



Ministry of Higher Education and Scientific
Research
University of Oran 1 – Ahmed Ben Bella –
Institute of Criminology



The Digital Crime Scene

Dissertation submitted as partial fulfilment of requirements
for the degree of academic **Master**

Branch : Law

Specialization: criminology

Presented by :

Boussadia Mohammed El Amine

Supervised by :

Dr.Hezil Djelloul

Board of Examiners

Dr.Hezil Djelloul	University of Oran 1 Ahmed Ben Bella	Supervisor
Dr.Mekki Ahmed	University of Oran 1 Ahmed Ben Bella	President
Dr. Mekhzoumi Mohammed El Habib	University of Oran 1 Ahmed Ben Bella	Examiner

AcademicYear: 2025/2026

Dedication

I dedicate this humble work to my wonderful mother my lovely father, my brothers.

Special thanks to the person who encourages me all the time without forgetting those who gave me support and help .

Acknowledgments

I would like to start by thanking my supervisor Dr. Hezil Djelloul Your guidance,

valuable insights and expertise has contributed immensely to this thesis and motivated me

throughout this process.

I would also like to thank my family and friends who have accompanied and encouraged me .

I would also like to thank the members of the committee, Dr Mekki Ahmed and Dr. Mekhzoumi Mohamed El Habib who have given their time to read and evaluate this humble work.

Abstract

This study examines the conceptual and procedural framework of the digital crime scene, a complex virtual space where crime transcends physical boundaries to encompass data and technological clouds. This shift imposes significant challenges regarding the fragility of digital evidence and its susceptibility to damage or alteration. Through a descriptive-analytical approach, this thesis aims to shed light on the modern technical and operational methods essential for inspecting the electronic crime scene, starting from the moment of discovery and preservation, leading to forensic analysis and the extraction of evidence that ensures legal admissibility before the judiciary. Furthermore, the study highlights the necessity of balancing the effectiveness of criminal investigations with the protection of individual privacy, emphasizing the importance of developing laws to keep pace with the technological surge, especially since these crimes rely primarily on software. It also addresses the aspect of promoting electronic awareness to protect individuals from cyberattacks that may compromise their sensitive data or financial assets.

KeyWords: Digital Evidence , Crime Scene , CyberSecurity , Digital Forensics , Malware , Investigations , Protocols , Meta Data , Admissibility , Investigative Tools

الملخص

تتناول هذه الدراسة الإطار المفاهيمي والإجرائي لمسرح الجريمة الرقمي، وهو ذلك الفضاء الافتراضي المعقد الذي تتجاوز فيه الجريمة حدودها المادية لتشمل البيانات والسحب التكنولوجية، مما يفرض تحديات جسيمة تتعلق بهشاشة الدليل الرقمي وسرعة تعرضه للتلف أو التغيير. حيث ان من خلال تسليط الضوء على الأساليب التقنية والعمليات الحديثة الضرورية لمعينة مسرح الجريمة الإلكتروني بدءاً من لحظة الاكتشاف والحفظ، وصولاً إلى التحقيق الجنائي واستخراج الأدلة التي تضمن الحجة القانونية أمام القضاء. كما تبين هاته الدراسة ضرورة الموازنة بين فعالية التحقيق و حماية خصوصية الافراد مع التأكيد على أهمية تطوير القوانين لتواكب التقدم التكنولوجي اذ أن هذا النوع من الجرائم يعتمد اساسا على البرمجيات المعلوماتية و الادوات الالكترونية ايضا لا يغفل جانب نشر الوعي الإلكتروني مهم و فعال للحماية من الهجمات السيبرانية التي قد تمس ببياناتهم الحساسة أو اختراق حساباتهم .

الكلمات المفتاحية : الأدلة الرقمية، مسرح الجريمة، الأمن السيبراني، الأدلة الجنائية الرقمية، البرمجيات الخبيثة، التحقيقات، البروتوكولات، البيانات الوصفية، المقبولية، أدوات التحقيق .

List of Acronyms

IOT : Internet of things

TCP : Transmission Control Protocol.

IP : Internet Protocol

UDP : User Datagram Protocol

OS : Operation System

LAN: Local Area Network

DNS : Domain Name Service

FTP; File Transfer Protocol

NAS : Network Attached Storage

SAN : Storage Area Network

RAS : Remote Access System

DHCP : Dynamic Host Configuration Protocol

IaaS : Infrastructure as a Service

PaaS : Platform as a Service

SaaS : Software as a Service

NFATs : Network Forensic Analysis Tools

ICT : Information and Communication Technologies

NIST : The National Institute of Standards and Technologies

DoS : Denial of Service

2FA : Two-Factor Authentication

SMTP : Simple Mail Transfer Protocol

GENERAL INTRODUCTION

The Digital Crime Scene is the virtual space where illegal activities are committed using modern technological means. Crime is no longer limited to the physical and tangible, but has extended to include data, servers, and technological clouds, creating a hidden and complex environment that requires special tools and methodologies to deal with it in order to extract the evidence within it.

This research falls within the specialization of Law and Criminology, as it focuses on the procedural and technical aspects of digital forensic investigation. The research addresses the crime scene from the moment of its discovery, through the search and inspection processes, leading to the extraction of digital evidence and its presentation to judicial authorities, while taking into account legal guarantees.

It aims to shed light on the correct operational procedures in the digital crime scene and clarify how to maintain the integrity of digital evidence from damage or alteration (due to its fragile nature) to ensure its legal admissibility before courts as a reliable material evidence. Furthermore, among the research purposes is to raise public awareness of the necessity of understanding the nature of cybercrimes and their danger to their data and personal information, so they do not fall into such problems or be exposed to electronic attacks that may cost them the loss of their money or sensitive personal data.

To achieve the objectives of the study, the descriptive-analytical approach was adopted, by describing the nature and characteristics of the digital crime scene, and analyzing the technical and legal procedures followed in dealing with the devices and data under investigation.

The reason for choosing this topic is due to the widespread prevalence of cybercrime and the increasing reliance on digital evidence in proving contemporary crimes, as well as traditional crimes that can be proven through digital evidence. The scientific passion for understanding modern techniques achieved in accordance with developments in the technological world, as well as the massive use of these means by individuals, has necessitated the tightening of their oversight and the development of laws to make them flexible and appropriate for time and place, as well as spreading electronic awareness in various fields.

The crime scene has undergone a massive evolution; whereas the traditional crime scene was confined to a specific geographical location relying on Locard's principle of physical exchange, the total reliance on cloud computing and the Internet of Things (IoT) has led to the emergence of national electronic crime scenes—some tangible and others intangible—as well as intangible, cross-border crime scenes. This historical transformation has forced security and judicial authorities to develop their methods from visual inspection to technical examination and forensic data analysis. This is a modern science that emerged with the development of electronic equipment (computers, the internet, and phones).

The research question designed for this research is What is the conceptual framework of the digital crime scene, and to what extent do operational and technical procedures in examining the digital crime scene contribute to obtaining sound and secure digital evidence ?

- What is the Digital Crime Scene ?
- Has Digital Evidence become an admissible proof before the judiciary ?
- What are the technical challenges faced in investigating a digital crime scene. ?
- What are the methods in investigation, tools and types of digital crimes ?

In this research, we adopted a twofold plan consisting of **Chapter 1** : The Theoretical and Technical Framework of the Digital Crime Scene The following elements were addressed The Legal and Technical Definition of The Digital Crime Scene, Types of Digital Environments, The Legal Admissibility of Digital Evidence and Challenges in Digital Crime Scene . The second **Chapter** Operational Procedures in The Digital Crime Scene, Privacy in The search and Investigation of Digital Evidence, The digital forensic Process, Internet Forensics and Investigation Methods for Collecting Digital Evidence.

CHAPTER ONE

The Theoretical and Technical Framework of the Digital Crime Scene

Chapter one : The Theoretical and Technical Framework of the Digital Crime Scene

The physical world is no longer the sole arena for illicit activities. The heavy reliance on modern technologies ranging from cloud computing to the Internet of Things (IoT) has led to the emergence of the 'digital crime scene' as a complex, invisible environment that necessitates tools and methodologies fundamentally different from traditional forensic approaches.

A digital crime scene is a logical space comprised of data streams, server logs, and traces residual in volatile device memory. Therefore, this chapter holds critical importance in establishing the theoretical and technical framework governing the handling of such evidence. Understanding the nature of digital evidence—being volatile, easily manipulated, and multidimensional is the fundamental first step toward ensuring its legal integrity and evidentiary value before the judiciary.

This chapter aims to shed light on the core concepts of cybercrime and to deconstruct the technical architecture of the digital crime scene. It focuses on the fundamental principles of digital forensics, spanning from the identification of the digital crime scene and digital artifacts, through the processes of data collection and preservation, down to analysis conducted in a manner that ensures the integrity and reliability of the evidence.

Approaching the digital landscape requires a precise balance between deep technical expertise and strict adherence to legal standards, ensuring that the truth we extract from 'bits' of data remains robust as compelling evidence in the face of evolving technical and legal challenges.

1.1 The Legal and Technical Definition of The Digital Crime Scene.

With the rapid pace of digital transformation and the deep integration of information technology into every aspect of modern life, geographical boundaries are no longer the sole determinant of criminal activity. A complex virtual environment has emerged, serving as a fertile ground for novel patterns of crime. This qualitative shift in the nature of crime has imposed significant challenges on law enforcement agencies, most notably concerning the concept of the 'crime scene,' which has transitioned from a tangible, physical space to an invisible, digital realm characterized by fluidity and vastness.

Defining the nature of the cybercrime scene is not limited to technical or forensic aspects, but also extends to legal considerations. And the history of the emergence of this science, beginning from the traditional crime scene, until the evolution of events and the development of technologies, leading up to the technical crime scene. This necessitates redefining the criminal scene as a connected electronic space where parties interact and leave behind digital traces that constitute the backbone of modern criminal investigation.

1.1.1 The Legal Definition of The Digital Crime Scene

The digital crime scene also referred to as Cyberlaw is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", the Internet. It is less a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, law of torts, privacy, constitutional law and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet.¹

Scene of Investigation : It is the virtual, digital, scene where data resides and moves within the computer environment and its networks, in its memory and the hard drives contained therein. In this case, the investigation must only be conducted by an IT specialist."²

We point out at the beginning that there is no unified legal term to denote the criminal phenomenon emerging in the computer environment, and subsequently in the network environment. These terms have varied, as this variation accompanied the emergence and development of the phenomenon of information technology-related crime, starting from the term computer misuse, passing through 'information crimes, white-collar crimes, to 'hackers' crimes, then computer and internet crimes, and finally reaching Cybercrime.

