# Smartphone Forensics

Dr. Michael Spreitzenbarth

# Dr.-Ing. Michael Spreitzenbarth

- Dipl.-Wirtsch-Inf. an der Universität Mannheim mit Schwerpunkt in den Bereichen IT-Security und Digitale Forensik

- Dr.-Ing. an der Universität Erlangen-Nürnberg mit Forschungsthemen in den Bereichen der forensischen Analyse von Smartphones sowie im Bereich der Detektion und automatisierten Analyse von mobilem Schadcode (Malware)

- 3 Jahre Teamleiter in einem CERT für die Themen Mobile-Security sowie Incident Handling auf mobilen Endgeräten

- Auditor für IT-Sicherheit (RED-Team)

CISSP® GMOB GRID GASF

7.7
Billion

7.1
Billion

1.200

a dog named
BOO BOO

$20,000 in
GOLD BARS

Und Über
22.000
Smartphones

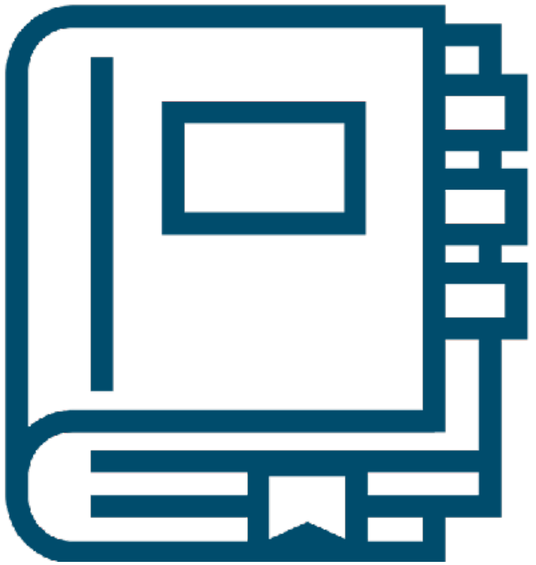
two
SAXAPHONES

an uncle's
FUNERAL ASHES

# Agenda and Dates

# Agenda

- **2018-05-11: Mobile Device Forensics**
- 2018-05-18: Android and Forensic Investigation of this OS
- 2018-05-25: Apple iOS and Forensic Investigation of this OS
- 2018-06-01: Mobile Malware
- 2018-06-08: Hacking Android Apps



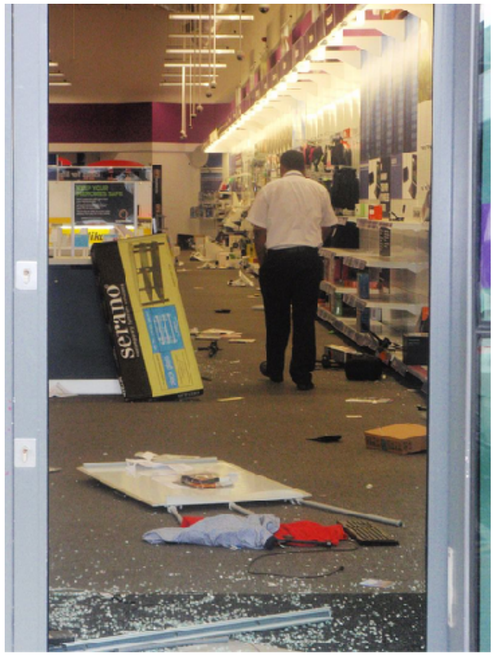
# Why is this topic relevant?

# Evidence Treasure Trove

- Nearly everyday media is reporting about criminal cases in which mobile devices play a major role
  - either as evidence -> data on a phone (like messages, pictures or voicemails)
  - or the phone was the root cause of the crime -> theft

# London Riots 2011

The 2011 England riots occurred between 6 and 11 August 2011, when thousands of people rioted in several London boroughs and in cities and towns across England. The resulting chaos generated looting, arson, and mass deployment of police and resulted in the deaths of five people.



It said: "Everyone from all sides of London meet up at the heart of London (central) OXFORD CIRCUS!!, Bare SHOPS are gonna get smashed up so come get some (free stuff!!!) fuck the feds we will send them back with OUR riot! >:O Dead the ends and colour war for now so if you see a brother... SALUT! if you see a fed... SHOOT!"

[2]

# San Bernardino shooting 2015

SAN BERNARDINO, Calif. — A heavily armed man and woman terrorized this city on Wednesday, killing at least 14 people and wounding at least 17 at a social services center before leading the police on a manhunt culminating in a shootout that left the two suspects dead, the authorities said.

In early 2016, Apple was embroiled in a battle with the FBI over privacy, specifically whether it could (or would) crack an iPhone 5C following the San Bernardino terrorist attack. Apple refused to specifically create a backdoor piece of software that would circumvent the security protections built into iOS, citing concerns for the privacy of the other millions of people out there using iPhones and iPads. Ultimately, it became a moot point: the FBI purchased software to crack the iPhone in question. The agency refused to say how much it spent, but now Senator Dianne Feinstein has revealed that it cost $900,000 to break into the shooter's phone.

[4]

# Australian murder case 2016

Data from an Apple Watch may have helped investigators in Australia solve a murder from 2016. According to Australia's *ABC News*, investigators collected data from the Apple Watch belonging to the victim, 57-year-old Myrna Nilsson, and the data showed that Nilsson's niece, Caroline Nilsson, had in fact staged a home invasion, and committed the murder herself. The Apple Watch's activity and heart rate measurements helped ascertain the timing of the murder. leading to the younger Nilsson's arrest.

[3]

# Lawsuit against Hussein K. 2018

Am Tag 20 des Prozesses gegen Hussein K., den mutmaßlichen Mörder der Studentin Maria L., hat am Dienstag ein Kriminalpolizist ausgesagt, der K.s Smartphone ausgewertet hat. 1400 Kontakte inklusive denen in den sozialen Netzwerken und 50.000 Bilder waren im Handy des Tatverdächtigen sichergestellt worden.

Im Fall von Hussein K. kamen die Ermittler nun zu folgendem Ergebnis: In der Zeit zwischen etwa 2.30 Uhr und 4.00 Uhr bewegte sich Hussein K. **nur wenige Schritte**, was darauf hindeuten könnte, dass er das Opfer Maria L. womöglich wesentlich länger misshandelt hat, als bisher angenommen. In Bezug auf das Urteil ist das insofern relevant, da ein **Handeln im Affekt** aufgrund dieser Beweislage vom Gericht als unwahrscheinlich angesehen werden kann, was das Strafmaß erhöhen würde.

Während des besagten Zeitraumes wurde von der App außerdem zweimal „Treppensteigen" aufgezeichnet – also die **Überwindung von Höhenunterschieden**. Die Ermittler vermuteten, dass Hussein K. hierbei das Opfer die Böschung hinunter geschleift hat und später wieder hinauf geklettert ist. Dies wurde vor Ort von den Ermittlern **mit einem iPhone simuliert**, wodurch die Vermutung bestätigt werden konnte.

[1]

# The Relevance of Mobile Device Data

- Mobile devices have come a long way since their inception
- Data contained on such devices can nowadays be compared to a personal diary
- …often also combined with company’s most secret documents
- …personal financial status
- …health data
- …our everyday habits, patterns, and routines

„Mobile Device Data is today’s equivalent to yesterday’s DNA evidence.“

**Lee Reiber**

# Smartphones & Mobile Devices

# Important Identifiers

- **IMEI** is a unique 15 digits long identifier of a mobile device and stands for International Mobile Equipment Identity.
- **TAC** is the Type Allocation Code and tells you the type/version of device. This number has 6-8 digits and is the first part of the IMEI.
- **ICCID** is the serial number of the SIM card itself. This number is often also printed on the card.
- **IMSI** is the International Mobile Subscriber Identity and is a unique identifier for a SIM card on the network.

