An Investigation on Forensic Opportunities to Recover Evidential Data from Mobile Phones and Personal Computers

Philip Naughton and M A Hannan Bin Azhar
Computing, Digital Forensics and Cybersecurity
Canterbury Christ Church University
Canterbury, United Kingdom
Email: {p.naughton78, hannan.azhar}@canterbury.ac.uk

***Abstract*— This paper is a summary of experiments conducted to explore forensic opportunities available to the Law Enforcement Agency in the recovery of artefacts resulting from criminal use of popularly chosen applications. The experiments were conducted using forensic examination tools and techniques on a mobile phone running an Android operating system (OS) and another using Apple's OS, as well as a computer running Windows 10 OS. These examinations involved the forensic acquisition and analysis of artefacts resulting from simulated criminal use of common messaging applications, running on both mobile smart phones and personal computers. Many of the complexities and factors effecting successful forensic data acquisition, such as encryption and ephemeral burn functions were also explored together with data analysis.**

Keywords- Digital forensics; data acquisition; messaging applications; mobile phones and PCs .

I. INTRODUCTION

Increased data download speeds have made it possible for new social media applications (Apps), delivering rich content between users, to work effectively in a way that was not previously possible. By 2016, the improvements in mobile data speeds had resulted in 71% of all adults in the UK owning a smartphone, up from 66% in 2015 [1]. This growth in smart phone ownership combined with improvements in 4G network coverage across the UK and ever more sophisticated Apps in terms of functionality and content delivery, explains why there is continuous high demand for Apps from both the Apple and Google stores.

Data recovered from digital devices is vital in identifying a suspect's on-line activity to prove or disprove his/her alleged involvement in a criminal offence. Police forces utilise all their available intelligence sources to inform their decision making in order to prioritise which of the thousands of devices seized every day during criminal investigations will be examined for evidence. They also must make decisions, based on demand pressures, which devices will not be examined at all, despite the potential possibility of evidence being on them. When reviewing forensic examination processes, Her Majesty's Inspector of Constabulary (HMIC) reported negatively that during a review of a UK force, there were significant delays caused to investigations because computers and other media submitted to Digital Forensic Examiner (DFEs) were taking too long to forensically examine [2]. Despite all the best efforts of an intelligence led forensic prioritisation approach, the delays in examinations were potentially impacting negatively on the efficiency of serious crime investigations. So further studies were required to identify which platforms and Apps would offer more forensic opportunities to the Law Enforcement Agencies (LEAs) while recovering evidential data from a collection of suspect devices. This in turn could potentially assist the LEAs in their decision making and prioritising of the many devices submitted to them for forensic examination, which eventually would help with the case load management. This paper reports forensically sound analysis and results in gathering evidential data from the Apps commonly used in criminal activities and installed on both smart phones and personal computers (PCs).

Section 2 of this paper reviews existing work by academic and subject matter experts in relation to the topic of this research paper. A brief explanation on the methodology used will be discussed in Section 3. Results and analysis will be reported in Section 4. Finally, Section 5 concludes the paper.

II. LITERATURE REVIEW

The literature review sought to identify known challenges and opportunities that tend to frustrate or enhance forensic opportunities for LEAs to recover digital evidence from devices (mobile smart phones and PCs). This paper considered a digital forensic opportunity to mean when a file or chat log sent by a criminal between devices could be acquired from these devices by employing forensic examination software tools to recover these artefacts. The topics covered in the research ranged from the scope and limitations of the forensic tools available to potential future hardware and software developments, such as cloud based technology. Understanding the differences between App types available on the market and any built-in anti-forensic features was important to be able to assess how their difference might impact on the results of this paper's experiments.

