

TrewMTE Starter Kit TWO MFW08

Mobile Telephone Evidence

Comparative and Holistic Approach to Mobile Telephone Evidence

Presenter - Gregory Smith TrewMTE

Trew & Co (TrewMTE)

Tel: 00442084608034

Web: <http://trewmte.blogspot.com>

Email: trewCO@compuserve.com



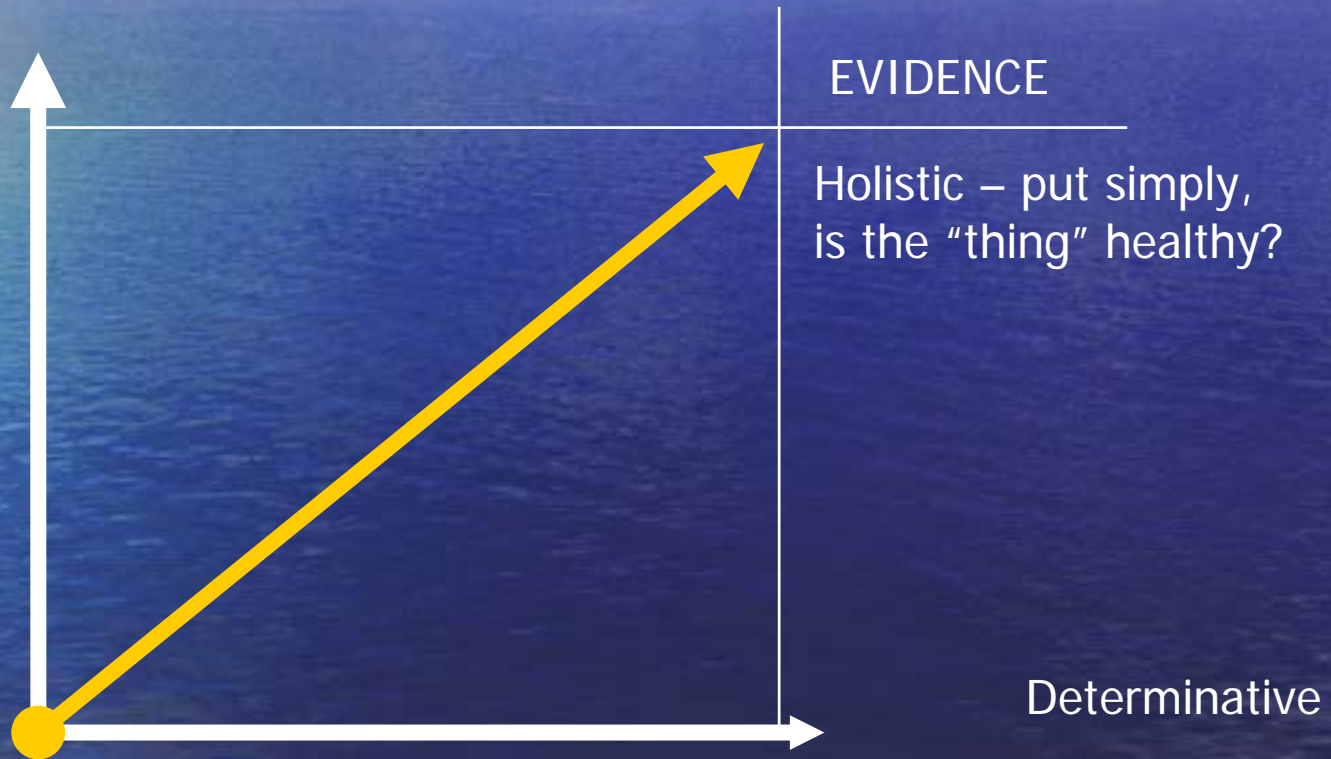
TREW MTE

Mobile Telephone Evidence
Training



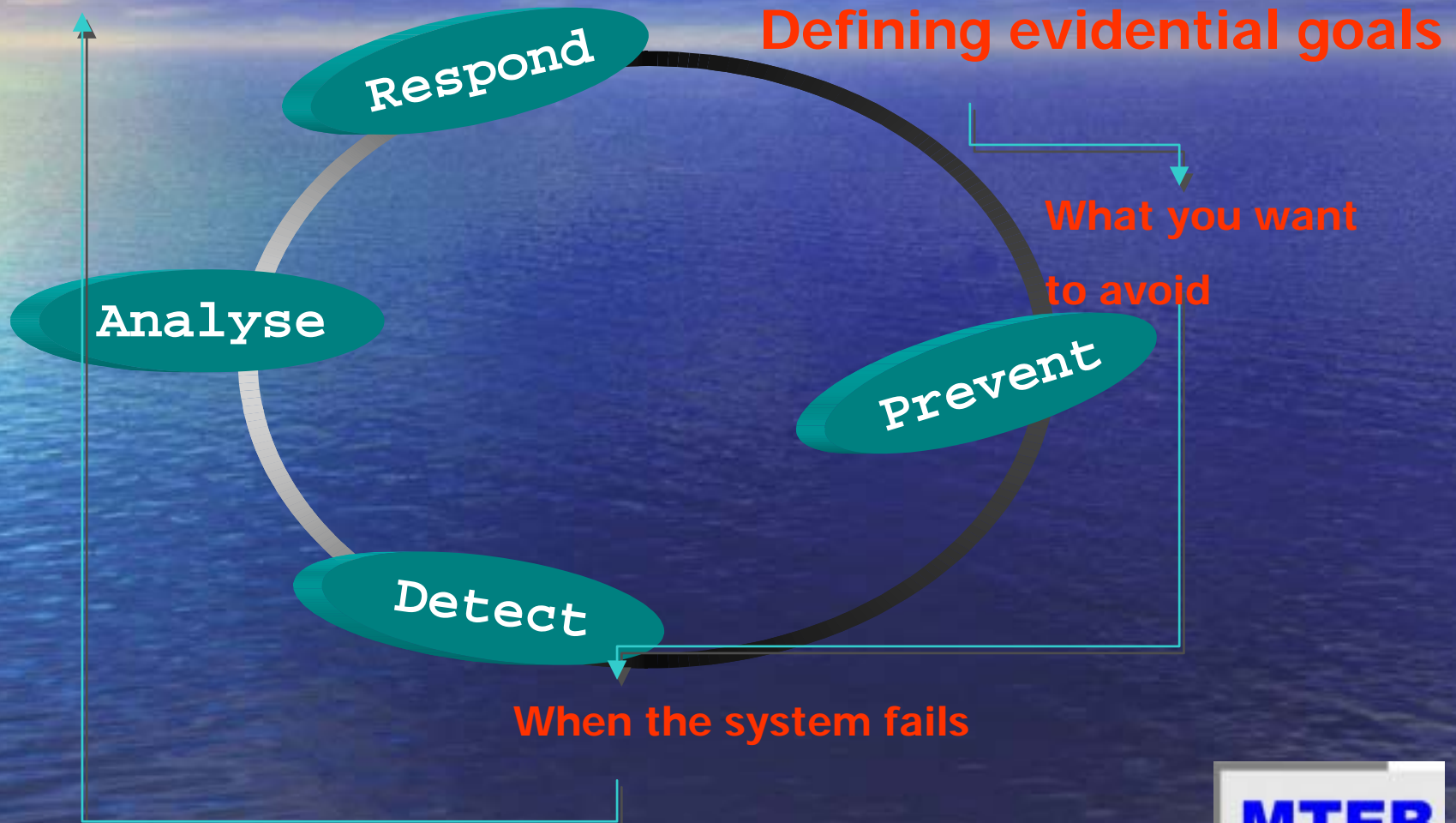
Comparative and Holistic

Comparative



Comparative and Holistic

Impact on evidence at court



Topics of Discussion

- 1 Seizure Procedure
- 2 Handling and device assessment procedure
- 3 Good inwards procedure (for examination)
- 4 Laboratory environment procedure
- 5 Examination procedure
- 6 Post examination procedure
- 7 Quarantine procedure

Topics of Discussion

1 Seizure Procedure

- policy on basic practice and practises
- policy on advanced practice and practises
- policy for the unusual seizure

Topics of Discussion

2 Handling and device assessment procedure

- Is this an urgent matter?
- Is the device safe?
- Has the device been made safe?
- Does the device require fingerprint/DNA etc?
- etc

