International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

Extraction of Persistent, Nonvolatile and Deleted Data from Windows Phone without JTAG Implementation

Diwakar Yash Dilipkumar[1], Dr. Ravi K Sheth[2]
[1]Student, Raksha Shakti University, Ahmedabad, Gujarat, India
[1]Assistant Professor, Department of IT, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT

Cybercrime is spreading day by day and now become a part of routine life of users. With easily availability of smartphones and internet, which creates opportunity for the cyber criminals to commit such cybercrimes by utilizing smartphones. In today's world the majority of the devices used in day to day life are Android and iOs but still there are some Windows Phone available in use. In the black market the price of Windows Phone is high due to its high security features and lake of available forensic tools. Before the seizure of AlphaBay and Hansabay (TOR Marketplace) the price of windows phone was high due to secure file system and robust architecture of Windows Phone. The available tool are not sufficient for extracting the forensic artifacts. So in this paper author has proposed and implement the method which is used for physical acquisition without using JTAG on hardware of windows Phone to extract persistent, nonvolatile and deleted data.

Keywords : Windows Phone Forensic, Mobile Forensic, Cyber Forensic, Data Carving, Device Recovery

I. INTRODUCTION

Smartphones provide all-most similar features and functionality which are available in Computers and Laptops. The mobility and flexibility is the main features which is used to store their personal and confidential information. Easy communication via internet technology provides feasibility to share and communicate on social media, Emails, internet banking, and web browsing. Android, ios and windows are the major operating systems for smartphones. Nowadays smartphones are used as a tool and medium to commit a cybercrime. In this paper we describe that the physical image of the windows phone can be generated without JTAG or any hardware tweaks. In JTAG the risk of device failure is high. This research considers the acquisition and forensic analysis of the windows phone.

Microsoft developed Windows Phone Opertaing System absolutely free in September 2010. Since the starting of the device of Windows Phone (WP) devices are available in limited data sets hence the crimes using WP is also on the increase. In the Darkweb the black-market place – Alphabay and Hansabay sold many Windows phone due to its high security features and security. Criminals use that phone to commit crime. Windows Phone comes with software version 8, 8.1 and 10 These versions have lots of variations in their design, practicality and its implementation within the device.

II. WINDOWS PHONE ARCHITECTURE

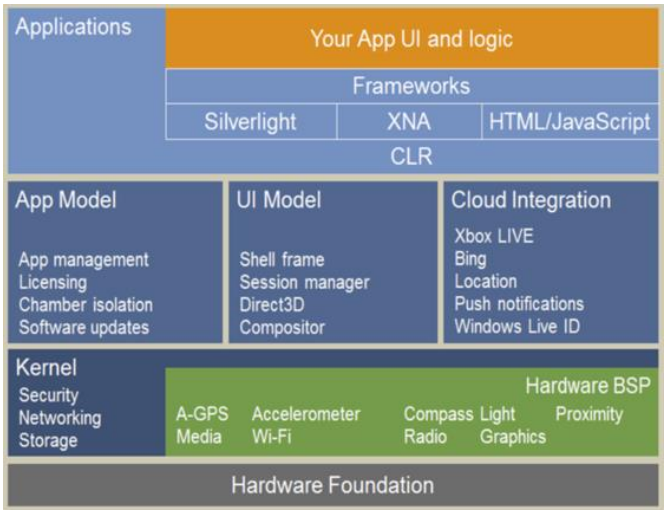

Figure 1. Windows Phone Architecture

In the architecture of Windows Phone, the First layer is Hardware Foundation which provide full access to the hardware. After that kernel the OS has been loaded to the main memory. In the architecture of windows phone the application uses custom space which cannot be shared with other app. [1]

As come to the Boot process it contains UEFI and Sauceboat Components. Secure boot is a feature of UEFI that helps to protect device against malware. Trusted Boot checks the bootloader is trusted or not. [2].

