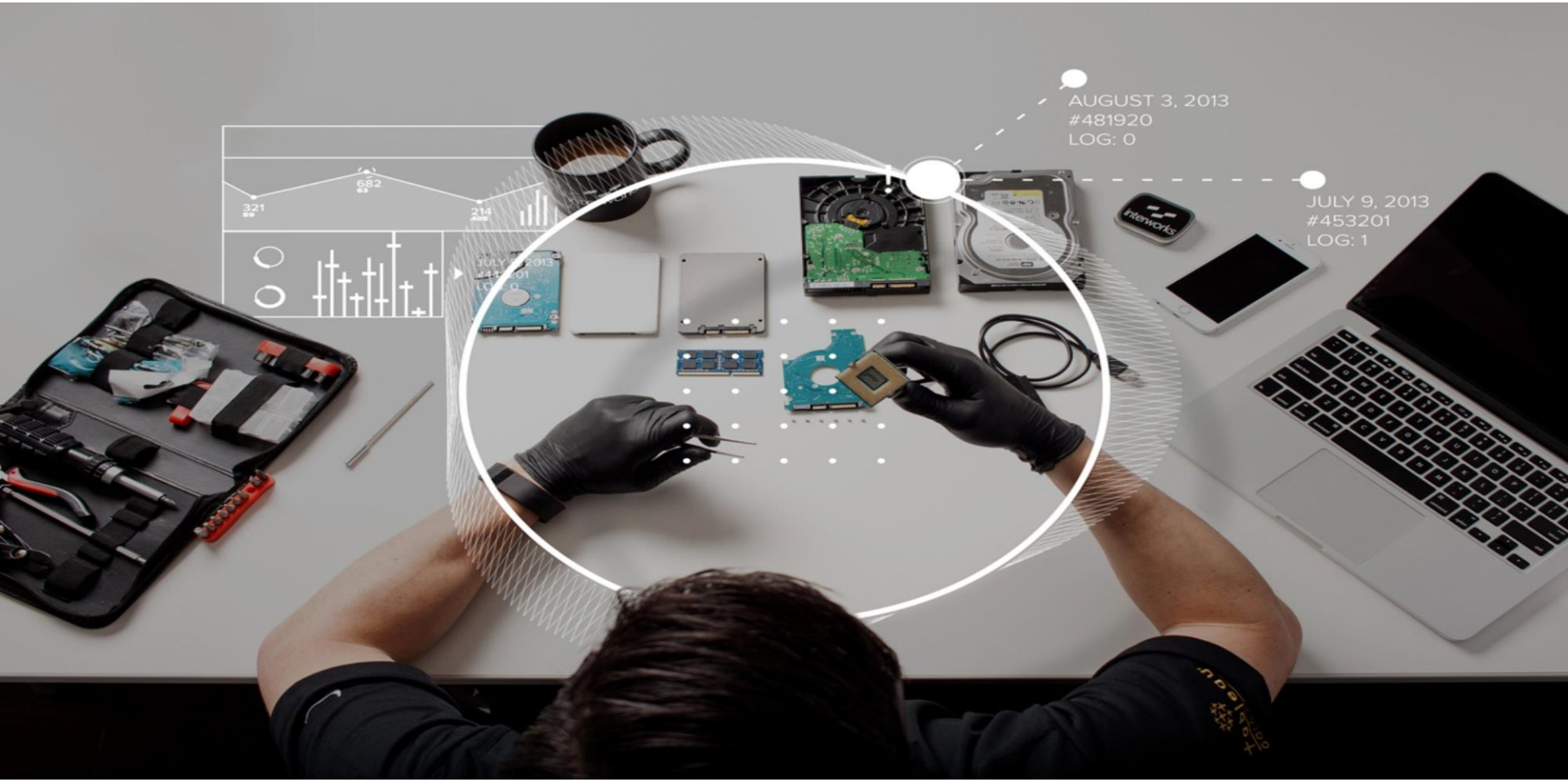


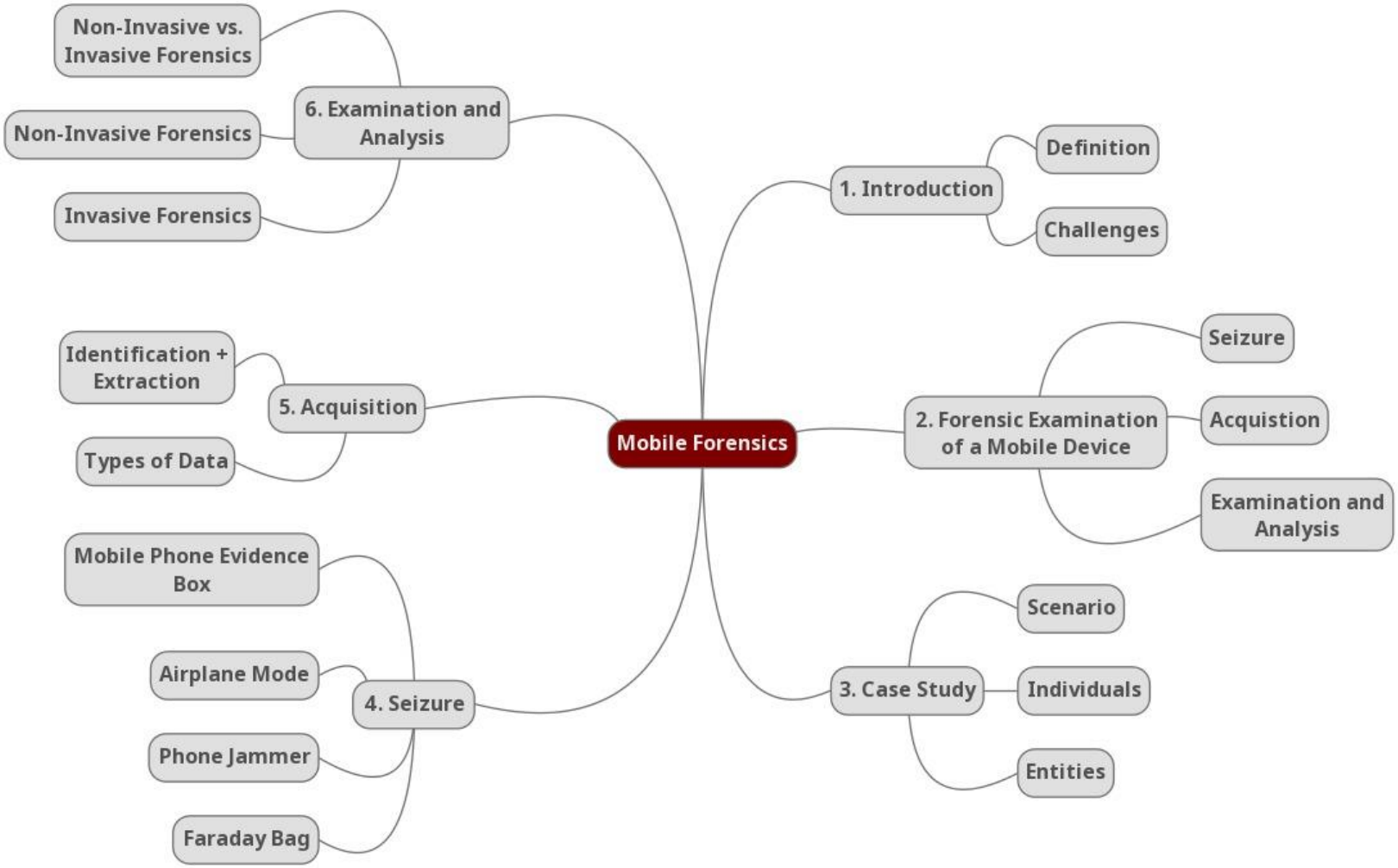
Chapter 5: Mobile Forensics

Introduction to Digital Forensics

Fröhlich, Hosh | 06.11.2018

https://thecybersecurityplace.com/wp-content/uploads/2017/11/DF1.jpg

Slide 2


Mobile Forensics
1. Introduction
Definition
Challenges
2. Forensic Examination of a Mobile Device
Seizure
Acquistion
Examination and Analysis
3. Case Study
Scenario
Individuals
Entities
4. Seizure
Mobile Phone Evidence Box
Airplane Mode
Phone Jammer
Faraday Bag
5. Acquisition
Identification + Extraction
Types of Data
6. Examination and Analysis
Non-Invasive vs. Invasive Forensics
Non-Invasive Forensics
Invasive Forensics

Literature

- The Role of Mobile Forensics in Terrorism Investigations:
