Forensic Analysis of Mobile Banking Applications in Nigeria

Article *in* i-manager s Journal on Mobile Applications and Technologies · June 2019

DOI: 10.26634/jmt.6.1.15704

4 authors:

Andrew A Uduimoh
Federal University of Technology Minna
3 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Ismaila Idris
Federal University of Technology Minna
42 PUBLICATIONS **338** CITATIONS
SEE PROFILE

Oluwafemi Osho
Federal University of Technology Minna
39 PUBLICATIONS **244** CITATIONS
SEE PROFILE

Shafi'i Muhammad Abdulhamid
Federal University of Technology Minna
108 PUBLICATIONS **1,466** CITATIONS
SEE PROFILE

FORENSIC ANALYSIS OF MOBILE BANKING APPLICATIONS IN NIGERIA

By

ANDREW A. UDUIMOH *

OLUWAFEMI OSHO **

IDRIS ISMAILA ***

SHAFI'I M. ABDULHAMID ****

*-** Lecturer, Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria.
*** Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.
**** Senior Lecturer and Head, Department of Cyber Security Science, Federal University of Technology Minna, Nigeria.

Date Received: 11/01/2019 Date Revised: 26/01/2019 Date Accepted: 03/04/2019

ABSTRACT

Advancement in mobile technology has made smart mobile devices to provide users with functionalities, which make these devices virtually indispensable in today's world. Mobile device users can now perform tasks that in past could only be performed on a personal computer. This is made possible by the variety of applications that run on these devices, from basic utility applications to social networking applications, health applications, and even mobile banking applications. Forensic analysis and security assessment of mobile banking applications in some countries have shown that sensitive user data such as login credentials and transactions details can be retrieved from the internal memory and cache of mobile devices. In this work, forensic acquisition and analysis of five mobile banking applications in Nigeria are performed, using the Universal Forensic Extraction Device (UFED) Touch and Forensic Recovery of Evidence Device (FRED). Analysis shows similar results with previous studies: the mobile banking applications did retain valuable user data, including user login credentials and transaction details. Security and privacy of user data need to be given higher priority by developers and proprietors of these applications.

Keywords: Mobile Phone, Forensics, Mobile Banking, Android OS.

INTRODUCTION

The ubiquity of mobile devices and the kind of functionalities they provide their users have made them such indispensable tools. Growth in technological advancement has brought about various versions of mobile device with powerful functionalities, and processing capabilities, which have continued to increase. Today, these mobile devices can store large volume of information, including users' personal, commercial, and location data (Srivastava & Tapaswi, 2015). Consequently, more users are using mobile devices. About 5 billion people out of about 7.1 billion people own a mobile device (Al Mushcab & Gladyshev, 2015).

One sector in the mobile technology has increasingly become a veritable platform for extending services is the banking industry. This is known as mobile banking. Essentially, it is a banking services provided for customers to be able to carry out their banking functions through their mobile devices (Bezovski, 2016). Bank customers can receive information about their accounts and perform real financial transactions using their mobile devices (Garba, 2016). Reports have predicted that considering its rate of growth, estimated to be more than 40% annually, by 2020 mobile banking adoption would have exceeded traditional Internet banking (Iovation, 2012).

In Nigeria, the need for reduction in the cost of banking services and to improve financial inclusion, among other objectives, led to the introduction of a cashless policy in 2012 (Atanda & Alimi, 2012; Nweke, 2012). To a large extent, the progress made so far in the implementation of this policy owes much to the introduction of mobile banking services. Nigerian banks, today, offer a plethora of mobile banking services (Agu, Simon, & Onwuka, 2016).

Two key concerns in mobile banking are security and privacy (Adesuyi, Oluwafemi, Oludare, Victor, & Rick, 2013; Chanajitt, Viriyasitavat, & Choo, 2018). These requirements can influence the perception and acceptance of mobile banking. Mobile users, naturally, want to be assured of the security of their information when banking via their mobile phones (Bezovski, 2016; Dahunsi & Akinyede, 2014; Kamoru, 2014; Jumoke, Olugbenga, & Mudasin, 2015). One way mobile banking service providers enhance user security and privacy is by managing users' Personal Identifiable Information (PII) in a secure manner. This information include users' banking credentials and transaction data.

Regrettably, studies have shown that some mobile banking applications store users' credentials in plain text and other Personal Identifiable Information (PII) in the memory of mobile devices. The implication of this is that once a user's mobile phone is stolen by a criminal, sensitive data of forensic value can be extracted. This may lead to identity theft and financial loss, to mention but two.

A lot of research have explored the possibility of acquiring sensitive user and application data retained in mobile devices, e.g. (Srivastava & Tapaswi, 2015; Al Mutawa, Baggili, & Marrington, 2012; Dibb & Hammoudeh, 2013; Immanuel, Martini, & Choo, 2015; Walnycky, Baggili, Marrington, Moore, & Breitinger, 2015; Satrya, Daely, & Nugroho, 2016; Yang, Dehghantanha, Choo, & Muda, 2016; Azfar, Choo, & Liu, 2015; Al-Hadadi, & AlShidhani, 2013; Sgaras, Kechadi, & Le-Khac, 2014; Mahajan, Dahiya, & Sanghvi, 2013; Anglano, 2014; Sahu, 2014; Lone, Badroo, Chudhary, & Khalique, 2015; Jain, Sahu, & Tomar, 2015). Some of the applications considered include social networking and mobile health applications.

However, very few studies have focused on analysis of mobile banking applications. These include the works of (Chanajitt et al., 2018; Stirparo, Fovino, & Kounelis, 2013; Ntantogian, Apostolopoulos, Marinakis, & Xenakis, 2014).

Currently, to the best of our knowledge, there are no studies that have considered mobile banking applications in Nigeria. This paper focuses on the forensic analysis of five Android-based mobile banking applications in Nigeria. The objectives are to determine how much user data is generated and retained by the application after registration and performing transaction, and whether the data can be used to identify actions or transactions performed by the user. The choice of Android is due to its popularity and the fact that all the banks in Nigeria that offer mobile banking services have developed an Android version of their respective applications.

1. Literature Review

1.1 Android Operating System

Android is an open source operating system based on the Linux kernel. Over the last few years, it has gradually grown and currently account for the largest mobile market share. Development and maintenance of the platform is overseen by Android Open Source Project (AOSP). Since the first announcement of the first version, Android Apple Pie (Android 1.0) in 2007, successive versions have been released using the names of dessert in alphabetical order. The latest version is Android Oreo (8.1), released on December 5, 2017 (Summerson, 2018). Android versions older than 4.0 are no more supported by Google manufacturer or application developers, though a few devices still use these versions, they are now considered as "Legacy versions" and need to be updated to Android 4.0 and above (Hildenbrand, 2016).

1.2 Location of Data on Android Devices

The location of data in Android devices is closely tied to the state of the data. Basically, there are two states: data in transit and data at rest. Data can reside in a transit memory storage or a permanent memory storage.

1.2.1 Data in Transit

Data can reside in three locations: Random Access Memory (RAM), Network Service Provider, and the Cloud. Data, such as call, SMS, MMS logs, voice mail, Electronic Serial Number (ESN), International Mobile Subscriber Identity (IMSI), International Mobile Equipment Identity (IMEI), emails, web activity, and subscriber information can be retained for several days by service provider, depending on the law and regulation of the country. Important data, such as device site analysis and triangulation, which can be used to identify the location of the device user, can be retrieved from the service provider. Authentication passwords and password reset security response from application are cached on the volatile memory. Network interface data, open and listening sockets, Address Resolution Protocol, and authentication credentials can be retrieved from RAM memory (Heriyanto, 2013).

1.2.2 Data at Rest

Data at rest can be stored in any of these five locations; NAND-flash memory (non-volatile), memory like Secure Digital Card (SD card) and Embedded Multimedia Card (EMMC), removable media, such as Universal Integrated Circuit Card (UICC) also called Subscriber Identity Module card (SIM), and lastly, data backups for Android. Potential data, such as call logs, voice mail, SMS/MMS, voice mail, personal email, Google search history, web history, YouTube, pictures and videos, game history and interactions, geo-location, corporate email and attachments, user names and password, calendar items, instant messenger, and corporate files can be retrieved from NAND-Flash Memory and SD card/eMMC. UICC and SIM card store personal data, such as address list/contact list, IMSI, Integrated Circuit Card identity number (ICCID), Local Area Identity (LAI), allowed network information, key pin encryption, SMS, and EMS (Heriyanto, 2013).

