Proactive Forensic Support to Android Device

FINAL PROJECT REPORT

Submitted by

KARTHIK M. RAO CB.EN.P2CYS14006

in partial fulfillment for the award of the degree of

MASTER OF TECHNOLOGY
IN
CYBER SECURITY

TIFAC-CORE IN CYBER SECURITY
AMRITA SCHOOL OF ENGINEERING
AMRITA VISHWA VIDYAPEETHAM
COIMBATORE - 641 112

MAY 2016

Proactive Forensic Support to Android Device

FINAL PROJECT REPORT

Submitted by

KARTHIK M. RAO CB.EN.P2CYS14006

in partial fulfillment for the award of the degree of

MASTER OF TECHNOLOGY
IN
CYBER SECURITY

Under the guidance of

Prof. Prabhaker Mateti
Associate Professor
Computer Science and Engineering
Wright State University
USA

TIFAC-CORE IN CYBER SECURITY
AMRITA SCHOOL OF ENGINEERING
AMRITA VISHWA VIDYAPEETHAM
COIMBATORE - 641 112

MAY 2016

AMRITA VISHWA VIDYAPEETHAM
AMRITA SCHOOL OF ENGINEERING,COIMBATORE -641 112

BONAFIDE CERTIFICATE

This is to certify that this final project report entitled **"Proactive Forensic Support to Android Device"** submitted by **KARTHIK M. RAO (Reg.No : CB.EN.P2.CYS14006)** in partial fulfillment of the requirements for the award of the **Degree of Master of Technology** in **CYBER SECURITY** is a bonafide record of the work carried out under my guidance and supervision at Amrita School of Engineering.

Dr. Prabhaker Mateti
(Supervisor)

Dr. M. Sethumadhavan
(Professor and Head)

This final project report was evaluated by us on.....

INTERNAL EXAMINER

EXTERNAL EXAMINERS

AMRITA VISHWA VIDYAPEETHAM
AMRITA SCHOOL OF ENGINEERING,COIMBATORE
TIFAC-CORE IN CYBER SECURITY

DECLARATION

I, KARTHIK M. RAO (Reg.No: CB.EN.P2.CYS14006) hereby declare that this final project report entitled **"Proactive Forensic Support to Android Device"** is a record of the original work done by me under the guidance of **Prof. Prabhaker Mateti**, Associate professor, Wright State University, and this work has not formed the basis for the award of any degree / diploma / associateship / fellowship or a similar award, to any candidate in any University, to the best of my knowledge.

Place : Coimbatore

Date : Signature of the Student

COUNTERSIGNED

Dr. M. Sethumadhavan
Professor and Head, TIFAC-CORE in Cyber Security

ABSTRACT

Keywords:

Contents

1 Introduction **1**

1.1 Known things about Android . . . 1
1.2 Motivation . . . 1
1.3 Problem Statement . . . 1
1.4 Aim . . . 1
1.5 Organization . . . 1

2 Background **2**

2.1 Mobile Forensics . . . 3
2.2 Forensic Analysis Techniques . . . 3
2.2.1 Timeline Analysis . . . 3
2.2.2 File System Analysis . . . 3
2.2.3 File Carving . . . 3
2.2.4 Strings . . . 3
2.2.5 Hex . . . 3
2.3 Challenges in mobile forensics . . . 3
2.4 Ethics . . . 3
2.5 Why Android? . . . 3
2.6 Data Storage in Android . . . 3
2.7 Android Partitions . . . 3
2.8 Stealth File Volumes . . . 3
2.9 Monitoring File and Directory Changes . . . 3
2.9.1 FileObserver . . . 3
2.9.2 inotify . . . 3
2.9.3 Other file monitoring tools . . . 3
2.10 Sand-box . . . 3

2.11 Sensor data as evidence . . . 3
2.12 Integrity of forensically sound data . . . 3
2.13 Encryption . . . 3

3 Proposed System **4**
3.1 Architecture of Forensic module . . . 5
3.1.0.1 Primary Sources . . . 5
3.1.1 Secondary Sources . . . 5
3.1.2 Temporary Storage . . . 5
3.1.3 Evidence Transmission . . . 5
3.1.4 Real Time Analysis . . . 5
3.1.5 Data Storage Phase . . . 5
3.2 Hiding Process . . . 5
3.3 Keystroke logging . . . 5
3.3.1 Using Swiftkey . . . 5
3.3.2 Using Man-in-the-Binder . . . 5
3.4 Call Recording . . . 5
3.5 Compression . . . 5
3.6 Sensor Details Capture . . . 5
3.7 Hashing . . . 5
3.8 Uploading to the cloud . . . 5
3.9 Real-Time Data Collection . . . 5
3.10 Stealth Challenges . . . 5

