universidade
de aveiro

Computer Systems Forensic Analysis
AFSC

Mobile Forensics

Artur Varanda

School Year 2023-2024

Forensic value of phones

Phones, especially smartphones, have a huge potential of providing evidences

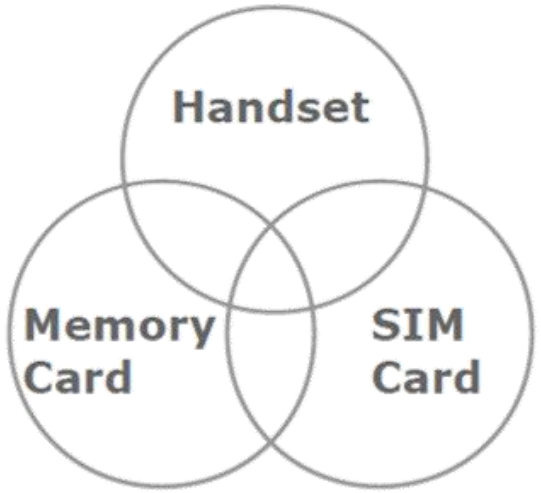
- are part of our everyday life
  - ✓ screen checks/day and h/day usage of smartphones
  - ✓ they store a huge amount of diverse information:
  - ✓ logs of calls, messages, GPS, network connections contents of messages, emails, multimedia (photos and video), social networks, etc…

- sales of smartphones surpassed PCs by the end of 2011

Phones' data locations

Where is data located in phones?

- data can be physically stored in 3 different locations:
  - ✓ handset, memory card and SIM card
- some types of data may be found in more than one location:
  - ✓ contacts on SIM and handset
  - ✓ pictures on handset and memory card



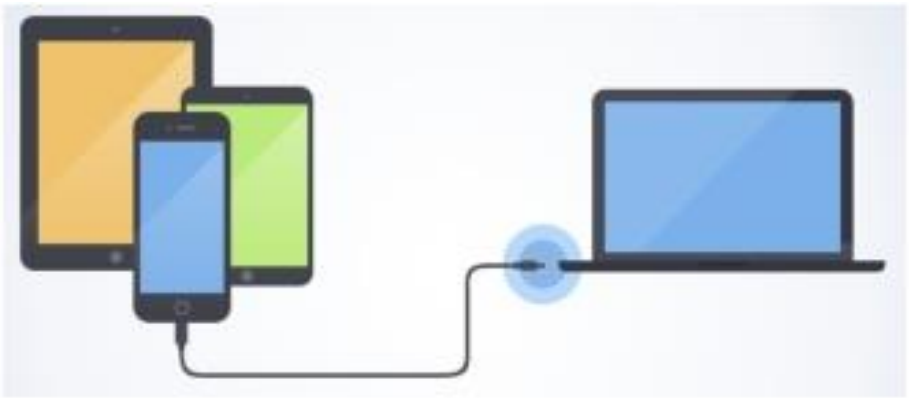
Acquiring data from phones

Retrieval approach:

- Examine every area (handset, memory card and SIM) independently
  - ✓ to be sure of capturing all the information you can

Can data be stored anywhere else?

- Service providers → requires additional legal procedures
- Cloud services → might require additional legal procedures
- Handset backups → more common in iOS devices



SIM cards?

Disambiguation

- UICC (Universal Integrated Circuit Card) – is the technical name of the physical part of the smart card
- SIM (Subscriber Identity Module) – is a logical module stored inside the smart card
  - ✓ in the early stages a SIM consisted of the hardware and the software

A given card can contain multiple SIMs
This would allow multiple phone numbers or accounts to be accessed by a single UICC.

12-in-1 UICC : https://multi-com.eu/,details,id_pr,2769,key,sim-max-12-in-1-card.html

Universal Integrated Circuit Card (UICC)

How many sizes/formats exist?