Topics of Discussion

3 Good inwards procedure (for examination)

- Device containment
- Paperwork
- Target data requirement
- Allocation of resources
- Deliverables
- etc

Topics of Discussion

4 Laboratory environment procedure

- Examination tools (x-ray etc)
- Anti-static approach
- Gloves
- Radio dampening field or chamber
- Photograph/video
- etc

Topics of Discussion

5 Examination procedure

- Examination devices
- Target SIM/USIM
- Target Mobile Telephone/Smart 'Phone
- Extraction and harvesting of data
- Contemporaneous notes
- etc

Topics of Discussion

6 Post examination procedure

- Evidence containers and seals
- Labelling
- Signing off
- Notification work completed
- Report writing
- etc

Topics of Discussion

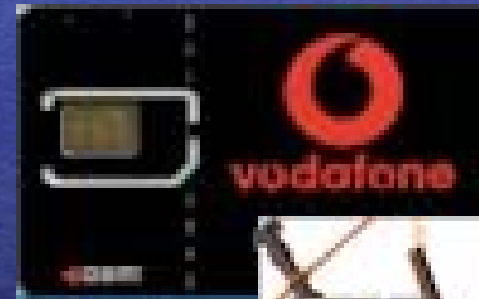
- Quarantine procedure
- Stores containment area
- Documented receipt in stores (goods in)
- Release from responsibility to hold device (goods out)
- Distribution of data
- etc

The Role of the Professional Examiner

- *Forensically Retrieve & Analyse Stored Data*
- *Produce evidence in usable format*
- *Attend court*
- *Attend interviews*
- *Attend warrants*
- *Give advice and support*
- *On call rota 24/7/365*

What is a SIM Card?

- *SIM – Subscriber Identity Module*
- *Manufactured in accordance with GSM specification (e.g. 11.11)*
- *Are network specific*
- *Both read only and read/write functions*
- *SIM card can do no more without a mobile phone or other suitable device (PCMCIA card phone etc.)*
- *Secure for data storage (PIN)*
- *Advancement/Service Accessibility*



What is a SIM Card?

- *SIM – Subscriber Identity Module*
- *There are two types of SIM card, subject to the same mandatory requirements:*
- *The first is the size of a credit card, called ISO size:*



- *And the second is the size of a postage stamp, called a plug-in card:*



What is a SIM Card?



SIM – Serial Numbers

ICCID number

- The card must have a unique serial number called an ICCID (Integrated Circuit Card Identity) number, which must be electronically recorded in the card's memory. Because the ICCID number is mandatory it is allocated a unique data file address with the SIM card memory where that memory space cannot be allocated to any other data than the ICCID number. The unique data file location address is 3F00:2FE2. A user cannot erase or alter an ICCID when recorded into this memory location.
- There are important reasons for the ICCID number. Most importantly, when a SIM Card is supplied or sold to a subscriber in order that the subscriber can make or receive mobile telephone calls using the subscription details recorded in the SIM, the Card becomes a Charge Card. A benefit is acquired (service) and a detriment incurred (payment) by mobile telephone account holder and network operator alike. For that purpose the implementation and structure of the ICCID is recorded in the International Telecommunications Union Telecommunications Recommendation - ITU-TE118 International telecommunication charge card numbering scheme.

SIM Serial Number

- On the face of an SIM card the ICCID number may be reproduced in whole or part. When the number appears on the face of the card it is termed the SIM Serial Number (SSN).

What is a SIM Card?

SIM – Serial Numbers

ICCID number

- **Another important reason for the ICCID number is that it forms part of the security for the card. One security feature derived from the ICCID number are global access codes (PUK) that can be used to unlock the card or personalisation implemented to certain files in SIM where the user has lost or forgotten their personal access codes.**

What is a SIM Card?

