Chapter 1 Network Forensics: Fundamentals

ABSTRACT

Network forensics investigations aim to uncover evidence about criminal or unauthorized activities facilitated by, or targeted to, a given networking technology. Understanding the fundamental investigative principles is equally important as understanding each of the modern networking technologies for every forensics scientist or practitioner. This chapter provides an overview of the network forensic fundamentals from a contemporary perspective, accenting the formalization of network investigation, various investigative techniques, and how the network forensics support the legal system.

INTRODUCTION

This chapter overviews the fundamentals of the network forensics practice. An updated network forensics definition is provided to reflect the proliferation of new networking solutions including mobile devices, smart objects, industrial controls systems, and cloud computing platforms. The standardized network forensics investigation process recommended by the International Standardization Organization (ISO) is presented throughout the chapter with supporting examples of mobile network investigations. In the same context, the network forensics techniques and their role in the legal system are also discussed. The chapter concludes with a brief review of the current mobile technology to set the accord for the remainder of this book.

DOI: 10.4018/978-1-5225-5855-2.ch001

DEFINITION OF NETWORK FORENSICS

Network forensics is a cross-discipline of digital forensics and communication networks. Digital forensics is the application of scientific methods to investigate evidence from digital sources about security incidents or criminal activities (Palmer, 2001; Ruan *et al.*, 2011). Communication networks refer to any infrastructure used for exchange of information in digital form between two or more network entities. In the early years, the network forensics focused on investigating Internet Protocol (IP) based networks for evidence in relation to malicious traffic packets or irregular traffic flows in violation of the networking policies and principles (Khan *et al.*, 2016).

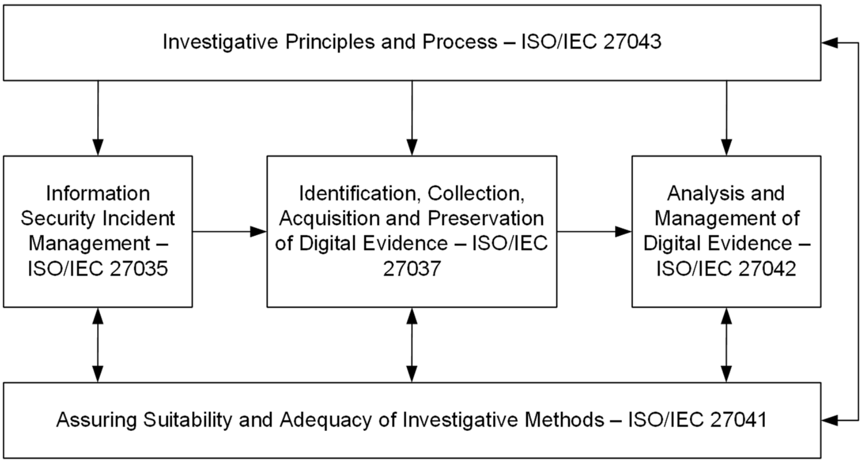
As both the networks and the malicious behavior evolved, the forensics practice broadened to include mobile networks, cloud computing, Internet-of-Things (IoT), industrial control systems, and software-defined networks. The investigations in these environments follow the common network forensics investigation process with techniques, tools, and procedures tailored specifically for each of them. Modern network forensics thus refer to the *scientific methods for identification, collection, acquisition, and preservation of digital evidence from networking environments for further analysis, interpretation, and presentation in investigating security incidents and criminal activities*.

NETWORK FORENSICS INVESTIGATION PROCESS

Background

The formalization of network forensics is necessary to ensure the soundness and reliability of the investigative process and the veracity of evidence presented in court (Slay *et al.*, 2009). To demonstrate the suitability of the scientific methods for production of network evidence, various formal models have been proposed in the past (Marshall, 2011; Joshi and Pilli, 2016). The ISO recognized that the inconsistency between these models can greatly affect the quality, validity, and credibility of the digital evidence and devised accreditation through the set of interrelated standards depicted in Figure 1. These standards lay down the fundamental set of principles with guidance on how they can be applied in common scenarios. As such, the ISO/IEC SC27 standards are suitable for investigations in various networking environments to ensure the quality of the network forensics products.