# From Mobile to Smart

1983


1998

2007


2018

# Knock-Offs

- Devices manufactured in China, Peru, Mexico and Taiwan that imitate well known smartphones.
- Those devices hold about 30% of the global market and nearly 800 mid where manufactured in 2015.
- Common manufacturers are Nokla, LC, iOrange, GooPhone, OPhone and SCI-Phone.
- Can often be easily detected because of changeable batteries and multi-SIM-support.
- Devices run Android or a custom Java OS.

# Mobile Phones

- also known as „Burner Phones“
- limited capacity (most devices are only able to store 10-20 SMS)
- only capable of SMS, phone and minimal app support
- most of those devices run a Java-based OS
- Nokia devices run S40 or S60
- cheap and easy to get
- very common by criminals

# 1st Generation Smartphones

- 1st generation smartphones run Symbian OS
- capacity of up to 32 GB (sometimes even more by using sd-cards)
- Webbrowser and a larger amount of Java-based apps available
- first devices with WhatsApp and other messengers
- capable of storing thousands of SMS and hundreds of pictures
- first generation of devices with GPS

# 2nd Generation Smartphones

- The 2nd generation of smartphones was the 1st generation of iPhones and Android-based devices.
- Next „evolution“ of Symbian OS with official app stores and thousands of apps.
- Those devices started to be part of people everyday lives.


# Todays Smartphones

- Run Android 6+ or iOS 9+
- capacity is currently going way above 128GB
- equipped with hundreds of sensors to store and measure movement, light or surrounding noice
- are nowadays used like notebooks 2-3 years ago
- store detailed user profiles and huge amount of sensitive data

# Smart Accessories





# Introduction into Smartphone Forensics

# The Word „Forensic“

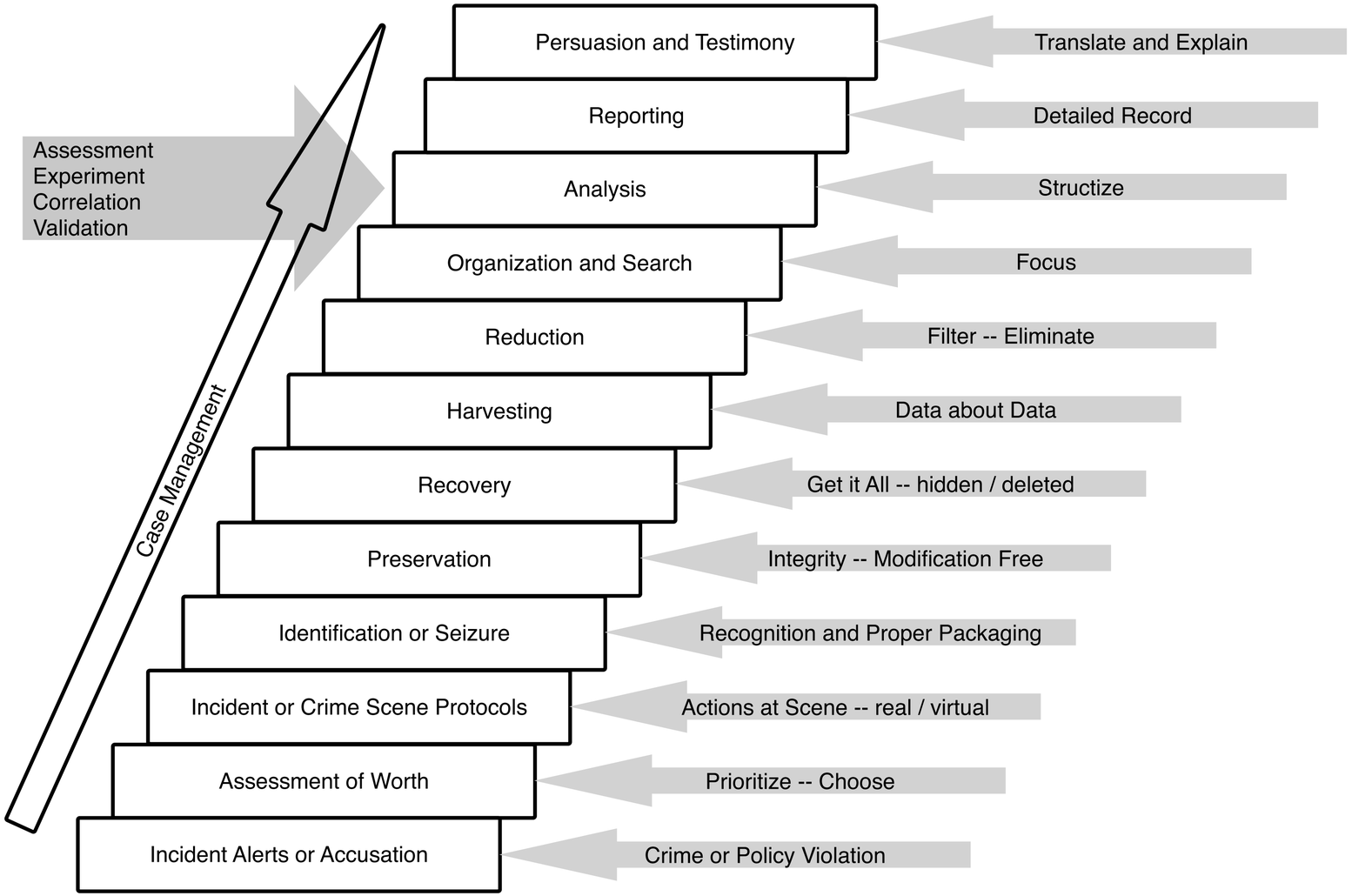
- NIST describes „forensic science“ as „the application of science to the law“
- Generally spoken, „Forensics“ can be scientific examination of fossils, a crime scene, any kind of physical things, post mortem bodies, and digital data.
- In a lot of cases „forensics“ also means, that **nothing** has been modified during the examination.
- As this is not possible when it comes to mobile devices, you will often read „forensically sound“.
- For the course of this lecture, we will use the word „forensic“ even if it should be „forensically sound“.

# Forensic Principles

1. Greatest care must be taken that evidence is as little as possible manipulated or changed.

2. The course of a digital investigation must be understandable and open to scrutiny. At best, the results of the investigation must be reproducible by independent investigators.

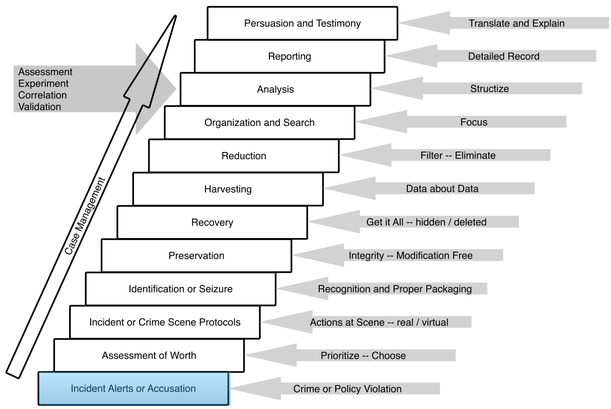
# Investigative Process Model by Casey




E. Casey, Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition. Academic Press, 2011.

# Incident Alerts or Accusation

- The accusation is the start signal for the whole process.
- Within this phase the sources are evaluated and detailed inquiries are requested.