1.3 Mobile Acquisition

The retrieval of data from the memory of mobile device is known as mobile acquisition. This is done by imaging a copy of the data on the mobile device and other peripherals connected to it (Yusoff, Mahmod, Abdullah, & Dehghantanha, 2014). One of the challenges often faced by forensic examiners borders on the type of acquisition to be used for a new brand of mobile device or software version. This is due to the frequent release of new brands of mobile devices, operating system platforms, and versions (Jonkers, 2010). Existing forensic tools will usually require to be updated by the developers before they can be used on the new device or software. As a matter of fact, currently, there are no forensic tools capable of retrieving all data on a mobile device. These tools are also limited to operating systems platforms. But as more forensic tools are developed, the way data is been acquired may be modified to accommodate more data type acquisition (Singh, Yadav, & Rastogi, 2015).

1.3.1 Manual Acquisition

Manual acquisition is done by having physical interaction with the Mobile device, going through the menu option of the device and gathering evidence from the display on the screen. There are some devices that are virtually impossible to be acquired by forensic tools; such devices can only be acquired by manual examination. Even devices that are supported by some tools still require some form of careful manual examinations, to supplement other acquisition methods. Care is required in manual acquisition as examiners could press a button that can trigger actions that can compromise data integrity, like the “send button” (ACPO, 2007). The procedures involved in manual examination can be quite long and tedious. For instance, some legislations require that photographs of each button pressed during examination must be taken (Jonkers, 2010).

1.3.2 Logical Acquisition

Logical acquisition is also known as files system acquisition. This is because the tools and techniques used interact with the file system of the storage (Kong, 2015). Logical acquisition accesses the files system of a mobile device and is able to acquire the entire file system. It provides information, such as time stamp, date, and location of file system. Data that is not deleted but allocated as unused memory can be retrieved by this method, but deleted data cannot be retrieved as logical acquisition does not access lower file systems. Logical acquisition method is largely supported by almost all devices (Singh et al., 2015).

1.3.3 Physical Acquisition

Physical acquisition involves imaging bit-by-bit, the internal memory of a mobile device. This acquisition method focuses on the physical storage of the device. Unlike logical acquisition, physical acquisition is able to access the lower files systems of a device and retrieve deleted data (Srivastava & Tapaswi, 2015).

Deleted data still remain on the disk, as it is only the link to the data location that is actually deleted and not the actual content of the data (Leom, DOrazio, Deegan, & Choo, 2015). Physical acquisition or extraction method might involve physically dismantling the device to remove the memory from the device using tool like Joined Test Action Group (JTAG), or using a boot loader to gain lowest access to the device. This procedure require skills and can damage the device (Barmpatsalou, Damopoulos, Kambourakis, & Katos, 2013). Due to the acquisition of deleted data, and the level of file system access, physical acquisition is more preferable in the forensic community than logical acquisition. Physical acquisition requires low level access.

1.3.4 Pseudo Physical Acquisition

Introduced by Klaver (Klaver, 2010), pseudo physical acquisition combines features of both logical and physical acquisitions (Barmpatsalou et al., 2013). For Windows mobile devices, it involves making a copy of the flash file system over an ActiveSync connection. It requires overwriting RAM and, maybe, flash memory by loading a dedicated dll into the device.

2. Materials and Methods

2.1 Materials and Tools

The materials and tools used are:

- Samsung GSM SGH-i747 Galaxy SIII: This mobile device runs Android version 4.4.2 known as KitKat. The specifications are displayed in Table 1.
- Cellebrite UFED Touch 4.0: Universal Forensic Extraction device is a mobile forensic tool, manufactured by an Israeli company known as Cellebrite. The device makes it possible for a forensic investigator to extract, decode, and analyse data in a way that is forensically sound and acceptable in the court of law. UFED supports Logical extraction, file system extraction, and physical extraction.
- Forensic Recovery Evidence Device (FRED): Forensic Recovery of Evidence Device (FRED) is a digital forensic workstation manufactured by Digital intelligence. It can be used to acquire digital evidence from digital devices such as hard disk, mobile phones, flash drives and Secure Digital (SD) cards. UFED Physical Analyzer and UFED Reader are data analysis applications to analyse dumped data, while the Physical Analyzer is used to analyse data extracted through physical extraction, and Reader is used to report the result of the analysis.
- SanDisk removable drive: This is a 32GB memory drive used to store data extracted from UFED Touch, which was later transferred to the FRED for analysis.
- Five mobile banking applications: These were downloaded from Google Play Store. Accounts were opened with the relevant banks.
- 1 Airtel SIM card: Used to access Internet services via Airtel network.

Characteristics	Value
OS	Android 4.4.2 KitKat
Network	GSM / HSPA / LTE
Dimension	136.6 x 70.6 x 8.6 mm (5.38 x 2.78 x 0.34 inch)
Weight	134 g (4.73 oz)
Chipset	Qualcomm MSM8960 Snapdragon S4 Plus
Resolution	720 x 1280 pixels (~306 ppi pixel density)
Processor	Dual-core 1.5 GHz Krait
Camera	8 MP, f/2.6, autofocus, LED flash, 2.0 MP Front Camera
Memory	16 GB, 2 GB RAM Expandable MicroSD, up to 64 GB
Connectivity	GPS, Wi- Fi. BT, Hot knot, OTG
Battery Capacity	Removable Li-Ion 2100 mAh
Sensor	1/3" sensor size, geo-tagging, touch focus, face/smile detection
SIM	Micro SIM
Screen	4.8 inches (~65.9% screen-to-body ratio)

Table 1. General Specification of Samsung Galaxy SIII

2.2 Acquisition Procedures

2.2.1 Manual Evaluation

The manually evaluation involves opening the application from the application manager to view application info. This will show if data is retained behind in the internal memory and the cache after performing transactions. This done by opening Settings>Application manager>All apps. This might be a little different for different Android devices. The secure mobile banking application and the selected mobile banking applications were used to perform financial transactions and the application information of the different Mobile banking applications were opened to show the data in size of the internal memory and cache.

2.2.2 Physical Extraction Procedures

The following steps were followed in carrying out the physical extraction:

- The mobile banking applications were downloaded from Google Play Store, installed and registered following the procedures of each banks.

- All the applications were used to perform transactions. Table 2 presents a summary of the transactions.
- The phone was left idle for thirty minutes after performing these transactions. Then the device was used for making call for about ten minutes. Within this waiting time, the UFED Touch was switched on and allowed to boot.
- Next the device was browsed and Samsung GSM SGH-i747 Galaxy SIII was selected. This gave an option for three different extraction types: logical, file, and physical extraction.
- Another page to choose between ADB and Bootloader was displayed. Bootloader option was selected.
- Then a page to choose where the extracted data will be stored was displayed. This page presented removable drive or Personal Computer (PC). Removable drive was selected.
- The SanDisk drive was then inserted into the USB port of the UFED touch.
- Selecting the continue option brought a page that displayed the instructions, which was followed in extracting the mobile device.
- The phone battery was then removed and reinserted (The phone battery was fully charged before experiment commenced).
- The phone was not powered on.
- Cellebrite extension cable A, with T-133 yellow head was connected to the phone, but the USB end of the extension cable was not connected to the UFED Touch.
- After the downloading mode appeared on the mobile phone screen, the USB end of the Cellebrite extension cable A was then connected to the USB port of the UFED Touch.
- Then continue was selected. The physical memory extraction was initialized. The extraction process, which produced a memory dump, lasted about four hour twenty-three minutes.

S/N	Banking App	Transfers	Airtime
1.	Bank A	600 to bank D	
2.	Bank B	3000 to bank E	Airtel Airtime 500
3.	Bank C	600 to bank A	Airtel Airtime 200
4.	Bank D	700 to bank C	Airtel airtime 200
5.	Bank E	500 to bank B	Airtel Airtime 400

Table 2. Summary of Transactions Performed on the Mobile Banking Applications

- After the extraction process was completed, the SanDisk drive was removed and the phone was disconnected from the UFED Touch.

