including SQLite databases and plist files containing user information and activities. The only phone that they did not get any results for was the Blackberry (Awan, 2015).

In another study, by Chang and Yen (2019), they focused on one application, Instagram. They mention how previously "flourishing" social media applications like Facebook, Google +, and LinkedIn are being replaced by newer and emerging social networking sites like Instagram. The reason they choose Instagram is because of the popularity it has among teens and young Millennials. They state that 41% of Instagram users are 24 years old or younger, in the United States. They forensically examine Instagram on an Android phone as well as the web version using different internet browsers. They find many forensic artifacts left by the different browsers as well as the Android phone (Chang & Yen, 2019).

In a 2012 study by Mutawa et al., the authors discuss the forensic analysis of Facebook, Twitter, and Myspace. The study was conducted on three different smartphones, the iPhone, an Android, and a Blackberry. They were conducting the study to determine if there were any artifacts that remained from these applications, on the internal memory of these phones. They found in their study that user data and artifacts were able to be found on all devices and applications except for the Blackberry, which was similar in results as the study by Awan in 2015 (Al Mutawa et al., 2012; Awan, 2015). As this study was done in 2012 and the Awan study was done in 2015, it does say something for the privacy factors and anti-forensics of the Blackberry and the inability to find any forensic data on those devices. The applications chosen for Mutawa et al.'s study was not inclusive of only teens usage, but of the entire population.

In a study by Scrivens and Lin (2017) focuses on the applications Google Hangouts and Facebook Messenger. They populated an Android device with these applications and user data like previous studies mentioned. The purpose of the study was to find any forensic artifacts

found on the phone's internal storage, left by Facebook Messenger and Google Hangouts. They were able to find that both applications did leave behind a significant amount of unencrypted user data that would be relevant in a forensic investigation (Scrivens & Lin, 2017).

A 2014 study on the WhatsApp Messenger application discussed using an Android emulator to and populating it with the app and user data, in place of using a physical phone. The purpose of the study was to find forensic artifacts left by WhatsApp Messenger on an Android device. They were able to find artifacts relating to contacts and chats. The authors chose WhatsApp Messenger because of its general popularity among all users, mentioning the app has over 400 million active users as of 2013 (Anglano, 2014).

Another study including WhatsApp and Viber was conducted in 2013, proposing to find forensic artifacts on five different Android devices with these applications installed. The authors mention that WhatsApp and Viber are two of the most downloaded applications in the Google Play Store, giving this as the reason they chose these applications to perform forensic analyses on. The authors found that using a forensic tool, Cellebrite, they were not able to find as many artifacts as when they manually reviewed the file structure and database files of these applications. They mention that it was important to manually review the application and the files contained within the applications file structure to obtain relevant forensic artifacts that the forensic tool did not obtain at all (Mahajan et al., 2013).

The gaining popularity of health and fitness data motivated a study for an application analysis of user data from nine different health and fitness tracker apps. The apps included in the study were those of MapMyFitness, RunKeeper, Strava, MyFitnessPal, Runtastic, Health Infinity, Fitness Tracker, Nike Training, and JEFIT. The social considerations of these applications include adding friends, sharing goals, or results of a workout, mapping locations and sharing those, also. These considerations were not analyzed in this study but would be very interesting to investigate. Some of the data gathered and extracted from these applications were names, birthdays, sex, height, weight, emails, locations, following, followers, and workout descriptions. Although these are mainly used for personal activity tracking, a lot of this information can potentially be shared with strangers and friends (Hassenfeldt et al., 2019).

The National Institute of Standards and Technology, NIST, has documented frameworks and guidelines of how to properly conduct extractions and analyses on mobile device forensics (NIST, 2019). The guidelines are reviewed and set standards for the forensic fields of study.

Social media applications and their related data are a part of the internal memory artifacts section of the framework and guidelines. The requirement for a successful forensic tool analysis states that all social media application data available from the extraction file will be presented by the forensic tool (NIST, 2019). This potentially could not be the case if there are applications that are not fully supported by the forensic tools.

The gaps found in the previously mentioned literature are two-fold. One gap is the fact that none of these previous studies focuses on applications that are most popular among teenagers. This is an important gap to fill, as teens use smartphones and applications more than any other generation. It is important to understand what applications they are using and fill that gap on forensic analyses of those applications. The other gap to fill within these previous studies, is examining the applications that forensic tools are not fully supporting. As one study mentioned, the forensic tool used to examine Viber did not see any forensic artifacts that were there if the examiner looked through the application manually (Mahajan et al., 2013). It is important to understand which applications are not currently or fully supported by forensic tools examiners are using to analyze devices. In this study, these gaps are investigated, and the goal is to fill both mentioned gaps that come from previous studies.

CHAPTER 3. METHODOLOGY

3.1 Hypothesis

This study aims to investigate emerging mobile applications used by teens and to what extent they are being supported by forensic tools, based on the number of artifacts found. The research question this study explored was: to what extent are digital forensic tools supporting new and emerging mobile applications seen recently in investigations involving teenagers?

Due to the rapid evolution and changes of mobile applications, there were no similar studies found that were investigating this question, making this study exploratory in nature.

The hypothesis for this study was:

H_1: New and emerging mobile applications are limited in the extent of support forensic tools provide, where there are incomplete or missing artifacts not recovered from the applications.

In this context, limited means that the application is not well supported by the forensic tools, as in the forensic tool does not provide all viewable data that can be manually seen on the device that is being examined. The forensic tool is not providing access to data that the examiner knows is located on the application. The application could be considered limited in support from a forensic tool if there is content on the phone, like text messages, the examiner knows is located on the device, and the forensic tools are not able to extract or show that known information.

3.2 Procedure

The design for this study includes two parts and five phases. Figure 3.1 displays a diagram of how this research was outlined.

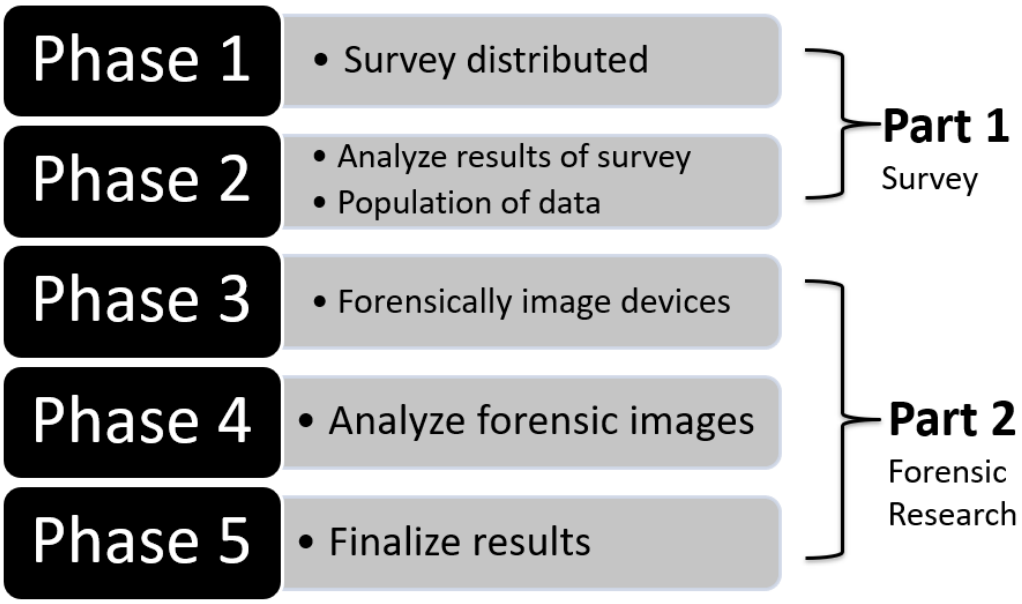

Figure 3.1 - Outline of study design

Phase 1

This study began with a survey that was created through Qualtrics. Qualtrics is an online survey creation, collection, and analysis tool that is provided by Purdue University ("Qualtrics Purdue University Innovative Learning," n.d.). The survey was distributed through group email listserv's and used convenience sampling. The survey was laid out with several questions, dichotomous and open ended. The survey was kept short, as to not have participants become inattentive. By keeping the survey short, the goal was to have the participants alert and attentive when answering the questions. The survey was also kept anonymous, preventing the collection of personal and identifying information about participants. Only participants who were over 18 and were residents of the U.S. were allowed to complete the survey. The participants obtained an anonymous link to the survey that they receive from an email posting in an email group listserv they are a part of. Their personal email addresses were not known, as the email was sent to a general group distribution list. The questions that were presented in the survey did not ask for identifiable information that could link the participants back to their identity. No personal information such as name, or exact place of work was asked or collected. Once the survey was

distributed through the group email listserv, and results were gathered, the information was analyzed using a statistical software to determine if there appears to be common applications that the participants provided, that they are seeing more often within investigations involving teens and those applications not being supported by forensic tools. The groups that were chosen to be included in the sample were from IACIS (International Association of Computer and Investigative Specialists) and ICAC (Internet Crimes Against Children). Since this group of participants that received the survey were a part of a professional digital forensics' organization and law enforcement task force focused on digital crimes, it was assumed that they were familiar with the types of issues the survey overviewed. The analysis of this data took place once all data was collected. Further detail on the survey design and sample is provided in Section 3.3 and 3.4.

Phase 2

The analysis of the data was processed using Qualtrics to initially process the collection of the raw data, and then Qualtrics and IBM® SPSS (Statistical Product Service Solutions v.26) to complete the analysis of the data by running statistical analyses. More specific detail on statistical analyses is provided in the Section 3.5 Analytical Methods.

Once this data was analyzed, the top three mobile applications listed that were not supported by forensic tools were chosen to be the applications included in this study. These included Monkey, Houseparty, and Likee. A test device was provided for this study, as the mobile applications require a device for them to be installed. The test phone was a factory reset Android device, to provide the best possible results for the analysis of the applications. A Samsung Galaxy Note 4 (SM-N910V) running Android version 5.1.1 was the test device being used in this scenario. This device was not rooted. The choice made to not root the device stems from the way law enforcement investigators and analyst receive and handle evidence. If the device were to be rooted, this potentially could destroy the information on the device and could change data, losing the integrity of the evidence. The most realistic approach to this study was to not root the device. Figure 3.2 displays the technical detail of the test device and the version numbers of each of the applications chosen. These version number for the applications were the most up to date version at the time of this study.

Table 3.1 - Device and application technical details

Application	Monkey	Houseparty	Likee
Application Version	6.1.0	1.34	3.26.60
Device Type	Samsung Galaxy Note 4 32GB	Samsung Galaxy Note 4 32GB	Samsung Galaxy Note 4 32GB
Model	SM-N910V	SM-N910V	SM-N910V
OS version	5.1.1	5.1.1	5.1.1
IMEI	990004807995950	990004807995950	990004807995950

When populating the information on the test mobile device, guidelines outlined by NIST were followed (Ayers et al., 2018). To begin the population process for the mobile device, unique identifiers of the phone were documented. The only data that would need to be populated on this test device would be the social media application data from the chosen applications. According to NIST, their framework for social media application population says to identify and document the profile information, status updates, personal messages, etc. For each application the data points (artifacts) were different, based on the type of application and its features (Ayers et al., 2018). Below Table 3.1, 3.2, and 3.3 show the different types of data that was populated for each application, along with the actual content of data, and how many different number of each artifact was populated. It was not clear what data was going to be populated for each application until the applications were downloaded, it was understood how each application worked, and the type of data that was collected by the applications. The data that was populated is referred to, in this study, as known data. The data for each application was directly populated to each application manually by hand, as if a real user was interacting with the applications. This was the only possible way to populate user data that was known at the time of this study. Each application was gone through thoroughly and every type of data point the application collected, was populated. All data points and artifact types were recorded as the population process continued.

For each application, the test device was factory reset. This process consisted of downloading one application, populating the known data, performing the forensic extraction of

the device, then factory resetting the device for the next application. The default Android factory reset setting was used to perform this process.