Regardless of the designations, what is agreed upon globally and locally is the gravity of these crimes and their negative impact on the security and stability of societies in all developed and developing countries alike. Like all new discoveries that open doors and horizons and push the wheel of progress and prosperity forward on one hand, they open other doors to crime in its various forms on the other.³

We observe that the Algerian legislator did not limit itself to defining the electronic crime scene specifically, but rather addressed in Article 2 of Law No. 09-04 some definitions related to crimes connected to information and communication technologies, including Information System: any isolated system or group of interconnected or related systems, one or more of which performs an automated processing of data in execution of a specific program, which brings us closer to the concept of the electronic crime scene⁴.

¹ Prashant Mali ,Cyber law& Cybercrimes , Foreword by Justice Rajesh Tandon EX- chairman cyber regulations appellate Tribunal of India , First Edition 2012,p 1-2.

² ايت حمودة كاهنة، البحث و التحري الجنائي في مسرح الجريمة الالكترونية ، جامعة حسيبة بن بوعلي، الشلف ، مجلة

الفكر القانوني و السياسي، المجلد السابع العدد الاول (2023) ، تاريخ نشر المقال 2023/05/15، ص187

³ عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير،كلية

الاسكندرية، مصر ، 2009، ص11.

⁴ Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 5août 2009 portant règles particulières relative la prévention et à la lutte contre les infraction liées aux technologies de l'information et de la communication, JOURNAL OFFICIEL DE LA REPUBLIQUE ALGERIENNE N° 47,16aout 2009.

1.1.2 The Technical definition of The Digital crime scene .

In any case, one of the first tasks lies with defining the scene - a crime scene is any physical scene, anywhere, that may provide potential evidence to an investigator in which digital evidence types may reside. The typical crime scene is a physical, tangible environment where many evidence types including digital devices may exist. Many of those in an investigative role will likely be content with their understanding of this environment having likely spent much time training in this context. In comparison, the so-called 'digital crime scene is one which exists in a digital realm, described upon physical digital devices which themselves may both be present at a physical crime scene in which a first responder is in attendance, and also in environments which extend beyond this locality. In any given crime scene, one or more digital crime scenes may exist, and these may stretch beyond what could be considered the physical boundaries of a traditional crime scene (see fig. 1)¹

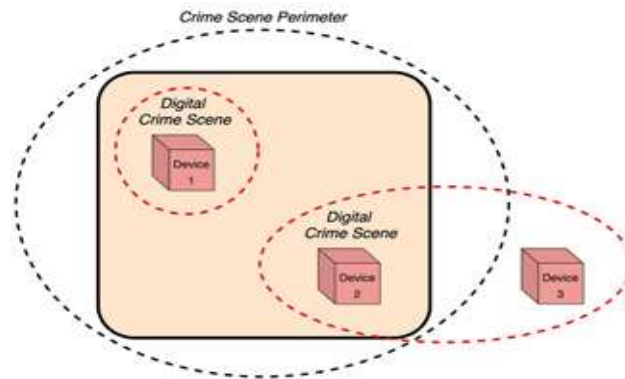


Fig. 1 : digital crime scene within crime scene

A computer being investigated can be considered a digital crime scene and investigated as a subset of the physical crime scene where it is located . Physical evidence may exist around a server that was attacked by an employee and usage evidence may exist around a home computer that contains contraband. Furthermore, the end goal of most digital investigations is to identify a person who is responsible and therefore the digital investigation needs to be tied to a physical investigation.²

Digital forensics is the application of forensic science to electronic evidence in a legal matter.

While there are many different subdisciplines and many types of devices, communication, and storage methods around today, the basic tenets of digital forensics apply to all of them.

These tenets encompass four areas:

¹ **Graeme Horsman**, Digital evidence and the crime scene , School of health and life sciences, Teesside University, Middlesbrough, Tees Valley, United Kingdom, science&justice 61 (2021) 761-770, p 762.

² **BrianD. Carrier, M.S. and Eugene H. Spafford,Ph.D**, Defining Event Reconstruction of Digital Crime Scenes, J forensic Sci, Nov.2004, Vol.49, No. 6, p 1.

- Acquisition.
- Preservation.
- Analysis.
- Presentation.

Each of these areas includes specific forensic processes and procedures.¹

1.2 Types of Digital Environments

The challenge of the admissibility of digital evidence cannot be approached in isolation from understanding the structural nature of the environments that generate it. Cyberspace is not a monolithic entity, but rather a collection of diverse environments that differ in their technical architecture, communication protocols, and data storage methods.

1.2.1 The Internet of Things (IOT)

IoT is a digital connection of devices and objects that are embedded with the internet, sensors, and intelligence for establishing communication with people or other IoT-based objects.²

The Internet of Things (IoT) refers to the network of physical objects, It is fast growing and already has billions of devices connected. This is different from the current Internet, which is largely a network of computers, including phones and tablets.

The things in the IoT can be anything from household appliances, machines, goods, buildings, and vehicles to people, animals, and plants. With the IoT, all the physical objects are interconnected, capable of exchanging data with each other without human intervention. They can be accessed and controlled remotely. This is going to completely transform our lives—it will be truly revolutionary. like Smart Watches, Gaming Consoles, Drones, Smart TV, Home kits/Smart Speakers.³

1.2.2 Protocols

1.2.2.1 TCP/IP

While there are many different types of network protocols in use throughout the world, the TCP/IP Transmission Control Protocol/Internet Protocol suite of protocols forms the most popular network protocol currently in use. Although this is partially due to the fact that the Internet is based on it, TCP/IP has solidified its place as the protocol of choice for corporate networks because most operating systems support this protocol. It can also be used on any topology for example, Ethernet, Token Ring, and so on.

This fact becomes very useful when you are trying to network different types of systems to one another for example, Microsoft Windows computers and devices, Apple computers and

¹ **Larry Daniel, Lars Daniel**, Digital Forensics For Legal Professionals, 2012, USA, p 11.

² **Vibha Soni**, IOT for Beginners, FIRST EDITION, 2022, India. p 8.

³ **Perry Xiao**, Designing Embedded Systems and the internet of things (IoT) with the ARM Mbed, London south Bank University, first edition, 2018, UK, p 23.

devices, and Linux computers and devices. In addition, TCP/IP is a routable protocol, so its packets can be transferred across many different types of networks before they reach their final destination.

The U.S. Department of Defense originally developed the TCP/IP protocol as a hacker-resistant, secure protocol for transmitting data across a network. It is considered to be one of the most secure of the network protocols. In addition, because the U.S. government developed it, no one actually owns the TCP/IP protocol, and so it was adopted as the transmission standard for the Internet.¹

No matter what type of computer platform or software is being used, information must move across the Internet in the form of TCP/IP packets. This protocol calls for data to be grouped together in bundles called network packets.

The TCP/IP packet is designed primarily to allow for message fragmentation and reassembly. It exists through two header fields, the IP header and the TCP header, followed by the data field²

1.2.2.2 UDP (User Datagram Protocol)

Where TCP offers a connection-oriented service, the User Datagram Protocol (UDP) is connectionless. This means that there is no establishment of a connection and no tracking at the operating system of the communication between the two systems. Every communication message is done as a one-off. At the operating system level, there is no tracking. Messages are sent and promptly forgotten. By this, I mean that the network stack within the operating system kernel, the core of the operating system, handles UDP and TCP messages. If any tracking is done, it can be done within the application.³

You may be wondering, if TCP offers guaranteed delivery and sequencing and all the other goodness it has to offer, why would anyone have any use for UDP? In reality, there are a lot of uses for UDP. UDP is fast and lightweight. It has little in the way of overhead and you don't have to wait for a connection to be established before you send a message along. Once the application has prepared a message, it's out the door. Any application that is concerned with speed, like streaming video, will want to use UDP. If you are streaming video, you don't want to be hung up waiting for a particular segment to arrive if there is out-of-order delivery. With UDP, you send it on its way; if one or two datagrams are dropped or lost or arrive out of order, they are simply discarded or forgotten. You likely won't miss them at all. Waiting for them would cause a jarring experience for watching or listening. Trying to insert out-of-order messages into the stream when they arrive would be similarly jarring, though for different reasons. As a result, UDP is best for any application that needs real-time transmission capabilities.

¹ Charles J.Brooks,et al , CYBERSECURITY ESSENTIALS, 2018, CANADA, p 299 .

² Charles J.Brooks,et al , op.cit p 299 .

³ Ric Messier, NETWORK FORENSICS, 2017, Canada,p 38.

Because the protocol itself doesn't do a lot other than offer a means of transport and multiplexing, the headers are very simple. This also helps with speed because fewer bytes, even if it's not all that many fewer for each datagram, means it can get to the recipient much faster and requires less processing on the receiving end.¹

1.2.3 Network Servers

Server-type computer equipment provides service to other client computers. We can find them mainly in business environments performing functions of a file server, mail, web services, database, user management, etc.²

All servers perform the basic functions we've described so far; however, in practice they may vary significantly in the primary application they perform for the network's clients. The following list describes some of the various implementations found in different types of networking environments:

- ❖ General-purpose servers are employed in most small businesses for multiple purposes such as handling departmental email and providing file, print, and web services running on standard network operating systems.
- ❖ Appliance servers are specialized servers that provide specifically bundled hardware and software components. This makes for relatively easy installation and administration.
- ❖ Application servers run programs accessed by multiple users, and they often interact with informational databases.
- ❖ Mail servers are client/server types of application servers used to receive and store electronic mail messages in private mailboxes, even when users are not actually logged directly on to the network.
- ❖ Firewall servers control the connections between two networks, such as acting as an Internet gateway, where access control blocks unwanted traffic while allowing acceptable communications.
- ❖ Proxy servers act as intermediaries between network computers and the Internet.
- ❖ Web servers host web pages for intranet and/or Internet access and can be configured to host more than one site, depending on the server's underlying OS.
- ❖ Database servers are used to store and process data in response to client queries, where organizations must manage large quantities of data.
- ❖ Terminal servers are special-purpose computers fitted with multi-ported asynchronous modem connections, as well as ports designed to interface with host machines acting as terminals on one side and with a LAN, on the other side.
- ❖ DNS (Domain Name Service) servers contain database listings used to resolve human-readable computer names to IP addresses.
- ❖ Gateway servers provide interfacing between different types of networks, protocols, or mechanisms to provide access to another system.

¹ Ric Messier, op. cit ,pp 38-39.

² INTERPOL, Guidelines For Digital Forensics First responders, march 2021, p 31.

