

Mobile Telephone Evidence

Mobile Telephones, SIM Cards and Cell Site Analysis Forensic Investigation and Evidential Analysis

SWITCH ON ~ UPDATE = LOSE EVIDENCE

Location Information

LOCI

TMSI

CA560938

LAI

02F21001F9

TMSI Time

28

Location Update Status

00

TMSI : CA560938

LAI:

MCC: 202 Greece

MNC: 01 Cosmote

: LAC: 01F9

TMSI Time : 28

Location Update Status: Updated

BCCH Information

99F402FDC27FFE040C0000000000000

A primary objective of dealing with mobile telephone evidence is the avoidance, as best possible, of contaminating or destroying of data arising from an applied examination methodology. The objectives are to ensure authentication, original and genuineness. A factor that is equally important is preventing or minimising losses of automated data in order to speed up investigation enquiries that can be relevant to terrorism, kidnap and robbery to conspiracies etc; this list is endless. When referring to automated data, this is meant in terms where data is generated that is not created due to human intervention i.e. setting the handset CLOCK, which is largely erroneous at the best of times and on the scale of evidence is the least significant bit of information. **Why is it important then to ensure correct examination methodology, and, how can using automated data assist speed up investigation?** Reported by Greg Smith

EXAMINATION METHODOLOGY

Experience has taught over the 13 years of examining GSM mobile telephones that it is important to:

- 1) Examine the SIM card first,
- 2) then, obtain the handset IMEI
- 3) and, finally, examine the Mobile Station

Apart from the issues associated with originality and genuineness of the evidence that may be served in evidence, it is **known** by switching ON the handset first, with the SIM card inserted (combined they are called a *mobile station* or MS), will materially alter data on a SIM card. The key questions are what data is altered and how important is that lost data? For this issue of Mobile Telephone Evidence Newsletter the examples of how data are updated in the *EFLOCI* and *EFBCCH files* when an examiner switches ON the *mobile station* (MS) are considered.

When an MS is switched ON it routinely scans the radio environment to determine the radio coverage that is around it. The MS will equally search data in the *EFLOCI* and *EFBCCH files* in the SIM card to assist, or compare radio coverage areas, so that the MS can camp on the mobile network. Should the data in the *EFLOCI* and *EFBCCH files* be the same as the data transmitted in the radio coverage area in which the MS is located then the *EFLOCI* and *EFBCCH files* will still be refreshed and updated with new coverage data in those *files*. Of course, as the MS moves around updating continues and the last radio coverage area in which the MS was located is recorded in those *files* when the MS is switched OFF. Looking at the case of trafficking suspect. By removing the SIM card from the handset and extracting and harvesting the data from will not alter the data in the SIM. Following data recovery the last network and radio coverage area are known.

Mobile Telephone Evidence

PAGE-2

SWITCH ON ~ UPDATE = LOSE EVIDENCE

Wouldn't that information be important in a trafficking suspect case? Well, the last network used does identify whether the SIM was last used in the subscriber's home network or abroad (roaming). The radio coverage area is also known to indicate a location area, which the MS had been in when last switched ON.

The suspect has just got off a plane and detained at the airport. Does the investigator or examiner switch ON the MS? One might think that as the plane came in from Italy the last network used by the MS was Italy. The experienced examiner may think, 'what if the suspect is bluffing?' Say the MS was in Greece, but carried on a flight to Italy and the user hasn't used the mobile since leaving Greece (for example, to maintain radio silence). Switching ON the MS at the UK airport means updating (see Figure 2) the *EFLOCI* and *EFBCCH files*, thus losing evidence (see Figure 1). For the record, do not be fooled into thinking radio-dampening fields will combat this problem, for they do not. MSs used in radio dampening fields cause the data to be nulled in the *EFLOCI file* as it is updated with the Mobile Country Code (MCC) and Mobile Network Code (MNC) with the home network details. The Location Area Code (LAC) is lost along with Temporary Mobile Subscriber Identity (TMSI), which is itself location based, and any TMSI time (if relevant). The *EFBCCH file* cannot detect the channels identified in the Broadcast Control Channel (BCCH) of the radio coverage and therefore the previous BCCH data are overwritten with FFFFFFFF.

