Cyber Security Investigation for Raspberry Pi Devices

Feng X.; Onafeso Babatunde and Liu E.
Computer Science and Technology
University of Bedfordshire
Luton, United Kingdom
xiaohua.feng@beds.ac.uk, babatunde.onafeso@study.beds.ac.uk and enjie.liu@beds.ac.uk
Tel. +44(0)1234 400 400

Abstract— Big Data on Cloud application is growing rapidly. When the cloud is attacked, the investigation relies on digital forensics evidence. This paper proposed the data collection via Raspberry Pi devices, in a healthcare situation. The significance of this work is that could be expanded into a digital device array that takes big data security issues into account. There are many potential impacts in health area. The field of Digital Forensics Science has been tagged as a reactive science by some who believe research and study in the field often arise as a result of the need to respond to event which brought about the needs for investigation; this work was carried as a proactive research that will add knowledge to the field of Digital Forensic Science.

The Raspberry Pi is a cost-effective, pocket sized computer that has gained global recognition since its development in 2008; with the wide spread usage of the device for different computing purposes. Raspberry Pi can potentially be a cyber security device, which can relate with forensics investigation in the near future. This work has used a systematic approach to study the structure and operation of the device and has established security issues that the widespread usage of the device can pose, such as health or smart city. Furthermore, its evidential information applied in security will be useful in the event that the device becomes a subject of digital forensic investigation in the foreseeable future. In healthcare system, PII (personal identifiable information) is a very important issue. When Raspberry Pi plays a processor role, its security is vital; consequently, digital forensics investigation on the Raspberry Pies becomes necessary.

KEYWORDS: Big Data Forensics, Healthcare, Raspberry Pi Application, the Internet of Things (IoT) Services PII cyber laws

I. INTRODUCTION

Under Internet of Things concept, the increasingly interconnected smart ‘things’ open up new opportunities for building a much wider range of smart services and applications. Smarter and low power devices can be interconnected to provide more powerful and valuable services. Intel has introduced low power system-on chip, such as “*Quark1*”, which can be used to build the smart devices. As one of the simplest digital device, size can be as small as a credit card, but can be as powerful as a single-board computer. These features make the Raspberry Pi a strong candidate upon building the smart and powerful IoT devices, such as the IoT gateway or IoT devices that require additional computational power and off-load functions from aggregator or server to improve system performances. Raspberry Pi enabled device has many potential in supporting various IoT applications. Cyber Security would be a major concern if Raspberry Pi being used to build the smart device. Currently it is under-researched (). In this paper, we represent a case study for the Raspberry Pi, as an IoT system device in situations where not only attacks come from a Raspberry Pi, but also attack targeted Raspberry Pi (Feng, 2015).

A number of artifact developments have been for attack happened in typical cloud Healthcare environment; such as big data in smart city the digital forensics evidence acquisition has been done and demonstrated. Further work is still in progress at the Security and Forensics Laboratories, Department of Computer Science and Technology, University of Bedfordshire, United Kingdom.

Bio-informatics has been rapidly developed recently. The IoT application in healthcare is increasing. The consequence of these is cyber security and trustworthiness (Liu, 2014) issues. Feng (2016) has pointed out that digital forensics is one of the solutions potentially including some of the cyber issues such as PII and cyberstalking.

The layout of this paper is as follows: Section 2 discusses the background of this research project. Section 3 presents forensic concepts while Section 4 presents the review of forensic investigation process models and related researches/technology. Section 5 presents the study and experimentation on the device; Section 6 presents the results and observations while Section 7 presents the evaluation. Section 8 shows conclusions and suggests future planned work.

II. BACKGROUND

The field of Digital Forensics Science has been tagged as a reactive science by some ones, who believe research and study in the field often arise as a result of the need to respond to event which brought about the need for investigation; this work was carried as a proactive research that will add knowledge to the field of Digital Forensic Science. The Raspberry Pi is a cost effective, pocket sized computer that has gained global recognition since its development in 2008; with the wide spread usage of the device for different computing purposes. It could be assumed that the device is envisaged to be involved with forensics investigation in the near future.

This work has used a systematic approach, Raspberry pi 2 to study the structure and operation of the device and has established security issues that the widespread usage of the device may pose as well as evidential information that will be useful in the event that the device becomes a subject of digital forensic investigation in the foreseeable future.

The Raspberry Pi is a cost-effective, pocket size computer around the size of a bank card. The idea about developing an affordable, compact and programmable computer for little children was first conceived in 2006 at the University of Cambridge's Computer Laboratory when Upton, Mullins, Lang and Mycroft (2014) started growing concern about the decline in figures of aspiring Computer Science candidates and the level of their computer programming skills. This decline which they attributed to the expensive and obscure nature of current computers led to the design and development of a tiny and affordable computer with programming capability for children. This idea became a reality in 2008 when they teamed up with Pete Lomas of Norcott Technologies and David Barben, co-author of Elite to form the Raspberry Pi foundation. Three years later and with advancement in the design of powerful and affordable processors for mobile devices, the Raspberry Pi computer was born and under a manufacture license deal with element14/Premier Farnell and RS Electronics, It was mass produced and peaked at two million in sales within two years of production (Raspberry, 2011).

The Raspberry Pi device has been widely used to roll out various educational projects like; the RACHEAL Pi, a Raspberry Pi offline educational server which provides educational contents from myriad of creative commons like Khan Academy, CK12 and various textbooks to students in remote locations where there is no internet access (Upton, 2014). The Raspberry Pi has gained profound recognition among hobbyists, professionals, programmers and regular everyday computer users for various purposes and projects such as that which involve the combination of many Raspberry Pi devices to achieve maximum computing power at low energy (Cox, 2014) and the "*Big Threat of Small Computers*"; a project with the goal to turn a Raspberry Pi computer into a system that will automatically execute complex attacks against a network (Senator, 2014).

At cyberstalking cases, Raspberry Pi could be as a target of an attack object too (Conrad, 2016). Then, it is worth to test both side (A-party and B-party) in Laboratories and the testing results could have a broader significance than the Raspberry Pi we initial planned with (Feng, 2015).

III. DIGITAL FORENSICS CONCEPTS

Motivation for This Project

With millions of units of the device already sold and still selling and additionally with promising and prospective uses to be realized, it is safe to assume that the Raspberry Pi device will play a role within computer security and digital forensics investigation in the near future. Moreover, digital forensics has been termed by some as a reactive science; saying that study and research in the field are most times as a result of the need to react to the occurrence of an event. For that reason, it is imperative that the Raspberry Pi device be studied in order to identify any cyber security threat that may arise as a result of its widespread popularity and to additionally establish evidential information that are recoverable from it in the case of non-conventional usage or compromised state. The outcome of the study will form a basis for reference when the need arise for a forensic investigation to be carried out on the device.

The Definition

The Oxford Dictionary defines, forensics as "scientific tests or techniques used in connection with the detection of a crime". It additionally stated that the term forensics originated from the Latin word forensics which means in open court or public. Consequently, forensic investigation can be defines as the science that involves investigative processes, means and techniques used for collection and analysis of evidence relating to a crime in order to establish facts and results that are openly acceptable and can be used to make open decisions often in a court of law. Forensic investigations have been recorded as far back as the 18th century in Lancaster, England where John Toms was convicted of murder when torn bit of newspaper found in a gun matches the piece found in his pocket (RAUT, 2008).