SIM – Subscriber Account Number

IMSI number

- The mobile network operator identifies and validates a subscriber to its network using the International Mobile Subscriber Identity (IMSI). No other SIM card or subscriber should have the same IMSI number allocated.
- The IMSI number is transmitted over-the-air (OTA) to the network and used in the authentication security processing procedure in order that a subscriber can make or receive mobile telephone calls. Once recorded into a SIM, the IMSI number cannot be erased or altered by a subscriber. The IMSI number is mandatory and composed of 15-digits. It is a mandatory requirement that the IMSI number is recorded into a data file that cannot be used for any other data other than the IMSI number. For this purpose it has a prescribed electronic address 7F20:6F07 for Vodafone and mm02 and 7F21:6F07 for Orange and T-Mobile.
- When a GSM mobile telephone makes a call the mobile network uses the subscriber's IMSI directing call traffic and for charging purposes. It does not use the mobile telephone number for outbound/inbound calls from/to a mobile telephone and the mobile telephone number is not transmitted by the mobile telephone to the mobile network.

What is a SIM Card?

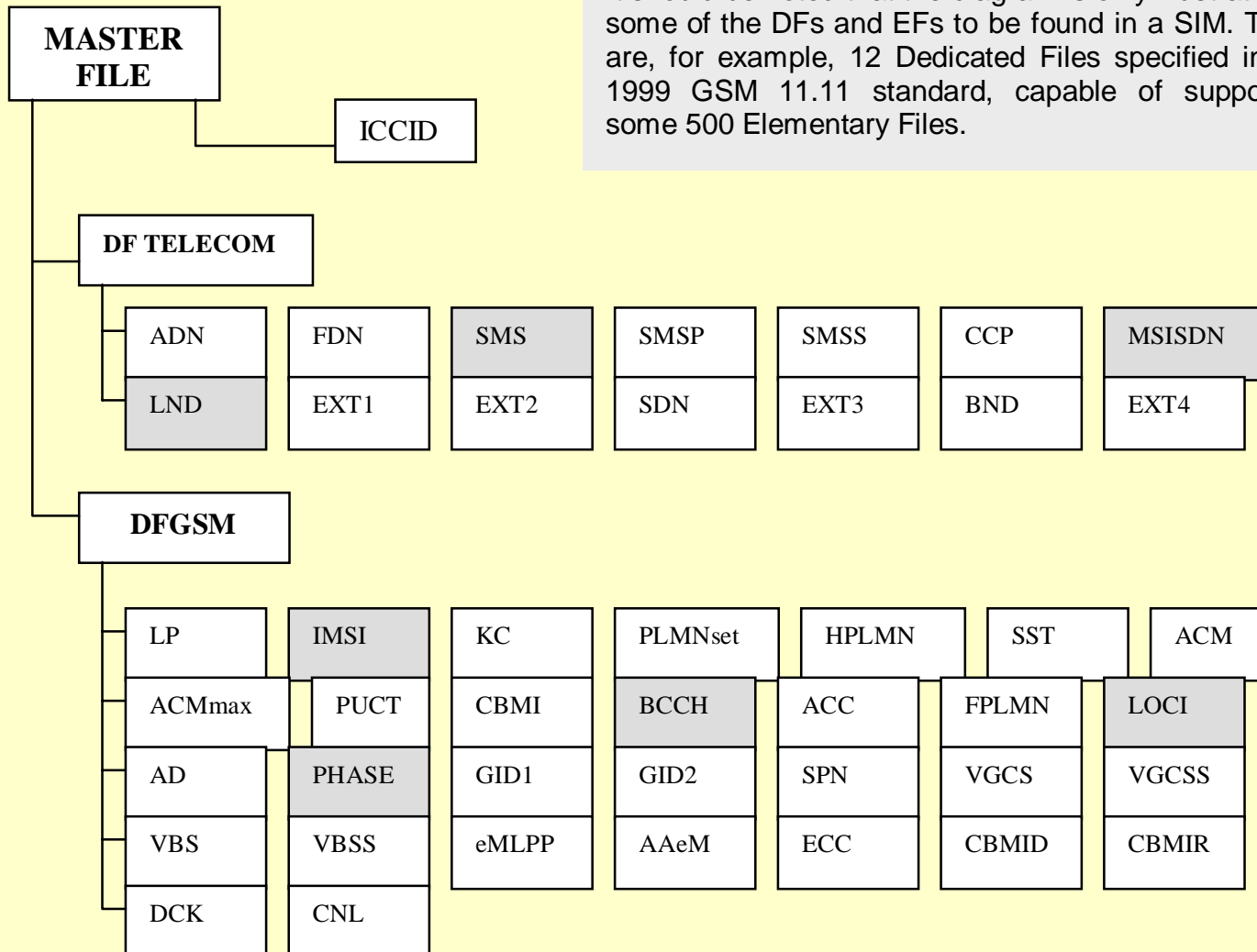
SIM – Serial Numbers

Mobile Telephone Number