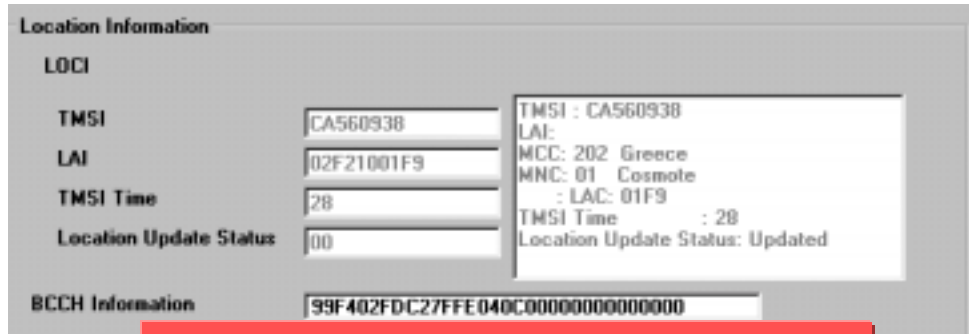


Figure 1 - Before EFLOCI & EFBCCH FILES updated

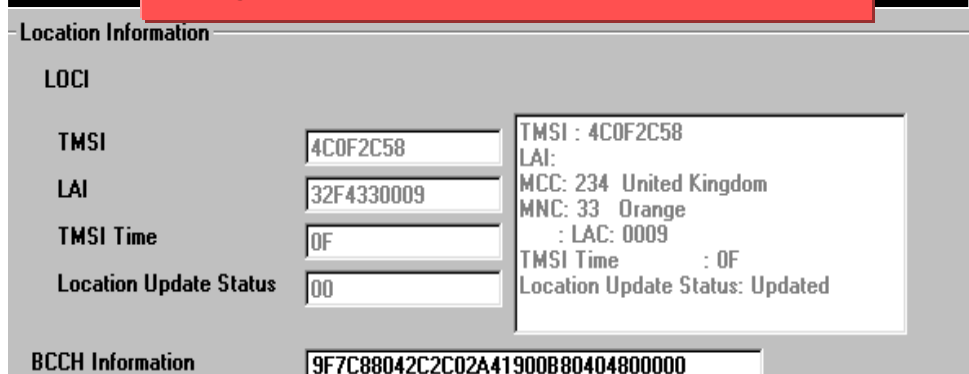


Figure 2 - Updated EFLOCI & EFBCCH FILES

FIGURE 1

The top Location Information identified in the extracted and harvested data displays that the SIM was last used on the Cosmote GR mobile network in Greece. The Location Area Code is in fact for the island of Kefalonia and covers the region of the Island called Argostoli. The investigator/examiner will note that a TMSI has been allocated for the geographical area in which the MS was last operative, confirming ciphering of communications might be active on the radio network. Interestingly, there is a TMSI Time as well indicating the period within which the MS must perform periodic location update. Working with the above harvested data, it won't be immediately known that Argostoli Kefalonia is the relevant area, but the fact that it is known that the mobile network operator Cosmote and Greece are known, some factors can be worked out. It takes about 3/4 hours flight time between Greece and e.g. Gatwick. Data in Visitor Locator Registers (VLR) and Base Station Subsystem (BSS) can be held between 1 day to 7 days. With possible stop over by suspect in Italy, could be less than 7 days, there is a chance to retrieve location data from the network regarding location

movements of the MS. Could be vital information which is lost instantly by merely examining the MS first rather than SIM.

FIGURE 2

The screen image demonstrates data that has been updated in the *EFLOCI* and *EFBCCH files* following the MS being switched ON first, indicating the consequences of not examining the SIM card first.

