Survey of Mobile Device Forensics Acquisition Tools Selection

Anthony Kabala
Department of Computer Engineering

Iowa State University
Ames, U.S.A.
ajkabala@iastate.edu

***Abstract*—Mobile Device Forensics is a new field of study in digital forensics and requires different tools than those developed for digital forensics for desktop and laptop computers. Mobile devices are becoming a more relevant source of digital forensic data than desktop and laptop computers as more people than ever use them as their main form of digital interaction with their work and in their personal lives. This leads to the need for special tools to extract the data in these mobile devices while still adhering to scientifically and legally acceptable methods. One of the first tools utilized in ascertaining this data from mobile phones is performed by mobile device acquisition tools that perform level 1, 2, and 3 data extractions that include manual extraction, logical extraction, and physical extraction respectively. This research will survey the existing methods for selecting a tool for mobile device forensics acquisition and provide an additional set of parameters to add to the selection method of these tools. The previous methods utilized that will be surveyed focus on the iOS and Android operating system support by the tools as well as the tools level of extraction they support from level 1 to 3. The methods I propose include reviewing the version year of the tool reviewed with that from the surveyed work and that listed by the manufacturers of these tools currently. The operating system support is also reviewed in my methods and has the addition of the version of the operating system supported. This allows the tool to be compared with the currently available mobile devices on the market to analyze the usefulness of the tool currently for forensics investigation of mobile devices. Thorough this investigation is concluded that several of the previously reviewed tools do not meet the current market share mobile device standards and are not a good investment for law enforcement and military and intelligence groups. It is concluded that the tools manufacturers that have tools shown to work with current mobile devices is the best investment for these forensics' groups.**

I. Introduction

The burgeoning field of Mobile device forensics is a subset of digital forensics created out of the need to be able to apply scientifically and legally acceptable methods to retrieve digital evidence from mobile devices. Mobile devices encompass digital mobile phones, tablets, and now smart watches. These devices also have a significant connection to the cloud through online storage online computation of data and may house data that may not even be present on the local mobile devices. Of the top challenges faced with mobile device forensics include preserving and collecting the data stored on these mobile devices with the ever-changing hardware and software on these mobile devices. With new hardware and software coming out on an almost quarterly basis digital investigators are challenged with old techniques and procedures not working with the new technological changes. The big problem faced by forensics investigators is how to apply scientifically and legally acceptable methods to retrieve digital evidence from mobile devices. In the past a desktop or laptop computer could be used to reveal a lot of digital data about a user's actions and behaviors, and several tools were created for the acquisition and analysis of this data. However, there has been a significant shift towards everyday digital device users to manage not only a significant portion of their work using mobile devices but, also their own personal devices. Desktop and laptop computers are no longer the leading form of digital data evidence that most people interact with, mobile device data is. In the U.S. 81% of the people have a smartphone while 96% have a cellphone [1]. This has caused the problem that well-established digital methods that work on desktop and laptop computers, unfortunately don't always work on mobile devices that may perform similar functions that the desktop or laptop computers performed. This has led to a need for digital tools to be developed, that adhere to the same forensically sound methods that desktop computers do, specifically for mobile devices. This is a very large area of study and this paper will focus on surveying the selection of mobile device forensics tools for data acquisition on smart phones with a focus on those in the U.S. market for determining an appropriate tool to select. Therefore, through a survey of mobile device forensics acquisition tools of current smartphone in the U.S. we can then predict how to properly select the correct forensics tools and methods for mobile device data extraction while maintaining scientifically and legally acceptable methods that provide admissible evidence in court in the U.S.

II. Related Surveys and Background

First, we need to understand the methods needed to perform data extraction from mobile devices that are legally and scientifically acceptable. The mobile forensics process mimics that of forensics at large and includes: preservation, collection and acquisition, examination and analysis, and reporting shown in Fig. 1. [2, 3, 4].

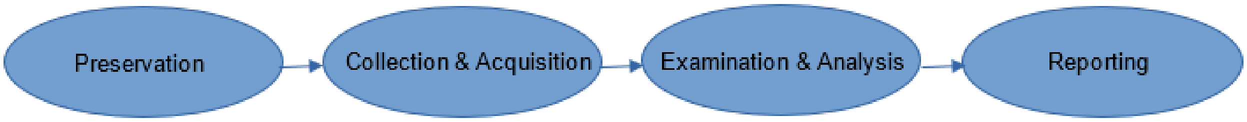


Figure 1 Mobile Forensics Process

The first procedure is preservation that ensures that no data is altered intentionally or unintentionally [3, 4] while performing the investigation of the mobile device. This means that the data on the mobile device is changed by the actions of the investigator. Unfortunately, due to the nature of different data extraction methods data may be lost while using one method over another to extract different locations of digital data. What happens is that one data extraction method may destroy or alter part of the digital data, making that altered data inadmissible, in order to acquire data that is more significant to the specific case. For example, if the phone is locked it may require loading a bootloader onto the phone so that an investigator can get access to the data on the phones hard drive. This would however alter the data that is on the phone and violate the preservation protocol. Due to the nature of digital forensics it is not always possible to not violate the preservation protocol to some degree. According to Saleem and Popov, NISTs tool analysis doesn't seem to take the different levels of value for different types of information in their tool analysis scheme [12]. Several options for determining the triage of data preservation and extraction have been documented over the years most notably in NISTs guidelines for mobile device forensics as well as others and will be evaluated for their efficacy. The next step is collection and acquisition. These steps merge to some degree with the preservation steps requirements.

