

INVESTIGATION OF RESIDUAL DATA ON SECOND HAND SMART PHONES

Sirapat Boonkrong^{1,*} and Tongpool Heeptaisong²

Received: March 17, 2021; Revised: September 27, 2021; Accepted: September 27, 2021

Abstract

Due to rapid changes in technology, many new models of smart phones are introduced to the market every year. This has led to people changing their smart phones more frequently, which means more smart phones have become available in the second hand market for those who would like to own them at lower prices. The research was begun with a question of whether or not there would be any data belonging to the previous users remained on the phones, and if so, how much of it would still be accessible. In order to answer the questions, thirty second hand smart phones with different versions of both iOS and Android operating systems were bought from the second hand market in Thailand. The main aim of this research was to determine the types of data, if any, that still remained on the obtained second hand smart phones. The experiment showed that approximately 63 per cent of the second hand smart phones investigated in this research still contained data that were both confidential and recoverable. The awareness of this security issue is hoped to be raised as a result.

Keywords: Data forensics, Data privacy, Data recovery, Remnant data, Residual data, Smart phones

Introduction

At One of the primary goals of information security is to prevent unauthorised access to information, which means that personal information should remain undisclosed. There are many ways to ensure data privacy, and many have considered the CIA triad as the fundamental security characteristics. The CIA triad includes confidentiality (the C), integrity (the I) and availability (the A), with confidentiality being the focus of this article.

Confidentiality is when data or information are kept as a secret and are only accessible to authorised entities. The mechanisms that have been

frequently applied to accomplish the goal are cryptography and access control. Access control is concerned with allowing authorised users to gain an access to the data or information. Cryptography is, on the other hands, a means for encoding the data so that it cannot be read by unauthorised parties. The lack of any of these mechanisms is one of the main causes of unauthorised data leakage.

With today's technology, apart from personal computers (PC) and laptops, smart phones have become increasingly more popular and used. This is because of their small portable sizes as well as their

¹ School of Information Technology and DIGITECH, Suranaree University of Technology, Nakhon Ratchasima, Thailand. E-mail: sirapat@g.sut.ac.th

² Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok, Bangkok, Thailand. E-mail: tongpool.h@itd.kmutnb.ac.th

* Corresponding author

computational ability which is on a similar level as an ordinary computer. Statistics suggest that the number of smart phone users has exceeded three billion worldwide. The number is also forecast to grow by several hundred million in the next few years (Statista, 2019a), as shown in Figure 1.

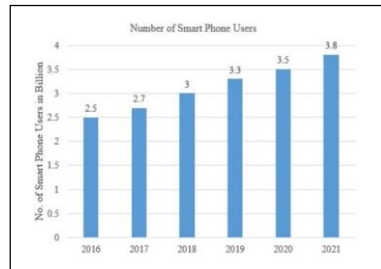


Figure 1. Number of Smart Phone Users

The smart phone's capabilities for easy communication and collaboration together with the 4G technology, and 5G technology in the near future, are not the only factors that contribute to the increasing number of smart phone users. Another motive for owning a smart phone is the price. The trend of the smart phone prices appear to go in the opposite direction to the amount of smart phone usage. In other words, the average selling prices of smart phone have been continually dropping since the year 2012. In more detail, the average selling prices of smart phones was approximately 276.20 US dollars in 2012. However, in 2019, the average prices decreased to approximately 214.70 US dollars (Statista, 2019b). This decreasing trend of the smart phone prices is illustrated in Figure 2.

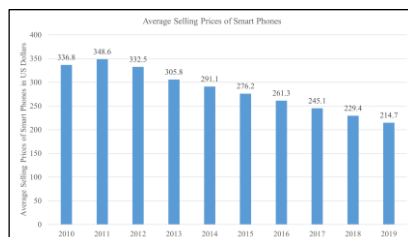


Figure 2. Average Selling Prices of Smart Phones

From the reasons stated above in addition to the rapid changes of today's technology, there are people who change their smart phones frequently. Some have chosen to sell the old ones to smart phone shops. Some have chosen to sell them directly to new owners. This has created a new market for those who want to own a smart phone at a lower price. The market is known as the second hand smart phone market.