4 Related Work **6**
4.1 Ethics . . . 6
4.2 Companion Projects . . . 6
4.3 Commercial products . . . 6
4.4 Academic Research . . . 6
4.4.1 Proactive . . . 6
4.4.2 Reactive . . . 6
4.4.3 Forensic related . . . 7

5 Results and Discussion **8**
5.1 Status of Proposed System . . . 9
5.1.1 File system Changes detection . . . 9

5.1.1.1 `inotifwait` in Linux . . . 9
5.1.1.2 `inotifwait` in Android . . . 9
5.1.1.3 FileObserver . . . 9
5.2 Tracking user activities . . . 9
5.2.1 GPS and Network Location . . . 9
5.2.2 Sensor data . . . 9
5.2.3 WiFi metadata and router details . . . 9
5.2.4 Application installed . . . 9
5.2.5 Browser artefacts . . . 9
5.2.6 Calendar data . . . 9
5.2.7 Call log monitoring . . . 9
5.2.8 Dictionary word changes . . . 9
5.2.9 SIM details . . . 9
5.3 Call recording . . . 9
5.4 Keylogger . . . 9
5.5 Uploading to cloud . . . 9
5.6 Hide Forensic Process . . . 9
5.7 Stealth File Volume . . . 9
5.8 Impact on Battery Consumption . . . 9
5.9 Contribution to Lag . . . 9
5.10 Local Storage . . . 9

6 Conclusion and future work **10**

7 Appendix **11**
7.1 **Appendix A:** `inotifwait` in Linux . . . 11
7.2 **Appendix B:** FileObserver log . . . 11
7.3 **Appendix C:** Sample output of Sensors . . . 11
7.4 **Appendix D:** Sample output of phone artefacts . . . 11
7.5 **Appendix E:** Code to upload to Google Drive . . . 11

List of Tables

List of Figures

1

Introduction

1.1 Known things about Android

1.2 Motivation

1.3 Problem Statement

1.4 Aim

1.5 Organization

2

Background

2.1 Mobile Forensics

2.2 Forensic Analysis Techniques

2.2.1 Timeline Analysis

2.2.2 File System Analysis

2.2.3 File Carving

2.2.4 Strings

2.2.5 Hex

2.3 Challenges in mobile forensics

2.4 Ethics

2.5 Why Android?

2.6 Data Storage in Android

2.7 Android Partitions

2.8 Stealth File Volumes

2.9 Monitoring File and Directory Changes

2.9.1 FileObserver

2.9.2 inotify

2.9.3 Other file monitoring tools

2.10 Sand-box

2.11 Sensor data as evidence

3

Proposed System

3.1 Architecture of Forensic module

3.1.0.1 Primary Sources

3.1.1 Secondary Sources

3.1.2 Temporary Storage

3.1.3 Evidence Transmission

3.1.4 Real Time Analysis

3.1.5 Data Storage Phase

3.2 Hiding Process

3.3 Keystroke logging

3.3.1 Using Swiftkey

3.3.2 Using Man-in-the-Binder

3.4 Call Recording

3.5 Compression

3.6 Sensor Details Capture

3.7 Hashing

3.8 Uploading to the cloud

3.9 Real-Time Data Collection

3.10 Stealth Challenges

4

Related Work

4.1 Ethics

4.2 Companion Projects

4.3 Commercial products

4.4 Academic Research

4.4.1 Proactive

Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition

Adding Proactive Forensic Support to Android

ANDROPHSY – Forensic Framework for Android

Android Forensics: Automated data collection and re-porting from a mobile device

4.4.2 Reactive

FORENSIC ANALYSIS OF SMARTPHONES: THE ANDROID DATA EXTRACTOR LITE (ADEL)

New acquisition method based on firmware update protocols for Android smartphones