There are several types of mobile device data acquisition techniques starting with manual acquisition then moving onto logical acquisition and then JTAG and Chip-off acquisition [3, 4, 11]. Physical and logical acquisition is known as post-mortem acquisition because it occurs after the devices has been powered down [4]. With the recent development of mobile devices arriving with whole drive encryption enabled by default in the operating system of newer mobile devices such as those that have the iOS 11 or later are encrypted by default [13]. Manual acquisition can be performed using the phones user interface and then taking pictures of the screen. This method is very time consuming and could cause sections of memory to be altered losing data [3]. Logical acquisition performed through the use of wired or wireless interface connections to the smartphone and a computer, commands are then sent to the smartphone to extract data.

The next set of methods extract data from the flash memory that can contain unencrypted data including passwords and keys that can help decrypt data that may be extracted through logical acquisition or provide data that can help perform logical acquisition using passwords and keys extracted from flash memory. However, the binary data extracted can be difficult to interpret directly. These methods are hex dumping, JTAG, and Chip-off. JTAG and Chip-off methods can be used to extract data from damaged or locked and encrypted devices. Hex dumping uses software tools to dump the flash memory while JTAG physically connects wires to the test access ports (TAPs) to extract binary data from the flash memory. The chip-off method is performed by cutting and grinding the memory chip off the PCB to read it and dump its binary data.

Mobile device forensics encompasses not only digital devices but also mobile cloud data storage. However, this survey will focus on the data extraction techniques for mobile devices while touching on the importance of mobile cloud data extraction as a future research topic that is a subset of mobile device forensics.

To help determine which mobile forensics technique and tools to use it is important to know what mobile device hardware and software is on the mobile smartphone being analyzed. It is not always possible to know what the exact model or hardware is on a mobile device but a close approximation can be made based off the smartphones physical design including physical features such as placement of cameras, buttons, logos, and possibly identifying numbers within a battery compartment, if it can be opened without losing valuable data from the phone [3]. If the smartphone is on it may reveal information eluding to the operating system on the device and what version of the operating system is on the device. Determining the operating system of the device may be more difficult. However, not determining the operating system could cost valuable data due to increased security protocols and altered functions between different version of the operating systems that if not taken into consideration in the acquisition phase can cause data to be lost [3]. If these other methods to determine the hardware and software versions on the phone fail the author suggests that the phones type can be approximated based off current market share percentages of phone types, models, and operating system statistics. Section III shows the survey I have put together of current market shares and I then use that data in section IV to review the selected acquisition tools available and those referenced in the previous surveys that I surveyed to select the most useful acquisition tool to have currently.

Saleem and Popov propose a slightly different approach to selecting the best tool for mobile device forensics [12]. They suggest using multi criteria decisions analysis. NISTs tool selection analysis is based off of different devices while Saleem and Popov propose to use the same device for the selection process and comparison between tool. This author also proposes a similar approach that is analyzed in section IV but is based off of the tool's current usefulness for the market share of mobile devices available. Saleem and Popov use DecideIT to perform their multi-criteria decision analysis. The criteria used to decide which is the better tool to use it based on several sets of information on a smart phone including:

PIM, messages, call logs, emails, internet history standalone files and application files.

Mobile device acquisition tools require a significant investment for law enforcement and military and intelligence groups in terms of cost for the software and hardware devices and the cost of training for personnel using the tools. I will be surveying the NISTs guidelines for mobile device acquisition ((and the other one or 2)) in addition to my own survey of the usefulness of a specific tool to best meet the current demand for forensics tool for current mobile devices in section IV to help show the proposed best tool surveyed to use currently given the significant investment and the usefulness of the tool currently.

III. Research Methods

The NISTs guidelines for mobile device acquisition ((and the other one or 2)) have several older reviews of the tools that don't necessarily encompass the current mobile devices on the market. So, I propose to use a different method to determine the mobile forensics tool to select for the current mobile device environment. Also, if the other methods to determine the hardware and software versions on the phone fail the author suggests that the phones type can be approximated based off current market share percentages of phone types, models, and operating system statistics. The average lifespan for a smartphone is now estimated at 2.75 years [5] so it can be assumed that the smartphone being examined will most likely fall within this period of available phones. Within the U.S. the current market share of smartphones is as follows: Apple 46%, Samsung 25%, LG 12%, Motorola 7%, and others 10% [6]. Further breaking down the Apple smartphone model market share it can be seen that the percentage of each iPhone is: iPhone 8 13%, iPhone 6s 13%, iPhone X 9%, iPhone XR 9%, iPhone 7 9%, iPhone 6s+ 7% and others as can be seen in Fig. 2. [7].