A second hand smart phone can be defined as a smart phone that has been pre-owned and used prior to being sold to a new owner. This has raised a couple of important questions. Has the data of the previous owner been completely erased before selling the phone to a new owner? Can the new owner recover any data on the second hand smart phone he or she has acquired?

There have been several researches that studied the disposal of ordinary computer hard disks (Garfinkle and Shelat, 2003) and memory cards (Jones *et al.*, 2019). However, the two mentioned questions related to smart phones have not been directly answered by any existing researches. It is, therefore, necessary to carry out the research which will provide awareness of whether or not it is safe to sell a personal or a company smart phone to the second hand market without thinking about it carefully.

The contributions of this paper are in two folds. First, different types of smart phones based on operating systems were studied to determine whether or not the data could be recovered. Second, we attempted to recover the data from the available smart phones. Where possible, an analysis was carried out in order to understand more of what we were able to recover.

Background knowledge and related work

This section describes basic knowledge and the work related to our work. We begin with the description of basic architecture of smart phones and how data are stored. Several methods that can be used to recover data are then explained.

Smart phones and their architecture

A smart phone (Nusca, 2009) can be defined as a device or a mobile phone that has its own operating system and has the capabilities similar to those of a personal computer, but is smaller and easily portable. A smart phone contains the capabilities of voice communication of a telephone, note taking and appointment making of a PDA (personal digital assistant), still image and video recording of a camera as well as the ability to use the Internet of a personal computer. A smart phone also consists of a touch screen for ease of use.

The smart phone market has over the years increased in size mainly due to better communication capability, especially with the 4G technology and the upcoming 5G. The competition in the market has also been fierce among different operating systems including iOS and Android of Apple and Google, respectively (Reisinger, 2012). This is the reason why these two smart phone operating systems are the focus of this paper.

Figure 3 shows a typical architecture of a smart phone. It can be seen that a smart phone usually consists of (Arora, 2012): (1) a baseband processor (BP) which is responsible for radio signal communication; (2) an application processor (AP) whose main function is to deal with managing user interfaces of smart phone applications; (3) Flash which in turn contains a mobile control unit (MCU) for running smart phone software, post programmable memory (PMM) for ensuring the correct display of languages, and content (CNT) for storing images and sounds of the factoring settings; (4) EPROM which assists in processing and computation of different parts of a smart phone such as battery, camera, sensors and radio transmission; and (5) data flash which acts as the main storage for storing data such as images, videos and other types. This means that the data flash is considered the important component for our research in trying to recover the data from it.

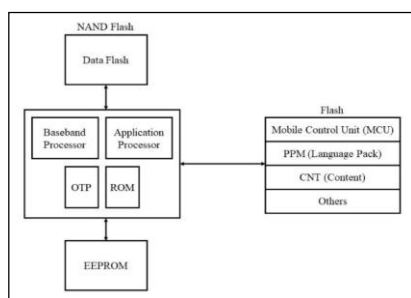


Figure 3. A Typical Smart Phone Architecture

Data flash makes use of flash memory, which is small in size and non-volatile. The type of flash memory that is typically used in smart phones is known as the NAND Flash.

There are two types of file systems used in the flash memory. The first is FAT-16. The second is FAT-32 (Lim and Park, 2006; Dowler, 2011). The FAT-16 file system is the same as the file system used on a floppy disk. That means if the FAT-16 is used in the flash memory, the smart phone will see it as a large floppy disk. The FAT-32 file system, which is what today's hard disks use. That means for the reading and writing data on the flash memory the FAT-16 is a more convenient choice. However, the FAT-32 file system is also used, but with additional components of the master boot record (MBR), boot sector (BS) and file allocation table (FAT). The file allocation table is of our interest in this study because it keeps the list of files, their sizes and location on the flash memory. This implies that when a file is modified or deleted from the flash memory, the information will be updated in the file allocation table. Even though

the FAT-32 appears to be more complex than the FAT-16, it is the file system that is more commonly used on smart phones today.

Data recovery from smart phones

This paper's main aim is to attempt to recover data from second hand smart phones. It is, therefore, necessary to understand the theory and principle behind the action of recovering data from flash memory.

