A forensic evidence recovery from mobile device applications

John K. Alhassan*, Agbejule Gbolahan, Ismaila Idris, Shafi'i Muhammad Abdulhamid and Victor O. Waziri

Department of Cyber Security Science,
Federal University of Technology,
Minna, Nigeria
Email: alhassan.jk@futminna.edu.ng
Email: oagbejulegbolahan@yahoo.com
Email: ismaila.idris@futminna.edu.ng
Email: shafii.abdulhamid@futminna.edu.ng
Email: waziri.victor@futminna.edu.ng
*Corresponding author

Abstract: In recent past, there are a lot of research advancements in mobile forensics tools. This is so due to increase usage of mobile phones in storage of information, law enforcement, mobile online transactions, and also negatively by criminals due to increased computational capabilities. Mobile forensics devices continue to remain a very challenging task due to poor user data retrieval techniques for evidence retrieval. Recently, third party applications assume a veritable feet because it is supported by majority of mobile devices platforms, thereby making it easy to extract information of its users' for future criminal audit. This paper proposes an evidence data retrieval method from InstagramApp using two networks-based platforms [that is, pure peer-to-peer (PPP) and special cluster peer (SCP)-based], whose concept is to manage mobile device communication and generate multiple copies of users data/information to be dumped across three servers. The forensic test results were obtained from PPP and SCP developed to securely extract data from mobile devices. This shows that, SCP outperformed PPP in terms of the time taken to fulfil forensic auditor's request, throughput and broadband utilisation which are 42.82% to 57.18%, 56.81% to 43.19% and 35.41% to 64.53% respectively.

Keywords: mobile forensic; evidence recovery; pure peer-to-peer; special cluster peer; SCP; mobile device.

Reference to this paper should be made as follows: Alhassan, J.K., Gbolahan, A., Idris, I., Abdulhamid, S.M. and Waziri, V.O. (2018) 'A forensic evidence recovery from mobile device applications', *Int. J. Digital Enterprise Technology*, Vol. 1, Nos. 1/2, pp.79–95.

Biographical notes: John K. Alhassan obtained his BTech in Mathematics/Computer Science at the FUT Minna, Niger State, Nigeria. He earned his Master of Science in Computer Science at the University of Ibadan, Nigeria in 2006, and Doctor of Philosophy in Computer Science at the Federal University of Technology, Minna, Niger State, Nigeria. He carried out part of his PhD research at the United Institute of Informatics Problems, National

Academy of Sciences of Belarus Minsk, Republic of Belarus. He is currently the Ag.HOD of Cyber Security Science, FUT Minna, Nigeria. He has published 12 journal articles and four conference proceedings. He is a member of Computer Professionals Registration Council of Nigeria.

Agbejule Gbolahan holds a Master's degree in Cyber Security Science from the Federal University of Technology, Minna, Nigeria. His research interests are information security, data mining, machine learning, and evolutionary algorithm.

Ismaila Idris is with the Department of Cyber Security Science. He obtained his Bachelors degree from the Federal University of Technology, Minna. He earned his MSc from the University of Ilorin and his PhD degree from the University of Teknologi Malaysia. His research interests are information security, data mining, machine learning and evolutionary algorithm.

Shafi'i Muhammad Abdulhamid received his PhD in Computer Science from the Universiti Teknologi Malaysia, his MSc in Computer Science from the Bayero University Kano, Nigeria and his Bachelor of Technology in Mathematics/Computer Science from the Federal University of Technology Minna, Nigeria. He has published many academic papers in reputable international journals, conference proceedings and book chapters. He has been appointed as an editorial board member for *Big Data and Cloud Innovation*, and *IJTRD*. He has also been appointed a reviewer of several ISI and Scopus indexed journals. Currently, he is a Senior Lecturer at the Department of Cyber Security Science, FUT Minna, Nigeria.

Victor O. Waziri is an Associate Professor of Cyber Security Science in the FUT Minna, Nigeria. He is a member of the following professional bodies; The Computer Professionals Registration Council of Nigeria (CPN) and The Nigeria Computer Society (NCS). He has published many papers in reputable journals at both international and local levels. He lectures various courses in the department that include cryptography, network security, clouds security, data mining, computational theory, automata and programming languages.

1 Introduction

Recently, digital forensic experts have turned their attention to mobile communications technologies, because of widespread usages and applications to daily lives of people across the world. Assessing phone and its data extraction are still areas of concern to present-day forensic examiners. Mobile devices continuously have influenced the way people live and relate with others, therefore, phones can be a potent tool for committing crimes and other social vices. Also, phone can play big roles such as witness when crimes are committed, which can be used as evidence (Yusoff et al., 2014).

Mobile phones are enabled with functionalities similar to desktops and laptops computers such as large amount of data stored on the them especially personal information such as address book, e-mail, test messages, digital photograph, call history, passwords, calendar items, memos, and credit card details, which can be used largely to address sensitive queries during investigations. Mobile devices effectively communicate, connect to social networks, sketch, exchange photographs, record events, take notes, consume audio and video, access internet and blog (Walls et al., 2011).

In the past ten years, third party applications are vehemently most deployed platform for mobile digital forensics. Digital evidence produced by mobile devices have potential of being lost totally because it is vulnerable to overwrite by new data or remote destruction commands received across wireless networks. More so, in case of effective mining information, there is need to interrelate with the device frequently in order to alter the state of system. In computer systems, interacting with a mobile device can destroy or modify obtainable evidence (Martini et al., 2015). This is an area considered for this paper, the way of improving mobile device evidence recovery.

The purpose of this research paper is to propose a procedure for evidence data retrieval method from InstagramApp using two networks-based platforms [that is, pure peer-to-peer (PPP) and special cluster peer (SCP)-based], whose concept is to manage mobile device communication and generate multiple copies of users data/information to be dumped across three servers. The rest of the paper is organised as follows: Section 2 details the related works in the field of mobile computing for evidence retrieval. Section 3 presents the research methodology that includes the descriptions of the proposed method and performance evaluation metrics. Section 4 presents the implementation and results, while Section 5 presents the conclusion derived from results.

