

# TrewMTE Starter Kit MFW08

## Mobile Telephone Evidence

Overview GSM, Directives, Legal, Standards  
Presenter - Gregory Smith TrewMTE

Trew & Co (TrewMTE)  
Tel: 00442084608034  
Web: <http://trewmte.blogspot.com>  
Email: [trewCO@compuserve.com](mailto:trewCO@compuserve.com)



# TREW MTE

Mobile Telephone Evidence  
Training

**MTEB**  
Mobile Telephone Examination Board

# Presenter - Gregory Smith

- Principal of Trew & Co - consulting forensic engineers & Chief Training Officer Trew MTE
- Trew & Co operates Trew MTE (Mobile Telephone Evidence) and Mobile Telephone Examination Board (MTEB)
- 20yrs experience of telecom evidence. 18yrs of which handling wireless evidence. 14yrs of which dealing with GSM evidence (thus in at the start of GSM in UK)
- Trains law enforcement and security specialists in mobile telephone examination and evidence
- Independent expert engaged by both prosecution and defence but not on retainer by any party

# Overview of GSM Expert Qualifications

- There are no academic qualifications for mobile telephone evidence, thus reliant upon:
- Knowledge of all the current and historical technology not merely parts of it
- Skill - knowing what to look for and its application to a case
- Experience (the longer the better) as different development generations of GSM technology can be served in evidence

# Overview of GSM Expert Qualifications

- Mobile Telephone Evidence Diploma (MTEdip) by 2008/2009
- Support from law enforcement
- Support from education
- Support from industry
- Mobile 'Phone training courses undertaken will act as credits to Diploma

# Mobile Telephone History

## PIONEERS

- 1868 – James Clerk Maxwell postulates EM wave phenomenon “ethereal wind” theory
- 1886 – Heinrich Rudolf Hertz establishes proof of EM wave (Hertz cycle)
- 1893 - Guglielmo Marconi first use of wireless and first patent of wireless communications
- 1905 – Reginald Fessenden first transmission of speech and music via a wireless link

# Mobile Telephone History

## Founding Forefather

- 1908 – Nathan B. Stubblefield invented the first mobile 'phone a 100-years ago



<http://www.sundaymirror.co.uk/news/sunday/2008/05/04/world-s-first-mobile-invented-100-years-ago-98487-20404740/>

# Mobile Telephone History

## PIONEERS

- 1921 – 1970 was known as the pre-cellular era
- 1980 – Popular analogue cellular era for the world general
- 1990 – Introduction of digital cellular era

# Mobile Telephone Market

- 70-million subscribers in UK – 2007 beyond population saturation
- Estimated nearing 200 million handsets/SIM cards in UK (approx 3 per person) with intro of £5.00 handsets/SIM purchase (inclusive SIM credit 2008)
- 55,000 Masts in UK - 2007 (could be higher if small masts and indoor coverage added)
- Migration to household base stations and mini-masts with introduction of femtocells – estimates are 2-4 million households with femtocells by 2012

# GSM Mobile Telephone Market

- GSM started 1991 (Phase 1 technology rollout) - basic content service - voice, text messages, fax and services call forwarding/barring
- Phase 2 technology introduced 1995 offering enhanced voice capability and new services - Caller Identification (CLI), call waiting & holding and call conferences
- Phase 2+ is in fact a series of Releases (R96, R97, R98, R99 etc) that introduce new and improved network capability and services for use by SIM cards & handsets. Such as localised news, downloads, images, enhanced text messages etc

# GSM Mobile Telephone Market

- Four UK mainland operators - Vodafone, mmO2 (BT Cellnet), Orange & T-Mobile (One-2-One)
- numerous service providers - Carphone Warehouse, Phones4U, The Link etc
- Increasing number of Virtual Mobile Operators (VMOs) - Virgin Mobile, Tesco, Sainsbury's, easyMobile, BT, etc

# GSM Mobile Telephone Market

Two types of subscriber

- Monthly Account holder who receives a monthly bill - thus account holder is traceable
- Prepaid Account holder - no requirement to provide identity of user, account user does not receive a monthly bill but adds credit to account as and when

# Impact of GSM Mobile Evidence in Criminal Cases

- From 1993 to 1996 approx 30-100 cases per year
- 1997 to 2000 200-300 cases per year
- 2000 to 2008 tens of hundreds of cases per year
- Research Nexis/Lexis Law Database, Times Law Reports, Bailii and Internet etc