Table 3.2 – Artifacts populated for Houseparty

Houseparty Artifact type	Data	# of Artifacts Populated
Email	REDACTED@gmail.com	1
Full name	Spring	1
Username	Springtest2020	1
Password	Encrypted token	1
Date of birth	3/19/2002	1
User activities	Added user sender_1 and sender_2 - 3/29/2020 3:45pm	2
Video calls	Group video call invite with sender_1 & sender_2	1
Video call activity	Played trivia in group call	1
Video call log	List of accepted and denied calls by user	4
Notes (messages)	Content of chat messages with user, date, and time	9
Waves	Logs of users sending waves via Notes	3
Facemail	Log of users sending Facemail invites via Notes	2
Contacts	List of contacts added with usernames	4
TOTAL		31

Table 3.3 - Artifacts populated for Monkey

Monkey Artifact type	Data	# of Artifacts Populated
Username	Spring2020	1
Password	Encrypted token	1
First name	Spring	1
Date of birth	3/19/2002	1
Gender	Female	1
Phone number	765-761-2492	1
Profile pictures	Image1, Image2, Image3, Image4, Image5	5
Profile bio	"vibing"	1
Profile song	Dance Monkey – Tones & I	1
Contacts	List of contacts	1
Following count	15	1
Follower count	5	1
Chats	Chats that were sent and received	41
Account activities	Action: Deleted 2 images from profile pics	1
Moments	Created and posted moment video	1
Moment activity	Jamal liked moment	1
Video chats	Chatted with Mark, shontefoster, Jeff, king2300	4
Followed	Followed Blue, Jovel, Angel, Matthew, Everest, Jon, Mariane, ethan, teddycoolman,	9
Followers	Shontefoster followed me	1
TOTAL		74

Table 3.4 - Artifacts populated for Likee

Likee Artifact type	Data	# of Artifacts Populated
Phone number	765-721-2492	1
Username	Spring2020	1
Location	Lafayette, IN/West Lafayette, IN	1
Profile picture	Image1	1
Account Activity	Added image to profile 4/2/2020 4:48pm	1
Fans (followers)	List of users who follow account	5
Messages	Log and content of sent and received messages	8
Video activity	User activities likes, comments, deleted draft video	8
Password	purdue2020	1
DOB	3-19-2002	1
LikeeID	501218583	1
Astrological sign	Pisces	1
Level	4	1
Gender	Female	1
Comments	Comment posted on savvanahlbrant's video "hey!"	1
Hometown	Lafayette, IN	1
Bio	"Hi"	1
Education	Purdue	1
Career	Position: test, Company: Google, from 2020.04- now	1
Following	List of users who is followed	12
Videos	Video posted to feed/profile	1
Follower count	Number of followers on profile	1
Following count	Number of following accounts on profile	1
TOTAL		52

Phase 3

After adding the known data to each application, the device was then forensically imaged after each data population cycle using NIST framework 800-101 (Ayers et al., 2014), and Cellebrite UFED 4PC version 7.31.0.2 and analyzed using Cellebrite Physical Analyzer version 7.31.0.222 and Magnet Axiom version 3.10.0.18500. The device was placed into airplane mode, debugging options were turned on for the device, the device was plugged into the Cellebrite UFED 4PC using cable 133 and then following the on-screen instructions for the device profile SM-910V on UFED 4PC, the device was forensically imaged. For each application, an advanced logical, ADB file system, and advanced ADB physical extraction were completed using the SM-N910V profile on Cellebrite UFED 4PC. At this time, the SHA256 hash values of the forensic images/extractions were recorded. The SHA256 hash values of the forensic images/extractions were later compared to the SHA256 hash values of the images once processing and analysis of the forensic images were complete. When these hash values match, this shows evidence integrity that no data has changed from the time of the extraction to the end of the analysis. Once the forensic images were complete, the extractions were combined in Cellebrite Physical Analyzer, and Magnet AXIOM Examine where the data was loaded into readable formats. The goal in this phase was to forensically image the device for each application. Table 3.5 displays the forensic tools used and their versions at the time of this study.

Table 3.5 - Forensic tools and versions used

Tool	Cellebrite UFED 4PC	Cellebrite Physical Analyzer	Magnet AXIOM
Version	7.31.0.2	3.31.0.222	3.10.1.18500

Phase 4

Once the device was forensically imaged, per application, using Cellebrite UFED 4PC, and the initial analysis was performed on the application data using Cellebrite Physical Analyzer and Magnet Axiom. This initial assessment of the data pertained to viewing the application data shown by the forensic tools to see the artifacts recovered and what the forensic tools were able to parse, or automatically find and categorize artifacts in a user-friendly display.

When using Cellebrite Physical Analyzer, the feature "App Genie" was used. This feature says it can find and parse 3rd party application data and look through SQL databases and other files to try to recover all data possible associated with the application chosen. With Magnet AXIOM, this tool also has a similar feature, Dynamic App Finder. Neither feature recovered all known artifacts. Since all of the known artifacts were not recovered by the forensic tools, a manual analysis was performed. A manual analysis included looking at the SQL databases of the applications and other files containing data inside the file structure of the applications, shown in Figure 3.2 and Figure 3.3. This was completed using Cellebrite and Magnet AXIOM's built in database viewers, as well as text viewers and a Realm database viewer, Realm Studio. This step was completed to search for the missing known artifacts that could have been stored somewhere else that the forensic tool did not parse or extract correctly.

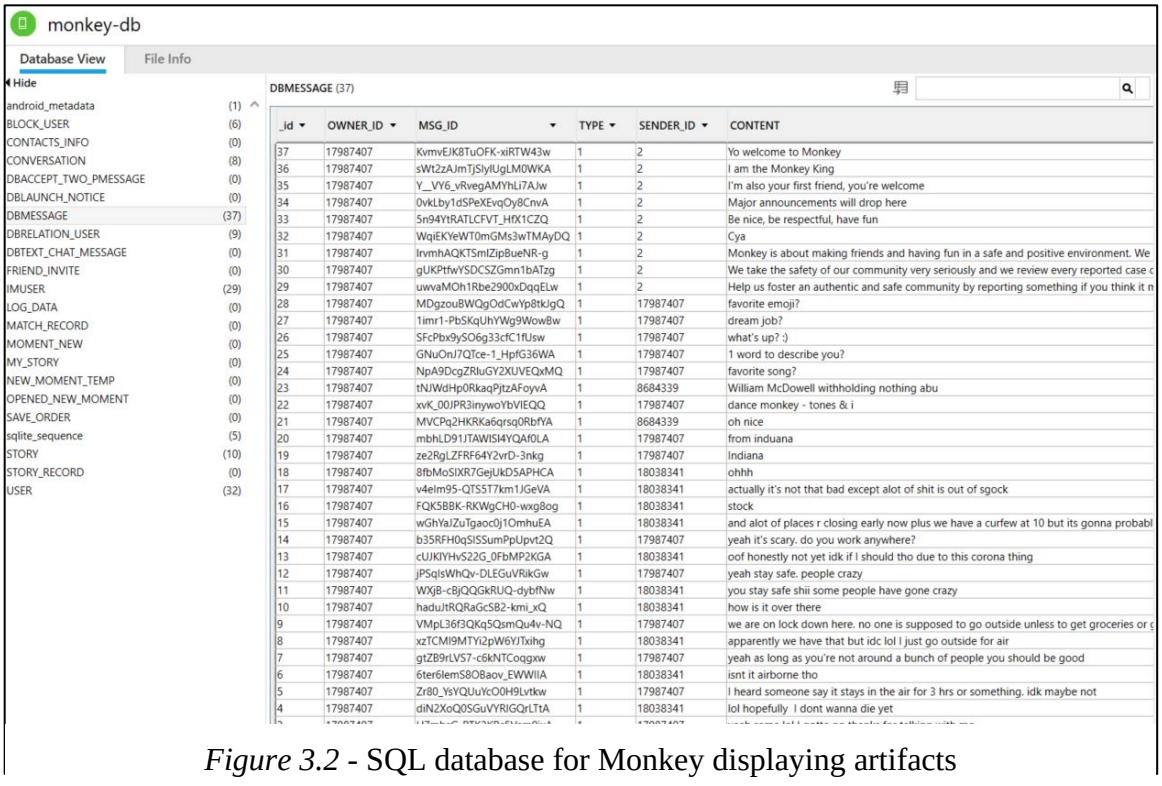

Figure 3.2 - SQL database for Monkey displaying artifacts

Figure 3.3 - XML file from Monkey displaying artifacts

Phase 5

The final phase of this study was to compare the application data found manually, automatically parsed by forensic tools and the populated application data that was not recovered by the forensic tools. There was a known number of artifacts that were populated, and this known number was compared to the found number found during the analysis Phase 4. These results were compared to the forensic tools' list of supported applications, determining if the tools state they have added support for the applications that were tested. To measure the accuracy, reliability, and validity of the forensic tools, and the tool's ability to extract the user data from applications is a complex topic, as there are many unknown variables that could affect where the user data is stored on the physical device not. One way to verify accuracy of the forensic tool, would be to verify a specific piece of information known to be on the application, is also found on the forensic tool's extraction report of that same device. One way to measure reliability of the forensic tool is to test if the same information is showing on one tool as is showing on another. This was used in verifying reliability of Cellebrite Physical Analyzer to

Magnet Axiom. To measure the validity of the tools, this was done by showing the accuracy and reliability of the tools, and showing the tools are functioning like they are supposed to be, with no error. To enhance the accuracy, reliability, and validity of these forensic tools, SHA256 hash values were calculated to show no changes occurred on the forensic image of the device throughout the analysis process. These steps were implemented in the analysis of the applications using the forensic tools.

3.3 Survey Design

The survey for this study was a 26-question online questionnaire. The survey design was a mixture of closed and open-ended questions. The question design was a mixture of dichotomous answers and using open ended response answers. See Appendix A for the entire survey and all questions included in the study.

The first set of questions asked about the demographics of the participants, without asking for any personal and identifying information. The questions were anonymous in nature. Those first questions include asking if they qualified for the survey, age, and if they are a resident of the U.S.

The second set of questions asked the participants to categorize their job role, and their working environment. Then they were asked about the length of time they had worked in their field, the size of their department they worked in, and if they are involved in investigations involving mobile devices or social media. If they answered no to the question regarding if they are involved in investigation involving mobile devices or social media, they were transferred to the end of the survey, where they can no longer answer any further questions. If they answer yes to the previous question, participants were asked about the amount of cases they work involving digital forensics, and the frequentness of mobile applications not being fully supported by forensic tools they work with.

The next set of questions include asked about specific apps, and whether they have encountered them before. The apps that participants were asked about were “Yubo”, “Yolo”, “Houseparty”, “Monkey”, “Lipsi”, and “Likee”. These applications were chosen based on several sources including (Newton, 2016; Newport Academy, 2019; C. Brown, 2019; Dinham, 2017; Protect Young Eyes, n.d.; Castillo, 2017). They were also asked that if they have encountered those applications in their investigations, were they supported by forensic tools.

After those specific app questions, the participants were given the chance to list other applications they had come across in their investigations that were not supported by forensic tools. Then, they were asked to list specific apps that were becoming more prevalent in investigations involving teens and if they were supported by forensic tools.

Finally, the participants were asked if more support for newer emerging mobile applications would be beneficial to their cases and to list how it would benefit them. This was the end of the survey, once the participants finished, they were directed to an end of survey screen.

3.4 Sample

For this survey, the sample consisted of individuals who are members of IACIS (International Association of Computer Investigative Specialists) and the ICAC task force (Internet Crimes Against Children). IACIS is an organization of specialized and trained individuals who have completed certifications in the field of digital forensics. It is an accredited organization and is highly recognized in the digital forensics field. IACIS includes members from all over the U.S., including 70 other countries worldwide. It focuses on providing law enforcement focused training to its thousands of members (IACIS, n.d.). The ICAC task force is a national network of federal, state, and local law enforcement agencies who engaged in proactive and reactive investigations of those involved in child abuse and exploitation involving the internet (ICAC, n.d.).

To qualify for the study, participants were over the age of 18 and current residents of the U.S. The sample consisted of members of the IACIS and ICAC email list. The sample was distributed through each organizations group email listserv's that is distributed to all members. The way the sample was recruited was by sending out an email with an anonymous link to the survey and gathering responses through this method. This study used convenience sampling for this survey. Since this was not a completely random selection of participants, the results may lead to issues of sampling error. As this group of participants consisted of only members from the IACIS and ICAC organizations, the entire population of digital forensic examiners was not fully represented, but this group did represent the population enough for an accurate representation, for this study's purpose. The total number of participants was 53 and after cleaning the incomplete responses and removing participants who did not pass qualification questions, the total complete responses was 38. This was a response rate of 72%. This was a

good number to work with, as it was large enough to get a good and diverse response from the sample group. Results are typically more reflective of a population with more responses, but this number was enough to get an understanding of answering the research question.