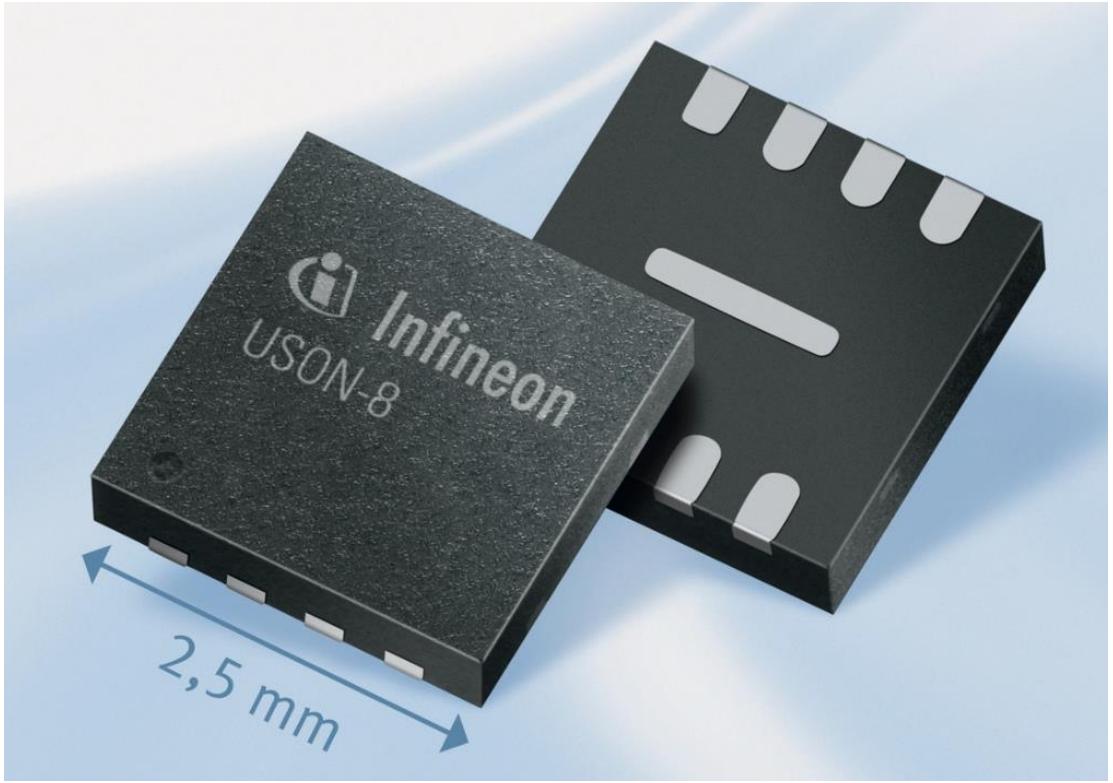
Variant	1FF	2FF ("Mini SIM")	3FF ("Micro SIM")	4FF ("Nano SIM")
Year of launch	1991	1996	2003	2012
Dimensions (mm)	85.6 x 53.98	25.0 x 15.0	15.0 x 12.0	12.3 x 8.8

These are user replaceable

Universal Integrated Circuit Card (UICC)

Embedded UICC (also know as eSIM)

- permanently embedding into devices used in machine-to-machine (M2M) applications
- not replaceable by a regular user
- 2 formats MFF1 and MFF2 { both have the same size
  - ✓ MFF1 is socketable (replaceable with special tools)
  - ✓ MFF2 is soldered



These are non user replaceable

Universal Integrated Circuit Card (UICC)

Main characteristics

- processor
- storage
  - ✓ memory to store text based user data e. g. SMS, contacts and calls
  - ✓ traditionally held just 16 to 64 KB, but there are some with 1 GB

UICC are also known as "SIM cards"