A. App types

There are three main App types: Native, Web and Hybrid. 'Native Apps' are built with a mix of platform-specific technologies running in most cases on either Android or iOS platforms. Each platform uses different technologies. Android programmers for example mainly build their Apps with Java [3], making occasional use of Python, whereas iOS developers use the Objective-C programming language. Secondly, 'Web Apps', which run on a device's browser are rendered HTML web pages and look like an App. The third type of App is called a Hybrid. Here, developers build a standard Web App, primarily built using HTML5 and JavaScript, then insert it inside a thin native container that provides access to native

 ISBN: 978-1-61208-605-7

platform features that allows it to function like a native App. WhatsApp reported that over 60 million recent downloads were made of their native Apps [4]. The constant 'on' state of native Apps may potentially result in creating more opportunities for DFE from devices that are capturing more records of user activity, for example location data. Although native Apps usually performs better than Web Apps, a recent empirical study [5] reported that in about 31% of the situations, Web apps perform much better than the native apps, when providing the same functionality.

As Apps have become widely used, so too have the public's concerns regarding security. This has led to several App developers incorporating additional features to protect user data. Although data security is a good thing, it can however often frustrate DFE efforts to pursue criminals. WhatsApp for example has now built in end-to-end encryption anti-forensic features. Others such as Snapchat reportedly provide users with ephemeral messaging, which is described as the mobile-to-mobile transmission of multimedia messages that automatically disappeared from the recipient's screen after the message had been viewed [6]. That is to say they were automatically and permanently deleted from the user's device. However, other researchers were sceptical about Apps such a Snapchat's claims to permanently delete messages, photos and videos contesting that at best, the data is recorded, used, saved and then deliberately deleted; but at worst, the ephemeral nature is faked [7].

B. Law Enforcements' ability to acquire digital evidence

LEAs rely on physical and software inspection tools to conduct their forensic data acquisition and analysis of evidential data from digital devices. Commercially available forensic examination tools are constantly having to play catch up with the high frequency of App developer updates, as seen in Table 1, and this causes ongoing challenges in recovering evidential data from devices.

TABLE I. APPS UPDATE VERSION HISTORY.

Apps	Number of times App updated	
	Android	*iOS*
WhatsApp	13	4
Facebook messenger	5	4
Google photos	5	4
Skype	5	1
Twitter	5	5
Instagram	4	6
Kik	3	5
Dropbox	2	3
Snapchat	1	5

There is a general lack of hardware, software, and/or interface standardization within the industry ranging from the storage media and file system to the OS [8]. Each manufacturer develops their very own bespoke versions of the android OS specific to its hardware, which means that App developers must ensure that their product will work with every Android phone OS version in addition to iOS devices. Individual Apps, as seen in Table 1, do not get upgraded at the same time or frequency across platforms. From Table 1, it can be seen that the Android version for WhatsApp was updated thirteen times in just two months (January and February, 2017), whereas the Apple iOS version of the same App was updated four times in the same period. App updates for PCs tend to be far fewer and less frequent.

There are two types of physical data acquisition tools for mobile phones. They are used infrequently by LEAs due to the costs, both in conducting the processes and in replacing phones damaged during these processes, which tend to be destructive to the device. The first of these two techniques is called Chip-off, which is the process as involving the physically removing flash memory chips from a suspect's mobile phone and then acquiring the raw data using specialized equipment [9]. The second physical technique used called Joint Test Action Group (JTAG) is the process of soldering wires directly to the test access ports [10] on a device's circuit board. Again, this process is not widely used because of the risk of damage resulting from soldering contacts to the phone.

C. Cloud based technology

Cloud computing is the act of storing, accessing and sharing data Apps in remote locations [11]. In order to cope with the problem of limited storage capacity, mobile phone devices manufacturers recognise the need to use services which can seamlessly offload some of the tasks of a mobile application from the handset to servers [12]. However, others believe that because smartphones aren't expected to do as many things as PCs can, and what they can do they must do on less power, that this is the real driver for the use of cloud technologies [13]. Accessing cloud data may produce different but no less significant challengers for DFEs. As a consequence, many of the forensic software tool companies, at the time of this paper, were tasking their developers to work on cloud data acquisition tools.

