Forensic Investigation in Android Platform

Sudip Hazra

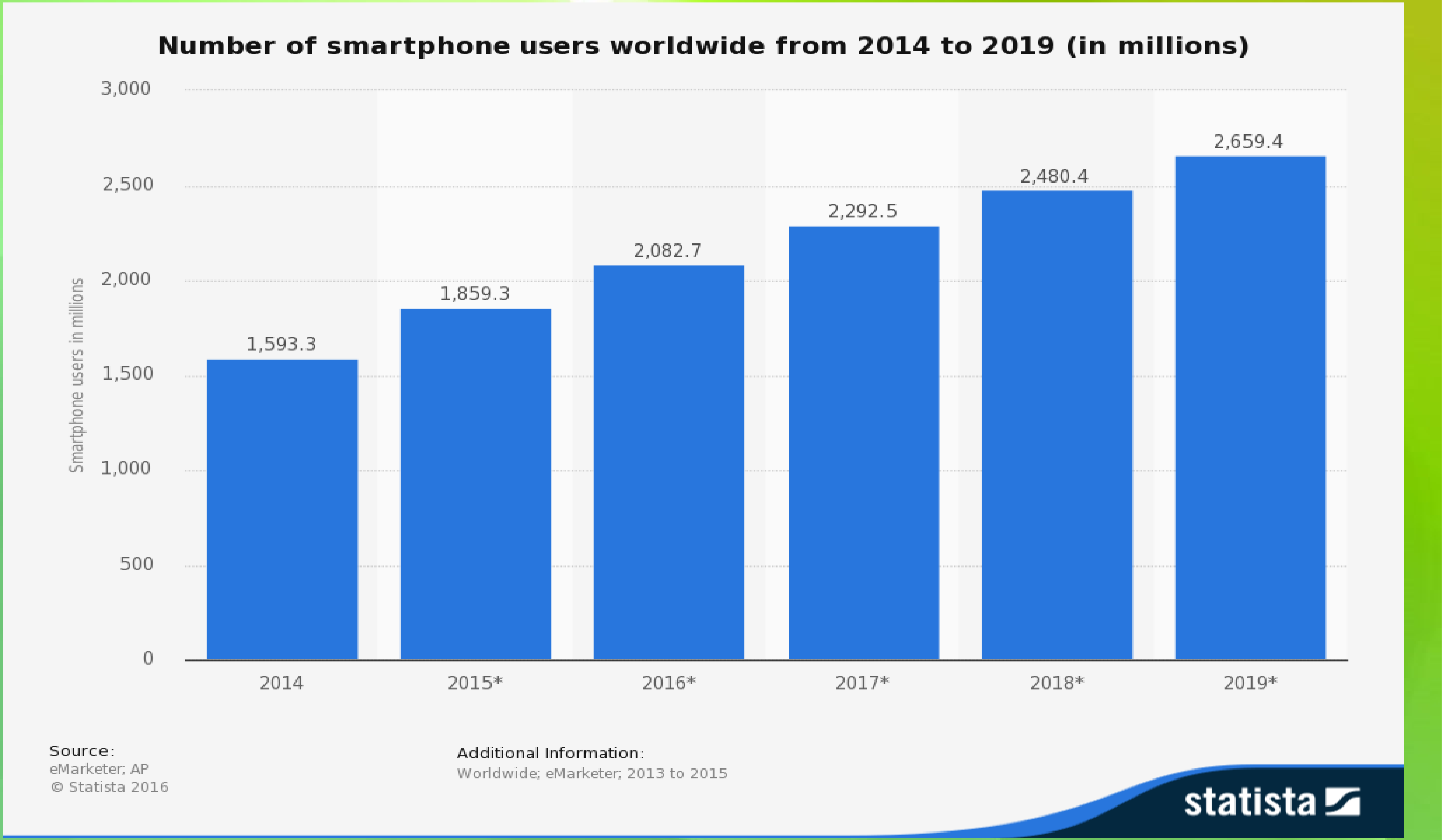
Guide: Prof. Prabhakar Mateti

Amrita University

3rd October , 2016

Motivation

Projected Number of Smartphone users

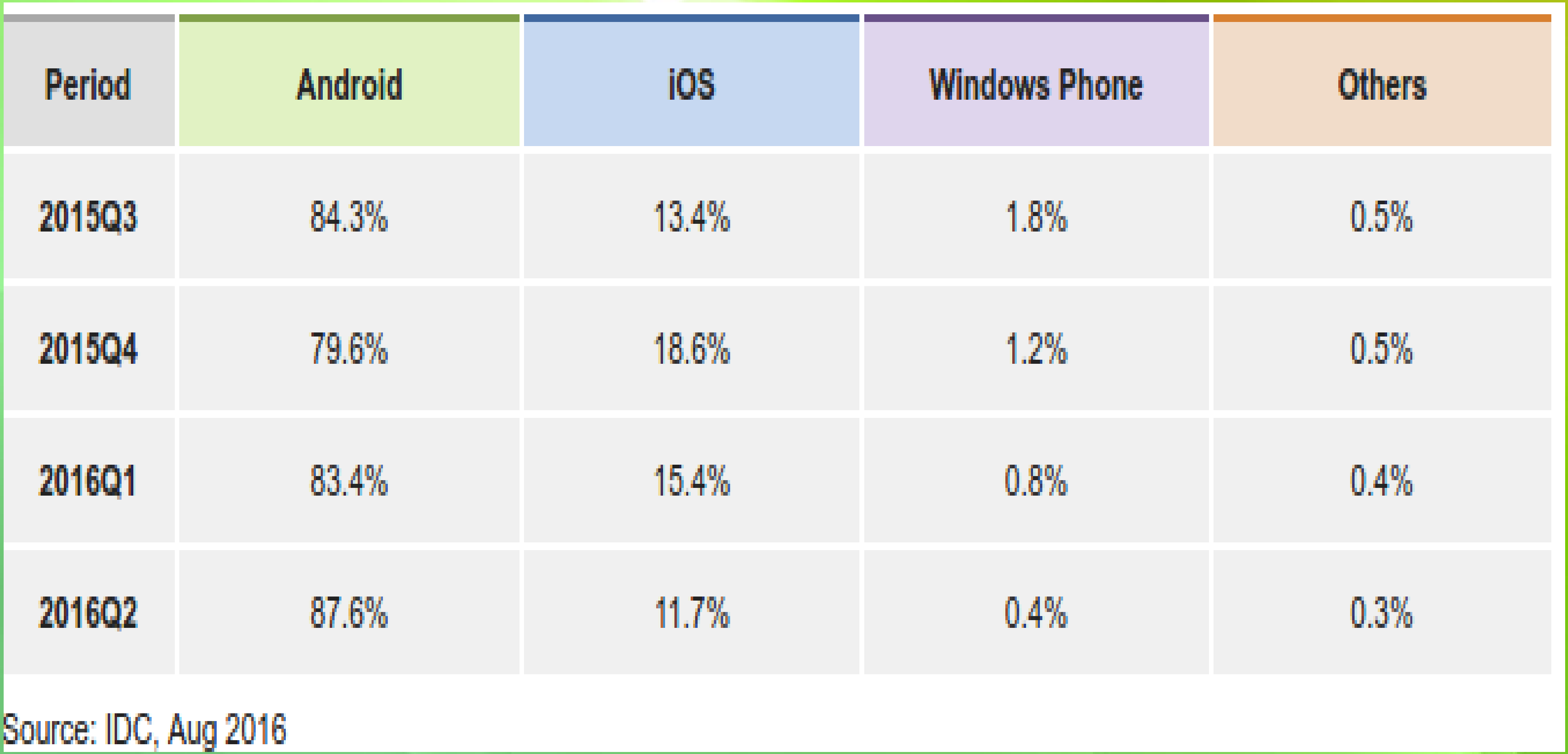


Source:
eMarketer; AP
© Statista 2016

Additional Information:
Worldwide; eMarketer; 2013 to 2015

Motivation

Smartphone OS Market Share, 2016 Q2



Period	Android	iOS	Windows Phone	Others
2015Q3	84.3%	13.4%	1.8%	0.5%
2015Q4	79.6%	18.6%	1.2%	0.5%
2016Q1	83.4%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%

Source: IDC, Aug 2016

Source:http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Motivation

Necessity Of SmartPhone Forensics

- Smartphones are now capable of doing a multitude of tasks in addition to traditional Call and Messaging.
  - Emails
  - Net-Banking
  - Social Networking
  - Navigation
  - Online Marketing
  - VPN and NFC.
  - In Case of Cyber Crime Investigation , these application data can be extremely useful for Forensic Analysis.