- mandatory in GSM networks
- standardized by 3GPP: https://www.3gpp.org/

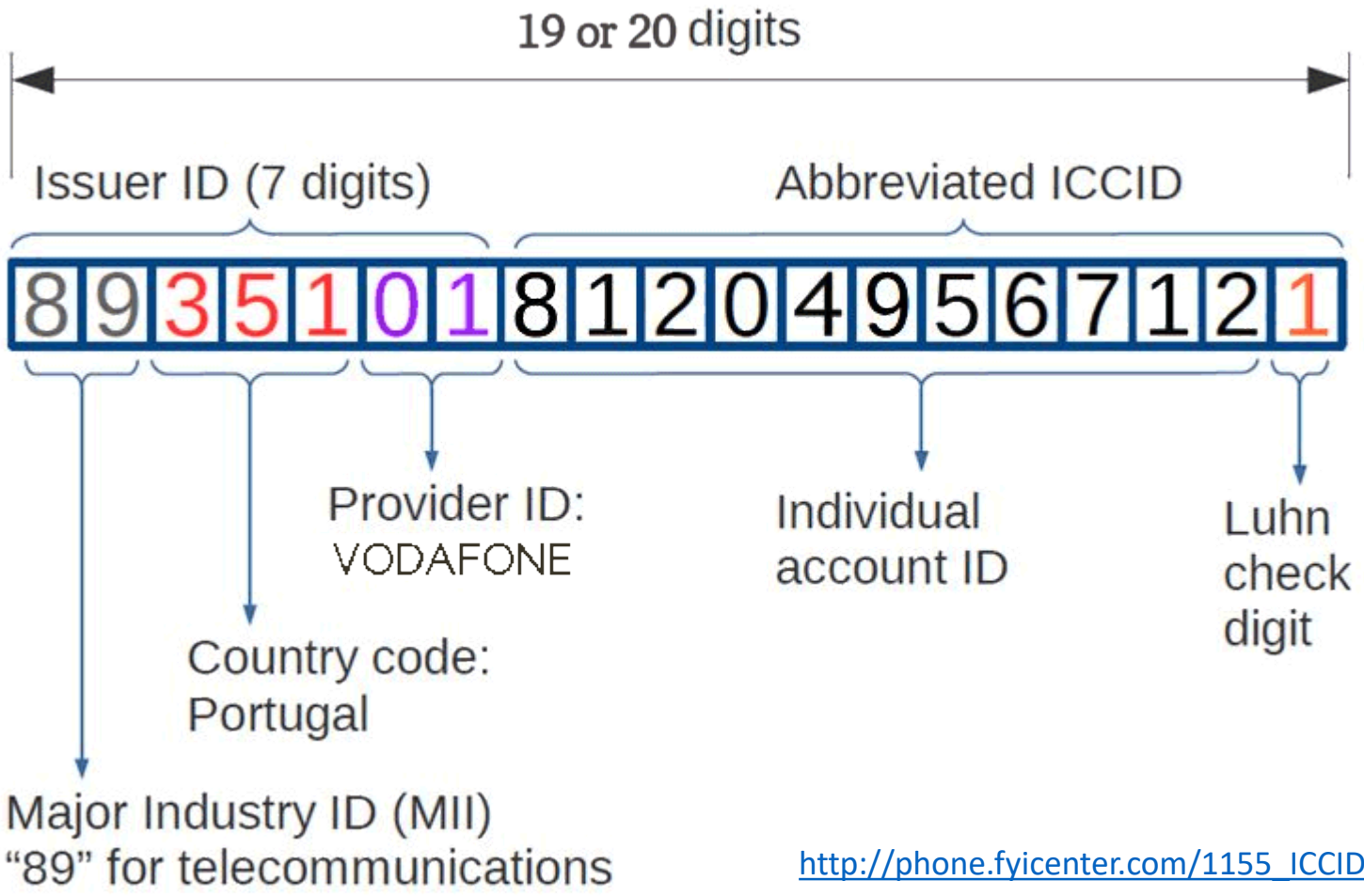
Universal Integrated Circuit Card (UICC)

Integrated Circuit Card Identifier (ICCID)

- uniquely identifies the card
- 19 or 20 digits in length
- often printed on the outside (may be abbreviated)
- always stored digitally in the card

ICCID identifies issuing service provider and country

Integrated Circuit Card Identifier (ICCID)



http://phone.fyicenter.com/1155_ICCID_SIM_Card_Number_Checker_Decoder.html

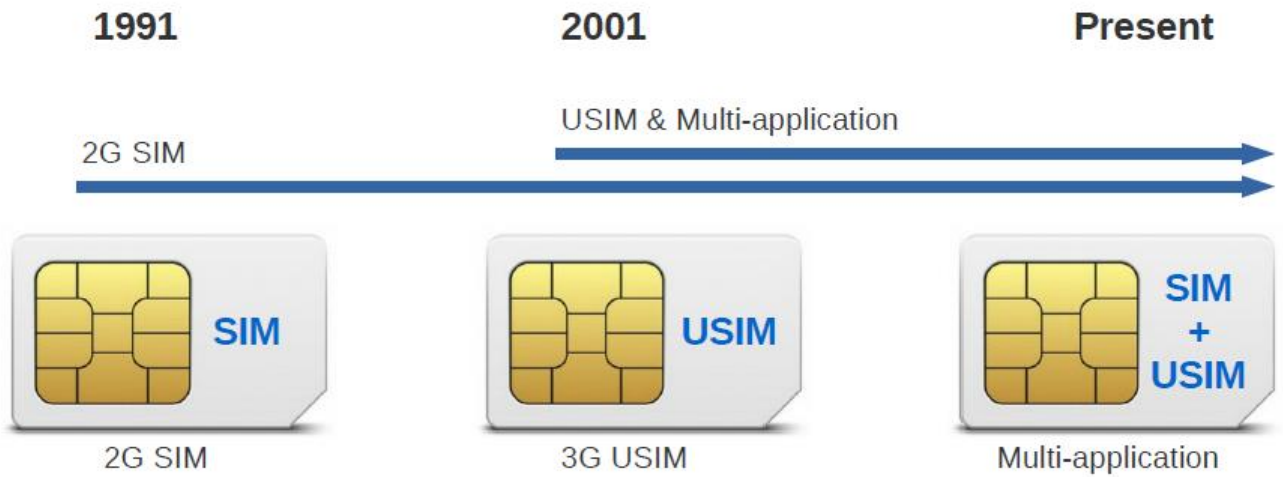
ICCID: 8935101812049567121

Subscriber Identity Module (SIM)

Role of the SIM

- **Authentication** - the mobile network uses a challenge/response security mechanism to allow access to the network;
- **Accountability** - the SIM contains a unique reference number that identifies both the card and the subscriber to ensure that associated costs are allocated correctly;