PCs do not share the same storage issues as mobile phones. They typically stores several terabytes (TB) of data [14]. A PC with a storage drive of 3TB can hold roughly 360 videos, 750,000 songs or 600,000 images. The sheer volume of the potential data on a drive of this capacity can cause DFE challenges when reviewing the data recovered during an examination of a suspect's PC. Despite PCs not having the same storage issues, they still make some use of cloud storage to make backups of their contents or user data, such as photos sent and received via Apps.

The Acquisition and Disclosure of Communications Data - Regulation of Investigatory Powers Act 2000 [15] governs UK LEAs' powers to acquire data. Although DFEs can technically acquire data from a cloud server in a foreign country using a suspect's device via a connection with that server, they may breach laws in that jurisdiction because UK courts cannot authorise such action in foreign countries.

III. METHODOLOGY

During the experiments, a set of test files and chat messages were sent between the devices via a set of test Apps

known to be commonly used to simulate potential communications between criminals. Experienced and qualified. Law enforcement forensic examiners were consulted in the planning and designing the experiments, so that the experiments were realistic and in accordance with what the professionals have to deal with in practice. To capture a representative sample of policing across the UK, fifteen forces were chosen to cover all the countries in the British Isles representing the diversity in policing experiences. The findings and conclusions from the experiments would therefore be comparable to those in real investigations.

Oracle's open source software VirtualBox [16] was used to create a virtual machine (VM) in a PC to be one of the three test devices. It was used rather than a physical machine because the VM PC had the advantage of only having a fresh Windows OS installed on it and the Apps needed for these experiments, which are detailed in Table 2. Therefore, the results found during the forensic examination of the device could not have been influenced by other software previously installed as could have been the case on an old re-used physical PC.

TABE II. VM PC SETUP AND CONFIGURATION.

Machine Type	*Specifications*		
	Operating system	*Installed software*	
PC – Oracle VM created and running on host machine Acer Aspire Laptop Intel Core i3	Windows 10 64 bit	Clean install Windows 10 with only the following Apps installed on the PC (VM). Current versions used as of 6th January 2017	
		Dropbox	Google photos
		Google search	Skype
		Twitter	WhatsApp
		Blue Stacks Android Emulator – used to install and run the Apps listed below. Current versions used as of 6th January 2017	
		Facebook Messenger	Instagram
		Kik	Snap Chat

The two mobile smart phones were also used during the experiments and are detailed in Table 3. The current versions of the same Apps detailed in Table 2 were also installed on both phones as of 6th January 2017. The iPhone was not jailbroken, neither was the Samsung rooted because these experiments did not involve the use of alternative Apps available outside of Apple or Android stores. No device OS or disk encryption were enabled on any of the test devices.

TABLE III. MOBILE SMART PHONES CONFIGURATIONS.

Phone types	**Specifications**		
	Model	*OS version*	*Kernel version*
Samsung Galaxy J3	SM-J320FN	Android 5.1.1	3.10.65.8870959
iPhone 5c	A1507	IOS 10.1.1	XNU based on Darwin 16

Two forensic workstations were set up to facilitate the forensic examination of all three devices being investigated. Forensic software tools were then used to examine devices to acquire and analyse the test sample data from them. One of the workstations used for investigation had Cellebrite UFED [17] software tool installed, which was used for examining all the Apps on both smart phone devices. Its job was to acquire artefact evidence from the mobile phones and analyse the recovered data. The second workstation had an open source forensic acquisition and analysis tool installed called Autopsy version 4.3.0 [18]. Autopsy is a digital forensics platform and graphical interface to digital forensics tools.

The forensic examinations were conducted following the guidelines set by the Association of Chief Police Officers (ACPO) [19] namely the first principle, by not taking action to change the data, and the third principle, by keeping an audit trail, so that an independent third party could examine the procedures and achieve the same result. Tools which pose risks in breaching these principles were not used in the experiment. One example of such tools was RetroScope [20], which can recreate multiple previous screens of an Android App in the order they were displayed from the phone's memory. But use of such tools may be considered as the breach of the first principle of the ACPO guidelines [19] due to the restructure of data and hence were not used in the study.

