SWINBURNE UNIVERSITY OF TECHNOLOGY

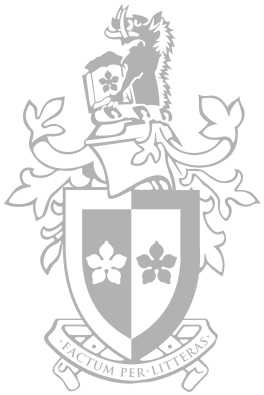
ICT30010 eForensic Fundamentals

Lecture 8

Mobile Technologies

Troy Pretty

Digital Forensic Analyst



SWINBURNE UNIVERSITY OF TECHNOLOGY

Lecture outline

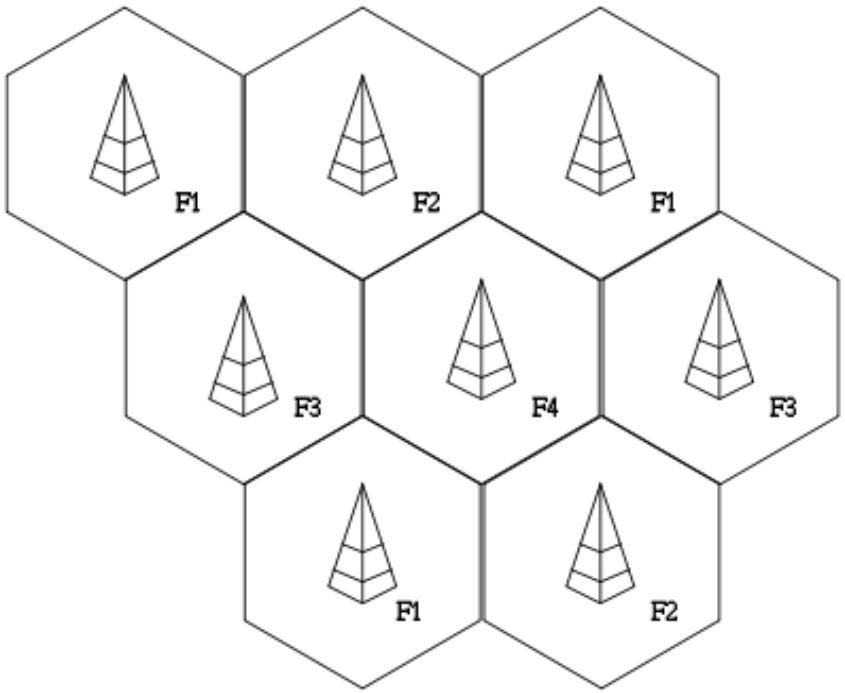
- Mobile technologies
  - Mobile networks and protocols
  - Mobile software
- Mobile Data Storage
- Value to investigation
- Legal Authority

Overview of mobile technologies

- Mobile technologies include mobile telephony, broadband wireless, SMS, MMS and similar
- Users of such technologies purchase a handset (or modem) and subscribe to a network
  - Traditional handsets which offer voice and SMS
  - Smartphones such as iPhone and Android
- Users are often unaware of the huge infrastructure needed to support such communications

Cellular networks

- Coverage using cells allows communications frequencies to be reused
  - Frequency (bandwidth, spectrum) suitable for mobile communications is very limited and so is often auctioned by governments for huge sums of money
    - Efficient use of spectrum one of the key design issues of cellular networks
    - Cellular coverage often modeled using hexagons that slightly overlap



Cellular networks (GSM)

- Each base station (Base Transceiver Station – BTS) is connected to a Base Station Controller (BSC)
- Each BSC is connected to a Mobile Switching Centre (MSC)
- The MSC is connected to other MSCs, other networks and contains a number of important databases

Cellular Networks

- Base Transceiver Station (or Base Station)
  - Antennae, Transmitter, Receiver
  - Backhaul which might be microwave, fibre optic or coaxial cable
- Base Station Controller
  - Responsible for frequency allocation
  - Usually located with MSC or BTS

Cellular networks

- As a user moves from one area of coverage to another, they may be disconnected from one base station and connected to another one
  - A process called “Handover” or “Handoff”

Cellular networks (GSM)

Global System for Mobile Communications (GSM)

Mobile Station =

Subscriber Identity Module
(SIM)

+

Mobile Equipment
(ME)

