Unit 4: Mobile Network Investigations

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Mobile Network Technology
- Types of evidence
- How data may be acquired

1.2 INTRODUCTION

The use of mobile devices is increasing rapidly, with devices like the BlackBerry, iPhone, and G1 providing a wide variety of services, including communication (e.g., voice, SMS, e-mail), Internet access (web browsing), and satellite navigation (GPS). These technological advances

create new opportunities for criminals while providing valuable sources of evidence. The bombs in the 2004 train bombings in Madrid apparently used cellular telephones as timers. The terrorists in the recent Mumbai attacks communicated using satellite telephones. Drug dealers and organized criminals are heavily dependent on inexpensive prepaid cellular telephones that are essentially anonymous and disposable.[146]

Mobile network investigations are also commonly performed for "conventional crimes," often focusing on location information, logs of telephone calls, printouts of SMS messages, and associated metadata. A mobile device is generally defined as any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers.

1.3 MOBILE NETWORK TECHNOLOGY

In the late 1980s, the mobile telephony system in Europe was based exclusively on the ETACS network created by various telephone companies and consisting of analog radio links operating at the frequency of 800 MHz. Although at the time it was considered to be the start of a revolution, few would have imagined how quickly the phenomenon would burgeon both into a fad and into a system for keeping close track of individuals.

The weak points of the ETACS network were the lack of coverage abroad, continuing interference with other users, and the ease of cloning. It often happened that some unknown party obtained possession of the serial number of a mobile device, combined it with a new account to elude the NSP and generated telephone traffic paid for by the unwitting victim. In the mid-1990s, the GSM network was introduced. It operated at a frequency of 900 MHz and later 1.8 GHz. GSM was introduced precisely to eliminate once and for all the problem of interference among radio links and, being digital, to make conversations more secure.[147]

The next revolution in mobile network technology came about in 2003 when the Japanese colossus Hutchinson Whampoa entered the European market with H3G, the third generation of mobile telephony. The telephone now became a video-telephone, using the 2.1 GHz band. In the

[146] Curran, Kevin & Robinson, Andrew & Peacocke, Stephen & Cassidy, Sean (2010) Mobile Phone Forensic Analysis
[147] (Bucks.edu, 2020)
<https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/IntroToMobileForensics.pdf>

area of electronic communication services, it is necessary to distinguish between "telephony" and "telematic" services.

TELEPHONY	TELEMATIC
Telephone calls, including voice calls, voice messaging, conference calls, and data transmitted via telefax.	Internet access, E-mail.
Supplementary services, including call forwarding and call transfers	Fax, SMS and MMS messages via the Internet
Messaging and multimedia services, including SMS services	Telephony via Internet (Voice over Internet Protocol-VoiP)

A mobile device begins to leave its traces on the mobile network the moment it is turned on. When a device is powered on, it announces itself to the mobile network, generating a refresh of the authentication process. Like every technical device, a mobile device also releases technically sensitive information.[148] For example, an International Mobile Subscriber Identity (IMSI) is essentially a unique number that is associated with a particular subscriber on a GSM or UMTS mobile network. The IMSI is stored on the SIM card in a mobile device and is used to authenticate the device on the mobile network and to control the other details such as HLR (Home Location Register) or copied locally in the VLR (Visitor Location Register). In order to avoid interception of this sensitive number, the IMSI is not directly sent over the network. It is substituted by a TMSI (Temporary Mobile Subscriber Identity), which is a temporary number, usually created for a single session. At the request of digital investigators, NSPs can use these unique identifiers to query their systems for all activities relating to a particular subscriber account.[149]

1.4 INVESTIGATIONS OF MOBILE SYSTEMS

Investigations used to be carried out exclusively by people. In the pure spirit of investigation, you started from information obtained through an undercover agent followed by operations

[148] ACPO (2009) Practice Guide for Computer-Based Electronic Evidence, (2009), <www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf>

[149] Gratzer,V, Naccache, D., Znaty, D (2006) Law Enforcement, Forensics and Mobile Communications PerCom Workshop, Pisa - Italy, 13-17 March 2006, pp: 256-260

involving trailing suspects and intercepting ordinary mail. Without the help of technological systems, these investigations tended to last much longer than their more modern counterparts.[150]

Today, the initiation of an investigation may involve, in addition to verbal information, an anomalous bank record, an image from a surveillance camera, or of course highly visible crimes such as theft or murder.