2.2.3 Extracted Memory Analysis Procedures

For analysis of the dumped data, the following steps were undertaken:

- The SanDisk flash was inserted into the FRED workstation, which had UFED Physical Analyzer and UFED Reader installed on it.
- The Physical Analyzer was opened. It recognized the Samsung GSM SGH-i747 Galaxy SIII.
- The memory dump, in .bin format, was loaded into the computer memory, spanning about thirty minutes.
- The analysis page was then opened which had the physical image with different folders of the applications that were installed on the mobile device. Each of these application folders (with names like com.bankA.Amobile) were all carefully opened and analysed using database view, hex view, and file info view on the Physical Analyser page. The folders were specifically investigated for relevant user data, including login credentials and transaction details.

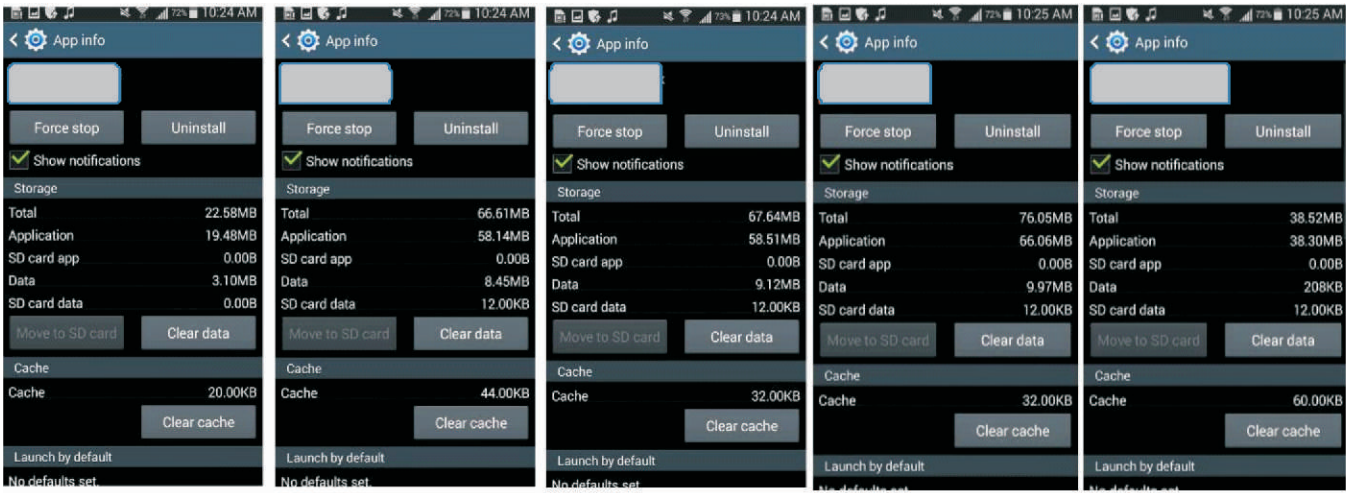
3. Findings

3.1 Manual Evaluation

Manual evaluation of the internal memory and cache of the mobile device revealed substantial user data generated and stored in the device memory after transactions had been performed. Figure 1 presents information on the five mobile banking applications. With the exception of the fifth app, which had 200 KB worth of user data generated, the average user data size for the four other apps was 7.66 MB, with range from 3.10 MB to 9.97 MB.

3.2 Forensic Acquisition and Analysis Evaluation

Presented in Table 3 are the specific user data extracted upon the forensic acquisition and analysis. Analysis showed that all of the mobile banking applications stored at least three PII of the users, including account number, account



10:24 AM
App info
[redacted]
Force stop | Uninstall
☑ Show notifications
Storage
Total 22.58MB
Application 19.48MB
SD card app 0.00B
Data 3.10MB
SD card data 0.00B
Move to SD card | Clear data
Cache
Cache 20.00KB
Clear cache
Launch by default
No defaults set.

10:24 AM
App info
[redacted]
Force stop | Uninstall
☑ Show notifications
Storage
Total 66.61MB
Application 58.14MB
SD card app 0.00B
Data 8.45MB
SD card data 12.00KB
Move to SD card | Clear data
Cache
Cache 44.00KB
Clear cache
Launch by default
No defaults set.

10:24 AM
App info
[redacted]
Force stop | Uninstall
☑ Show notifications
Storage
Total 67.64MB
Application 58.51MB
SD card app 0.00B
Data 9.12MB
SD card data 12.00KB
Move to SD card | Clear data
Cache
Cache 32.00KB
Clear cache
Launch by default
No defaults set.

10:25 AM
App info
[redacted]
Force stop | Uninstall
☑ Show notifications
Storage
Total 76.05MB
Application 66.06MB
SD card app 0.00B
Data 9.97MB
SD card data 12.00KB
Move to SD card | Clear data
Cache
Cache 32.00KB
Clear cache
Launch by default
No defaults set.

10:25 AM
App info
[redacted]
Force stop | Uninstall
☑ Show notifications
Storage
Total 38.52MB
Application 38.30MB
SD card app 0.00B
Data 208KB
SD card data 12.00KB
Move to SD card | Clear data
Cache
Cache 60.00KB
Clear cache
Launch by default
No defaults set.

Figure 1. Application Information of Mobile Banking Applications

S/No	Mobile banking App	Account Number	Account Balance	Account Type	Phone number	Registered E-mail	Transfer Details	Login Credentials
1.	A		✓	✓	✓			✓
2.	B	✓	✓		✓		✓	
3.	C	✓	✓		✓	✓	✓	
4.	D	✓	✓		✓		✓	
5.	E	✓			✓			

Table 3. Summary of User Data Forensically Retrieved from Mobile Banking Applications

balance, account type, phone number, cash transfer details, and login credentials. These data were stored in unencrypted form. In four each of the five mobile banking applications, the account number and balance were retrieved. In the case of apps B, C, and D, the transfer details were extracted in plaintext. Regrettably, user login details were found for app A during the investigation. This was in addition to the retrieval of other vital information, such as account balance, account type, and phone number of the user. Screenshots of results for the mobile banking apps are displayed in Appendix.

These results, which were not different from those discovered in (Chanajitt et al., 2018; Stirparo et al., 2013; Ntantogian et al., 2014) suggest the fact that security was not given due consideration in the development of those mobile applications.

Conclusion

The objectives of this study were to determine how much user data is generated and retained by the application after registration and performing transaction, and whether the data could be used to identify actions or transactions performed by the user. The findings revealed the storage of sensitive user personal and transaction data in the internal memory of the investigated mobile banking applications.

While functionality can easily influence the perception of an application, the need for privacy and security should not be neglected, especially for mobile applications that deal with sensitive user data.

Mobile banking applications should not retain any user data after the user logs out or the current session is timed out by the application. It is therefore pertinent that this and other security considerations must be deliberately built into the system architecture. There are existing guidelines that developers can consult to ensure secure mobile banking application development, e.g. the OWASP Mobile Application Security Verification Standard (OWASP).

Acknowledgment

We wish to appreciate the management of the National Information Technology Development Agency (NITDA) for granting us permission to use their CERRT Lab for our forensic investigation and analysis.

References

[1]. **ACPO. (2007).** Good Practice Guide for Computer-Based Electronic Evidence Official release version 4.0, *Good Pract. Guid. Comput. Electron. Evid*. (vol. 4).

[2]. **Adesuyi, F. A., Oluwafemi, O., Oludare, A. I., Victor, A. N., & Rick, A. V. (2013).** Secure authentication for mobile banking using facial recognition. *(IOSR-JCE) J. Comput.*

Eng., 10(3), 51-59.

[3] **Agu, B. O., Simon, N. P. N., & Onwuka, I. O. (2016).** Mobile banking-adoption and challenges in Nigeria. *International Journal of Innovative Social Sciences & Humanities Research,* 4(1), 17-27.

[4]. **Al Mushcab, R., & Gladyshev, P. (2015).** iPhone 5s Mobile Device.*Int. Work. Secur. Forensics Commun. Syst.* (pp. 146-151).

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

[6]. **Al-Hadadi, M., & AlShidhani, A. (2013).** Smartphone forensics analysis: A case study. *International Journal of Computer and Electrical Engineering,* 5(6), 576-580.

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

[8]. **Atanda, A. A., & Alimi, O. Y. (2012).** *Anatomy of Cashless Banking in Nigeria: What Matters?* (No. 41409). University Library of Munich, Germany.

[9]. **Azfar, A., Choo, K. K. R., & Liu, L. (2015).** Forensic taxonomy of popular Android mHealth apps. *arXiv preprint arXiv:1505.02905.*

[10]. **Barmpatsalou, K., Damopoulos, D., Kambourakis, G., &Katos, V. (2013).** A critical review of 7 years of mobile device forensics. *Digital Investigation,* 10(4), 323-349.