2 Related works

A system for recovering information from phones having unknown format of storage known as DECODE was presented by Walls et al. (2011). This technique was used to analyse different data structures with a classic dynamic programming algorithm to identify call logs and entries of address book stored on the various phone models. A conceptual evidence collection and analysis methodology for android devices because of the widespread usages for different applications, which require sound evidence gathering and analysis, was developed by Martini et al. (2015). This method rely on booting a live collection OS from the devices volatile memory (or RAM) upon the identification and preservation procedures (that is, radio suppressing device to avoid remote wiping). The purpose of live OS was to gather data in order to effectively obtain a copy without modifying contents of secondary memory. However, transportation of data between mobile phones and designated PC is through the USB. Through extensive study of phone records, the mutual behaviour at large scales and focus on the manifestation of unusual events can be determined in both time and space (Candia et al., 2008; Tassone et al., 2017). Thus, interaction archives of social media sites like Whatsapp, WeChat, KakaoTalk, Facebook, etc. can be retrieved from the mobile phones of lawbreakers and can be used as important digital evidences for the investigation and prosecution of criminal cases (Okongwu and Adebayo, 2013; Wu et al., 2017; Smith et al., 2017; Choi et al., 2017). Logical mining of information in the Android phone was collected by using a recognised mobile phone forensic tool-XRY to mine numerous data of forensic interest such as user e-mail ID and list of tasks (Osho et al., 2015; Azfar et al., 2017; Azhar and Barton, 2017).

A generic forensic method used to carry out forensics analysis across all smart phones platforms such as Blackberry, Android, iOS, and Symbian was developed by Chang et al. (2013). The author captures forensic evidential data from memory cards and sticks, subscriber identity module (SIM), and mobile phone internal/flash memory through pre-

installed forensic app memory card. Also, there is need to block RF signal on the smart phones during forensic examination, which makes unsuitable for online or remote evidential data capturing. An android forensic data analyser (AFDA) was proposed by Kasiaras et al. (2014) to collect end-user's data stored in critical system areas; thereafter, inter-correlate them in respect to a time and location-based series of activities. The aim was to speedup time and effort of investigators as well as interrelating artefacts for a more robust and comprehensive ways. It supports fewer smartphone operating systems (Android OS).

Two data recovery techniques for deleted files on android powered mobile phones by examining the structure of YAFFS2 and NAND file system were examined by Chang et al. (2013). The author recommended a method for recovering YAFFS2 file system deleted on Android devices. A research on cloud computing situation to avoid physical access to media reposing the data of users, a great division from several existing forensic tools that require physical access to the storage media of users was proposed by Choo (2013). The success of this method of forensic is hampered by data fragmentation and distribution across the universe in several data centres, which throw up technical and jurisdictional issues.

A pure PPP system contains of identical peer nodes that concurrently function as both clients and servers (Rizzo et al., 2017). A PPP storage system is on the heterogeneity of involved devices: while most of current P2P solutions are targeted to PC-like hardware, Beekup is premeditated to gracefully adapt to diverse hardware and software capabilities, from implanted devices to professional servers. Each node of the P2P storage network managed by beekup, hosts an instance of the beekup service, whose architecture (Cafasso et al., 2017).

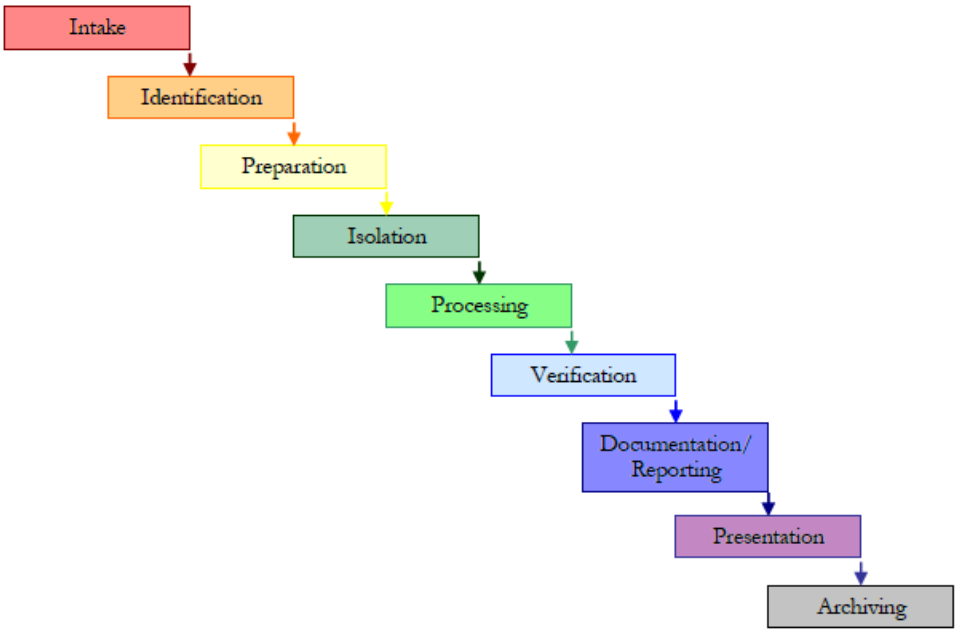
2.1 Overview of mobile devices forensics

At present, several models of cellular phones in the market have varied proprietary operating systems, services, embedded file systems, peripherals and applications. The original design of cellular phones is to communicate through network to other networks usually by means of bluetooth, wireless (WiFi) and infrared technologies. Studies revealed that the best way to preserve data on the phone is by isolation from neighbouring networks, which is unlikely. Cellular phones have numerous interior, detachable and online data storage facilities (Finneran, 2014).