- ❖ Router servers manage the shared resources of all other routers in the network, as well as the various transmission speeds and different protocols being used within an organization's network.
- ❖ Bridge servers use multiple network interfaces to connect groups of computers. They translate between protocols and help to reduce network traffic.
- ❖ FTP (file Transfer Protocol) servers transfer files across the Internet, an extranet, or an intranet through the use of FTP client software.
- ❖ NAS (Network Attached Storage) servers move storage out from behind the file server and put it directly on the transport network, permitting any network user with access rights to directly access stored NAS data.
- ❖ SAN (Storage Area Network) servers operate in enterprise storage environments with disk array controllers and tape libraries attached. They are capable of providing large-scale data protection and , retrieval.
- ❖ RAS (Remote Access System) servers allow clients to dial in to a computer from a remote site, even if they are not connected to a LAN.
- ❖ Print servers help to decrease the administrative and management workload by streamlining both local and remote printer control.
- ❖ DHCP (Dynamic Host Configuration Protocol) servers are used to temporarily assign dynamic IP addresses to both network workstations and Internet clients.¹

1.2.4 Metadata

Metadata can be a veritable gold mine of useful information in a case. The prefix meta in English is used to express the idea that some information is about its own category. Hence the meaning of metadata is data about data, just as metacognition means knowing about knowing. While this might seem somewhat cryptic, when you get down to the nuts and bolts, metadata is not hard to understand in principle, but can be confusing in detail. Metadata can be found inside a file, kind of behind the scenes where an ordinary computer user will not see it, or in an external data store such as Internet history files that record information about files.

The information stored within metadata can be used to build timelines, establish alibis, and so much more. In the hands of a skilled digital forensics expert, metadata can shed light on a particular issue in a case, or it can be the turning point altogether.

In many cases, tiny snippets of metadata can change how entire sequences of events are interpreted. However, a word of caution about metadata: Metadata alone, like any snippet of digital evidence. is rarely enough to "prove" something. Nearly all digital evidence requires some type of corroboration through a combination of evidence. electronic or otherwise. Relying on a single piece of electronic evidence can lead to misunderstandings without properly establishing a foundation for that evidence.

¹ Charles J.Brooks,et al, op.cit , pp 328 329 230.

1.2.4.1 THE PURPOSE OF METADATA

The purpose of metadata is to store information about other data. This can help with the organization and retrieval of data. For instance, web pages on the Internet have metadata in such forms as meta-tags. A meta-tag is coded into a website where you do not see it, but it contains information about a website, such as keywords so that it can be easily found when those keywords match your Google search. Metadata can also be found inside many pictures and videos, containing copyright information if there is any, as well as information such as when the picture was taken and the make and model of the camera the picture was taken with. Or, as in the case of office documents, when searching for a document in Microsoft Windows, you can choose to search for documents by the author, the creation date, the last modified date, and so forth. All of this information is contained in the document's metadata.

1.2.4.2 COMMON TYPES OF METADATA

In the following sections, the more common types of metadata are discussed as well as where the metadata can be found and how it is used as evidence.

A- File system metadata

File system metadata includes the times recorded by the operating system when a file is modified, accessed, or created. File system metadata is easily misinterpreted and can be very difficult to understand.¹

B- Internet metadata

There are two types of Internet metadata:

- ❖ Web page
- ❖ Browser metadata

1- Web page metadata

Metadata for web pages is contained within the "code" of the web page and is in the form of meta-tags, page titles, page headers, and meta-descriptions. While this type of metadata can be interesting, it is almost entirely controlled by the user who creates the web page and rarely offers very much in the way of forensic value.

The original purpose of web page metadata was to assist search engines such as Yahoo or Google in finding and indexing web pages. However, widespread abuse of meta-tags, keywords, and meta-descriptions has resulted in modern search engines largely ignoring this metadata in favor of actual page content.

If you examine the web page metadata, you will notice that what the metadata does not contain is any information about when, where, or by whom the web page was created. This web page could have been created on a computer and never published to the web. If this is

¹ Larry Daniel, Lars Daniel, op. cit, pp 179-180.

the only evidence you have, you have no evidence at all. This is why web page metadata is of limited value in a forensic examination.

2- Browser metadata

While it is not commonly referred to as metadata, the history stored by Internet browsing programs certainly qualifies as data about websites and pages that have been visited, and websites or pages marked as favorites by the user. Browser meta-data is used extensively as forensic evidence in all kinds of cases.

C- Document metadata

Document metadata is metadata stored inside a document that provides information about the authorship, editing time, and even the computer on which the document was created. All of the major office suites such as Microsoft Office, WordPerfect Office, OpenOffice, and Star Office record metadata in some form inside the word processing documents, spreadsheets, and presentations created with the programs in these suites.

D- Picture metadata

Picture metadata can contain information about the make and model of the camera used to take the picture or about the software used to modify a picture. you will see the image was modified using Adobe Photoshop CS. When a photo has been modified using a program like Adobe Photoshop, the original camera information can be lost. However, the metadata will contain the name of the editing program that was used to modify the picture.¹

1.2.5 Cloud Computing

Here is the National Institute of Standards and Technology (NIST) working definition:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources e.g., networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models.²

The five essential characteristics are:

- ❖ On-Demand Self-service
- ❖ Broad Network Access
- ❖ Resource Pooling
- ❖ Rapid Elasticity

¹ **Larry Daniel, Lars Daniel**, op. cit, pp 180-181-182-183.

² **Peter Mell, Timothy Grance**, The NIST Definition of Cloud Computing, Special publication 800-145, september 2011, USA, p 2.

- ❖ Measured Service

The three delivery models are:

- ❖ Infrastructure as a Service (IaaS)
- ❖ Platform as a Service (PaaS)
- ❖ Software as a Service (SaaS)

The four deployment models are:

- ❖ Public Cloud
- ❖ Private Cloud
- ❖ Hybrid Cloud
- ❖ Community Cloud

Cloud computing is the IT foundation for cloud services and it consists of technologies that enable cloud services.¹

1.3 The Legal Admissibility of Digital Evidence

In recent times, amid rapid technological advancements, digital evidence has emerged as an indispensable cornerstone of the contemporary evidentiary system. Given its inherent nature—characterized by speed, abstraction, and susceptibility to alteration—digital evidence has imposed a dual legal and technical challenge on legislators and the judiciary alike. The legal admissibility probative value of digital evidence lies not merely in its status as a novel means of proof, but in its fragile nature, which necessitates rigorous standards to ensure its reliability and integrity.

1.3.1 Definition of Digital Evidence

Digital evidence can be described as information of probative value stored or transmitted in a binary format that can or may be relied on in the court of law.

The birth of digital communication and technology has helped to remove a lot of obstacles in the traditional method of evidence collection and the conventional media associated with it, although the emergence of the internet, social media, and the mobile technology has changed our way of living and business.²

¹ Vivek Kale, *Creating Smart Enterprises*, 2018, New York, USA, p 142.

² Elizabeth Ozioma Edward, Joseph A. Ojeniyi, *A Systematic literature review on digital evidence admissibility: methodology, challenges, and research directions*, ICECCO 2019, Department of cybersecurity science Federal University of technology minna, Nigeria. p 1.

1.3.2 Need for the admissibility of digital evidence

The majority of crimes currently have a digital component; this duplicates the quantity of digital evidence stored for an estimated period of 18 to 24 months. Governments and police are required by law to preserve digital evidence for a case's history, often indefinitely. Until the presentation of the digital evidence in court, the evidence must be collected, preserved and properly distributed. The systems currently used often involve multiple steps that do not meet the demands of the growing digital world. The volume of digital evidence continues to grow, and these tasks will soon become operationally and economically unfeasible for the agencies responsible for performing these tasks .

Consequently, electronic discovery continues to grow in the legal community. There is an aspect that largely continues to elude the mainstream consciousness. That is the reason behind the need for the long-term preservation of digital evidence.

Most users have the criterion that, because of their easy reproducibility, digital information, in contrast to analogue information, has an unlimited life. Unfortunately, this defining criterion of digital documents tends to blind users regarding their real world transience and vulnerability. Because of the rapid development of technology and the evolution of the rules that continuously require a relentless and substantial input of time, manpower, and funds to safeguard digital data and its preservation, digital evidence requires more attention than other media.

Computer forensics involves four key elements: identification, preservation, analysis, and presentation of digital evidence, The preservation is concerned with ensuring evidential data remains unchanged or changed as little as possible.¹

1.3.3 Increasing Awareness of Digital Evidence

By now it is well known that attorneys and police are encountering progressively more digital evidence in their work. Less obviously, computer security professionals and military decision makers are concerned with digital evidence. An increasing number of organizations are faced with the necessity of collecting evidence on their networks in response to incidents such as computer intrusions, fraud, intellectual property theft, child pornography, stalking, sexual harassment, and even violent crimes.

More organizations are considering legal remedies when criminals target them and are giving more attention to handling digital evidence in a way that will hold up in court. Also, by processing digital evidence properly, organizations are protecting themselves against liabilities such as invasion of privacy and unfair dismissal claims. As a result, there are rising expectations that computer security professionals have training and knowledge related to digital evidence handling.

¹ **Fernando Molina Granja, Glen D. Rodríguez Rafael**, The preservation of digital evidence and its admissibility in the court, J. Electronic Security and Digital Forensics, vol. 9, No. 1, 2017, Peru, pp 7 8.

Balancing thoroughness with haste is a demanding challenge. Tools that are designed for detecting malicious activity on computer networks are rarely designed with evidence collection in mind. Some organizations are attempting to address this disparity by retrofitting their existing systems to address authentication issues that arise in court. Other organizations

are implementing additional systems specifically designed to secure digital evidence, popularly called Network Forensic Analysis Tools (NFATs). Both approaches have shortcomings that will be addressed gradually as software designers become more familiar with issues relating to digital evidence.¹

1.3.4 Admissibility

For digital evidence to be admissible, the investigation must be lawful, carried out under the authorization of judicial authorities; otherwise, the proceedings shall be deemed null and void, even if the evidence itself is conclusive. The omission of any mandatory procedural step renders the evidence inadmissible before the court.

The Code of Criminal Procedure, under the section concerning 'the interception of correspondence, recording of audio, and capturing of images' for specific crimes—including those related to Information and Communication Technologies (ICT)—stipulates that the competent Public Prosecutor may authorize the interception of correspondence conducted via wired or wireless communication means. This includes implementing technical arrangements, without the consent of the individuals concerned, to capture, fix, transmit, or record speech uttered privately or confidentially by one or more persons in private or public places, or to capture images of one or more persons in a private location . Such authorization is granted for a maximum period of four months, renewable under the same formal and temporal conditions until the requirements of the investigation or judicial inquiry are met .²

Regarding searches, Law No. 09-04, in Article 6, provides that searches are subject to the provisions of the Code of Criminal Procedure. However, it specifies certain instances where searches may be conducted, even remotely, for:

- a) An information system or a part thereof, as well as the data stored therein.
- b) An information storage system.

In the case provided for in paragraph 'a' of this article, if there are reasonable grounds to believe that the data being sought is stored in another information system and can be accessed from the first system, the search may be promptly extended to that system or part thereof, provided that the competent judicial authority is notified in advance.