Scientific breakthrough over the years in various facet of life has opened the gateway to the possibilities of applying knowledge acquired in one subject area to another; this has led to the birth of many other novel cross-subject areas in the 20th century, which has been useful in exploration and development. Forensic science is a mature field that involves the use of acquired knowledge, achieved innovations and established fact in sciences to investigate and solve crimes. The science comes as a result of years of studying and experimenting; for example, the discovery of Deoxyribonucleic acid (DNA) that can be traced back to genetic experiments on plants conducted by Gregor Mendel in the 19th century, this discovery led to subsequent research by Jeffreys (1985) which gave birth to DNA fingerprinting, DNA profiling; a technique used to identify individuals based on certain characteristics in their DNA.

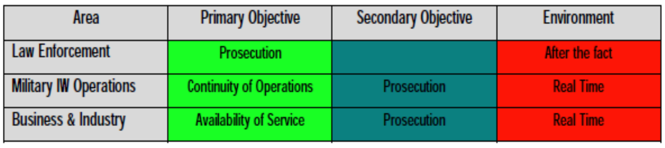
This technique was first used in 1988 to assist police solve a rape and murder case in Narborough, Leicestershire, UK which led to the prosecution of Colin Pitchfork and exoneration of Richard Buckland in 2006 This technique is now an important part of forensics science. Various fields of forensic science, like Forensic Medicine, Forensic Anthropology, Forensic Odontology, Forensics Etymology, Forensics Mathematics (DNA profiling), and Digital Forensics have additionally emerged and have proved useful to investigate and solve crime cases over the years. Furthermore, in a Smart City project Raspberry Pi can play a node processor in a centralised healthcare system (Liu, 2014), in order to deal with potential big data process, while cyber security of Raspberry Pi to protect PII (Personally identifiable information) data being critical (Feng, 2015) especially when data at the cloud environment (Feng, 2012), then digital forensics preparation becomes crucial (Feng, 2016).

The proliferation of digital electronic devices and our dependency on them in this information age has given rise to a new form of crime that can be categorized as computer crimes or computer-related crimes. This new wave of crime through the years has risen and is growing bigger with significant impact on government, business and individuals. This became a growing challenge for law enforcement agencies as they found themselves in situations where they have to retrieve or confiscate one digital device or the other from a crime scene which needs to be analysed to solve a crime. Furthermore several businesses and government need to investigate why and who attacked their critical infrastructure/intellectual properties. The need to investigate this new form of crime with its new form of evidence (digital) led to the passing of new legislative laws and the birth of the new science known as Digital Forensics Science (DFS).

Digital Forensic Science

Digital Forensic Science was defined at the first Digital Forensic Research Workshop held in Utica, New York on August 7-8, 2001 as “The use of scientifically derived and proven methods towards the presentation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations ” (DFRW, 2001). This definition identifies two purposes for DFS; to investigate activities related to digital crime in order to determine justice (solve crime) or to determine why there is/was a deviation from planned or normal operations (incidence response), and evidently identifies parties involved in DFS with their aims as shown in the *Figure 1* below.

Each party use different approach to investigation, this is largely due to their varying objectives.



Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business & Industry	Availability of Service	Prosecution	Real Time

Figure 1 Parties involved in Digital Forensic Science (DFRW, 2001)

For example, law enforcement will not embark on an investigation until there exist sufficient information and fact that a crime has been committed whereas business and industry or military can move into investigation as soon as the slightest hitch is discovered so as to ensure availability of service, continuity of operations, protection against critical infrastructure and intellectual properties or protection against data/information theft but can still be after the fact in some cases as well for example as part of incidence response and disaster recovery.

Digital forensic is a relatively mature but new field of study whose maturity can be said to be as a result of need; i.e. prominence and increased rate of computer crimes through the years prompted the need for a platform of investigation to address the issue. This is why compared to other forensic science field like DNA fingerprinting which came as a result of years and years of studying and experimentations, digital forensics seems to still lag behind in some aspects. However, like every other forensic science field, digital forensic science consists of four intertwined components namely (Feng, 2016):

- The Crime
- The Evidence
- The Science
- The Law

Laws, standard and regulations like ACPO guidelines and First Responder’s guidelines govern what can be collected as evidence, how it should be collected or when it can be collected from a crime scene. The science constitute the processes (methods and procedures) used to gather and analyze evidence to produce results and facts. The facts and results established form the scientific analysis of the evidence can then be used to make informed decision in a forum like court proceedings using laws, like Computer Misuse Act, The RIPA 2000 or business continuity decisions by corporate management. If compared to PRINCE2 project management technology; a structured methodology that defines the use of processes and techniques to managing projects (ILX, 2015), Digital Forensics Science can be said to consist of components and processes as well. Digital Forensics could additionally sort out cyber psychology issues (Conrad, 2016; Feng, 2016). The components being Crime, Evidence, Science and Law as mentioned above while the processes can be said to be the established activities that starts from collection of evidence through to the presentation of report of analysis.

Depending on the parties involved, this process may or may not include the detection of the crime. For example, a digital forensic investigator working with the law enforcement may only be involved after crime have been found to involve the use of a digital device whereas an investigator working for a corporate organization may be part of the security team that discovered a security breach which led to the investigation. This process seems to be the scope of work for a digital forensic investigator and it is very crucial as it must conform to the laws guiding it and must moreover be accurate to avoid making wrong decision or judgment based on inaccurate investigation.

IV. THE EXISTING WORKS

In order to establish a foundation for a discipline, researchers often construct models to reflect their perception of the field of study. Researchers in the field of Digital Forensics have over the years developed various models for the digital forensics investigation process; the goal is to create a model that conforms to the law component of the field while still retaining its scientific nature.

Digital Forensics Investigation Process Models

Adopting the existing paradigm used in the handling of physical documentary evidence in legal cases, proposed a digital investigation process model as shown in Figure 2.

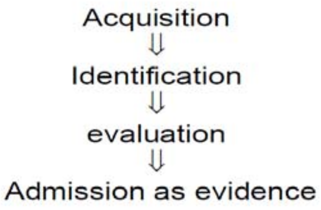
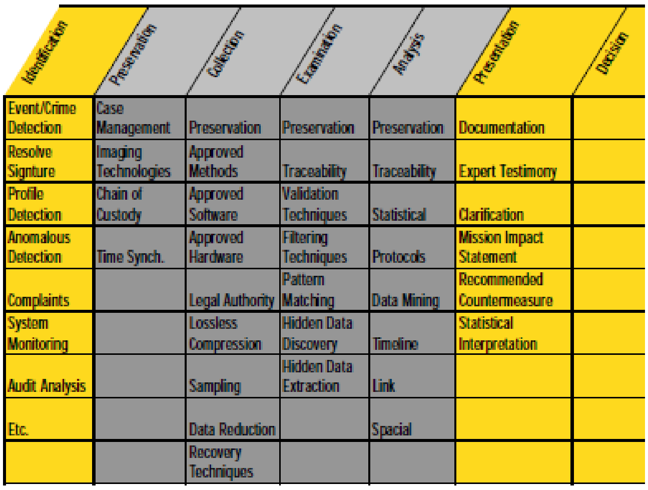


Figure 2 Forensic Process Model

Participants at the Digital Forensics Research Workshop which consisted of practitioners of the science, researchers in computing field, law enforcement agency, business, military, and so on agreed on the model shown in Figure 3.