  - https://link.springer.com/content/pdf/10.1007%2Fs11036-016-0791-8.pdf
- Forensics Data Acquisition Methods for Mobile Phones:
  - https://www.researchgate.net/publication/261465980_Forensics_data_acquisition_methods_for_mobile_phones
- An Analysis of Smartphones Using Open Source Tools vs. the Proprietary Tool Cellebrite UFED Touch
  - http://www.marshall.edu/forensics/files/BACHLER_MARCIE_Research-Paper_Aug-5.pdf

Mobile Forensics

Mobile Forensics

“Mobile Forensics is the application of forensically sound techniques and principles, to gather electronic data off mobile devices for legal purposes or corporate ones.”

http://aohpt.com/wp-content/uploads/2015/04/challenges.jpg

Challenges

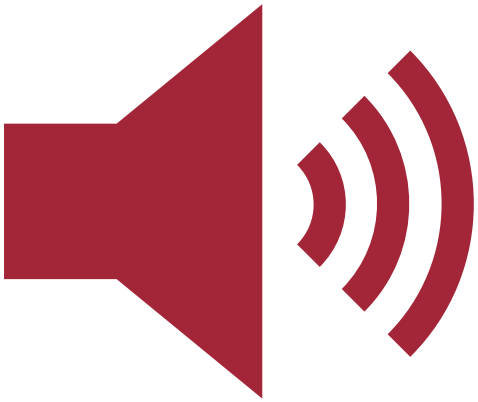