There are two main methods for reading and recovering data from flash memory. They are physical acquisition and logical acquisition (Krishnan *et al.*, 2019). The first method, physical acquisition, is when data are extracted in the form of binary from flash memory of a smart phone. The binary data are then used to (re)construct a file or files. One way to achieve this is to carry out what is known as forensic de-soldering, which requires direct access to the chip and circuit board of the smart phone (Breeuwsma *et al.*, 2007). This is an invasive way, which creates a risk of damaging the smart phone. A less risky method is to connect the smart phone via the JTAG port before extracting the binary information. Unfortunately, only a few smart phones have this port available (Klaver, 2010).

Due to the difficulty of the physical acquisition, Klaver (2010) proposed a method called pseudo physical acquisition which requires that a piece of software is to be installed on a smart phone in order to connect with the operating system during the booting period. However, the problem with this method is that the software used for this purpose needs to be evaluated and approved by National Institute of Standards and Technology's Forensic Tool Testing Project.

A more convenient method for recovering data from smart phones is the logical acquisition method, which allows for direct interaction with the smart phone so that data that are or used to be stored on it can be acquired. Examples of software that applies this method include XRY Logical, Universal Forensics Extraction Device and Mobile Internal Acquisition Tool (MIAT) (Dellutri *et al.*, 2008). Our research made use of another type of software which needed to be installed on a computer in order to connect to smart phones. The software used in this research included Recuva, Puran File Recovery and Pandora Recovery.

Related work

It has been stated in previous sections that newer smart phones models with better capabilities have been continually produced, which has caused more people to purchase new phones all the time. In turn, this has also created a second hand smart phone

market for those who would like to own a smart phone at a lower price.

Before selling their smart phone to the second hand market, the job of the owners is to sanitise their phone to ensure that no private data are left on the flash memory. The problem is that disk sanitisation does not completely help with the issue of data privacy (Gallagher, 1991). In other words, it has been stated that there is still no way the owners can be certain that their data have been entirely erased. However, our research does not look into how to improve data deletion methods as many studies already exist (Skorobogatov, 2005; Lee *et al.*, 2011; Reardon, 2013). Instead, the focus of this research is on what can really be recovered from second hand smart phones.

Data recovery is considered as the counter process of data erasure. There are three major events that cause a data recovery process. The first is when there are damages to the operating system. The second event is when there are damages to the storage unit such as hard disk and flash memory. The third is when data have been “erased” from the storage unit. This research attempts to carry out data recovery from the third event. In other words, in the event that previous owners of smart phones had “erased” their data prior to selling them.

Previous studies (Gutmann, 1996; Amari, 2009) explain that when data are “erased” from the storage unit, they are not really “erased” or totally removed from it. Only the indexes or references that points to the data are removed, but the actual data or at least parts of them still remain. Moreover, even though the data remain in the storage unit, their area of storage can be overwritten with new data, because they are deemed as “erased”. However, it is still possible to recover the “erased” data or fragments of them. This is why it has interested us in trying to study whether anything can be recovered from the second hand smart phones, even after the previous owners have deleted their data or reset their phone.

Methodology

The aim of this research is to attempt to recover data on the second hand smart phones that were available to us. This section, therefore, explains in detail how the experiments were carried out.

As allowed by the research budget and in order not to alert sellers of one party purchasing a large number of second hand smart phones, the research began with the acquisition of thirty smart phones from the second hand markets in Thailand in 2019. The second hand smart phones were purchased from several sources including physical smart phone shops and online smart phone shops. As is the case

with second hand equipment, the smart phones varied in manufacturers, models and condition. However, the experiment was designed in such a way that fifteen iOS devices and fifteen Android devices were to be acquired. The iOS and Android operating systems were the focus of this study because, as of June 2020, the market shares of Android and iOS mobile operating systems were 74.6% and 24.82%, respectively (Statcounter, 2020). Due to the fact that we were only interested in what could be recovered from each smart phone, the variation of smart phone brands, models as well as the versions of the operating systems was not of the main concern.

Smart phone specification

Upon the acquisition of the thirty second hand smart phones, each phone's characteristics and specification, including manufacturer, model, CPU, RAM, size of the storage unit and detail of the operating system were recorded. In more detail, Table 1 shows the number of smart phones with different versions of operating systems that were used in the experiment Table 1. also illustrates that the types and versions of the smart phone operating systems varied from the older version in iOS 4.0 and Android 4.2.1 to the near latest version at the time of this investigation in iOS8.1 and Android 6.1.