¹ **Eoghan Casey**, Digital Evidence and computer crime : Forensic Science, Computers, and the Internet, Second Edition, 2004, USA, p 19

² **Loi n° 25-14** du 9 Safar 1447 correspondant au 3 août 2025 portant code de procédure pénale, JOURNAL OFFICIEL DE LA REPUBLIQUE ALGERIENNE N° 54, 13 août 2025, Art 114-116.

If it is determined beforehand that the data being sought, which can be accessed from the first system, is stored in an information system located outside the national territory, it must be obtained with the assistance of the competent foreign authorities, in accordance with relevant international agreements and the principle of reciprocity.

The authorities in charge of the search may enlist any person who has expertise in the operation of the information system under investigation or in the measures taken to protect the stored data, in order to assist them and provide all necessary information to fulfill their mission.¹

1.3.5 Authenticity and Reliability

The process of determining whether evidence is worthy is called authentication.

Authentication means satisfying the court that (a) the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or via technological features in the system or the record.

Authentication is actually a two-step process, with an initial examination of the evidence to determine that it is what its proponent claims and, later, a closer analysis to determine its probative value. In the initial stage, it may be sufficient for an individual who is familiar with the digital evidence to testify to its authenticity. For instance, the individual who collected the evidence can confirm that the evidence presented in court is the same as when it was collected. Alternately, a system administrator can testify that log files presented in court originated from her/his system.²

1.3.6 Casey's Certainty Scale

Computers can introduce errors and uncertainty in various ways, making it difficult to assess the trustworthiness of digital evidence meaningfully. Although courts are warned to consider the computer systems involved carefully, little guidance is provided.

Business records that are generated by computers present structural questions of reliability that transcend the reliability of the underlying information that is entered into the computer. Computer machinery may make errors because of malfunctioning of hardware, the computer's mechanical apparatus. Computers may also make errors that arise out of defects in the software, the input procedures, the database, and the processing program. In view of the complex nature of the operation of computers, courts have been cautioned to take special care to be certain that the foundation is sufficient to warrant a finding of trustworthiness and

¹ Loi n° 09-04, op. cit, Art 06.

² Eoghan Casey, op.cit p 156.

that the opposing party has full opportunity to inquire into the process by which information is fed into the computer.

Computer networks complicate reliability considerations because multiple systems and mechanisms are involved. Possibly because of the complexity and multiplicity of computer systems, there is a lack of consistency in the way that the reliability of digital evidence is assessed. To improve our ability to assess the reliability of digital evidence, we need a consistent method of referring to the relative certainty of different types of digital evidence.

1.3.7 Best Evidence

When dealing with the contents of a writing, recording, or photograph courts sometimes require the origin a evidence. This was originally intended to prevent a witness from misrepresenting such materials by simply accepting their testimony regarding the contents. With the advent of photocopiers, scanners, computers, and other technology that can create effectively identical duplicates, copies became acceptable in place of the original, unless a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances it would be unfair to admit the copy in lieu of the original Best Evidence Rule.

Because an exact duplicate of most forms of digital evidence can be made, a copy is generally acceptable. In fact, presenting a copy of digital evidence is usually more desirable because it eliminates the risk that the original will be accidentally altered. Even a paper printout of a digital document may be considered equivalent to the original unless important portions of the original are not visible in printed form. For example, a printed Microsoft Word document does not show all of the data embedded within the original file such as edits and notes.¹

1.3.8 Scientific Evidence

In addition to challenging the admissibility of digital evidence directly, tools and techniques used to process digital evidence have been challenged by evaluating them as scientific evidence. Because of the power of science to persuade, courts are careful to assess the validity of a scientific process before accepting Its results.

If scientific process is found to be questionable, this may influence the admissibility or weight of the evidence, depending on the situation.

In the United States, scientific evidence is evaluated using four criteria developed in *Daubert v. Merrell Dow Pharmaceuticals*, 1993. These criteria are:

- ❖ whether the theory or technique can be and has been tested.
- ❖ whether there is a high known or potential rate of error, and the existence and maintenance of standards controlling the technique's operation.
- ❖ whether the theory or technique has been subjected to peer review and publication.

¹ Eoghan Casey, op.cit Pp 159 163.

- ❖ Whether the theory or technique enjoys "general acceptance within the relevant scientific community.

Thus far, digital evidence processing tools and techniques have withstood scrutiny when evaluated as scientific evidence. However, testing techniques or tools and determining error rates is challenging, not just in the digital realm. Although many types of forensic examinations have been evaluated using the criteria set out in Daubert, the testing methods have been weak. "The issue is not whether a particular approach has been tested, but whether the sort of testing that has taken place could pass muster in a court of science." Also, error rates have not been established for most types of forensic examinations, largely because there are no good mechanisms in place for determining error rates. Fingerprinting, for example, has undergone recent controversy. Although the underlying concepts are quite reliable, in practice, there is much room for error. Therefore, errors are not simply caused by flaws in underlying theory but also in its application. This problem applies to the digital realm and can be addressed with increased standards and training.

One approach to validating tools is to examine the source code. However, as noted earlier, many commercial developers are unwilling to disclose this information. When the source code is not available, another form of validation is performed - verifying the results by examining evidence using another tool to ensure that the same results are obtained. Formal testing is being performed by the National Institute of Standards and Technology (NIST) and some organizations and individuals perform informal tests. However, given the rate at which computer technology is changing, it is difficult for testers to keep pace and establish error rates for the various tools and systems. Additionally, tool testing does not account for errors introduced by digital investigators through misapplication or misinterpretation. Therefore, the most effective approach to validating results and establishing error rates is through peer review - that is to have another digital investigator double check findings using multiple tools to ensure that the results are reliable and repeatable.¹

1.3.9 The probative value of digital evidence under Algerian legislation

The Algerian legislator has permitted the proof of crimes by any means of evidence, with the exception of those crimes for which the law specifically requires a particular type of evidence. Upon reviewing Law No. 09-04, which outlines the specific rules for the prevention and combatting of crimes related to information and communication technologies (ICT), we find it devoid of any specific provisions regarding the probative value of digital evidence. This silence by the Algerian legislator is interpreted as subjecting digital evidence to the same general rules as all other forms of evidence.

¹ Eoghan Casey, op.cit p 168

Regarding the admissibility of digital evidence before the judiciary, the judge is governed by the principle of personal conviction intime conviction regarding the evidence presented, and possesses full discretionary power to evaluate such evidence.¹

When discussing evidence in cybercrimes, the Algerian legislator has addressed this in the new Code of Criminal Procedure, Law No. 25-14, under Article 349, which stipulates that cybercrimes may be proven by any means of evidence, except those prohibited by law. Furthermore, the judge may render a verdict based on their own personal conviction. As previously mentioned, the judge has absolute freedom in assessing the evidence and forms their personal conviction based on the discussions and pleadings presented before them in court.²

1.4 Challenges in digital crime scene

One of the major challenges in digital forensics today is the massive volume of unstructured data, which often contains inherent uncertainties and errors. These pose a significant barrier for investigators attempting to establish the authenticity of digital evidence for presentation in court as definitive proof to substantiate the facts attributed to offenders. Under this heading, we will discuss some of the challenges encountered by the digital investigator.

1.4.1 challenges in digital forensics

1.4.1.1 IoT Security Challenges

The evaluation of IoT from limited access networks to a distributed public network increased the needs for security alarms to protect interconnected IoT devices from intrusions such as data modifications, malicious code injection, sniffing, and Denial of Service (DoS) and many other threats . SonicWall reported that IoT malware attacks increased 215.7% to 32.7 million in 2018 compared to 10.3 million in 2017.

The first two quarters of 2019 exceeded 55% in the first two quarters of 2018. If this rate continues, it will be another record year for IoT malware attacks . highlighted that though there are existing technologies and protocols dealing with issues of threats to security,

the limitations on the IoT devices and network prevents a straightforward adaptation and implementation of IoT solutions in the new arising sets of security scenarios.

¹ براهيمى جمال، التحقيق الجنائي في الجرائم الالكترونية، اطروحة نيل شهادة الدكتوراه، جامعة مولود معمري - تيزي وزو، الجزائر، ص176.

² Loi n° 25-14, op.cit, art 349 .

At present, the adopted security protocol and cryptographic setting requires a lot of resources and IoT devices such as smartphones, tablets, PCs, routers, active sensors or passive RFID tags, have very limited resources and capabilities to support the implementation and adaptation of traditional security protocols solutions.

the implementation and adaptation of traditional security protocols solutions still remain as a challenge making it difficult to provide confidentiality of data transmission. Since unattended IoT devices are not supervised because they operate in a self-support manner with limited maintenance this further leads to concern in terms of data integrity trust. As a result, the data obtained from IoT devices is likely to be of low quality or corrupted .

There are various security challenges and limitations related to IoT. which are affecting large scale adoption. In this section, these challenges and limitations have been discussed in detail:

A- Privacy

User privacy and data protection is an important issue in IoT security taking into consideration the ubiquitous characteristics of the IoT environment. The ability of the IoT sensors and devices to sense, collect and transmit data over the internet pose a threat to individuals' privacy. IoT nodes are known to collect people's private data without them even noticing. although an abundance of research has already been proposed with respect to privacy, many topics still need further investigation.

According to a report by Aaron , Nest thermostat which is one of the most secure IoT devices, can be hacked and controlled while the device boots up.

Hackers can load their custom software onto it which would stop Thermostat data from being sent back to Nest's servers . The compromised Nest Thermostat will then act as a jumping off point to take control of other devices in a home which allows hackers to access sensitive information about people such as their presence in the house or their sleeping schedule.

smart device apps can also be as vulnerable as the device itself. A study by security research team at Checkmarx showed how attackers bypass user permissions and take control of Google and Samsung camera apps. Attackers are able to remotely take photos, record video, spy on conversations, identify people's location, and more .¹

¹ **T.Janarthanan, et al**, IOT Forensics: An Overview of the Current Issue and Challenges,Sheffield Hallam University, Sheffield, England, p 229.

B- Authentication

The identification and authentication of objects could be challenging because of the nature of the IoT environment. It is essential to consider managing identity authentication in the IoT, as multiple users and devices need to authenticate each other through trustable services . In addition, efficient key deployment and key management is a challenge in IoT devices as it could cause overhead on IoT nodes. Moreover in the absence of a guaranteed Certificate Authority (CA), other mechanisms are required for validating cryptographic keys and ensuring integrity of key transfer.¹

C- Heterogeneity

IoT devices connected to different types of entities with varying capabilities complexity and vendors. These devices come with different configurations, dates, release versions and the use of technical interfaces which are designed for altogether different functions. Thus, the requirement to develop protocol to work with all the different devices is required , that one more challenge that must be considered in IoT is the dynamic environment, at one time a device might be connected to a completely different set of devices than in another time; thus to ensure security optimal cryptography system is needed with adequate key management and protocols.