The data that has been updated is automated data and original information was lost not because of the MS user or the mobile network operator, but as a direct consequence of the applied examination methodology used to extract and harvest the data. By examining the MS first has caused seven GSM information elements (IEs) in two element files (EFs) to be altered (thus corrupted) by the examiner:

- TMSI
- MCC
- MNC
- LAC
- TMSI TIME
- Location Update
- BCCH information

Mobile Telephone Evidence

PAGE-3

SWITCH ON ~ UPDATE = LOSE EVIDENCE

7F20:6F7E (Location Information)	7F20:6F7E (Location Information)
Response: 00 00 00 0B 6F 7E 04 00 11 F0 1F 01 02 00 00	Response: 00 00 00 0B 6F 7E 04 00 11 F0 1F 01 02 00 00
File ID :6F7E	File ID :6F7E
Type of file :EF	Type of file :EF
Structure of file :Transparent	Structure of file :Transparent
File Size :000B	File Size :000B
Read Access :CHV (PIN) 1	Read Access :CHV (PIN) 1
Write Access :CHV (PIN) 1	Write Access :CHV (PIN) 1
Increase Access :CHV (PIN) 0	Increase Access :CHV (PIN) 0
Rehabilitate :CHV (PIN) 1	Rehabilitate :CHV (PIN) 1
Invalidate Access :CHV (PIN) 15	Invalidate Access :CHV (PIN) 15
File Status :Not Invalidated	File Status :Not Invalidated
CA 56 09 38 02 F2 10 01 F9 28 00	4C 0F 2C 58 32 F4 33 00 09 0F 00
TMSI : CA560938	TMSI : 4C0F2C58
LAI : MCC: 202 Greece	LAI : MCC: 234 United Kingdom
MNC: 01 Cosmote	MNC: 33 Orange
LAC: 01F9	LAC: 0009
TMSI Time : 28	TMSI Time : 0F
Location Update Status: Updated	Location Update Status: Updated

Figure 3 - Changes to EFLOCI File where MS examined first

The data in EFLOCI file 7F20:6F7E is also repeated at 7F21:6F7E, which means that this elementary file would also be updated during examination, thereby losing even more evidence due to an examination methodology of examining the MS first. It is important to recognise that the EFLOCI file is a mandatory file that cannot be accessed by the MS user, thus falls under the provisions of automated data.

7F20:6F74 (Broadcast Control Channels)	7F20:6F74 (Broadcast Control Channels)
Response: 00 00 00 10 6F 74 04 00 11 F0 FF 05 02 00 00	Response: 00 00 00 10 6F 74 04 00 11 F0 FF 05 02 00 00
File ID :6F74	File ID :6F74
Type of file :EF	Type of file :EF
Structure of file :Transparent	Structure of file :Transparent
File Size :0010	File Size :0010
Read Access :CHV (PIN) 1	Read Access :CHV (PIN) 1
Write Access :CHV (PIN) 1	Write Access :CHV (PIN) 1
Increase Access :CHV (PIN) 0	Increase Access :CHV (PIN) 0
Rehabilitate :CHV (PIN) 15	Rehabilitate :CHV (PIN) 15
Invalidate Access :CHV (PIN) 15	Invalidate Access :CHV (PIN) 15
File Status :Not Invalidated	File Status :Not Invalidated
99 F4 02 FD C2 7F FE 04 0C 00 00 00 00 00 00	9F 7C 88 04 2C 2C 02 A4 19 00 B8 04 04 80 00 00

Figure 4 - Changes to EFBCCH File where MS examined first

The data in EFBCCH file 7F20:6F74 is also repeated at 7F21:6F74, which means that this elementary file would also be updated during examination, thereby losing even more evidence due to an examination methodology of examining the MS first. It is important to recognise that the EFBCCH file is a mandatory file that cannot be accessed by the MS user, thus falls under the provisions of automated data.