This sample group was chosen because of the expertise of the IACIS and ICAC member group and their diversity, when it comes to geographical area within the U.S. Members are involved in law enforcement investigations of digital devices and should be aware of mobile applications among teens and their support with forensic tools. ICAC is focused on digital crimes happening online to the younger generations, making the ICAC organization a very good group to include in the study. The reasoning for only using U.S. residents for this study was because of the diversity of applications that are used between countries and the differences that would make on the survey. Some apps are not available to those in some countries as they are in others, so it might restrict the ability to examine those select applications if they were to have appeared in the survey results. Some limitations for using only these two groups would include, results not directly reflecting views of teens by using adult's opinions and these are only the views of two groups of those involved in the field and could limit the responses or views of an entire population. Using only IACIS and ICAC members could potentially limit the responses from the survey, but this was the best implementation due to time constraints. This survey and the sample was approved to use by Purdue University's IRB (Institutional Review Board), see Appendix B.

3.5 Analytical Method

The first part of this study dealt with the survey and analysis of the survey data. The data that was collected from this survey was analyzed using quantitative analytical methods. The data was exported from Qualtrics, once the survey ended. Statistical testing was completed on the collected results using IBM® SPSS (Statistical Product and Service Solution v.25). Once the data was imported into SPSS from Qualtrics, the data was cleaned of any missing or incomplete data and removing any outliers. Participants that did not completely finish the survey, those partial answers were removed. Those who did not pass the qualification questions, over 18, US resident, those results were also removed from the final results. Results were tested by performing a frequency analysis and other descriptive statistics on the questions that were dichotomous. Questions that asked about specific applications and whether they were supported by forensic tools, those applications were totaled by frequency count. Then, in some open-ended

questions, participants listed more applications they had come across that were not supported by forensic tools, either. These were also totaled by frequency count. Demographics were analyzed with the frequency tests and descriptive statistics.

The second part to this study was the analysis of the applications, the user data found within them, and the forensic tools' abilities to parse the application data, meaning automatically find and categorize artifacts in a user-friendly display. The forensic extraction was completed using Cellebrite UFED 4PC v.7.31.0.2. This analysis was completed using Cellebrite UFED Physical Analyzer v.3.31.0.222 and Magnet Axiom v.3.10.0.18500. To finish this analysis, a thorough examination of the application files and any database files contained in the application file structure was completed. A known number of artifacts were placed and populated on the test phone and application. This known number was compared to the found number of artifacts during the analysis phases of the research. The goal of the application analysis was to find user data that was placed on the test phone and application during the data population phase.

3.6 Summary

This chapter has provided an overview of how the methodology of this study was achieved. The hypotheses, procedure, survey design, sample, and analytical method were outlined and described. A survey took place through an online collection site. It was distributed to participants through a professional digital forensics' organization and law enforcement task force email list. Once the data was collected, quantitative analyses were conducted. When the results were found, further manual analysis into the top three applications that meet the specified requirements mentioned in the procedure were completed.

CHAPTER 4. ANALYSIS AND RESULTS

The data from the survey was collected and assessed initially with Qualtrics, then imported to IBM® SPSS (Statistical Product and Service Solutions v.26). A frequency analysis and other descriptive statistics were conducted on the survey results. A frequency count of applications listed by survey takers was tabulated for the applications participants listed as applications used by teens and was not supported by forensic tools. This list of applications was then used to determine which applications would be used to test and analyze further in the next phases of this research.

4.1 Results of Survey

There was a total of 53 responses recorded, after removing partial results and those who did not qualify, leaving 38 complete responses, a 72% response rate. After analyzing the survey data, and it was found that the top 6 applications reported that were being seen in investigations involving teens and not supported widely by forensic tools were Yolo, Snapchat, Monkey, Houseparty, Likee, and Yubo, respectively. Snapchat has been widely researched and many papers and resources have documented the forensic artifacts of Snapchat (Alyahya & Kausar, 2017; AJI et al., 2017). For this reason, Snapchat was eliminated from the top results of this research. The app, Yolo, was found to rely on Snapchat for its primary functions, and most activity on Yolo, was sent and received through Snapchat. For this reason, Yolo was removed from the top applications for this research. The applications that were chosen for the next steps of this research are stand-alone applications that do not rely on any other social media applications to function. This eliminated any application cross contamination of data and keep all artifacts and data within one single application, rather than spread across many different applications. The top three application that were chosen for this research, based on survey results, are Monkey, Houseparty, and Likee.

4.1.1 Descriptives

The survey included qualification questions that eliminated the participants from the study if a certain answer was chosen. One participant input that they were not over 18 years of

age, and seven input that they were not residents of the U.S. These responses were considered invalid since they failed to meet the qualification requirements set in the methodology section. These invalid responses were removed from the sample. Several others did not complete the questions fully, giving a total of 38 complete responses.

When looking at the demographics of the participants, several questions were asked to determine what type of job role they had, their work environment, and the time they had worked in the field. Results for those questions showed that 67% of participants worked in an investigator or detective job role type, and the remaining 33% were analyst or examiners, showed in Figure 4.1.

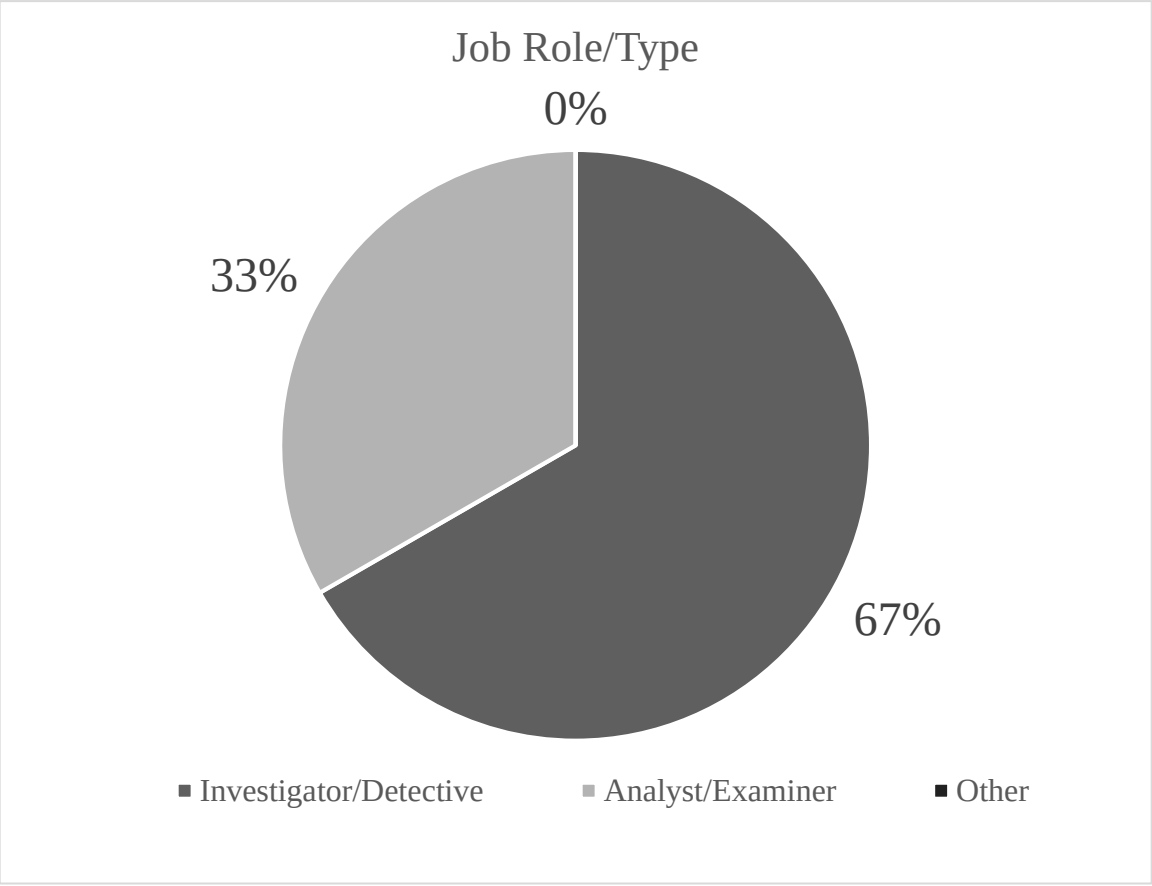

Figure 4.1 - Job role/type demographic chart

Another question regarding the work environment of the participants is shown in Figure 4.2. This chart shows that almost 70% of participants were local law enforcement, and only 15% were state law enforcement, and 10% being federal law enforcement officials. There were only a

small number of participants that were not law enforcement officials, 2.5% being from a law firm and 2.5% working in an academic organization. The difference in the amount of local law enforcement compared to the percentage of the other work environment types was surprising and could have an impact on the results of the applications listed by those participants.

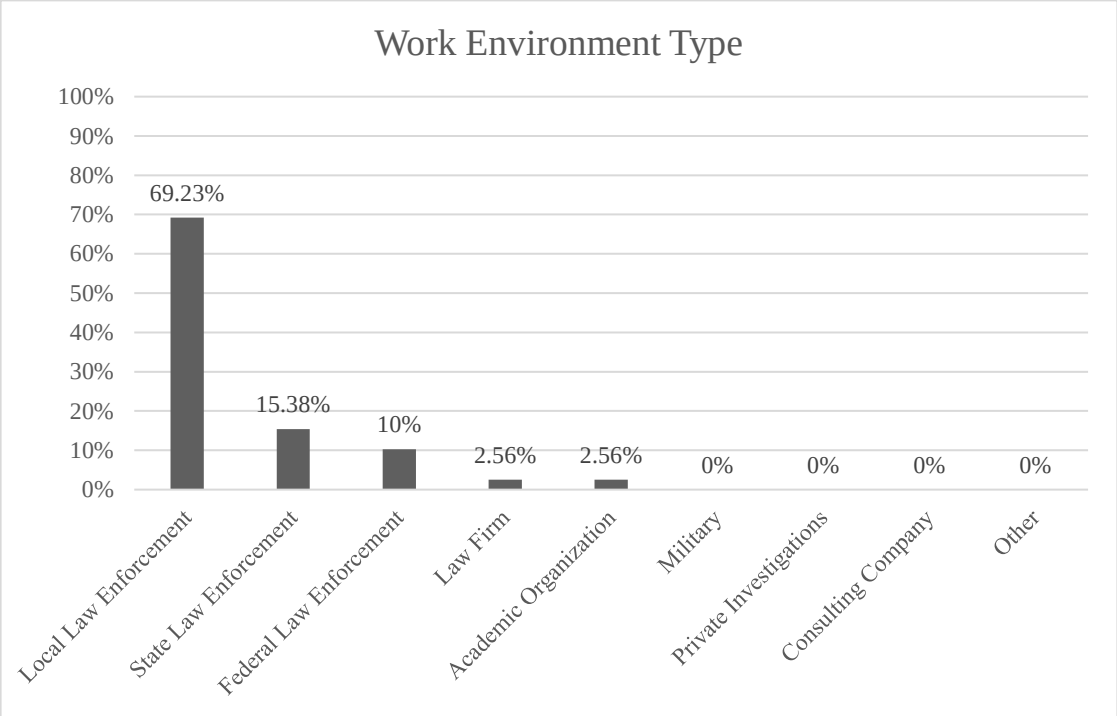

Figure 4.2 - Work environment type demographic chart

Another demographic question was asked, and it asked about the time the participant had experienced in their field. Figure 4.3 shows the results of that question. Over half of the participants stated they had more than 10 years of experience in their field. With this much experience in the sample of participants, the hope is the experience leads over to giving good experienced results to the survey questions.