The first phase of the investigation involves interviewing people who may have relevant information and continues with monitoring the means of communication of suspects or others associated in some way with the case. In addition to the traditional telephone, there are other monitoring points such as electronic mailboxes, places visited by the suspect, Telepass accounts (devices used for automatic highway toll payment), credit card accounts, and other financial operations.

Nowadays, investigations are supported by software that is customized to meet different requirements. The investigator enters all the data available on a subject into the interception system, and the server performs a thorough analysis, generating a series of connections via the mobile devices involved, the calls made or received, and so on, providing criminal police with a well-defined scheme on which to focus the investigation, and suggesting new hypotheses or avenues that might otherwise be hard to identify. Thanks to the support of the NSP, the data can be supplemented with historical information or other missing data such as other mobile devices connected to a given BTS on a given date and time. Data can also be provided for public payphones, which are often used to coordinate crimes. Again, thanks to a connection with the NSP, it is possible to obtain a historical record of telephone calls made and the location of the payphone with respect to other mobile devices. The same sort of record may also be obtained for highway travel using Telepass (the conventional name for automatic wireless toll payment), including average speed and stops.[151]

Having historical data of various kinds relating to an investigation accessible in a database can greatly assist the initial examination of a newly acquired mobile device. By extracting all

[150] Harrill, D C, Mislan, R. P. (2007) A Small Scale Digital Device Forensics ontology, Small Scale Digital Device Forensics journal, Vol 1, No 1, June 2007

[151] McCarthy, P. (2005) Forensic Analysis of Mobile Phones <http://esm.cis.unisa.edu.au/new_esml/resources/publications/forensic%20analysis%20of%20mobile%20phones.pdf>

telephone numbers in the phonebook of a mobile device seized during a search and entering names and numbers into the electronic system, digital investigators perform powerful analysis even in the initial phases of the investigation thanks to cross-referencing capabilities.

1.5 TYPES OF EVIDENCE

Mobile networks can provide information of relevance to an investigation, including the location of a mobile device, the past usage associated with a particular device or subscriber, as well as the context of communications.[152]

- ***Localization Parameters***

The term localization parameters describe the information that can be combined to localize an active mobile device and its related user. These localization parameters can be useful to track the position of a mobile device user, for several purposes, both for prosecution and defense.

- ***Determining the position of a given mobile device***

The simple act of turning on a device and leaving it in an idle state will generate data on the network that can be used to determine its approximate location. As a mobile device is moved from one location to another, it updates the network. Speaking, there is a timeframe where the mobile device "announces" itself to the network. The possible alternatives as follows:

a) Cell identification

The mobile device can be reached by looking at the cell to which it is currently connected. There is a range of accuracy that starts from a few hundred meters in urban areas, up to 32 km in suburban areas and rural zones. The accuracy depends on the known range of the particular base station serving the mobile device at the time of positioning. The poor value of 32 km can be enhanced with the use of the so-called Enhanced Cell Identification (general accuracy of 550 meters).

b) Time difference of arrival (TDOA)

[152] McCarthy, P and Slay, J (2006) Mobile phones: admissibility of current forensic procedures for acquiring data. In Proceedings of the Second IFIP WG 11.9 International Conference on Digital Forensics, 2006

This method also referred to as multilateration, measures the time it takes for a signal to travel from a mobile device to multiple base stations to estimate the device location. "It is a method commonly used in civil and military surveillance applications to accurately locate an aircraft, vehicle or stationary emitter by measuring the time difference of arrival (TDOA) of a signal from the emitter at three or more receiver sites."

c) Time of arrival (TOA)

This approach is effectively the same as TDOA, but this technology uses the absolute time of arrival at a certain base station rather than the difference between multiple stations.

d) Enhanced Observed Time Difference (E-OTD)

This method is similar to TDO, but in this case, the position is calculated by the mobile device, not the base station. In essence, the mobile device receives signals from multiple base stations at the same time that a specially placed receiver receives the signals. The precision of this method can vary from 50 to 200 m.

e) Assisted-GPS

A third-party service that generally relies on Cell Identification.