Subscriber Identity Module (SIM) - GSM types



USIM - Universal Subscriber Identity Module

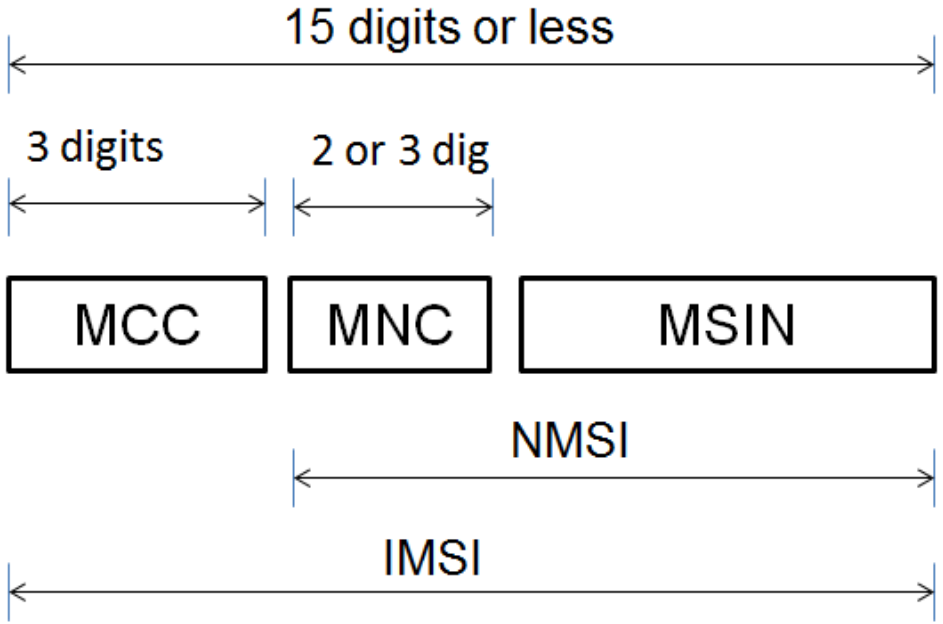
- for 3G and newer networks
- compared with SIM:
  - ✓ higher security, bigger and improved phonebook, can run small applications

Multi-application cards have 2 partitions: SIM + USIM

International Mobile Subscriber Identity (IMSI)

IMSI

- uniquely identifies the subscriber
- stored digitally in the card
- cannot be changed in a normal card
- can also identify issuing service provider and country
- usually not know by the owner
- composed by:
  - ✓ Mobile Country Code (MCC)
  - ✓ Mobile Network Code (MNC)
  - ✓ Mobile Subscription Identification Number (MSIN)



- MCC Portugal: 268
- MNC
  - ✓ 01 - Vodafone
  - ✓ 03 - NOS
  - ✓ 06 - MEO

https://www.msisdn.net/list-of-mcc-mnc/

MSISDN

- just like the IMSI, the DSISDN is also an important number used for identifying a mobile subscriber
- used for routing calls to the subscriber
- it is the number normally dialed to connect a call to the mobile phone
- The ITU-T recommendation E.164 limits the maximum length of an MSISDN to 15 digits. 1-3 digits are reserved for country code.

MSISDN = Country Code + Subscriber Number

Phones vary enormously

Huge variation between dierent handsets

- shape, keyboard, connectivity, features, memory, etc


What they have in common?

International Mobile Equipment Identifier (IMEI)

All handsets must be uniquely identified by IMEI

International Mobile Equipment Identifier

IMEI

- printed under the battery, or the back of the device
- stored digitally in the handset
  - ✓ can be displayed on most phones by entering *#06#
- first 8 digits identify manufacturer and model

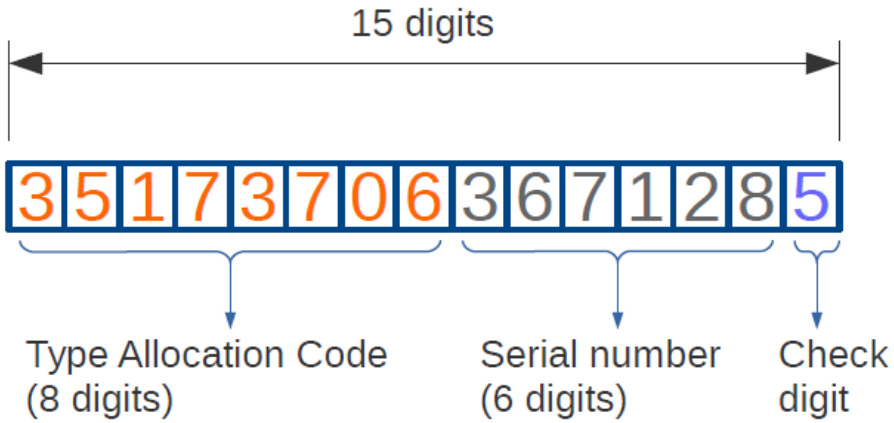
*#06#

IMEI

355995057333900 / 01

355996057333908 / 01

https://www.imei.info/



XRY Software

Supports device search by the first digits of TAC

https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity
https://en.wikipedia.org/wiki/Type_Allocation_Code (Manufacturer and model)
https://en.wikipedia.org/wiki/Reporting_Body_Identifier (GSMA-approved group that allocated the TAC)
https://en.wikipedia.org/wiki/Luhn_algorithm (Check digit computation)

Potential Evidence

What data can potentially be an evidence on the (U)SIM?