Figure 1. ISO/IEC SC27 digital forensics standards


Investigative Principles and Process – ISO/IEC 27043
Information Security Incident Management – ISO/IEC 27035
Identification, Collection, Acquisition and Preservation of Digital Evidence – ISO/IEC 27037
Analysis and Management of Digital Evidence – ISO/IEC 27042
Assuring Suitability and Adequacy of Investigative Methods – ISO/IEC 27041

ISO/IEC 27035:2016 - Information Security Incident Management

The production of credible network evidence begins by establishing an *investigative readiness* (International Standardization Organization, 2016). The investigative readiness is a structured approach in handling security incidents and is achieved in five distinct phases:

1. Plan and prepare
2. Detection and reporting
3. Assessment and decision
4. Responses
5. Lessons learned

For network-related security incidents, the plan and preparation phase includes development of *incident management plan* and *investigative capabilities*. The plan encompasses further development of *policies* describing which traffic events are considered malicious or irregular that constitute a network security incident. The plan also requires development of *procedures* describing the steps for responding to an incident. The *network protection controls* such as firewalls, intrusion detection and prevention, or unified threat management systems are recommended as incident response capabilities together with an *incident response team* and a relationship with one or several Law Enforcement Agencies (LEA)s.

The detection and reporting phase describes the steps for registering or receiving external information about a security event. Security events can be detected with alarms of abnormal network activities and recognition of potentially malicious traffic or reported by an external agency (e.g. LEA or a Computer Emergency Response Team – CERT). This alarm or external report is further assessed in regards the network policies to make a decision on whether the security event is actually a network security incident (or is discarded as a false alarm). If it is an incident, the incident response team categorizes and classifies it according to its severity, contains the incident, restores the normal network operations, and proceeds in collecting the related evidence. The evidence may need to be used at a future time for disciplinary or legal proceedings, therefore it is important for the team to be trained in handling digital forensics evidence. In case the security incident warrants cooperation with an external agency, there must be established procedures and handover interfaces for evidence delivery. Once the incident is resolved, the investigation is reviewed so the policies, procedures, and network security controls are further improved for other emerging threats.

ISO/IEC 27037:2012 - Identification, Collection and Acquisition, and Preservation of Digital Evidence

With ISO/IEC 27035:2016 in place, the investigation follows the ISO/IEC 27037:2012 guidelines for identification, collection, acquisition and preservation of network evidence (International Standardization Organization, 2012). The initial phases of the network forensics investigation process are: *identification*, *collection & acquisition*, and *preservation* of digital evidence.

Identification

The identification is the search for, recognition, and documentation of potential network evidence. Consider a lawful interception of mobile traffic including calls and texts for a prepaid user during a period of 30 days. The mobile network investigators need to be able to uniquely recognize the traffic based on the user's phone numbers or other network identifiers that the investigators were able to obtain. Further, investigators need to search for the meta-data corresponding to the user activity in these days, e.g. prepaid account activity, or network registrations. For both types of potential mobile network evidence, investigators need to document the evidence, the network elements and persons involved, and the identifier(s) used to search for the subjects of the investigation. Chapter 4 and Chapter 5 provide further details on mobile network evidence identification.

Collection and Acquisition

ISO/IEC 27037:2012 distinguishes between collection and acquisition of digital evidence to remain general enough for all digital forensics investigations. The collection is the process of gathering data that contain potential digital evidence, while acquisition happens when investigators create a copy of the data to maintain the original condition of the potential digital evidence. In most investigations, the collection and acquisition is essentially one step because the network infrastructure is distributed in nature so it is infeasible to physically access the network elements (e.g. routers, security appliances, or servers) to make a copy of the stored data. In the interception example above, the investigators are making copies of the call and text contents in real-time as they are realized over the mobile network, i.e. they acquire the *content-of-communication* (CC) to bring it as a potential digital evidence under forensic custody. They also acquire the meta-data for the targeted subjects immediately after the interception is concluded as the *interception-related information* (IRI) to ensure its original condition when in forensic custody. Both the CC and IRI data are delivered over standardized and secured handover interfaces between the mobile operators and the LEAs rather than sending the network equipment for local analysis. Chapter 6 through Chapter 8 discuss the lawful interception as an investigative practice and the handling of CC and IRI as mobile network evidence.