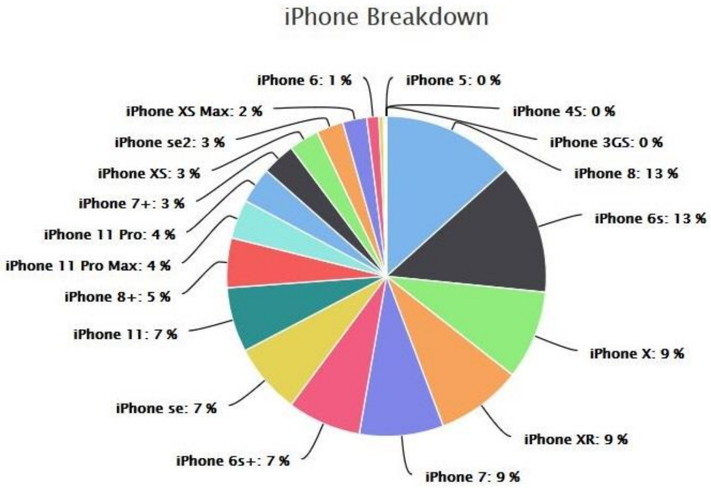
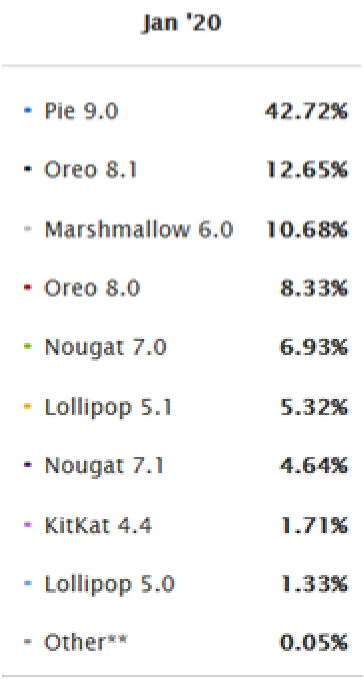


Figure 2 iPhone Model Market Share [7]

The operating system version on each iPhone can be broken down to: iOS version 14.X 8.5%, 13.X 88.7%, 12.X 2.4%, and other 0.4% [7]. The specific iOS versions market share on each iPhone can be further broken down to get an even more accurate estimate if the iPhone model is known. The Samsung smartphone model with the highest market share is within the latest Galaxy series [8]. The current market share of each operating system for smartphones is: iOS 57.33%, Android 42.29%, and Windows 0.1% [9]. iPhone is the only smartphone that has the iOS operating system so it is highly likely that any Samsung, LG, or Motorola smartphone has the Android operating system. The market share breakdown of the different versions of the Android operating system can be seen in Fig. 3. [10].