[11]. **Bezovski, Z. (2016).** The future of the mobile payment as electronic payment system. *European Journal of Business and Management,* 8(8), 127-132.

[12]. **Chanajitt, R., Viriyasitavat, W., & Choo, K. K. R. (2018).** Forensic analysis and security assessment of Android m-banking apps. *Australian Journal of Forensic Sciences,* 50(1), 3-19.

[13]. **Dahunsi, F. M., & Akinyede, R. O. (2014).** ICT perspectives on the feasibility analysis of the cashless economy in Nigeria. 7(5) 109-118.

[14]. **Dibb, P., & Hammoudeh, M. (2013).** Forensic data recovery from android os devices: an open source toolkit. In *2013 European Intelligence and Security Informatics Conference* (pp. 226-226). IEEE.

[15]. **Garba, F. A. (2016).** A new secured application based mobile banking model for Nigeria. *Int. J. Comput. Sci. Inf. Technol. Secur. (IJCSITS)*. 1-8.

[16]. **Heriyanto, A. P. (2013).** Procedures and tools for acquisition and analysis of volatile memory on android smartphones. *Australian Digital Forensics Conference.*

[17]. **Hildenbrand, J. (2016).** Inside the different Android Versions. *Android Central,* Retrieved from https://www.androidcentral.com/android-versions

[18]. **Immanuel, F., Martini, B., & Choo, K. K. R. (2015).** Android cache taxonomy and forensic process. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 1094-1101). IEEE.

[19]. **Iovation. (2012).** *Fighting Mobile Fraud: Protecting Businesses and Consumers from Cybercrime.* Retrieved from https://www.bankinfosecurity.com/whitepapers/fighting-mobile-fraud-protecting-businesses-consumers-from-w-594

[20]. **Jain, V., Sahu, D. R., & Tomar, D. S. (2015).** Evidence Gathering of Line Messenger on *iPhones. Int. J. Innov. Eng. Manag.*, 4(2), 1-9.

[21]. **Jonkers, K. (2010).** The forensic use of mobile phone flasher boxes. *Digital Investigation*, 6(3-4), 168-178.

[22]. **Jumoke, S., Olugbenga, S. B., & Mudasin, H. (2015).** Nigerian cashless culture: The open issues. *International Journal of Engineering Sciences*, 4(4), 51-56.

[23]. **Kamoru, O. K. (2014).** The prospects & problems of information technology in the banking industry in Nigeria. *IOSR J. Comput. Eng.,* 16(5), 1-8.

[24]. **Klaver, C. (2010).** Windows mobile advanced forensics. *Digital Investigation*, 6(3-4), 147-167.

[25]. **Kong, J. (2015).** Data extraction on MTK-based android mobile phone forensics. *Journal of Digital Forensics, Security and Law,* 10(4),1-12.

[26]. **Leom, M. D., DOrazio, C. J., Deegan, G., & Choo, K. K. R. (2015, August).** Forensic collection and analysis of thumbnails in android. In *2015 IEEE Trustcom / BigDataSE / ISPA* (Vol. 1, pp. 1059-1066). IEEE.

[27]. **Lone, A. H., Badroo, F. A., Chudhary, K. R., & Khalique, A. (2015).** Implementation of forensic analysis procedures for Whatsapp and Viber Android applications. *International*

Journal of Computer Applications, 128(12), 26-33.

[28]. Mahajan, A., Dahiya, M. S., & Sanghvi, H. P. (2013). Forensic analysis of instant messenger applications on Android devices. *International Journal of Computer Applications*, 68(8), 38-44.

[29]. Ntantogian, C., Apostolopoulos, D., Marinakis, G., & Xenakis, C. (2014). Evaluating the privacy of Android mobile applications under forensic analysis. *Computers & Security,* 42, 66-76.

[30]. Nweke, F. (2012). Nigeria in 2012: The Vision of Cash-less Economy. *Proceedings of the Nigeria Economic Summit Group..*

[31]. OWASP. (n.d). *OWASP Mobile Application Security Verification Standard v1.0.*

[32]. Sahu, S. (2014). An analysis of WhatsApp forensics in Android/smartphones. *International Journal of Engineering Research,* 3(5), 349-350.

[33]. Satrya, G. B., Daely, P. T., & Nugroho, M. A. (2016). Digital forensic analysis of Telegram Messenger on Android devices. In *2016 International Conference on Information & Communication Technology and Systems (ICTS)* (pp. 1-7). IEEE.

[34]. Sgaras, C., Kechadi, M., & Le-Khac, N. A. (2014). Forensic acquisition and analysis of Tango VoIP. *International Conference on Challenges in IT, Engineering and Technology (ICCIET 2014).*

[35]. Singh, V. N., Yadav, M., & Rastogi, P. (2015). A forensic approach for data acquisition of smart phones to meet the challenges of law enforcement perspective. *Journal of Indian Academy of Forensic Medicine*, 37(2), 183-186.

[36]. Srivastava, H., & Tapaswi, S. (2015). Logical acquisition and analysis of data from android mobile devices. *Information & Computer Security,* 23(5), 450-475.

[37]. Stirparo, P., Fovino, I. N., & Kounelis, I. (2013, October). Data-in-use leakages from Android memory-Test and analysis. In *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 701-708). IEEE.

[38]. Summerson, C. (2018). What's the Latest Version of Android? In *How-To Geek.* Retrieved from https://www.howtogeek.com/345250/whats-the-latest-version-of- android/ [Accessed: 12-Aug-2018].

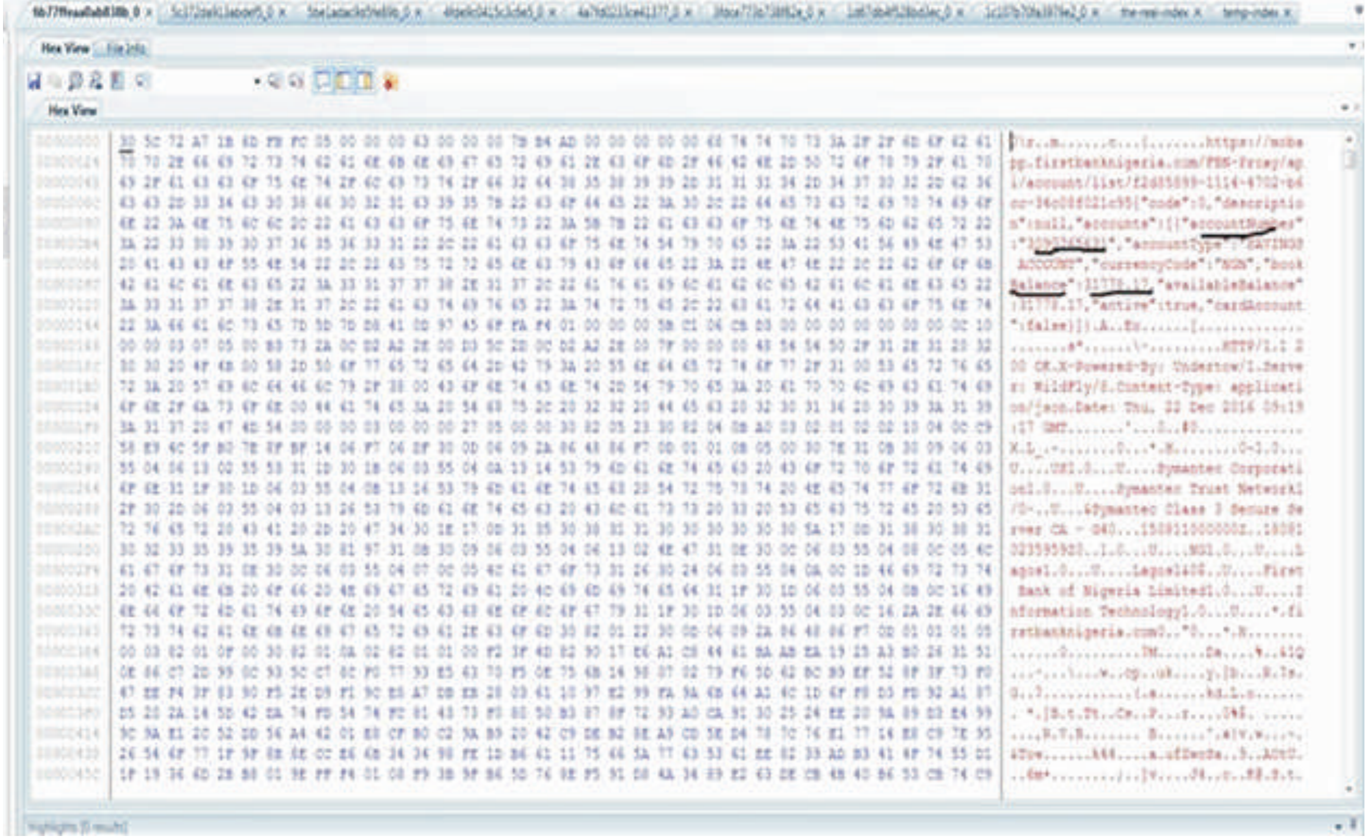
[39]. Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of Android social-messaging applications. *Digital Investigation,* 14, S77-S84.