The test files used during the experiments were selected to represent common illegal communications between criminals, such as the distribution of child pornography or documents detailing stolen bank account details. While consulting with the law enforcement processionals, it was found that MD5 (message-digest algorithm) was widely used in their forensic laboratories. All test files used in the experiments had their MD5 hash value calculated before they were sent. These hashes were used to conduct keyword searching during the examination in order to manually trace and locate the test data files on the devices, which might not have otherwise been recovered during the use of a forensic tool's automated examination process and in its basic reporting mechanism.

Every time the forensic examination software located one of the sent test files and messages on the devices, which could be attributed to one of the test Apps, then a count was recorded for the App and its device. Once the first examinations were completed, the test data was deleted from each device, as is commonly done by criminals to hide their activity and incriminating files. Only the App's general user interfaces were used during this data deleting phase. The forensic examination of each device was then repeated and once again test files recovered and attributable to test Apps were counted. The totals of the successfully recovered files were calculated and considered as positive forensic opportunities because each recovered test file represented a crime having been committed and therefore the recovery of such a file could potentially lead to the prosecution of an offender.

IV. RESULTS AND ANALYSES

This section outlines the results and analysis from the experiments conducted during this research exploring the difficulties and opportunities in forensically acquiring evidential data from Apps running on both phones and PCs.

A. Cloud technology challenges

Apps like Instagram store most of the users' images and messages in the cloud and store cached links on the device to these images so that the user can find them again. The difficulty here for DFE is that the images may no longer be stored on the device itself for recovery via examination. None

 ISBN: 978-1-61208-605-7

of the test files were recovered from the Instagram App across all three devices.

B. Web forensic opportunities on PCs

Web based Apps, such as Dropbox on PCs are now offering more evidence than in the past because of backups of files, documents and images from mobile phones and other devices being synchronised via the internet to the PC. This leaves a copy of the data, which can be potentially recovered by forensic examination of the PC. Only Dropbox and WhatsApp were found to offer consistent forensic opportunities to recover test files from across all three device types.

C. App developer updates issues

The forensic tools tended to check one App at a time for potential digital evidence as they worked through fully examining the mobile devices. If it came to an App that had been updated the tool could no longer recover data from it (because the data is was now stored in a different location on a different SQLite database than previously), and tended to finish the examination. Forensic tools data acquisition processes appear sensitive to the versions of operating software used on a device. On occasions data was found but not reported by the tool. These issues with the commercial forensic tools get fixed regularly, but until the glitch does get fixed evidential data could potentially be missed.

The situation is however less severe with App updates on PCs because Microsoft regulate their operating systems and for Apps to run on them they have to comply with the operating system and fit with its controls. Therefore, there is not as much variance on PCs as on Android phones in particular and also iPhone.

D. Ephemeral messaging challenges

Snapchat, on both mobile phones and PCs, does not store images. After a very short period of time they are deleted by the software automatically. None of the test files were recovered, either pre or post file deletion, from this App. The recovery of data is low and only occurring when the message has not been already read. Although some users often screen capture the Snapchat message and store it on their device, this is often recoverable by examiners.

It is noteworthy that phones back up files to a PC through a process of synchronisation. This process takes place so that the phone's data can be later restored back to the phone if necessary, for example if it encounters an OS issue. Although not tested during these experiments, this synchronisation function facilitates opportunities to recover data that was once on a mobile phone, not from examining the phone itself, but from examining the PC where the phone's data was backed up. This approach by forensic examiners may capture user data, which may no longer be recoverable from the mobile phone itself because the user deleted it.

E. Encrypted services

WhatsApp was the only App tested during this paper's experiments that purported to provide users with end to end encryption. Encryption is more common on mobile phones than on PCs but does not totally frustrate DFE. For example, sometimes thumb nail pictures still exist on a device, which can be viewed even if the criminal were to subsequently encrypt the photo. Despite WhatsApp encryption services, it was found to offer forensic opportunities across all three device types.