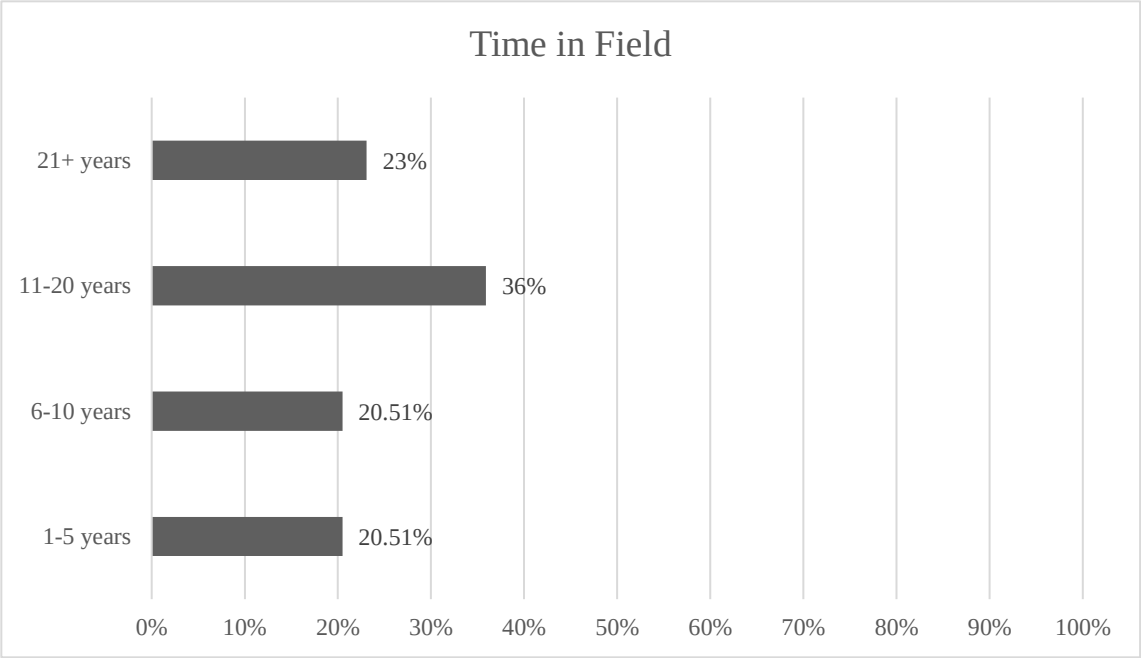

Figure 4.3 - Time in field demographic chart

In the responses from the survey, the applications that were listed as being seen in investigations involving teens and not supported by forensic tools consisted of a wide variety of applications. Displayed in Figure 4.4, when asked how often participants come across mobile applications that were not fully supported by forensic tools to get the information they needed from a device, the majority (79%) of the participants listed that in at least half of their cases or more, they experienced applications that weren't supported by their forensic tools. This leaves the question of how much evidence or how many important artifacts are being missed during investigations if most of the participants are experiencing difficulty with getting information from mobile applications.

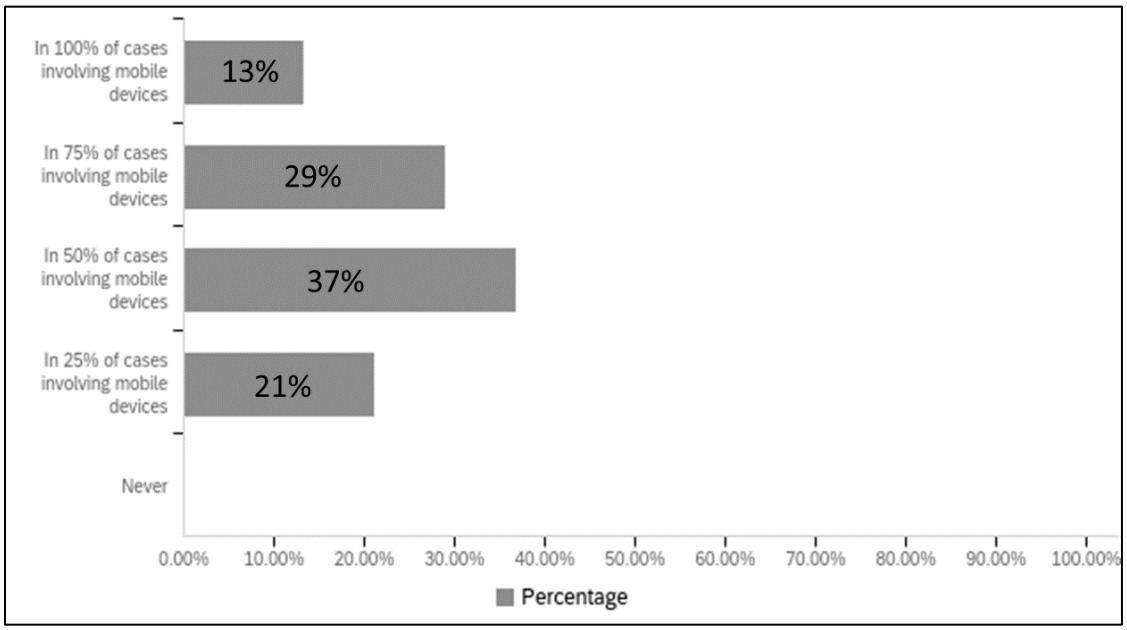

Figure 4.4. Survey results showing the percentage of cases not fully supported by forensic tools

When asking about specific applications and if participants had a case involving those applications, the results showed, in Table 4.1, the top applications were Yolo with 7 cases, Monkey with 7 cases, Houseparty with 6 cases, Likee with 4 cases, and Yubo with 4 cases. The top applications listed, out of the ones given, that were not supported by forensic tools were, Yolo, Monkey, Houseparty, Likee, and Yubo, shown in Figure 4.5. There was a total of 45 different applications listed by participants stating these applications were involved in an investigation they were a part of.

Figure 4.5 - Top 5 applications from survey (appeared in investigation, not supported)

Table 4.1 - List showing applications listed by participants on survey

Application	Was NOT supported by tools in their experience	Was supported by tools in their experience	Was sometimes supported by tools in their experience	Involved in a case
Yolo	6	0	1	7
Snapchat	5	0	0	13
Monkey	5	0	2	7
Houseparty	3	0	3	6
Likee	3	1	0	4
Yubo	3	0	1	4
Tiktok	2	0	0	13
Kik	2	0	0	7
Facebook Messenger	2	0	0	3
Grindr	1	0	0	5
Whisper	1	0	0	4
Whatsapp	1	0	0	3
Lipsi	1	1	0	2

4.2 Monkey Results

During the analysis of the Monkey application version 6.2.0 using Cellebrite Physical Analyzer and Magnet Axiom, there were many artifacts that were located and many that were missing. Table 4.5 lists the number of total artifacts populated, the amount found and not found by Cellebrite and Magnet AXIOM, and the amount found manually for each application.

According to Magnet's Artifact Guide (Magnet Forensics, 2019) they do not mention or list Monkey as an application they support. In Cellebrite's Supported Apps document (Cellebrite, 2019b), Monkey was not listed as an application their tool supports, either. During the process of populating the test phone with content, there were 74 different artifacts placed on the application. These artifacts included general account information, account activities, moments, video chats,

following list, follower list, and text chats shown in Table 3.3. When using Cellebrite to analyze the data, only 61% of the known artifacts were manually found. Cellebrite was able to parse 45% of the known artifacts that were on the application, including several unknown artifacts that were not documented in the artifact population process. The unknown artifacts included pieces of information that were not placed on the device during the population process, but the application collected during app use. When using Magnet Axiom to analyze the data, 61% of the artifacts were found manually. Magnet Axiom was not able to parse any of the artifacts. Figure 4.6 shows the percentage of artifacts found manually, parsed by Cellebrite, and Magnet for each application. The SHA256 hash values, shown in Table 4.6 of the forensic extractions matched the SHA256 hash values of the files imported into Cellebrite and Magnet Axiom after the analysis was completed, showing that no data was changed or manipulated during the analysis process of this study. Table 4.2 displays the known and unknown artifacts found, the artifact type, recovery type, data populated, and location or file path the content was located.

For the Monkey application, the artifacts that were not able to be found automatically by the tool, or manually by further analysis consisted of specific user activities pertaining to changing of their profile, adding profile pictures, the actual profile pictures of the test user account, moments, which are videos posted on a user's profile feed, and activities pertaining to the moments. A list of video chats was found with users associated with times and dates of when the calls occurred, but there was one specific user's call that was not able to be found. The users that the test account followed were not able to be found, or a count of how many users the test account followed. Text chats were found, associated with dates and times those occurred, but a section of text chats during a specific time was not able to be found. Unknown artifacts that were not documented in the data population process were found during the analysis process, and consisted of User ID, device ID, coordinates of the city the test user was in, the gender the test profile was searching to match with, the account creation date, and links to video and audio clips that appeared to be videos that were viewed.

Table 4.2 - Monkey findings

Artifact type	Known/Unknown	Recovery Type	Data	Location File Path
Username	Known	Manual	Spring2020	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Password	Known	Manual	Encrypted token	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
First name	Known	Cellebrite Parsed	Spring	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Date of birth	Known	Cellebrite Parsed	3/19/2002	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Gender	Known	Cellebrite Parsed	Female	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Phone number	Known	Cellebrite Parsed	765-761-2492	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Profile pictures	Known	Manual	2 profile image links	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Profile bio	Known	Manual	"vibing"	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Profile song	Known	Manual	Dance Monkey – Tones & I	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Moment screenshot	Known	Manual	Screenshot of Moment video posted	data/data/cool.monkey.android/cache/image_manager_disk_cache/297e8180b3eab4b71492052118ef8c115f961439d9470bc663150ee425ecf77d.0
Contacts	Known	Manual	List of contacts, names, usernames, follower counts, locations, etc	data/data/cool.monkey.androif/databases/monkey-db – DBRELATION_USER table
Following count	Known	Manual	15	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Follower count	Known	Manual	5	data/data/cool.monkey.android/shared_prefs/cool.monkey.android.xml
Chats	Known	Cellebrite Parsed	Most chats that were sent and received	data/data/cool.monkey.androif/databases/androidvideocache.db – SourceInfo table
Links to videos viewed	Unknown	Manual	Web links to videos viewed	1. data/data/cool.monkey.androif/databases/androidvideocache.db – SourceInfo table 2. data/data/cool.monkey.androif/databases/androidvideocache.db – Story table
UserID	Unknown	Manual	17987407	data/data/cool.monkey.androif/databases/com.amplitude.api – Store table
DeviceID	Unknown	Manual	1c3aaf91-61d64a0-b8f5-a4ee22d5ea	Data/data/cool.monkey.androif/databases/com.amplitude.api – Store table
App version	Unknown	Manual	6.2.0	Data/data/cool.monkey.androif/databases/google_app_measurment.db – Apps table
Networks connected to	Unknown	Manual	PurdueCyber2G	Data/misc/wifi/networkHistory.txt

4.3 Houseparty Results

During the analysis of the application, Houseparty version 1.34, Cellebrite Physical Analyzer and Magnet Axiom were used to analyze the data. When referencing Magnet's Artifact Guide (Magnet Forensics, 2019) and Cellebrite's Supported Apps document (Cellebrite, 2019b), Houseparty was not mentioned or listed on either document as being supported by the tool. When populating the test phone with the Houseparty application and data, it was determined that there were 31 different artifacts placed on the application. Table 4.5 lists the number of total artifacts populated, the amount found and not found by Cellebrite and Magnet AXIOM, and the amount found manually for each application.

The type of data populated on the application were general information, user activities, video calls, notes (private and group messages), facemail (video messages), and friends (contacts). When Cellebrite was used to analyze the application data, the software was able to

find and parse 29% of the total known artifacts populated, including 1 artifact that was unknown and not documented in the data population process. 100% of the artifacts were found manually, using Cellebrite's database viewer and other previewing features. When using Magnet Axiom, none of the artifacts were found or parsed by the tool. All artifacts were able to be found by searching the raw data manually in Axiom. Figure 4.6 shows the percentage of artifacts found manually, parsed by Cellebrite, and Magnet for each application. The SHA256 hash values, shown in Table 4.6 of the forensic extractions matched the SHA256 hash values of the files imported into Cellebrite and Magnet Axiom after the analysis was completed. Table 4.3 displays the known and unknown artifacts found, the artifact type, recovery type, data populated, and location or file path the content was located.

During the analysis of the Houseparty application, all artifacts were able to be found. There were no known artifacts that were not able to be somehow located, whether that be automatically parsed by the forensic tools, or manually found through the deep analysis of the applications database files and other files from the app. There were a few unknown artifacts that were found by the tools and manually. Those artifacts consisted of a user ID for the user of the application and of other users that were contacted through video calls and messages ("Notes"), an account creation date, network information of Wi-Fi the user connected to, and a screen grab of what the camera was pointed at a specific time. During the analysis, Cellebrite provided good previewing features of all the different types of files that were found associated with the application, but Magnet Axiom did not provide those same type of previewing tools. With Magnet Axiom, the files had to be extracted and then viewed with default programs from the computer, like Notepad.