- Platforms
- Applications
- Cloud Data
- Security Mechanisms

Biometrical Lock

Biometrical Lock

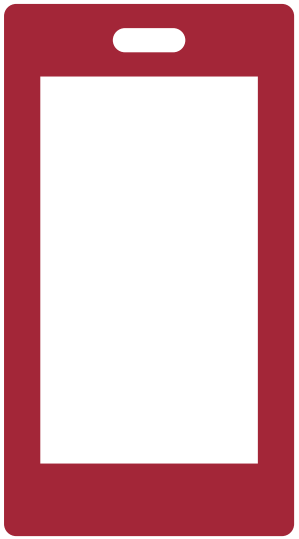
Retina

Voice



Fingerprint

Forensic Examination of a Mobile Device



- Seizure
- Acquisition
- Examination and Analysis

Storage Locations

Data Stored…

- On the Device
- On the SIM
- On the Memory
- In the Cloud
- In the cellular provider’s records

Possible Evidence

Possible Evidence

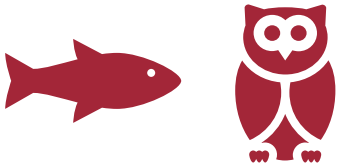
- Address book and call/SMS/MMS history
- Email and web browser history
- Photos and videos
- Social media information
- Application and delete data

Case Study

Individuals

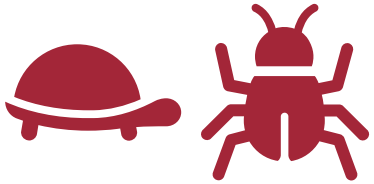
Alice: Disgruntled Wife, wants a divorce