The established that the Presentation, Collection, Examination and Analysis phases are the core processes in a digital forensics investigation process. But depending on the environment and parties involved, it is safe to say other phases are equally relevant as well. For instance, the identification is a core process in the case of incidence response in organizations, and furthermore the presentation is crucial in both criminal case and incidence response as the investigator is responsible for interpreting observations and results in an understandable manner to decision makers (Judge, Jury or Management of law enforcement).

However, in a main work by Carrier (2003), they provide a valuable review of all the study before them and developed a new model which they called Integrated Digital Investigation process.



Identification	Preservation	Collection	Examination	Analysis	Presentation	Decision
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation	
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony	
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure	
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
Etc.		Data Reduction		Spacial		
		Recovery Techniques				

Figure 3 Investigative Process Model for DFS (DFRW, 2001)

Integrate in the sense that it was developed by mapping the digital forensic investigation context unto the already established physical forensic investigation processes. The model consists of 17 phases which are further organized into 5 groups depicted in the figure below. It was developed to be applicable in both law enforcement and corporate environments.

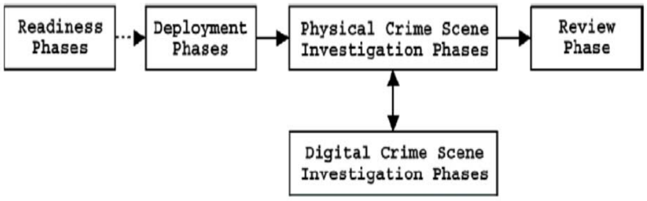

Readiness Phases
Deployment Phases
Physical Crime Scene Investigation Phases
Review Phase
Digital Crime Scene Investigation Phases

Figure 4 Integrated Forensics Investigation Process model (Carrier, 2003)

This was further modified in 2004 by Carrier, (2005); with focus on the digital crime scene investigation phases using the concept of abstraction layers, events and event reconstruction which they used to present another model called the Event Based Digital Forensic Process Model.

Beebe and Clark (2005) proposed the Hierarchical and Objective Based Framework for Forensic Investigation which is a multi-tiered process model with several objective based subtasks, particularly under the data analysis phases. They adopted the concept of file system and memory abstraction layers from Carrier (2005) and introduced the Survey, Extract, and Examine sub-phases as an objective based approach to the Data Analysis Phase.

In the light of the above, looking through all the proposed forensics investigation process models, it is safe to conclude they all have one thing in common; i.e. the basic forensic investigation process involve

- Evidence Preservation
- Evidence Collection
- Evidence Examination
- Evidence Analysis
- Result Presentation

Each process is multi-layered in its own application and sequential to the next. Each step is in addition equally as important as every other step and a flaw in one will have effect on the next. For example collection of insufficient or contaminated evidence will lead to insufficient examination which will in turn lead to inaccurate analysis that may render the result inconclusive or insufficient. Digital Forensic Analysis work by Carrier (2005) which presented the description of the purpose and goal of digital forensic tools using the concept of abstraction layers took a significant standpoint in digital forensic analysis. It used the concept of abstraction layers to define six major categories of analysis shown below:

- Physical Media Analysis
- Media Management Analysis
- File System Analysis
- Application Analysis
- Network Analysis
- Memory Analysis

In his book *File System Forensic Analysis*, Carrier (2005) presented the forensic analysis areas of conventional PC and Laptop as shown in Figure 5.

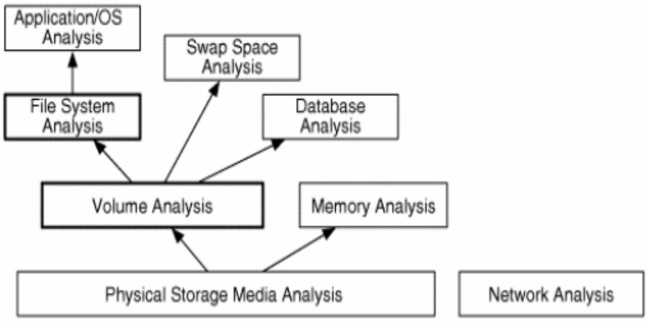


Figure 5 Layers of analysis based on the design of digital data

The bottom layer (Physical Storage Media Analysis) represents the analysis of physical storage media like hard disks, memory chips, and CD ROMs. He further broke down the analysis of a hard disk drive as shown in Figure 6.

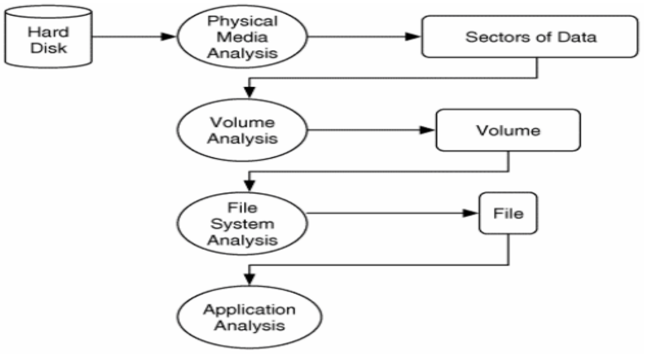


Figure 6 Process of analyzing data at the physical to the application level

Raspberry Pi

Whilst reviewing the potential digital device used for health data, we found Raspberry Pi is a suitable one in many situations. However, it was still not fully developed in cyber security circumstances. So we started from Raspberry Pi. The Raspberry Pi usually supports optimized variations of Linux based operating systems due to its low processing power. However the Pi 2 model B is packed with much processing power and is able to support GNU based Linux distributions like Snappy Ubuntu and even Microsoft Windows 10. It comes in different models; a comparison of these models is presented in Table 1.

The *Raspberry Pi 1*, Model B revision 2, was used for the purpose of this work simply because it is available and reachable for experiment at the moment; the layout is shown in Figure 7.

Model	**Processor**	**RAM**	**Storage**	**Ethernet NIC**	**USB port**
Model A	Single core 700MHz	256 MB	SD card	None	1
Pi 1 Model A+	Single core 700MHz	256 MB	Micro SD Card	10/100 Mbit/s	1
Pi 1 Model B rev 1	Single core 700MHz	256 MB	SD Card	10/100 Mbit/s	2
Pi 1 Model B rev 2	Single core 700MHz	512 MB	SD Card	10/100 Mbit/s	2
Pi 1 Model B+	Single core 700MHz	512 MB	Micro SD card	10/100 Mbit/s	4
Pi 2 Model B	Quad core 900MHz	1 GB	Micro SD card	10/100 Mbit/s	4

Table 1 Raspberry Pi Computer model comparison

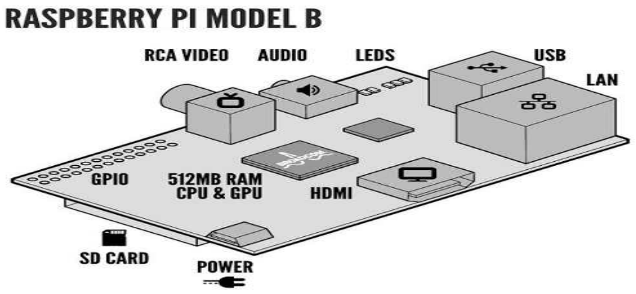


Figure 7. Raspberry Pi Model B rev 2 layout (Raspberry, 2015)

The device has an installer manager developed by the Raspberry Pi Foundation called NOOBS (New Out Of Box Software) which can be used for the basic installation of operating system on to the device. The NOOBS can be used to install the operating systems listed below.