F. Duplication of test files

Large numbers of duplicate copies of the test data were found during the forensic examinations across all three devices both pre and post file deletion. There appeared to be duplicate files stored within all the Apps examined as well as in other locations on the devices not easily attributable to any App. The Apps themselves and/or the devices' OS appeared to be creating and storing duplicates of the test data that had been sent. Duplicate video files for example were found to be part copied and stored in the device's cached memory resulting from what appears to be user video playback activity on the device.

During the iPhone examination, significant numbers of files were recovered that had been saved in UNIX executable format. This occurs when files are originated from a non-Apple operating system and no extension is put on the file. However, on some occasions this did not happen with files that were received on the iPhone from the PC because the files were received with extensions. Even though such files had lost their information of resource forks (type/creator codes, specifically) during transmission from the PC to the iPhone, iOS could still use the extensions to associate the specific file types. In such scenario, both the UNIX and reconstructed files were stored on the iPhone and could both be recovered. Both files had the same time stamps on them indicating that they were the same file as the one sent from the PC.

Some of the recovered files on the iPhone had been saved within the "thumbs.db" files, which were created by Windows OS without user's knowledge as per default settings. This type of file generates a quick preview of the content of a folder using a thumbnail cache. During experiments, such cache files appeared to have been sent along with the test video and picture files. Recovered artefacts from these files could be used to prove that illicit photos were previously stored on a suspect's hard drive even after the deletion of the content.

Backups of media contents in both Kik and WhatsApp were found to cause duplicates of photos and videos. For example, the exact same file was recovered from the Kik App stored in the folders "content_manager/data_chache" and also "attachments" within the path "Backup/Applications/group.com.kik.chat/cores/private/41b3f76b03e54d9dac449d1c1ab5955b/". Photographs received from WhatsApp were found to be stored into Apple's photos as well as in the App's databases. During this process files stored in "bmp" and "gif" appeared to be duplicated into a "jpg" format before being stored in Apple's photos.

G. Device type factor

Table 4 is a summary of the positive forensic examination results found by device type during experiments. The second column from the left shows the number of test files sent to the device and therefore could have been potentially recovered

 ISBN: 978-1-61208-605-7

from it. Every time one of the test files was found that could be attributable to one of the test App, a note was recorded. This was done, pre and post deletion, for each of the devices.

TABLE IV. POSITIVE FORENSIC EXAMINATION RESULTS BY DEVICE TYPE.

	Total test files that could be potentially recovered	Pre – deletion files actually recovered	Post – deletion files actually recovered	Actual links to files stored in the cloud recovered Pre -deletion	Actual links to files stored in the cloud recovered Post - deletion	Grand totals of files recovered
PC	266	29	29	10	10	78-30%
iOS	210	14	12	22	17	65-30%
Android	218	18	14	2	0	34-16%

The remaining columns in Table 4 show the actual number of files found both pre and post deletion. As can be seen in the column on the far right of Table 4, the PC appeared to offer DFE the most forensic opportunities with 30% of the test sample files being recovered, which is similar to the number recovered from the iPhone. Only 16% of the test files were recovered from the android phone.

Most PCs run Microsoft operating systems. The file structures and OS run on these devices' hard drives are all the same despite the PCs and the hard drives being manufactured by numerous different companies. This may explain why, at 78 files and 30% recovery, the PC offered most opportunities compared with the android phone. This is likely to be as a result of the frequency of upgrade of the android operating system, as shown in Table 1, and the lack of regulation and uniformity around its development between phone manufacturers.

All the forensic examination tools used have had development updates since the experiments were conducted. However, the experiments were not repeated with the updated forensic software tools so it is not possible to say whether the updates to the tools may have improved the recovery of the test files, improving positive forensic opportunities.

H. App type factor

None of the test files recovered could be attributable to Instagram or Snap chat, which is likely to be because of their ephemeral security features. Table 5 shows the ranking of the Apps, in terms of the number of test files recovered on each device and across all devices. It was observed that across all devices, Google Photos, Dropbox and WhatsApp were the top three Apps which offered the most forensic opportunities to recover the test files.