Preservation

Once the potential evidence is in forensic custody, the preservation takes place to protect its integrity so to ensure its usefulness for the investigation. The preservation method is dependent on the type of network evidence. If the evidence is volatile, i.e. acquired in real-time as the CC during a lawful interception, investigators need to stored it in a safe place, with integrity checks in place, and at least one back-up copy. The back-up is important because if the evidence is tampered or lost, it will be impossible to be recreated or re-acquired again. This holds also for the meta-data, although there is a possibility for the investigators to request a copy for some of the information like the prepaid account history because most mobile operators are obliged by law to keep copies of aggregated meta-data for three or more years. The chain-of-custody also plays a critical role in the potential evidence preservation, especially for privacy sensitive data like the intercepted calls or texts. Investigators need to ensure that only authorized parties have access to the data and limit the disclosure of the CC. Chapter 6 and Chapter 7 elaborate on the preservation of mobile network evidence to safeguard the privacy of the involved parties.

ISO/IEC 27042:2015 - Analysis and Interpretation of Digital Evidence

ISO/IEC 27042:2015 guidelines describe the methodology for extracting the probative value out of the potential digital evidence (International Standardization Organization, 2014a). The analysis can be carried out in two modes: *static analysis* and *live analysis*. The static analysis is the inspection of raw consequential data (e.g. packet captures, logs files, or traces) and meta-data (e.g. file permissions and timestamps) in *non-real* time. Static analysis should normally be carried out on a copy of the original potential digital evidence (as described in ISO/IEC 27037:2012) to avoid accidental spoliation or obfuscation. The live analysis is inspection of the live version of the systems and is carried out in *real-time* while the network traffic is actually in transit. In these circumstances, great care must be taken to minimize the risk of damaging and losing the potential network evidence with a full and detailed record of all forensic processes performed. In both cases, the forensic analysis can be facilitated with forensic tools adequate for examination of the potential network evidence (as described in ISO/IEC 207041:2015). The product of the network forensic analysis is the segment of the data selected as the actual network forensics evidence that is next subjected to interpretation.

The objective of interpretation is to evaluate the network forensics evidence based on its contents and context including key patterns, topics, relevant people, etc., to derive meaning in respect to the investigated security incident or criminal activity. The interpretation involves fact finding and validation/verification of results. In searching for facts, it is important to distinguish between facts that have been found in the evidence, and facts inferred from additional data or information provided. For example, a lawfully intercepted CC from a mobile network is a fact. If combined with the meta-data of the call, the conversation can be placed in time and the broad location of the calling and/or called party can determined. This distinction is important when reporting these facts so the logical process of inference can be validated. The interpretation of the network evidence is dependent on its context of creation, that is, the investigators need to consider information about the network operation itself.

In our example, this information can include call handling configurations (e.g. active call forwarding rules, prepaid balance), geographical mapping of the cell towers used to realize the call, etc. This is important so that the investigators ensure the quality of the network evidence (completeness, source and original purpose, prevention of evidence obfuscation). If the contextual information changes, the interpretation may also have to change to reflect this. The network forensics interpretation is delivered as a formal report that contains the information about the competence of the investigators, the nature of the investigation, the factual details, the contextual information, any analytical and interpretative limitations, list of processes and tools used, the final interpretation and conclusion, and if needed, a recommendation for further investigative work. Chapter 7 and Chapter 8 detail the analysis and interpretation of mobile network evidence including specific tools, techniques, and procedures.

ISO/IEC 27043:2015 - Incident Investigation Principles and Processes

ISO/IEC 27043:2015 guidelines describe a harmonized digital investigation model for various operational scenarios involving digital evidence (International Standardization Organization, 2014b). This model is shown in Figure 2 and provides a succinct guidance on the exact logical steps to be followed during any kind of investigation in such a way that, if challenged in any court of law, no doubt should exist as to the accuracy of the investigation and the quality of the evidence. ISO/IEC 27403:2015 outlines four classes of investigative processes: *readiness*, *initialization*, *acquisitive*, and *interpretative*. In parallel, there is a set of concurrent actions: authorization, documentation, information flow management, chain-of-custody, digital evidence preservation, and interaction with the physical crime scene.