- ICCID and IMSI
- phonebook / contacts
- SMS messages, including deleted (if not overwritten)
- call information

	SIM	USIM
Dialled	Yes (no time, date or duration)	Yes (optionaly: time, date and duration)
Received	No	Yes (optionaly: time, date and duration)
Missed	No	Yes (optionaly: time, date and duration)

What happens when a SMS on the (U)SIM is deleted?

- the message status is changed to indicate message no longer required
- however, the content of the message is typically left intact
- message is only overwritten when space is required for a new SMS
- So deleted SMS may be retrieved by accessing SIM via a card reader

Each SMS message has a maximum length

- 160 characters (for the GSM Latin alphabet)
- less characters per message for Arabic, Hebrew, etc
- long SMS are split into 2 or more separate messages

Potential Evidence

Network data on SIM card

- location area information can be retrieved from SIM card but its value is limited
  - ✓ likely to reflect location of seizure, but could be used to ensure the handset hasn't been switched on after seizure
- list of allowed or forbidden networks
- other network information can also be retrieved, e. g. TMSI, Kc, etc
  - ✓ may not be relevant to many investigations
  - ✓ more details: Forensics Wiki (https://forensics.wiki/sim_cards/) and (https://en.wikipedia.org/wiki/SIM_card)

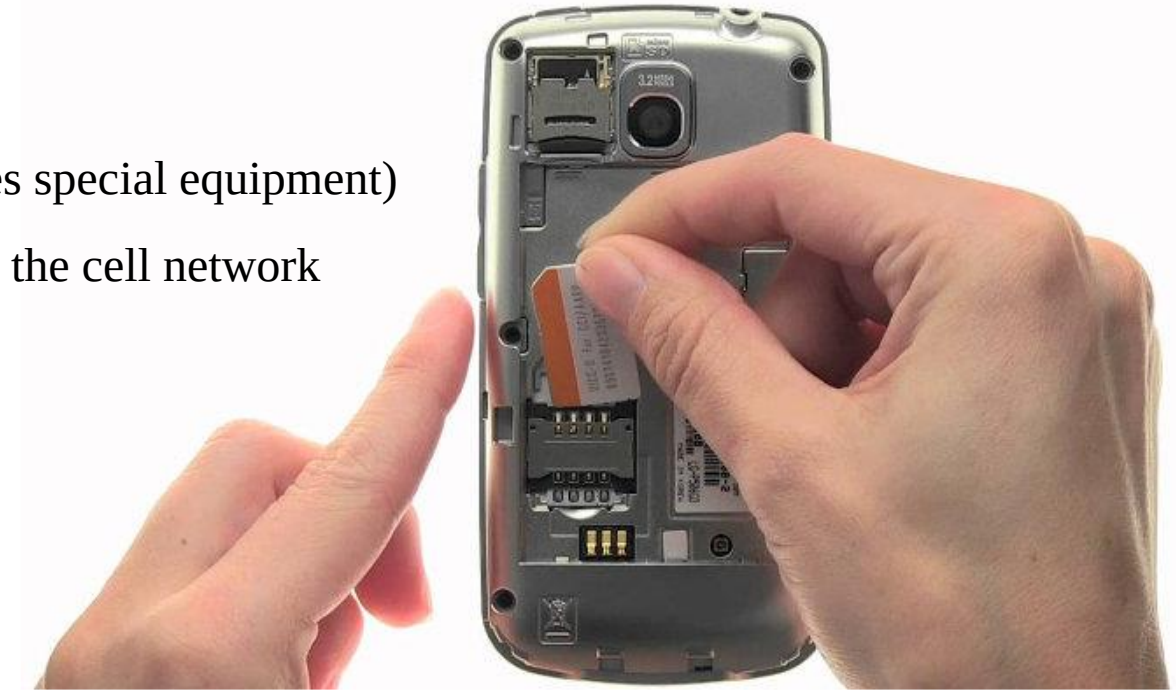
Warning

Some feature phones only work with a SIM card inserted.