In practice, several tools are applied in the process of extracting desired data or document from the cellular phone and its media store. Also, these tools process cellular phones and report inconsistent (or error prone) information, which require accuracy verification for extracted data (Abdulhamid and Abd Latiff, 2017). Cellular phones store different types of data with varying usages in the course of time. The widespread popularity of smart phones makes it insufficient to record only the phonebook, call history, photos, SMS messages, notes, and calendar records and media storage compartments. There is need to record the data from increasing amount of applications installed, which warehouse abundant information such as GPS location, passwords and history of browsing. Mobile phone data is usually preferred for the purpose of intelligence that increased focus on phones because it's easy for phones to be processed in that field (Goode, 2003).

Majority of the time, certain data is required that involves complete extraction of the physical memory and embedded file system in order to prosecute a complete forensic analysis and possible recover deleted data (Willassen, 2003). Consequent upon this, fresh strategies and processes for extraction and documentation of data mined from phone evolved as shown in Figure 1.

Figure 1 A process of mobile phone data extraction and documentation (see online version for colours)



Source: Willassen (2003)

2.2 Mobile device technology

Often, mobile devices are referred as modest computers having a CPU, batteries, storage, input interfaces such as a mouthpiece or keypad; and output interfaces such as an earpiece or screen. During forensic examination, the general focus is on data in memory that require knowledge of components of input and output in order to utilise them (Lin et al., 2014). However, to recover deleted data, advanced investigation is carried out with use of special tools that interface with the mobile device. It is adequate to make use of cable to retrieve certain information of concern from a mobile device's data port. In many situations, there is need to attach a specialised connector straight to the circuit board to collect all information required in prosecuting a case. Understanding data manipulation and storages on mobile devices is necessary to retrieve available forms of digital evidence from handheld devices and translate it into a human readable form without altering it (Kausar, 2014).

Mobile devices make use of radio waves to connect to networks at varied frequencies and standard protocols of communication. The most common mobile communication protocols are code division multiple access (CDMA), global system for mobiles (GSM) and integrated digital enhanced network (iDEN). GSM devices are assigned a unique number known as international mobile equipment identity (IMEI), which includes a device's serialised number (Jansen and Ayers, 2007). In CDMA-based phones, the electronic serial numbers (ESN) is an 11-digit number in which the first three digits describe its producer and the remainder uniquely identifies the mobile device. Mobile devices have diverse identifiers based on the producer, MAC address of hardware, location and technology as shown in Figure 2.

Figure 2 Mobile devices with various identifiers

2.3 SIM cards

SIM cards connect to the network and safeguard information such as certain user-created activities, for mobile phones. SIM cards have a certain standard for type and location of information to be stored on the card. SIM cards come in slightly diverse sizes and shapes. Therefore, a SIM card reader cannot support or read data from all types of SIM cards. SIM cards are made up of a ROM, microprocessor and RAM. SIM cards are assigned special integrated circuit card identifier (ICC-ID) (Martini et al., 2015).

The ICC-ID holds the mobile country code (MCC), mobile network code (MNC) and card serial number. These smart cards are used to authenticate users on GSM and UMTS networks. The SIM card keeps information about the network and user such as an authentication key (known as Ki), for establishing a connection to the network. The subscriber's personal identification number (PIN) restricts the SIM unauthorised accesses and usages. The subscriber's mobile subscriber ISDN (MSISDN) is popularly referred to as user phone number (Lin et al., 2014).

However, majority of the stored information of a SIM card is unknown or inaccessible by the subscriber. There is no far distinction between the mobile device and the SIM card; a SIM card can be moved to other mobile devices with ease.

2.4 Types of evidence on mobile devices

The smartphone evidentiary value extends this elementary functionality and related information as shown in Table 1.

Table 1 Mobile device and associated evidence

Baseline phone	*Hardware*	*Evidence*
Smartphone	User-created information, phone-created information, internet-related information, installed third party applications	Handset date and time, IMEI, address book, SMS, calendar, memos, to-do list, call register, photographs, videos, audio, maps, MMS, GPS waypoints, stored voicemail, files stored on system, connected system, online accounts, purchase media, email, Internet usage, social networking information, alternate messaging and communication system, additional capabilities, malware applications, penetration and testing.
Local workstation	Transferred information	Tethered mobile devices, backed-up third party applications, store accounts, and purchase media.
Carrier	Tracking information, usage information	Connected cell towers over time, location at specific times, current location, billing information, call register over time, Internet usage, undelivered messages.
SIM card	Identifiers, usage information	Subscriber identifier (IMSI), SIM card identifier (ICC-ID), SMS, abbreviated dial names/numbers, last dialled numbers, location area

Source: Choo (2013)

2.5 Location information

A location service now is a very sensitive data, which have the capability to be misused by fraudulent third parties. There have been a number of circumstances of potential misuse recorded. This information obtained from cell phone providers is not the only concern that has generated attention in recent times. No longer would an appeal to the cell phone provider be necessary, as at least some of the historic evidence would be deposited on the mobile phones. Although this data is still accessible on Android devices, the iPhone platform was updated to moderate the size of information saved on the mobile phones, delete these files totally when location services are turned off, and encrypt this data on the device, which assists in restricting illegal access.

The capability to estimate the mobile devices location during a period of interest is a potent investigative tool. Certain mobile devices keep record of cellular towers location contacted, which potentially offer a chronological record whereabouts of the user's whereabouts for a specific duration. Exchangeable image file (EXIF) data embedded in digital photographs enhance evidentiary value, that is, time and date the photograph was generated, and the type of device deployed. The GPS synchronises of location of the photograph created. On board GPS provide the user with mapping functionality that assists forensic investigators with waypoints, plotted destinations and routes taken (Walls, 2011).