JTAG- Joint Test Action Group is the industry standard which should be followed by the PCB manufacturers. Which is mainly used for storing the firmware and transfer data into non-volatile device memory. For each and every manufacture has to follow IEEE standard and to provide JTAG points available at the circuit board. For JTAG some opensource tools are available and some commercial tools are available which provide accurate trace analysis and simulator.

III. ACQUISITION TYPE

Direct Acquisition-

The direct acquisition techniques are generally performed on the windows phone if the appropriated device is either not secured or the PIN/Password/Pattern lock is known by the investigator, this manner each data accessible to the user is accessible to the examiner via the standard user interface (UI). solely the “disturbing” purpose is that if relying on only this methodology, system files, systems logs or system partition isn't accessible.

Logical Acquisition-

The logical acquisition could be a bit-by-bit copy of a given logical storage, (the storage might refer to user data partition similarly as system data partition), and this acquisition technique produces, in general, a relatively manageable file which might be analyzed and parsed by forensic tools. A full device backup, as an example, can be thought of as a logically acquired image.

Physical Acquisition-

Physical acquisition acquires information directly from hardware by direct access to a given disk or flash memory. Physically acquiring a device is usually a headache however if with success done, the created copies are often used to recover deleted fragments and permits the examiner to place his hands on information remnants. Physical acquisition continuously starts by a dumping phase then a decoding part.

IV. EXISTING SYSTEM

Currently there are some commercial tools available which provide the Logical Acquisition of the windows phone such as Magnet Forensic, MobileEdit Forensic, MobileCheck, Oxygen Forensic Suite, Paraben E3:DS etc. In the logical Acquisition of the device some of the information

can be obtained but deleted information cannot be obtained.

MobileEdit Forensic –
MOBILedit Forensic is also searches, examines and report on the different datasets available from Mobile devices. MOBILedit connects to cell phone devices via an Infrared (IR) port, a Bluetooth, Wi-Fi, or a cable interface. While connectivity has been established, the phone model is identified by its manufacturer, model number, and serial number (IMEI) and with a corresponding picture of the phone which is required for the proper data extraction. [3]

Windows Phone is a very robust OS, which gives it better security and stability, but there is no tool available which gives full access of the phone data. You can manage files using a few tools but it doesn't manage all your contacts, messages and other important information. So MbileEdit can read contact using Bluetooth and cable connection, manage media files. [4]

In this the device can detect the files which is available to the user via MTP mode connection.
MobileCheck
CDAC's MobileCheck is a digital forensics solution for acquisition and analysis of Mobile phones. It is used for the Logical Acquisition of the windows device which give Files and Folder information. [5]

Magnet AXIOM Process –
Magnet AXIOM Process is used for analysis and logical acquisitions of windows phone. Magnet Internet Evidence Finder (IEF) has added support for a number of native and third-party apps for Windows Phone. This tool creates Windows Phone image acquired through JTAG or Chip-off, and a few of the artifacts that have been added with the IEF. This required skilled person to handle this tool properly. [6]

Parabean E3:DS –
Paraben's E3:DS tool was designed for acquisition process for Windows Phone7 model and also it provides contact, image and calendar.

Oxygen Forensic Suite-
Oxygen Forensic Suite is leading examination tools for smartphones and other type of mobile devices. It is mainly used to acquire information stored in Windows Phone accounts directly (login and password required). Physical Windows Phone device is not needed to acquire or decrypt the data which is called cloud extraction of the data and it parse Contacts and Messages. [7]

For the physical Acquisition of the windows phone you have sound knowledge of hardware (RIFF JTAG Box, PCB) and chip assembly. It is also important to find out proper JTAG point available in the Windows phone hardware. [8]

V. METHODOLOGY

In this paper we have implemented the method by which we can acquire physical dump of the windows phone. There is no requirement of PIN unlock or not. We are able to unlock mass storage mode and connect phone to the Windows out special script to find the artifacts from whole windows phone. When performing logical acquisition, the device provides the data.

Figure 2. Windows Phone Acquisition Model

Provided data is available in the device and while performing this method we can retrieve deleted data from unallocated space and slack space.