TABLE V. POSITIVE FORENSIC EXAMINATION RANKS BY APP TYPE.

PC		
	App	*Recovered files*
1st	Google photos	20
2nd	Dropbox	18
3rd	Skype	16
4th	Twitter	10
5th	Whatspp	8

Iphone		
	App	*Recovered files*
1st	Google photos	22
2nd	Drop box	17
3rd	WhatsApp	12
4th	Kik	10
5th	Twitter	4

Samsung		
	App	*Recovered files*
1st	WhatsApp	11
2nd	kik	10
3rd	DropBox	6
4th	Skype	4
5th	Facebook Messenger	3

All devices		
	App	*Recovered files*
1st	Google Photos	42
2nd	Dropbox	41
3rd	WhatsApp	31
4th	Skype	20
5th	Kik	20
6th	Twitter	14
7th	Facebook Messenger	3

TABLE VI. POSITIVE FORENSIC EXAMINATION RESULTS BY FILE TYPE.

Test File types	Files recovered
Jpeg	50
Chat logs	23
MS Word document	20
Bitmap	19
MP4	17
GIF	16
Avi	12
Mpeg	11
Winzip	5
3GP mobile phone images	4
Total files succesfully sent	**177**

Table 6 shows that Jpeg was the most widely recovered of all the test files. Jpeg files have two sub-formats, one of which is JFIF (Jpeg File Interchange Format). JFIF is often used on the web. In the mandatory JFIF APP0 marker [21], segment parameters of the image are specified and this is where an uncompressed thumbnail can be embedded. Because of the embedding of a thumbnail, the hash value for the file is changed, which explains why duplicates of the files look the same to the user but are in fact not identical.

V. CONCLUSIONS

Although some files could no longer be recovered after they had been deleted during the experiments, a significant number could still be recovered again. It was not possible to send all the test files to the smart phones. The iPhone was only capable of receiving 210 of the test files compared with 266 to the PC because of OS and App differences. Of the test files that were successfully sent to the iPhone, 30% of those were successfully recovered. It was possible to send slightly more test files, in total 218, to the Samsung phone than the iPhone but only 16% were recovered.

Duplicates of the test files resulting from OS and App processes were also recovered during the experiments. A law court may decide to take these into consideration, if found on a suspect's device, even though these files may not always be easily associated with any particular App because, for example, they may be stored in unallocated space on the device's memory. However, because of hash value differences between the file sent from one suspect's device with that duplicate file recovered on the second suspect's device, the DFE would need to be able to explain how and why the file had been altered to prove it actually came from the first suspect, thereby linking them together.

None of the test files sent using ephemeral Apps, Snap chat and Instagram, were recovered. However, they may be recoverable using specific forensic examination processes [22]. This causes additional complexities for DFEs. If mobile phones, and in particular Android based phones, were to consistently offer fewer opportunities to recover evidence both now and in the future, then that would potentially represent a degradation in LEAs' capabilities, given that large numbers of criminals are moving to using their phones as the primary device to connect to the internet.

In future, a more longitudinal study will be necessary to take into account the impact of updates by OS and App

 ISBN: 978-1-61208-605-7

developers on the tools. It will be worth conducting a statistical analysis to determine if the ability to retrieve data is related to the number of updates of the operating platform made by the developer. Establishing whether the OS continues to create and save duplicate files to the cloud despite the auto save function being disabled would be useful. Knowing the effects that such an action may have on the numbers of recoverable duplicate files and their storage locations, such as cache, would be helpful.

REFERENCES

[1] OFCOM, "Communications Market Report (UK)", 2016, Available online: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/26826/cmr_uk_2016.pdf, Last accessed September 2017.

[2] HMIC, "National Child Protection Inspections", 2014, Available online:https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/greater-manchester-national-child-protection-inspection.pdf, Last accesed September 2017.