Table 1. Smart Phones and Their Operating Systems

Operating System	Number of Smart Phones	Total Storage Capacity
iOS 4.0	3	424 GB
iOS 6.1.3	3	
iOS 6.1.4	3	
iOS 7.0	2	
iOS 8.0	2	
iOS 8.1	2	
Android 4.2.1 (Jelly Bean)	1	152 GB
Android 4.2.2 (Jelly Bean)	2	
Android 4.4 (Jelly Bean)	1	
Android 5.0 (Lollipop)	1	
Android 5.1 (Lollipop)	6	
Android 5.1.1 (Lollipop)	3	
Android 6.1 (Marshmallow)	1	

Data recovery

The next step was to install open source data recovery software on our laptop computer, whose specification is shown in Table 2.

It can be seen that this research took a different method and technique used in previous studies undertaken on hard disks (Garfinkle and Shelat,

2003) and memory cards (Szewczyk and Sansuroah, 2010; Robins *et al.*, 2016; Jones *et al.*, 2019). The previous studies appeared to have gone into using digital forensic techniques for recovering data on either hard disks or memory cards, which we believe would not really reflect the ability of ordinary or home users. That means the reason that open source software was used because we would like to show that even if a normal user purchased a second hand smart phone, it would still be possible for him or her to try to recover the data by using easy-to-find open source software, i.e., not having to spend any money on any special tools or pieces of proprietary data recovery software. The open source data recovery software used in our experiment were Puran File Recovery, Pandora Recovery and Recuva, all of which were straight forward to install. Furthermore, more than one piece of software was used in the experiment due to their different capabilities, and because we would like to ensure that the data recovery process was as complete as possible.

Table 2. Specification of Laptop Used in the Experiment

Manufacturer and Model	Asus ZenBook UX303LB
Processor	Intel Core i7 5500U Processor
Memory	DDR3L 1600 MHz SDRAM, On Board Memory of 4GB
Hard Disk	500 GB HDD 5400/7200 RPM
Operating System	Windows 10 Pro

The steps that were carried out are as follows. Firstly, a smart phone was connected to the laptop, one at a time, via a cable. Secondly, after the smart phone had been detected by the computer, Puran File Recovery, Pandora Recovery and Recuva were started, one at a time, so that the scanning and data recovery processes could begin.

Once the data recovery process was done, an analysis was carried out. The recovered data were analysed in two dimensions. First, we looked at the amount and types of data that were recovered. Second, the analysis was done more deeply by examining the relationship between the operating systems and the recovered data. In other words, by looking at the relationship, we should be able to see which type and version of the operating system was more tolerant to the recovery of data. In addition, as a by-product, we hoped that the obtained data would also tell us about the typical behaviours of smart phone users.

Results and Discussion

Prior to the experiment, the research plan was informally informed to variety of people. It was interesting to receive different responses. For example, some people were certain that files would be recovered and we would see many private data, such as images and videos. Some were also sure that we would find many files, but unsure whether they would be meaningful or even legible. Some suggested that no data would be recovered at all because they believed that previous owners would have already been very careful when making their used smart phone available on the market. Therefore, this section describes and explains what was found as a result of the data recovery experiment on second hand smart phones.

Amount of Recovered Data

An attempt to recover data on the thirty second hand smart phones, fifteen with iOS operating systems and fifteen with Android, was carried out. The initial findings show that a total of 2.2 GB of data was recovered, consisting of 514 MB from the iOS devices and 1.7 GB from the Android devices. The results are summarised in Table 3.

Table 3. Amount of Recovered Data from Different Devices

Device Type	Amount of Recovered Data
iOS Devices	514 MB
Android Devices	1.7 GB

Types of Recovered Data

The results of this initial study indicate that there were no pattern or consistency to what led to data to be recoverable. In more detail, out of the fifteen devices and six versions of iOS operating system, we were able to obtain data from only five devices and two versions of the operating system. Moreover, it was observed that even if some of the devices were the same model with the same version of the operating system, we were able to recover data from one device but not the other. This is shown in Table 4.