Mobile Telephone Evidence

PAGE-4

SWITCH ON ~ UPDATE = LOSE EVIDENCE

The discussion in this article has made reference to automated data. The relevance of this is as indicated early, that it is generated by the mobile network and not by human input. Because this is the case, it has important legal implications as well. As Dr Indira Carr, Law Lecture at University of Exeter points out (when referring to Collier, PA and Spaul BJ on Forensic Methodology for automated recordings); "information recorded...by machine...is no more hearsay than a film or an audio tape of an incident." The law treats automated data as 'real' evidence as it does not suffer from "the supposed unreliability of information from or transmitted through human sources." This includes information input by human sources. Therefore the securing and examination of a device that produces 'real' evidence should be treated so as to avoid loss. The methodology applied to examining a device must equally be shown to be reliable so that the device in its examination (extraction and harvesting of data) from the target device can be compared to the original data in a device to show they are identical (*R .v. Wood*). Indeed, were the data in a device had been altered its admissibility (because of contamination) might move under the hearsay rule because of the shift of emphasis to it being potentially unreliable information. It would need to be shown that the altered data, thus altered state of the original device, has not been contaminated elsewhere. Also, that it was not wilfully intended to lose data (*Cox v Riley*; *R .v. Whitely*). Best practice, meant in terms of what should be avoided as opposed to what should be done, regarding mobile telephone examination is essential if mobile telephone evidence is to be seen as safe to rely in Court. MTE Newsletter has referred to this in numerous, previous editions. Using the *EFLOCI* and *EFBCCH files* as the examples, what a Court may need to know is not that the Location Information and Broadcast information defines details about radio coverage area and radio channels in that coverage, but rather the fact of it. Readers may think this is analogous to the commentary by Professor Smith [1983] Crim LR 472 regarding bank statements. Had a bank clerk accessed the bank account of a customer and used a method known to cause full or partial deletion of data, would that be an acceptable process?

How can a methodology be effective if there is no clear statement that emphasises the fact that a particular matter can no longer be established from the device whose data has altered due to an applied examination procedure? This is viewed in context not only with which device is examined first, but also the external machine used to extract and harvest data, and whether the machinery imposes, due to the limitations in its own capability, that the data from the original device should fit with how the machinery functions, as opposed to the machinery functioning to the capability of the device under examination. Headway has been made in relation to this last point as current practice tends to follow the policy that using examination machinery best suited to the device under test is desirable. It may even be fair to suggest that some of the examination machines in use

today might meet the **Daubert Test**, were that Test to be a required standard for all devices. However, the first point about examination methodology has still not been satisfactory resolved, this largely appears so as the methods used to examine mobile telephones appears to be applied subjectively. This is not to suggest a wilful (*my way is best*) approach by some to examiners of mobile telephones, it is occurring due to conflicting advice. That conflicting advice arises because someone thought that the handset CLOCK was more important than automated data stored on a SIM card being altered arising from an applied examination methodology. The CLOCK argument has never really established significant results because the CLOCK set by the user (not automated) is inherently unreliable. This comment is not intended to dismiss the handset CLOCK as entirely irrelevant, but on the scale of high to low evidence it is in the lower quadrant when it comes to deciding which device should be examined first - SIM or MS. Indeed, in the last several years, handsets have included in their electronic circuitry an onboard battery. When the external battery is removed, the CLOCK is not lost as the onboard battery maintains the last data for quite sometime. There is a sufficient time period in which to examine the SIM, obtain the handset serial number, re-insert the SIM, and reconnect the battery in order to examine the MS, without losing original data at first instance on the SIM.

A further argument has been made about **PIN/Password**. Here again this appears to be subject to a subjective approach. PIN/Password may not be relevant:

- if the MS is seized whilst it is switched ON. Leaving it switched ON and sticking the MS in a faraday bag wont prevent data being altered on the SIM because the MS, whilst in the bag, will be blocked in its attempt to update to the radio network, thus will alter data on the SIM in the *EFLOCI* and *EFBCCH files*.
- If it were possible to galvanise an opinion from global practices, on the whole most tend to require the MS to be switched OFF at seizure in order to maintain as best possible the integrity of the original data at the time of seizure.
- And in fairness why should the seizing officer be expected to explain away at Court why *events* occurred, when it is the examiner's job to know how to cope with PIN/Password issues.

The art of mobile telephone examination is to perfect a suitable method for examination and by doing so to indicate an attempt at perfection in the processes applied. Losing automated data does not instil confidence of such a fact. Moreover, losing automated data whether it is Location Information or the header details of an SMS text message can severely hamper an investigation and slow it down.

SPEEDING UP INVESTIGATION

At the beginning of this article it posed the questions, 'Why is it important then to ensure correct examination methodology, and, how can using automated data assist speed up investigation?' One example of why correct examination methodology is important arises where the

Mobile Telephone Evidence

PAGE-5

SWITCH ON ~ UPDATE = LOSE EVIDENCE

mobile station (MS) is switched ON and updates data in the SIM card, losing potentially important evidence. What equally needs to be discussed is what the impact might be to slowing down or hampering an investigation.