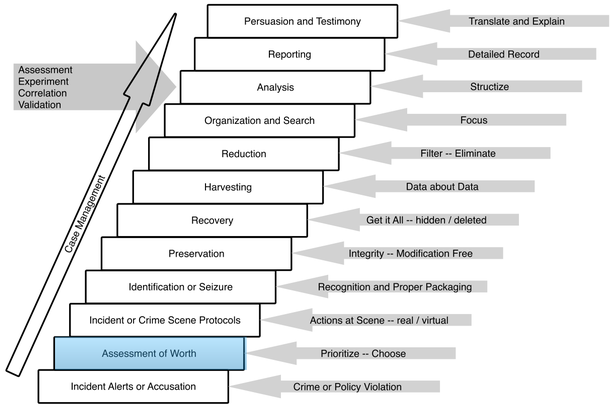
# Assessment of Worth

- In the scope of the assessment of worth the interest of prosecution is compared to the costs that would occur for prosecuting the criminal action.

- For companies this often results in a decision against prosecution (at least for smaller incidents).

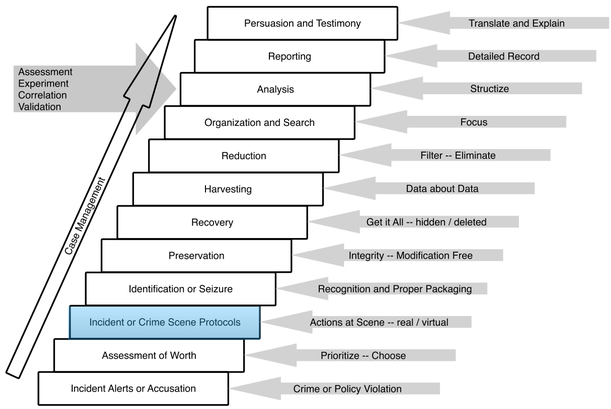
- The advantages of a prosecution lie in a possible compensation, the improvement of one’s own security as well as a certain effect of deterrence.

- The disadvantages of a prosecution are the need of resources, the possible downtime during which the investigated systems cannot be used productively and most of the time a negative public scatter effect.



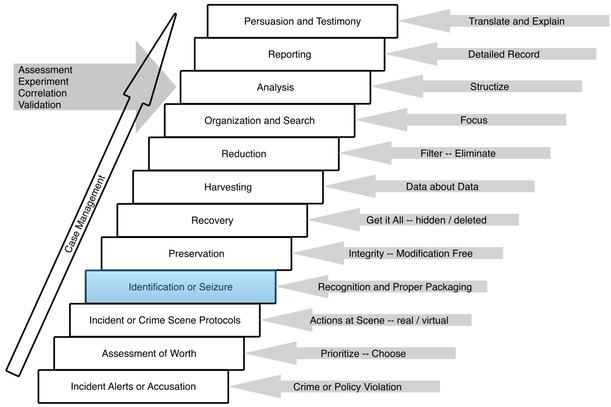
# Incident or Crime Scene Protocols

- Within the classic criminalistics it is often demanded that the crime scene is spaciously closed.
- For digital forensics this means: “freeze the evidence in place and provide ground truth for all activities that follow”.
- For the different kinds of digital traces it has to be checked on an individual basis how the process of freezing can be guaranteed.
- Altogether it holds true that the risk of changing traces has to be minimized.



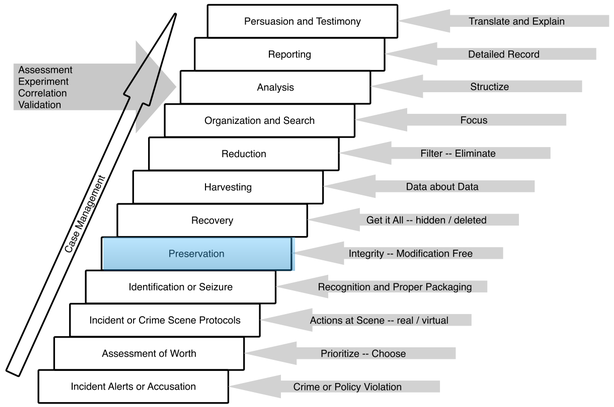
# Identification or Seizure

- During a traditional impoundment all subjects that could act as evidence are picked up.
- Here it is important that no changes are made to the evidence. In addition, the environment of evidence might be of great relevance.
- Simultaneously to the impoundment the chain of custody starts.
- Good description of what to pick up, can be found in
  - “Electronic Crime Scene Investigation: A Guide to First Responders”, published by the US Department of Justice
  - “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations”, published by the US Department of Justice



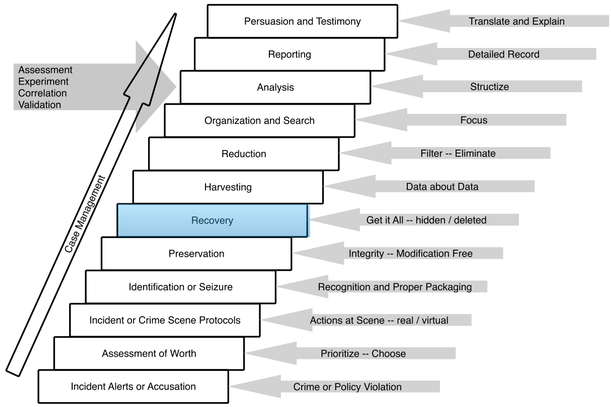
# Preservation

- When securing evidence it has to be assured that these are not modified.
- This is why all evidence is documented, photographed, sealed and afterwards locked away.
- In the case of digital evidence this means that first of all, copies of evidence are created; further investigation is only done on the copies.
- To prove the authenticity of copies of evidence cryptographic hash functions are used.
- During the phase of copying the work of forensic experts begins.



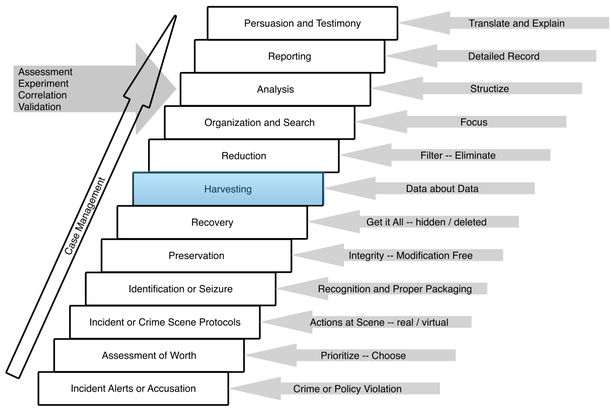
# Recovery

- “throwing out a large net”
- In particular this phase includes the retrieval of evidence that had been deleted, hided, masked or that has been made inaccessible in any other way.
- It is recommended to make use of synergies with other evidence. For example, it is reasonable to test if a note with passwords has been found at the crime scene if encrypted data needs to be read.