Table 4.3 - Houseparty findings

Artifact Type	Known/Unknown	Recovery Type	Data	Location File Path
Email	Known	Cellebrite Parsed	REDACTED@gmail.com	data/com.herzik.houseparty/files/default.realm – RealmUser table
Full name	Known	Cellebrite Parsed	Spring	data/com.herzik.houseparty/files/default.realm – RealmUser table
Username	Known	Cellebrite Parsed	Springtest2020	data/com.herzik.houseparty/files/default.realm – RealmUser table
Password	Known	Cellebrite Parsed	Encrypted token	data/com.herzik.houseparty/files/default.realm – RealmUser table
Date of birth	Known	Manually	3/19/2002	data/com.herzik.houseparty/files/default.realm – RealmUser table
User activities	Known	Manually	Added user sender_1 and sender_2 - 3/29/2020 3:45pm	data/com.herzik.houseparty/files/default.realm – RealmHouseAdd table – joining users field
Video calls	Known	Manually	Group video call invite with sender_1 & sender_2	data/com.herzik.houseparty/files/default.realm – RealmParty table
Video call activity	Known	Manually	Played trivia in group call	data/com.herzik.houseparty/files/default.realm – RealmTriviaDeck
Video call log	Known	Manually	List of accepted and denied calls by user	data/com.herzik.houseparty/databases/instabug.db
Notes (messages)	Known	Manually/Cellebrite parsed few	Content of chat messages with user, date, and time	1. data/com.herzik.houseparty/files/default.realm – RealmNote table 2. data/com.herzik.houseparty/files/default.realm – RealmHouseItem – greet field
Waves	Known	Manually	Logs of users sending waves via Notes	1. data/com.herzik.houseparty/files/default.realm – RealmInteraction table 2. data/com.herzik.houseparty/databases/instabug.db
Facemail	Known	Manually	Log of users sending Facemail invites via Notes	1. data/com.herzik.houseparty/files/default.realm – RealmFacemail table 2. data/com.herzik.houseparty/files/default.realm – RealmNote table
Contacts	Known	Cellebrite pared	List of contacts added with usernames	data/com.herzik.houseparty/files/default.realm – RealmPublicUser table
UserID	Unknown	Manually	5e80f57874e05b272aff3cb4	data/com.herzik.houseparty/databases/instabug.db
Network Info	Unknown	Manually	PurdueCyber2G	data/com.herzik.houseparty/databases/instabug.db
Cached photos	Unknown	Manually	Screenshot of what was on camera screen at specific time 3/30/2020 1:01PM	data/system/recent_images/9_task_thumbnail.png
Account creation date	Unknown	Manually	3/29/20 3:22PM	data/com.herzik.houseparty/files/default.realm – RealmUser table

4.4 Likee Results

The analysis of the application, Likee version 3.26.60, found many known artifacts and several unknown artifacts. Cellebrite Physical Analyzer and Magnet Axiom were used to analyze the application data. Both Cellebrite and Axiom's documents that list the applications each tool supports (Magnet Forensics, 2019; Cellebrite, 2019b), did not list Likee as one. During the population process of the Likee application and content to the test phone, 52 different artifacts were populated. . Table 4.5 lists the number of total artifacts populated, the amount found and not found by Cellebrite and Magnet AXIOM, and the amount found manually for each application. The different type of artifacts and data that were used were general account information, users that were followed, users that followed the test account (fans), private

messages, videos, and user activities. When using Cellebrite to analyze the application data, the software was only able to find and parse 3% of the total number of known artifacts. When browsing manually for the artifacts in databases and other files, only 42% of the total known artifacts were found using Cellebrite and Magnet Axiom, including 10 unknown artifacts that were unknown and not documented in the data population process. Magnet Axiom was not able to parse any of the artifacts. Figure 4.6 shows the percentage of artifacts found manually, parsed by Cellebrite, and Magnet for each application. The SHA256 hash values, shown in Table 4.6 of the forensic extractions matched the SHA256 hash values of the files imported into Cellebrite and Magnet Axiom after the analysis was completed. Table 4.4 displays the known and unknown artifacts found, the artifact type, recovery type, data populated, and location or file path the content was located.

With the Likee application, there were more artifacts not found than those that were. This is not a good sign for examiners dealing with the rise of popularity for this application. For artifacts that were found and parsed by a tool, Cellebrite was the only tool to find any data. Cellebrite Physical Analyzer was able to find two (2) contacts that interacted with the test user. For the known artifacts that were manually found consisted of some general user/profile information like phone number, username, location, profile picture, followers (“Fans”), messages, and activities associated with a video posted. There were very many other artifacts that were not found at all, consisting of other user/profile information like astrological sign, level of profile, gender, hometown, bio, education, career, who test account was following, content of video posted, and account activities like likes, deleted videos, and comments. There were several unknown artifacts not documented in the population process that were found during the analysis consisting of location coordinates of where the test user logged in, network names the test user was using, user ID, IP address the application was using as some type of proxy, application version, type of device test user was using with the application, a device ID, and advertising ID, and the device MAC address.

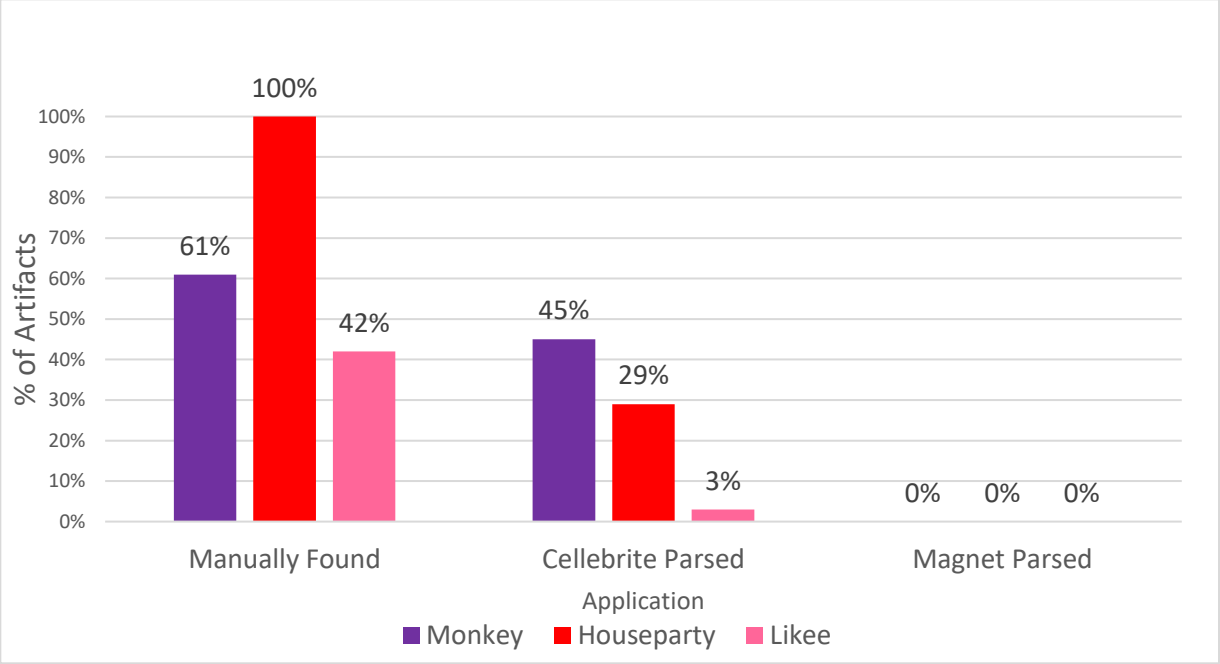

Figure 4.6 - Graph showing the percentage of artifacts found per application

Table 4.4 - Likee findings

Artifact Type	Known/Unknown	Recovery Type	Data	Location File Path
Phone number	Known	Manual	765-721-2492	Data/video.like/files/mmkv_0/g_lk_app_status.kv
Username	Known	Manual	Spring2020	Data/video.like/files/mmkv_0/g_lk_app_status.kv
Location	Known	Manual	Lafayette, IN/West Lafayette, IN	Data/video.like/files/mmkv_0/device_loactions.kv
Profile picture	Known	Manual	Picture of keyboard	Data/video.like/files/.tem_album_1585860519764
Fans (followers)	Known	Cellebrite parsed	List of users who follow account	Data/video.like/databases/push_u2519598877.db
Messages	Known	Manual	Log and content of sent and received messages	Data/video.like/databases/message_u2519598877.db – Messages table
Video activity	Known	Manual	User activities like likes, comments, etc.	Data/video.like/databases/push_u2519598877.db – push messages table
UserID	Unknown	Manual	1775368419	Data/video.like/databases/message_u2519598877.db
IP address	Unknown	Manual	47.88.68.71	Data/video.like/files/mmkv_0/ip.kv
Type of device	Unknown	Manual	Samsung SM-N910V	Data/video.like/databases/bigo_stats.db-journal
DeviceID	Unknown	Manual	46a692a6-6402-385e-8b21-5fe60e9b6lbd	Data/video.like/files/mmkv_0/device_id.kv
AdvertisingID	Unknown	Manual	90183c49-0b24-4fd8-b6d7-12c940e5f070	Data/video.like/files/mmkv_0/com.twitter.sdk.andorid.AdvertisingPreferences.kv
Device MAC address	Unknown	Manual	C0:BD:D1:23:58:0D	Data/video.like/files/mmkv_0/pref.kv

4.5 Summary

The aim of this study was to understand which mobile applications are being seen in investigations involving teens and to what extent those applications are being supported by top forensic tools, based on the number of artifacts found. A survey took place through Qualtrics, asking participants from reputable organizations for their opinions of which applications they are seeing, and which application aren't being supported by the forensic tools. After collecting survey results the applications were tested and analyzed, giving the final results. The hypotheses for this research stated the forensic tools would either fully support these applications, not support the applications at all, or the extent of support would be limited for these applications. Results showed that with the applications that were tested during this study, the support from the forensic tools were limited, based on the ability of the tools to correctly and fully recover all known artifacts populated to the mobile applications. These findings support H_1.

Overall there were successes in the forensic tools being able to automatically parse recoverable data from the mobile applications, but there were also many missing artifacts that needed manually recovery. With two of the applications, some populated artifacts were not able to be found at all.

There was one odd finding when running and verifying the hash values of each application's forensic image file. The hash values for some .bin files contained in the physical extraction were the exact same for each application. The hash value of the physical extraction .bin files were compared for each application when the extraction was complete, and then again when the analysis was complete. The hash values matched for Monkey before and after analysis, Houseparty before and after analysis, and Likee before and after analysis, but each application's hash values for bin files 1-11 and 16-21 for each application matched with each other, as well. The bin files 12, 14, 15, 22, 23, 25, 26, 27 were different from application to application. The explanations that can be speculated for this occurring is that during the extraction process through Cellebrite UFED 4PC, the hash value of a ".bin" container was given, and not the hash value of the contents of the ".bin" file, the bin file 1-11 and 16-21 are imaging parts of the device's storage that the applications do not touch, therefore having the exact same content, or there was some glitch or mistake that occurred during the hashing process.

Table 4.5 shows the total number of artifacts populated, the total Cellebrite and Magnet AXIOM were able to automatically parse or recover, the total not found by the tools, and the amount found manually within each forensic tool. This table also lists the total unknown artifacts that were found, but unknowingly collected by the application during the data population process. Table 4.7, 4.8, and 4.9 show a comparison of each application's artifacts that were found and not found by the forensic tools.