2.6 Malicious code on mobile devices

Online banking and shopping transactions are being conducted on mobile devices, thereby making it susceptible to attacks. More sophisticated malware allows criminals to divert SMS messages linked to online banking transactions, which make it possible to rip-off money from bank account of victims (Willassen, 2003). Also, there are mobile devices monitoring programs to obtain users' logs including Blackberry, Windows Mobile and iPhone. Spouseware is one of common monitoring program that effectively eavesdrop mobile devices of users. Text messages, Internet browsing, calls, and GPS locations are safely recorded, which are accessed through a website by a person having related details of credentials (Finneran, 2014; Madni et al., 2017).

However, stored information is available to authorised persons having related username and password for specific MobileSpy installed. Usually, these programs provide traces on mobile devices, which is identifiable during forensic investigation. Mobile devices are veritable tool to launch malicious attacks against other secure systems. Many network and computer security tools have been transferred to mobile device platforms such as wireless network security analysers, port scanners, and penetration testing frameworks (such as Metasploit) have been built for Android and Apple iPhone devices. Unofficially, these application types are readily deployed for crime and illicit activities. The availability of such applications is of high benefits in computer abuse examinations (Choo, 2013; Abdulhamid et al., 2017).

2.7 Mobile device forensics tools

There are continuous works carried out in the development of forensic tools for the purpose of taking out particular data from different mobile devices alongside the logical approach of Bluetooth, infrared, or physical approach of cable or JTAG. These tools send commands to the phone and responses are recorded for information extracted phone memory based on phone types and models. Certain forensic tools transmit and run executable usually called a *software agent* on the mobile device, which obtain device data. Software agent built for forensic purpose cannot run on the evidential device, which requires no data. When certain mobile device files are inaccessible through the operating system, more important information is not be readily available. There is limitation to the use of a software agent because it can modify the device data through overwriting approach.

Powering on a mobile device executes the first code known as *boot loader*. The code is the most basic operation similar to BIOS on Intel PCs. Deployment of a mobile device simply lunch the boot loader to trigger operating system in order to allow user to relate with the device. However, there is possibility of interrupting the boot loader and by extension to prevent the lunch of operating system and constrained to operate custom processes. Consequent upon this, forensic tools make use the boot loader to gain access to the mobile device memory. Extracting the memory chips from a phone and reading them directly is by far the toughest method with the opportunity of interfacing data directly. The most low-level physical extraction technique is chip extraction (Abdulhamid and Abd Latiff, 2017). But, this approach is limited by similar challenges as JTAG extraction, and guaranteed to give raw memory structures alone. Also, it has a high failure rate. After successful extraction process, flash chips must be read in order to acquire data referred to

as *chip off* processing. There are many commercial device programmers obtained presently including Data I/O FlashPAK II, and XeltekSuperPro 5000.