D- Policies

Current policies that are implemented in computer and network security may not be applicable for IoT due to its heterogeneous and dynamic nature. Hence, there must be policies and standards developed to ensure that the data will be managed, protected and transmitted in an efficient way. This includes a mechanism to enforce such policies is needed to ensure that every entity is applying the standards. Similarly, for every IoT service involved a Service Level Agreement (SLAs) must be clearly identified to introduce trust by human users in the IoT environment which will further results in its growth and scalability .

Most of the technical security concerns are related to manufacturing standards. update management. physical hardening, user's knowledge and awareness . Weak and guessable default passwords, hardware issues, unpatched embedded operating systems and software, insecure data transfer and storage and Lack of encrypted firmware updates by companies could allow the device to be compromised. Many IoT devices have operational limitations such as low processing power and small memory which is just enough to perform the allocated tasks and they can't handle proper software updates.

Due to lack of awareness and user's ignorance, factory default passwords are usually forgotten to be changed. Some devices are set with a poor password which is easy to be breached for malicious purposes. Many well-known companies recently provide two-factor

¹ T.Janarthanan, et al, op.cit,pp 229-230.

authentication (2FA) to eliminate the risk of security challenges but still millions of IoT devices do not support this feature.

Changing factory default passwords, installing necessary updates, disable remote access to IoT devices when not needed, disable features that are not being used can also reduce the risk of being compromised. Wi-Fi networks are also one of the first points of security attacks which make the entire network vulnerable. Setting strong passwords and encryption methods for Wi-Fi networks, can mitigate the risk of security attacks.¹

1.4.1.2 Computational Forensics

A- Definition

The hypothesis-driven investigation of a specific forensic problem using computers, with the primary goal of discovery and advancement of forensic knowledge.²

Computational forensics works toward:

- ❖ In-depth understanding of a forensic discipline
- ❖ Evaluation of a particular scientific method basis
- ❖ Systematic approach to forensic sciences by applying techniques of computer science, applied mathematics, and statistics.

It involves modeling and computer simulation (synthesis) and/or computer-based analysis and recognition.

B- The Objectives of Computational Forensics

1- Large-Scale Investigations

Cybercrime investigations and investigations in large multinational corporations share the properties of large volumes of data from a wide range of sources. The ability to efficiently and effectively manage the data during the digital forensics process requires the application of computational methods.

Flaglien researched a method for automatic identification of malware traces across multiple computers, inspired by challenges from large-scale online bank fraud investigations. The objective of the research was to efficiently identify patterns in large, complex datasets using link-mining techniques, in a forensically sound fashion.

As part of a PhD project, Shalaginov researched the use of Neuro-Fuzzy (NF) methods based on large-scale network traffic analysis in digital forensics investigations. The purpose of the research was to identify patterns of benign and malicious activity in network traffic dumps through the use of NF algorithms, handling large-scale datasets with reduced classification model complexity. The research has been continued in several papers.

¹ T.Janarthanan, et al, op.cit,pp 230-231.

² André Årnes, Digital forensics, Norwegian University of technology and science, Norway, 2018, pp 313.

2- Automation

Digital forensics has to a large degree been dependent on manual processes, supported by checklists, process descriptions, and some built-in automation and scripting in forensic tools. There is, however, a need for more comprehensive automation in order to reduce manual efforts and increase the quality of digital forensics. As we have observed in this textbook, there is extensive potential for automation in all steps of the digital forensics process.

As an example, we studied a method for partial automation of the forensic reconstruction of computer intrusions . The research utilized a virtual environment to efficiently execute a repeatable forensic reconstruction experience, explained through two scenarios - The Trojan Did It! and A Multistep Attack.

In Fossen investigated a method for automating the geolocation of IP addresses, using triangulation based on multiple, geographically dispersed measurements. The prototype, referred to as GeoLocate, used the constraint-based geolocation (CBG) method and network Looking Glass services to estimate the location of an IP address in 1 to 2 minutes.¹

3- Analysis

The analysis of digital evidence can be significantly strengthened through computational methods. Whereas a human analyst can spot anomalies and patterns based on experience, computational methods can establish timelines, perform link analysis, and identify patterns in a predictable manner. Validated computational forensics methods will support human analysts in deducing conclusions based on evidence, in less time and with higher certainties.

As an example, investigated methods for the identification and extraction of cryptographic keys from volatile memory in computer devices.

A new method, interrogate, was implemented to allow for a higher success rate for forensic analysis, and the results demonstrated that the chances of locating forensic keys were surprisingly high.

Bjelland studied how approximate hash-based matching, also known as fuzzy hashing, could be used to identify complex and unstructured data that has a certain amount of byte-level similarity. The research resulted in several analysis and visualization tools and demonstrated that approximate hash-based matching has potential for helping investigators discover information based on data similarity.

As part of a completed PhD thesis project, Nguyen studied the effectiveness of intrusion detection by correlation feature selection (CFS), with the purpose of automatically obtaining a feature set for network traffic without involving expert knowledge The results successfully demonstrated the ability to remove redundant features while still keeping classification accuracies, leading to improved performance compared to other methods.

¹ André Årnes, Op.cit., pp 313-314 315 .

4- **Forensic Soundness**

Any method used for digital forensics must take forensic soundness into consideration.

Computational forensics must ensure that evidence integrity and chain of custody are built in, thus reducing the probability of both unintentional mistakes and intentional evidence tampering. In a similar fashion to automated testing for software quality assurance, forensic tool testing should be performed at all levels from source code validation to unit testing, functional verification, and last but not least software security testing.

1.4.1.3 Disciplines of Computational Forensics

- ❖ It should be further noted that the research area of computational forensics is not limited to digital evidence but also encompasses computational methods for other forensic disciplines. This includes, but is not limited to:
- ❖ Signal and image processing: Transforming signals and images for better human or machine processing.¹
- ❖ Computer vision: The automatic recognition of objects eg, face recognition and similarity to other known images in computer images or video.
- ❖ Computer graphics and data visualization: The synthesis of two-dimensional images or three-dimensional scenes from multidimensional data for better human understanding
- ❖ Statistical pattern recognition: The classification into one or more classes based on abstract measurements, identifying whether a sample belongs to a known class and with what probability.
- ❖ Machine learning: A mathematical model is learned from examples.
- ❖ Data mining: Large volumes of data are processed to discover nuggets of information e.g., the presence of association, number of clusters, and outliers.
- ❖ Robotics: Human movements are replicated by a machine, for example for the purpose of forensic reconstruction experiments.

1.4.1.4 Research Agenda

Digital forensics as a research field is constantly evolving with increasingly complex technologies. Consequently, there is a range of open questions that can be investigated.

As an inspiration, we include the research agenda from the Testimon Forensics Group:

Large-scale investigations: Research in the area of large-scale investigations; automatic searching through terabytes of electronic storage within closed systems and the Internet (including the dark net).

¹ André Årnes, Op.cit, pp 315 316.

Internet and cloud forensics: Research and development for the rapid acquisition, correlation, and analysis of Internet and cloud-related evidence. New tools and methods for evidence acquisition and analysis are constantly needed, with a corresponding need for educating law enforcement and practitioners in the field.

Cross-media search and data integration: Technologies for cross-media search and data integration to access diverse sources of information, in particular data enrichment from Internet sources.

Encrypted evidence: Algorithms for the analysis of encrypted evidence and cryptographic credentials.

Computational intelligence: Design of advanced computing technologies to achieve more objective evidence analysis and final decision making by implementing computational intelligence.

Attribution and profiling Development of methods and tools for digital penetrator attribution and profiling, visualization of serious criminal relationships and associations, and geographical mapping of digital and physical evidence.¹

1.4.2 Challenging Aspects of Digital Evidence

Digital evidence as a form of physical evidence creates several challenges for digital forensic analysts. First, it is a messy, slippery form of evidence that can be very difficult to handle. For instance, a hard drive platter contains a messy amalgam of data pieces of information mixed together and layered on top of each other over time. Only a small portion of this amalgam might be relevant to a case, making it necessary to extract useful pieces, fit them together, and translate them into a form that can be interpreted.

Second, digital evidence is generally an abstraction of some digital object or event. When a person instructs a computer to perform a task such as sending an e-mail, the resulting activities generate data remnants that give only a partial view of what occurred . Only certain results of the activity such as the e-mail message and server logs remain to give us a partial view of what occurred. Furthermore, using a forensic tool to recover a deleted file from storage media involves several layers of abstraction from magnetic fields on the disk to the letters and numbers that we see on the screen. So, we never see the actual data but only a representation, and each layer of abstraction can introduce errors .

Third, digital evidence is usually circumstantial, making it difficult to attribute computer activity to an individual. Therefore, digital evidence can only be one component of a solid investigation. If a case hinges upon a single form or source of digital evidence such as date-time stamps on computer files, then the case is unacceptably weak. Without additional information, it could be reasonably argued that someone else used the computer at the time. For instance, password protection mechanisms on some computers can be bypassed, and many computers do not require a password, allowing anyone to use them. Similarly, if a

¹ André Årnes, Op.cit, pp 316 317 .

defendant argues that some exonerating digital evidence was not collected from one system, this would only impact a weak case that does not have supporting evidence of guilt from other sources.

Fourth, the fact that digital evidence can be manipulated or destroyed so easily raises new challenges for digital investigators. Digital evidence can be altered or obliterated either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion. Fortunately, digital evidence has several features that mitigate this problem.

- ❖ Digital evidence can be duplicated exactly and a copy can be examined as if it were the original. It is common practice when dealing with digital evidence to examine a copy, thus avoiding the risk of altering or damaging the original evidence.
- ❖ With the right tools, it is very easy to determine if digital evidence has been modified or tampered with by comparing it with an original copy.
- ❖ Digital evidence is difficult to destroy. Even when a file is “deleted” or a hard drive is formatted, digital evidence can be recovered.
- ❖ When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of

The ease with which digital evidence can be altered or destroyed creates challenges in many investigations in the form of evidence dynamics.

1.4.2.1 Evidence Dynamics and the Introduction of Error

Investigators and digital evidence examiners will rarely have an opportunity to examine a digital crime scene in its original state and should therefore expect some evidence dynamics: any influence that changes, relocates, obscures, or obliterates evidence, regardless of intent between the time evidence is transferred and the time the case is resolved. Offenders, victims, first responders, digital evidence examiners, and anyone else who had access to digital evidence prior to its preservation can cause evidence dynamics.

Some examples of evidence dynamics encountered in past cases:

- ❖ A system administrator attempted to recover deleted files from a hard drive by installing software on an evidential computer, saving recovered files onto the same drive. This process overwrote unallocated space, rendering potentially useful deleted data unrecoverable.
- ❖ Consultants installed a pirated version of a forensic tool on the compromised server. In addition to breaking the law by using an unlicensed version of digital forensic software, the installation altered and overwrote data on the evidential computer.¹

¹ Eoghan Casey, Digital Evidence and computer crime, third edition, Maryland,USA, 2011, pp 25 26 27.