Table 4.5 - Total artifacts found/not found per application

Application	Monkey	Houseparty	Likee
Total Artifacts	74	31	52
Cellebrite parsed	34 known 6 unknown	9 known 1 unknown	2
NOT found within Cellebrite	29	0	30
Found manually w/ Cellebrite	45	31	22 known 10 unknown
Magnet parsed	0	0	0
NOT found within Magnet	29	0	30
Found manually w/ Magnet	45	31 known 1 unknown	22 known 10 unknown

Table 4.6 - SHA 256 hash values for .bin files

After Extraction			
.bin file	Monkey	Houseparty	Likee
mmcblk0p12.bin	3937C54377CD31883AB7225791F4092EC48999EA11A428D27D91982A0BA924191	73CA7C53E0F76AA9B30A0341A834B04EDAD31953FA291BA0F8EC79B419ABD792	E90C0F826963F40B58E421F9E0EF8B2FBFED9C5B7380CC2C4D6C5606224A5CF685
mmcblk0p14.bin	A4457CD9F92BD2551682406 6F98ED4E15CCF77675018 0A6E9417E0B438A92CF8	3086977A50F901ED78F53C828FC415BD68D5F8B5B63000B8C7407974B3005EE0	98CEDE942775A24C33ABE53F2A305ADE17ADADB08054A84FE17E8675B4006556
mmcblk0p15.bin	6424B13806DA9F3F64FA4CEBB95F2498DB0CB2FB0140E9E6377DFD1F0A301598	F1B42BE64745C26DB38340A285B9B1E6B7CDBC054500D76CE1D11D2678 36F649A	EB99349BF0E5BA2CD402791D475CF8D04585CCC246B38F3F98270639063A2CE5C
mmcblk0p22.bin	30F0942333AF9E2C53370E172D37CAA9EEDCBC16E30FAE9EC339E3744EA4F9A1	0AD4DF1AC403EE88053686551D20BC441C87696005EB12C056A68B5C9A73689F	693118BA97E9B82EC8AA4DB2FC552A575029E32591243D3DB40AE5DD275DC628
mmcblk0p23.bin	48FE22E13FD8DC83242EE18BB22B14888069B726737 53FDB2ADDD9EE6F9D4FB89	42B68048257E6F6CB7361886B955BE59F39693FE3978 73CB25DFCF0E543074B8A	6505B8E54072C4F965B1A3B28FA00B701F980D36A0F78E0DD1181C836E94EF6E
mmcblk0p25.bin	8FFF48CC63982DED1191EE475572 76A8F0D09DE553176C373AC7B86B2A7ACE1D6	82F4909B2F45FD54A5104 58EF1633DBC4771A3B171B80AF4A1599DCF217B89DB	C90E2F17F464FD3EE248FA222E1219B2D2802C66D6D17D9319AD36B598FC8014
mmcblk0p26.bin	A3CC8A74996B3C3670D6490B472B5940B0F5896371347 0024CAF6AD4320E3801	F6678C923629250 0DCE8AA45F2D823F09573E4103360D071C187A32D4BB0806797	A9389F5F85C8AFEA0488B5778D01FBEF6466483E77772BDE2F88BAEACA091CADD2
mmcblk0p27.bin	52383F6F6E7E4087555 8C1E70544E8ACA2E564F7412BE1B0A6748744A9D1340F0	38EBC54A91C46E7B11D557582E05E1E857A1DF61007CAC7205B0A5D784880DBBD	D44A708996CEE81592CF8EDDF1244A694C717C8BF08B83F9C1A44C44EEACFD2C

After Analysis			
.bin file	Monkey	Houseparty	Likee
mmcblk0p12.bin	3937C54377CD31883AB7225791F4092EC48999EA11A428D27D91982A0BA924191	73CA7C53E0F76AA9B30A0341A834B04EDAD31953FA291BA0F8EC79B419ABD792	E90C0F826963F40B58E421F9E0EF8B2FBFED9C5B7380CC2C4D6C5606224A5CF685
mmcblk0p14.bin	A4457CD9F92BD2551682406 6F98ED4E15CCF77675018 0A6E9417E0B438A92CF8	3086977A50F901ED78F53C828FC415BD68D5F8B5B63000B8C7407974B3005EE0	98CEDE942775A24C33ABE53F2A305ADE17ADADB08054A84FE17E8675B4006556
mmcblk0p15.bin	6424B13806DA9F3F64FA4CEBB95F2498DB0CB2FB0140E9E6377DFD1F0A301598	F1B42BE64745C26DB38340A285B9B1E6B7CDBC054500D76CE1D11D2678 36F649A	EB99349BF0E5BA2CD402791D475CF8D04585CCC246B38F3F98270639063A2CE5C
mmcblk0p22.bin	30F0942333AF9E2C53370E172D37CAA9EEDCBC16E30FAE9EC339E3744EA4F9A1	0AD4DF1AC403EE88053686551D20BC441C87696005EB12C056A68B5C9A73689F	693118BA97E9B82EC8AA4DB2FC552A575029E32591243D3DB40AE5DD275DC628
mmcblk0p23.bin	48FE22E13FD8DC83242EE18BB22B14888069B726737 53FDB2ADDD9EE6F9D4FB89	42B68048257E6F6CB7361886B955BE59F39693FE3978 73CB25DFCF0E543074B8A	6505B8E54072C4F965B1A3B28FA00B701F980D36A0F78E0DD1181C836E94EF6E
mmcblk0p25.bin	8FFF48CC63982DED1191EE475572 76A8F0D09DE553176C373AC7B86B2A7ACE1D6	82F4909B2F45FD54A5104 58EF1633DBC4771A3B171B80AF4A1599DCF217B89DB	C90E2F17F464FD3EE248FA222E1219B2D2802C66D6D17D9319AD36B598FC8014
mmcblk0p26.bin	A3CC8A74996B3C3670D6490B472B5940B0F5896371347 0024CAF6AD4320E3801	F6678C923629250 0DCE8AA45F2D823F09573E4103360D071C187A32D4BB0806797	A9389F5F85C8AFEA0488B5778D01FBEF6466483E77772BDE2F88BAEACA091CADD2
mmcblk0p27.bin	52383F6F6E7E4087555 8C1E70544E8ACA2E564F7412BE1B0A6748744A9D1340F0	38EBC54A91C46E7B11D557582E05E1E857A1DF61007CAC7205B0A5D784880DBBD	D44A708996CEE81592CF8EDDF1244A694C717C8BF08B83F9C1A44C44EEACFD2C

Table 4.7 - Monkey artifacts found and not

Monkey		
Type of Artifact	Found	Not Found
Username		X
Password		X
First name	X	
Date of birth	X	
Gender	X	
Phone number	X	
Profile pictures		X
Profile bio	X	
Profile song		X
Contacts		X
Following count		X
Follower count		X
Chats	X* (not all were found)	
Account activities		X
Moments		X
Moment activity		X
Video chats		X
Followed		X
Followers		X

Table 4.8 - Houseparty artifacts found and not found by forensic tools

Houseparty		
Type of Artifact	Found	Not Found
Email	X	
Full name	X	
Username	X	
Password	X	
Date of birth		X
User activities		X
Video calls		X
Video call activity		X
Video call log		X
Notes (messages)		X
Waves		X
Facemail		X
Contacts	X	

Table 4.9 - Likee artifacts found and not found by forensic tools

Likee		
Type of Artifact	Found	Not Found
Phone number		X
Username		X
Location		X
Profile picture		X
Account Activity		X
Fans (followers)	X	
Messages		X
Video activity		X
Password		X
DOB		X
LikeeID		X
Astrological sign		X
Level		X
Gender		X
Comments		X
Hometown		X
Bio		X
Education		X
Career		X
Following		X
Videos		X
Follower count		X
Following count		X

CHAPTER 5. DISCUSSION

Results from this study showed that the extent of support from the forensic tools for these tested applications, was limited, based on the ability of the tools to correctly and fully recover all known artifacts populated to the mobile applications. These findings support H_1, which stated that new and emerging mobile applications are limited in the extent of support forensic tools provide, where there are incomplete or missing artifacts not recovered from the applications.

When comparing the number of artifacts that were found by the tools automatically, and the amount of artifacts that had to be manually recovered, the results show that the tools are not parsing or recovering all artifacts that can be found within the applications data. These tools are missing a vast amount of artifacts that are within the data the tools see and read, the tools are just unable to comprehend the data within certain files. The new features of Cellebrite PA and Magnet AXIOM, state they are able to find and recover artifacts embedded within databases and other files containing artifacts. This did not work to what was expected when testing these applications, Monkey, Houseparty, and Likee.

Houseparty was the only application where all known artifacts were able to be found manually. Cellebrite was only able to find 29% of those artifacts. This is not an acceptable number when the artifacts are there, just not in plain sight.

With the Monkey application, only 61% of the known artifacts were manually found, and with Likee only 42% were manually found. There can be many variables concerning the reason why these artifacts were not able to be found. There is a possibility that some artifacts could be stored in the cloud, on a server owned by the application. The applications connect to the Internet and pull-down information from their own cloud servers, displaying them on the application, rather than physically storing that information on the device. This way of storing data, prevents the data from appearing on the physical device, making it difficult to impossible to recover that data.

5.1 Monkey

Monkey and the forensic tools had success but did not recover known artifacts that could make a difference when involved in a criminal case. Compared to all of the other applications, Cellebrite was able to parse or recover the most artifacts from Monkey. This may have been the case because of the way Monkey was storing its application data. Most of the known artifacts were stored in an XML file and a SQL database. Cellebrite might have been able to see these artifacts based on the type of file they were stored in. Overall, Monkey was the most successful application, based on the number of artifacts the forensic tools were able to automatically recover from the applications files.

5.2 Houseparty

With Houseparty, all known artifacts were able to be found manually by viewing application files by hand. Some reasonings as to why the success of the forensic tools were significantly less with this application may be because of the data file and file types Houseparty was storing its data in. Houseparty used a Realm database to store the majority of the known artifacts. Cellebrite was not able to display this type of file, so the use of a Realm database viewer helped in viewing the artifacts. With the use of Realm Studio 3.10.0, most of the known artifacts were found using this viewer. Once viewed with the correct software, this database was organized, and most artifacts were easily found. This was a great example of how the forensic tools may not automatically find all the important artifacts an examiner may be looking for, but through a more thorough examination of the applications files, the important information is there, just not in plain sight.

5.3 Likee

Likee was not an application that was easy to analyze or find the known artifacts. The forensic tools were the least successful in finding known artifacts within this application. Again, a reason as to why the forensic tools were not very successful in finding the known artifacts could be the data file and file types the artifacts were stored in. Several of the known artifacts were located in ".kv" files. Cellebrite and Magnet AXIOM were both unsuccessful in recovering any data from this file type, but it was decipherable when viewing the data file with a text editor.

With the amount of missing artifacts the forensic tools did not recover, locating specific information that could be crucial to an investigation, may be impossible without the skills and knowledge of looking through different file types.

5.4 Limitations

One limitation this study faced was the short amount of time that data points were populated on the devices, around two (2) days per application. This could be extended to see if the application keeps all data from several weeks back, to current and more recent data points.

Another limitation that was considered was the variability in the devices used. There is a major difference in the ability to extract data from newer devices to older devices. In this study, an older device was chosen, because of the ability of the forensic tools to extract a full physical extraction of the devices data. A full physical extraction, which is a bit for bit copy of the devices data, should contain all data related to the application being tested. If a newer device was chosen as the test device, a full physical extraction may not have been possible, and depending on the operating system the device is running, that could also limit the data extraction capabilities from the forensic extraction tools that were used. There is a wide variability in extraction ability when dealing with different devices, meaning if using a different test device, the results could drastically change.

An additional limitation that was considered was the different versions of each of the applications, and that if analyzing a different version of each application, it may yield different artifact results.

A limitation occurring with the survey included the survey being a convenience sample. Because of time and funding constraints, a perfectly balanced sample was not able to be obtained for this study but working with the available participants gave as fair of a representation of the total population as possible. The number of responses limited the results of the survey, as well. If there were more survey participants, the results could have been different.

Despite all of the stated limitations, this study provided good research and still resulted in important and valid findings.

5.5 Conclusion

The survey for this study revealed that there are a variety of applications law enforcement are seeing during investigations involving teens, that are not being supported by forensic tools. The research and testing part of this study revealed the many artifacts found and not found for the top applications listed from the survey. Most of these artifacts that were found, were found manually by analyzing the application files like databases, xml files, and other files found within the application's structure. These analyses showed that the forensic tools well known to law enforcement, are not parsing these known and available artifacts. Most of these missing artifacts are there in the application's data file, but the tools are not seeing them. The extent that forensic tools are supporting these new and emerging applications is limited, based on the findings and the number of artifacts the forensic tools were able to recover.