3 Methodology

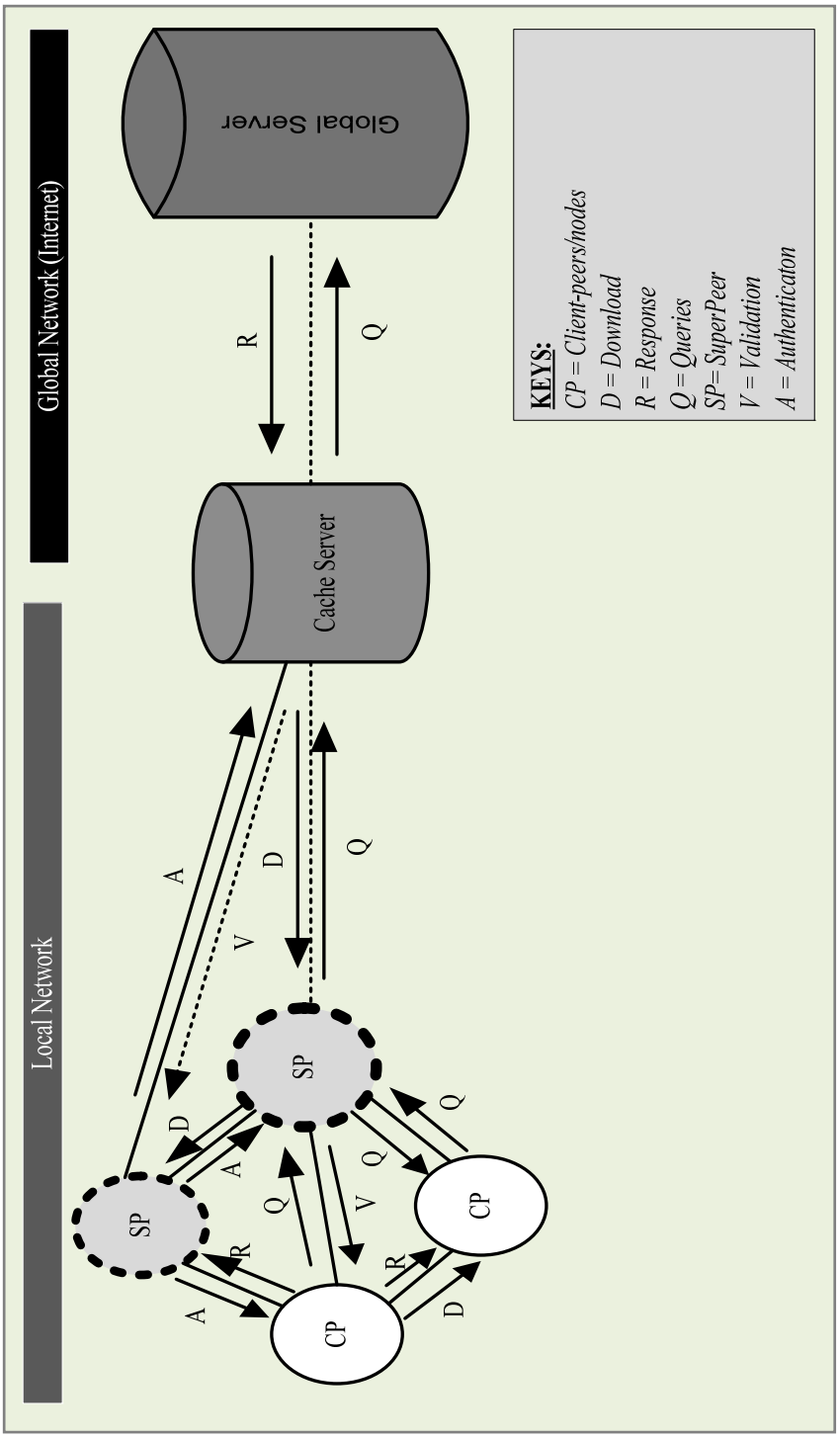
3.1 Description of proposed model

The proposed forensic evidence recovery model is built on the basic principle of PPP network that involves information and data exchanges across network. Mobile devices utilised third party application to send and receive data such as SMS, chats and multimedia files. The choice of PPP network is appropriate because the forensic model capacity increases as the growing number of mobile users and data provided to the entire network. Preciously, a common server for coordinating information of mobile devices was non-existent. Again, mobile devices have capability to connect and disconnect at any given time without specified rules to govern these operations. To monitor relationships existing within mobile devices, this study proposed new rules for entry and exit; this achieved an authentication process was built using the PPP structure that is absent in traditional evidence forensic models. The paper holds that all user data or (content) was domiciled with a local network or cache servers with secure identification scheme. Apart from the conventional operations of request, download and upload content, this evidence recovery model adds another operation of user data and device verification (or authentication). This model's architecture comprises an ad-hoc network of pure cluster PPP network along with special centralised servers for user's data and devices management. The components of the system include: mobile devices, cache servers, global server, networks interconnectivity, user data (or content) and user profile manager, and model operations as shown in Figure 3 and also the steps of the proposed model as presented in Algorithm 1.

The steps of operation for the proposed model include:

Algorithm 1	*Steps of operation for the proposed model*
1	Install the PPP application on user devices or peers.
2	Setup the local network by allotting the supernodes (at least two) and configure cache server.
3	Generate mobile device user's profile and store on a supernode.
4	Create and assign identification scheme to user generated data to be stored on a designated supernode on the local network and thereafter moved to the global server.
5	Mobile devices generate upload, download, and share files/content information to be stored on lookup in Supernode of local network.
6	Queries and search for information are directed at the supernode linked to the mobile device.
7	Search for user generated data beginning from peers, supernodes, cache server and global server until information needed is located.
8	Update lookup tables on the supernodes concerning profiles of mobile
9	Devices, data identifier and status of networks.

Figure 3 Architecture of forensic evidence recovery model (see online version for colours)



3.2 Performance evaluation metrics

Forensic audits were carried using three metrics using the two models to ascertain their effectiveness including:

a rate of file download expressed by equation (1)

$$\begin{aligned} &\textit{File download rate of model} \\ &= \frac{\textit{number of bytes received by system from Cache server}}{\textit{total number of bytes received by download from Cache server}} \end{aligned} \tag{1}$$

b search yields is the measure the speed that fraction of user data copies were found and returned by the audit search queries of the model in the lookup when compared both models setups is given by equation (2):

$$\begin{aligned} &\textit{System search yield} \\ &= \frac{\textit{number of copies of content found by system search queries}}{\textit{the number of stored search content in the lookup}} \end{aligned} \tag{2}$$

c ratio of search success calculates the number of objects found or not found by a forensic auditor mobile device on the network is given by equation (3):

$$\begin{aligned} &\textit{Ratio of search success of system} \\ &= \frac{\textit{number of search successful}}{\textit{total number of searches by both models}} \end{aligned} \tag{3}$$

d throughput is the measure of number of flows carried by the network at a particular point in time for the two models compared to measure their capacities.

4 Results

4.1 Implementation

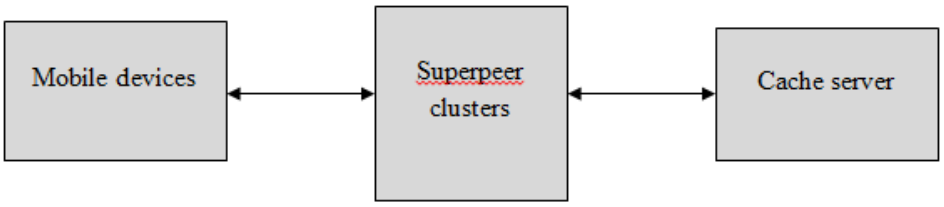
The implementation was carried out in four stages:

- *Stage one*: this selects participating mobile devices, and choice of appropriate cluster superpeers. The local network consists of superpeers cluster, regular mobile devices (or peers) and cache server as shown in Figure 4.
- *Stage two*: this stage setup network TCP protocol and rules governing the ways mobile devices coordinate, search for user data, data usage reports, path of communications, data security verification, file sharing lookup information and, responses and queries processing during forensic audit. The pong, pings and downloads messages broadcasting are partially initiated by the mobile devices and fully transmitted by the superpeers clusters, which is the new feature introduced into the pure PPP network model.
- *Stage three*: the key operations the system were highlighted in details as follows: Firstly, the mobile devices generated user data and identification scheme, thereafter

the details about location and device security features were sent to superpeers clusters for coordination and generation of lookup tables for third party applications. The superpeers clusters were specialised mobile devices (or peers) responsible to themselves and other devices connected to the network. The superpeers clusters received requests messages supplied by individual participating peer (or mobile device) either for data or verification needs; then it acts as the central point of coordination for cache servers, source server and several other mobile devices. Superpeers clusters have capability to define paths to be reached by queries in order to supply the responses (or downloads) for a forensic auditor. In addition to that function, superpeers cluster route all requests by peers to closest peer or cache server in order to satisfy such query messages and stores copies of the log for tracking purposes. Furthermore, mobile devices have storage facilities for maintaining the lookup information, user generated data and requests completely satisfied. Likewise, superpeers clusters store larger/comprehensive lookup tables, updates cache servers and record user data usages; they are available at all times for the purpose of rendering speedy and fair services such audit.