Motivation

Types of Mobile Forensics Investigation:

- Reactive Forensics :
  - Investigation done after Crime has happened.
- Proactive Forensics:
  - A suspect or potential terrorist is monitored proactively in realtime to prevent a crime.

Motivation

Need For Proactive Forensics

- Reactive Forensics Investigations is Susceptible to:
  - Applications like Uninstall-It can potentially wipe out all user data .
  - Device Encryption can be a barrier for investigation.
  - Criminals can use some anti-forensics tools to make their device resistant to forensics investigations.

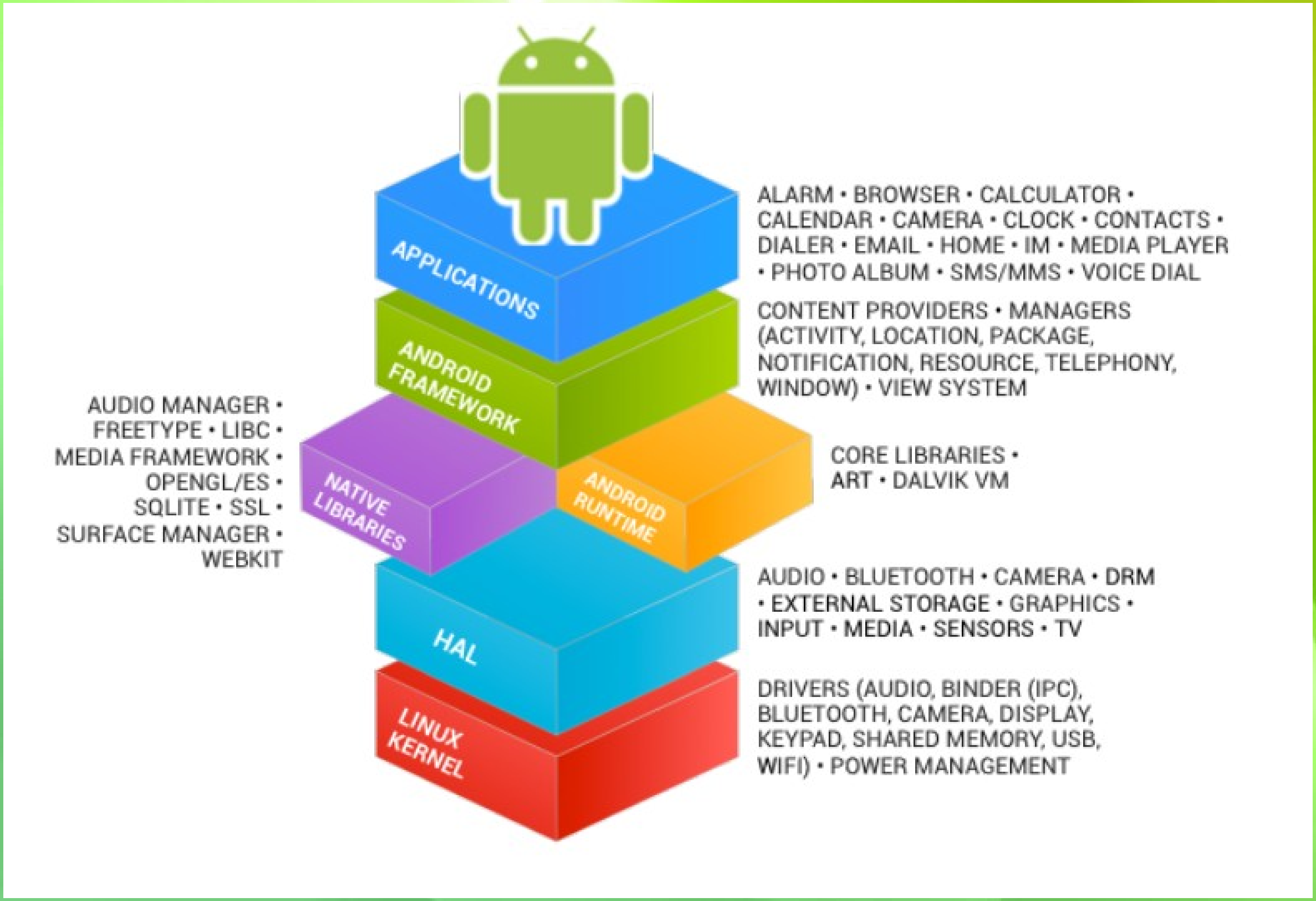
Motivation

Need For Proactive Forensics

- Advantages of Proactive Forensic Investigations:
  - Real-time monitoring and analysis is possible.
  - Data Encryption will not be a hindrance in evidence collection.
  - Ability to retrieve deleted data and logs.
  - Abililty to prevent potential crimes.