- ❖ Responding to a computer intrusion, a system administrator intentionally deleted an account that the intruder had created and attempted to preserve digital evidence using the standard backup facility on the system. This backup facility was outdated and had a flaw that caused it to change the times of the files on the disk before copying them. Thus, the date-time stamps of all files on the disk were changed to the current time, making it nearly impossible to reconstruct the crime.
- ❖ During an investigation involving several machines, a first responder did not follow standard operating procedures and failed to collect important evidence. Additionally, evidence collected from several identical computer systems was not thoroughly documented, making it very difficult to determine which evidence came from which system.

Media containing digital evidence can deteriorate over time or when exposed to fire, water, jet fuel, and toxic chemicals. Errors can also be introduced during the examination and interpretation of digital evidence. Digital evidence examination tools can contain bugs that cause them to represent data incorrectly, and digital evidence examiners can misinterpret data. For instance, while a digital evidence examiner was examining several log files, transcribing relevant entries for later reference, he transcribed several dates and IP addresses incorrectly; for example, he misread 03:13 A.M. as 3:13 P.M., resulting in the wrong dial-up records being retrieved, implicating the wrong individual. Similarly, he transcribed 192.168.1.54 as 192.168.1.45 in a search warrant and implicated the wrong individual.

There are many other ways that evidence dynamics can occur.

Although Bolander was found guilty, his computer was destroyed before sentencing. Additionally, a floppy disk containing evidence was mostly overwritten, presumably by accident. The evidence dynamics in this case created a significant amount of controversy.

Evidence dynamics create investigative and legal challenges, generally making it more difficult to determine what occurred and making it more difficult to prove that the evidence is authentic and reliable. Additionally, any conclusions that a forensic examiner reaches without the knowledge of how evidence was changed will be open to criticism in court, may misdirect an investigation, and may even be completely incorrect.¹

¹ Eoghan Casey, third edition, op.cit, pp 27 28.

Summary

This theoretical chapter provides a comprehensive overview of the digital crime scene, incorporating several general technical and legal definitions. It explains the most significant technical terms and network protocols utilized in the computing world. Furthermore, it discusses the legal admissibility of digital evidence as conclusive proof in court by Algerian judges, highlighting the core principles upon which the legal system is built. Finally, the chapter addresses the challenges and difficulties that investigators encounter while performing their assigned duties.

CHAPTER TWO

Operational Procedures in the Digital Crime Scene

Chapter Two : Operational Procedures in the Digital Crime Scene

The concept of a crime scene in the digital age is not limited to a specific physical location; it extends to encompass complex and dynamic technical spaces, where physical boundaries blur and data becomes the core of forensic evidence. Transitioning from searching for traditional evidence to extracting digital evidence requires a precise technical procedural framework to ensure the integrity of the evidence.

This chapter examines the operational procedures followed in handling the digital crime scene, starting with the legal standards for protecting privacy during investigations, moving through the digital forensic process, and culminating in methods for collecting evidence from the internet(internet forensics). This presentation aims to provide a comprehensive view of the procedures followed to conduct digital investigations effectively and legitimately, thereby ensuring the admissibility of evidence before judicial authorities.

1.1 Privacy in the search and investigation of Digital Evidence

Dealing with a digital crime scene presents a dual procedural challenge; while the requirements of an investigation necessitate comprehensive access to data to extract digital evidence, privacy remains a fundamental right that must not be overlooked by the competent authorities during search and investigative operations.

Today, the investigator no longer searches for tangible material evidence, but instead navigates through complex algorithms, deleted logs, encrypted data, and cross-border cloud environments.

Consequently, the search for digital evidence is no longer a simple procedural act; it has become a complex legal process that requires a delicate balance between the 'needs of justice' in uncovering the truth and the 'right to privacy' as a fundamental human right. This necessitates that the competent authorities adhere to strict regulations to ensure the legitimacy of procedures and the integrity of evidence before the judiciary.

1.1.1 Characteristics of Electronic Evidence:

Given that electronic evidence consists of electronic oscillations, its location is not fixed to a specific place.

A- Electronic Evidence is Reproducible:

Identical copies can be extracted that possess the same value and probative force as the original. This is a feature not available in traditional evidence, providing a guarantee for preserving it against damage.

B- Electronic Evidence is Volatile and Unstable:

It is subject to continuous change, whether due to manual data manipulation or automatic processes by certain programs. This is the case with electronic scans performed by antivirus software on stored files, or programs that clear temporary/residual files. Consequently, obtaining this type of evidence can be difficult. However, it is not impossible; with digital forensic tools, it can be accessed smoothly and extracted in its entirety.

C- Electronic Evidence is Borderless (Transnational):

In most cases, electronic evidence does not have a defined physical space; rather, it exists in multiple locations, whether within national borders or abroad. While some may attribute this to the nature of the internet and the global reach of its networks, it is primarily due to servers located outside the country. Owners lease these servers to clients and grant them specific access privileges. This is particularly relevant in Algeria, where there is a lack of large-scale server infrastructure, necessitating the leasing of such services from abroad.

1.1.2 Functional Characteristics of Electronic Evidence:

A- Electronic Evidence Contains More Detailed Information About Facts:

Compared to traditional evidence, digital forensic evidence can provide—in addition to general information or data about the crime—what is known as "Metadata" (data about data). This significantly assists justice systems in uncovering the truth. For example, a photo taken by a digital camera does not only provide general information about the image content (such as the sky, clouds, or people and their physical descriptions); it simultaneously provides detailed information including the type of camera used, the precise date and time (hour/minute/second) of capture, and the geolocation coordinates. Advanced tools can even provide the IP address if the image was captured via a smartphone or computer. The same applies to emails, which provide not only the message content but also deep information such as the sender's name and address, the creation date of the message, and any modifications made to it, all of which are invaluable to investigative bodies.¹

¹ صهيب سهيل غازي زامل، البحث و التحري عن الدليل الالكتروني في المسائل الجزائية، دراسة مقارنة ، اطروحة الحصول على شهادة الدكتوراه، كلية الحقوق و العلوم السياسية ،جامعة وهران 2، الجزائر، ص ص 22-23.

B- Electronic Evidence Simultaneously Monitors and Analyzes Information About the Perpetrator:

Electronic evidence can record an individual's movements, behavioral habits, and certain personal matters. Consequently, criminal investigation may achieve its goals more easily, quickly, and accurately compared to using traditional evidence.

C- Electronic Evidence is Characterized by High Storage Capacity:

Cloud storage can hold hundreds or even thousands of pieces of evidence, and computer storage media contain an almost infinite amount of evidence.

D- Electronic Evidence is Difficult to Eliminate:

Electronic evidence can be retrieved after deletion, repaired after damage, and revealed after being hidden, making it difficult to dispose of—one of its most critical characteristics compared to traditional evidence. Many computer programs are specifically designed to recover data that has been deleted, even if the user performed a standard "Delete" command or even a full "Format" of the hard disk. Whether the files are images, graphics, or documents, they can often be recovered using specialized data recovery tools. This makes it challenging for a perpetrator to hide a crime from the eyes of security and justice, provided that investigators are aware that a crime has occurred. In fact, the perpetrator's attempt to destroy the evidence is in itself recorded in the system's memory, which can be extracted and used as evidence of guilt against them.¹

1.1.3 Assessment of the risks to the rights and freedoms of data subjects

The privacy risks specified in this section are in line with CNIL PIA Methodology and ISO 29134 (CNIL, 2017; ISO, 2017).

1.1.3.1 Illegitimate access to data

Illegitimate access may lead to considerable damages to the data subjects due to the amount and privacy sensitivity of the data such as discrimination, damage to reputation, financial loss etc. Further, any unauthorised disclosure may have a negative influence on the discovery of truth in criminal investigations. For instance, a situation where a suspect finds out by means of an unauthorized access that he/she is under secret investigation may frustrate the investigation.

Some main threats that can lead to an illegitimate access are as follows:

- ❖ Data process/read for wrong case.
- ❖ Unencrypted data transmission from third parties.
- ❖ Unauthorized person access to the big data forensic platform

¹ صهيبي سهيل غازي زامل، مرجع سابق، ص 23-24.

- ❖ Investigation report (paper documents) sent to wrong destination.
- ❖ Access to data after case is closed.
- ❖ No systematic monitoring of authorizations.
- ❖ Illegitimate cross-referencing of data (ISO, 2017).

1.1.3.2 Unwanted change of data

Unwanted change of data may cause the big data forensic platform to fail to operate correctly. Also, the processing could be misused for evidence manipulation; a piece of evidence might be altered in other valid data such as data about location or move-ments, economic situation, etc. As a result, there might be occasions where someone commits a crime and an innocent person is accused of it and personal data are processed in a manner that is incompatible with specified and legitimate purposes.

Some main threats that can lead to unwanted change of data access are as follows:

- ❖ Errors during updates, configuration or maintenance (ISO, 2017).
- ❖ Malicious code injection (CNIL, 2017).
- ❖ Replacement of an original document (paper) by a forgery (ISO,2017).
- ❖ Replacement of components (ISO, 2017).
- ❖ Authorizations not granted at case level.
- ❖ Not to ensure separation of duties (e.g., between system administrators, operators and investigators).
- ❖ Errors while uploading seized digital material.
- ❖ Insufficient knowledge of the software.

1.1.3.3 Disappearance of data

Disappearance of data may dramatically effect data availability.

In digital investigations, data availability should be high, preferably 24/7, otherwise the amount of evidence found in digital material will decrease and time needed to solve a case will increase. Like unwanted change of data, data disappearance may cause to malfunction. In consequence, the outcomes of these feared events may produce adverse legal effects concerning the data subject.

Some main threats that can lead to disappearance of data are as follows:

- ❖ Processing capacity overload (ISO, 2017).
- ❖ Denial of service attack (CNIL, 2017).
- ❖ Ageing of archived documents (CNIL,2017).
- ❖ Loss of encryption key.¹
- ❖

¹ M. Bas Seyyar, Z.J.M.H Geradts, Privacy impact assessment in lagre-scale digital forensic investigations, Forensic Science International: Digital Investigation, university of Groningen, PO Box72, 9700 AB Groningen,Netherlands,17January 2020, p 5.

- ❖ Assignment of poorly trained employees.
- ❖ Under tested software/hardware integration.

1.1.4 The measures envisaged to address the risks

In this section, we discuss appropriate measures for a big data forensic, to address the privacy risks identified in the previous section.

