Thesis Proposal

Name: Sudip Hazra

Proposed Topic: I want to work in Proactive Android Forensics. I am particularly interested in continuing the work of Aiyyappan and Karthik in building a Proactive androd forensic ROM.

Advisor: Prof. Prabhakar Mateti (Wright State University)

Background:

Smartphones nowadays are capable of doing a multitude of tasks which was not possible with conventional phones, with the increase in complexity of smartphones , Forensics Investigators are finding difficulty in gathering forensic artifacts for evidence. Conventional evidence collection involves seizuire of electronic evidence and then dumping the physical memory to search for artifacts. There are dedicated devices such as Celebrite UEFD Classic forensic tool. Softwares were also used to find artifacts in the phone memory ,however the usefullness of these tools are only limited to the availability of data after the crime, If the criminal is smart enough he either encrypt the data or can easily use applications such as uninstall-it to remove any user data and then format the phone multiple times to remove any traces of his criminal activity, the forensics investigator will be helpless in such scenario and the criminal will walk free.The need for proactive forensics arises from here, proacttive forensics can help the investigator get the relevant artifacts even if the data has been deleted.Smartphones are also being used by terrorists and anti-socials to evade authorities as some apps used by them encrypts the communication between two-parties like whatsapp and telegram. In this situation , if we are able to develop a framework which can proactively monitor user activities in real-time then it will be of immense help to forensics investigators. The framework must be able to transmit user data in stealth to avoid detection by suspicious parties .Also the framework must be able to monitor Network connections as well as user activities. The data has to be uploaded in stealth to the cloud as the amount of data generated must be huge and it will cause device lag and memory consumption in phone memory. The framework must also be able to download the data in machine of the investigator and an automated tool will generate the report of the artifacts to create Solid evidence which can be produced in court.

The android mobile has several partitions and out of it the userdata and cache partition are most important in terms of investigation because they contain user data.In the android file hierarchy the /cache ,/data,/sbin ,/sdcard are important for forensics investigations.

Related Work

Forensic Analysis of Instant Messenger Applications on Android devices.
Adiya Mahajan Et.al have done forensic investigation on whatsapp and viber using Celebrite UEFD Classic device , they were able to extract whatsapp and viber data however on using the physical analyzer software of Celebrite, it succeeded incase of whatsapp but failed in case of viber. Manual Analysis of the viber folder were needed. Pretty much everything was extracted like chat messages, images videos with timestamp, however the data in internal memory of sdcard was encrypted.

Critique:
They did not test it after the deleting the data , was the tool able to extract data from the unallocated space is unknown.

Whatsapp Network Forensics: Decrypting and understanding the whatspp call signalling messages
Karpisek Et. Al studied the calling feature in whatsapp where they first de-synchronised the full handshake of whatspp and then monitored the entire handshaking procedure. Whatsapp was using OPUS voice codec in RTP .
They were able to observe the entire call process where a connection with atleast 8 whatsapp servers were made between calls .

Critique: I coulnot find as such beacause of my lack of knowledge of the whatsapp protocol, OPUS codec and RTP.

Forensics Analysis of Whatsapp Messenger on Android Smartphones
Anglano Et.Al wrote a very good paper decoding the whatsapp artifacts and step by step linking to what is the greater picture . Artifacts were carefully correlated to infer all the required information and tracing events even if the messages were deleted using whatsapp logs.

Critique: Very little support what will happen if whatsapp is removed using Uninstall-it like app or the phone is formatted.

M.S Thesis on Forensic Analysis of whatsapp on Android Smartphone
Neha Thakur
Whatsapp Forensics can be done in two ways :
If whatsapp folder is in Sdcard can be decrypted using WhatsapXtract Tool which is now obsolete beacause the Key has changed andd we need to edit the code to add the new key.
Memory Forensics of volatile memory can also be done , suing memfetch to extract selective portions of ram , taking the heap of the selected appliaction and running data extraction tool on the memory dump. Recently deleted messages can be easily discovered. Used a tool called WhatsappRamXtract.

Network and device Forensics analysis of Android Social-Messaging Applications

Walnycky Et.Al took a survey of Network Forensics of 20 most popular Android Messaging Apps Unfortunately only 4 apps passed the of privacy . TextMe might be a potential trojan and some apps even send the messages over the network in plaintext. In Apps like MessageMe ,MeetMe ,Oovoo the author was able to see both sent and received messages in plaintext. Full Video reconstruction was possible in case of Tango,Nimbuzz,MessageMe.Whatsapp succesfully passed the test. MITM is perfectly possible in some apps, They used an program called Datapp to generate the report.