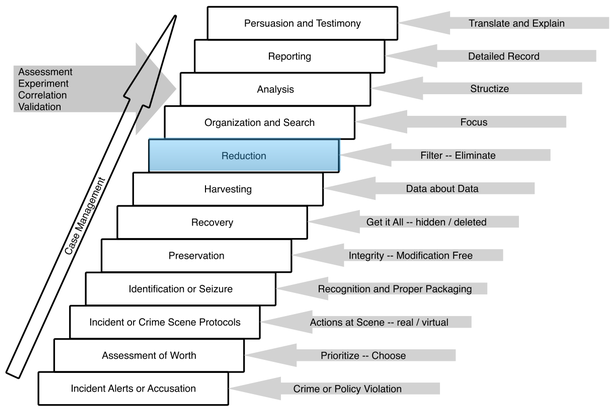
# Harvesting

- During analysis of evidence a well-structured organization of the normally huge data amount is needed.
- For this reason, one should investigate meta data – instead of the real data – first.
- For example: data can be grouped according to file type or access time.



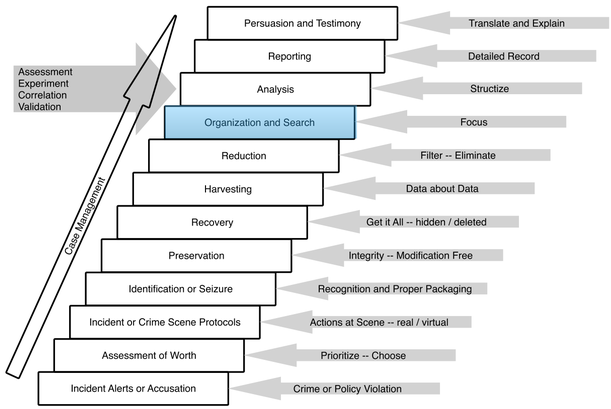
# Reduction

- The task of reduction lies in eliminating irrelevant data.
- The result of this phase is “the smallest set of digital information that has the highest potential of containing data of probative value”.
- In this context, hash databases of known files like e.g., The NIST National Software Reference Library are helpful to exclude already known files.



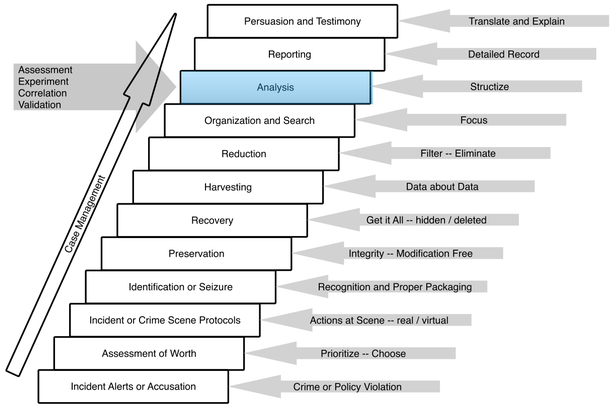
# Organization and Search

- Aspects of organization are the structuring of data as well as the enabling for scanning.
- Therefore, often indices and overviews are created or files are sorted by their type to meaningful directories.
- This simplifies the referencing of data within the following steps.



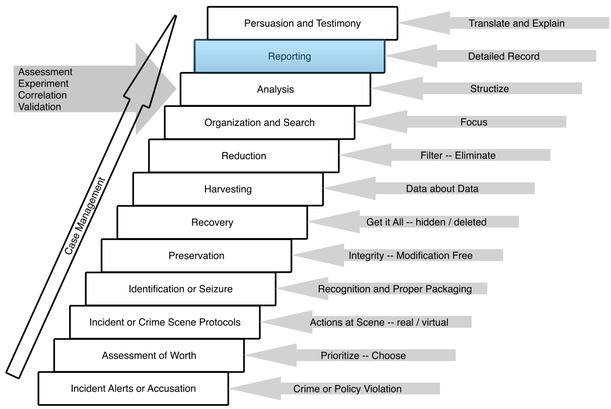
# Analysis

- This phase includes the detailed analysis in consideration of file content.
- Amongst others, connections between data and persons have to be drawn in order to determine the responsible person.
- Moreover, the evaluation of content and context is made according to means, motivation and opportunity.
- Within this step, experiments are helpful to determine undocumented behavior and to develop new methods.
- All results need to be tested and need to be testable with scientific methodology.



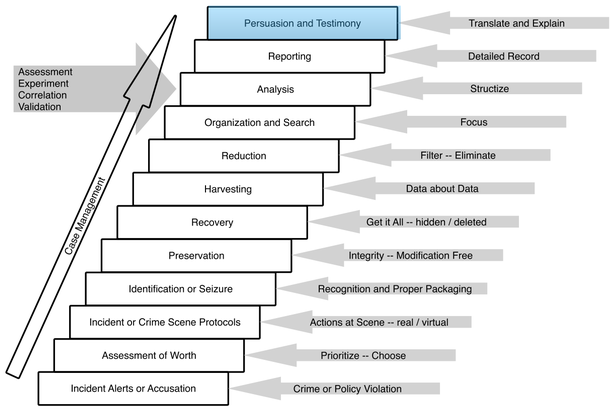
# Reporting

- The report is not only for presenting results but also to demonstrate how one has come to the stated results.
- For this, all considered rules and standards should be documented.
- In addition, all drawn conclusions need to be justified and alternative explanation models need to be discussed.



# Persuasion and Testimony

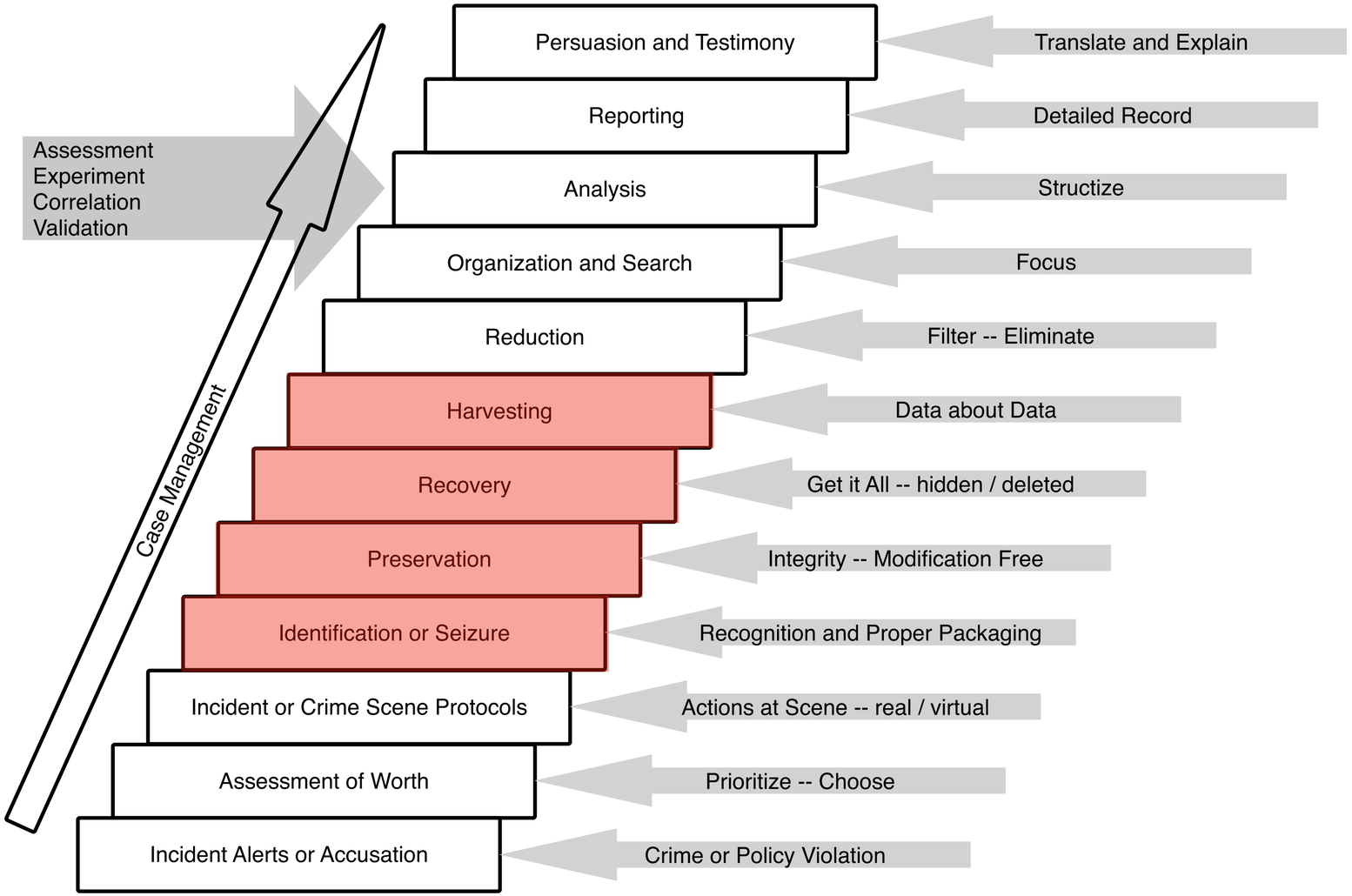
- Finally, it comes to the testimony as an authority of the subject at court.
- The most important aspect is the trustworthiness of the authority.
- A technology adverse audience or difficult analogies can be problematic.