Readiness Processes

The readiness processes help the pre-incident preparation and include planning, implementation and assessment phases. This class of processes is optional to the network investigation processes and is effectuated by an organization rather than the investigator(s). However, for networks that are subject to regulation or are categorized as critical infrastructures (e.g. mobile networks or industrial control systems), the readiness is required to ensure that the forensic investigation will yield digital evidence without negative consequences to the involved parties (i.e. privacy intrusion or environmental pollution). The planning phases includes identification of all sources of potential network evidence and the necessary policies and processes for this evidence to be handed over for further analysis or to the external LEAs. If for example, a mobile operator has to implement lawful interception capabilities, follow the regulatory requirements for wiretapping invocation, establish the lawful interception architecture, and create the handover interfaces with LEAs for evidence delivery. The implementation phase includes the procurement of the required equipment, testing of the handover interfaces for security, and appointment of responsible entities on both sides. The assessment phase is set in place to ensure that all the regulatory and technical requirements are met prior to instantiating any network investigation. The readiness process and the legal framework for mobile network investigations is discussed in Chapter 6.

Initialization Processes

The initialization processes deal with incident detection, first response, planning, and preparation of the network investigation. The incident detection and first response phases correspond with the detection and reporting phases from the ISO/IEC 27035:2016 guidelines. In these phases the investigation is initialized by registering or receiving external information about a security event. Assuming lawful interception capabilities in place, the investigation is initialized by receiving a request for target subjects of lawful interception (identified by a list of phone numbers, for example) by a LEA. The planning and preparation phases follow to determine the period, format and type of interception (e.g. only calls and text messages in the next 30 days), the registration status (e.g. currently active prepaid subscriber registered in the Chicago metropolitan area), and the transfer of the intercepted material in real-time over the handover interface to the LEA. Chapter 6 provides the initialization mechanics for mobile network investigations.