- *Stage four*: this gives an overall perceptive of the model. To test the network connectivity, a mobile device was connected to a superpeer in the cluster (such as http://gnutellahosts.com: 6,346) on the network for stability and availability. A web cache (http://gnutellahosts.com) displaces a host/port used to search network in order to determine participating devices. It acts as *host caches*, that is, a unique application program for storing active network hosts connections at a particular time. Consequent upon that, event data search can be accurately obtained concerning a mobile device investigated as evidence recovery tool.

Figure 4 Structure of category 1 of system



4.2 Outcomes of mobile data evidence audits

The special pure cluster PPP network is a mobile user data network consisting of large distributed mobile devices (or peers), two special supernodes, a cache server and source server. The aim of the model was to deliver secure user data and information to forensic experts with high performance and availability for mobile devices. The common user generated data include: web objects, third party applications support, adaptive streaming media and social networks. This paper evaluated outcomes of the pure PPP network (PPP) and the supernodes cluster pure PPP (SCP) network evidence recovery models. The details of experimental parameters are presented in Table 2.

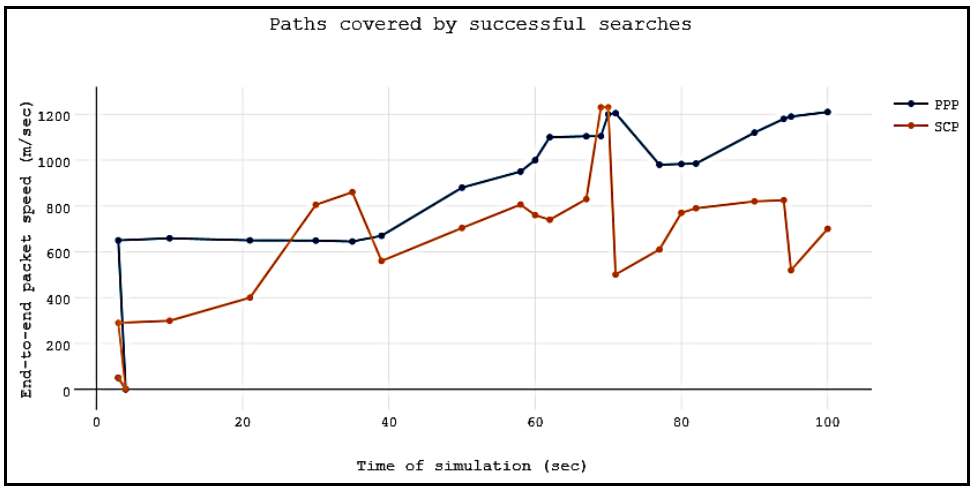
Table 2 Experimental parameters

Parameters	*Value*
Number of mobile devices	25
Number of superpeers	3
Number of cache servers	2
Number of origin server	1
File type	Picture
File format	PNG
Total simulation time	100 sec
Simulation mode	Manual
Metrics	Throughput, delays and downloads
Third party application	Instagram

4.2.1 Paths covered to complete searches compared

The distances indicated level of speedups for the two models compared. The path covered to complete requests messages were measured for the PPP and SCP as illustrated in Figure 5.

Figure 5 Paths covered to complete audit searches for PPP and SCP models (see online version for colours)

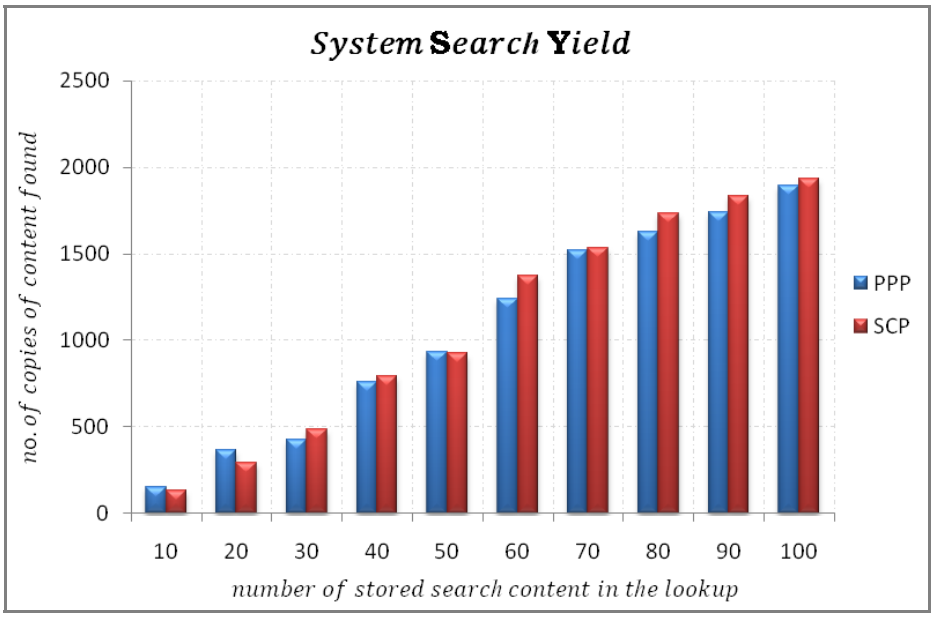


In Figure 5, the paths traversed by the search query across the network models differ significantly. In fact, the superpeer clusters stores the lookup tables for the various nodes located on the network; thereby simplifying the search distances covered. SCP network outclassed PPP network by 42.82% to 57.18%. This implied lesser paths are covered by SCP network in completing a full search (that is, minimised delays) when compared to the PPP network.