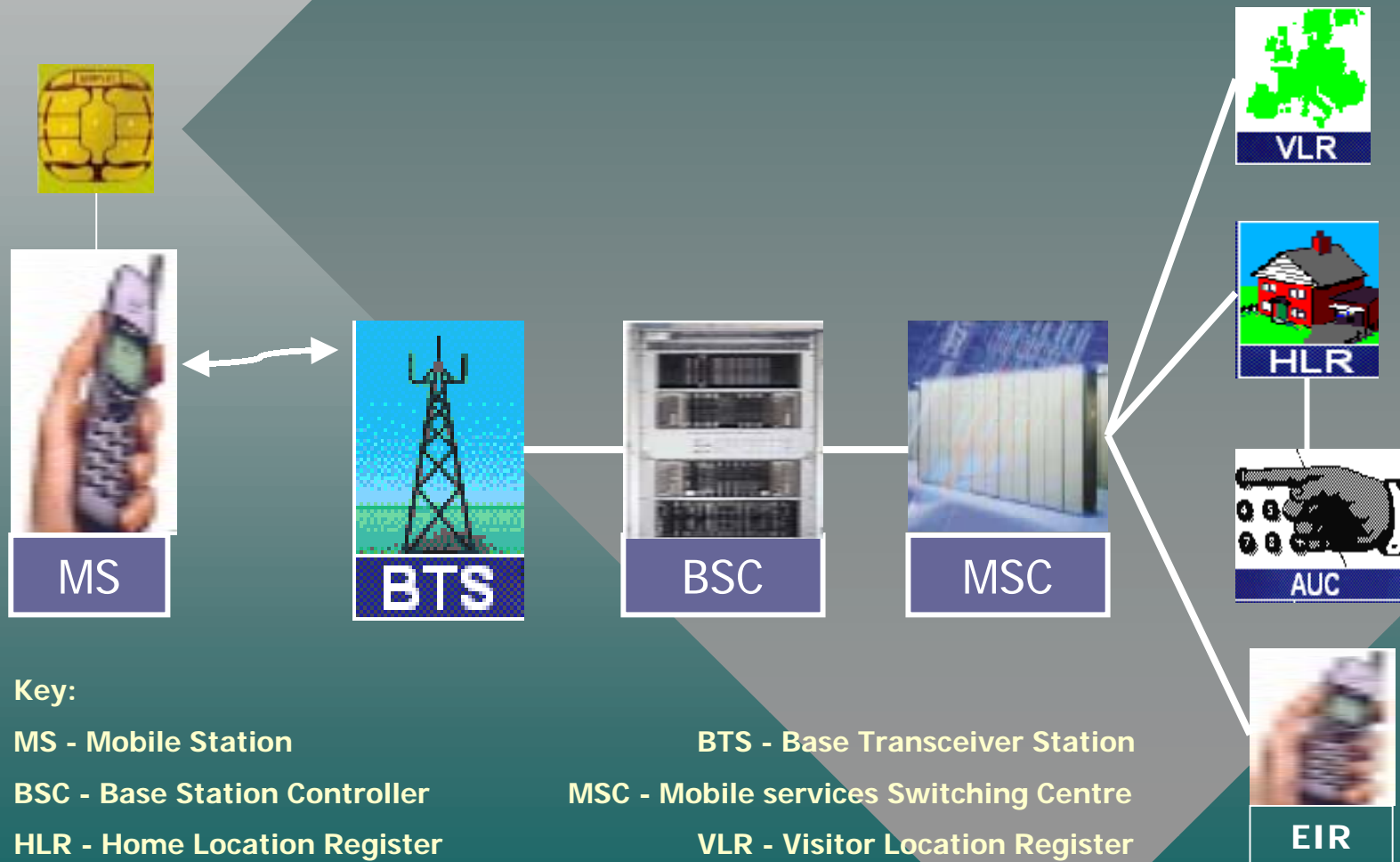
Mobile Telephone Evidence

# Overview of Global Systems for Mobile (GSM) Communications

# Pro's and Con's of Mobile Telephone Evidence

## Network Structure

# Global System for Mobile (GSM) Communication System Component Parts



## Key:

MS - Mobile Station

BSC - Base Station Controller

HLR - Home Location Register

AUC - Authentication Centre

BTS - Base Transceiver Station

MSC - Mobile services Switching Centre

VLR - Visitor Location Register

EIR - Equipment Identity Register

# Mobile Telephone Evidence

- A **SIM card** is required to validate the subscriber to the network and authenticate the user so as to allow calls to be made or received, but the SIM can do no more without a mobile telephone
- A **Mobile Telephone** has a power supply, keys for dialling 'phone numbers and the radio circuitry in order that the SIM and handset can communicate to the mobile network
- When operating together the SIM card and mobile telephone are known as a **Mobile Station (MS)**

# Mobile Telephone Evidence

- A **Mobile Station (MS)** talks to a **Base Transceiver Station (BTS)**, the mast so to speak, when it is within range of it. Radio coverage propagated from the mast can be omni-directional (360 degrees) or sector directed (degrees). To determine the radio coverage area requires **best server plots/density maps** and **single cell predication maps** to comprehend the RF footprint of the coverage from the mast
- There maybe many masts in a particular geographical area and all will be controlled by an allocated **Base Station Controller (BSC)**