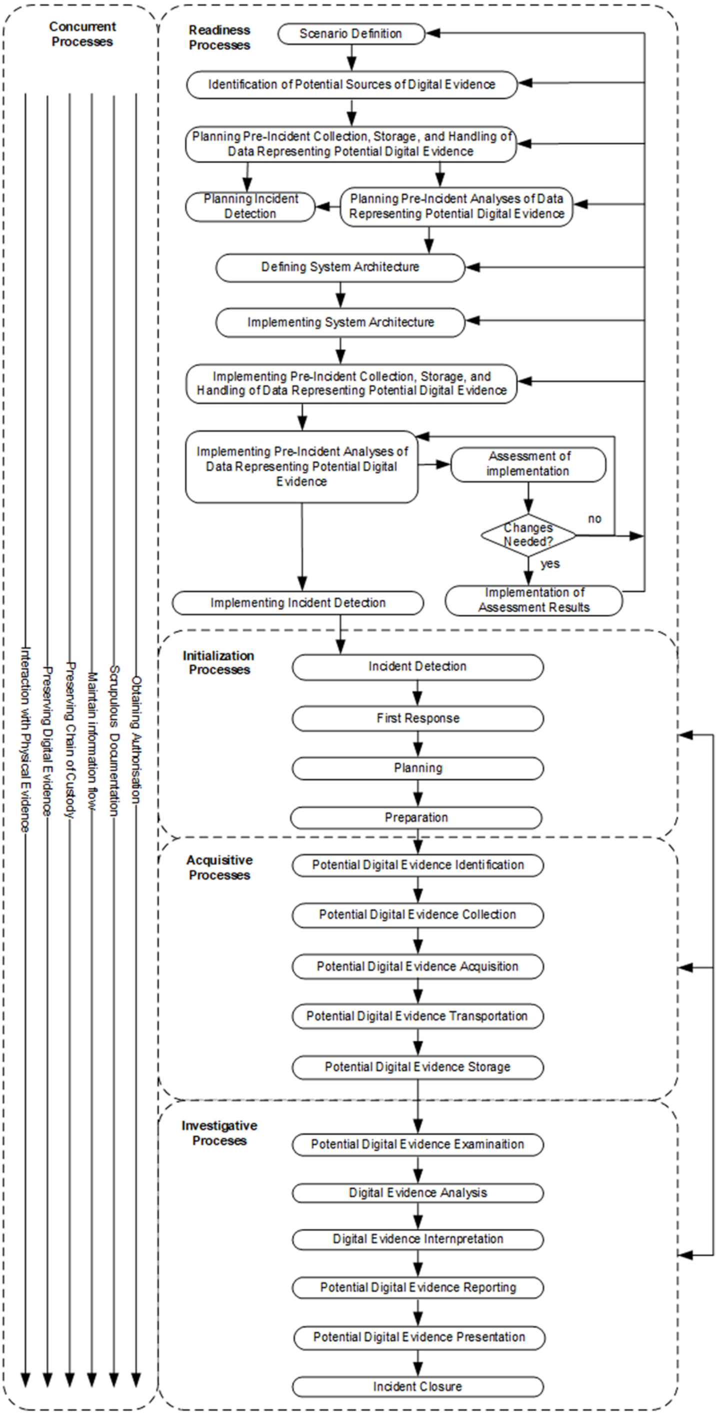
Acquisitive Processes

The acquisitive processes are concerned with the acquisition of network evidence following the steps described in ISO/IEC 27035:2012. In the interception example, the identification and acquisition corresponds to activation of the lawful interception feature for the target subjects on the network side for all the calls and text messages they will eventually send/ receive in the next 30 days. The network evidence in this case is the content of the calls and the text messages together with the associated network meta-data. During the acquisition, investigators need to document the registration status and if there are any changes to the user profile on the network side during the lawful interception period (e.g. the subject has roamed in Canada in the last 7 days of the investigation period and cannot initiate originating calls due to insufficient balance on the prepaid account). Investigators can decide to include historical information from the targets' prepaid accounts to form the context of evidence creation as discussed in ISO/IEC 27042:2015. During the acquisition, the intercepted material is transferred in real-time over the handover interfaces to the LEA, where it is securely stored for further analysis. Chapter 6 through 8 elaborate the acquisition of digital evidence from the second generation (2G) up to the forthcoming fifth (5G) of mobile networks.

Investigative Processes

The investigative processes closely follow the ISO/IEC 27042:2015 guidelines for analysis and interpretation of digital evidence. The potential digital evidence – the content of the calls and the text messages with the associated meta-data - is analyzed together with the prepaid balance history of the targeted subject of investigation. The overall information is interpreted to create the mobile activity profile of the subjects for the period of the investigation. The profile includes the list of other parties contacted in this period and subject's coarse movement pattern (e.g. traveled to New York and after two days roamed in the Montreal area for the last 7 days of the investigation period). The investigators detail the profiling to reflect the subject's inability to initiate calls due to an insufficient balance while in roaming, i.e. supporting the fact that the subject

Figure 2. Common Network Investigation Model


Concurrent Processes
Interaction with Physical Evidence
Preserving Digital Evidence
Preserving Chain of Custody
Maintain information flow
Scrupulous Documentation
Obtaining Authorisation
Readiness Processes
Scenario Definition
Identification of Potential Sources of Digital Evidence
Planning Pre-Incident Collection, Storage, and Handling of Data Representing Potential Digital Evidence
Planning Incident Detection
Planning Pre-Incident Analyses of Data Representing Potential Digital Evidence
Defining System Architecture
Implementing System Architecture
Implementing Pre-Incident Collection, Storage, and Handling of Data Representing Potential Digital Evidence
Implementing Pre-Incident Analyses of Data Representing Potential Digital Evidence
Assessment of implementation
Changes Needed?
no
yes
Implementing Incident Detection
Implementation of Assessment Results
Initialization Processes
Incident Detection
First Response
Planning
Preparation
Acquisitive Processes
Potential Digital Evidence Identification
Potential Digital Evidence Collection
Potential Digital Evidence Acquisition
Potential Digital Evidence Transportation
Potential Digital Evidence Storage
Investigative Proceses
Potential Digital Evidence Examinaition
Digital Evidence Analysis
Digital Evidence Internpretation
Potential Digital Evidence Reporting
Potential Digital Evidence Presentation
Incident Closure

has only sent two and received three text messages, but made no calls. The profile is then presented in the court of law to support the hypothesis for the implicated criminal activities of the subject. The investigation concludes with the closure phase where the investigators decide whether to reiterate the investigation, reject or accept the hypothesis, and safely store the intercepted evidence for the period required by the interception regulation and local laws. Chapter 6 through 8 elaborate the analysis, interpretation, and presentation of mobile network evidence in practice.