4.2.2 System search yield

The obtained during system search yield, which was carried out for PPP network and SCP network as illustrated Figure 6.

Figure 6 System search yield (see online version for colours)



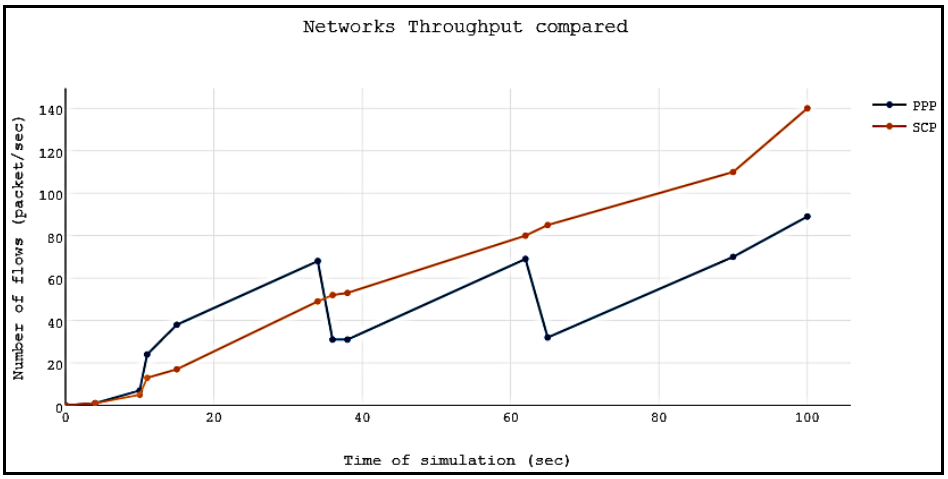
In Figure 6, the system search yield of the both networks slightly show similarity in terms of the number of copies of contents found search queries delivered. Both the PPP and SCP network model provides similar system search yield security standards for data created by different peers across the network.

4.2.3 Networks throughput compared

Throughput indices, which was carried out for PPP network and SCP network as illustrated Figure 7.

In Figure 7, the throughputs of the both networks slightly show similarity in terms of supports delivered. The SCP network model provides centralised control and common security standards for data created by different peers across the network. Evidence recovery during forensic activity was simplified because data and mobile devices were required to be declared and entered on the lookup tables, which ensured copies stored on network in order to increase reliability of user data and efficiency of the network model. The PPP network's throughput underperformed by 43.19% to 56.81% for the SCP network.

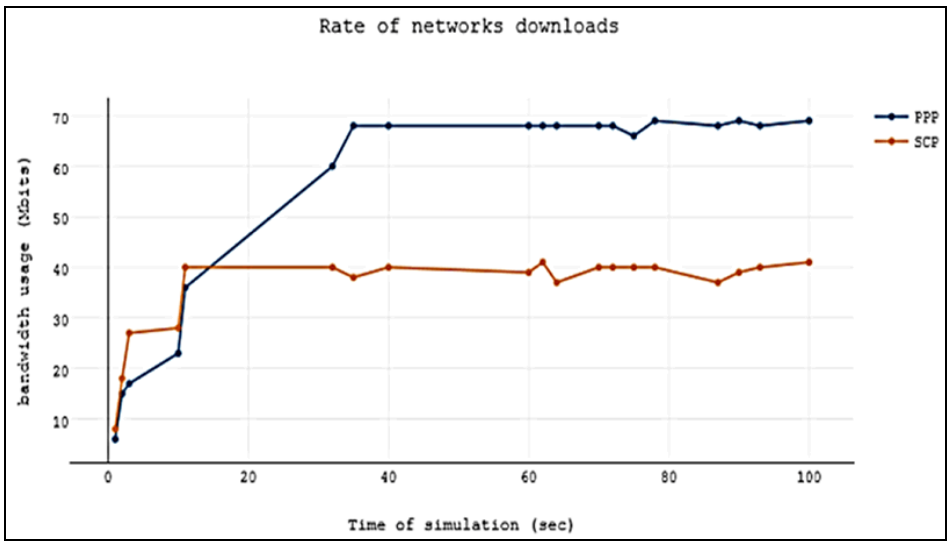
Figure 7 Network throughput for forensic audit compared for PPP and SCP (see online version for colours)



4.2.4 Rate of model utilisation

The rate of network utilisation indicates the traffic level supported by the different network models compared as shown in Figure 8.

Figure 8 Rate of network utilisation by forensic auditors (see online version for colours)



In Figure 8, the rate of network utilisation was slightly stable for SCP network because of the introduction of cache servers and superpeers clusters. The network traffic is higher for

PPP network at any point in time as the number of connections of mobile devices increases. The lack of coordination and control in the usage of the network resources cause higher network activity such as download. The request floods and user data duplications processes were higher in PPP network. The unauthorised access to the network by mobile devices made the PPP network unsalable and congested traffic. The SCP coordinates the network activities such as downloads because of the specialised superpeers clusters. The use of network resources required appropriate user authorisation that offered security. The data transmitted across the network were reliable due to common security standards defined for all mobile devices generating data from third party applications. The authenticity of user data or information passed on the network can be easily verified by forensic auditors. The overall performance score for SCP network was 35.41% against 64.59% scored by PPP network.

5 Conclusions

Third party applications on mobile devices have provided a veritable means for conducting forensic evidence recovery online by means of SCP network models. This acquires users' devices details and associated data and stores them on the network at different points to protect modification intentionally or accidentally. Physical connection of mobile devices was not required as in the case of previous methods to obtain forensic evidence data. The auditor's mobile device connects to the local cluster peer network in order to access devices generated data for scrutiny. Thereafter, information or data generated from third party applications were securely dumped onto several caches and servers for protection and integrity of data generated online across the network models.