Mobile network technologies

AMPS
1G
1979

GSM
2G
1991

UMTS
3G
1998

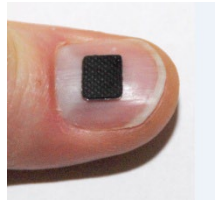
LTE
4G
2009

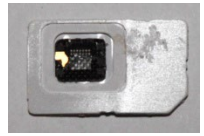
5G
2019

Pictures from wikipedia, samsung, blackberry, cnet

Physical SIM/USIM

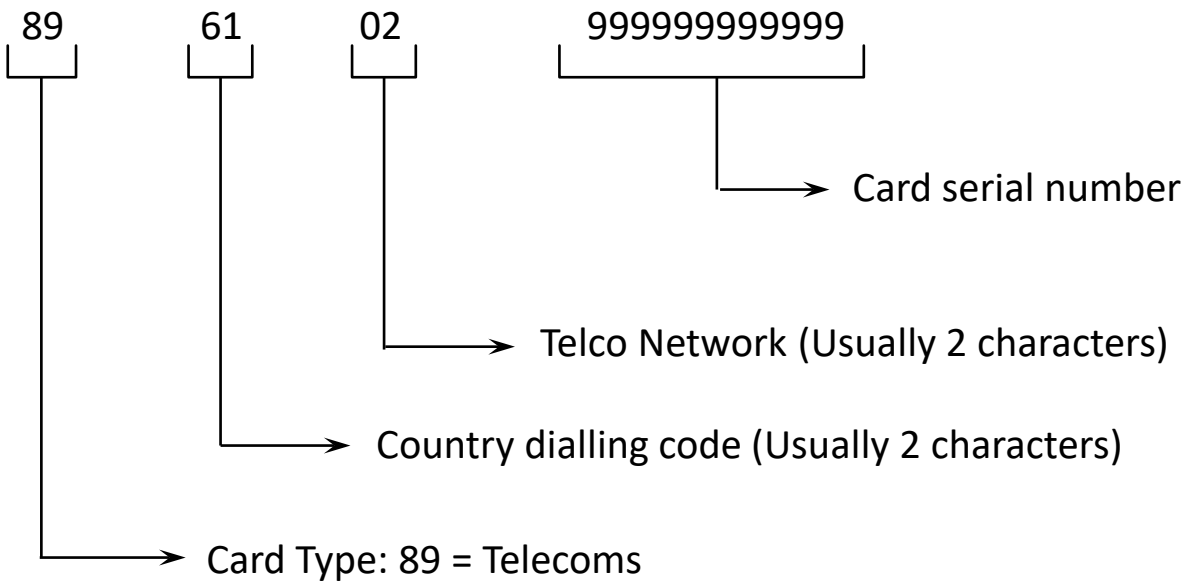
- SIM for 2G
- USIM for 3G+, UMTS
- Dual mode (SIM/USIM)
- Variety of designs, with 6 to 8 contacts.
- Chip is tiny and fragile
- Plastic is packaging
- ESIM?
  - Software based





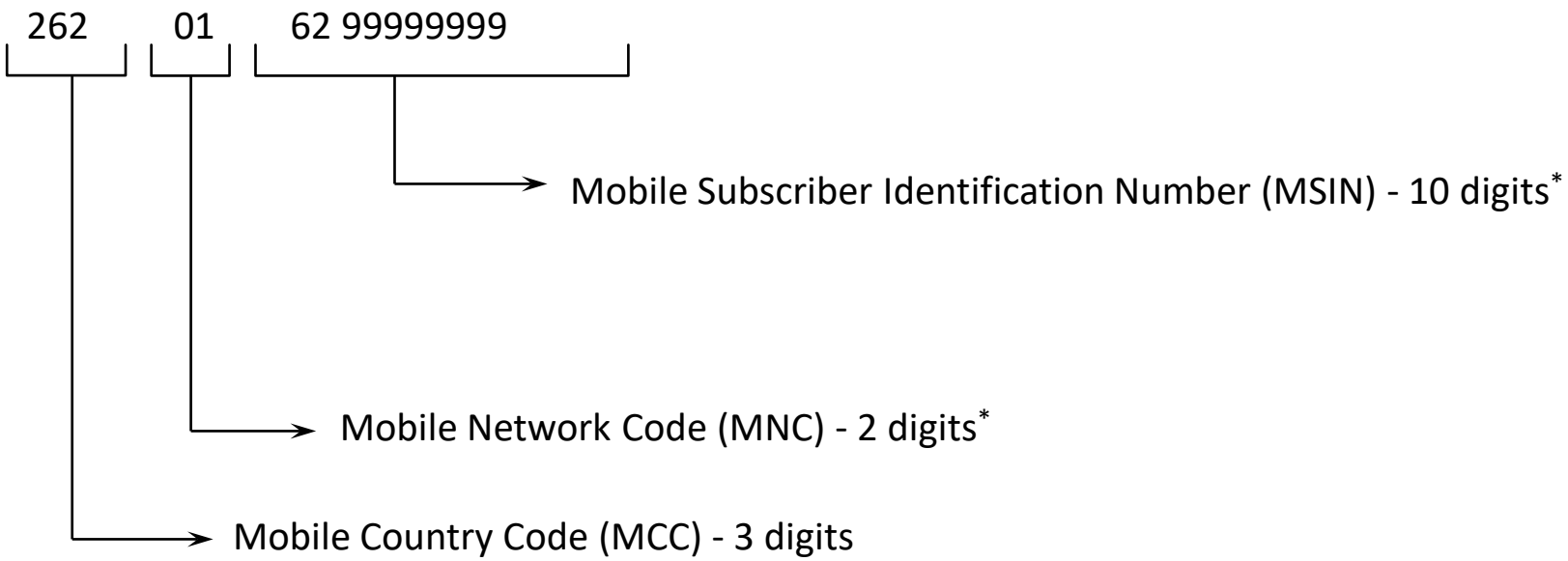
Integrated Circuit Card Identifier (ICCID)