- Raspbian (Debian version)
- Pidora (Fedora version)
- OpenELEC
- OSMC
- RISC OS
- Arch Linux
- RaspBMC

The Raspbian OS is the most commonly used among regular users of the device as it is recommended by the Raspberry Pi foundation and in addition it does not require network connectivity for installation as other OS available on the NOOBS platform does. There in addition exist other operating systems distributions optimised to work on the device, for example FreeBSD, Open SUSE and Kali Linux. For the purpose of this work, the Raspbian operating system was selected for study because it is basic to the device and recommended by the Raspberry Pi Foundation.

Rajchada (2016) discussed JTAG techniques which could be a direction in later stage researches. The current project has collaborated with NHS "Smart City" project, which potentially elaborate the Raspberry Pi application to a further higher level and with many relevant issues to explore the extents. Research at the University of Texas, USA has achieved some results (Rajchada, 2016). However, discuss with those has beyond the scope of this paper; that should not at this research stage.

V. STUDY AND EXPERIMENTATION

This work was approached in three stages; the first stage was the study and observation of the Raspberry Pi device's operations to identify analyzable evidences and their various locations, the second stage entailed setting up a scenario to emulate possible real life attack and compromised state of the device and lastly the final stage involved adopting a Digital Forensic Investigation Process Model to carry out the investigation of the setup scenario.

The Study and Observation of the Device

In order to study and observe the device, this work adopted the concept of abstraction as proposed by Carrier (2003) in his study on examining forensic tools using the concept of abstraction layers. This concept of abstraction layers was used to break down and categorize analyzable objects from the Raspberry Pi for the purpose of study and observation.

The concept of abstraction layers can be used to study huge amount of data by categorizing them into smaller convenient chunks as this will provide better understanding of all the underlying processes and transformations that the data undergoes during processing. A storage medium on a computer stores data in the form of binary; i.e., 0s and 1s no matter what type of data it is, but an application retrieving this data from storage will gather this series of 0s and 1s and format it into a structure that meets it need; for example a text editor will retrieve 0s and 1s from a storage media which will then be formatted into a readable alphanumeric character for the purpose of presentation to the user using the ASCII code translation; this translation is regarded as a layer of abstraction. According to Carrier (2003), each abstraction layer can be identified as having to take in an input and a set of instructions on how to process the input to produce an output and a margin of error as depicted below shown in Figure 8.

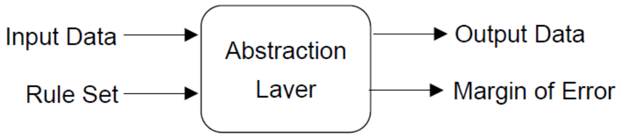


Figure 8 Abstraction Layer representation of data (Carrier, 2003)

The output of one abstraction layer can serve as an input into another layer. In the case of the text editor, the displayed alphanumeric characters can be series of commands that is fed into an interpreter/compiler abstraction layer to perform actions as a computer program. The layer responsible for handing over its output to another layer for processing is called the boundary layer. This work used this concept of abstraction layers to breakdown the Raspberry Pi device as presented below with the aim of studying and understanding its structure and operations.

***a) Physical Media Layer**:* This is the physical media layer of abstraction, which translates the storage media layout and contents to a standard interface, in this case the controller that regulates the representation and writing of the 0s and 1s in blocks to the flash memory chip on the SD card. The analysis of this layer includes processing the custom layout of data, as well recovering deleted data after it has been overwritten.

***b) Media Management Layer**:* This layer represents the logical organisation of the physical storage media. In this case the logical partitioning of the SD card storage. The study here will include learning the arrangements of bytes and sectors into partitions.

c) File System Layer: The file system layer of abstraction represents the translation of bytes and blocks of the partitions into directories and files. In this case the operating system file system that exists on the SD Card.

d) ***Application Layer***: The application layer of abstraction is responsible for translating data received from the file system abstraction layer into the appropriate format needed by the particular application. Forensic analysis here involves examining application data like log files, configuration files, pictures, user created files, and so on and possibly executable files. According to Carrier (2004) the Application layer of abstraction can be further categorised into several categories but for the purpose of this study it categorised into two broad categories as the follows.

*i. Operating System Layer**:*** The Operating System can be viewed as a special type of application that provides a platform for other applications to use the computer's processing power and resources to process their data. For example a user uses a Microsoft word application installed on a Windows or Mac Operating System environment to create a document; without the Operating System the user cannot use the word processing application.

*ii. Application Packages Layer**:*** This layer represents a broad category of all application packages that can be used by users to create files. The type of files here can be specific to a particular application or can be process-able in a way by some other too; for example a Microsoft Word application cannot open a portable document files *(pdf)* peculiar to packages like Adobe reader or Foxit Reader, whereas a notepad application can be used to edit an executable file created with a programming application like Python. Files can be categorised at this layer as executable, document, images, videos too. Analysis at this layer includes, content examination, metadata, application data, services logs and so on.

***e) Network Layer*:** The network layer of abstraction translates, organises and formats the data representation from a physical medium (network cables) or wireless medium (radio waves) to data that is used by an application. Analysis in this layer can involve examining streams of packets captured on the medium, Firewall, IDS/IPS alerts and so on.

f) Memory Layer: This layer translates the bytes of data in memory to processes and system data. Analysis at this layer may include identifying process information IDs, applications attributed to process, process owners, and so on.

In fact, the ideal simulation testing for smart city applications could be Raspberry Pi clusters. Those are not only for healthcare situation, but also for multi-application circumstances. However, due to constraints of the Lab experiments facilities, to date, the cluster testing has not been done. We would exploit combined digital forensics investigation could collaborate with forensics science experts to carry out a fully healthcare forensics investigation, including cyber psychology forensics issues (Conrad, 2016).

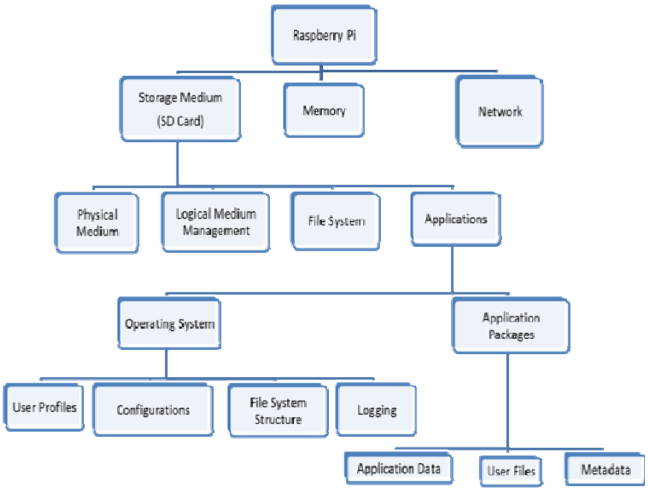


Figure 9 Breakdown Structure of Devices Study

This work was limited to the storage medium on the device, this is important because the device uses a different storage medium (SD card) as opposed to that of PCs and Laptops (Hard Disk Drives). In addition, the delicate nature of the USB type B mini used to provide power to the device and the exposure of the SD card storage medium put the device in the position where it will likely require an offline storage media analysis at most times. The study of the storage medium was approached in a layered manner as depicted in Figure 9. Nevertheless, more Lab work could be carried out next, in addition, a combined digital forensics investigation collaborate with forensics science experts to carry out a fully healthcare forensics investigation.