- ❖ Access to the platform should be permitted only to personnel who possess a security clearance.
- ❖ If an investigator is no longer working on a case, his/her access to the case data should be immediately withdrawn.
- ❖ LEAs should impose strict data retention periods in accordance with the requirements of all applicable legislation. In case of a need for longer retention periods, the data should be anonymized. Also, specifications on how to destroy the personal data in a secure manner should be developed. Procedural measures have to be in place to ensure retention and destroy policies are respected.
- ❖ Case data and queries made by investigators for searching traces should be kept encrypted.
- ❖ Software used in the platform especially forensic analysis tools should be analysed with regard to privacy.
- ❖ Confidentiality communication e.g., information covered by legal professional privilege should be excluded as evidence for criminal prosecution. Unfortunately, there does not exist a forensically sound procedure that is able to guarantee the protection of confidentiality communication and current practices require manual intervention. Hence, the disclosure of such information should, as far as possible, be protected. To this end, a list of keywords to filter out the relating privileged data might be specified in advance. The defence lawyer might be consulted for specifying the possible keywords. Search for these keywords should only be allowed with prior justification. It is possible that the traces are not correctly recognized as privileged and not filtered out during the investigation. In this case, an investigator might mark traces as privileged and filter them out immediately. Likewise, it is also possible that some data are incorrectly classified as privileged. In this case, an officer being not involved in the investigation may be designated and he/she may restore non-privileged data.
- ❖ To reduce the risk impact, it should be ensured that any disclosure of personal data is detected as soon as possible and supervisory authority e.g., PPS or DPA is informed accordingly.
- ❖ Datasets used for training and software testing should be anonymized.
- ❖ Strict access control policies should be in place to limit the risk of unauthorised access to personal data.¹
- ❖

¹ M. Bas Seyyar, Z.J.M.H Geradts, Op.cit., pp 5 6.

- ❖ Any user/system actions should be logged, attributed to diagnose any privacy breaches and to preserve the chain of evidence. Article 25 of the Police Directive sets out how detailed the logs should be as follows: the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The said article also limits the usage of logs. To protect the privacy of employees, logs might be pseudonymised too.
- ❖ To implement the principle of purpose limitation, the big data forensic platform should keep an explicit audit trail of user actions. Audit trails may verify that the actions of the forensic investigator are within the scope of a warrant/court order and also reinforce the evidence reliability.
To achieve a higher-level of auditing, unique user profiles which are tied to individual analysts and allow for varying degrees of access to data based on the tasks assigned and clearance given may be provided .
- ❖ It is important that the case data seized digital material are handled meticulously and carefully throughout the entire investigation: both when collecting data from third parties and when transferring it to the platform. The original digital material should be kept outside of the platform's processing, an exact copy should be made and used for searching traces. To monitor its integrity and minimize the errors, a hash function and a message authentication code (MAC) could be used.
- ❖ To ensure data accuracy, the data must be categorized according to its reliability. For this purpose, 4x4x4 (Belgium) or 5x5x5 (UK) grid structures could be used as an example. For instance, in UK 's structure, the data are described in 5 categories as follows: (A) Known directly to the source, (B) Known indirectly to the source but corroborated, (C) Known indirectly to the source, (D) Not known, (E) Suspected to be false By the same token, it is desirable to clearly distinguish primary data sources (the sources where data are actually generated) from secondary ones (sources that link existing data sets and reuse them).
- ❖ A distinction between different categories of data subjects should be drawn. The personal data of convicts, suspects, victims, witnesses and third parties should be treated differently as addressed in Article 6 of the Police Directive. For instance, different degree of anonymization e.g., irreversible or de-identified reversible may be used for different categories of data subjects.
- ❖ The potential discriminatory factors e.g., the training data, the learning algorithm etc. should be tested whether they create biases for natural persons especially for profiling. If so, they shall be prohibited.
- ❖ Algorithms and techniques which are scientifically derived and proven should be used in the platform. The margin of error associated with them should be determined by taking into account their potential impact on the natural persons .
- ❖ Competent authorities could be encouraged in publishing their PIA reports executive summary on a publicly available platform.¹

¹ M. Bas Seyyar, Z.J.M.H Geradts, Op.cit., pp 6 7.

1.1.5 Discussion of principles relating to processing of personal data in law enforcement sector

The processing of personal data in a big data forensic platform is not transparent. The data subjects such as suspects do not always know if and how their personal data are being processed. So, they cannot be asked to give their consent to the processing. They also lack insight into the accuracy and completeness of their personal data. The personal data of the persons who have nothing to do with the criminal investigation might also be processed in such a platform. These persons are not able to make use of their rights under Police Directive. It is actually impracticable for the competent authorities to be transparent about data processing of natural persons, as this involves a disproportionate amount of time and effort and the process of truth-finding may be frustrated. Since it is difficult to determine in advance which information is relevant to the case and which is not, data minimization might not be implemented in the criminal investigations.

Because the persons involved are often unable to exercise some of their rights, it is of great importance that the processing in a big data forensic platform is subject to an external control/audit by the supervisory authority. Additionally, the competent authorities might provide a clear explanation concerning the use of personal data in relation to forensic investigation within the big data platform in their website and/or social media account. In this context, an explanation of how to challenge the decisions made with the help of the platform may be put on the website for future reference.¹

¹ M. Bas Seyyar, Z.J.M.H Geradts, Idem.

1.2 The Digital Forensic Process

The extraction of evidence from digital media is not a random process; rather, it is a technical and legal activity subject to a strict methodology known as 'digital investigation procedures.' The importance of this element lies in establishing a practical methodological framework that ensures evidence is neither lost nor damaged, relying on a balance between technical professionalism in handling complex data and the procedural compliance imposed by the law. As shown in the diagram below, this is what is addressed in this section in a detailed and precise manner.

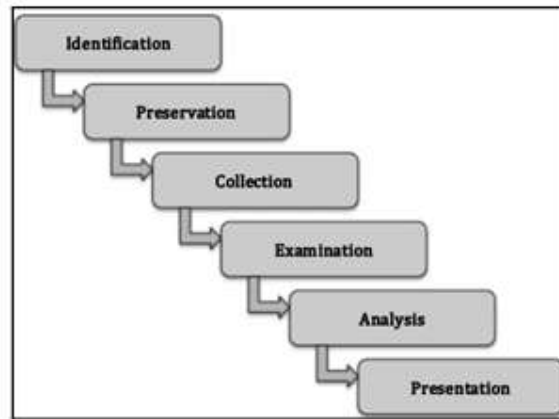


Figure 2.1 The digital forensics process

1.2.1 Identification

One principle that is often discussed in forensic science is the Locards exchange principle.

This principle postulates that when two objects come into contact, they leave a trace on each other. For example, if you walk into a house with carpeting, dirt from your shoes is left on the carpet and the carpet leaves fibers on the soles of your shoes. These traces that are exchanged form the bases of the science of trace evidence in the physical forensics world. In the digital world, we often have very similar trace evidence when two systems come into contact with each other. For example, if an individual browses to a website, the web server or web application firewall may record the individual's IP address within a collection log.

The website may also deposit a cookie on the individual's laptop. Just as in the physical world, evidence exchanged in this manner may be temporary and our ability to observe it may be limited to the tools and knowledge we currently have.¹

This principle can guide the identification of potential sources of evidence during an incident. For example, if a SIR is attempting to determine the root cause of a malware infection on a system, they would start by analyzing the infected system. As some malware

¹ Gerard Johansen, Digital Forensic and Incident Response, Birmingham, UK, 2017, p 34.

requires access to a C2 server, analysts can search firewall connection or proxy logs for any outbound traffic from the infected system to external IP addresses. A review of those connection IP addresses may reveal the C2 server, and potentially more details about the particular malware that has infected the system.

It should be noted though, that threat actors very easily manipulate digital evidence, so reliance on a single piece of digital evidence without other corroborating evidence should always be tempered with caution and should be verified before it can be trusted.

1.2.2 Preservation

Once evidence is identified, it is important to safeguard it from any type of modification or deletion. For evidence such as log files, it may become necessary to enable controls that protect log files from removal or modification. In terms of host systems such as desktops, it may become necessary to isolate the system from the rest of the network through either physical or logical controls, network access controls or perimeter controls. It is also critical that any users not be allowed to access a suspect system. This ensures that users do not deliberately or inadvertently taint the evidence. Another facet of preservation measures has been the increased reliance on virtual platforms. Preservation of these systems can be achieved through the snapshotting systems and saving to non-volatile storage.

1.2.3 The collection

The collection element is where digital forensic examiners begin the process of acquiring the digital evidence. When examining digital evidence, it is important to understand the volatile nature of some of the evidence that an examiner will want to look at. Volatile evidence is evidence that can be lost when a system is powered down. For network equipment this could include active connections or log data that is stored on the device. For laptops and desktops, volatile data includes running memory or the Address Resolution Protocol cache. The Internet Engineering Task Force (IETF) has put together a document titled Guidelines for Evidence Collection and Archiving (RF 3227) that addresses the order of volatility of digital evidence:

- ❖ Registers, cache
- ❖ Routing Table, ARP Cache, process table, kernel statistics, Memory (RAM)
- ❖ Temporary filesystems
- ❖ Disk
- ❖ Remote logging and monitoring data
- ❖ Physical configuration, network topology
- ❖ Archival media¹

It is imperative that digital forensic examiners take this volatility into account when starting the process of evidence collection. Methods should be employed where volatile evidence will be collected and moved to a non-volatile medium such as an external hard drive.

¹ Gerard Johansen, Op.cit.,pp 34,35 .

1.2.3.1 Proper Evidence Handling

The proper handling and securing of evidence is critical. Mistakes in how evidence is acquired can lead to that evidence being tainted and subsequently not forensically sound. In addition, if an incident involves potential legal issues, critical evidence can be excluded from being admitted in a criminal or civil proceeding. There are several key tenets of evidence handling that need to be followed:

- **Altering the original evidence:** Actions taken by digital forensic examiners should not alter the original evidence. For example, a forensic analyst should not access a running system if they do not have to. It should be noted that some of the tasks that will be explored have the potential to alter some of the evidence. By incorporating proper documentation and having a justifiable reason, digital forensic examiners can reduce the chance that evidence will be deemed tainted

- **Document:** One central theme you will often hear in law enforcement is the phrase if you didn't write it down, it didn't happen. This is especially true when discussing digital forensics. Every action that is taken should be documented in one way or another. This includes detailed notes and diagrams. Another way to document is photographs. Proper documentation allows for examiners to reconstruct the chain of events if ever the integrity of evidence is called into question.¹

1.2.3.2 CHAIN OF CUSTODY

The Chain of Custody for digital evidence is the chronological documentation of its handling from the time of collection until its disposal. The Chain of Custody can consist of signed paper forms, photographs, investigator's notes, examination reports, automatically generated logs and forensic hashes.

The Chain of Custody should uniquely identify the evidence. Computers, phones and other storage media can be identified by recording the manufacturer's name, model number and serial number. If no unique identifier exists, evidence can be tagged, labelled or bar coded for that specific purpose.

Digital evidence such as emails, digital documents, multimedia files or website captures can be identified by how, when and from whom it was received; or by how, when and from where it was collected²

As a minimum, the Chain of Custody should document the following:

- ❖ The person collecting or receiving the evidence.
- ❖ The source of the evidence.
- ❖ Date and time, including time zone information where applicable.
- ❖ Unique identifiers.
- ❖ How the evidence was collected, including the tools and methods used.