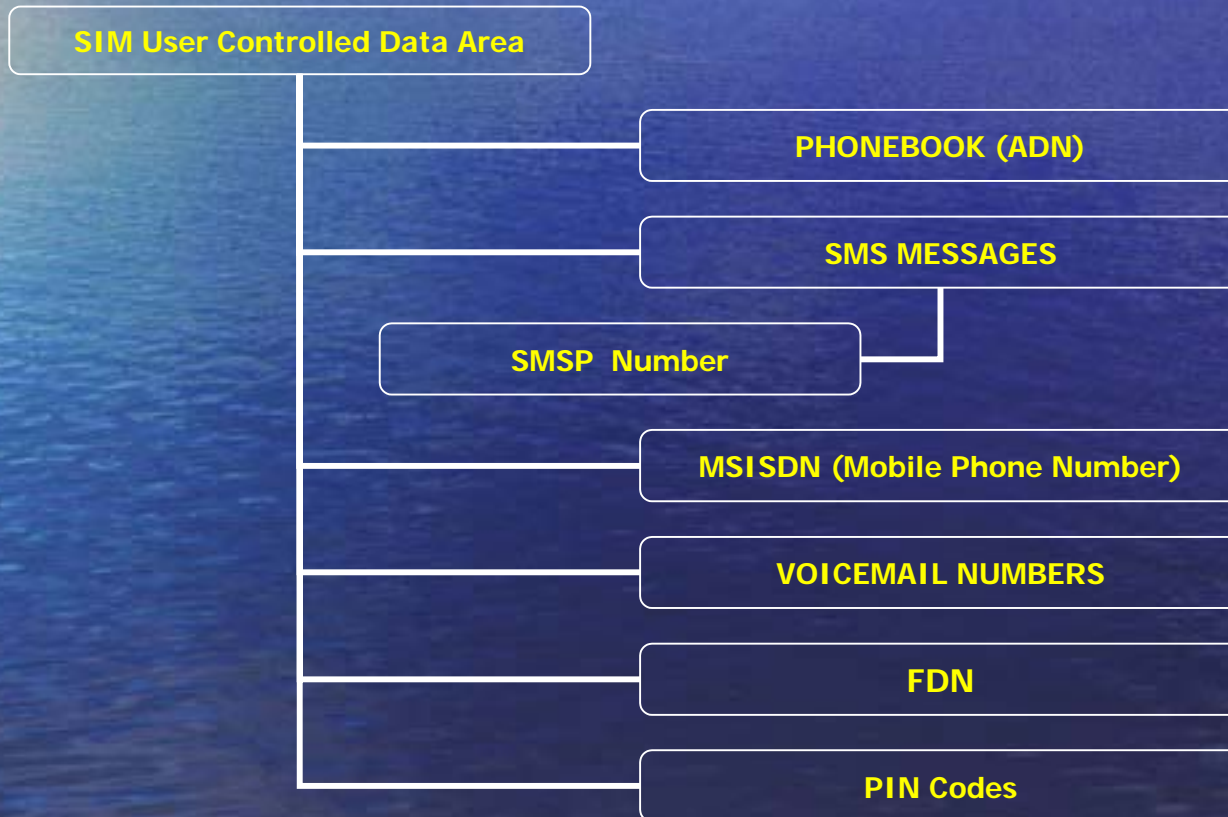
- The MSISDN is the technical term given for the directory *mobile telephone number* we commonly dial on the keypad. The MSISDN can be composed of up to 20-digits but generally 10-digits to 12-digits in length have been adopted for UK mobile telephone numbers. The number follows a numbering plan that has been agreed internationally, called the E164 telecommunications numbering scheme. The account holder's mobile telephone can be stored in a data file in the SIM's memory, but this is not a mandatory requirement. When this optional data is allocated and activated in the SIM card's memory it has a prescribed electronic address 7F10:6F40.
- It is possible for a user to view, edit and/or erase the mobile telephone number in this file. This means a user can input someone else's mobile telephone number. It does not automatically follow that a mobile telephone number that appears in this file is the 'phone number actually making the calls. Remember that the mobile network uses the IMSI number for routing calls from or to the handset. The reason why users do not use the IMSI for dialling is that the numbering structure would not be recognised by any other telecommunications network or system, hence why the E164 telecommunications numbering scheme is in place.