However, if the handset detects that the SIM card has changed (based on IMSI, ICCID or both) it could potentially delete the call register entries

Solution:

- when available, clone SIM card ICCID and IMSI (requires special equipment)
  - ✓ SIM with cloned ICCID and IMSI cannot connect to the cell network



SIM card security

- PIN (personal identification number) - if the PIN is enabled and entered incorrectly 3 times in a row, the SIM card will be blocked
- PUK (PIN unlock key) - if PUK is entered 10 times incorrectly, the SIM card will become **permanently** blocked and **unrecoverable**
  - ✓ PUK is a SIM-specific code assigned by the service provider
  - ✓ cannot be changed by the user

Without the PIN

- only ICCID can be read from the SIM card
- with the ICCID ask the service provider for the PUK ⇨ requires legal procedures

Mobile Station International Subscriber Directory Number (MSISDN)

- SIM cards can store one or more phone numbers (MSISDNs)
- but entries are **unreliable**
  - ✓ the number may never have been used
  - ✓ the MSISDN may have been ported over from a previous SIM
  - ✓ in older handsets the number may be missing or **edited by owner**
  - ✓ MSISDN must be confirmed with the service provider

Data Acquisition

Connection Interfaces

Interfaces to acquire data

- Cable – fast and secure
- Bluetooth – slower than cable, leaves footprints in PC and handset

XRY Device Manual details the preferred connection

- same handset with different connection interface may produce different results
- “Manually find devices and apps” and read info

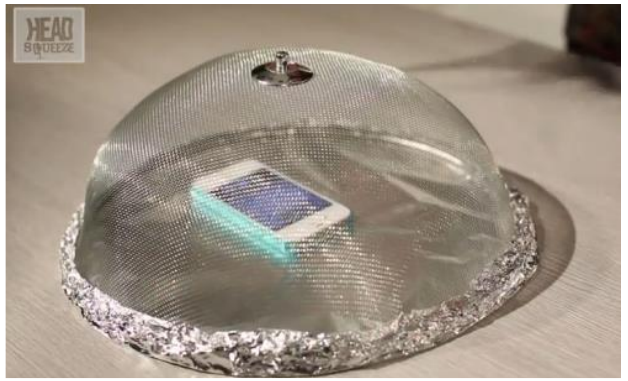
Network isolation

Ensure network isolation before data extraction

- airplane mode ON - many devices allow it in the block screen

or

- remove the SIM card and turn off Wi-Fi
- use a faraday cage
- signal jammers (might require special permission)



Importance of network isolation

- to avoid data changes (SMS, chat, calls, etc)
- to avoid remote locks or wipes

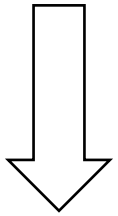
Logical acquisition

How it works?

- acquisition software asks handset what data is available
- handset may or may not provide data
  - ✓ usually, it's not possible to get deleted data
- different protocols are used for
  - ✓ different handsets and OS
  - ✓ different data types

Different types of logical acquisition

- full acquisition (through an agent app)
- ask the smartphone to do a backup



Logical acquisition

What data can be retrieved in a logical acquisition?

	SIM Card	Feature phone	Smartphone
Live data (undeleted)	Live SIM data can be retrieved	Live handset data can be retrieved	Live handset data can be retrieved
Deleted data	only SMS with card reader	deleted handset data cannot be retrieved	deleted handset data may be retrieved

Logical acquisition

Logical acquisition requires access to the OS.

How to beat the security code?

- ask the owner!
- XRY can get the security codes of some devices, check the “Device Manual"
- smudged swipe pattern
- manufacturers defaults (check user manual)
- on some devices XRY can do a physical acquisition without the security code

Physical acquisition

How it works?

- data is recovered in raw form
  - ✓ copy bit by bit
  - ✓ provides a lot of data, including deleted data (not overwritten)
  - ✓ requires decoding of the raw data
    - CPU intensive
    - software may not be able to decode everything
    - cannot be done if device is encrypted

What data can be retrieved in a physical acquisition?

	SIM Card	Feature phone	Smartphone
All data is extracted, bit by bit (there is no distinction between deleted and undeleted data)	N/A	Data can be decoded: previous IMSI/ICCID details + bluetooth pairings + some security codes + apps data + etc deleted data may be recoverable	encrypted devices cannot be decoded

Single hash for repeatability is not feasible

In mobile data acquisition hashing cannot be treated the same way as in HDD

- each time the handset is turned ON something changes
- it is not feasible to have a single hash value for the acquired image
- it is very important to hash ALL content individually (every file or digital object)
  - ✓ this is done automatically by acquisition software like XRY