# PC vs. Mobile Device

- The investigative process as described before is as generic as possible.
- In case of forensic investigations regarding computers this process is well documented and can be realized as described by Casey.
- In case of forensic investigations of mobile phones, this process is harder to adopt.
- A forensic experts needs his own procedures and techniques for nearly every type of smartphone.

# Investigative Process Model for Mobile Devices

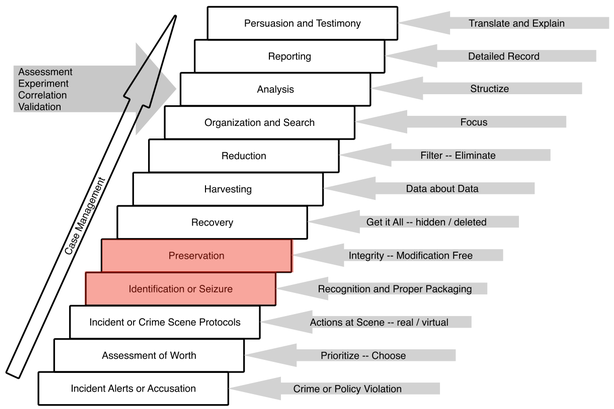



E. Casey, Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition. Academic Press, 2011.

# Seizure and Preservation

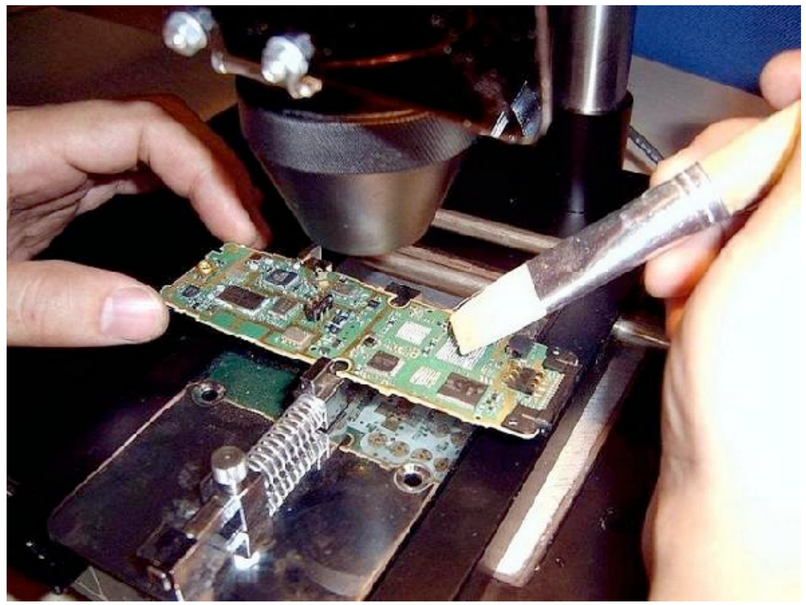
- To follow the guidelines of the investigative process, the original evidence should be cataloged and stored in a proper and controlled location after the copies have been made.

- When it comes to smartphones, it is not obvious how to create a duplicate from a modern device.



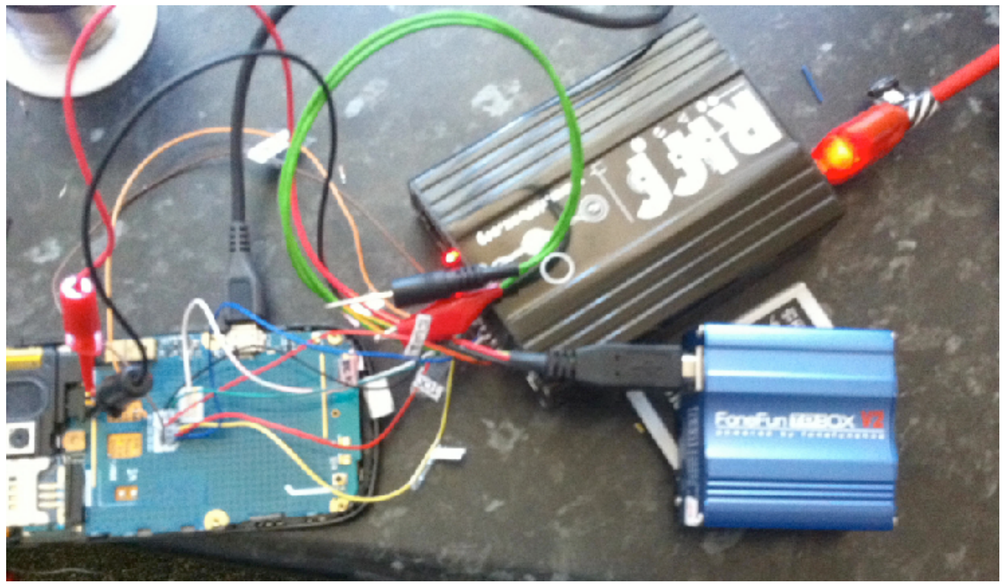
# Desoldering of the Flash Chips

- special hardware required
  (~20.000 EUR)
- high amount of knowledge is needed
- high risk to damage the chips
- if everything works, you will get the best results
  (as long as it is not encrypted based on a TPM)



# Using the JTAG Interface

- not all devices have a working JTAG interface
- special hardware required
  (~200 EUR)
- still high amount of knowledge needed,
  but the risk to lose data is much lower
- really good results if the device is supported



# Software Agents

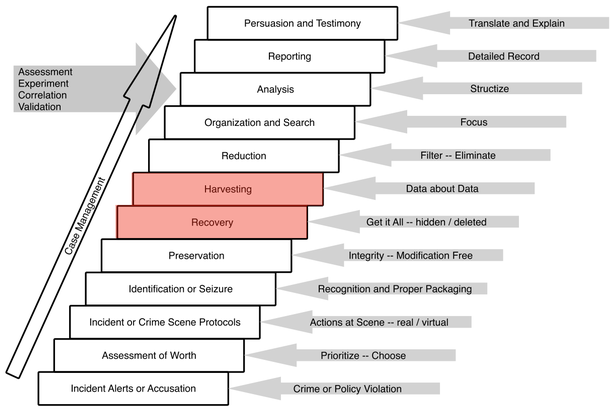
- Forensic apps that will be installed on the device
- Those apps use official permissions to access databases of the OS or other apps
- Data on the device will be modified; not an issue per se, but needs to be documented
- These apps can be tricked by a manipulated OS or anti-forensic apps (shadow database)
- Thus, the results are not really trustworthy

# The „most common“ Solution


- Special software will be installed on the PC and connects to the device via data cables
- The software is often using the default drivers of the manufacturer
- Through this way you can often only access unprotected parts of the device if no suitable exploit is available
- It is still one of the best solutions when it comes to Android or iOS devices.