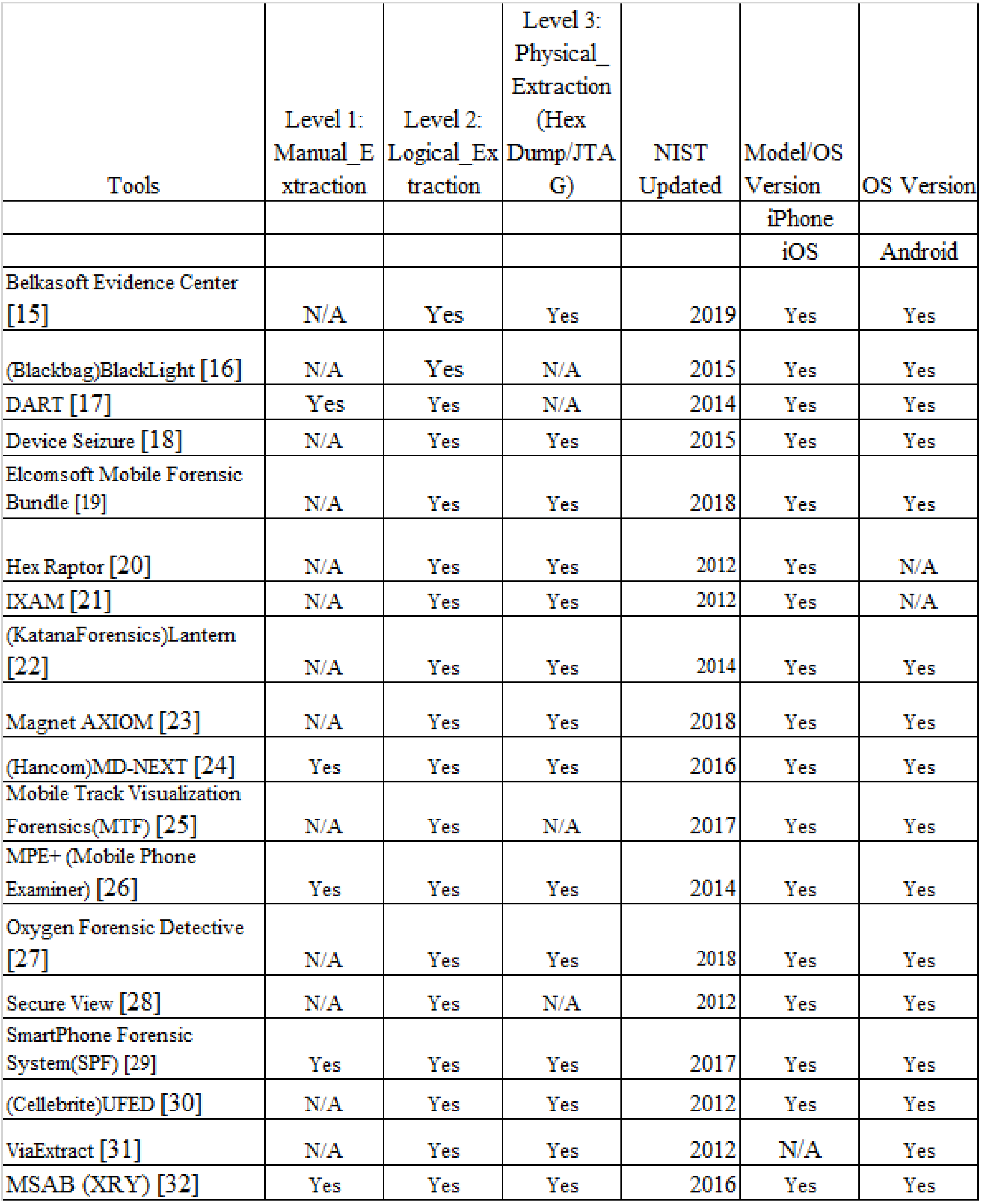


	Jan '20
• Pie 9.0	42.72%
• Oreo 8.1	12.65%
• Marshmallow 6.0	10.68%
• Oreo 8.0	8.33%
• Nougat 7.0	6.93%
• Lollipop 5.1	5.32%
• Nougat 7.1	4.64%
• KitKat 4.4	1.71%
• Lollipop 5.0	1.33%
• Other**	0.05%

Figure 3 Market Share of Android OS [10]

Because iOS is the predominant operating system available for mobile phones I believe that access to the iOS system is more important than ever. A recent vulnerability has been discovered that is called the checkm8 vulnerability that is a vulnerability in the boot-rom of iOS devices [11]. This means that an iOS device with the vulnerable boot-rom on it is susceptible to it. The boot-rom a piece of hardware on the iOS device that cannot be changed once the device is manufactured. This means that any device that has the vulnerable boot-rom is susceptible to this vulnerability and can never be updated to fix the issue. This is why I believe that this is another important parameter to check for in my review of acquisition tools.