Bob: Possible victim of a hack, or a cheating bastard



Frank & Grace: Evil couple, trying to set up Bob out of envy

Eve: Black Market Hacker

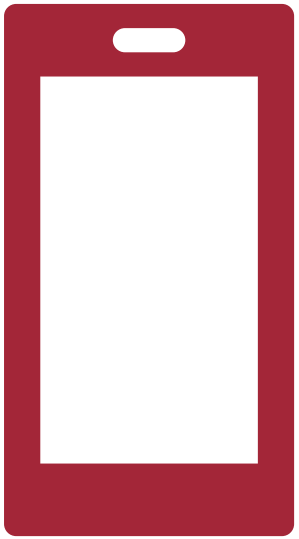


Charlie & Trainee: Forensic examiners

Scenario

- Bob & Alice, real-estate owners, business is flourishing
- Frank & Grace, coffee shop owners, business is failing
- Frank & Grace hire a hacker to set up Bob
- Eve hacks Bob’s phone, spoofs an affair
- Alice discovers the “affair”, and wants a divorce
- Bob hires Charlie, a forensic examiner
- Charlies tries to prove Bob’s innocence

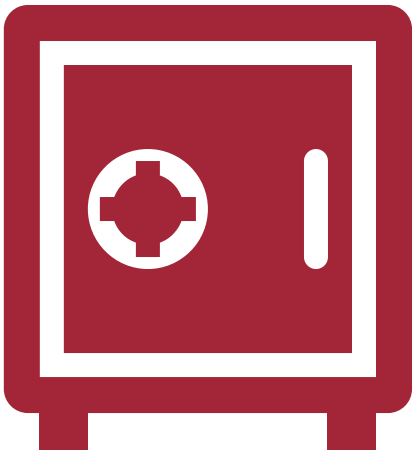
Entities



- Turned on
- Android Nougat
- Unlocked
- Internal & Micro-SD
- WLAN, LTE, GPS

Problems & Goals

http://www.justshovelmysnow.com/wp-content/uploads/2015/12/Fotolia_86265174_XL-768x662.jpg



Seizure

IMEI

International
Mobile
Equipment
Identity

MEID

Mobile
Equipment
IDentifier

IMEI/MEID

“IMEI and MEID are unique identifiers for mobile devices.”

SIM

Subscriber
Identity
Module

SIM

“An integrated circuit on chip meant to securely store the IMSI and other cryptographic keys.”