Concurrent Processes

The concurrent processes are a set of actions that should be followed throughout the network investigation include: authorization, documentation, information flow definition, chain-of-custody preservation, network evidence preservation, and interaction with the physical investigation. Prior to any lawful interception, mobile operators need to formally accept an interception request and authorize the investigation. The information flow definition and the realization of the interception are also required together with the documentation to reflect every change in subjects' mobile network activity or changes in the network configuration that can affect the context of evidence creation. The preservation of the chain-of-custody and the network evidence is critical during the investigation to ensure that no one has tampered (both digitally and physically) with the intercepted material and any other related evidence to ensure proper analysis, interpretation, and presentation in court.

ISO/IEC 27041:2015 - Assuring Suitability and Adequacy of Investigative Methods

The ISO/IEC 27041:2015 provides guidance for assuring suitability and adequacy of investigative methods. To assure the suitability of the lawful interception as a form of mobile network forensics investigation in real-time, the regulators, LEAs, and the mobile operators need to define and analyze the requirements for its realization. Following an agreement on the requirements, the lawful interception needs to be designed, implemented, verified, and validated in accordance with the local regulatory directives and laws, as well as with the global mobile technology standardization. If this is confirmed by all stakeholders, the interception architecture is deployed and regularly reviewed and maintained as needed. Chapter 6 elaborates on the suitability and adequacy of the lawful interception in greater detail.

TAXONOMY OF NETWORK FORENSICS TECHNIQUES

The ISO/IEC SC27 guidelines detail the network investigations to maximize the probative value of the network evidence, but say little about how to operationalize the investigations depending on the criminal activity or the nature of the security incident. Table 1 shows the taxonomy of network forensics techniques based on the various parameters used to identify the type of crimes or security incidents investigated (Joshi and Pilli, 2016; Khan *et al.*, 2016).

Table 1. Types of network forensics techniques

Category	Parameter	Description
Mechanism	Logging	Recording of network flows and patterns
	Packet Marking	Marking of network packets and flows (e.g. e.g. source destination IP/port, number of packets, etc.)
	Heuristic Base	Network topology analysis (e.g. nodes distances, traffic load, traffic distribution, etc.)
Data Source	Traffic	User network traffic
	Meta-data	Signaling (network control) traffic
	Traffic and meta-data	Combination of raw/signaling traffic
Data Instance	Packet header	Investigation based only on packet header information
	Packet payload	Investigation based only on packet payload information
	Packet flow	Investigation based on both the traffic header and the payload, e.g. the traffic flow
	Network node	Analysis of the network infrastructure
Forensic Processing	Centralized	Processing of potential network evidence centralized forensics server
	Decentralized	Processing of potential network evidence Distributed forensics servers
Time of Investigation	Real-time	The identification and acquisition of the potential network evidence at the time of its flow, e.g. in transit
	Non-real-time	Ex-post-facto or identification and acquisition of the potential network evidence after the attack
Purpose of Investigation	Attribution	Investigating the origin of security incidents
	Crime Reconstruction	Investigating the network events corresponding to criminal activities
	Evidence Validation	Validating evidence resulting from other investigations

These techniques need to be adapted to the specific technologies for each networking environment. The taxonomy mostly relates to Internet networks, but it can be modified for investigations in mobile networks, cloud computing, internet-of-things, industrial control systems, software-defined networks, or any other digital networks. Mobile network investigations use the same techniques with the addition of a *circuit marking* parameter for intercepting circuit-switched calls. The data sources in mobile networks typically include voice, messaging, packet services, localization information, charging records, and signaling traffic (the IRI or the network meta-data)