[40]. Yang, T. Y., Dehghantanha, A., Choo, K. K. R., & Muda, Z. (2016). Windows instant messaging app forensics: Facebook and Skype as case studies. *PloS One,* 11(3), e0150300.

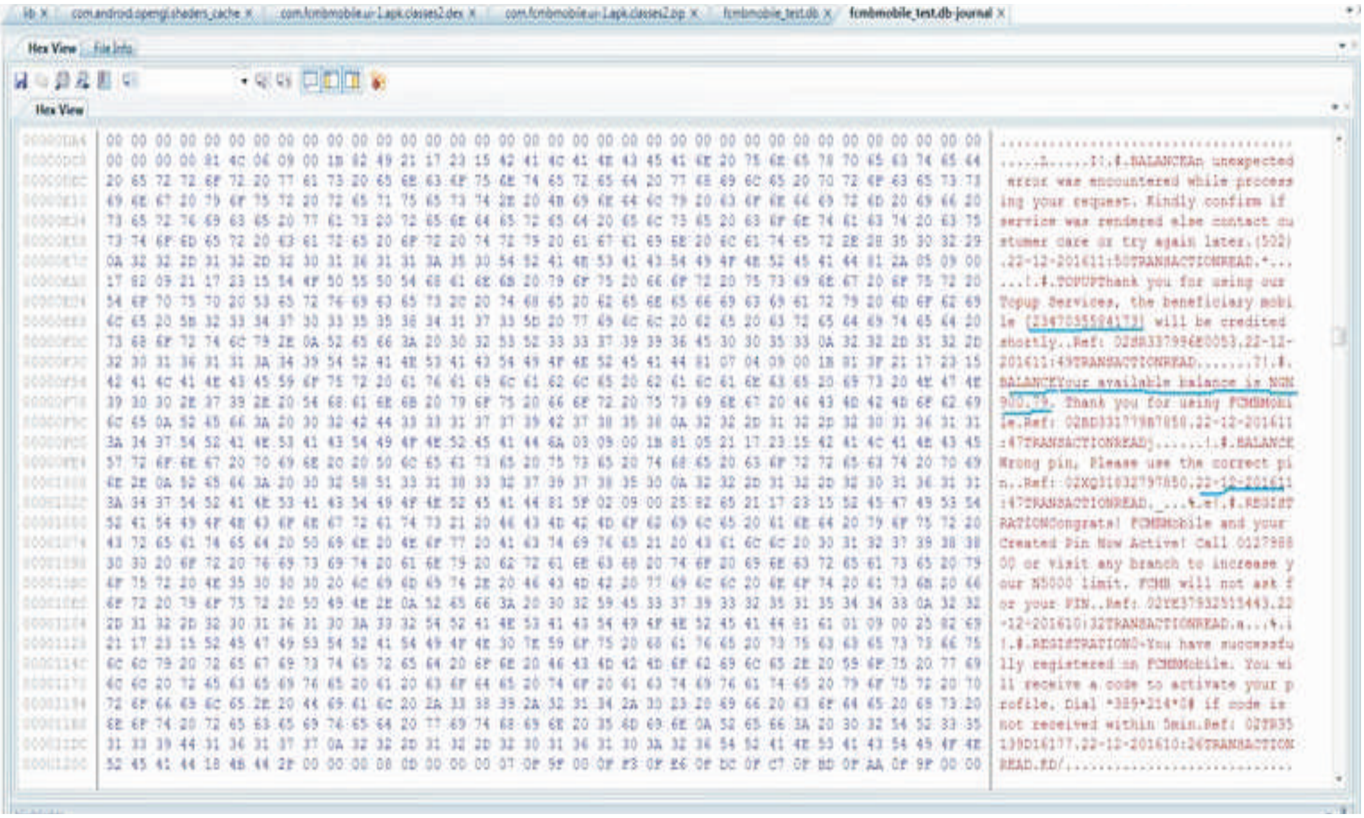
[41]. Yusoff, M. N., Mahmod, R., Abdullah, M. T., & Dehghantanha, A. (2014, April). Mobile forensic data acquisition in Firefox OS. In *2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 27-31). IEEE.

Appendix

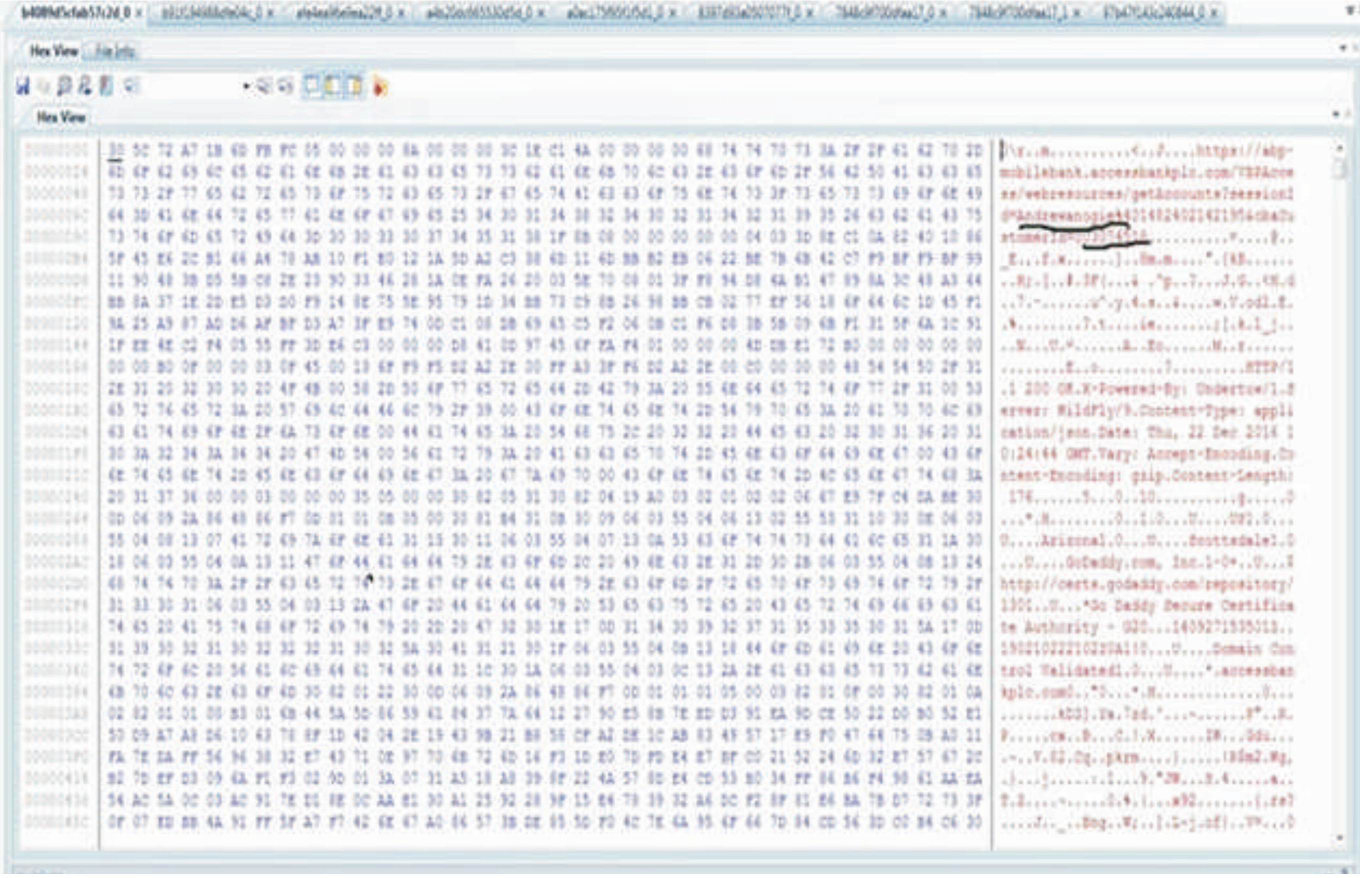
Screenshots of Extracted User Data From Mobile Banking Applications A - E respectively