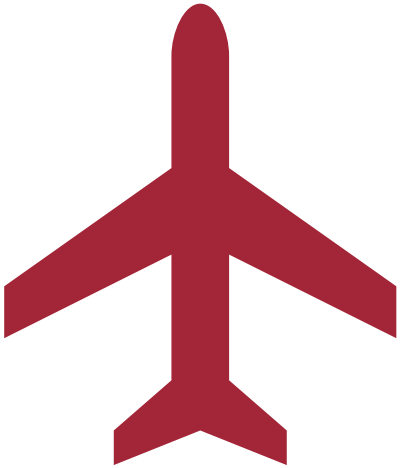
IMSI

International
Mobile
Subscriber
Identity

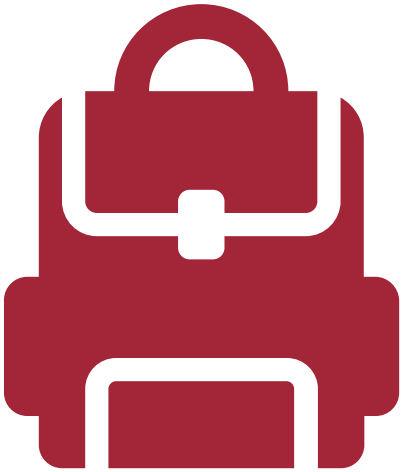
Seizure of Mobile Devices

Seizure of Mobile Devices

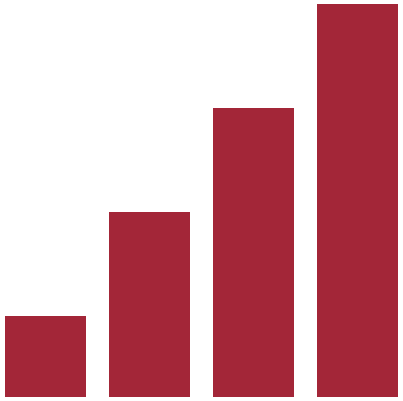
Airplane Mode



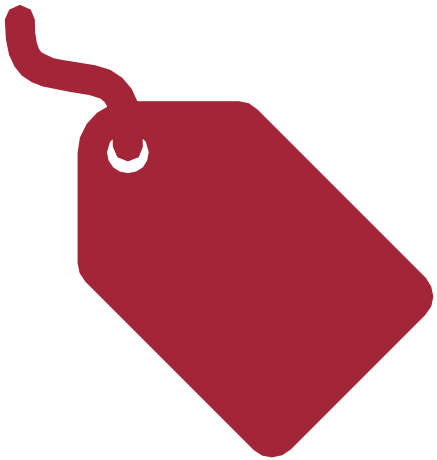
Faraday Bag



Phone Jammer



Faraday Bag, Phone Jammer Demo



Acquisition

Physical Acquisition vs. Logical Acquisition

- Physical
- Deleted Data
- Zero’s and One’s

- Logical
- Files and Folders
- Human-Readable

Types of Data

Types of Data

- CDR
- GPS
- Application Data
- SMS
- Photos and Videos (as evidence)

CDR

Call
Detail
Records

CDR – Call Detail Records

- Call start/end time
- Originating and terminating towers
- Whether a call was outgoing or incoming
- Call time duration
- Caller and called person