The forensics processing can be centralized, i.e. with one LEA working on evidence from one or multiple national mobile operators; or decentralized, i.e. coordinated forensic processing of different mobile network data by different LEAs. Decentralized processing is useful for handling evidence coming from different jurisdictions and international mobile carriers. The time of investigation corresponds with the interception of real-time traffic (CC) or non-real-time data (IRI or meta-data) that can be retrieved *ex-post-facto* (after the fact). The forensics investigations in mobile networks deal with *mobile network facilitated crimes* or *mobile network targeted attacks*. When investigating mobile network facilitated crimes, the objective of the investigation is to collect potential evidence that can later be used in crime reconstructions in the court of law. In some cases, the localization information about the whereabouts of the perpetrators at the time of the crime can be challenged. A forensic radio survey can be devised to investigate the network coverage to validate the localization evidence provided by the network as an independent on-site investigation. The mobile networks like every network can become a target for an attack on its services so any related incident also needs to be forensically investigated to determine the origin of attack and the vulnerabilities exploited. The objective is to provide the evidence of the mobile network targeted attack so that the mobile operators, equipment vendors, and standardization bodies can work on improving the security of the network infrastructure.

NETWORK FORENSICS IN THE LEGAL SYSTEM

The legal processing of network facilitated crimes is critically dependent on the quality of the network evidence, its pertinence to the criminal activity, and the trustworthiness of its interpretation (Casey, 2011; Daniel and Daniel, 2011).

Evidence Admissibility

Before any network evidence is admitted in courtroom, it must meet certain standards, that is, courts need to test its:

1. Relevance
2. Authenticity
3. Not hearsay or admissible hearsay
4. Best evidence
5. Not unduly prejudicial

It is critically important for any type of network evidence to be obtained with court authorization – or warrant – otherwise it will not be admitted in court. This is especially important when conducting lawful interceptions in mobile networks. In order to invoke an interception as "lawful", the investigators need to convince the court authorities the mobile traffic indeed is a source of potential evidence for a given crime. The main exceptions allowing warrantless investigations (or searches) in the US are plain view, consent, and exigency. Evidence can be obtained without a warrant if the investigators see the evidence in plain view, they have a valid consent from the network users, for emergency life threatening situations or threat of an immediate evidence destruction. Mobile localization data is often used to pinpoint the geographical position of a target user in the case of an emergency following a 911 call, for example.

To demonstrate authenticity of the network evidence, investigators provide proofs that it was obtained from a network infrastructure and that the chain-of-custody and integrity checks show the evidence was preserved while in forensic custody. Investigators also need to provide proofs for the reliability of the evidence or to show that the network infrastructure was functioning normally during the time the evidence was created. The original data acquired during the investigation is always considered the best evidence for the crime. Copies of the evidence can also be submitted as best evidence if investigators can demonstrate they are the exact duplicate of the original digital data. Network evidence might not be admitted if it contains hearsay because the speaker or the author of the evidence is not present in court to verify the truthfulness (Casey, 2011). For example, the CC needs to be verified to prove that the speakers in the phone conversations are actually the target subjects of the lawful interception.

Expert Reports and Testimony

Communicating the results of a network investigation in court is highly important in understanding the pertinence of the evidence to the criminal act. The investigators' report or testimony can easily become hard to follow if rendered in too many technical terms because very few are familiar with the specific language of the technologies investigated. When writing a report, investigators need to build a solid interpretation based on the facts and inferences with detailed entries of every stage of investigation so another competent investigator or expert can evaluate the evidence and associated conclusions. Investigative reports need to include the steps taken to prepare for the investigation, summarize the sources of potential digital evidence, the techniques, tools, and procedures used for examination, the forensics analysis and interpretation, the findings, and an elaborate conclusion. In reporting an investigation including a lawful interception, LEA's requests shall be included with the subjects' identifiers, mobile services of interest, the period of investigation, and any input information from a related mobile device forensics report. The CC needs to be accompanied with transcripts of the conversations or the messages together with the IRI or network metadata. The techniques and tools used for analysis of the mobile data have to be documented so the courts can test the scientific process used for interpretation (known as the Daubert test). Investigators need to clearly indicate their level of confidence in their interpretations and conclusions. In case further assistance is needed in verifying the evidence, investigators need to clearly indicate the need for additional forensics help (e.g. forensics speech recognition for the speakers included in the CC evidence).

CONCLUSION

Mobile technology is a dominant networking platform with 390 million users in North America in 2017 more than 80% of them being 4G Long Term Evolution (LTE) subscriptions. This means that there are more subscriptions than people on the continent; at least 8% of these subscriptions are either used for connecting smart objects, people have two or more mobile devices, or are inactive but registered with the mobile operators. In terms of traffic, an active smartphone in North America realized on average 6 GB/month and is expected to generate around 50 GB/Month in 2023 (Ericsson, 2018).