VI. AN OVERVIEW OF THE RASPBERRY PI BOOT PROCESS

The experiment condition is:

Time: 2015-2016 academic year

Location: C106 Security Laboratory

The steps are:

a) Once the device is powered on, the firmware initializes and load the “bootcode.bin” file from the FAT formatted first partition “/dev/mmc/blk0p1” of the SD card

b) The “bootcode.bin” looks for, loads and then execute the “start.elf” and fixup.dat files.

c) start.elf then reads the content of config.txt for GPU configurations.

d) It again reads the content of cmdline.txt, loads and executes the kernel.img (The Operating System Kernel Image) and then passes all instructions read from cmdline.txt to kernel.img.

e) The kernel then executes the commands passed to it in order to discover where the root file system is located; which in most cases in the second partition i.e. root=”/dev/mmc/blk0p2” line in the cmdline.txt.

f) The kernel then mounts that partition as the root file system “/” and proceeds with the rest of the boot process from the root file system.

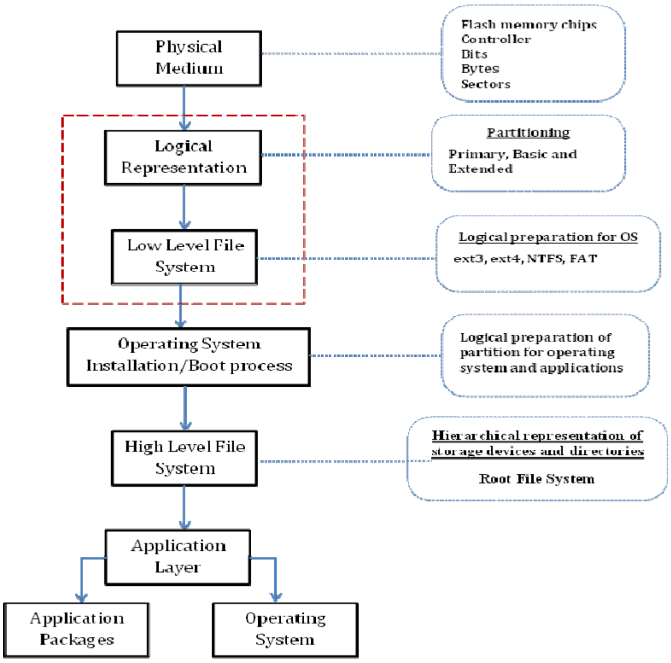

Physical Medium
Flash memory chips
Controller
Bits
Bytes
Sectors
Logical Representation
Partitioning
Primary, Basic and Extended
Low Level File System
Logical preparation for OS
ext3, ext4, NTFS, FAT
Operating System Installation/Boot process
Logical preparation of partition for operating system and applications
High Level File System
Hierarchical representation of storage devices and directories
Root File System
Application Layer
Application Packages
Operating System

Figure 10 Layered approach to study the SD card

Overview of the NOOBS installation Process

1) The device’s firmware loads and executes the bootcode.bin which comes as part of the NOOBS files copied to the SD card just like in the boot process.

2) The bootcode.bin as usual search for the start.elf file but since this is the installation process i.e. the very first time, start.elf does not exist. It then instead search for, loads and execute the recovery.elf instead.

3) The execution of recovery.elf switches the firmware into NOOBS mode in which the device loads and executes the recovery.img with instructions from recovery.cmdline as opposed to loading and executing the kernel.img with instructions from cmdline.txt in the normal boot process. It additionally in this mode loads recovery.rfs as the file system, the recovery.rfs contains the NOOBS graphical user interface as well as the several scripts for the installation.

4) Because this is the first time running NOOBS, there exists a runinstaller command in recovery.cmdline which runs the installer package.

5) The installer package then size up the first partition /dev/mmcblk0p1 to fit only just the earlier copied NOOBS files, it then labels this partition as “RECOVERY”.

6) It then creates a fresh extended partition /dev/mmcblk0p2 using the bulk of the free space available on the SD card

7) It further creates another 32MB partition /dev/mmcblk0p3, format it as ext4 and label it as “SETTINGS”. This partition contains the NOOBS setting files which holds information like what operating systems are installed, the partition they are installed on, the default operating system and so on.

8) The installer then removes the runinstaller from recovery.cmdline so that the process is not repeated at next boot.

9) At this point, NOOBS then presents the GUI based operating system installation menu to choose from.

10) As the Raspbian operating system was selected for installation, NOOBS loads the partition.json file. This creates a FAT formatted 60MB partition /dev/mmcblk0p5 from the extended partition /dev/mmcblk0p2, labels it as “boot” and extracts the content of boot.tar.xz into it.

11) It then uses up the rest of the extended partition to create an ext4 formatted partition /dev/mmcblk0p6, labels it as “/” (the root partition) and extracts the contents of root.tar.xz into it.

12) NOOBS then runs the partition_setup.sh to mount the newly created partitions

13) It then edits the cmdline.txt in the boot partition to replace the line “root =/dev/mmcblk0p2” with “root=/dev/mmcblk0p6”. It additionally edits the /etc/fstab to reflect same as well as change the boot partition to /dev/mmcblk0p5.

14) It finally updates the settings partition with the details of the newly installed operating system.

Primary Partitions	**Logical Partitions**	**File System**	**Label**	**Content**
/dev/mmcblk0p1	None	FAT	Recovery	NOOBS files and Operating System image for recovery
/dev/mmcblk0p2	2	Extended	No Label	Logical Partitions
	/dev/mmcblk0p5	FAT	Boot	Raspbian boot files
	/dev/mmcblk0p6	Ext4	"/" *(root partition)*	Raspbian root file system
/dev/mmcblk0p3	None	Ext4	Setting	NOOBS setting files

Table 2. Partitions on the NOOBS Raspbian installed SD card

This research focused on conventional NHS centralised healthcare systems, so the testing circumstances is still set as traditional environment.

The Table 2 below presents the partitions that exist on the SD card after installation with NOOBS while Table 3 presents the partitions that exist on an SD card installed using the typical raw installation.

The Table 3 is additionally demonstrating the setting being a typical traditional circumstance - the NHS healthcare system used facilities file systems.

Primary Partitions	**Logical Partitions**	**File System**	**Label**	**Content**
/dev/mmcblk0p1	None	FAT	Boot	Operating System boot files
/dev/mmcblk0p2	None	Ext4	"/" (root partition)	Operating System's root file system

Table 3. Partitions on a typical raw image installed SD card

The Figure 11 depicts the Raspbian root file system in the root partition "/"

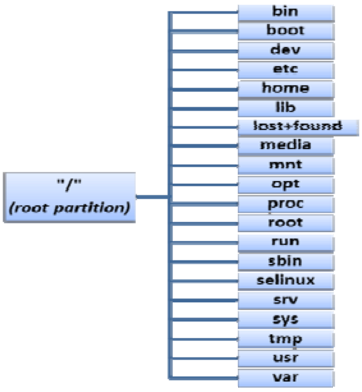


Figure 11. Raspbian Root File System

Scenario Setup

The scenario depicted in Figure 12 below was setup; an attacker compromised a Raspberry Pi device on the corporate network and used it violate a policy on the corporate server.