Table I Mobile Device Forensics Acquisition Tool Review NIST



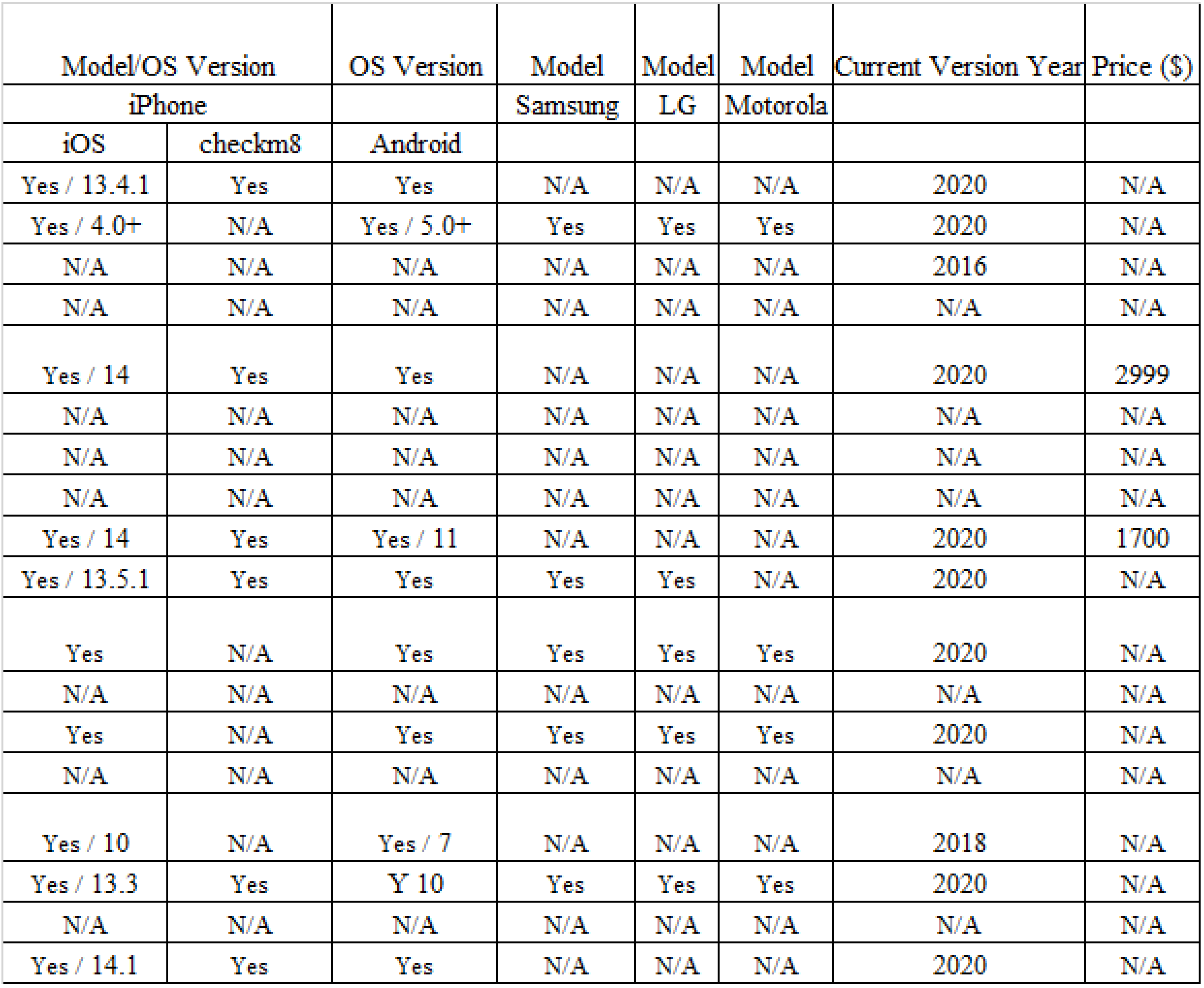
Tools	Level 1: Manual_E xtraction	Level 2: Logical_Ex traction	Level 3: Physical_ Extraction (Hex Dump/JTA G)	NIST Updated	Model/OS Version	OS Version
					iPhone	
					iOS	Android
Belkasoft Evidence Center [15]	N/A	Yes	Yes	2019	Yes	Yes
(Blackbag)BlackLight [16]	N/A	Yes	N/A	2015	Yes	Yes
DART [17]	Yes	Yes	N/A	2014	Yes	Yes
Device Seizure [18]	N/A	Yes	Yes	2015	Yes	Yes
Elcomsoft Mobile Forensic Bundle [19]	N/A	Yes	Yes	2018	Yes	Yes
Hex Raptor [20]	N/A	Yes	Yes	2012	Yes	N/A
IXAM [21]	N/A	Yes	Yes	2012	Yes	N/A
(KatanaForensics)Lantern [22]	N/A	Yes	Yes	2014	Yes	Yes
Magnet AXIOM [23]	N/A	Yes	Yes	2018	Yes	Yes
(Hancom)MD-NEXT [24]	Yes	Yes	Yes	2016	Yes	Yes
Mobile Track Visualization Forensics(MTF) [25]	N/A	Yes	N/A	2017	Yes	Yes
MPE+ (Mobile Phone Examiner) [26]	Yes	Yes	Yes	2014	Yes	Yes
Oxygen Forensic Detective [27]	N/A	Yes	Yes	2018	Yes	Yes
Secure View [28]	N/A	Yes	N/A	2012	Yes	Yes
SmartPhone Forensic System(SPF) [29]	Yes	Yes	Yes	2017	Yes	Yes
(Cellebrite)UFED [30]	N/A	Yes	Yes	2012	Yes	Yes
ViaExtract [31]	N/A	Yes	Yes	2012	N/A	Yes
MSAB (XRY) [32]	Yes	Yes	Yes	2016	Yes	Yes

IV. Review of Mobile Device Forensics Acquisition Tool Selection

Several approaches have been analyzed in section II including NISTs method of listing the different extraction levels that a tool can perform and what type of mobile phone they can be used on. In Table I. you can see that I have created a review of 18 different mobile forensics acquisition tools.