When analyzing the Monkey application, 61% of the known artifacts were found manually, with Cellebrite Physical Analyzer parsing 45% of the known artifacts and Magnet Axiom parsing 0%. With the Houseparty application, 100% of the known artifacts were found manually, with Cellebrite Physical Analyzer parsing 29% of the known artifacts and Magnet Axiom parsing 0%. For the analysis of the Likee application, 42% of the known artifacts were found manually, with Cellebrite Physical Analyzer parsing 3% of the known artifacts and Magnet Axiom parsing 0%. During the analysis of Monkey, six (6) unknown artifacts were found, one (1) was found with Houseparty, and ten (10) were found when analyzing Likee. Overall, based on the percentage of artifacts automatically recovered and found by the forensic tools, Monkey appeared to have the most success with the forensic tools, second being Houseparty, and Likee following in third.

Through this research, many artifacts were found and the ability to find these artifacts can now help examiners and analyst find the data they might be looking for to help their investigations. The capability to expand the abilities of these forensic tools to better support these applications is an option now that the locations of the artifacts are known.

The difference this research can make and the impact it could have on future investigations, cases, or research, is great. With knowing the locations of now known artifacts within these specific applications, practitioners can now refer to this research and the results found within this study to help further their own investigations or research. What this study has provided to the mobile forensics' community includes a reference guide for each application,

Monkey, Houseparty, and Likee on the locations and exact file path of where important forensic artifacts can be located on a forensic extraction. This study has laid out a methodology and model for population of data for these applications and how to forensically examine them to find forensic artifacts. This study has also shown the unreliability of professional forensic tools and reasons of why to not blindly rely on their findings, to determine the best evidence for an investigation. It is shown that these tools are missing important pieces of data that could have a large impact on investigative findings. There is now a roadmap created through this study, of what these forensic tools are missing and where to find these pieces of data within the forensic extractions. It is important for forensic practitioners to understand they cannot rely blindly on these tools to show the best evidence. It is important to have the skills and the knowledge to understand how to manually review this type of data. Forensic investigators, examiners, analysts, practitioners need to understand the data behind the scenes of the tool, not just what is displayed on the surface.

REFERENCES

10News Staff. (2019, September 27). *21 apps parents should look out for on their kids' phones*. 10NEWS. https://www.wtsp.com/article/news/local/sarasotacounty/apps-parents-monitor-children-targeted-predators/67-10f7e344-c634-4670-b009-1002ab76a874

Acevedo, N. (2019, November 9). *Two Disney employees among 17 arrested in child pornography sting in Florida*. NBC News. https://www.nbcnews.com/news/us-news/two-disney-employees-among-17-arrested-child-pornography-sting-florida-n1079266

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).

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation, 9*, S24–S33.

Alyahya, T., & Kausar, F. (2017). Snapchat analysis to discover digital forensic artifacts on android smartphone. *Procedia Computer Science, 109*, 1035–1040.

Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation, 11*(3), 201–213.

Awan, F. A. (2015). *Forensic examination of social networking applications on smartphones*. 36–43.

Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (NIST SP 800-101r1; p. NIST SP 800-101r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Ayers, R., Livelsberger, B., & Guttman, B. (2018). *Quick start guide for populating mobile test devices* (NIST SP 800-202; p. NIST SP 800-202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-202

Bentley, F., Church, K., Harrison, B., Lyons, K., & Rafalow, M. (2015). Three hours a day: Understanding current teen practices of smartphone application use. *ArXiv Preprint ArXiv:1510.05192*.

Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Brown, C. (2019, August). *The Most Popular Apps for Teenagers: What's Hot, What's Not*. Your Teen Magazine. https://yourteenmag.com/technology/the-most-popular-apps-for-teenagers

Brown, F. (2019, October 24). Apps that you definitely shouldn't let your children use. *Metro*. https://metro.co.uk/2019/10/24/apps-definitely-shouldnt-let-children-use-10975952/

Castillo, M. (2017, August 3). *This popular teen app is quickly turning into Chatroulette 2.0, complete with all its issues*. CNBC. https://www.cnbc.com/2017/08/03/popular-teen-app-monkey-turning-into-chatroulette-2-point-0.html

Cellebrite. (2019a). *2019 Industry Trend Survey: Law Enforcement*. https://www.cellebrite.com/en/insights/industry-survey/

Cellebrite. (2019b). *SupportApps-Android*. Cellebrite.

Cellebrite. (2019c). *SupportApps-iOS*. Cellebrite.

Cellebrite. (2019d, September 4). UFED Physical Analyzer 7.23: Enhance your investigation management process with new tools and capabilities. *Cellebrite*. https://www.cellebrite.com/en/productupdates/ufed-physical-analyzer-7-23-enhance-your-investigation-management-process-with-new-tools-and-capabilities/

Chang, M. S., & Yen, C. P. (2019). Forensic Analysis of Social Networks Based on Instagram. *International Journal of Network Security*, *21*(5), 850–860.

CNN, D. S. (2019, October 4). *FBI director claims encryption plan would make Facebook a "dream come true" for child pornographers*. CNN. https://www.cnn.com/2019/10/04/politics/fbi-facebook-child-encryption/index.html

Connected Children: How Young is "Too Young" for a Smartphone? (2018, April 20). *Parenting NI*. https://www.parentingni.org/blog/connected-children-how-young-is-too-young-for-a-smartphone/

Dinham, P. (2017, April 6). *Warning over Houseparty app after men perform lewd acts | Daily Mail Online*. https://www.dailymail.co.uk/news/article-4385918/Warning-House-Party-app-men-perform-lewd-acts.html

Dushi, D. (2019). *The phenomenon of online live-streaming of child sexual abuse: Challenges and legal responses*.

Dwyer, R. G., Letourneau, P., McKee, T., & Moran, R. (2016). *Protecting Children Online: Using ResearchBased Algorithms to Prioritize Law Enforcement Internet Investigations, Technical Report*. US Department of Justice.

ECPAT International. (2018a, July). *ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf*. TRENDS IN ONLINE CHILD SEXUAL ABUSE MATERIAL. https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

ECPAT International. (2018b, July 26). Online child sexual abuse material – the facts. *ECPAT International*. https://www.ecpat.org/news/online-child-sexual-abuse-material-the-facts/

Edwards, L. (2009). *Pornography, Censorship and the Internet* (SSRN Scholarly Paper ID 1435093). Social Science Research Network. https://papers.ssrn.com/abstract=1435093

Europol. (n.d.). *Child Sexual Exploitation*. Child Sexual Explotation. Retrieved November 22, 2019, from https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation

Farid, H. (2019). *House Committee on Energy and Commerce Fostering a Healthier Internet to Protect Consumers*. 5.

Farrugia, L., Lauri, M. A., Borg, J., & O'Neill, B. (2018). Have You Asked for It? An Exploratory Study About Maltese Adolescents' Use of Ask. Fm. *Journal of Adolescent Research*, 0743558418775365.

George, D. (2016, September 20). *As online 'sextortion' against children grows, feds urge back-to-school awareness—The Washington Post*. https://www.washingtonpost.com/local/education/online-sextortion-against-children-growing-feds-urge-back-to-school-awareness/2016/09/19/395a6cbe-7b5b-11e6-beac-57a4a412e93a_story.html

Hassenfeldt, C., Baig, S., Baggili, I., & Zhang, X. (2019). *Map My Murder: A Digital Forensic Study of Mobile Health and Fitness Applications*. 42.

Hobson, J. (2018, January 22). *Snapchat "Has Become A Haven" For Child Predators, Criminal Justice Scholar Says*.

Horsman, G. (2018). A forensic examination of the technical and legal challenges surrounding the investigation of child abuse on live streaming platforms: A case study on Periscope. *Journal of Information Security and Applications*, *42*, 107–117.

Hughes, D. M. (1999). Pimps and Predators on the Internet. *The Coalition Against Trafficking in Women*.

IACIS. (n.d.). IACIS. Retrieved November 3, 2019, from https://www.iacis.com/

ICAC. (n.d.). *ICAC Task Force*. Retrieved April 8, 2020, from https://www.icactaskforce.org/

ICE HSI. (2019, November 14). *ICE HSI helps remove more than 3,500 sexual predators from community, up 18% over last year*. https://www.ice.gov/news/releases/ice-hsi-helps-remove-more-3500-sexual-predators-community-18-over-last-year

Judge, S. M. (2018). *Mobile Forensics: Analysis of the Messaging Application Signal*. University of Central Oklahoma.

KNXV-TV. (2019, June 14). *Dangerous social media apps kids are using that parents need to know about*. WFTS. https://www.abcactionnews.com/news/political/national/dangerous-social-media-apps-kids-are-using-that-parents-need-to-know-about

Lenhart, A. (2015). Teens, Social Media & Technology Overview 2015 | Pew Research Center. *Pew Research Center*. https://webcache.googleusercontent.com/search?q=cache:L2gIOnR0ssQJ:https://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/+&cd=1&hl=en&ct=clnk&gl=us&client=firefox-b-1-d

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. *Pew Research Center*, *21*, 2–86.

Magnet Forensics. (2019). *Artifact Reference*. 923.

Mahajan, A., Dahiya, M., & Sanghvi, H. (2013). Forensic analysis of instant messenger applications on android devices. *ArXiv Preprint ArXiv:1304.4915*.

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle school students' social media use. *Journal of Educational Technology & Society*, *21*(1), 213–224.

Menn, J. (2019, November 17). Exclusive: Interpol plans to condemn encryption spread, citing predators, sources say. *Reuters*. https://www.reuters.com/article/us-interpol-encryption-exclusive-idUSKBN1XR0S7

Mindock, clark. (2019, October 16). *More than 300 arrested in sting of 'largest dark web child sex abuse marketplace run by bitcoin.'* The Independent. https://www.independent.co.uk/news/world/americas/child-porn-bitcoin-arrests-us-jong-woo-son-a9159146.html

Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization. *Journal of Adolescent Health*, *47*(2), 183–190. https://doi.org/10.1016/j.jadohealth.2010.01.007

MyNorthwest. (2019, November 19). *Washington operation "Net Nanny" brings in another 16 sexual predators*. MyNorthwest.Com. https://mynorthwest.com/1606339/washington-operation-net-nanny-arrests-november-2019/?

Naspretto, A. (2019, October 24). *Police warns parents about teens on social media apps*. https://www.ksnblocal4.com/content/news/Police-warns-parents-about-teens-on-social-media-apps-563827871.html

National Center for Missing & Exploited Children. (n.d.). *Online Enticement*. Retrieved October 12, 2019, from http://www.missingkids.com/theissues/onlineenticement

National Center for Missing & Exploited Children. (2017a). *The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports*. NCMEC. www.missingkids.com/content/dam/missingkids/pdfs/ncmec-analysis/Online Enticement Pre-Travel.pdf

National Center for Missing & Exploited Children. (2017b). *Trends identified in CyberTipline sextortion reports*. NCMEC. www.missingkids.com/content/dam/missingkids/pdfs/ncmec-analysis/sextortionfactsheet.pdf

National Center for Missing & Exploited Children. (2019, October 3). *End-to-End Encryption*. http://www.missingkids.org/blog/2019/post-update/end-to-end-encryption

Newport Academy. (2019, February 22). *The Most Dangerous Apps for Teens*. Newport Academy. https://www.newportacademy.com/resources/well-being/dangerous-apps-for-teens/

Newton, C. (2016, September 28). *Meerkat built a new app in secret, and almost 1 million people are using it*. The Verge. https://www.theverge.com/2016/9/28/13081014/meerkat-houseparty-video-app

NIST. (2019, May). *Mobile Device Forenisc Tool Specification, Test Assertions and Test Cases Version 3.0*. NIST.GOV. https://www.nist.gov/system/files/documents/2019/07/11/mobile_device_forensic_tool_test_spec_v_3.0.pdf

Perlroth, N. (2012, June). After Rapes Involving Children, Skout, a Flirting App, Bans Minors. *Bits Blog*. https://bits.blogs.nytimes.com/2012/06/12/after-rapes-involving-children-skout-a-flirting-app-faces-crisis/

Perlroth, N. (2019, November 19). What Is End-to-End Encryption? Another Bull's-Eye on Big Tech. *The New York Times*. https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html

Protect Young Eyes. (n.d.). The Monkey App: Information for Parents from Protect Young Eyes. *Protect Young Eyes*. Retrieved November 20, 2019, from https://protectyoungeyes.com/apps/monkey-parental-controls/

Qualtrics | Purdue University Innovative Learning. (n.d.). Retrieved November 4, 2019, from https://www.purdue.edu/innovativelearning/supporting-instruction/instructional-technology/qualtrics.aspx

Ramdass, T. (2016). *Social Networks and Internet-Facilitated Child Exploitation: A Review of Existing Material and Call for Research*.