The role of the examiner when defined in a nutshell is to receive evidence, extract and harvest the data, and hand back the output evidence. This may be a crude definition, but it's to the point. No where in that definition is there a long drawn out description that investigations will be held back because the examiner doesn't know how to handle a particular matter or will lose data because of applied examination methodology. That being the case, the investigator wants to process the important data the examiner has obtained. The speed at which that processing needs to be done depends upon the type and severity of the case. In this article the roaming argument has been used and it hinted at the type of case being relevant to trafficking, because it brings home the severity of a possible negligent approach in relation to losing evidence due to examination methodology. For instance, how on earth could the examiner possibly re-create the lost Location and BCCH information? Put simply, it is highly unlikely. The same is most likely to be true even if this had not been a roaming matter and the MS had moved around in different radio Location Areas in the UK. It makes sense therefore to discuss the roaming data in context with how it could have been used had the data not be lost.

On page 2, above, gave a brief interpretation of the data in the *EFLOCI* and *EFBCCH files* and it was shown that the data originated in Kefalonia Greece and that the local geographical area relevant to the radio Location Area was Argostoli. Argostoli is the main centre on Kefalonia because the airport is there and also small docks and harbour. When viewed in this light suddenly the data in the *EFLOCI* and *EFBCCH files* take on a new dimension an opens up possible lines of enquiry an Investigator might have been able to use, but for the data being lost.

What is equally as interesting about the Location Information is the use by the mobile network operator of TMSI Time. TMSI Time is the T3212 timer informed to the MS indicating the period within which the MS must perform periodic location update. This is interesting, as TMSI Time is an early GSM Phase 1 (pre-1995) requirement for mobile networks and MSs. It was removed when GSM Phase 2 was adopted (see GSM09:91/GSM11:11). The fact that data shown in the *EFLOCI file* was caused to be recorded using MS Phase 2+ (handset and SIM) should be a noteworthy. Neither device requires TMSI Time to operate in the mobile network. This indicates the Base Station (BS) is transmitting Phase 1 requirements. This could be due to perhaps a large number of the population still using Phase 1 MSs or that old BTSs are still being used in Kefalonia. If it is the latter issue, what an interesting forensic footprint, especially if it turns out to be that in Kefalonia, out of say 20 BTSs on the island, only 3 BTSs are Phase 1 - thus defines possible location where the broadcast data was relevant, particularly when coupling

the BCCH Information (GSM11:11), which "stores information received from the last serving cell about the channels used for the BCCH in the neighbouring cells" (Redl, Weber & Oliphant). Combining both sets of data (TMSI Time and BCCH) for this particular matter under discussion, along with Location Information, provides for some compelling evidence. But, alas, the TMSI Time evidence along with the BCCH Information has been overwritten also, thus lost, due to the applied examination methodology of examining the MS first.

Equally, when seeking calls records, having the data from the *EFLOCI file* assists the investigator refine the enquiries as to what data could be sought in the Call Records, such as cell site data - NGR, address, post, Site & Cell ID, coverage bearing, sector etc. Indeed, enquiries to the UK home operator could be run in parallel with enquiries to the Cosmote operator under Chapter 2 Section 7 of the Crime (International Co-operation) Act 2003 - mutual provision of evidence (in criminal matters). I could of course have referred to co-operation agreements between international law enforcement agencies (ICPO etc) but as a national mobile network operator (particularly located in EU) may not be bound by some conventions, without a court order, the judicial authority procedure has been referred by reference to the Act 2003. However, the loss of evidence has potentially hindered an investigation - at best by causing delays to getting results and worse removing vital clues as to possible location (where trafficked persons maybe being held).

OBSERVATIONS

The article has demonstrated that where a SIM is not examined first and an MS is switched ON the latter procedure causes data in files to be automatically updated. This leads to a loss of evidence, which is not only foreseeable, but quite unnecessary. The data that was lost was not generated as a consequence of human sources but automatically generated by the mobile radio network - which is considered 'real' evidence. Of course, this article is not definitive in that other data in the SIM are updated as well, but it would be simply too long an article to cover everything. Moreover, the article has looked at one aspect of GSM mobile 'phone SIM evidence and with 3G USIM the position is even more complicated.