Motivation

Android Architecture


APPLICATIONS
ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL
ANDROID FRAMEWORK
CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM
NATIVE LIBRARIES
AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT
ANDROID RUNTIME
CORE LIBRARIES • ART • DALVIK VM
HAL
AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV
LINUX KERNEL
DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

Source:https://developer.android.com

Motivation

Common Partitions in Android

Bootloader	
Boot	
Recovery	
Userdata	Relevant For Forensic Investigation
System	
Cache	Relevant For Forensic Investigation

Motivation

Android File Hierarchy

Acct	
Cached	Relevant For Forensic Investigation
Data	Relevant For Forensic Investigation
Dev	
Init	
Mnt	
Proc	
Root	
Sbin	Relevant For Forensic Investigation
Sdcard	Relevant For Forensic Investigation

Problem Statement

- What changes can be made to the Android Rom so as to facilitate Proactive Investigation.
- How to enable stealth to avoid Detection and send forensics artifacts to the cloud.
- How to acquire the forensic artifacts from the cloud and automate the process of report generation .

Methodology

- File System Modifications must be monitored.
- Application data and logs must be monitored.
- Ability to transfer the collected data to a remote cloud server as discretely as possible.
- Remote Activation and Deactivation of the Spy app must be supported.

References

Aiyyappan, P. 2015. Android forensic support framework. M.Tech thesis, Amrita Vishwa Vidyapeetham,Ettimadai, Tamil Nadu 641112, India. Advisor: Prabhaker Mateti.

Link: http://cecs.wright.edu/~pmateti/GradStudents/index.html.

- Basis of our work
- Implemented inotify() and fileobserver() in android kernel.
- Forensic Support Spy app.

References

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

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

- Continued the work on Forensic Rom.
- Main focus on Development of the spy app.

References

Forensic Analysis of WhatsApp on Android Smartphones,M.S Thesis, Neha S. Thakur, University Of New Orleans,2013.

Link:http://scholarworks.uno.edu/td/1706/

- Used Two types of Extraction.
- WhatsappXtract Tool(Obsolete).
- Memory analysis by volatility framework.

References

Akarawita, I. U., Perera, A. B., and Atukorale, A. 2015. Androphsy–forensic framework for Android.

Link: http://ieeexplore.ieee.org/document/7377696/

- Can do both physical and logical acquisition.
- Better than Oxygen and ViaExtract CE Tool.
- Opensource

References

Alexios Mylonas Et.Al ,Smartphone Forensics: A Proactive Investigation Scheme for Evidence Acquisition.

Link:http://dl.ifip.org/db/conf/sec/sec2012/MylonasMTMG12.pdf

- Framework for collection of forensic data.
- Negotiated by an independent party.
- Implementation?

References

Tilo Muller, Michael Spreitzenbarth, and Felix C. Freiling ,Frost(Forensic Recovery of Scrambled Telephones)

Link: https://www1.cs.fau.de/filepool/projects/frost/frost.pdf

- Bypass Android Encryption
- Bruteforced PIN.
- Data loss in Ram poportional to temperature

References

Justin Grover, Android forensics: Automated data collection and reporting from a mobile device.

Link: https://www.sciencedirect.com/science/article/pii/S1742287613000480

- Droidwatch app to collect data with user consent.

- Prone to tampering

References

Daniel Walnycky, Network and device forensic analysis of Android social-messaging applications.

Link: http://www.sciencedirect.com/science/article/pii/S1742287615000547

- Analysed the calling feature of whatsapp
- Decrypted network packets.

References

Cosimo Anglano, Forensic analysis of WhatsApp Messenger on Android smartphones.

Link:http://arxiv.org/pdf/1507.07739.pdf

- Linking Various whatsapp artifacts together.

- Was able to get the complete profile using whatsapp logs.

Questions?