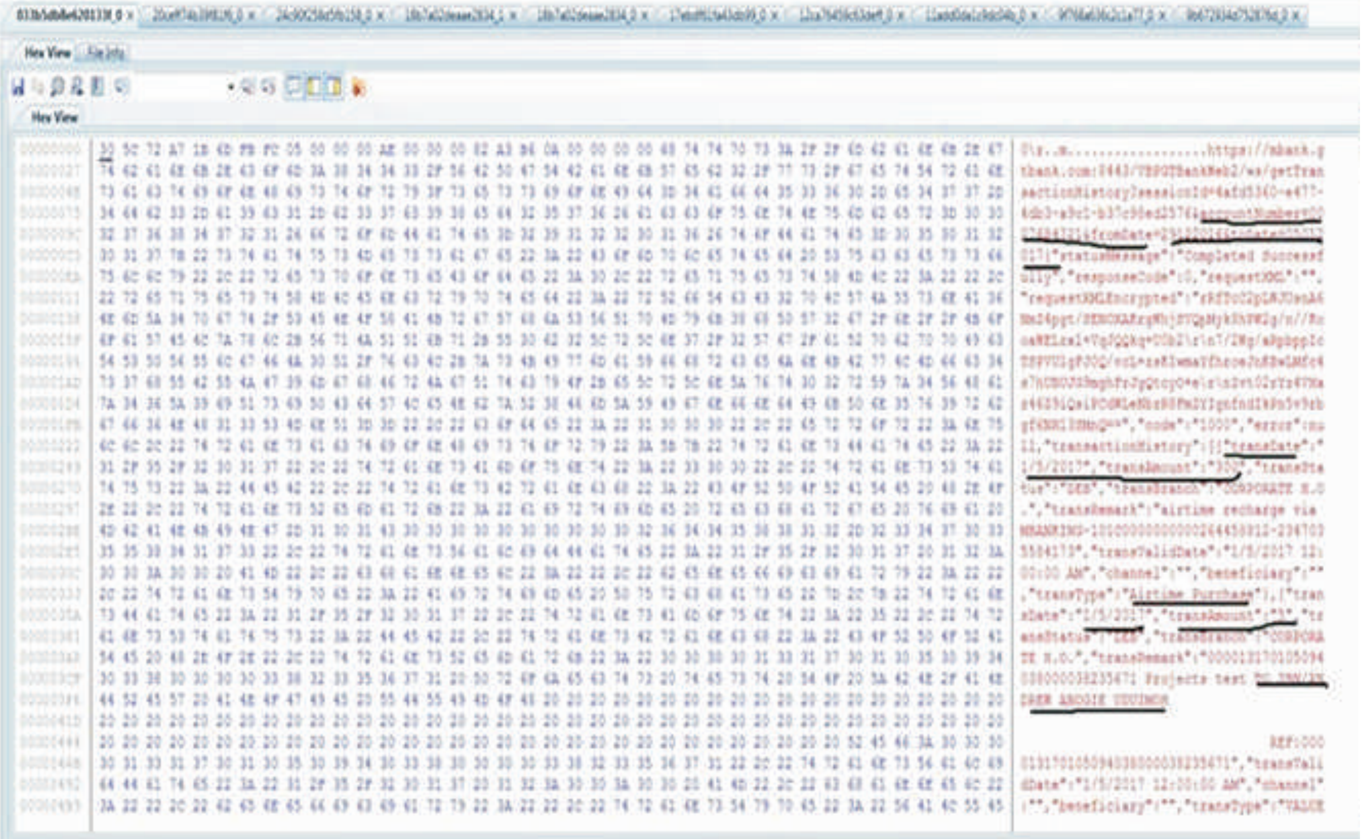
```
..r..m......c...{.......https://mobe
pp.firstbanknigeria.com/FBN-Frimy/ap
i/account/list/f2d85899-1114-4702-b4
cc-36c08f021c95{"code":0,"descriptio
n":null,"accounts":[{"accountNumber"
:"3093345433","accountType":"SAVINGS
 ACCOUNT","currencyCode":"NGN","book
Balance":31778.17,"availableBalance"
:31778.17,"active":true,"cardAccount
":false}]}.A..Ex......[.............
........e".....\-..........HTTP/1.1 2
00 OK.X-Powered-By: Undertow/1.Serve
r: WildFly/8.Content-Type: applicati
on/json.Date: Thu, 22 Dec 2016 09:19
:17 GMT........'...0..#0............
X.L_.-........0....*.H.........0-1.0...
U....US1.0...U....Symantec Corporati
on1.0...U....Symantec Trust Network1
/0-...U....&Symantec Class 3 Secure Se
rver CA - G40...150811000000Z..18081
023595920..1.0...U....NG1.0...U....L
agos1.0...U....Lagos1402..U....First
 Bank of Nigeria Limited1.0...U....I
nformation Technology1.0...U....*.fi
rstbanknigeria.com0.."0...*.H.......
......0..........TM.......Ca....\..4tQ
...^...\...w..cp..uk....y.[b...R.Ts.
G..?.................(.e......hd.L.o.......
. *.[B.t.Tt..Ce..P...r....O4$. .....
....R.T.R....... B......'.#|V.w....%.
4Tow......A44.....a.ufDeda...5..AdtU.
..Gm+..........j..]v.....J4..c..#8.3.t.
```


lib
com.android.opengl.shaders_cache
com.fcmbmobile.ui-1.apk.classes2.dex
com.fcmbmobile.ui-1.apk.classes2.zip
fcmbmobile_test.db
fcmbmobile_test.db-journal
Hex View
File Info
Hex View

```
....................................
.....Z......!!.#.BALANCEAn unexpected
 error was encountered while process
ing your request. Kindly confirm if
service was rendered else contact cu
stomer care or try again later.(502)
.22-12-201611:50TRANSACTIONREAD.*...
...!.#.TOPUPThank you for using our
Topup Services, the beneficiary mobi
le (2347035594173) will be credited
shortly..Ref: 02SR337996E0053,22-12-
201611:49TRANSACTIONREAD.......7!.#.
BALANCEYour available balance is NGN
900.79. Thank you for using FCMBMobi
le.Ref: 02BD331779B7050,22-12-201611
:47TRANSACTIONREADj.......!.#.BALANCE
Wrong pin, Please use the correct pi
n..Ref: 02XQ31032797850,22-12-201611
:47TRANSACTIONREAD._...%.e!.#.REGIST
RATIONCongrats! FCMBMobile and your
Created Pin Now Active! Call 0127988
00 or visit any branch to increase y
our N5000 limit. FCMB will not ask f
or your PIN..Ref: 02YE37932515443,22
-12-201610:32TRANSACTIONREAD.a...%.i
!.#.REGISTRATION0-You have successfu
lly registered on FCMBMobile. You wi
ll receive a code to activate your p
rofile. Dial *389*214*0# if code is
not received within 5min.Ref: 02TB35
139D16177,22-12-201610:26TRANSACTION
READ.8D/............................
```