Table 4 also informs us that data were recoverable on the older versions of the iOS operating system. In other words, we were only be able to obtain data from the devices with the iOS versions 4.0 and 6.1.3. The newer versions, including iOS 6.1.4, iOS 7.0, iOS 8.0 and iOS 8.1, appeared to be more tolerant to the data recovery

Table 4. Recovered Data on iOS Devices

Device Number	Operating System	Types of Recovered Data					
		Image	Video	Sound	Text	Contact	Browser History
1	iOS 4.0	✓	✓	-	✓	✓	✓
2	iOS 4.0	✓	-	-	✓	-	✓
3	iOS 4.0	✓	-	-	✓	-	✓
4	iOS 6.1.3	-	-	-	-	-	-
5	iOS 6.1.3	✓	✓	-	✓	✓	✓
6	iOS 6.1.3	✓	✓	-	✓	✓	✓
7	iOS 6.1.4	-	-	-	-	-	-
8	iOS 6.1.4	-	-	-	-	-	-
9	iOS 6.1.4	-	-	-	-	-	-
10	iOS 7.0	-	-	-	-	-	-
11	iOS 7.0	-	-	-	-	-	-
12	iOS 8.0	-	-	-	-	-	-
13	iOS 8.0	-	-	-	-	-	-
14	iOS 8.1	-	-	-	-	-	-
15	iOS 8.1	-	-	-	-	-	-

Table 5. Recovered Data on Android Devices

Device Number	Operating System	Types of Recovered Data					
		Image	Video	Sound	Text	Contact	Browser History
1	Android 4.2.1 (Jelly Bean)	✓	-	-	✓	-	-
2	Android 4.2.2 (Jelly Bean)	✓	✓	✓	✓	-	-
3	Android 4.2.2 (Jelly Bean)	✓	✓	✓	✓	-	-
4	Android 4.4 (Jelly Bean)	✓	✓	✓	✓	-	-
5	Android 5.0 (Lollipop)	✓	✓	✓	-	✓	-
6	Android 5.1 (Lollipop)	✓	✓	✓	✓	✓	-
7	Android 5.1 (Lollipop)	✓	-	-	-	✓	-
8	Android 5.1 (Lollipop)	✓	-	-	✓	✓	-
9	Android 5.1 (Lollipop)	✓	✓	✓	✓	✓	-
10	Android 5.1 (Lollipop)	✓	-	-	-	✓	-
11	Android 5.1 (Lollipop)	✓	-	-	✓	✓	-
12	Android 5.1.1 (Lollipop)	✓	✓	✓	✓	✓	-
13	Android 5.1.1 (Lollipop)	✓	✓	✓	✓	✓	-
14	Android 5.1.1 (Lollipop)	✓	✓	✓	✓	✓	-
15	Android 6.1 (Marshmallow)	-	-	-	-	-	-

process by the open source software used in this research. Moreover, no sound files were recoverable at all, not even on the older versions of the iOS operating system.

For the Android devices, of the fifteen machines and seven versions of Android, we were able to recover data from fourteen devices and six versions of Android. What we recovered on which device are illustrated in Table 5.

Similar to the iOS devices, there does not appear to be any standard in the Android operating system on what can be or cannot be recovered. This is supported by the information in Table 5. that although the version of the operating system is the same on different devices, the recovered data were different. This claim is clearly illustrated on the Android 5.1 (Lollipop) devices. We were able to obtain more data types on some of these devices than the others of the same version of Android.

Another thing that can be observed from Table 5 is that on the Android 6.1 (Marshmallow),

which was the newest out of all the devices we purchased, no data were recoverable at all. This is consistent with the iOS operating system in that the newer the operating system, the more tolerant to data recovery it appeared to be. In addition, interestingly we could not recover any browsing history from any of the fifteen Android devices at all.

Analysis on Recovered Data

Once the data had been recovered from the second hand smart phones, a brief analysis was carried out in order to determine what had actually been left on those devices. Table 6 summarises these results.

Table 6 reveals that approximately 2.2 GB of data were recovered from the thirty second hand smart phones, with 1,163 files being images, 45 files being videos and the rest were text and other types of data. For the text data type, this included SMS messages, textual notes, calendar, reminders,

contact information, call history and browsing history. We were also able to recover a lot of files that could not be opened on our computer used in the experiment.