What is a SIM Card?

It should be noted that the diagram is only illustrative of some of the DFs and EFs to be found in a SIM. There are, for example, 12 Dedicated Files specified in the 1999 GSM 11.11 standard, capable of supporting some 500 Elementary Files.



Data Stored on SIM Cards



Data Stored on SIM Cards

SIM Service Provider Controlled Data Area

SIM Information (ICCID/SSN, IMSI, PLMN)

Network List

Info/Interactive Services

LND

SDN

PIN/PUK Code

What is a Mobile Phone?

- Digital wireless communication device
- Make/Receive voice calls
- Send/Receive text & multimedia messages
- Organiser functionality
- Music Player
- Games Console
- Digital Still photography
- Digital Video player/recorder



What is a Mobile Phone?

Mobile Telephones (Wireless devices)

- A mobile telephone first and foremost is a digital wireless data device in its own right. It has been suggested a mobile telephone is first and foremost a computer, which is misleading, not only from the point it usurps the laws of physics, but legally as well. Mobile telephones are recognised in European Directives (Telecommunications Terminal Equipment Directive 91/263/EEC, particularly the provisions of Article 4, and the Radio and Telecommunications Terminal Equipment (RTTE) Directive 99/5/EC). The provisions of European Directives applied for recognition of the technology, harmonisation and removal of trade barriers and other requirements. National laws (Communications Act 2003, Telecommunications Act 1984 (parts of which have been repealed) and the Wireless Telegraphy Act 1949 provisions are applied to this technology. There are applicable Statutory Instruments as well. National laws are applied to protect sovereignty over the spectrum, permission and purpose of use (the opposite being hijack of the airwaves), protection against interference, law interception and so on.



What is a Mobile Phone?

Mobile Telephones (Wireless devices)

- Behind, but supporting the aerial and radio circuitry, a mobile telephone has computer architecture in order to action commands and receive response from the radio network and devices connected to it. It also has a memory for the retention of user content. The purchaser owns the handset and there are various makes and models of handset available.