=

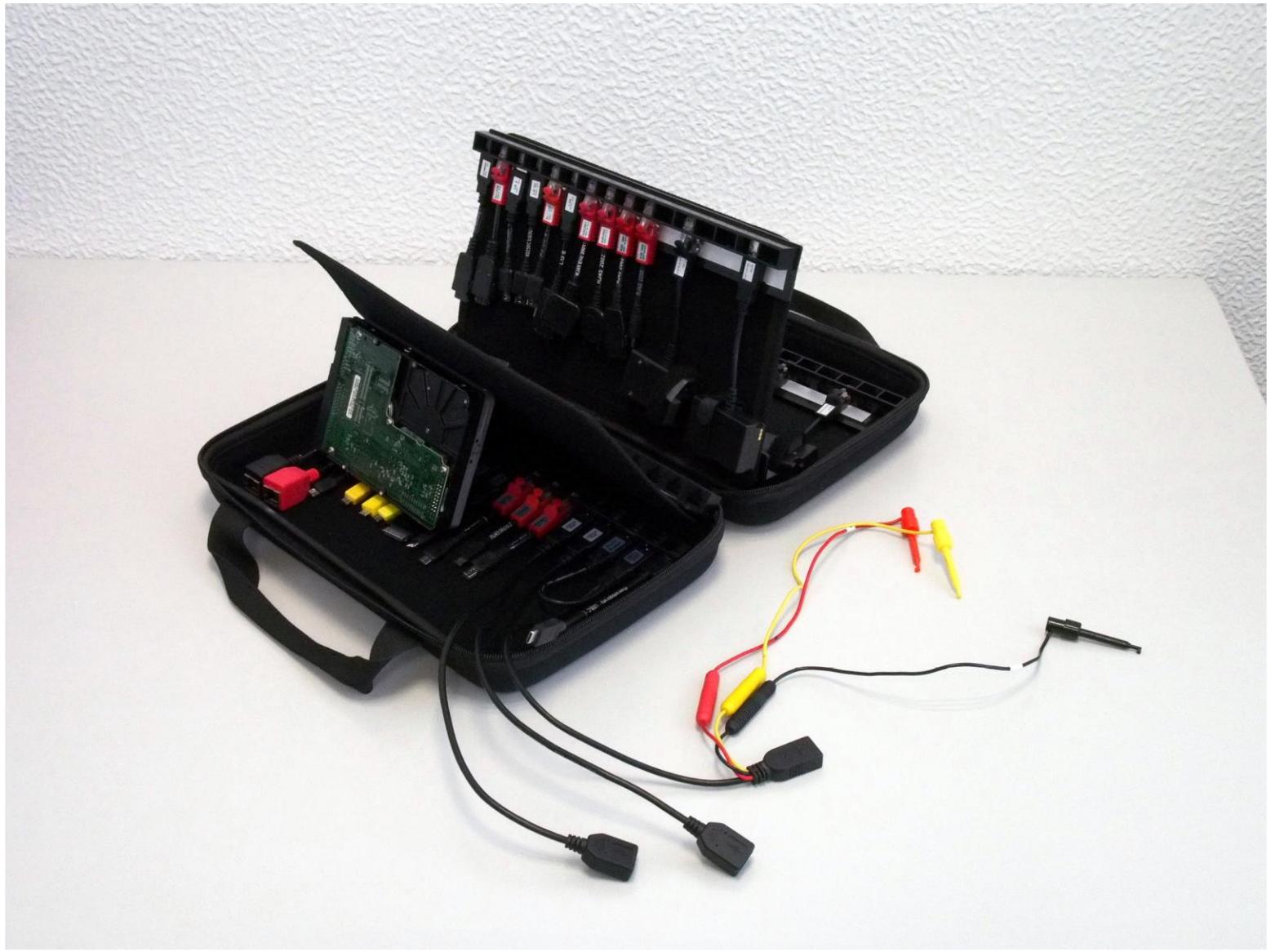
```
79054025
255fb1a2
6e4bc422
aef54eb4
```