Roberts, K. (2019, October 22). *9 Men Arrested in Undercover Child Predator Sting*. Www.Theepochtimes.Com. https://www.theepochtimes.com/9-men-arrested-in-undercover-child-predator-sting_3123665.html

Scrivens, N., & Lin, X. (2017). *Android digital forensics: Data, extraction and analysis*. 26.

Sederstorm, J. (2019, January 15). *7 Arrested In Florida After Allegedly Using Gaming App To Lure Teen Boy Into Sex Slavery*. Oxygen Official Site. https://www.oxygen.com/crime-time/agaming-app-discord-allegedly-used-to-lure-teen-boys-into-human-trafficking-florida

Seto, M., Buckman, C. B., Dwyer, R. G., & Quayle, E. (2018). *Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims*. NCMEC. www.missingkids.com/content/dam/missingkids/pdfs/ncmec-analysis/Production and Active Trading of CSAM_ExecutiveSummary.pdf

Stolberg, S. G., & Pérez-Peña, R. (2016, February 5). Wildly Popular App Kik Offers Teenagers, and Predators, Anonymity. *The New York Times*. https://www.nytimes.com/2016/02/06/us/social-media-apps-anonymous-kik-crime.html

Taylor, M., Haggerty, J., Gresty, D., Almond, P., & Berry, T. (2014). Forensic investigation of social networking applications. *Network Security*, *2014*(11), 9–16.

Valentino-DeVries, J., & Dance, G. J. X. (2019, October 2). Facebook Encryption Eyed in Fight Against Online Child Sex Abuse. *The New York Times*. https://www.nytimes.com/2019/10/02/technology/encryption-online-child-sex-abuse.html

WBAY. (2019, October 24). *Man pleads not guilty to walking 351 miles to have sex with underage girl*. https://www.wbay.com/content/news/Man-pleads-not-guilty-to-walking-351-miles-to-have-sex-with-underage-girl-563782671.html

Westlake, B. G. (2019). The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–29). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_52-1

White, B.R. & Supreme Court of the United States. (1982). *U.S. Reports: New York v. Ferber, 458 U.S. 747 (1982).* Library of Congress, Washington, D.C. 20540 USA. https://www.loc.gov/item/usrep458747/

Wurtele, S. K., & Kenny, M. C. (2016). Technology-Related Sexual Solicitation of Adolescents: A Review of Prevention Efforts. *Child Abuse Review*, *25*(5), 332–344. https://doi.org/10.1002/car.2445

APPENDIX A. SURVEY QUESTIONS

Survey

Are you 18 or older?

o Yes

o No

Skip To: End of Survey If Are you 18 or older? = No

Are you a U.S. resident?

o Yes

o No

Skip To: End of Survey If Are you a U.S. resident? = No

What role best fits your job type?

o Investigator/Detective

o Analyst/Examiner

o Academic/Researcher

o Other - (please specify) _____

What category would your work environment fit?

o Local Law Enforcement

o State Law Enforcement

o Federal Law Enforcement

o Military

o Private Investigations

o Law Firm

o Consulting Company

o Academic Organization

o Other (please specify) _____

How long have you worked in your field?

- o 1-5 years
- o 6-10 years
- o 11-20 years
- o 21+ years

What is the size of your department?

- o 1-10 employees
- o 11-50 employees
- o 51-100 employees
- o 101+ employees

Are you involved with investigations involving mobile devices, like cell phones, and/or social media?

- o Yes
- o No

Skip To: End of Survey If Are you involved with investigations involving mobile devices, like cell phones, and/or social me... = No

How many cases do you work per year that involve digital forensics of some kind?

- o None
- o 1-10
- o 11-50
- o 51-100
- o 101+ cases

How often do you come across mobile applications that are not fully supported by forensic tools?

- o In 100% of cases involving mobile devices
- o In 75% of cases involving mobile devices
- o In 50% of cases involving mobile devices

- o In 25% of cases involving mobile devices
- o Never

Have you had a case involving the Yubo application (formally known as Yellow)?

- o Yes
- o No

Display This Question:

If Have you had a case involving the Yubo application (formally known as Yellow)? = Yes

Was Yubo supported by forensic tools?

- o Yes
- o No
- o Sometimes

Have you had a case involving the Yolo application?

- o Yes
- o No

Display This Question:

If Have you had a case involving the Yolo application? = Yes

Was Yolo supported by forensic tools?

- o Yes
- o No
- o Sometimes

Have you had a case involving the HouseParty application?

- o Yes
- o No

Display This Question:

If Have you had a case involving the HouseParty application? = Yes

Was HouseParty supported by forensic tools?

- o Yes
- o No
- o Sometimes

Have you had a case involving the Monkey application?

- o Yes
- o No

Display This Question:

If Have you had a case involving the Monkey application? = Yes

Was Monkey supported by forensic tools?

- o Yes
- o No
- o Sometimes

Have you had a case involving Lipsi?

- o Yes
- o No

Display This Question:

If Have you had a case involving Lipsi? = Yes

Was Lipsi supported by forensic tools?

- o Yes
- o No
- o Sometimes

Have you had a case involving the Likee application (formally known as Like)?

- o Yes
- o No

Display This Question:

If Have you had a case involving the Likee application (formally known as Like)? = Yes

Was Likee supported by forensic tools?

o Yes

o No

What other applications have you come across that are not fully supported by forensic tools?

o List here: (Please list as many as you can)

_____

What new and emerging applications have you come across in investigations involving teens?

o Yes - List here: (Please list as many as you can, including ones previously mentioned above) _____

o No

Display This Question:

If What new and emerging applications have you come across in investigations involving teens? = Yes - List here: (Please list as many as you can, including ones previously mentioned above)

Are these new applications supported by forensic tools?

o Yes

o No

o Sometimes

Would more support for new mobile applications be beneficial to your cases?

o Yes

o No

o N/A

Display This Question:

If Would more support for new mobile applications be beneficial to your cases? = Yes

How so?

_____

APPENDIX B. IRB NARRATIVE

PURDUE UNIVERSITY

This Memo is Generated From the Purdue University Human Research Protection Program System, Cayuse.
Date: November 22, 2019
PI: MARCUS ROGERS
Department: PWL COMPUTER INFO & TECH
Re: Initial - IRB-2019-502
New and Emerging Mobile Apps Among Teens - Are Forensic Tools Keeping Up?

The Purdue University Human Research Protection Program (HRPP) has determined that the research project identified above qualifies as exempt from IRB review, under federal human subjects research regulations 45 CFR 46.104. The Category for this Exemption is listed below . Protocols exempted by the Purdue HRPP do not require regular renewal. However, The administrative check-in date is **November 22, 2022**. The IRB must be notified when this study is closed. If a study closure request has not been initiated by this date, the HRPP will request study status update for the record.

Specific notes related to your study are found below.
Decision: Exempt
Category: Category 2.(i). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording).
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects.

Findings:
Research Notes:
Any modifications to the approved study must be submitted for review through Cayuse IRB. All approval letters and study documents are located within the Study Details in Cayuse IRB.

What are your responsibilities now, as you move forward with your research?

Document Retention: The PI is responsible for keeping all regulated documents, including IRB correspondence such as this letter, approved study documents, and signed consent forms for at least three (3) years following protocol closure for audit purposes. Documents regulated by HIPAA, such as Release Authorizations, must be maintained for six (6) years.

Site Permission: If your research is conducted at locations outside of Purdue University (such as schools, hospitals, or businesses), you must obtain written permission from all sites to recruit, consent, study, or observe participants. Generally, such permission comes in the form of a letter from the school superintendent, director, or manager. You must maintain a copy of this permission with study records.

Training: All researchers collecting or analyzing data from this study must renew training in human subjects research via the CITI Program (www.citiprogram.org) every 4 years. New personnel must complete training and be added to the protocol before beginning research with human participants or their data.

Modifications: Change to any aspect of this protocol or research personnel must be approved by the IRB before implementation, except when necessary to eliminate apparent immediate hazards to subjects or others. In such situations, the IRB should still be notified immediately.

Unanticipated Problems/Adverse Events: Unanticipated problems involving risks to subjects or others, serious adverse events, and noncompliance with the approved protocol must be reported to the IRB immediately through an incident report. When in doubt, consult with the HRPP/IRB.

Monitoring: The HRPP reminds researchers that this study is subject to monitoring at any time by Purdue's HRPP staff, Institutional Review Board, Research Quality Assurance unit, or authorized external entities. Timely cooperation with monitoring procedures is an expectation of IRB approval.

Change of Institutions: If the PI leaves Purdue, the study must be closed or the PI must be replaced on the study or transferred to a new IRB. Studies without a Purdue University PI will be closed.

Other Approvals: This Purdue IRB approval covers only regulations related to human subjects research protections (e.g. 45 CFR 46). This determination does not constitute approval from any other Purdue campus departments, research sites, or outside agencies. The Principal Investigator and all researchers are required to affirm that the research meets all applicable local, state, and federal laws that may apply.

If you have questions about this determination or your responsibilities when conducting human subjects research on this project or any other, please do not hesitate to contact Purdue's HRPP at irb@purdue.edu or 765-494-5942. We are here to help!

Sincerely,

Purdue University Human Research Protection Program/ Institutional Review Board

PURDUE
UNIVERSITY

This Memo is Generated From the Purdue University Human Research Protection Program System, Cayuse IRB .

Date: April 14, 2020
PI: MARCUS ROGERS
Department: PWL COMPUTER INFO & TECH
Re: Modification - IRB-2019-502
New and Emerging Mobile Apps Among Teens - Are Forensic Tools Keeping Up?

The Purdue University Institutional Review Board has approved the modification for your study " *New and Emerging Mobile Apps Among Teens - Are Forensic Tools Keeping Up?*. " The Category for this Exemption is listed below. This study maintains a status of exempt and an administrative check-in date of November 22, 2022. The IRB must be notified when this study is closed. If a study closure request has not been initiated by this date, the HRPP will request study status update for the record.

Specific details about your modification approval appear below.
Decision: Exempt
Findings:
Research Notes:

What are your responsibilities now, as you move forward with your research?

Document Retention: The PI is responsible for keeping all regulated documents, including IRB correspondence such as this letter, approved study documents, and signed consent forms for at least three (3) years following protocol closure for audit purposes. Documents regulated by HIPAA, such as Release Authorizations, must be maintained for six (6) years.

Site Permission: If your research is conducted at locations outside of Purdue University (such as schools, hospitals, or businesses), you must obtain written permission from all sites to recruit, consent, study, or observe participants. Generally, such permission comes in the form of a letter from the school superintendent, director, or manager. You must maintain a copy of this permission with study records.

Training: All researchers collecting or analyzing data from this study must renew training in human subjects research via the CITI Program (www.citiprogram.org) every 4 years. New personnel must complete training and be added to the protocol before beginning research with human participants or their data.

Modifications: Change to any aspect of this protocol or research personnel must be approved by the IRB before implementation, except when necessary to eliminate apparent immediate hazards to subjects or others. In such situations, the IRB should still be notified immediately.

Unanticipated Problems/Adverse Events: Unanticipated problems involving risks to subjects or others, serious adverse events, and
noncompliance with the approved protocol must be reported to the IRB immediately through an incident report. When in doubt, consult with the HRPP/IRB.

Monitoring: The HRPP reminds researchers that this study is subject to monitoring at any time by Purdue's HRPP staff, Institutional Review Board, Research Quality Assurance unit, or authorized external entities. Timely cooperation with monitoring procedures is an expectation of IRB approval.

Change of Institutions: If the PI leaves Purdue, the study must be closed or the PI must be replaced on the study or transferred to a new IRB. Studies without a Purdue University PI will be closed.

Other Approvals: This Purdue IRB approval covers only regulations related to human subjects research protections (e.g. 45 CFR 46). This determination does not constitute approval from any other Purdue campus departments, research sites, or outside agencies. The Principal Investigator and all researchers are required to affirm that the research meets all applicable local/state/ federal laws and university policies that may apply.

If you have questions about this determination or your responsibilities when conducting human subjects research on this project or any other, please do not hesitate to contact Purdue's HRPP at irb@purdue.edu or 765-494-5942. We are here to help!

Sincerely,

Purdue University Human Research Protection Program/ Institutional Review Board
Login to Cayuse IRB