The tools are reviewed according to NISTs guidelines [14]. The different parameters that NIST uses to specify the capabilities of a tool are based on the different extraction levels that can be used during acquisition to extract data from a mobile phone. There are 3 levels that are specified: Level 1 Manual Extraction, Level 2 Logical Extraction, and Level 3 Physical Extraction which includes hex dumping and JTAG. In order to compare NISTs review of the available mobile forensics' tools with my own review of these tools is by using the latest update of the tool listed on NISTs website [14]. This way I can show how my own method of analyzing the usefulness of these acquisition tools compares and can be

Table II Mobile Device Forensics Acquisition Tool Review



Model/OS Version		OS Version	Model	Model	Model	Current Version Year	Price ($)
iPhone			Samsung	LG	Motorola		
iOS	checkm8	Android					
Yes / 13.4.1	Yes	Yes	N/A	N/A	N/A	2020	N/A
Yes / 4.0+	N/A	Yes / 5.0+	Yes	Yes	Yes	2020	N/A
N/A	N/A	N/A	N/A	N/A	N/A	2016	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Yes / 14	Yes	Yes	N/A	N/A	N/A	2020	2999
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Yes / 14	Yes	Yes / 11	N/A	N/A	N/A	2020	1700
Yes / 13.5.1	Yes	Yes	Yes	Yes	N/A	2020	N/A
Yes	N/A	Yes	Yes	Yes	Yes	2020	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Yes	N/A	Yes	Yes	Yes	Yes	2020	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Yes / 10	N/A	Yes / 7	N/A	N/A	N/A	2018	N/A
Yes / 13.3	Yes	Y 10	Yes	Yes	Yes	2020	N/A
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Yes / 14.1	Yes	Yes	N/A	N/A	N/A	2020	N/A

updated to be more current given my own approach. The next parameter that I reviewed from NISTs available tools is their usefulness with the current phones and phone operating systems that are available currently with the most market shares. NIST reviews weather or not the different tools actually support iOS or the Android Operating system on mobile phones. However, it does not show the version of the operating system that is supported. As was discussed in section II important data can be lost or inaccessible to an investigator if the tool used to acquire the data off the phone does not support the operating system on the phone. This is why I propose a review of the acquisition tools to access the usefulness of these tools to support the current operating system of the phones with the leading market shares currently on the market.

Given the age of the last review of most of these tools by NIST it is apparent that a mobile forensics investigator could end up selecting a tool to use that doesn't support the latest operating systems of the mobile phones most likely to be encountered in the field currently with several tools not having an updated review by NIST since 2012. Given the age of some of these tools it is possible that some of these tools are not even supported by the manufacturer anymore and might not even be available anymore. That is why I have also included a review of the acquisition tools current version year available in my review to analyzed the usefulness of the tool given the current demand.

I don't propose duplicating the work of NIST and others, but enhancing it with a review that updates the parameter data to account for current trends in the mobile device market and including several additional parameters to enhance the limited parameters that are available from NIST including the lack of information about the supported mobile device operating system versions. Therefore, given the datedness of a lot of the information provided by the current reviews of NISTs mobile device forensic acquisition tool selection I have created my own review of mobile device forensics acquisition tools that can be seen in Table II.

As can be seen in Table II most of the tool manufacturers do not provide details about the specific operating systems versions that their tools support and those that do provide that information provide only limited amounts of it. I attempted to contact MSAB about a more thorough description of what operating systems their XRY tools support because they suggest that that is what an interested party should do if interested in knowing more detail about their tools. Unfortunately, I have not gotten any responses yet. Also, I attempted to download several tools but were unable to due to restrictions to only distribute to law enforcement and military and intelligence groups. I chose to use the iOS and Android parameters that NIST used but I enhanced them by adding the operating system version that the tools support. This way it can be seen whether or not the tool is useful for current phones. As mentioned earlier in this section several of the tool manufacturers list support for the iOS and Android systems but they do not provide much information about the operating system versions that they support. A couple of the manufacturers did say that they listed the support operating system version in more detail with a trial copy of their tools. However, it was not possible to get a copy of the tools without being a law enforcement or militarily and intelligence group. Without this data an investment in these tools that do not show to support the current operating system versions might end up causing useful data in an investigation to be lost because it could not be accessed using the tool. The tools that do show what versions of the operating systems are available do not provide very much information about them. As can be seen in Table II only 8 out of the 18 different tools provide available information about what operating system versions they support. I also included the parameter for the availability of using the checkm8 vulnerability to access the iOS system data [11]. The checkm8 vulnerability is described in section III and is an important parameter to check for in the acquisition tools because it allows the predominate operating system, the iOS system, on the market in the U.S to be accessible to digital forensics investigators. As can be seen in Table II many of the tools do not support the use of the checkm8 vulnerability or do not provide data about its support and therefore significantly limit these tools abilities to be as useful as the other tools that do. This is because without access to this vulnerability a lot of the potential data needed for the investigation would be unavailable, and a different tool would need to be purchased and trained for. This would cause the investigation team to lose valuable time and money to work on this case and other cases. I also included the parameters: Samsung, LG, and Motorola. These parameters represent weather or not the tool supports acquisition of data off these mobile phone manufacturers. I included these phone manufacturers because they make up 44% of the current market share of mobile phones available. These phones use the android operating system so they are linked to the android operating system parameters utility of the different tools. I then reviewed the current version year available of the different tools to determine whether or not the tool was updated to support newer mobile forensics needs. In my review I found that many of the tools reviewed by NIST had not been updated for many years and 7 or the 18 listed tools I was not able to find any recent information about them or any supporting information about them on their original company website or through a search in the case that the website and owner of these tools had changed. It was found that 7 out of the 18-lack support online and I believe are no longer useful for the currently available mobile phones and devices. They may be useful on older devices that my still be in service but this author would strongly suggest not investing anymore resources in these 7 tools that don't appear to be supported anymore. The last parameter I reviewed was the price of the different tools for mobile device forensic acquisition. This was one of the most difficult pieces of information to get without specifically contacting the manufacturer for the information. As mentioned earlier I checked several of the manufacture's tools for trial versions and almost all of them required me to be a law enforcement or military and intelligence agency. This significantly limited my ability to review this aspect of these devices but could be the topic of a future analysis of these tools.