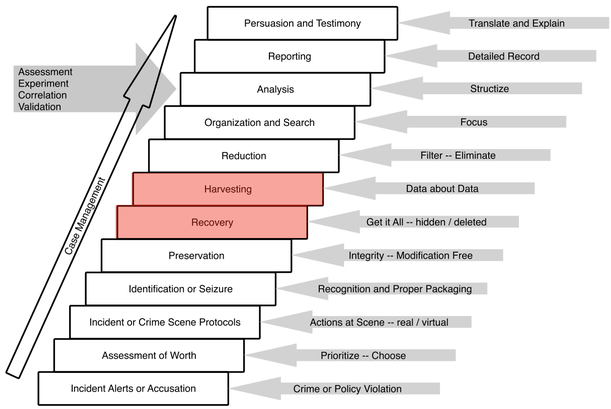
# Data Recovery and Harvesting

- This phase includes the retrieval of evidence that had been deleted, hided, masked or that has been made inaccessible in any other way.
- To achieve this tasks deep knowledge of the file system and other important data structures are needed.
- From the perspective of digital forensics, hard drives and low-level structures of various file systems are rather well studied.
- The effects of NAND technologies on the amount of recoverable data on storage devices, however, is still not completely understood today.
- Since wear leveling techniques tend to “smear” outdated data all over the device, it is often conjectured that digital investigations can profit from the widespread introduction of NAND flash, because it is harder for criminals to delete files and cover their traces.



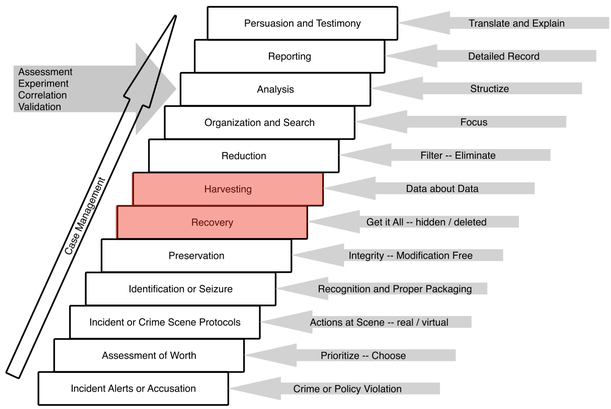
# Filesystems on modern Mobile Devices

- There are file systems that are aware of the generic flash limitations.
- Such file systems are much easier to analyze since they implement techniques like wear leveling in software.
- The most common example of such a file system is YAFFS2.
- This filesystem has been used on Android devices until Android 4.x



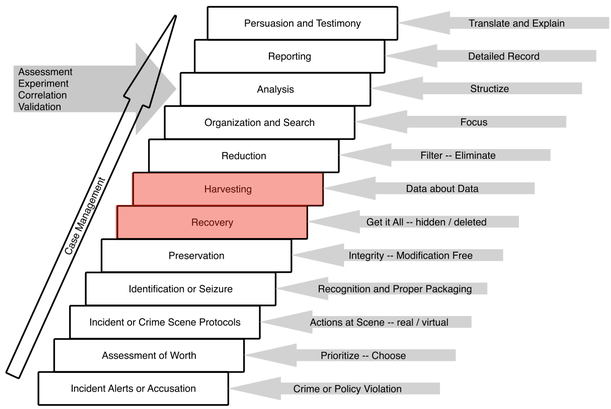
# Filesystems on modern Mobile Devices

- Since Android 4.x most of the Android-based smartphones use Ext3 and Ext4.
- Those file systems are very well known and a large amount of tools to support the analysis exist.



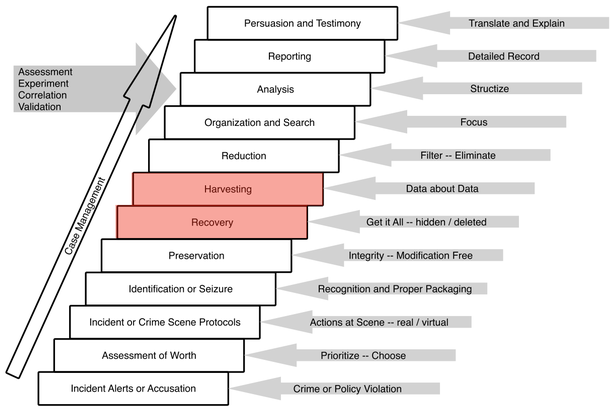
# Filesystems on modern Mobile Devices

- On Apple iOS-based devices the Apple file system HFS+ has been used in the past.
- This file system is also very well known and tool support is available (even if not to the same extent as for Ext3/Ext4).



# Filesystems on modern Mobile Devices

- Since iOS 11, Apple has changed from HFS+ to the new file system called APFS.
- This file system is relatively new and only a limited number of tools and internals exist which makes it harder for a forensic investigator to harvest or even recover data.
- But at the same time, it makes it also harder for a criminal to hide data on purpose.



# The Role of the Network Operator

- When it comes to mobile device investigations, we have one additional „player“ that is very important for the course of investigation:

**The mobile network operator**

- This data source can provide information to the law enforcement even if the actual device is not available or damaged/encrypted.

# Background

- Following the 2004 terrorist attacks in Madrid, the European Union issued a directive to harmonize regulations in EU member states concerning the retention of data generated by publicly available electronic communications services.

- The directive seeks to enable law enforcement to access traffic data pertaining to suspects, e.g., to discover who the suspects communicated with and the digital services that had been used.

# What Data is allowed to be stored

- According to this directive the following data has to be stored for a time period between six months and two years:
  - the source of a communication (subscriber ID or phone number);
  - the destination of a communication (subscriber ID or phone number);
  - the date, time and duration of a communication;
  - the type of communication (SMS message, MMS message or phone call);
  - the communication device (e.g., the IMEI of the device);
  - the location of mobile communication equipment (e.g., GPS data or at least the location of the mobile cell that was used);

# The EU Directive and German Law

- According to the EU directive 2006/24/EC, this data is required to be available to “competent” national authorities in specific cases, “for the purpose of investigation, detection and prosecution of serious crime, as defined by each Member State in its national law”.

- For Germany this has been done with the following law „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“

# Mobile Device Forensics

# SIM/UICC Card

„Microprocessor equipped tokens, able to store and process a diverse range of data and applications“

**European Telecommunications Standard Institute (ETSI)**

# SIM Card Characteristics

- A SIM card comprises the following components:
  - microprocessor (CPU)
  - RAM
  - ROM for firmware
  - EEPROM for nonvolatile storage
- Some parts of the card are protected by a PIN and can only be accessed by providing the correct PIN to the card. If the PIN is not available the network operator can provide you the PUK for this card if you can tell them the ICCID.
- Interaction with the card happens through APDU commands as defined in ETSI TS 102.221 (there you will also find the response codes).