The main contributions of this research work are; it helps in establishing evidence in the court of law and police report for criminal case through mobile forensic analysis. Academically, this research work has contributed to the advancement of mobile forensic analysis as a new area of research by the introduction of this model.

References

Abdulhamid, S.M. and Abd Latiff, M.S. (2017) 'A checkpointed league championship algorithm-based cloud scheduling scheme with secure fault tolerance responsiveness', *Applied Soft Computing*, Vol. 61, pp.670–680.

Abdulhamid, S.M., Abd Latiff, M.S., Chiroma, H., Osho, O., Abdul-Salaam, G, Abubakar, A.I. and Herawan T. (2017) 'A review on mobile sms spam filtering techniques', *IEEE Access*, DOI: 10.1109/ACCESS.2017.2666785.

Azfar, A., Choo, K.K.R. and Liu, L. (2017) 'Forensic taxonomy of android productivity apps', *Multimedia Tools and Applications*, Vol. 76, No. 3, pp.3313–3341.

Azhar, M.H.B. and Barton, T.E.A. (2017) 'Forensic analysis of secure ephemeral messaging applications on android platforms', in *International Conference on Global Security, Safety, and Sustainability*, January, pp.27–41, Springer, Cham.

Cafasso, M., Suarez, M., Lindfors, V. and Niemela, J. (2017) *U.S. Patent No. 9,591,019*, US Patent and Trademark Office. Washington, DC.

Candia, J., González, M.C., Wang, P., Schoenharl, T., Madey, G. and Barabási, A.L. (2008) 'Uncovering individual and collective human dynamics from mobile phone records', *Journal of Physics A: Mathematical and Theoretical*, Vol. 41, No. 22, p.224015.

Chang, X., Tang, X. and Wu, J. (2013) 'Forensic research on data recovery of android smartphone', *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering*, pp.1188–1191.

Choi, J., Park, J. and Kim, H. (2017) 'Forensic analysis of the backup database file in KakaoTalk messenger', in *Big Data and Smart Computing (BigComp), 2017 IEEE International Conference on*, February, pp.156–161, IEEE.

Choo, K.R. (2013) 'Cloud and mobile forensics: own cloud as a case study', *Digital Investigation*, Vol. 10, No. 4, pp.287–299.

Finneran, M.F. (2014) 'Mobile security and incident readiness: preparing for threats', *Gigaom Research*, Vol. 1, No. 1, pp.1–16.

Goode, A.J. (2003) 'Forensic extraction of electronic evidence from GSM mobile phones', *IEEE Seminar on Secure GSM and Beyond: End to End Security for Mobile Communications*, pp.91–96.

Jansen, W. and Ayers, R. (2007) 'Guidelines on cell phone forensics', *Recommendations of the National Institute of Standards and Technology*.

Kasiaras, D., Clarke, N., Zafeiropoulos, T. and Kambourakis, G. (2014) 'Android forensic data analyzer (AFDA): an open source tool to automatize event correlation analysis on android devices', *International Journal for Information Security Research*, Vol. 4, No. 4, pp.501–509.

Kausar, F. (2014) 'New research directions in the area of smart phone forensic analysis', *International Journal of Computer Networks and Communications*, Vol. 6, No. 4, pp.99–106.

Lin, Y., Huang, C., Wright, M., and Kambourakis, G. (2014) 'Mobile application security', *IEEE Computer Society*, Vol. 1, No. 1, pp.12–23.

Madni, S.H.H., Latiff, M.S.A., Abdullahi, M. and Usman, M.J. (2017) 'Performance comparison of heuristic algorithms for task scheduling in IaaS cloud computing environment', *PloS one*, Vol. 12, No. 5, p.e0176321.

Martini, B., Do, Q. and Choo, K.R. (2015) 'Conceptual evidence collection and analysis methodology for android devices', *Cloud Security Ecosystem*, Vol. 1, No. 1, pp.285–307.

Okongwu, N.O. and Adebayo, O.S. (2013) 'Cyber crimes analysis based-on open source digital foresics tools', *International Journal of Computer Science and Information Security*, Vol. 11, No. 1, p.30.

Osho, O., Yisa, V.L. and Ogunleke, O.Y. (2015) 'Mobile spamming in Nigeria: an empirical survey', in *Cyberspace (CYBER-Abuja), 2015 International Conference on*, November, pp.150–159, IEEE.

Rizzo, F., Spoto, G.L., Brizzi, P., Bonino, D., Di Bella, G. and Castrogiovanni, P. (2017) 'Beekup: a distributed and safe P2P storage framework for IoE applications', in *Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on*, March, pp.44–51, IEEE.

Smith, J., Lacey, D., Koenig, B. and Grigoras, C. (2017) 'Triage approach for the forensic analysis of Apple iOS audio files recorded using the 'voice memos' app', in *Audio Engineering Society Conference: 2017 AES International Conference on Audio Forensics, Audio Engineering Society*, June.

Tassone, C.F., Martini, B. and Choo, K.K.R. (2017) 'Visualizing digital forensic datasets: a proof of concept', *Journal of Forensic Sciences*, 162, No. 5, pp.1197–1204.

Walls, R.J., Miller, E.L. and Levine, B.N. (2011) 'Forensic triage for mobile phones with decode', *Proceedings of USENIX Security Symposium*, pp.1–14.

Willassen, S.Y. (2003) 'Forensics and the GSM mobile telephone system', *International Journal of Digital Evidence*, Vol. 2, No. 1, pp.1–17.

Wu, S., Zhang, Y., Wang, X., Xiong, X. and Du, L. (2017) 'Forensic analysis of WeChat on android smartphones', *Digital Investigation*, Vol. 21, pp.3–10.

Yusoff, M.N., Mahmod, R., Abdullah, M.T. and Dehghantanha, A. (2014) 'Performance measurement for mobile forensic data acquisition in Firefox OS', *International Journal of Cyber-Security and Digital Forensics*, Vol. 3, No. 3, pp.130–140.