ICCID is the unique ID to reference a SIM card



International Mobile Subscriber Identity (IMSI)

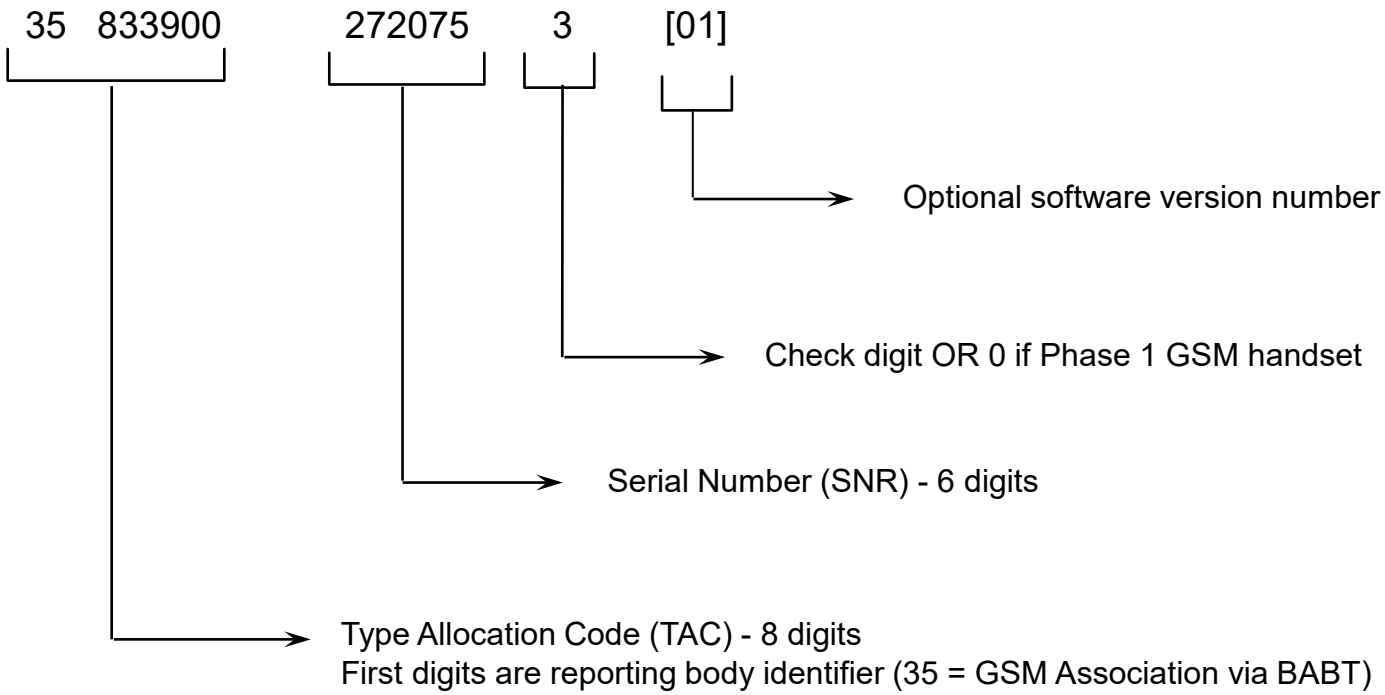
IMSI is the unique ID to identify the subscriber



* The length for MNC and MSIN has become more variable, mainly because of GSM 1900 in USA with >100 operators

International Mobile Equipment Identity (IMEI)

IMEI is the unique ID allocated to the mobile equipment (ME) / Handset



Device/Network Communications

- Mobile devices are very chatty
  - Even when not making a call, a great deal of information is exchanged between the network and the device
  - Location of the device
  - Base station connection information such as frequencies available, timing information and similar
  - Signal strength from neighboring base stations to help with handover decisions
- Lots of useful information made available just by turning the device on

Where is data stored?