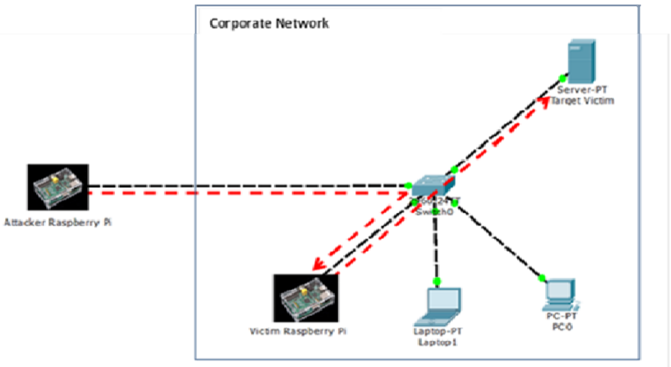


Figure 12. Case Study Scenario Setup

Investigation Process

The investigation process was carried out simultaneously using two distributions of Linux operating systems namely Kali Linux and Community Enterprise Operating System (CENTOS) to ensure repeatability and reproducibility. The process was broken down into four stages as described below and the Integrated Digital Investigation Process Model by Carrier (2003) was modified and used to carry out the investigation process.

a) Server Investigation:

This stage was observed as part of an incidence response to violation of organizational policy detected on the corporate server. Evidence collection, examination and analysis were performed and which pointed to the Victim Raspberry Pi.

b) Raspberry Pi Investigation I:

This was carried out to investigate the Victim Raspberry Pi storage media for evidence of the attack.

c) Raspberry Pi Investigation II:

A clear motive was assumed to establish a link between the crime and the suspect, this led to further investigations to prove the innocence of the victim Raspberry Pi user and to furthermore point towards the real attacker.

d) Attacker Raspberry Pi Investigation II:

This was observed as an escalation process from the organization to law enforcement. It included the investigation of the attacker's storage device to uncover evidences related to the case which are substantial enough for prosecution.

Crucial phases of the investigation process like image acquisition and evidence verification was repeated and reproduced using forensic tools like FTK and Encase as well.

VII. RESULTS AND OBSERVATIONS

Through A-party and B-party experiments, the outputs are shown as follows.

Some Identified Important Files and Directories

1) ***dmesg***:

The dmesg file located in /var/log contains certain information that are useful for forensic investigation. The file contains details about the startup processes that the device undergoes when it is powered on. Information about every internal device or external devices like USB storage medium, USB adapter and so on that was attached to the device during start-up can be found here.

2) ***user.log***:

The user.log file located additionally inside the /var/log contains information about the various wireless access points that the Raspberry Pi device has been connected to. This can come in handy in cases where it is required to investigate what wireless networks the device has been connected to. This file contains the logs too about when a system shutdown, reboot and so on was initiated on the device

3) ***wpa_supplicant.conf***:

This file located inside the /etc/wpa_supplicant directory as well contains information about access points SSIDs and their pre shared key

4) ***kern.log***:

The kern.log file located additionally in /var/log contains information about the kernel operations which includes detected hardware and hardware drivers. This file is helpful in investigations where only the SD card storage is available and it is required to know the model of the Raspberry Pi device which the card was used on, as it contains information about the device and its component hardware. It is furthermore contains information about the USB devices which have been connected to the device, this is useful in investigations where it is required to find out if a particular USB device has been accessed on the device.

5) ***history.log***:

This file located inside /var/log/apt gives the history of installed, uninstalled, updated packages on the devices. APT (Advanced Package Tool) is a tool in Debian based Linux distributions for installing, uninstalling and updating applications packages. This apt history file is particularly useful in investigations where it is required to find out what software applications has been removed from a Raspberry Pi device as part of an effort by the perpetrator to remove evidence in order to hinder investigation.

6) ***.bash_history***: This file holds the history of all the commands that were issued at the bash command prompt terminal. It is a hidden file that can be found in a user's home directory. For the default Raspberry Pi user, it is located in the /home/pi directory.

7) ***.cache***: This is a hidden directory located in /home/pi as well, which contains a cache directory for the default web browser (Epiphany) which came preinstalled with the Raspbian OS. The epiphany-browser subdirectory under it contains cached information about the web pages visited using the browser, this can come in handy in investigations where it is required to analyze a user's browsing habit.

8) ***.config***: This is another hidden directory located inside /home/pi, this directory contains subdirectories in it, importantly the "epiphany" subdirectory which contains the following files:

i. bookmarks.rdf: this file contains the list of bookmarked pages on the epiphany browser

ii. cookies.sqlite: this is a SQLite database file which contains the web browser cookies

iii. ephy-history.db: this is an important file in digital forensic investigations, it is a database of browsing history, it contains all webpages that the user has visited on the epiphany browser

9) ***WebpageIcons.db***: this is a SQLite database file as well, which contains certain history about the usage of default browser; it is located in /home/pi/.local/share/epiphany-browser and additionally contains useful information for digital forensic investigations.

Security Issue

The Raspbian operating system has secure shell protocol (SSH) opened on port 22, secure shell is a protocol used for establishing remote log on. This port should be closed in situations where remote access to the device is not required. Another security issue observed on the device was that the Raspbian operating system comes preinstalled with a default user under the username of "pi" and password "Raspberry", this is a big security problem as users often use this default username and password as it is or some users even create a new user with their own username and password while they leave the default Pi user. The recommendation here is that, when it is not in use, the default Pi user should be disabled or the password must be changed to a very strong password when in use.

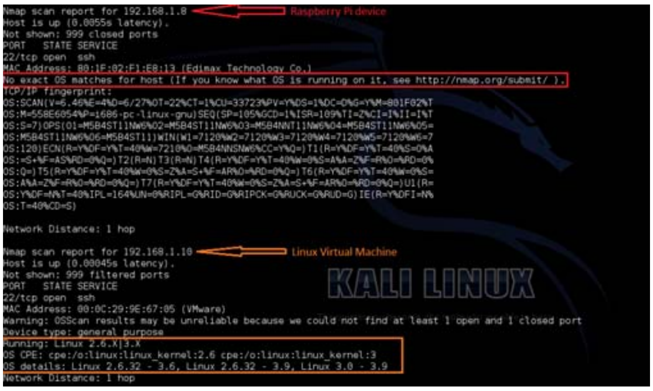
The bigger picture here is that with millions of Raspberry Pi devices in millions of homes, the devices can be hijacked and turned into an army of botnets that can be used to participate in a mass email spamming or distributed denial-of-service attacks (DDoS), hence it is recommended that a policy should be put in place to enforce changing the password after installation. In addition, port 22 should be filtered using a firewall or closed when remote logon is not required.

Operating System Fingerprinting

It was observed that the Raspberry Pi device does not give as much footprints in network scanning using tools like Nmap as does the PC or Laptop platform; an operating system scan was performed on the network using the command Nmap –O (Figure 13) and Nmap –A, but the results of the scan indicates that the Raspberry Pi device does not return any information about the operating system it is running. This is a good thing as it makes it challenging for an attacker to determine the existence of the device on a network. The result of the Nmap –A command however gave a guess about the operating system, but this is only a guess as the kernel version of the operating system was not revealed. This can still pose a challenge for an attacker because most network equipment like switches and routers run operating systems that are Linux kernel based.