# SIM Card Content

- Nowadays nearly no data is stored on the SIM card itself, as the card is relatively slow compared to the internal flash memory of the device.
- But still, you should always have a look at it, especially when dealing with feature/burner phones.
- Content that can be stored on the SIM card:
  - Contacts
  - SMS messages
  - Fixed dialing numbers (favourites)
  - Call logs

# Understanding the ICCID

- The ICCID (unique serial number of the card) hold important information
- Let’s take an ICCID and see what it means: `89490170105114482419`
- `89` - System Code (89 represents ISO 7812)
- `49` - Country Code
- `017` - Issuer Identification Number
- `0105` - Month and Year of production
- `11448241` - Unique Serial Number
- `9` - Checksum

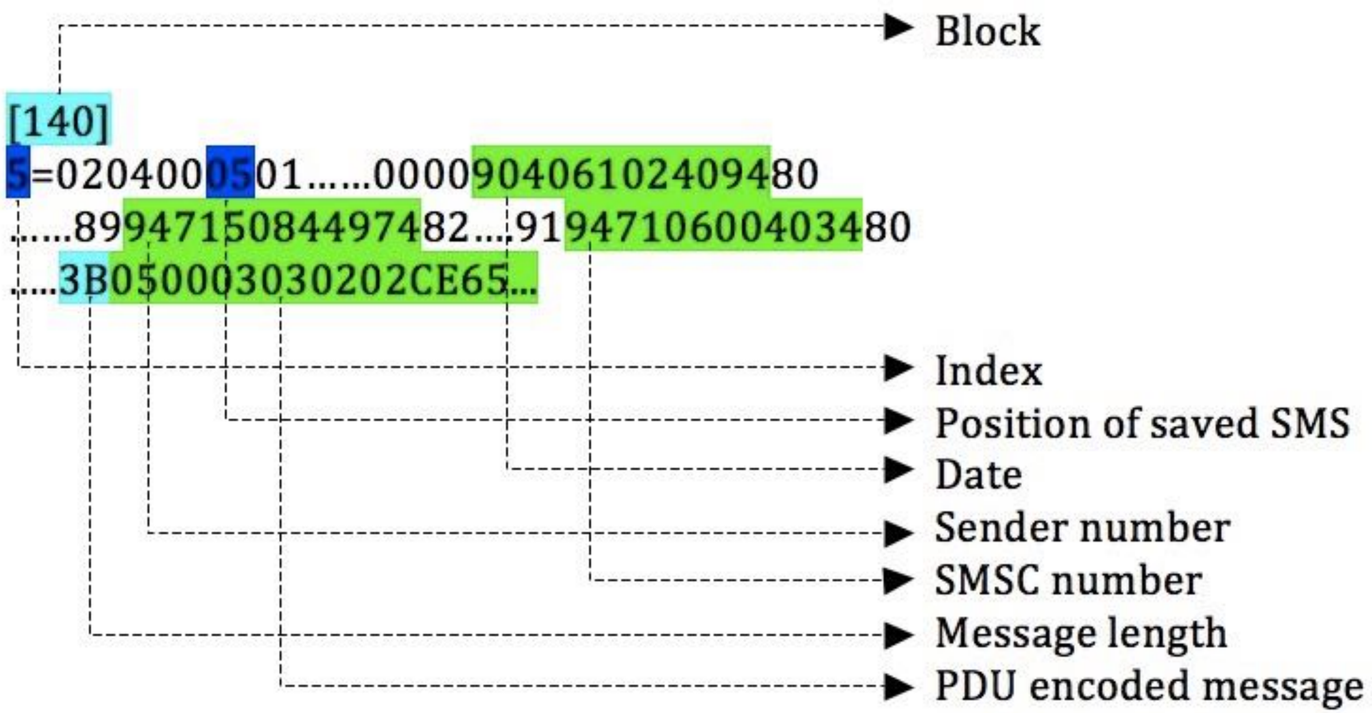
# Nokia S40

- Java-based OS
- closed source
- very limited in functionality and features
- very limited capacity
  (stores only last 10 SMS messages and last 10 calls)

# Acquisition Options

- Best support by Twister Box
- Flasher box allows to get full physical image of the storage
- Nokia backup software solution is also providing suitable results but not as trustworthy as the physical image.

# SMS Message


[140]
5=020400050 1.....0000 90406102409480
.....89947150844974 82....91947106004034 80
....3B050003030202CE65...
Block
Index
Position of saved SMS
Date
Sender number
SMSC number
Message length
PDU encoded message