- SIM Card
- Phone (Internal Memory)
- Memory card (External Memory)
- Network / Service Provider / Cloud

Data Types

- Contacts
- Call registers
- Text messages
- Calendar
- Identification numbers
- Multimedia messages
- Internet
- WiFi/Bluetooth
- Subscriber numbers
- Email
- Photos
- Ringtones
- Videos
- Sound recordings
- Applications
- GPS/SatNav

Data Storage – Internal Memory

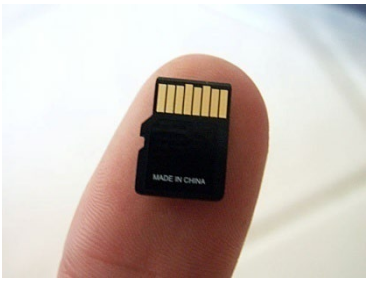
- Flash memory
  - Can be read and written
  - Stores data without power source (non-volatile)
- Chip is fixed directly to circuit board
- Often uses proprietary file system (eg YAFFS, APFS)
- Can only be fully read by manufacturer
  - JTAG / Chip-off becoming more available

Data Storage – SIM Card

- Network Information (IMSI, preferred/forbidden networks,etc.)
- Contacts
- SMS Messages
- Subscriber Phone Number (user-modifiable, often blank)
- USIM allows extended attributes such as email

Data Storage – Memory Cards

- Lots of standards
- Use standard file system
  - Typically FAT32
- Store user selected data
- Generally multimedia only
- May be internal or external



Data Storage – Cloud/Network

- 3rd Service Providers
  - Email
    - Hotmail, Gmail, Yahoo
  - Social Media
    - Facebook, Instagram, Snapchat
  - Chat Applications
    - Skype, Zoom
- Source of communications and contacts
- Issues with lawful access
  - Unauthorised access
  - Overseas service providers

Online Account Encryption

- Online accounts increasingly leverage encryption (Skype, Facebook etc.)
  - In transit
    - HTTPS
  - At rest
    - File
    - Database
  - Both

Online Account Encryption

- Analysis Challenges
  - Encrypted in transit but not at rest
    - Download and parse filesystem databases
  - Encrypted at rest but not in transit
    - Review data as it is transmitted (lawful?)
  - Encrypted at rest and in transit
    - Can be challenging
    - Crack or obtain password
    - Look for weaknesses in implementation of encryption
  - Look for data on other storage devices

Value

- Source of a crime
  - Hacking into a website
  - Sending abusive text messages
- Planning a crime
  - Calling or messaging co-offenders
  - Internet searches/history
- Evidence of a crime
  - Photos/videos of drugs/guns/assaults

Value

- Storage capacities and processing power rival traditional computers
- Mobile nature results in offending anytime/anywhere

Complexities

- There is an increasing differentiation between the Carrier, the Internet Service Provider and the Application Service Provider
  - For example, a customer might use Telstra's twisted pair copper wire to carry ADSL which connects them to ISP iiNet from where they make use of Google Apps
  - Linking identity to a particular IP packet in such an environment is quite challenging
  - Identifying the person who has requested a particular IP traffic stream is not straightforward

Authority/Authorisation

- Forensic investigator integrity
  - Cant break the law in the pursuit of evidence
- Need to ensure adequate authority to conduct investigation
  - Internal
    - Employment contract, HR/Manager authority
  - Outsourced
    - Contact/Scope of Work
  - Law Enforcement
    - Search warrant approved by the courts

Authority/Authorisation

- Forensic investigation uncovers online account passwords
  - Can these be used to login to the accounts?
    - CRIMES ACT 1958 - SECT 247G
    - Unauthorised access to or modification of restricted data
    - Maximum 2 years imprisonment

Authority/Authorisation

- Compromise investigation
  - Tarnish reputation
  - Evidence discounted/excluded
  - Termination of employment
  - Criminal Investigation?

Summary

- Mobile technologies
- Mobile Data Storage
- Value to investigation
- Legal Authority