V. Conclusion and Future Analysis

There were several obstacles that were faced when researching the parameters of the different tools. The main issues were the amount of data that the manufactures shared. Not knowing the operating systems versions supported or the hardware systems supported in more detail made it difficult to give a completely accurate review of the parameters that the tools support. However, given the data that I was able to ascertain I can still conclude that several of the tools are much more useful as mobile device forensics acquisition tools on current mobile devices than others. The 7 tools that I could not find current versions information for I have to conclude are not a good investment and several are not even available to be purchased anymore as the manufacturer stopped supporting them. I have to conclude that due to the limited amount of information I was able to ascertain form the manufactures I would suffer several of the tools as the better selection for mobile device forensics acquisition with current market trends in the U.S. However, I would suggest that an investment in these suggested tools be first trial run to help further select the better tool. Future research could solve this issue or research on the practitioner procuring the tool would be in order to better utilize the resources available to the different mobile forensics' groups. The tools I suggest taking through a trial run are those that were found to have the most recent operating system versions supported. Those include: Belkasoft Evidence Center, (Blackbag)BlackLight, Elcomsoft Mobile Forensic Bundle, Magnet AXIOM, (Hancom)MD-NEXT, (Cellebrite)UFED, and MSAB (XRY). However, this is still a large number of tools to trial run so given my approach it is still possible to further select down the trial runs to include those that include the checkm8 vulnerability exploit acquisition utilization form the previous list of tools.

Due to the selective nature of who these mobile forensics acquisition tool companies are willing to share data about their tool's capabilities and supported hardware and software I propose a future analysis and review can be performed if a way can be found to convince these tool manufacturers to provide a more exhaustive list of supported devices and software for mobile phones. This would allow a review of these tools that would be more useful to mobile forensics investigators and help reduce the cost of purchasing and training personnel to use tools that may not support the needs of their clients be it law enforcement or military and intelligence.

Cloud storage and computing seems to be the future trend of information and data [4]. Current mobile devices rely heavily on cloud computing and cloud storage. So, a wealth of data is transferred from the mobile device to the cloud server and processed on the cloud server. Several mobile forensics acquisition tools claim to be able to be able to acquire data from the cloud services of mobile devices. Therefore, a future survey of the existing literature about cloud computing forensics of mobile devices is in order to address the significant amount of forensically useful data stored on the cloud about mobile device users.

Another future analysis that could be performed is to get access to trial versions of the software and therefore the data about all the supported operating systems versions and hardware devices that the tools support that many of the manufacturers explained was available in their trial tools.

References

[1] Demographics of Mobile Device Ownership and Adoption in the United States. (2020). Retrieved 21 October 2020, from https://www.pewresearch.org/internet/fact-sheet/mobile/

[2] Gary Palmer, A Road Map for Digital Forensic Research, Digital Forensic Research Workshop (DFRWS), Final Report, Aug. 2001.

[3] National Institute of Standards and Technology. (2014). *Guidelines on Mobile Device Forensics*. NIST Special Publication 800-101 Revision 1.