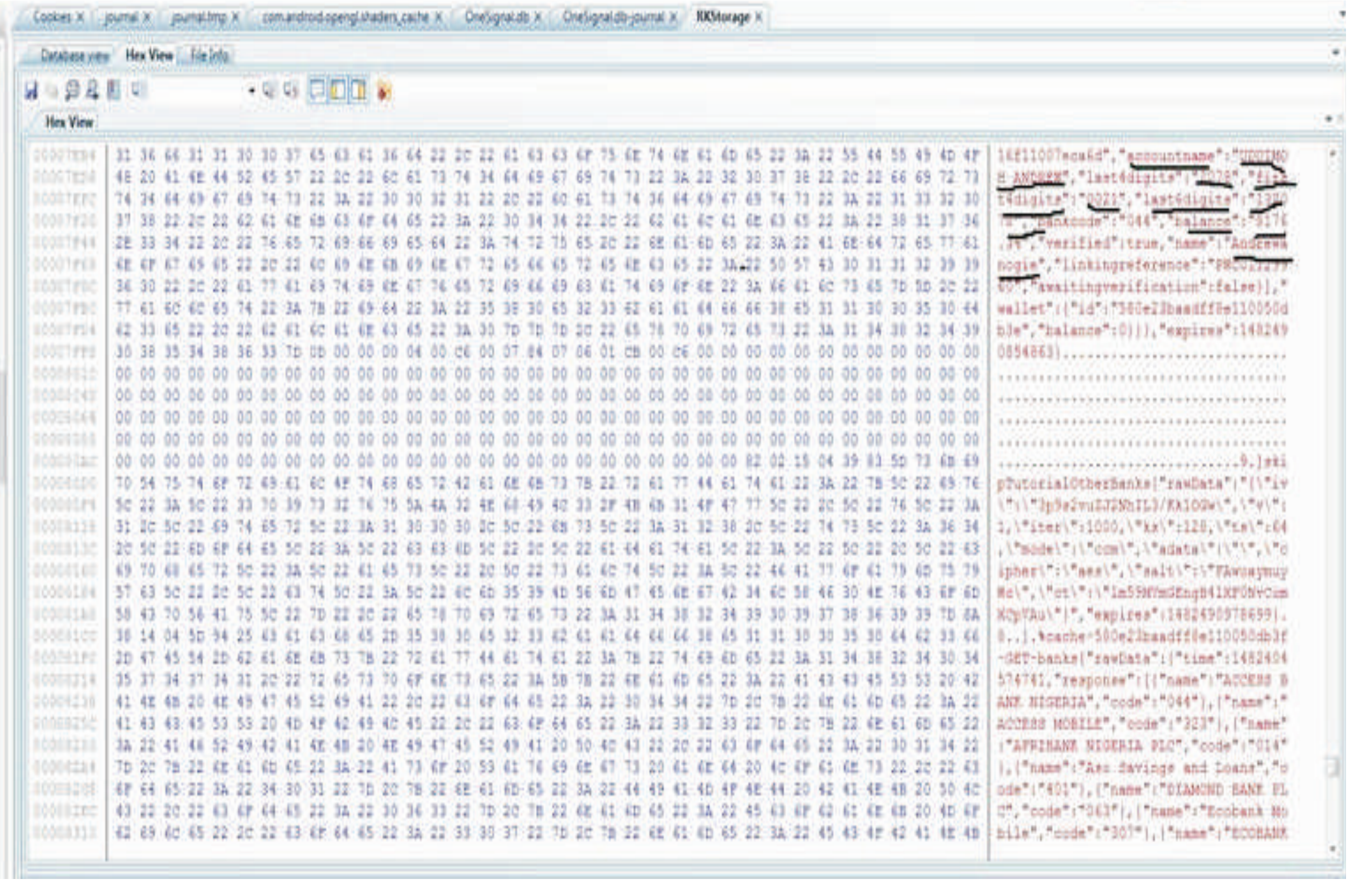


```
?\r..m..........<..?....https://abp-
mobilebank.accessbankplc.com/VBPAcce
ss/webresources/getAccounts?sessionI
d=Andrewanogie442148240214219S4cha3u
stomerID=[illegible]..........?....?..
_E...f.x......]..Um.m.....".[AB......
..R;.[..$.3F(...4 .^p..7...J.G..4N.d
..?.~.......w^.y.4.s..4.....w.Y.od1.E.
.%........7.t....i#........;[.&.1_]..
..N...U.*.....A..Eo.......M..#......
........E..o........?.........HTTP/1
.1 200 OK.X-Powered-By: Undertow/1.S
erver: WildFly/9.Content-Type: appli
cation/json.Date: Thu, 22 Dec 2016 1
0:24:44 GMT.Vary: Accept-Encoding.Co
ntent-Encoding: gzip.Content-Length:
 176......5...0..10...........$.....0
...*.H.........0..1.0...U....US1.0...
0....Arizona1.0...U....Scottsdale1.0
...U....GoDaddy.com, Inc.1-0+..U...
http://certs.godaddy.com/repository/
1301..U...*Go Daddy Secure Certifica
te Authority - G20...140927153511..
150210222102Z0A1!0...U....Domain Con
trol Validated1.0...U....*.accessban
kplc.com0..*0...*.H...............0...
........A0D}.Ym.Tad."....~.......$*..R.
P......cm...B....C.1.X........IW...Gdu..
.~..Y.G2.Cq..pkrm.....}......!BGm2.Wg.
..}....}......r.1....?.*JW....S.4......a..
T.S.........5.4.(....a92........{.fe?
....J.._..Bog..W;..].L~j.df|..Y*...0
```



```
0\r..m.....................https://mbank.g
tbank.com:8443/TBPGTBankWeb2/ws/getTran
sactionHistory?sessionId=4afd5360-e477-
4db3-a9c1-b37c96ed257d&accountNumber=00
[illegible]&fromDate=2[illegible]&toDate=[illegible]
017|"statusMessage":"Completed Successf
ully","responseCode":0,"requestXML":"",
"requestXMLEncrypted":"rKfDoC2pLAJOenA4
Nm24pgt/XENOKARrqMhjSTQgMykBNfWGg/n//Rc
oaMZLcal+VqJQQkq+OObI\r\nT/2Wp/mPgbppIc
TSPVOlgFJOQ/ecL+zeKlwmaYfhcoeJcRSwLMfc4
e7hCMOJ3MeghFrJpQtcyO+e\r\n2vt02zYz4YMa
z4635QslPC0RLeNbz8BFmZYIgnfndIkPn5v9zb
gfKNR13NhQ==","code":"1000","error":nu
ll,"transactionHistory":[{"transDate":"
1/5/2017","transAmount":"300","transSta
tus":"DEB","transBranch":"CORPORATE H.O
.","transRemark":"airtime recharge via
MBANKING-1010000000000264450812-234703
5584173","transValidDate":"1/5/2017 12:
00:00 AM","channel":"","beneficiary":""
,"transType":"Airtime Purchase"},{"tran
sDate":"1/5/2017","transAmount":"5","tr
ansStatus":"DEB","transBranch":"CORPORA
TE H.O.","transRemark":"000013170105094
0380000038235471 Projects test TC_TRN/IN
DREW ANOGIE UDUIMOR

                                 REF:000
0131701050940380000038235471","transVali
dDate":"1/5/2017 12:00:00 AM","channel"
:"","beneficiary":"","transType":"VALUE
```



```
31 36 66 31 31 30 30 37 65 63 61 36 64 22 2C 22 61 63 63 6F 75 6E 74 6E 61 6D 65 22 3A 22 55 44 55 49 4D 4F   16f11007eca6d","accountname":"[redacted]
48 20 41 4E 44 52 45 57 22 2C 22 6C 61 73 74 34 64 69 67 69 74 73 22 3A 22 32 30 37 38 22 2C 22 66 69 72 73   [redacted]","last4digits":"[redacted]","[redacted]
74 34 64 69 67 69 74 73 22 3A 22 30 30 32 31 22 2C 22 6C 61 73 74 36 64 69 67 69 74 73 22 3A 22 31 33 32 30   t4digits":"[redacted]","last6digits":"[redacted]
37 38 22 2C 22 62 61 6E 6B 63 6F 64 65 22 3A 22 30 34 34 22 2C 22 62 61 6C 61 6E 63 65 22 3A 22 38 31 37 36   [redacted]","bankcode":"044","balance":"[redacted]
2E 33 34 22 2C 22 76 65 72 69 66 69 65 64 22 3A 74 72 75 65 2C 22 6E 61 6D 65 22 3A 22 41 6E 64 72 65 77 61   [redacted]","verified":true,"name":"[redacted]
6E 6F 67 69 65 22 2C 22 6C 69 6E 6B 69 6E 67 72 65 66 65 72 65 6E 63 65 22 3A 22 50 57 43 30 31 31 32 39 39   nogie","linkingreference":"[redacted]
36 30 22 2C 22 61 77 61 69 74 69 6E 67 76 65 72 69 66 69 63 61 74 69 6F 6E 22 3A 66 61 6C 73 65 7D 5D 2C 22   [redacted]","awaitingverification":false}],"
77 61 6C 6C 65 74 22 3A 7B 22 69 64 22 3A 22 35 38 30 65 32 33 62 61 61 64 66 66 38 65 31 31 30 30 35 30 64   wallet":{"id":"580e23baadff8e110050d
62 33 65 22 2C 22 62 61 6C 61 6E 63 65 22 3A 30 7D 7D 7D 2C 22 65 78 70 69 72 65 73 22 3A 31 34 38 32 34 39   b3e","balance":0}}},"expires":148249
30 38 35 34 38 36 33 7D 0D 00 00 00 04 00 C6 00 07 84 07 06 01 CB 00 C6 00 00 00 00 00 00 00 00 00 00 00 00   0854863}............................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ....................................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 82 02 15 04 39 83 5D 73 6B 69   ..............................9.]ski
70 54 75 74 6F 72 69 61 6C 4F 74 68 65 72 42 61 6E 6B 73 7B 22 72 61 77 44 61 74 61 22 3A 22 7B 5C 22 69 76   pTutorialOtherBanks{"rawData":"{\"iv
5C 22 3A 5C 22 33 70 39 73 32 76 75 5A 4A 32 4E 68 49 4C 33 2F 4B 6B 31 4F 47 77 5C 22 2C 5C 22 76 5C 22 3A   \":\"3p9s2vuZJ2NhIL3/KA1OGw\",\"v\":
31 2C 5C 22 69 74 65 72 5C 22 3A 31 30 30 30 2C 5C 22 6B 73 5C 22 3A 31 32 38 2C 5C 22 74 73 5C 22 3A 36 34   1,\"iter\":1000,\"ks\":128,\"ts\":64
2C 5C 22 6D 6F 64 65 5C 22 3A 5C 22 63 63 6D 5C 22 2C 5C 22 61 64 61 74 61 5C 22 3A 5C 22 5C 22 2C 5C 22 63   ,\"mode\":\"ccm\",\"adata\":\"\",\"c
69 70 68 65 72 5C 22 3A 5C 22 61 65 73 5C 22 2C 5C 22 73 61 6C 74 5C 22 3A 5C 22 46 41 77 6F 61 79 6D 75 79   ipher\":\"aes\",\"salt\":\"FAwoaymuy
57 63 5C 22 2C 5C 22 63 74 5C 22 3A 5C 22 6C 6D 35 39 4D 56 6D 47 45 6E 67 42 34 6C 58 46 30 4E 76 43 6F 6D   Wc\",\"ct\":\"lm59MVmGEngB4lXF0NvCom
58 43 70 56 41 75 5C 22 7D 22 2C 22 65 78 70 69 72 65 73 22 3A 31 34 38 32 34 39 30 39 37 38 36 39 39 7D 8A   XCpVAu\"}","expires":1482490978699}.
38 14 04 5D 34 25 63 61 63 68 65 2D 35 38 30 65 32 33 62 61 61 64 66 66 38 65 31 31 30 30 35 30 64 62 33 66   8..].%cache-580e23baadff8e110050db3f
2D 47 45 54 2D 62 61 6E 6B 73 7B 22 72 61 77 44 61 74 61 22 3A 7B 22 74 69 6D 65 22 3A 31 34 38 32 34 30 34   -GET-banks{"rawData":{"time":1482404
35 37 34 37 34 31 2C 22 72 65 73 70 6F 6E 73 65 22 3A 5B 7B 22 6E 61 6D 65 22 3A 22 41 43 43 45 53 53 20 42   574741,"response":[{"name":"ACCESS B
41 4E 4B 20 4E 49 47 45 52 49 41 22 2C 22 63 6F 64 65 22 3A 22 30 34 34 22 7D 2C 7B 22 6E 61 6D 65 22 3A 22   ANK NIGERIA","code":"044"},{"name":"
41 43 43 45 53 53 20 4D 4F 42 49 4C 45 22 2C 22 63 6F 64 65 22 3A 22 33 32 33 22 7D 2C 7B 22 6E 61 6D 65 22   ACCESS MOBILE","code":"323"},{"name"
3A 22 41 46 52 49 42 41 4E 4B 20 4E 49 47 45 52 49 41 20 50 4C 43 22 2C 22 63 6F 64 65 22 3A 22 30 31 34 22   :"AFRIBANK NIGERIA PLC","code":"014"
7D 2C 7B 22 6E 61 6D 65 22 3A 22 41 73 6F 20 53 61 76 69 6E 67 73 20 61 6E 64 20 4C 6F 61 6E 73 22 2C 22 63   },{"name":"Aso Savings and Loans","c
6F 64 65 22 3A 22 34 30 31 22 7D 2C 7B 22 6E 61 6D 65 22 3A 22 44 49 41 4D 4F 4E 44 20 42 41 4E 4B 20 50 4C   ode":"401"},{"name":"DIAMOND BANK PL
43 22 2C 22 63 6F 64 65 22 3A 22 30 36 33 22 7D 2C 7B 22 6E 61 6D 65 22 3A 22 45 63 6F 62 61 6E 6B 20 4D 6F   C","code":"063"},{"name":"Ecobank Mo
62 69 6C 65 22 2C 22 63 6F 64 65 22 3A 22 33 30 37 22 7D 2C 7B 22 6E 61 6D 65 22 3A 22 45 43 4F 42 41 4E 4B   bile","code":"307"},{"name":"ECOBANK
```

