International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Firefox OS Forensics: Guidelines and Challenges

Rakesh T[1], Anu Rachel Abraham[2]

[12] Department of Computer Science and Engineering, College of Engineering Kallooppara, Kerala, India

Abstract*: The smartphone technology has progressed and appealed many companies in developing mobile operating systems. Mozilla Corporation lately released Linux-based open source mobile OS, termed Firefox OS. The advent of Firefox OS has created novel challenges, concentrations and prospects for digital investigators. Hence, forensic analysis for Firefox OS is straightway needed in order to investigate any criminal objectives. At present Mobile forensics tools can only obtain and scrutinize the removable media of such devices and still not able to do analysis with the internal storage or system data. Forensic acquisition and analysis of Firefox OS based device found from a crime scene is challenging due to lack of technologies and methods to acquire and analyze internal file system and application logs etc. This paper debates the challenges in accomplishing complete analysis of such devices in a Forensic way and strategies for the investigators to investigate the criminal cases effortlessly and find out the evidences that are admissible in court.*

Keywords*:* Firefox OS**,** Mobile Forensics, Preservation, Acquisition, Forensic Process

1. Introduction

Mozilla Corporation has lately released a Linux-based open source operating system, namely Firefox OS. This has created a dare for digital investigators in acquiring and analyzing evidences from devices running in Firefox OS that found in an event of crime. There are more to discover in mobile forensic procedures that are suitable for Firefox OS. Present Mobile forensics tools can only acquire and analyze the removable media of such devices and still not able to do analysis with the internal storage or system data. The technical aspect of an investigation is separated into different sub branches, relating to the type of digital devices involved: Computer forensics, forensic data analysis, Network forensics and mobile device forensics. Mobile phones are significant part of our lives and they are used in our day-to-day lives because of their features. Smart phones are analogous to business laptops. Nowadays smart phones that are used in criminal acts also investigates the criminal cases. Smart phones are used in digital forensics to catch out the evidence so that it can be presented in court and accepted by the court. The criminal cases are resolved by saving the data in the phone applications. Currently smart phones also play an important part in digital forensics. Smartphones can achieve the same functionality of computers, so there are potential evidences in the phone memory and SD card which may be evidence.

These are the common evidence that can be obtained from a mobile device: -

- Call logs
- Text messages
- Camera
- Contacts
- Calendar
- Deleted files

Existing Smartphone forensic techniques are limited to various platforms like

- IOS
- Android
- Blackberry OS etc.

The forensic investigator or analyst will want evidence of the crime. In most types of crimes there are four phases conducted in mobile forensics Investigation: -

- Preservation
- Acquisition
- Analysis
- Presentation

In first phase of preservation, the forensic agent preserves the evidences. The crime scene is isolated and then the evidences are documented. The Smartphone device is placed in a faraday cage that is used to safeguard the device from the rays, as there should not be any changes in the data. Second phase is acquisition phase in this phase cloning is done on SD card, phone memory, SIM card. The next phase is analysis phase. In this phase, the evidences are analyzed. Investigator decides in this phase which tool to use for the forensic analysis. Then finally the last phase is the presentation phase. In this phase all the evidences are documented and presented.

2. Process and Challenges

In this section, we give a sketch of the main steps to be carried out during the mobile forensics procedure on Firefox OS mobile device. A few issues that could be faced while performing them are listed.

In most types of crimes, the below four phases are conducted in mobile forensics Investigation: -

A. Preservation
B. Acquisition
C. Analysis
D. Presentation

A. Preservation

This phase is very significant in digital forensics; in this phase the investigator preserves the device in its original form. In this phase the cell phones that are involved in the activity are seized, so that

there should not be any change in the evidences. Seizing the mobile device means to cut off all the wireless networks. Any failure in this stage can result in the failure of all the further stages. The aim of seizure is to preserve the evidence before it shuts down.

Preservation encompasses the search, recognition, documentation, and collection of electronic-based evidence. For presenting the evidence successfully, either in a court of law or a less formal proceeding, it should be preserved. Failure to preserve evidence in its original state could risk an entire investigation, possibly losing valuable case-related information. This step is performed by the initial responders who first reach at the scene. Their prime task is to secure and barricade off the scene and ensure the security of all individuals. Then, the entire scene is logged/documented using any media of recording. This is done to generate a perpetual record of the scene.

There are three basic steps involved:

- **Safeguarding and Evaluating the Scene:**

This step safeguards that the mobile device found is with proper authorizations for the commencement of the investigation. If the device is not handled properly then it may cause data loss. Also other biometric examination procedure like fingerprinting or DNA tests are conducted to establish the link between the device and owner, so if the device is not taken care of properly physical evidence may also be contaminated.