First of all by Reverse Engineering of Windows Device Recovery Tool find out the location of bootloader and the path which is used to convert phone to Mass storage mode. After that FTK Imager is used to create raw image of the whole windows phone. That raw image can be further analyzed into autopsy and that is used for data carving

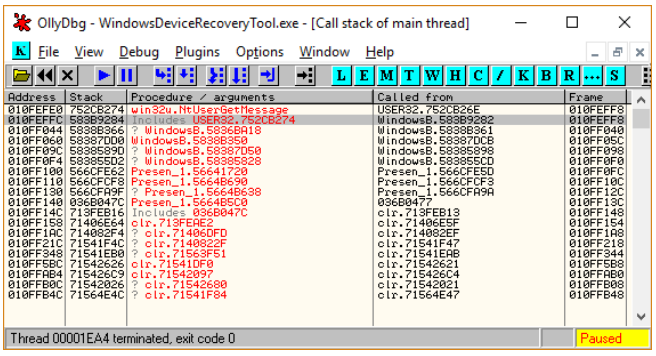

Figure 3. Winodws Device Recovery tool call stack

As per the windows phone acquisition model the windows phone was connected to the forensic workstation in MTP mode and after that the bootloader has been unlocked. To unlock the bootloader, we have done reverse Engineering of Windows Phone Device Recovery Tool and find out the location of the bootloader which can be unlocked while recovery process has been implemented.

While find call stack of main thread of WDRT find out the location address at 0x010FEFC which call USER32 dll file and at that location the conversion has been started from UEFI mode to Mass storage mode. After that we can easily create dd image of the windows phone by FTK Imager and that image can further analyze to recover the forensic artifacts from the windows phone.

As come to the data carving process the available data should be carved with the use of available tools and scripts.

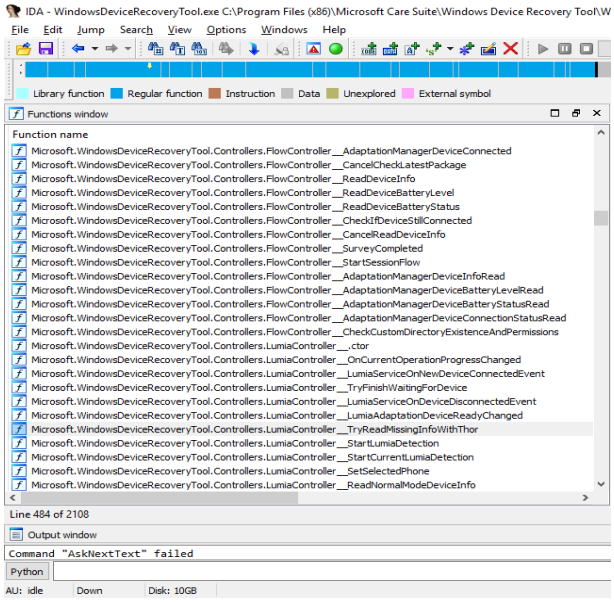

Figure 4. IDAPro View for finding the flow of WDRT

For the analysis purpose no single tools can be used. In the forensic process single tools are not sufficient for the complete analysis. So, mixture of both OS windows and Linux can be implemented in the latest feature of Windows 10 Operating system as Windows Subsystem Linux. WSL used to switch from windows kernel to Linux kernel easily while using custom script that is used to analyze the artifacts recovered by the raw image file.

Custom Script

For the analysis purpose the custom script has been implemented in Windows Subsystem Linux which find the Forensics artifacts from the carved data.
Custom Script uses shell script, python and follow the below sequence.

1) Run batch file while connecting windows phone via standard USB cable to forensic workstation which must be windows 10.
2) Script will have initiated device to the recovery mode and put it into mass storage stage.
3) After that by using FTK Imager the raw image of the connected physical device has been made.
4) Autopsy is used to carve the data.
5) After that command goes to WSL and that is convert carved data to the forensic Artifacts.