[3] S. Bommisetty, R. Tamma, and H. Mahalik, "Practical Mobile Forensics", Packt Publishing, 2014.

[4] AppBrain, "WhatsApp Inc. summary", Available online: http://www. appbrain.com/dev/WhatsApp+Inc./, Last accessed September 2017.

[5] Y. Ma, X. Liu; Yi. Liu; Yu. Liu and G. Huang "A Tale of Two Fashions: An Empirical Study on the Performance of Native Apps and Web Apps on Android", IEEE Transactions on Mobile Computing, ISSN: 1536-1233, doi: 10.1109/TMC. 2017.2756633, in press.

[6] J. B. Bayer, N. B. Ellison, S. Y. Schoenebeck and E. B. Falk, "Sharing the Small Moments: Ephemeral Social Interaction on Snapchat", Information, Communication & Society, vol. 19, pp. 956-977, 2016.

[7] F. Roesner, B. T. Gill and T. Kohno, "Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-Destructing Messages", Financial Cryptography and Data Security, Lecture Notes in Computer Science, vol. 8437. Springer, 2014.

[8] J. Lessard and G. C. Kessler, "Android Forensics: Simplifying Cell Phone Examinations", Small Scale Digital Device Forensics Journal, vol. 4, no. 1, pp. 1-12, ISSN: 1941-6164, September 2010.

[9] V. Rao and A.S.N. Chakravarthy, "Survey on Android Forensic Tools and Methodologies", International Journal of Computer Applications, vol. 154, no. 8, pp.17-21, 2016.

[10] M. F. Breeuwsma, Forensic imaging of embedded systems using JTAG (boundary-scan), Digital Investigation, vol. 3, pp. 32–42, 2006.

[11] D. T. Hoang, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing, vol. 13, pp. 1587-1611, 2013.

[12] K. Yang, S. Ou and H. Chen, "On effective offloading services for resource-constrained mobile devices running heavier mobile Internet applications", IEEE Communications Magazine, vol. 46, pp. 56-63, January 2008.

[13] M. Lai, J. Wang, T. Song, N. Liu, Z. Qi and W. Zhou, "VSP: A Virtual Smartphone Platform to Enhance the Capability of Physical Smartphone", IEEE Trustcom, BigDataSE & ISPA, pp.1434-1441, August 2016.

[14] A. Klein, "Hard Drive Stats for Q2 2017", Available online: https://www.backblaze.com/blog/hard-drive-failure-stats-q2-2017/,Last accessed September 2017.

[15] Legistlation.gov.uk. "Regulation of Investigatory Powers Act 2000", 2000, Available online: http://www.legislation.gov.uk/ukpga/2000/23/contents, Last accessed September 2017.

[16] VirtualBox tool, Available online: https://www.virtualbox.org, Last accessed September 2017.

[17] Cellebrite UFED tool, Available online: http://www.cellebrite.com/Mobile-Forensics/Solutions, Last accessed September 2017.

[18] Autopsy tool, Available online: https://www.sleuthkit.org, Last accessed September 2017.

[19] Association Of Chief Police Officers, "ACPO Good Practice Guide for Digital Evidence v5", 2012, Available online: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, Last accessed September 2017.

[20] B. Saltaformaggio, R. Bhatia, X. Zhang, D. Xu., G. Richard III, "Screen after Previous Screens: Spatial-Temporal Recreation of Android App Displays from Memory Images". In Proc. 25th USENIX Security Symposium (Security'16), Austin, TX, 2016.

[21] Jpeg file format, Available online: https://www.w3.org/Graphics/JPEG/jfif3.pdf, Last accessed September 2017.

[22] M. A. H. B. Azhar, and T. Barton, "Forensic Analysis of Secure Ephemeral Messaging Applications on Android Platforms" In: Jahankhani H. et al. (eds) Global Security, Safety and Sustainability - The Security Challenges of the Connected World. ICGS3 2017. Communications in Computer and Information Science, vol. 630, pp. 27-41, Springer, 2017.

 ISBN: 978-1-61208-605-7