Determining the location of a mobile device can be important for assessing alibis of suspects or the whereabouts of victims in the past, and ongoing tracking of the location can be useful in cases of abduction, missing persons, and other ongoing criminal activities.[153]

From a practical perspective, there are tools that perform these techniques and display the results for digital investigators. Some of the information transmitted by the NSP to a monitoring centre is the position on the basis of cell and the IMSI code. This is extremely important information in that it makes it possible to track the people responsible for serious crimes as they move.

- ***Remote Activation of Electronic Devices***

Once, organized crime just used old-fashioned weapons. Now, with a mobile device and an Internet connection many more crimes can be committed. From the massacres of the 1990s to the latest terrorist attacks, mobile devices have played a fundamental role in the organization of

[153] National Institute of Standards and Technology (2007) Guidelines on cell phone forensics, <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>

crimes. With a ring or an SMS containing a code, it is possible to activate or deactivate an electronic device in any part of the world. This is why the ability to trace an SMS or even a simple ring signal is particularly important, along with the refinement of technology for capturing any signal or use, even if innocuous, of mobile phones.[154]

Unfortunately, organized criminal groups, having considerable financial resources, enjoy various advantages in terms of budget and decision-making speed in undertaking countermeasures to thwart the various investigation and law-enforcement bodies. They hire experts in technology as well as researchers who spend their days seeking out the latest solutions in terms of protection.

When criminal figures meet for business, they often protect their privacy by jamming signals in the area around their meeting place. This prevents mobile devices from linking to the BTS and thus connecting to the network. This prevents investigators from connecting to the cell and getting an idea of the geographical location of the meeting. The jamming mechanism also temporarily interrupts the operation of mobile phones in the area that might represent a threat of interception.

A mobile device jamming system emits a signal to prevent the use of mobile phones within a certain radius. It emits a wideband radio signal at the same frequency range used for transmitting signals from the BTS to the mobile phones. This signal prevents the mobile device from decoding the network signal and thus causes the mobile device to disconnect from the network.

- ***Usage Logs/Billing Records***

The logs maintained by an NSP can help digital investigators determine past usage of a mobile device, as well as communications between individuals. These logs are generated from Call Detail Records (CDR) maintained for billing purposes. The data in the resulting logs that are commonly provided to investigators are summarized here:

- Telephone number of user
- Numbers called
- IMEI number of mobile device

[154] Punja, S, Mislan, R (2008) Mobile Device Analysis, Small scale digital device forensics journal, Vol 2, No 1, pp: 1-16, June 2008, ISSN: 1941-6164

- Information about the cell: provides information about the location of the calling phone on the basis of the BTS where the connection was made
- SMS sent: excluding the text, which is available only via decodification using a telephone signal interception system.
- Date, time, and duration of calls

Depending on the equipment used, the logs generated on a particular mobile network may include a variety of other details. The Oracle Communications Services Gatekeeper is used by many NSPs world-wide for service delivery platform (SDP) infrastructure in a controlled, optimized, and automated way. Many external operators, including police units, have direct access to mobile network usage data via the Oracle Communications Services Gatekeeper solution, which is based on information technology, web and telecommunications industry standards such as Java Platform, Enterprise Edition (Java EE), web services, Session Initiation Protocol (SIP), IP Multimedia Sub-systems (IMS), Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). Investigators will find this data interesting for their activity.

- ***Text/Multimedia Messages***

A common use of mobile devices is to send messages in text or multimedia format. The Short Message Service (SMS) communication service, which has been in use for some fifteen years, allows transmission of a limited number of text characters using the telephony channel. The advantages of the service include the possibility of transmitting messages even in areas of very low GSM signal coverage, where a voice call would be disturbed or fail due to insufficient signal strength, and even when the voice channel is being used for a conversation.

SMS messages are intercepted using the same systems as used for intercepting voice calls. These systems not only record the telephone numbers of the originator and the recipient but also the entire text of the message. On some networks, the SMS messages are archived for extended periods. The Multimedia Message Service (MMS) is a more evolved form of SMS, where it is possible to attach other multimedia content to a classic text message, such as an audio, video, or photo file. Current interception systems also capture the multimedia content, saving it to a special folder for display or listening.