Table 6. Types and Sizes of Recovered Data

Data Type	Number of Recovered Files	Total Size of Recovered Data
Image	1,163	564 MB
Video	45	769 MB
Text	N/A	5 MB
Others	N/A	862 MB

It appeared that the images that were recovered from the second hand smart phones were mostly photographs of landscape, portrait, pets, tourist attractions and food. The photographs included some private properties such as a car, an office and a house, in some cases. Most of the video files were ones recorded on the smart phones themselves and containing videos of parties, concerts and trips.

For the text portion of the recovered data, we were able to obtain variety of file types. They included call history from which we were able to gather such information as the called phone numbers and the duration of the calls, the previous owner's bookmarked URLs, and SMS messages which were largely from mobile phone operators, social media and financial institutions. Many of the SMS messages caught our attention because they contained such confidential information as a PIN code for a chat application, an OTP (one-time password) for a banking application and an Apple ID confirmation code.

Furthermore, the names of the Web sites visited by the previous owners were also recovered with examples being social networking sites, film or movie Web sites, sports Web sites, second hand car Web sites and search history. In addition, on some of the smart phones, we were able to read calendar appointments which consisted of meetings and holidays.

In contrast to many claims and beliefs, very small amount of adult-rated content was found in this study. It is believed that this is due to the fact that smart phone users, especially the ones that had owned the thirty second hand devices, had become more aware of the privacy issues and their consequences.

On the whole, this investigation provided similar items to what was found on the second hand memory cards in the UK study (Jones *et al.*, 2019), which also found personal or selfie photographs, landscape images as well as some text information. However, our research on the second hand smart phone presented some additional information such as calendar appointments, SMS messages and

browsing history, which could provide a view, albeit not thorough, of what the previous owners were like.

Admittedly, the number and size of data that were recovered was far smaller than what we had anticipated to find on actively used smart phones. We believe that this is because the smart phones' previous owners (or even the second hand smart phone shops) had intentionally deleted their data in an attempt to at least ensure that the smart phone was as clean as possible before selling them to the new owners. Even though and even if that were the case, a handful of files were still recoverable.

Conclusions

This research was carried out with an aim of attempting to recover data from second hand smart phones, whose market has increasingly become larger, due to the need to own a smart phone at a lower price. In this study, thirty second hand smart phones of different models were purchased from various sources. Fifteen were iOS devices, while the other fifteen were Android devices. Although the number of devices appears small, we would like to think that a few conclusions can still be drawn from the study.

First, it is possible to remove at least some confidential and personal information from smart phones' storage units before dispatching them to the second hand market. This can be seen from a small amount of files that were recovered in relation to the total size of the smart phones' storage. We believe that the previous owners had at least put an effort in making sure that as many data as possible were deleted prior to selling their smart phones.

Second, even though erasing data from smart phones was not a complicated procedure and many had opted to do so, a lot of private and sensitive information still remained on the smart phones and was recoverable. The information recovered in our research included private images, SMS messages, personal contacts, call history and browsing history amongst others. This implies that the second hand smart phone market is filled with information that is private, sensitive and confidential.

Based on the findings, we would like to recommend that users are educated about the process for properly erasing data from a smart phone so that the risk of the leakage of personal data can be reduced. Another technique that has not been widely adopted is encryption. Smart phone vendors should provide a simple tool and encourage users to encrypt their data or to adopt a more secure access control mechanism on their smart phone.

It is obvious that our study only looked at thirty devices. Although with this small number of second

hand smart phones and with relatively little finance, we were still able to retrieve personal information from the smart phones deemed unwanted by the previous owners. At the moment, there also seems to be a lack of reports about this problem. We hope that this study will at least create an awareness (Kim *et al.*, 2015) to people who often change and sell their smart phones. In addition, if the deletion process is not improved nor done properly before smart phones are put in the second hand market, we think it is a matter of time before confidential and private information is exposed, which in turn will cause harms to the previous owner of the smart phone.

Acknowledgement

This research was supported and funded by Thailand's national research budget in the year 2016 (KMUTNB-GOV-59-51). The authors would like to thank Suranaree University of Technology and King Mongkut's University of Technology North Bangkok for providing equipment necessary to complete the study.