- **Documenting the Crime Scene:**

Documenting includes possessing the record of all the visible data on the mobile device. This is done chiefly for the non-electronic evidence such as invoices, manuals and packaging material. This delivers useful facts & figures regarding capabilities of the device, the network used, account information and PIN codes.

- **Isolation:**

Isolating the mobile devices from the other devices used for data synchronization is vital to keep new data from contaminating existing data. For example, if the mobile phone is found in water and then if it is connected with a personal computer then disconnecting a plug from the computer overwrites the data or the data is lost.

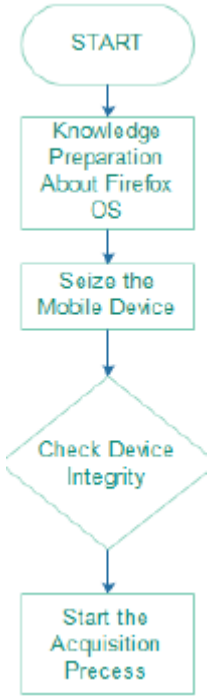

Figure 1: Preservation Phase for Firefox OS forensics

B. Acquisition

The second phase is acquisition phase after the preservation on the device is done. This part starts when the device is received at the forensic lab. In this phase the model and type of device is recognized. After this, the right tool for the acquisition is to be chosen since it is tedious due to the many no of devices in the market. There are wide series of cloned devices present as it is a process of producing acquisition that is done in the following: -

- SD card

In capturing evidence of SD card firstly, the used SD card is removed and the cloned SD card is made. Then as an alternative of the original SD card cloned SD card is used by the forensic analyst.

- Phone Memory

As here in phone memory the cloned memory is prepared then the it is used instead of the original memory. The original memory is detached from the phone so that there should not be any changes in the memory.

C. Analysis

In this phase investigator, decides which tool to support forensic analysis. 'Autopsy' is the finest tool that is found to be useful in analysing evidence image that are collected during acquirement of Firefox OS mobile device. As the

size of the storage media increases the forensic process slows down.

The following are approaches of analysis: -

- Analysis of External memory

In this stage, all the files are analysed especially the deleted files. In the study of External memory, the forensic analyst decides on the tool to analyse the SD card of the phone.

- Analysis of Internal memory

In phone memory, analysis of contacts, camera, call log, images, text messages, etc. are done. In this phase the investigator decides to use which tool to analyse the phone memory.

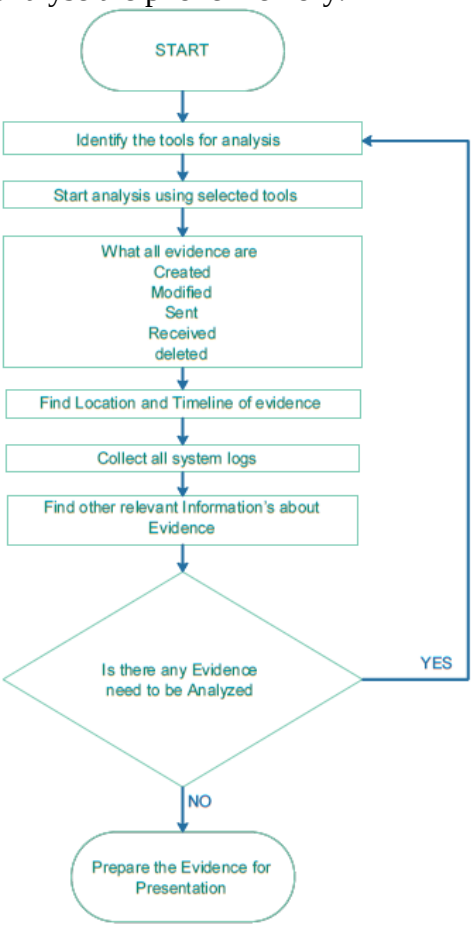

Figure 1: Analysis Phase

D. Presentation

The last stage is the presentation phase. In this, all the evidences are documented and are presented. Presentation phase displays the result of the analysis phase. The forensic examiner must know the anticipations of the audience as different audience have different expectations. As when investigator comes to know about the expectations of the audience it is easy for him/her to prepare the presentation. Whatever data was collected; it is presented in the presentation phase. The similar device but operates in dissimilar manner. When the image is produced then its integrity is checked. The integrity is most normally checked by the hash function and in the end all the functions are documented.