GPS

Global
Positioning
System

SMS

Short
Messaging
Service

Examination & Analysis

Non-Invasive Forensics
vs.
Invasive Forensics

Non-Invasive Forensics vs. Invasive Forensics

Non-Invasive Forensics

- Manual Extraction
- Logical Extraction
- JTAG
- Hex Dump

JTAG

Joint
Test
Access
Group

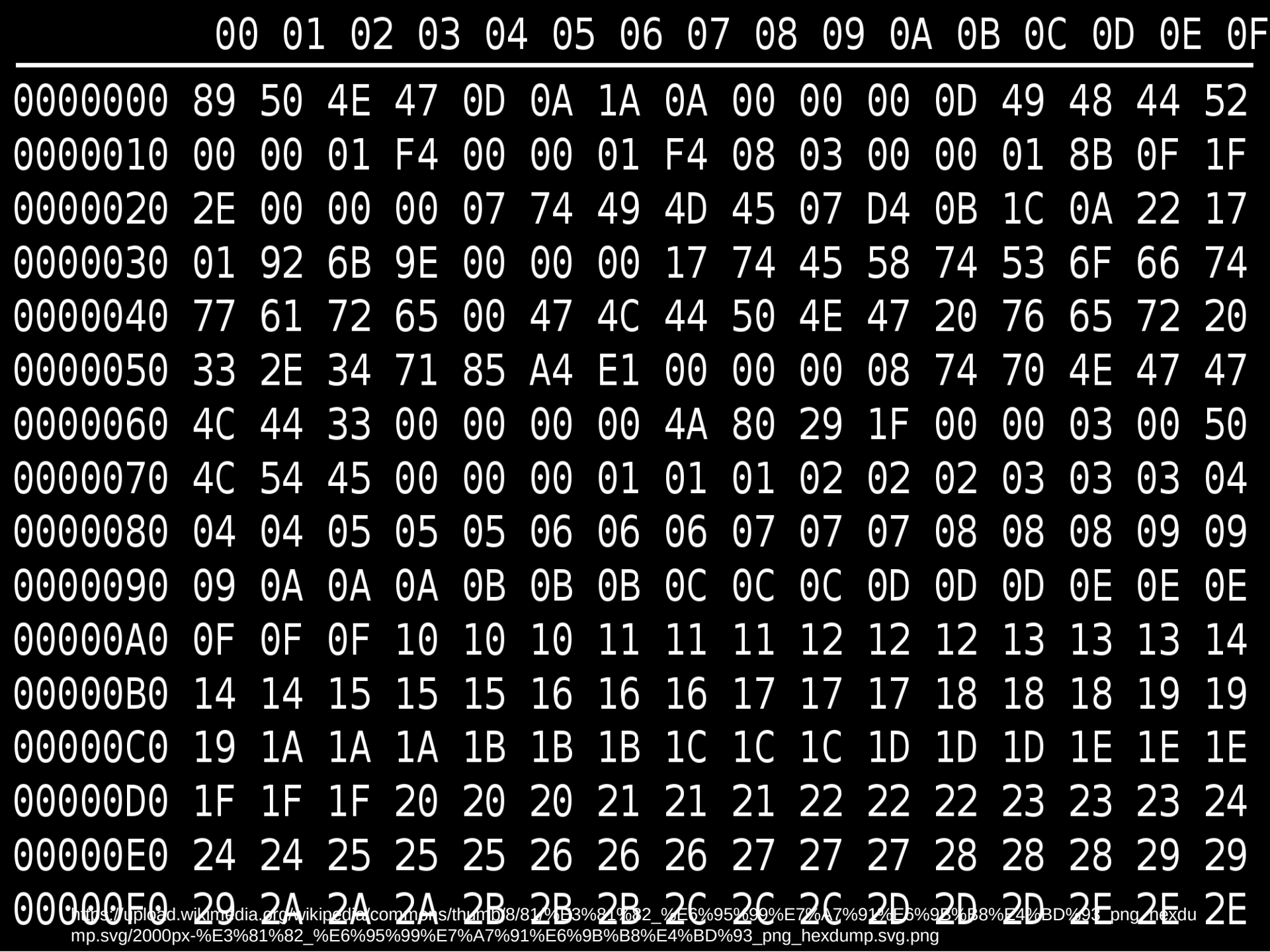
JTAG – Joint Test Access Group

“Non-invasive, physical acquisition. Used if the device is damaged, locked or encrypted through TAPs.”

TAP

Test
Access
Port

JTAG Demo



https://upload.wikimedia.org/wikipedia/commons/thumb/8/81/%E3%81%82_%E6%95%99%E7%A7%91%E6%9B%B8%E4%BD%93_png_hexdump.svg/2000px-%E3%81%82_%E6%95%99%E7%A7%91%E6%9B%B8%E4%BD%93_png_hexdump.svg.png