Forensic Toolkit

1) *ProDiscover and FTK:*



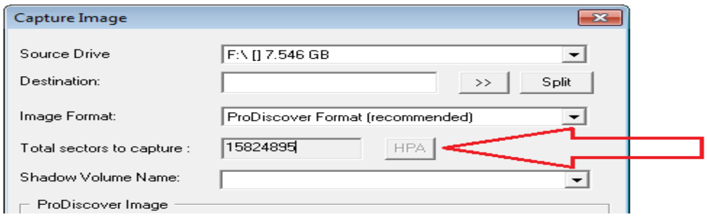
```
Nmap scan report for 192.168.1.8
Host is up (0.0055s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 80:1F:02:F1:E8:13 (Edimax Technology Co.)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.46%E=4%D=6/27%OT=22%CT=1%CU=33723%PV=Y%DS=1%DC=D%G=Y%M=801F02%T
OS:M=558E6054%P=i686-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=I%II=I%T
OS:S=7)OPS(O1=M5B4ST11NW6%O2=M5B4ST11NW6%O3=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=
OS:M5B4ST11NW6%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7
OS:120)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)

Network Distance: 1 hop

Nmap scan report for 192.168.1.10
Host is up (0.00045s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:9E:67:05 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.6, Linux 2.6.32 - 3.9, Linux 3.0 - 3.9
Network Distance: 1 hop
```

Figure 13. Result of the *Nmap -O* command to query for operating system

It was observed that the forensic tool *ProDiscover* is only able to view the FAT partition of the SD card; this is the reason why *ProDiscover* could not be used for data acquisition in this work as proposed. It was furthermore observed that *ProDiscover* and FTK does not copy the master partition table of a physical media; the master partition table (MPT) which usually takes up the very first few sectors of the physical storage device contains information about start and end of sectors of all partitions that exists on the media, this MPT is additionally used to hold the master boot record (MBR) in bootable media. *ProDiscover* and FTK only showed partitions (NTFS or FAT formatted) that exist on the physical device, whereas the MPT is not part of a partition; this explains why the tool could not access. Other toolkit may be used in the near future as the second stage.



Capture Image

Source Drive: F:\ [] 7.546 GB

Destination:

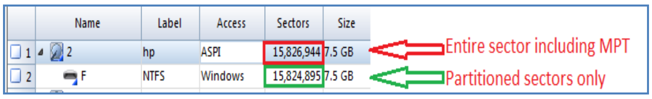
Image Format: ProDiscover Format (recommended)

Total sectors to capture : 15824895

Shadow Volume Name:

ProDiscover Image

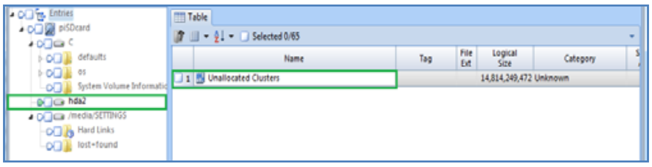
Figure 14. ProDiscover acquires only partitioned sectors excluding the MPT



	Name	Label	Access	Sectors	Size
□ 1	2	hp	ASPI	15,826,944	7.5 GB
□ 2	F	NTFS	Windows	15,824,895	7.5 GB

Figure 15. Encase gives option of acquiring the entire disk or partition

2) ***Encase:*** Moreover, it was observed that while the version of Encase available for this work was able to create the image of the entire SD card, it was unable to access the extended partition for analysis as shown in Figure 16 below.



	Name	Tag	File Ext	Logical Size	Category
□ 1	Unallocated Clusters			14,814,249,472	Unknown

Figure 16. Encase unable to access extended partition of image for analysis

VIII EVALUATION

This section presents the evaluation of this work. The approach of evaluation was through comparison to established platform, standards, and relevant/related works on other platforms. The elements of this work being evaluated are; the overall approach of the work, the approach to device's storage medium study and the results.

Overall Approach

Scientific method of approach has been used to attain numerous achievements through the ages, the manner of approach that was observed during the course of this work will be likened to stages involved in scientific method in an effort to evaluate and justify if it was worthwhile and/or meets its objectives.

- ***Observation***: This work was conceived as a result of the observation of the global popularity of the Raspberry Pi computer as a result of its cost effectiveness and potentials. This observation led to questions and the need to provide answers to these questions led to the initiation of this work

- ***Evidence Questions***:

1) Does this global popularity of the Raspberry Pi device raise any security issue?

2) Have there been any study or work relating to Raspberry Pi forensics in the field of digital forensics science.

The need for answering to these questions led to a research being initiated.

- ***Research***: The study of the basic operations and structure of the Raspberry Pi device was conducted using various approaches, methods, models and so on in an effort to establish possibilities of answers to the identified questions.
- ***Hypothesis***: The output of the study of the structure and operation of the device shed some lights which led to making strong assumptions about a possible security issue and the need for a Raspberry Pi forensic study in the field of digital forensics.
- ***Experiment***: In order to test assumptions in an effort to confirm or discard hypothesis, a scenario was setup to simulate a real life situation. Attacks were attempted and the investigative process was observed which served as a baseline study for Raspberry Pi forensic investigation.
- ***Analysis***: Results were analyzed which confirms hypothesis and recommendations were made
- ***Conclusions***: Analysis of the result was used to draw conclusions and identified evidential information were presented

Device's Storage Medium Study Approach

A key approach applied in this work was the use of the concept of abstraction layers to structure the study. The concept of abstraction is a proven method employed in computing to categorize data processing into manageable chunks for better understanding during study and troubleshooting following implementation; for example in the International Organization for Standardization, Open System Interconnect (OSI) model for computer networking. This concept of abstraction layers was used to design and structure a simple but all-encompassing model like the OSI model that was used to approach the study of the Raspberry Pi SD card storage medium in this work.

Show Result

Results were presented in the form of report. Some of the identified evidential information presented as a result of this work can be compared to those already available on established operating systems, like Windows. The table below presents the comparison between some of the identified evidences and locations.

	Windows	**Raspbian**
Installed/ Uninstalled Applications	_C:\Windows\System32\config\software\Microsoft\Windows\CurrentVersion\Program Path_	_/home/pi/apt/history.log_
Wireless network	_C:\WINDOWS\system32\config\software\Microsoft\WZCSVC\Parameters\Interfaces_	_/var/log/user.log_
USB Devices	_C:\WINDOWS\System32\config\system\ControlSet00x\Enum\USBSTOR_	_/var/log/kernel.log_
Mounted Devices	_C:\Windows\System32\config\system\MountedDevices_	_/dev/sd*_
Browser History	_C:\Windows\System32\config\Software\Microsoft\Internet Explorer_	_/home/pi/.config/ ephy-history.db:_
Users Logon Credentials	_C:\Windows\System32\config\SAM_	_/etc/shadow_

Table 4 Comparison of similar evidential information in Windows/Raspbian

IX CONCLUSION & SUGGESTED FURTHER WORKS

This work has identified, through demonstration, the possibility of how the Raspberry Pi device can be easily compromised due to a poor (default) configuration, a potential security threat that may arise if it should occur and the recommendations to ensure cyber secure usage of the device.

Besides, we have identified through study, possible evidential information available for the purpose of digital forensic investigation of the device.

While this work was not a thorough and comprehensive look at all areas of the Raspberry Pi device that will be useful for purpose of digital forensic investigations, it has paved way for further study to be carried out in the subject area and as a result the following further works identified are suggested.

- Raspberry Pi Memory Forensics
- Low level file system forensics of the device's SD card storage media (EXT and FAT)

- Study of the physical structure and operations of the SD card (Flash memory, Read/Write Controller, Data Writing and Reading techniques)

- A research and comparison of other optimized operating systems for the Raspberry Pi device, e.g. Kali Linux, Arch Linux, Pidora, EXEC and so on.

- The potential security that can arise as a result of such compromise (DDoS participation)

- The evidential information available for digital forensic investigation purpose if the device is compromised (Raspberry Pi storage medium analysis)

- *ProDiscover* and Encase cannot be used to analyze ext4 file system. New toolkit is needed.