# Reverse Nibble

81 50 10 61 02 30

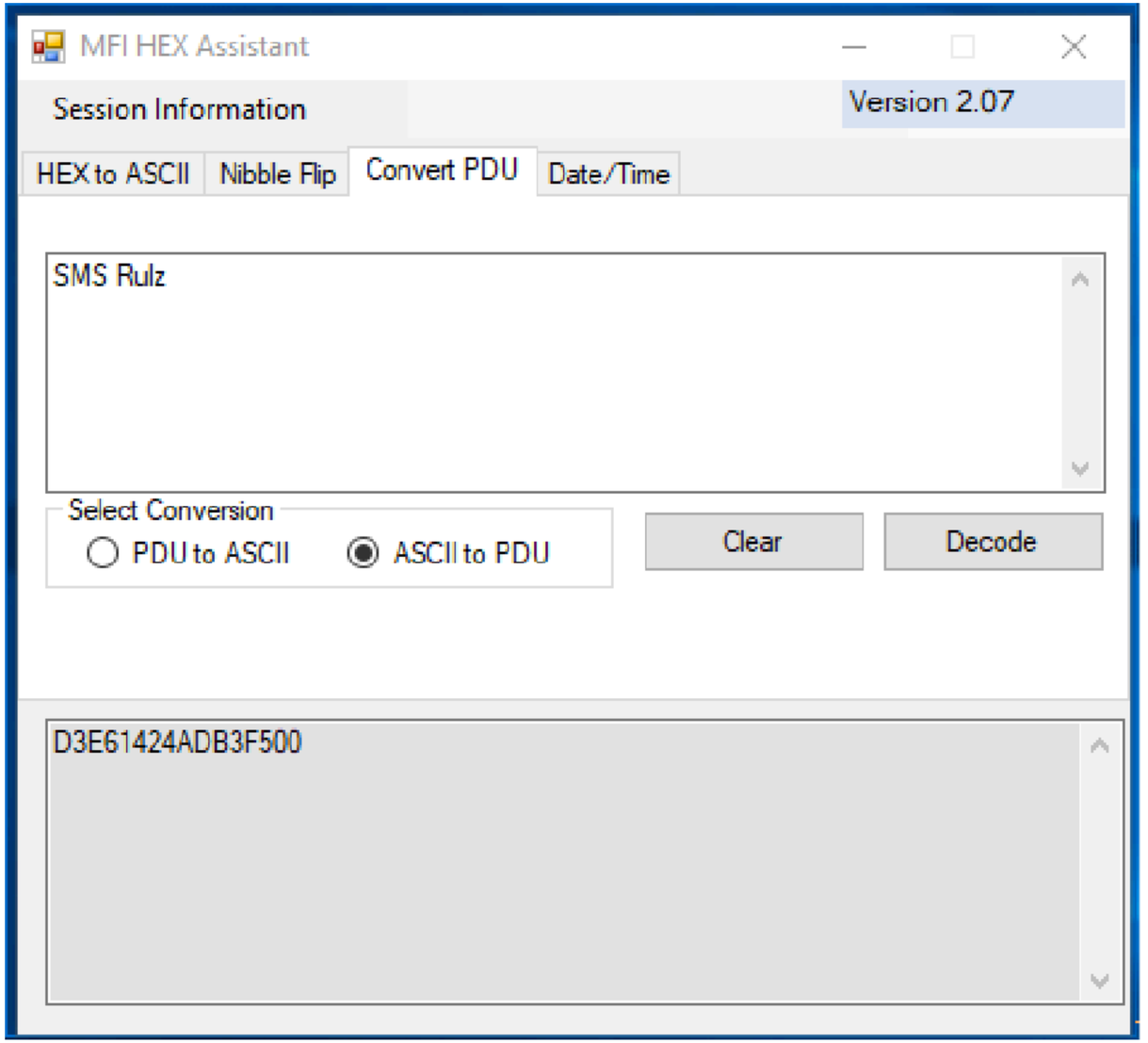
18 05 01 16 20 03

May 1st 2018, 16:20:03

# PDU Encoding

| **ASCII** | S | M | S | | R | u | l | z |
|---|---|---|---|---|---|---|---|---|
| **HEX** | 53 | 4D | 53 | 20 | 52 | 75 | 6C | 7A |
| **8Bit-Binary** | 01010011 | 01001101 | 01010011 | 00100000 | 01010010 | 01110101 | 01101100 | 01111010 |
| **Compress** | 1010011 | 1001101 | 1010011 | 0100000 | 1010010 | 1110101 | 1101100 | 1111010 |
| **7Bit-Binary** | 11010011 | 11100110 | 00010100 | 00100100 | 10101101 | 10110011 | 11110101 | |
| **HEX** | D3 | E6 | 14 | 24 | AD | B3 | F5 | |

# PDU Encoding



# Symbian OS

- Nokia elected Symbian OS for its older mobile devices and formed an alliance with them.
- Not only Nokia is using Symbian, the following manufacturers also used this OS:
  - Samsung, LG, Sony Ericsson, Motorola, Fujitsu, and Sharp
- Most common version of Symbian OS was version 7.x and 9.x
- These versions could be found as:
  - S60 1st - Nokia 3230, 6260, 6670 or 7610
  - S60 3rd - Nokia N95, N82, E71, E72, N96
  - S80 - Nokia 9300 or 9500
  - S90 - Nokia 7710 or 7700

# Acquisition Options

- Extensive support by nearly all commercial solutions
- Some commercial vendors even offer to unlock/circumvent the screen lock of Symbian based devices.
- Flasher box allows to get full physical image of the storage
  (Best support by Twister Box or HWK/UFS)
- Nokia PC Suite is also providing suitable results but not as trustworthy as the physical image.

# Evidence Locations

- If no sd-card is inserted in the device, all user related data (such as pictures or videos) are stored under C:\Data

- C:\Data\NEF\NEFConfig.xml
  contains the IMEI of the device (can be found on the external sd-card as well)

- C:\Favourites\BrowserBookmarks\Favourites.db
  contains all saved webpages/URLs

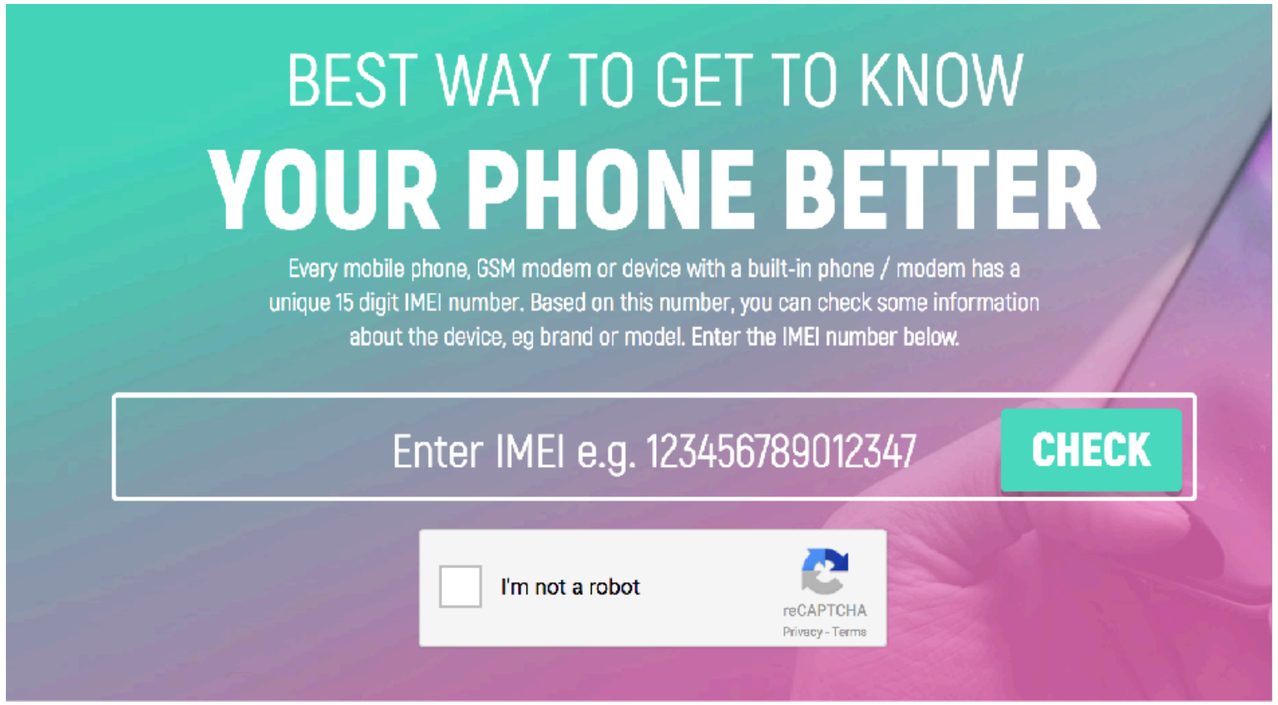
- Contacts are stored as vcf-files and are located within a proprietary database called DBS_100065FF_Contacts.cdb

- The database DBS_10207216_SWInstLog.cdb
  contains information of formally installed apps

# Check IMEI

- If you find a sd-card and want to know if the card belongs to a seized mobile device, the easiest way is to find the IMEI on the sd-card and use online-services to get more information regarding the device behind this IMEI.

- One example is http://imei.info



# Recap

- Why is mobile device forensics important nowadays?
- What are the most important identifiers?
- What „types“ of mobile devices are there?
- What are the forensic principles?
- Investigative Model by Casey and the differences when it comes to mobile devices
- The role of the network operator
- The SIM card and why it could be important during an investigation
- Understanding reverse nibble and PDU

# See you next week!

- [1] https://www.welt.de/vermischtes/article172287105/Mordprozess-Hussein-K-Die-Version-vom-Handeln-im-Affekt-ist-mit-dem-heutigen-Tag-obsolet.html
- [2] https://www.theguardian.com/media/2011/aug/08/london-riots-facebook-twitter-blackberry
- [3] https://appleinsider.com/articles/18/04/15/the-day-the-apple-watch-solved-a-murder-an-apple-crime-roundup
- [4] https://www.nytimes.com/2015/12/03/us/san-bernardino-shooting.html