Invasive Forensics

- Chip-Off
- Mirco Read

Chip-Off

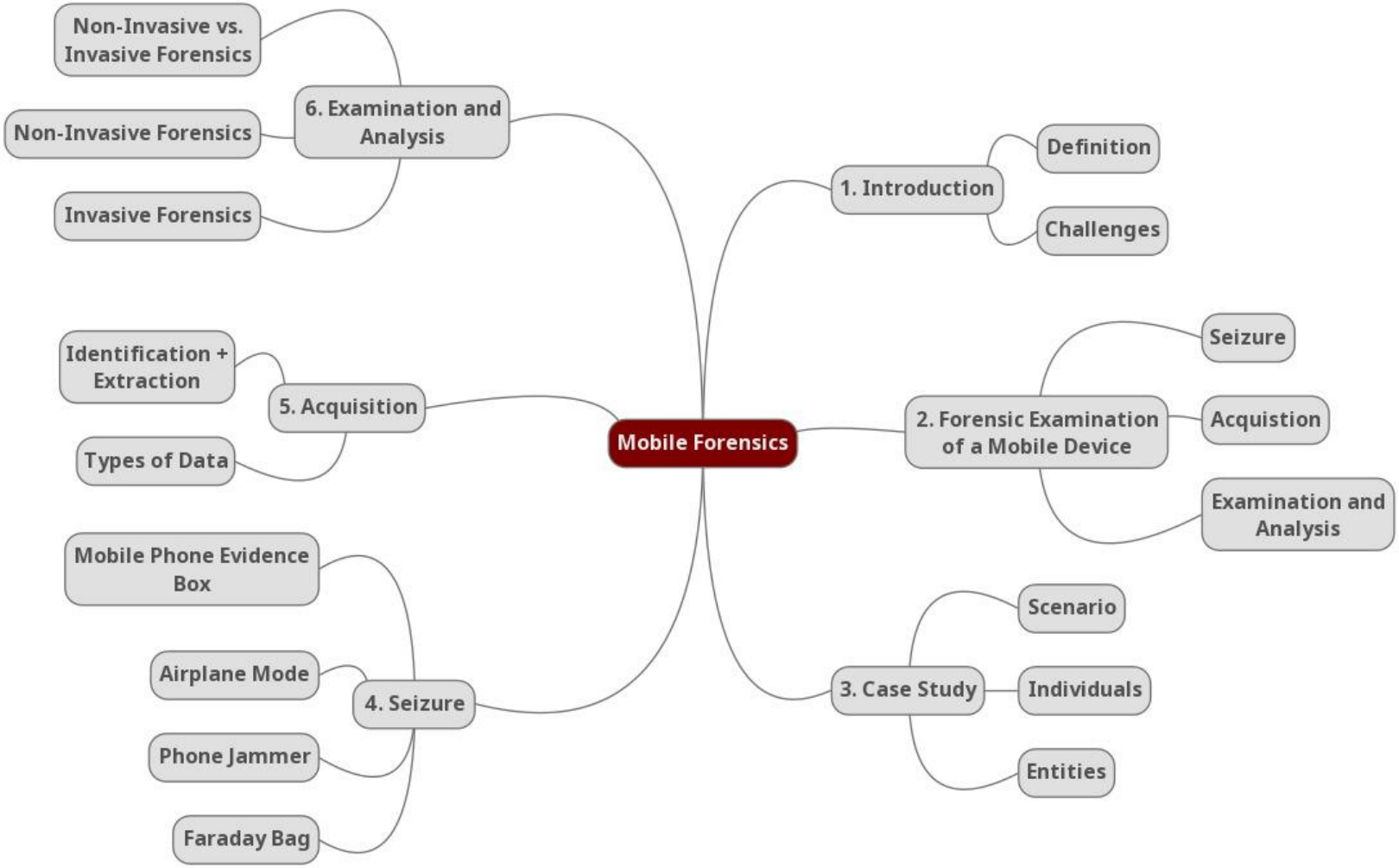
“Invasive forensics method. Memory chip is removed from the mobile device, and implanted in a functional device.”