ABOUT THE AUTHORS

Andrew Anogie Uduimoh, is a Lecturer in the Department of Cyber Security Science at School of Information and Communication Technology, Federal University of Technology (FUT) Minna, Nigeria. He received his B.Tech. in Mathematics/Computer Science, M.Tech. in Cyber Security Science from the Federal University of Technology (FUT) Minna. His areas of research interest includes Cyber Security, Digital Forensics, Mobile Forensics, Mobile Security, Machine Learning, Artificial Intelligence in Information Assurance Security, and Cyber Physical Systems.

Oluwafemi Osho is currently a Lecturer in the Department of Cyber Security Science at Federal University of Technology, Minna, Nigeria. Prior to this position, he headed the IT/Systems Department in one of the leading mortgage banks in Nigeria. A Certified Ethical Hacker (CEH), with expertise in cybersecurity, privacy, and trust. He is a member of different National and International Associations, including Global Commission for the Stability of the Cyberspace Research Advisory Group (GCSC-RAG) and Cyber Security Experts Association of Nigeria (CSEAN). Oluwafemi has published more than thirty research papers in reputable Journals, Conference proceedings, and other platforms.

Idris Ismaila is a consultant with a vast experience in the field of Cyber Security. He has lead and coordinated International Conferences on Cyber Security and has published many research papers in the field. He has two patent works with Innovation and Commercialization Centre (ICC), Malaysia. He is a member of editorial board of Journal of Computer Engineering and Information Technology and International Journal of Artificial Intelligence and Applications (IJAIA). His research interests include Digital Forensics, Malware Detection, Information Security, Data Mining, Computational intelligence, and Information Retrieval. He is a member board of trustee Cyber Security Experts Association of Nigeria and also the National Vice President of the Association, member of International Association of Engineers (IAENG), member of Association for Computing Machinery (ACM), and member of Computer Professionals Registration Council of Nigeria (CPN).

Dr. Shafi'i Muhammad Abdulhamid received his PhD in Computer Science from University of Technology Malaysia (UTM), MSc in Computer Science from Bayero University Kano (BUK), Nigeria, and a Bachelor of Technology in Mathematics/Computer Science from the Federal University of Technology (FUT) Minna, Nigeria. His current research interests are in Cyber Security, Cloud Computing, Soft Computing, Internet of Things Security, Malware Detection, and Big Data. 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 (BDCI) and Journal of Computer Science and Information Technology (JCSIT). He has also been appointed as a reviewer of several ISI and Scopus indexed International Journals. He has also served as Program Committee (PC) member in many National and International Conferences. He is one of the pioneer instructors at the Huawei Academy of FUT Minna and a holder of Huawei Certified Network Associate (HCNA). He is as well a member of IEEE Computer Society, International Association of Computer Science and Information Technology (IACSIT), Computer Professionals Registration Council of Nigeria (CPN), International Association of Engineers (IAENG), The Internet Society (ISOC), Cyber Security Experts Association of Nigeria (CSEAN) and Nigerian Computer Society (NCS). Presently, he is a Senior Lecturer and Head of Department (HOD) of Cyber Security Science, Federal University of Technology Minna, Nigeria. He is also supervising both Masters and PhD students (in both Nigeria and Malaysia).