Smart Device Forensics - Acquisition, Analysis and Interpretation of Digital Evidences

Ezhil Kalaimannan
Department of Computer Science
University of West Florida
Pensacola, FL 32514
ekalaimannan@uwf.edu*

Abstract

Smart Device Forensics is a classification under Digital Forensics, which primarily deals with the investigation of digital evidence found in smart devices such as Smart phones, tablets and televisions. There is an enormous rate of increase in threats with ever growing releases of smart devices and rapid advancement in innovative technologies. In this paper, we report a digital forensics investigation procedure to acquire and analyze digital evidences found in a smart device based on file systems, logical memory storage and operating system architectures.

Keywords: Digital Forensics; Smart Device; Digital Evidence; Online Social Networks; Cybersecurity

1. Introduction

With the proliferation of smart phones and tablets, there is an ever growing demand for the development of forensically sound methodologies and procedures to acquire and examine digital evidences found in these media. The traces of evidence found, continues to expand with a rate proportional to the daily dependency of these devices. Hence, these devices play a significant role from the vision of forensic practitioners and researchers.

In this research, we propose to analyze some of the popularly known tablets such as Google Nexus 7, HP Stream 7 and Apple Ipad 3rd Generation, on the basis of testing them in a forensically sound manner and examining, interpreting the traces of evidences acquired from these devices. The three important factors that would render the testing of these devices forensically challenging are the nature of file systems, logical memory, data structures and the number of third party applications available or can be installed/accessed by these devices [1]. The general phases of investigation process are outlined as follows [2]:

- Collection: This is the initial and the foremost step involved in the process of investigation. The main tasks are to find the potential traces of evidences from their sources such as smart phones and tablets.
- Identification: This step involves the extraction of data from various evidences that have been gathered in a forensically sound test environment.
- Preservation: This is one of the important step involved in the process of investigation, during which adequate measures are taken to secure the integrity of evidences according the requirement of justifying the case in a court of law.
- Examination and Analysis: This step is more focused towards the examination and analysis of the acquired evidences using proper forensic tools and software.
- Reporting: As like any process, the final stage is to document the results and proof of the conclusive evidence for the entire case.

Hence, the main goal of this research project is to test and forensically evaluate the tablet devices using various phases of a digital forensic investigation procedure. The experiments are planned to be conducted based on the aspect of multiple operating systems, memory organization and internal architecture of the smart devices in storing evidences. Artifacts such as email, contacts, photos, notes, third-party applications, calendar, and online documents will be subjected to experimentation.

2. Operating Systems Overview

The commonly known operating system [OS] for smart devices, to be considered in this research are:

*Corresponding author: Ezhil Kalaimannan (E-mail: ekalaimannan@uwf.edu).

978-1-4673-9795-7 2015

DOI 10.1109/CSCI.2015.58

- Windows: Windows is a popular and commonly known OS, derived from its original versions developed for PCs and desktops. Most versions of Windows OS have a set of standard features, such as multitasking and the ability to navigate a file system similar to that of Windows 9x and Windows NT, with support for many of the same file types. Much like its desktop counterpart, it comes bundled with a set of applications to perform basic tasks.

  Internet Explorer Mobile is the default web browser and Windows Media Player is the default media player used for playing digital media. Internet Connection Sharing, supported on compatible devices, allows the phone to share its Internet connection with computers via USB and Bluetooth. The user interface has changed much between versions but the basic functionality has remained similar. Windows Mobile has supported the installation of third party software since the original Pocket PC implementations.

- Android: The primary benefit of Android operating system is its compatibility with wide range of smart phones and tablets. This is achieved mainly by its Linux kernel interface which in fact is well-known for its compatibility to many different hardware platforms. Android offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different devices powered by Android.

  Android provides lot of advantages for the manufacturers of smart devices; however, at the same time poses great challenges for a forensic investigator. There are several versions of Android OS available in todays device market, out of which few of the popularly known implementations are Ice Cream Sandwich (ICS) and Jelly Bean.

- iOS: iOS is the operating system that runs on a variety of Apple manufactured smart devices such as iPad, iPhone, and iPod touch devices. The operating system manages the device hardware and provides the technologies required to implement native apps. The operating system also ships with various system apps, such as Phone, Mail, and Safari, which provide standard system services to the user.

  The iOS Software Development Kit (SDK) contains the tools and interfaces needed to develop, install, run, and test native apps that appear on an iOS devices Home screen. Native apps are built using the iOS system frameworks and Objective-C language and run directly on iOS.

3. Research Questions

- What are the key findings, which can be interpreted as potential evidence for a digital forensic case?
- Is there a methodology or comparison scheme, which the research can outline for classifying the evidences acquired from the tested devices based on operating systems, internal architecture or memory organization?
- Can this research suggest any evidence-based relationship between the artifacts or devices being tested?

4. Work in Progress

In this paper, a work in progress research to acquire and analyze digital evidences found on smart devices such as smart phones, tablets and televisions is illustrated. We intend to test them from the perspective of the various phases in a digital forensic investigation process.

Extensive experiments are planned to be conducted focusing on various areas of operating systems, memory organization and internal architecture of the smart devices in handling digital evidences. Interesting artifacts such as email, contacts, photos, notes, third-party applications, calendar, online storage and online social network accounts will be subjected to exploration. One more interesting venue for research, is to test and evaluate evidences based on online social network user accounts stored and used on these devices.

References

[1] Iqbal, A., Obaidli, H., Marrington, A., and Jones, A. Windows Surface RT tablet forensics, *Digital Investigation*, Vol. 11, No.1 , pp. 87-93, 20014.

[2] Ayers, R., Brothers, S., and Jansen, W. Guidelines on Cell Phone Forensics, *NIST Special Publication 800-101*, 2007.