[4] Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes. 2018. Current and Future
Trends in Mobile Device Forensics: A Survey. *ACM Comput. Surv.* 51, 3, Article 46 (April 2018), 31 pages.
https://doi.org/10.1145/3177847

[5] Smartphone trends affecting the product lifecycle | Commerce Blog. (2020). Retrieved 21 October 2020, from https://www.ingrammicroservices.com/blog/mobile-device-smartphone-lifecycle/

[6] US Smartphone Market Share: By Quarter: Counterpoint. (2020). Retrieved 21 October 2020, from https://www.counterpointresearch.com/us-market-smartphone-share/

[7] iOS Version Statistics. (2020). Retrieved 21 October 2020, from https://david-smith.org/iosversionstats/

[8] All Samsung phones by popularity. (2020). Retrieved 21 October 2020, from https://www.gsmarena.com/samsung-phones-f-9-0-r1-p1.php

[9] *2019 Most Popular Mobile Phones in the United States. (2020). Retrieved 21 October 2020, from https://discoverbigfish.com/blog/2019-popular-mobile-phones-united-states.html*

[10] Mobile Android version share worldwide 2018-2020 | Statista. (2020). Retrieved 21 October 2020, from https://www.statista.com/statistics/921152/mobile-android-version-share-worldwide/

[11] iCloud Activation Lock Screen Bypass | CheckM8. 2020. *Checkm8 | Activation Lock Bypass Software*. [online] Available at: <https://checkm8.info/> [Accessed 23 October 2020].

[12] Saleem, S., & Popov, O. (2013). Formal approach for the selection of a right tool for Mobile device forensics. In *5th International Conference on Digital Forensics & Cyber Crime*.

[13] The Art of iPhone Acquisition. (2020). Retrieved 23 October 2020, from https://blog.elcomsoft.com/2019/07/the-art-of-iphone-acquisition/

[14] Computer Forensics Tools & Techniques Catalog - Tool Search. (2020). Retrieved 1 November 2020, from https://toolcatalog.nist.gov/search/index.php?ff_id=5

[15] Belkasoft: Evidence Search and Analysis Software for Digital Forensic Investigations and Incident Response. (2020). Retrieved 1 November 2020, from https://belkasoft.com/

[16] Home. (2020). Retrieved 1 November 2020, from https://www.blackbagtech.com/

[17] High Tech Crime Institute Inc. 2020. *High Tech Crime Institute Inc*. [online] Available at: <https://www.gohtci.com/> [Accessed 1 November 2020].

[18] Paraben Corporation. 2020. *Advanced Cell Phone Forensics Software - Mobile Forensics By Paraben*. [online] Available at: <https://paraben.com/paraben-for-mobile-forensics/> [Accessed 1 November 2020].

[19] Co.Ltd., E., 2020. *Elcomsoft Mobile Forensic Bundle | Elcomsoft Co.Ltd.*. [online] Elcomsoft.com. Available at: <https://www.elcomsoft.com/emfb.html> [Accessed 1 November 2020].

[20] Hex Raptor [OFFLINE] Available at: < http://www.forensicts.com/> [Accessed 1 November 2020].

[21] iXAM [OFFLINE] Available at: < http://www.ixam-forensics.com/> [Accessed 1 November 2020].

[22] Katana Forensics [OFFLINE] Available at: < http://katanaforensics.com/> [Accessed 1 November 2020].

[23] Magnet Forensics. 2020. *Magnet AXIOM - Digital Investigation Platform | Magnet Forensics*. [online] Available at: <https://www.magnetforensics.com/products/magnet-axiom/> [Accessed 1 November 2020].

[24] Hancomgmd.com. 2020. [online] Available at: <http://www.hancomgmd.com/wp-content/uploads/2020/08/Releasenote_2Q_2020_final.pdf> [Accessed 1 November 2020].

[25] Salvationdata.com. 2020. *Mobile Track Visualization Forensics - Best Cellphone Forensics Software*. [online] Available at: <http://www.salvationdata.com/mtf-mobile-track-visualization-forensics.html> [Accessed 1 November 2020].

[26] AccessData. 2020. *Mobile Phone Examiner Plus (MPE+) 5.8.0*. [online] Available at: <https://accessdata.com/product-download/mpe-5-8-0> [Accessed 1 November 2020]

[27] Oxygen-forensic.com. 2020. *Oxygen Forensics - Mobile Forensic Solutions: Software And Hardware*. [online] Available at: <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective> [Accessed 1 November 2020].

[28] Secureview.us. 2020. *Mobile Forensic Technology - Secure View*. [online] Available at: <https://www.secureview.us/secure_view.html> [Accessed 1 November 2020].

[29] Salvationdata.com. 2020. *Smartphone Forensic System - Cell Phone Forensics Tools*. [online] Available at: <http://www.salvationdata.com/spf-smartphone-forensic-system.html> [Accessed 1 November 2020].

[30] Cellebrite. 2020. *Cellebrite UFED | Access And Extract Mobile Device Data*. [online] Available at: <https://www.cellebrite.com/en/ufed/> [Accessed 1 November 2020].

[31] *The Mobile App Security Company | Nowsecure*. [online] Nowsecure.com. Available at: <https://www.nowsecure.com/> [Accessed 1 November 2020].

[32] Eklund, P., 2020. *XRY Logical – MSAB*. [online] MSAB. Available at: <https://www.msab.com/products/xry/xry-logical/> [Accessed 1 November 2020].