4.4.3 Forensic related

Analysis of WhatsApp Forensics in Android Smart-phones

Fingerprints On Mobile Devices Abusing And Leaking

Ensuring the Authenticity and Non-Misuse of Data Evidence in Digital Forensics

Learning guides

5

Results and Discussion

5.1 Status of Proposed System

5.1.1 File system Changes detection

5.1.1.1 `inotifwait` in Linux

5.1.1.2 `inotifwait` in Android

5.1.1.3 FileObserver

5.2 Tracking user activities

5.2.1 GPS and Network Location

5.2.2 Sensor data

5.2.3 WiFi metadata and router details

5.2.4 Application installed

5.2.5 Browser artefacts

5.2.6 Calendar data

5.2.7 Call log monitoring

5.2.8 Dictionary word changes

5.2.9 SIM details

5.3 Call recording

5.4 Keylogger

5.5 Uploading to cloud

5.6 Hide Forensic Process

5.7 Stealth File Volume

5.8 Impact on Battery Consumption

6

Conclusion and future work

7

Appendix

7.1 Appendix A:`inotifwait` in Linux

7.2 Appendix B: FileObserver log

7.3 Appendix C: Sample output of Sensors

7.4 Appendix D: Sample output of phone artefacts

7.5 Appendix E: Code to upload to Google Drive

References

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

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.

Arrigo, B. A. 2014. *Encyclopedia of Criminal Justice Ethics*. SAGE Publications.

Artenstein, N. and Revivo, I. 2014. Man in the binder: He who controls ipc, controls the droid. *BlackHat Europe*.

Borello, G. 2014. Hiding linux processes for fun and profit. `https://sysdig.com/hiding-linux-processes-for-fun-and-profit/`.

Casey, G. 2013. Inserting keylogger code in android swiftkey using apktool . `http://www.georgiecasey.com/2013/03/06/inserting-keylogger-code-in-android-swiftkey-u`

CCLuser. 2012. Android pattern lock scripts. `http://www.cclgroupltd.com/product/android-pattern-lock-scripts/`.

Easttom, C. and Murphy, G. 2015. *CCFP Certified Cyber Forensics Professional All-in-One Exam Guide*. McGraw-Hill Education.

George, N. 2015. Network Ombudsman for Android. M.S. thesis, Amrita Vishwa Vidyapeetham, Ettimadai, Tamil Nadu 641112, India. Advisor: Prabhaker Mateti.

GITE, V. 2014. Linux: Hide processes from other users. `http://www.cyberciti.biz/faq/linux-hide-processes-from-other-users/`.

Grover, J. 2013. Android forensics: Automated data collection and reporting from a mobile device. *Digital Investigation 10*, S12–S20.

Hoog, A. 2011. *Android forensics: investigation, analysis and mobile security for Google Android.* Elsevier.

Inc., I. R. 2015. Smartphone os market share, 2015 q2. http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

Kaladharan, Y., Mateti, P., and Jevitha, K. 2016. An encryption technique to thwart android binder exploits. In *Intelligent Systems Technologies and Applications*. Springer, 13–21.

Kamardeen, J. 2015. Auditing Android system for anomalous behavior. M.S. thesis, Amrita Vishwa Vidyapeetham, Ettimadai, Tami Nadu 641112, India. Advisor: Prabhaker Mateti; http://cecs.wright.edu/~pmateti/GradStudents/index.html.

Mateti, P., Aiyyappan, P., George, N., Kamardeen, J., Sahadevan, A. K., and Shetti, P. 2015. Design and construction of a new highly secure Android ROM. Tech. rep., Amrita Vishwa Vidyapeetham, Ettimadai, Tamil Nadu 641112, India. 6. Advisor: Prabhaker Mateti; http://cecs.wright.edu/~pmateti/GradStudents/index.html.

McGovern. 2012. Inotifywait for android. https://github.com/mkttanabe/inotifywait-for-Android.

Raja, H. Q. 2011. Android partitions explained: boot, system, recovery, data, cache and misc. http://www.addictivetips.com/mobile/android-partitions-explained-boot-system-recovery-data-cache-misc/.

Sahu, S. 2014. An analysis of whatsapp forensics in android smartphones. *International Journal of Engineering Research 3,* 5, 349–350.

Tamma, R. and Tindall, D. 2015. Learning android forensics.

Wikipedia. 2012. Android's architecture diagram. https://en.wikipedia.org/wiki/Android_(operating_system)#/media/File:Android-System-Architecture.svg.

Wikipedia. 2015a. inotify. https://en.wikipedia.org/wiki/Inotify.

Wikipedia. 2015b. Mobile device forensics. https://en.wikipedia.org/wiki/Mobile_device_forensics.

Yaghmour, K. 2013. *Embedded Android: Porting, Extending, and Customizing.* " O'Reilly Media, Inc.".