# Mobile Telephone Evidence

- A **Base Station Controller (BSC)** can be considered a commander of an army (of masts) under its control to assist mobiles handover between masts in an area. BSC also acts as the conduit for the mobile station to talk with the mobile telephone exchange known as the **Mobile services Switching Centre (MSC)**. The MSC confers with the **Home Location Register (HLR)** to validate the subscriber and the HLR obtains authentication from the **Authentication Centre (AuC)** to allow calls. The MSC equally confers with the **Equipment Identity Register (EIR)** to ensure handset is not barred. All confirmations (hlr/auc/eir) are deposited in the **Visitor Location Register (VLR)** to enable the MS to make/receive calls

# Understanding GSM Development

This presentation has been created to enable law enforcement understand the importance of GSM Standards, and their interaction with European and domestic law. the Standards provide the technical know-how and technical explanation for processes, functions, memory and data relating to GSM that can be used in evidence. It is recommended law enforcement personnel following attendance on a Trew MTE training course make time to obtain, read and comprehend the various GSM standards.

Mobile Telephone Evidence

# Directives, Legislation & Standards

The Directives needed to ratify the accord between Member States, harmonise the legal principles and distinguish standards in order to be subsumed into existing or new domestic law.

# Directives, Legislation & Standards

## European Directives - "*Essential Requirements*"

- 91/263/EEC Telecommunications Terminal Equipment (TTE) Directive (relates to GSM 900MHz)
- 98/575/EC Common technical regulation for the general attachment requirements for mobile stations intended to be used with Phase II public digital cellular telecommunications networks operating in the GSM 1800 band
- 99/5/EC Radio & Telecommunications Terminal Equipment (R&TTE) Directive (relates to GSM & 3G)
- plus other directives

# Directives, Legislation & Standards

Then came

- Common Technical Regulations (CTR)
- Technical Basis for Regulation (TBR)
- ETSI Technical Standards (TS) &
- GSM Standards
- Objective - to meet the "*Essential Requirements*" emphatically stated by the Directives

# Directives, Legislation & Standards

UK Domestic Law directly/indirectly relevant to mobile telephony and evidence:

- Wireless Telegraphy Act 1949
- Wireless Telegraphy Act (amended)
- The Telecommunications Act 1984
- The Communications Act 2003
- Data Protection Act 1984 and 1998
- Mobile Telephone (Re-Programming) Act 2002
- Regulation of Investigatory Powers Act 2000

# Mobile Telephone Evidence GSM Standards

In order to determine that the “essential requirements” can be met through compliance with standards : ETSI - uses the word “shall” meaning “mandatory”

As the academic author William Webb stated in his book 'The Complete Wireless Communications Professional' at pages 306 and 307 when discussing GSM Standards :

- *' If the text is to form part of the final standard, it must be completely clear and unambiguous. For example, in English the words should, might, may, and could are all ambiguous - it is not clear whether a particular action is required or not required. ETSI guidelines mandate the use of the word shall to indicate a particular action must be performed.'*
- *When you read the word “shall” in a standard it is analogous to reading the word “shall” within a Statute, suggesting an affirmative duty emphatically stated by the Act.*

# Mobile Telephone Evidence GSM Standards

So how do “mandatory” requirements work.

- 1) Where technical **implementation** and **outcome** are *mandatory* (e.g. ICCID / IMSI)
- 2) Where technical implementation is *mandatory* but the outcome is *optional* (e.g. HPLMN)
- 3) Where technical implementation is *optional* but the outcome is *mandatory* if implemented (e.g SMS text messages)
- 4) Where technical implementation is *optional* but the outcome is *optional* if implemented (Cust Files: IMEI)

# Mobile Telephone Evidence

## GSM Standards

### SIM Card Standards

- GSM 11.11 (Foundation standard 5V), GSM 11.12 (3-Volt), GSM 11.18 (1.8-Volt)
- GSM 11.13 (Java)
- GSM 11.14 (SIM Application Toolkits)
- GSM 11.17 (Conformance Tests)
- GSM 09.91 (Backward compatibility)
- GSM 03.03 (Numbering, addressing)

### Fundamental standards that underpin GSM11:11

- ITU TE.118 (Numbering plan - ICCID)
- ITU TE.164 (Numbering plan – MSISDN)
- ITU TE.212 (Numbering plan - IMSI)
- ITU TE.214 (Numbering plan - MSRN)

# Mobile Telephone Evidence

## GSM Standards

### Mobile Telephone Handset Standards

- GSM 11.10 (Radio standard)
- GSM 09.90 (Backward compatibility)
- GSM 03.03 (Numbering, addressing)
- GSM 02.30 (MMI for PIN \*#06#)
- GSM 02.11 (Network Access & 999 etc)
- GSM 02.16 (IMEI)
- GSM 02.07 (MS features)
- GSM 02.06 (MS types)
- etc