Android Forensics : Automated Data Collection and Reporting Tool for Mobile Device
Justin Grover made the first of its kind android forensics tool which collected data with user consent and uploaded it to a remote server. The capabilities are limited and are susceptible to tampering . Droidwatch mainly uses content observers , Broadcast Receivers and Alarms for monitoring.Broadcast Receivers and Alarms can be tampered with. No data about social networking apps , no support was there for email.

Frost: Forensic Recovery of Scambled Telephones
Muller Et.Al deviced an forensic image which was flashed on to the phone and it was capable to bruteforcing Pin, direct recovery of encryption keys and decrypting user partition on phone itself. If the bootloader is locked not of much use , only option is to take memory dump.

Critique: All smartphones now comes with default locked bootloader, secondly only if the handset is instantly available to the expert , he can freeze the ram to minimize data loss and recover encryption keys from ram.

Smartphone Forensics : A proactive Investigative Approach.
Mylonas Et.Al suggested a proactive forensic framework which is regulated by an independent authority. Two modes of forensics namely Usermode and Network mode.

Critique: No information about Implementation , was the phone rooted or unrooted, functionality of the app not given.

Androphsy: Forensic Framework for Android
Akarawita Et.Al implemented a forensic framework which can acquire data both Physically and logically from the android smartphone. For physical acquisition they used DD program to clone the system image. For logical acquisition they use adbpull to clone the filesystem partition, other tools used were logcat,demsg ,dumpsys,scalpel and adb getprop to get device properties.Used Netcat to copy the system files to a remote server. It was better than other Opensource Forensic tools like Oxygen and ViaExtract CE tool. Rooting of the phone is necessary.

WorkDone
Studying various android system partitions and researching to add more stealth and added functionality to the framework developed by aiyyappan and karthik.Possible work can be adding borello's technique where he modifies the libc readdir.c , and hides the process however sysdig can see the hidden process .We can add the borello's method in libc directly with specific arguments, which when supplied the process will be shown.We can write a tool which automates the whole process of report generation based on relevant artifacts.Adding support to few more social networking apps and linking of messages, calls from this apps in relevant way to get the bigger picture , this can however be implemented in report generation tool.

References
1. Aiyyappan, P. 2015. Android forensic support framework. M.Tech thesis, Amrita Vishwa Vidyapeetham,Ettimadai, Tamil Nadu 641112, India. Advisor: Prabhaker Mateti.
http://cecs.wright.edu/~pmateti/GradStudents/index.html.

2. Karthik K.2016,Proactive Forensic Support for Android Devices,M.Tech thesis, Amrita Vishwa Vidyapeetham,Ettimadai, Tamil Nadu 641112, India. Advisor: Prabhaker Mateti.

http://cecs.wright.edu/~pmateti/Students/Theses/karthik-mtech-2016.pdf

3.Forensic Analysis of WhatsApp on Android Smartphones,M.S Thesis, Neha S. Thakur, University Of New Orleans,2013 ,http://scholarworks.uno.edu/td/1706/.

4.Akarawita, I. U., Perera, A. B., and Atukorale, A. 2015. Androphsy–forensic framework for Android. In International Conference on Advances in ICT for Emerging Regions (ICTer). Vol.250. 258.

5.Alexios Mylonas Et.Al ,Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition. Springer Volume 376 of the series IFIP Advances in Information and Communication Technology pp 249-260.

6.Tilo Muller, Michael Spreitzenbarth, and Felix C. Freiling ,Frost(Forensic Recovery of Scrambled Telephones) ,https://www1.cs.fau.de/filepool/projects/frost/frost.pdf.

7.Android Forensics : Automated Data Collection and Reporting Tool for Mobile Device, http://www.sciencedirect.com/science/article/pii/S1742287613000480.

8.Network and device Forensics analysis of Android Social-Messaging Applications,http://www.sciencedirect.com/science/article/pii/S1742287615000547.

9.Cosimo Anglano,Forensics Analysis of Whatsapp Messenger on Android Smartphones.http://arxiv.org/pdf/1507.07739.pdf

10.Mahajan Et.Al, Forensic Analysis of Instant Messenger Applications on Android Devices,International Journal of Computer Applications (0975 – 8887),Volume 68– No.8, April 2013.