Software tools

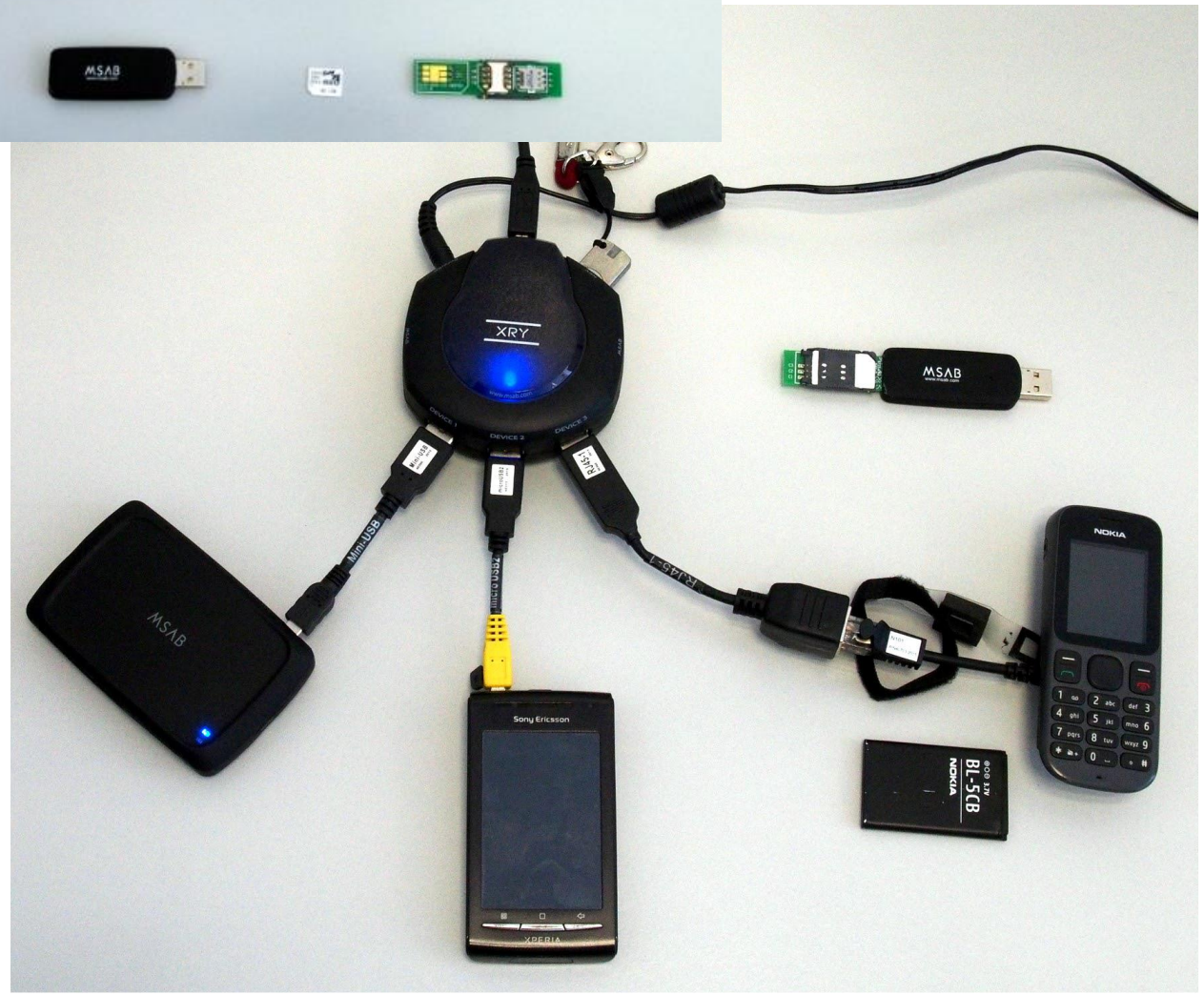
Some software tools:

- **XRY** - to acquire data on mobile devices
- **FTK Imager** - to acquire data on memory cards
- **Autopsy** - to analyze acquisitions, some support for Android
- **SQLiteBrowser** - to see browsers caches and mobile apps databases
- **file** - to identify le types regardless of extension
- **strings** - to extract strings (ascii, utf-8 or utf-16)
- scripting to speed up repetitive tasks
- phones specifications: https://phonescoop.com and https://gsmarena.com

Hardware tools



Hardware tools



Conclusions

Service providers can give additional information:

- subsriber details (name, address, payment details, etc)
- calls made/received
- SMS and MMS logs
- voicemail
- location information
- ICCID / IMSI / IMEI / phone number (MSISDN)
- PUK code

Exercise 1

Open the file `MAVEN.xrycase` with XAMN Launcher

1- open the `SIM` acquisition

- what is the card ID (ICCID)? Who issued this SIM card? what is the network operator?
- what is the phone number?
- click on `Device`, a new tab will open
- what was the last network the device was connected?

2 - open the `Agent` acquisition

- what is the phone brand and model?
- what is the device timezone?
- click on `ALL`, a new tab will open
- what is the phone number of `Kara Thrace`?
- what number was dialed on 16-06-2016 21:21:11 UTC?

3 - Look for MMS, choose MMS ID 1

- “launch” the image file and look at its properties (exif info)
- find the GPS coordinates, what is the address where the photo was taken?
- the photo on the MMS ID 2 was in the same area?

Exercise 2

Still in the file case `MAVEN.xrycase`, open the `Backup` acquisition

1 - add a word list filter with `Kik` (a messaging app)

- change to `File tree` view pane

2 - profile picture

- `/data/data/kik.android/8c66b2ac[...]/cache/profPics/`
- can you see the profile picture?
- can you tell the username?

3 - look for the app databases

- directory `/data/data/kik.android/databases/`
- save this file `8c66b2ac[...]37.`**`kikDatabase.db`**

4 - with SQLiteBrowser

- open database `kikDatabase.db`
- see contents of table `KIKcontactsTable`
- what is the photo time stamp of user `funnyordie`?

5 - with MFT Stampede

- convert the `photo-timestamp` to readable format

QUESTIONS?