References

- Amari, K. (2009). Techniques and Tools for Recovering and Analyzing Data from Volatile Memory. SANS Institute.
- Arora, M. (2012). Deciphering Phone and Embedded Security. EE Times, Available from: <http://www.embedded.com/print/4389844>. Accessed date: August 8, 2016.
- Breeuwsma, M., de Jongh, M., Klaver, C., van der Knijff, R., and Roeloffs, M. (2007). Forensic data recovery from flash memory. Small Scale Digital Device Forensics J., 1(1).
- Dellutri, F., Ottaviani, V., and Me, G. (2008). MIAT-WM5: forensic acquisition for windows mobile pocketpc. In W. W. Smari (Ed.), Proceedings of the workshop on security and high performance computing systems, part of the 2008 international conference on high performance computing and simulation: HPSC. Cyprus.
- Dowler, M. (2011). Flash Memory Data Recovery and Protection. PCStats., Available from: <http://www.pcstats.com/articleview.cfm?articleID=1869>. Accessed date: August 10, 2016.
- Gallagher, P.R. (1991). A guide to understanding data remanence in automated information systems. National Computer Security Center. p 339-353.
- Garfinkle, S.L. and Shelat, A. (2003). Remembrance of data passed: a study of disk sanitization. IEEE Security and Privacy, 1(1):17-27.
- Gutmann, P. (1996). Secure deletion of data from magnetic and solid-state memory. In: Proceedings of the Sixth USENIX Security Symposium. San Jose. p 131-134.
- Jones, A., Angelopoulou, O., and Noriega, L. (2019). Survey of data remaining on second hand memory cards in the UK. Computers & Security, 84:239-243.
- Kim, Y., Oh, T., and Kim, J. (2015). Analyzing User Awareness of Privacy Data Leak in Mobile Applications. Mobile Information Systems, 2015.
- Klaver, C. (2010). Windows mobile advanced forensics. Digital Investigation, 6(3-4):147-167.
- Krishnan, S., Zhou, B., and An, M. K. (2019). Smartphone Forensic Challenges. Int. J. of Computer Science and Security, 13(5):183-200.
- Lee, B., Son, K., Won, D., and Kim, S. (2011). Secure Data Deletion for USB Flash Memory. J. Inf. Sci. Eng., 27(3):933-952.
- Lim, S.H. and Park, K.H. (2006). An efficient NAND flash file system for flash memory storage. IEEE Transactions on Computers, 55(7):906-912.
- Nusca, A. (2009). Smartphone vs. feature phone arms race heats up; which did you buy? USA: ZDNet. Available from: <http://www.zdnet.com/article/smartphone-vs-feature-phone-arms-race-heats-up-which-did-you-buy/>. Accessed date: August 8, 2016.
- Reardon, J., Basin, D., and Capkun, S. (2013). Sok: Secure data deletion. IEEE Symposium on Security and Privacy (SP), 301-315.
- Reisinger, D. (2012). Worldwide smartphone user base hits 1 billion. CNet. Available from: <http://www.cnet.com/news/worldwide-smartphone-user-base-hits-1-billion/>. Accessed date: August 8, 2016.
- Robins, N., Williams, P.A., and Sansurooah, K. (2016). I Know What You Did Last Summer... an Investigation into Remnant Data on USB Storage Devices Sold in Australia in 2015. Proceedings of the Australasian Computer Science Week Multiconference. New York, USA: ACM.
- Skorobogatov, S. (2005). Data remanence in flash memory devices. Cryptographic Hardware and Embedded Systems-CHES 2005, p. 339-353.
- Statcounter. (2020). Mobile Operating System Market Share Worldwide. Available from: <https://gs.statcounter.com/os-market-share/mobile/worldwide>. Accessed date: Aug 5, 2020.
- Statista. (2019a). Statista: The Statistical Portal. Available from: <http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/>. Accessed date: Aug 8, 2016.
- Statista. (2019b). Statista: The Statistical Portal. Available from: <https://www.statista.com/statistics/484583/global-average-selling-price-smartphones/>. Accessed date: Aug 12, 2019.
- Szewczyk, P., and Sansurooah, K. (2010). The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia. Proceedings of the 10th Australian Digital Forensics Conference. Perth, Australia: SRI Security Research Institute, Edith Cowan University.