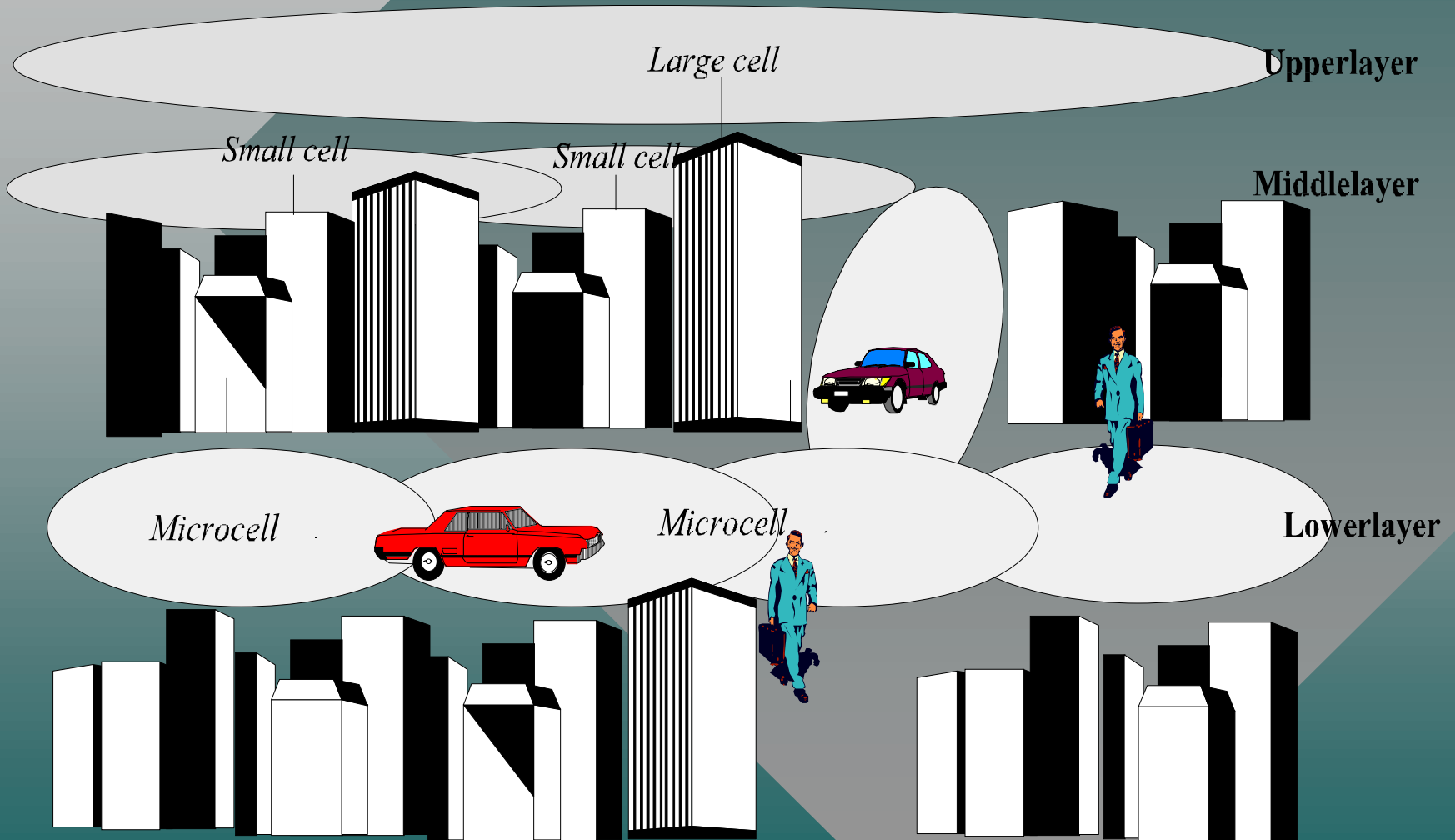
# Mobile Telephone Evidence

## GSM Standards

### Mobile Radio Network Standards

- GSM 03.22 (Network Architecture)
- GSM 04.08 (Radio Testing)
- GSM 05.05 (Transmission & Reception)
- GSM 05.08 (Radio Subsystem Link TA, Power Control)
- GSM 05.22 (Cell layers & Dwell Time)
- GSM 05.50 (Background to RF Requirements)
- GSM 08.51 (General BSC-BTS)
- ITU-R P.1546 (Point-to-area terrestrial predictions)

# Cell Layers & Dwell Time



Copyright GSM Association: France Telecom/CNET

# End of Part 1

Part 2 looks at comparative and holistic approach to mobile telephone evidence.

**For now any questions?**