The key to any investigation or analysis you perform will be your demonstration and documentation. Documentation must be kept in a way that will allow you, or someone else, to return to the materials later (e.g., six months, one year, or longer) and understand or even verify the findings of the examination. This means that your documentation should be clear and brief, and it should be detailed enough to provide a clear symptom of what you did, what you found, and how you deduced your findings.

It is mandatory for a forensic investigator to document all the way through the examination process in the form of concurrent notes involving to what was done during the acquisition and examination. Once the examiner concludes the investigation, the results need go through some form of peer-review to guarantee the data is checked and the investigation is thorough. The examiner's notes and documentation may comprise information such as the following:

- Examination start date and time
- The physical condition of the phone
- Photos of the phone and individual components
- Phone status when received—turned on or off
- Phone make and model
- Tools used for the acquisition
- Tools used for the examination
- Data found during the examination
- Notes from peer-review

3. Literature Survey

There number of crimes that use mobile devices directly or indirectly are increasing day by day. The techniques of mobile phone forensics are very helpful in detecting those crimes in which mobiles are involved. Basically, the focus of mobile forensics is to scrutinize the mobile phone and produce the evidences that are useful in discovering the crimes and aids the investigators to investigate the criminal cases effortlessly and find out the indications/ evidences that can be easily acknowledged in court. There is a need for a universal technique to be developed for forensic analysis. As this technique performs the forensic analysis of mobile phones without attaching them to the computers, this benefits

the investigators to easily advance the evidences of the criminal cases. The generic technique reclaims the evidences that are present. Here investigators attained the data from the phone without attaching it to the computers. Digital forensics is used to recover the digital evidences so that they are collected and presented in the court. Digital forensics entails four phases. The first phase is the preservation phase in which the evidences are preserved; second phase termed the acquisition phase in which the documents are acquired; the next phase -the analysis phase in which the evidences are analyzed by the investigators and the last and final phase of the presentation phase in which the evidences are documented and are presented in the court. Smartphones are extensively used in social networking too that have increased the crime rate.

4. Conclusions

Forensic acquisition and analysis of Firefox OS based device acquired from a crime scene is challenging due to lack of technologies and methods to acquire and analyze the internal file system and application logs etc. This paper acquaints with methodologies and techniques to accomplish complete analysis of such devices in a Forensic way and helps the investigators to investigate the criminal cases effortlessly and find out the evidences that are acceptable in court.

5. Acknowledgment

I hereby express my deep and sincere gratitude to my guide, Mrs. Anu Rachel Abraham for all the help and guidance offered to me to make this study a fruitful one. I extend my sincere thanks to Mr. Raj Kumar T, Head of the Department for all the support rendered to me to make this study. My thanks are also due to my classmates for their help and support for this project.

References

[1] Ravneet Kaur, Tejpal Sharma.:An Approach for Mobile Forensics Analysis. International journal of Science Technology & Management (IJSTM) ISSN: 2229-6646
[2] Mohd Najwadi Yusoff, Ramlan Mahmod, Ali Dehghantanha, Mohd Taufik Abdullah (2014) “Performance Measurement for Mobile Forensic Data Acquisition in Firefox OS”, International Journal of Cyber-Security and Digital Forensics 183-199, The Society of Digital Information and Wireless Communications, 2305-0012.
[3] Shivankar Raghav1 and Ashish Kumar Saxena “Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition”, Proceedings of 2009 Student Conference on Research and Development, 16-18 UPM Serdang, Malaysia.
[4] Swaminath (2015)” Internals of Firefox Mobile Operating System with NFC Components”, International Journal of Scientific and Research Publications, 2250-3153
[5] Rizwan Ahmed and Rajiv V. Dharaskar (2008), “Mobile Forensics: An Overview, Tools, Future trends and Challenges from Law Enforcement perspective”, 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government.
[6] https://www.mozilla.org/en-US/firefox/os/2.0/
[7] https://en.wikipedia.org/wiki/Dd_(Unix)
[8] https://www.android.com/
[9] https://www.windowsphone.com/en-in
[10] https://developer.mozilla.org/en/docs/Tools/Firefox_OS_Simulator

Author Profile

Rakesh T graduated the Degree of Bachelor of Technology in Computer Science and Engineering from Amrita Vishwa Vidyapeetham University in 2014. He is now pursuing his master degree in Computer Science with specialization in Cyber Forensics and Information Security at College of Engineering Kallooppara under Cochin University of Science and Technology.

Anu Rachel Abraham graduated the degree of Master of Technology from Karunya University, Coimbatore and is presently working as Assistant Professor in Computer Science and Engineering at College of Engineering Kallooppara, Kerala.