Technical aspects on the effects of updating have been demonstrated when an MS has been switched ON, and how the loss of evidence might lead to hindering an investigation.

Reference to case law has been stated to enable readers to comprehend that there are legal principles in place. These cases have been selected from research conducted by the author of this article for his publication '*Admissibility of Computer evidence in Criminal Proceedings*', which was commissioned by Dr D Bainbridge of Aston University.

What may arise from this article is that it may assist the debate on policy regarding examining mobile telephone evidence. What is as, or even more, important is the standard of evidence and whether the appropriate disclosures are being made to the Criminal Courts.

Mobile Telephone Evidence

END PAGE

ABOUT THE EDITOR

Greg Smith has been involved with forensics and technology evidence for 18 years, of which 17 years with wireless evidence, and of which 13 years dealing with Global System for Mobile (GSM) communications evidence. The extent to which he has dealt with wireless evidence relates to the original analogue mobile telephone system in the UK called TACS (Total Access Communications System) launched 1985. This wireless system was phased out of use in the 1990s, although the last TACS wireless licence expired in 2005. The predominant evidence for TACS related to investigating stolen and cloning mobile telephone integrated mobile telephone number (MTN) and electronic serial number (ESN). It required examination of the handset and transmitted identity to the network; the examination of the printed circuit board for modification components or circuitry used to hijack the use of a genuine user's identity; to re-program stolen identity into a stolen mobile and jettison original identity. To examine usage of stolen TACS mobile 'phones in relation to Phonebook and mobile calls. To conduct cell site analysis based on the use of Masts by the stolen mobile 'phones and Masts radio coverage area. The last bulk of TACS mobile 'phone cases ended between 1997/98. This was largely due to the introduction of GSM in 1992 and the four fully operational GSM networks by 1994. His work with GSM assisted in the introduction into evidence of the first GSM radio footprint maps, called digital cell footprint maps identified as Best Server Plots and Single Cell Prediction Maps. His work with GSM began in 1993 with mobile telephone and SIM card examination, and GSM cell site analysis. In 1999 Greg created the first GSM accredited mobile telephone courses in the UK delivered in 2001 and in 2003 set about creating the first 3G USIM courses in the UK, which began in November 2005. Greg's main skillsets is that he not only conducts research and development but also presents evidence in criminal courts of law, thus combining both R&D & evidential experience skillsets necessary when dealing with criminal proceedings. It is not possible to have a grasp of mobile telephone evidence simply from R&D, one needs to present it as evidence as well in order to comprehend how the law of evidence will accept it. More info on Trew MTE courses: trewCO@compuserve.com

List of law enforcement (Police) agencies that have attended the Trew MTE courses.

British Transport Police	Nottingham Constabulary
City of London Police	Norfolk Constabulary
Cambridgeshire Police	Northampton Police
Dorset Police	Northern Constabulary
Dyfed Powys Police	Northumbria Police
Gloucester Constabulary	Royal Canadian Mounted Police
Guernsey Police	Royal Military Police RMP Provost
Hampshire	Scottish Drug Enforcement Agency
Hertfordshire Police	South Wales Police
H M Customs & Excise	South Yorkshire Police Authority
Humberside	Staffordshire Police
Kent Constabulary	Sussex Police
Lancashire Eastern Div HQ	Tayside Police
Lancashire Constabulary	Thames Valley Police
Leicestershire Constabulary	Waltham Forest Borough Police
Leyton Police	West Mercia Police Authority
Lincolnshire Police	West Midlands Police
Lothian and Borders Police	
Metropolitan Police	
Ministry of Defence Police	
Ministry of Justice Belgium	

Not included in the list are the specialist security depts/organisations who have also received training

Mobile Telephone Surveillance (MTE) Newsletter, for law enforcement and security specialists. MTS Newsletter was the first publication for law enforcement dealing with market issues relating to mobile 'phones, SIM cards, network data and cell site analysis. MTS Newsletter provides delegates who had been on TREW MTE training courses to receive additional support in the field. If you want to know about MTE Newsletters or other publications send an email to Greg Smith: trewCO@compuserve.com