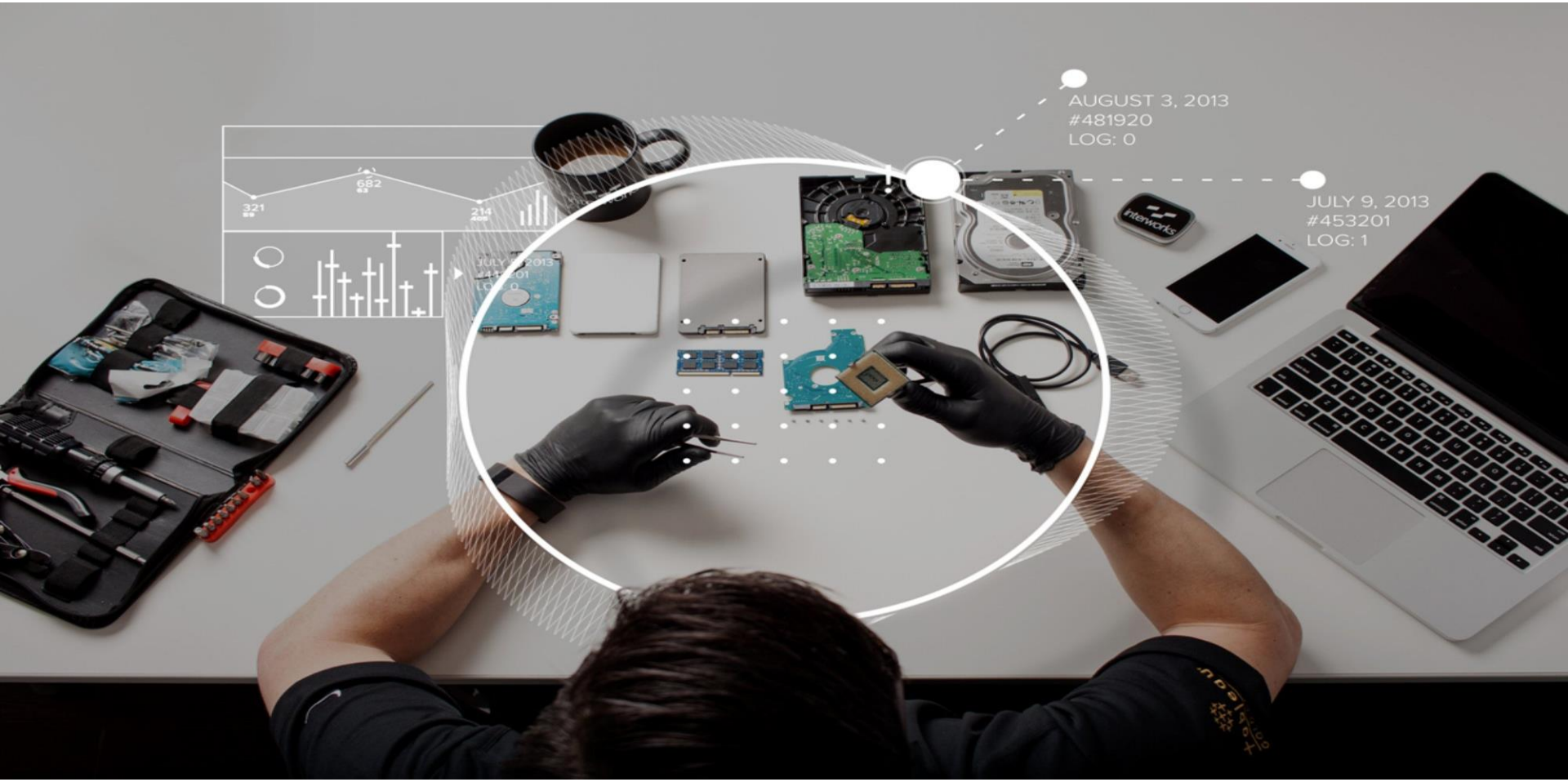
Chip-Off Demo

http://emc.missouri.edu/wp-content/uploads/2016/01/hitachi-s-4700-field-emission-scanning-electron-microscope.jpg

Results

- Spoofed text messages
- Downloaded pictures
- Presence confirmed
- CDR underlines spoofed-theory
- Traces of remote-access software


Mobile Forensics
1. Introduction
Definition
Challenges
2. Forensic Examination of a Mobile Device
Seizure
Acquistion
Examination and Analysis
3. Case Study
Scenario
Individuals
Entities
4. Seizure
Mobile Phone Evidence Box
Airplane Mode
Phone Jammer
Faraday Bag
5. Acquisition
Identification + Extraction
Types of Data
6. Examination and Analysis
Non-Invasive vs. Invasive Forensics
Non-Invasive Forensics
Invasive Forensics



Chapter 5: Mobile Forensics

Introduction to Digital Forensics

Fröhlich, Hosh | 06.11.2018

https://thecybersecurityplace.com/wp-content/uploads/2017/11/DF1.jpg