1.6 HOW DATA MAY BE ACQUIRED

Various laws have been enacted to define how traffic data retained by NSPs may be acquired. Therefore, it is essential for investigators to be familiar with the legislation in force in the country or jurisdiction in which they are operating. In certain countries, for example, the defendant's counsel or suspect's lawyer has the right to request directly from the NSP only those traffic data that refer to the "accounts registered in the name of the client."[155]

In other countries, on the other hand, there are authorities specifically assigned by law to identify measures for guaranteeing the rights of the parties involved in questions of telephone and telematic traffic data retention for detecting, investigating, and prosecuting crime. Precisely for this reason, anyone accessing or processing these data must adhere to certain principles:

- The legislated requirement to provide specific safeguards regarding the type and quantity of data to protect and the risks correlated with said protection. Providers are already required to prevent said risks by upholding common security obligations that go beyond merely the minimum measures required by law or regulation. These risks are then assumed by those who receive the data.
- The advisability of identifying, given the current situation, protective measures to be implemented in the processing of data by all providers so that the integrity of said data can be verified in an inspection (and admissible in dealings with the suspect or defendant's counsel) to ensure more effective security for telephone and telematic traffic data.
- The need to keep in mind the costs deriving from the implementation of the measures in the various countries or jurisdictions, also regarding the different technical and financial capacities of the parties involved.
- The transnational legislative context, especially in light of the opinions expressed by the various groups working to protect personal privacy.
- The technological state of the art, meaning that the various measures have to be periodically updated.

[155] Willassen, S Y (2003) Forensics and the GSM mobile telephone system, International Journal of Digital Evidence, Spring 2003, Vol 2, No 1, pp:12-24

These are important matters with which to be familiar, especially in the field of cross-border investigations and litigation.[156]

1.7 LET'S SUM UP

In this chapter, we studied the technology-based investigations and acquisition of data with respect to it. We discussed the investigations of mobile systems and finally, ended the discussion with different types of evidence that would be collected via mobile systems.

1.8 FURTHER READING

- Gibbs, K. E., & Clark, D. F. (2001). In E. Casey (Ed.), Handbook of computer crime investigation. Academic Press.
- International Engineering Consortium. (2007). Time Division Multiple Access (TDMA). Available online at www.iec.org/online/tutorials/tdma/index.asp
- Prevelakis, V., & Spinellis, D. (2007). The Athens affair, IEEE spectrum. Available at www.spectrum.ieee.org/jul07/5280
- EDRI (2006). Telecom Italia wiretapping scandal. Available on EDRI Online, www.edri.org/edrigram/number4.15/italy

1.9 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) Define mobile device?

A mobile device is generally defined as any instrument that can connect to and operate on a mobile network, including cellular telephones, wireless modems, and pagers.

2) Differentiate between Telephony and Telematic?

TELEPHONY	TELEMATIC
Telephone calls, including voice calls, voice	Internet access, E-mail.

[156] Casey, E, Bann, M, & Doyle, J (2009) Introduction to windows mobile forensics. Digital Investigation, 6(3–4)

messaging, conference calls, and data transmitted via telefax.	
Supplementary services, including call forwarding and call transfers	Fax, SMS and MMS messages via the Internet
Messaging and multimedia services, including SMS services	Telephony via Internet (Voice over Internet Protocol-VoiP)

3) How is the cell identified in the process of investigation?

The mobile device can be reached by looking at the cell to which it is currently connected. There is a range of accuracy that starts from a few hundred meters in urban areas, up to 32 km in suburban areas and rural zones. The accuracy depends on the known range of the particular base station serving the mobile device at the time of positioning. The poor value of 32 km can be enhanced with the use of the so-called Enhanced Cell Identification (general accuracy of 550 meters).

4) What is localization parameters?

The term localization parameters describe information that can be combined to localize an active mobile device and its related user.

1.10 ACTIVITY

Explain how the data is acquired through mobile device investigations along with how and what are the different types of evidence that are collected through the process? Briefly explain it with a relevant case study? (1000 words)