For this we have carved the Nokia Lumia 520 by using custom script which firstly unlock the bootloader and after that it take dd image of the windows phone and the forensic artifacts has been retrieved. For the call history, contact, SMS and MMS the store.vol file has been used to analyze.

We have parsed the 56 file system partitions from the raw image of windows phone using FTK. Now the aim is to recover call logs, text messages, deleted image/video, contacts, WhatsApp chat. For this the developed script is used to recover the call logs from the 'phone' database in the following location: -

\Users\WPCOMMSSERVICES\APPDATA\Local\User Data\.

As for the text messages, we know that these are stored in the 'store.vol' database in the following location: -
\Users\WPCOMMSSERVICES\APPDATA\Local\Unistore\.
And for the deleted data we have used opensource tool Autopsy which provide deleted data from unallocated space and slack space.
For the WhatsApp artifacts the architecture of WhatsApp for the windows has been consider and from that location the database of WhatsApp has been recovered.

VI. FINDING AND RESULTS

Table 1 – Recovered Artifacts Comparison

	MobileEdit Forensic	MobileCheck	Magnet AXIOM	Parabean E3:DS	Oxygen Forensic	WP Acquisition Model
IMEI	✓		✓	✓	✓	✓
Contact	✓	✓	✓	✓	✓	✓
SMS	✓		✓	✓	✓	✓
Call Log	✓	✓	✓	✓	✓	✓
MMS	✓		✓	✓	✓	✓
E-mail						✓

Catches						✓
IE Cookies						✓
Bluetooth Transfer list						✓
Cached History File						✓
PIN Hash						✓
Installed App list						✓
Wireless Network artifacts						✓
WhatsApp Artifacts						✓
Deleted Image/Video						✓

VII. CONCLUSION

Currently available tools provide the data which does not generate sufficient forensic artifacts. So in this paper we can conclude that with the physical acquisition of the windows phone we are able to acquire deleted data as well as the data which is accessible by direct acquisition. So We can say that the physical acquisition of the windows device is possible and we are able to recover SMS, Call History, Contacts, MMS, Deleted data including deleted multimedia. As compared to other tools on such tool is present which provide this much amount of data.

VIII. LIMITATIONS

Windows phone provide feature called Bit locker encryption, which is by default not enable nut if user has enable it the whole data is encrypted from hardware layer. If device is encrypted with bit locker this method cannot provide full decrypted artifacts.

IX. FUTURE WORKS

In the extension of this project the unencrypted dump should be taken or to find the methodology by which the bit locker key should be recovered first to decrypt the encrypted data. To bypass bit locker some method would be develop.

X. REFERENCES

[1]. Adesina, Ganiyu. (2014). Mobile Operating Systems and Application Development Platforms: A Survey. 6. 2195 - 2201. (https://www.researchgate.net/publication/279954676_Mobile_Operating_Systems_and_Application_Development_Platforms_A_Survey)

[2]. https://download.microsoft.com/download/B/9/A/B9A00269-28D5-4ACA-9E8E-E2E722B35A7D/Windows-Phone-8-1-Security-Overview.pdf

[3]. https://en.wikipedia.org/wiki/MOBILedit

[4]. https://support.mobiledit.com/portal/kb/articles/connecting-windows-phone

[5]. http://www.cyberfore+nsics.in/Products/MobileCheck.aspx

[6]. https://www.magnetforensics.com/mobile-forensics/analyzing-windows-phone-artifacts-with-ief/

[7]. https://www.oxygen-forensic.com/en/events/press-releases/413-oxygen-forensic-suite-2014-data-acquisition-from-my-windows-phone

[8]. Kumar, Satheesh & Kumar, Jinu & Suresh, Jithin. (2015). A Novel Method for Windows Phone Forensics. International Journal of Scientific and Engineering Research. 6. (https://pdfs.semanticscholar.org/6bc3/adbd00307c2393983ff8da97026b3c3d8e4d.pdf)

[9]. https://www.forensicswiki.org/wiki/JTAG_Nokia_Lumia_620