Through this research project, an investigation cyber security issues and evidential information recoverable from the Raspberry Pi devices has been carried out. The device as a botnet attacker and as an attack target are both tested for Digital Forensics Investigations.

Our research has paved way for further comprehensive exploration of all areas of the Raspberry Pi device security to be carried out in the digital forensic investigations domain.

In conclusion, Raspberry Pi device could play an IoTS network node device to sort out process limitation problem in healthcare. With its capability, there are potentials in IoTS healthcare to form a local process center to deal with big data in a distribute manner. We have demonstrated the IoTS node security when we go on, more benefit can be gained. We have explored the PII impact with Healthcare Systems as well. Raspberry Pi as a node processor, its security directly affected users' confidence.

REFERENCES

Azfar A, Choo K-K R and Liu L (2016), “An Android Social App Forensics Adversary Model”. In Proceedings of 49th Annual Hawaii International Conference on System Sciences (HICSS 2016), pp. 5597, IEEE Computer Society Press. http://dx.doi.org/10.1109/HICSS.2016.693

Anderson, R (2011), “Security Engineering”, 2nd Ed. Wiley UK 2011.

Beebe N and Clark J. (2005), “A Hierarchical, Objectives-Based Framework for the Digital Investigations Process”, Digital Investigation 2(2), pp 146. http://www.elsevier.com

Carrier B. (2003), "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," International Journal of Digital Evidence, vol. I, no. 4, 2003.

Carrier, B. (2005), “File System Forensic Analysis”, Indiana: Addison Wesley Professional, 2005, ISBN: 9780321268174

Carrier B. and Spafford E. H. (2003), "Getting Physical with the Digital Investigation Process," International Journal of Digital Evidence, vol. II, no. 2, 2003.

Carrier B. and Spafford E. H. (2004), "An Event-Based Digital Forensic Investigation Framework," 2004. http://www.dfrws.org/2004/day1/Carrier-event (18/5/2015)

Cohen, R. (2012) 'The past, the present, and the future of cloud computing', Intel Technology Journal, 16 (4), pp.20-24.

Conrad, Marc, Feng, X. & Gibbon, M. (2016), “The Forensics of Cyberstalking”, submitted to NCCR for Cyberstalking, Palgrave MacMillan Pivot, the Series on Cyber psychology.

Cox, S.; Cox, J.T.; Boardman, R. P.; Johnston, S. J. Scott M. and O’Brien, N.S. (2014), "Iridis-pi: a low-cost, compact demonstration cluster," Cluster Computing, vol. 17, no. 2.

DFRWS (2001), "Workshop 1 - A Framework for Digital Forensic Science," in A Road Map for Digital Forensic Research, G. Palmer, Ed., New York, DFRWS, 2001

Duncan Geoff (2014). “You can’t avoid the ‘Internet of things’ hype, so you might as well understand it”. http://www.digitaltrends.com/home/heck-internet-things-dont-yet/ (Accessed 18/7/2016).

EY (2015), “Cybersecurity and the Internet of Things, Insights on governance, risk and compliance”, March 2015 http://www.ey.com/Publication/vwLUAssets/EYcybersecurity-and-the-internet-of-things/$FILE/EYcybersecurity-and-the-internet-of-things.pdf (Accessed: 08/08/2015).

Fahad Abdullah Al (2015), “Cloud Computing Security Policy”, University of Bedfordshire, UK.

Feng X. and Zhao Y. (2016), “Digital Forensics Challenge to Big Data at the Cloud”, accepted by the Big Data & Smart Sustainable Society Workshop -2016, Toulouse-France.

Feng X. (2016), “Digital, Mobile Forensics and Cyber-Stalking”, University of Bedfordshire Annual Conference

Feng X. Onafeso, B. and Iron, A. (2015), “Digital Forensics Smart City Project with Raspberry Pi Cluster”, HEA 11th Annual Teaching Computer Forensics Workshop, UK

Feng X. Onafeso Babatunde and Liu E. (2015), “Investigating Security Issues and Evidential Big Data Recoverable from a Raspberry Pi Device for Healthcare Services” IoTBDH, UK.

Feng, X. and Zhang X. (2015), “Personally Identifiable Information Security in Cloud Computing”, IEEE International Conference on Computing and Technology Innovation (CTI-2015), May 2015,

Farrell Paul (2015), “Personal details of world leaders accidentally revealed by G20 organisers”, The Guardian, http://www.theguardian.com/world/2015/mar/30/personaldetails-of-world-leaders-accidentally-revealed-by-g20-organisers (Accessed: 31/3/2015)

GitHub (2015), "NOOBS (New Out of Box Software)," 2015. https://github.com/raspberrypi/noobs/blob/master/README.md. (Accessed: 30/5/2015).

GitHub (2015), "NOOBS partitioning explained," 2015. Available:https://github.com/raspberrypi/noobs/wiki/NOOBS-partitioningexplained. (Accessed 30/5/2015).

ICO (2014), “Find out how to request your personal information”http://ico.org.uk/for_the_public/personal_information. (Accessed: 7/5/2015).

ILX(2015) “What is PRINCE"https://www.prince2.com/what-is-prince2 (Accessed:17/5/2015).

ISO27018 (2014), “Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO 27018 Standard” http://www.iso27001security.com/html/27018.html (Accessed: 24/3/2015)

Jeffreys, A.; Wilson V. and S. L. Thein S.L. (1985), "Individual-specific "fingerprints" of human DNA," Letters to Nature, vol. 316-4, 1985.

Khoshgozaran A.; Shirani-Mehr Houtan and Shahabi C. (2012), “Blind evaluation of location based queries using space transformation to preserve location privacy”, Geoinformatica Journal, Volume 27, Issue 2, pp 413-427, ISBN: 978-3-642-03510-4 Nov 2012.

The Linux Information Project (2006), "Root Filesystem Definition," 2006. http://www.linfo.org/root_filesystem.html. (Accessed: 5/6/2015)

The Linux Information Project (2007), “The Linux Information Project, 2007”. Available: http://www.linfo.org/index.html. (Accessed: 5/6/2015)

Liu, E. and Feng X. (2014): “Trustworthiness in the Patient Centred Health Care System, Series: Communications in Computer and Information Science”, Volume, 426, SpringerVerlag, March, 2014

Nelson, B. Phillips A. and Steuart C. (2015) “Guide to Computer Forensics and Investigations”, Boston: Cengage Learning, 5th Ed. 2015.

Pollitt, M. (1995), "Computer Forensics: an Approach to Evidence in Cyberspace," National Information Systems Security Conference, vol. II

Rajchada C. et al (2016) “Forensic analysis and security assessment of Android m-banking apps” http://dx.doi.org/10.1080/00450618.2016.1182589 (Accessed: 21/11/2016)

Raspberry Pi Foundation (2011), “Raspberry pi” https://www.raspberrypi.org/about/. (Accessed: 8/5/2015)

Raspberry Pi Foundation (2015) "The Making of Pi," 2015. https://www.raspberrypi.org/about/. (Accessed: 8/5/2015).

RAUT, S. (2008) "Development of FORENSIC SC. through Ages"http://www.santoshraut.com/forensic/forensichistory.htm (Accessed: 11/5/2015).

Upton, L. (2014) "RACHEL-Pi – delivering education worldwide". https://www.raspberrypi.org/rachel-pidelivering-educationworldwide/ (Accessed: 8/5/ 2015).