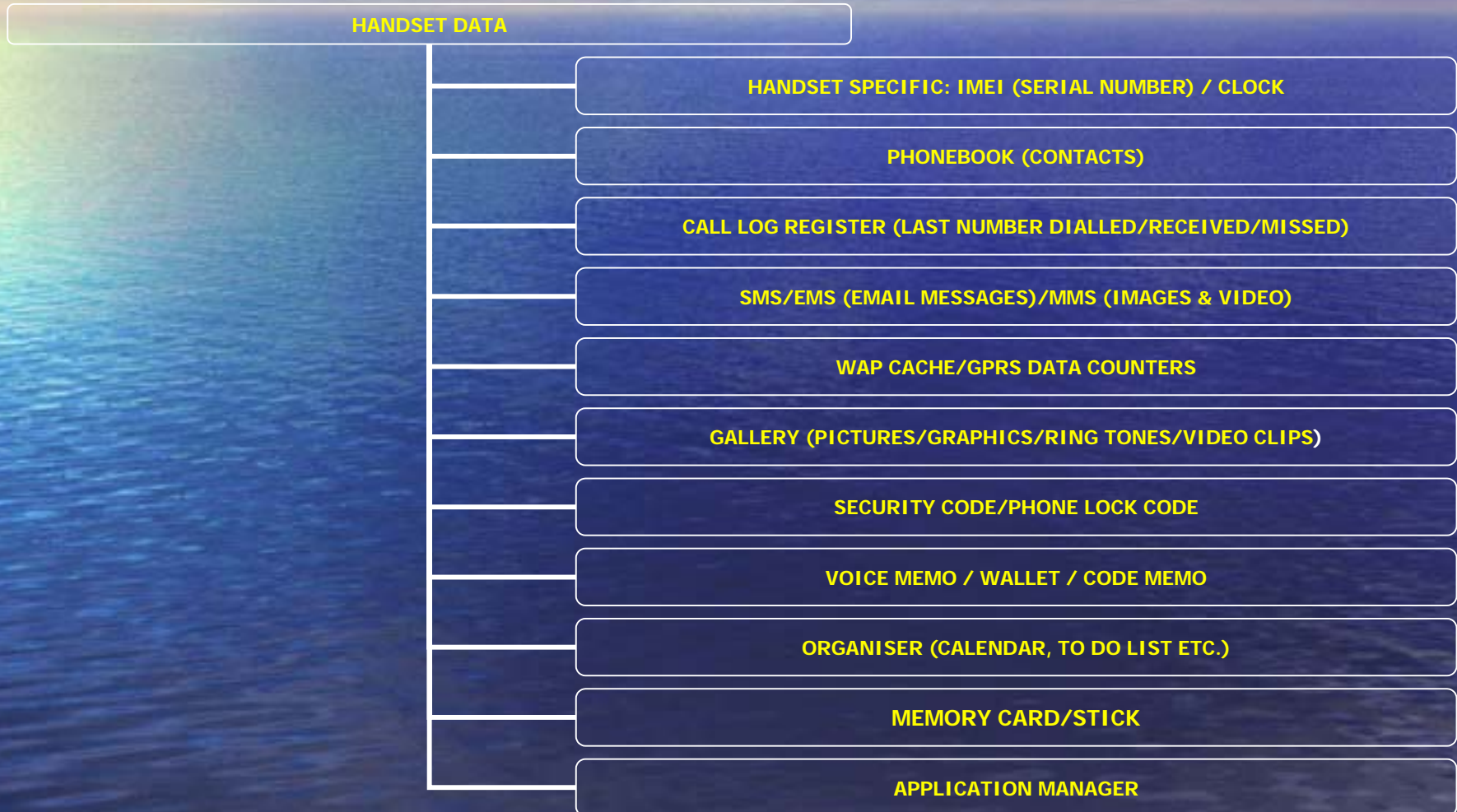
What is a Mobile Phone?

Mobile Telephone - Serial Number

- All mobile telephones at the time of manufacture are allocated a unique serial number defined as the International Mobile Equipment Identification (IMEI) number and are required to be registered with a regulatory body before the mobile telephone is supplied into the marketplace.
- The IMEI number, recorded in the handset, is composed of 15-digits and the structure of the number must comply with the mandatory standards. It is a requirement of the manufacturer to ensure the IMEI should not be altered or erased after manufacture. Each mobile telephone transmits, upon request, its IMEI number to the mobile radio network.



Data Stored on Handsets



Forensic Data Retrieval Out Side the Box

- Imaging or bit-nibble copy
- Deleted SIM data
- Deleted Handset Data
- Analysing electronic file (hex dump)
- Difficulties



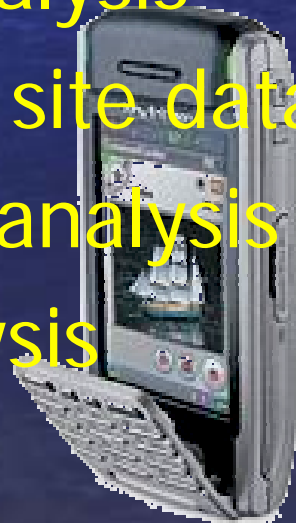
Comparative a flawed approach produces flawed results

- Interpreting Mobile Telephone Data
- Obtaining call records
- Call record analysis
- Obtaining cell site data
- Cell Site data analysis
- Cell Site Analysis



Holistically a flawed approach can result in a dismal of the evidence in aggregate

- Interpreting Mobile Telephone Data
- Obtaining call records
- Call record analysis
- Obtaining cell site data
- Cell Site data analysis
- Cell Site Analysis



End Of Part 2

Thank you

Any questions?



MTEB
Mobile Telephone Examination Board