From a legal perspective, a mobile penetration of more than a 100% implies that almost all crimes are facilitated by mobile devices, directly or indirectly. Consequently, evidence about mobile device network activity is becoming more prevalent in various court proceedings. From a forensics perspective, the millions of gigabytes of mobile data require understanding of the different mobile networking technologies, how the forensics principles apply respectively, the operationalization of the investigation process, and the applicable techniques in the production of mobile network evidence. Bringing this knowledge closer to the investigators, forensic practitioners, or researchers is the main goal of this book. The subsequent chapters elaborate on all of these topics to help interested readers understand the forensics context of the mobile networks, the role of mobile network evidence in the legal system, and the emerging challenges and opportunities in the ubiquitous mobile communications.

REFERENCES

Casey, E. (2011). *Digital Evidence and Computer Crime* (3rd ed.). Waltham, MA: Elsevier.

Daniel, L. E., & Daniel, L. E. (2011). *Digital Forensics for Legal Professionals: Understanding Digital Evidence From the Warrant to the Courtroom*. Waltham, MA: Syngress.

Ericsson. (2018). *Ericsson Mobility Report, Ericsson Mobility Report*. Available at: https://www.ericsson.com/en/mobility-report/reports/june-2018

International Standardization Organization. (2012). *ISO/IEC 27037:2012 guidelines for identification, collection, acquisition and preservation of digital evidence*. Available at: https://www.iso.org/standard/44381.html

International Standardization Organization. (2014a). *ISO/IEC 27042 -- Guidelines for the analysis and interpretation of digital evidence*. Available at: https://www.iso.org/standard/44406.html

International Standardization Organization. (2014b). *ISO/IEC 27043 -- Incident investigation principles and processes*. Available at: https://www.iso.org/standard/44407.html

International Standardization Organization. (2016). *ISO/IEC 27035:2011 -- Information security incident management*. Available at: https://www.iso.org/standard/62071.html

Joshi, R. C., & Pilli, E. S. (2016). *Fundamentals of Network Forensics* (1st ed.). London, UK: Springer; doi:10.1007/978-1-4471-7299-4

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications. Elsevier*, *66*, 214–235. doi:10.1016/j.jnca.2016.03.005

Marshall, A. M. (2011). Standards, regulation & quality in digital investigations: The state we are in. *Digital Investigation. Elsevier Ltd*, *8*(2), 141–144. doi:10.1016/j.diin.2011.11.001

Palmer, G. (2001) *A Road Map for Digital Forensic Research*. Academic Press.

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics. *Advances in Digital Forensics 7th IFIP WG 11.9 International Conference on Digital Forensics,* 35–46. 10.1007/978-3-642-24212-0_3

Slay, J., Lin, Y.-C., Turnbull, B., Beckett, J., & Lin, P. (2009). Towards a Formalization of Digital Forensics. In Advances in Digital Forensics V. New York: Springer. doi:10.1007/978-3-642-04155-6_3

KEY TERMS AND DEFINITIONS

2G: 2nd generation of mobile networks. The most dominant technology is the global system for mobility (GSM).

3G: 3rd generation of mobile networks. The most dominant technology is universal mobile telecommunication system (UMTS).

3GPP: 3rd generation partnership project.

4G: 4th generation of mobile networks. The 4G technologies are long term evolution (LTE) and the advanced version, LTE-advanced. Colloquially, the terms LTE/LTE-A are used as a synonym for 4G as they are the only global standard for mobile communication from the fourth generation.

5G: 5th generation of mobile networks. Still in standardization phase, the first 5G deployments are envisioned for 2020.

CERT: Computer emergency response team.

CC: Content-of-communication.

Exabytes: 10^{18} bytes or 1 billion gigabytes.

Gigabytes: 1 billion bytes. Bytes are units of digital information consisting of eight bits – zeroes or ones.

IoT: Internet of things.

IP: Internet protocol.

ISO/IEC: International Standardization Organization/International Electrotechnical Commission.

LEA: Law enforcement agency.

LTE: Long term evolution.

TCP/IP: Transmission control protocol/internet protocol.