¹ Gerard Johansen, Op.cit., pp 35,36.

² Conference of International Investigators (CII 2021), General principles for digital evidence, p3.

- ❖ Any additional documentation as required by the Organisation.¹

1.2.4 Examination

The examination phase details the specific tools and forensic techniques that are utilized to discover and extract data from the evidence that is seized as part of the incident. For example, in a case where malware is suspected of infecting a desktop system as part of a larger attack, the extraction of specific information from an acquired memory image would take part in this stage. In other cases, digital forensic examiners may need to extract Secure Shell (SSH) traffic from a network capture. The examination of digital evidence also continues the process of proper preservation in that examiners maintain the utmost care with the evidence during the examination. If the digital forensic examiner does not take care in the preservation of the evidence in this stage, there is the possibility of contamination that would result in the evidence being unreliable or unusable.

1.2.5 Analysis

Once the Examination phase has extracted the potentially relevant pieces of data, the digital forensic examiner then analyzes the data in light of any other relevant data obtained. For example, if the digital forensic analyst has discovered that a compromised host has an open connection to an external IP address, they would then correlate that information with an analysis of the packet capture taken from the network. Using the IP address as a starting point, the analyst would be able to isolate the particular traffic. From here, the analyst may be able to determine that the compromised host is sending out a beacon to a C2 server.

From here, using additional sources, the analyst may be able to determine what the particular attack vector is tied with that IP address.²

1.2.6 Presentation

The reporting of facts related to digital forensics needs to be clear, concise, and with or without objectivity. In nearly all instances, a forensic examiner will be required to prepare a detailed written report, which addresses every action and captures the critical data required. This report should be thorough, accurate, and without opinion or bias. This report will often be made part of a larger incident investigation and aids in determining the root cause of an incident.

Another aspect of presentation is the role that the forensic examiner might play in a criminal or civil proceeding. Testifying in court may be required if the incident under investigation has yielded a suspect or other responsible party. It is during this testimony that the forensic examiner will be required to present the facts of the forensic examination in much the same dispassionate manner as the report. The examiner will be required to present the facts and conclusions without bias and may be limited as to what opinions they testify to. How an examiner will be allowed to testify is often dependent on their training and experience. Some

¹ Conference of International Investigators (CII 2021), Idem.

² Gerard Johansen, Op.cit., pp 39,40.

may be limited to presenting the facts of the examination. Other times, as examiners acquire skills and have been deemed an expert witness, they may be able to offer an opinion.¹

1.3 Internet Forensics

We previously mentioned what revolves around the computer and how to deal with it. Now, we speak about the internet, which has become a foul place where triviality prevails and criminality has increased. Although it has its merits, the negatives are more predominant. However, the positive aspect is that with every click of a button, every email, and every online purchase, we leave behind digital traces invisible to the ordinary user, yet they represent a precious treasure for investigators to reach the perpetrator.

1.3.1 Network Devices

There are many devices in the telecommunication and broadband networks that contain potential electronic evidence. Network devices might include modems, data service unit (DSUs), multiplexers, routers, firewalls, switches, wiring hubs, and the list goes on. These devices, however, are technical in nature and require an experienced technician to reveal their contents.

The functions of these devices are generally related to the transmission and reception of some type of analog or digital communication signal. These devices are almost always transparent or invisible to the general user. The transmission of voice and data, however, would not happen without these devices.

Various network surveillance hardware and software are utilized to monitor and track network activities. Hardware devices such as monitors, protocol analyzers, and sniffers are employed in the surveillance systems. These specialized and complex devices can identify and capture numerous items of data and information from the network. Any and all network traffic is susceptible to surveillance. These transmissions might be protected, compressed, encapsulated, and encrypted. Some items of evidence may include:

- ❖ IP addresses.
- ❖ Logons and passwords.
- ❖ Data files.
- ❖ Date and time stamps .
- ❖ Messages .

A number of system vendors such as IBM, Cisco, Sun Microsystems, Symantec, Network Associates, and Hewlett-Packard provide hardware and software solutions oriented toward enterprise security and surveillance. Intrusion detection and prevention information could be critical in computer networking investigations. Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or network to identify possible security

¹ Gerard Johansen, Idem.

breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).¹

An ID system is any device that exercises access control to protect computers from exploitation. These systems are either host-based or network-based.

Data collection methods require significant storage and the need for occasional erasing of old data to make room for new. Many networking devices may possess a limited amount of data storage. The open source programs Tcpdump and windump as well as a number of commercial programs can be used for data capture and analysis.²

1.3.2 Layers of Network Abstraction

will review the technologies and protocols that support the Internet and what they may indicate for digital investigations

1.3.2.1 The Physical Layer

The lowest level of computer intercommunication is the physical layer. This layer transmits the digital zeros and ones from one location to another through a physical medium, such as electricity over copper wires, optical light through fiber cables, or radio waves through the air. This layer is of interest when one wishes to do network traffic interception as part of their investigation.

1.3.2.2 The Data Link, Network, and Transport Layers

The layers above the physical layer ensure that the zeros and ones are correctly received, and they determine which physical medium a given piece of data should be transmitted through. Three important protocols operating at this layer are the IP, the User Datagram Protocol (UDP), and the Transmission Control Protocol (TCP). IP is an addressing scheme used to determine where a given piece of data is going, and there are currently two versions of the IP address being used on the Internet: version 4 (IPv4) and version 6 (IPv6). UDP and TCP are data transport protocols that manage how data is sent from one IP address to another. The major difference between the two protocols is that TCP ensures that every packet is correctly sent from end to end, in the appropriate order. Because of the extra verification steps, sending data with TCP is slower than with UDP. TCP is thus commonly used for transmitting information such as web pages and email, and UDP is a more popular choice for services such as Internet telephony and streaming, where a certain level of packet loss and corruption is accepted.³

¹ **Robert C. Newman**, Computer Forensics, Evidence Collection and Management, 2007 By Taylor & Francis Group, USA, pp 109, 110.

² **Robert C. Newman**, Idem.

³ **André Årnes**, Op.cit., p 277.

A- IP Addresses

describes three steps for sending a network packet from one endpoint to another using the IP. First, the identity of the recipient must be determined, then the location of the recipient, and finally a route from the sender to the recipient. IP addresses deal with the second part (i.e., indicating the recipient's location). As mentioned, there are two IP versions currently being used, IPv4 and IPv6. IPv4 has been used for decades and is still the most commonly used version of IP address by far. An IPv4 address is commonly represented as four bytes represented as four numbers between 0 and 255 each separated by a dot, or as a 32-bit integer between 0 and approximately 4.3 billion. We can specify a range of IP addresses by writing the address as a prefix. A common syntax for such a prefix is an IP address, followed by a forward slash and a number between 0 and 32. Both versions 4 and 6 specify network ranges on this format. In the early days of the IP, large IP network prefixes were given to large organizations like IBM, meaning that a large part of these 4.3 billion IP addresses are reserved, though they may not be in use. This means that the rest of the Internet has far less IP addresses to share, and as more and more devices require addresses, available ones are running out. The IPv6 addressing scheme was extended – instead of using 32 bits to uniquely identify a network endpoint, it uses 128 bits, which gives us well over 340 trillion addresses to choose from.

1.3.2.3 The Session, Presentation, and Application Layers

The three upper layers of the OSI model provide further abstraction from how bits are physically transmitted between endpoints. The application layer enables protocols like the Hypertext Transfer Protocol (HTTP) and the File Transfer Protocol (FTP), two popular high-level protocols for requesting and transferring data. ¹

1.3.3 The Internet

The topics we cover in this section reveal how computer networks are able to connect to each other, both directly and through other networks. Together they enable every pair of Internet-connected computers to reach one another

1.3.3.1 Internet Backbone

A set of high-speed TCP/IP routers and interconnecting transmission lines that form a major trunk system for carrying multiple transmissions. Local and regional networks connect to backbones which then provide the long distance connections to other networks that are also attached to the same backbone or another backbone. Backbones are connected to each other at NAPs and private exchange points.²

¹ André Årnes, Op.cit., p 278.

² Pat Dalton, The Internet: A Primer, INFORMATION BRIEF, Minnesota House of Representatives, Research Department, October 1998, p 10 .

1.3.3.2 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol.

The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the autonomous systems AS's that traffic must transit to reach these networks. This information is sufficient to construct a graph of AS connectivity from which routing loops may be pruned and policy decisions at an AS level may be enforced.

BGP runs over a reliable transport level protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. Any authentication scheme used by the transport protocol may be used in addition to BGP's own authentication mechanisms.

The initial BGP implementation is based on TCP , however any reliable transport may be used. A message passing protocol such as VMTP might be more natural for BGP. TCP will be used, however, since it is present in virtually all commercial routers and hosts. In the following descriptions the phrase "transport protocol connection" can be understood to refer to a TCP connection. BGP uses TCP port 179 for establishing its connections.¹

1.3.3.3 Internet Service Providers (ISPs)

ISPs are organizations that provide access to the Internet to customers. Some ISPs are large, maintaining a global physical infrastructure, while others are small, providing Internet access to a relatively small number of customers in a small town or region. ISPs are organized into three tiers by their size: Tier 1, 2, and 3.

Tier 3 ISPs are the smallest, and they usually pay higher tier ISPs for transit on their infrastructure. Tier 2 ISPs are larger, maybe maintaining a national Internet infrastructure. These tier 2 ISPs may establish peering agreements with other tier 2 ISPs, sell transit to tier 3 ISPs, and buy transit from tier 1 ISPs. Tier 1 ISPs do not have to buy transit from any other ISP; they maintain large physical infrastructures, such as the subsea network cables connecting continents. Tier 1 ISPs establish peering agreements with other large ISPs to gain access to parts of the world where they do not have the infrastructure; they also sell transit to tier 2 and 3 ISPs.²

¹ **K. Lougheed**, A Border Gateway Protocol (BGP), Network Working Group, T.J. Watson Research Center, IBM Corp, June 1998, p 1.

² **André Årnes**, Op.cit., p 281.

1.3.4 Common Applications

There is no limit as to the types of applications that may run on the Internet. Indeed, it is infeasible to discuss every existing application within this title. However, some applications have manifested themselves over the years as so common that they are almost ubiquitous to the Internet itself. This chapter discusses three such applications: the Domain Name System, Email and the World Wide Web.

1.3.4.1 The Domain Name System

DNS is a foundational element of IP communications. DNS provides the means for improved usability of IP applications, such as insulating end users from typing IP addresses directly into applications like web browsers and enabling web servers to serve web pages compromised of diverse linked content. To communicate over an IP network, an IP device needs to send IP packets to the intended destination; and each IP packet header requires both source and destination IP addresses. DNS provides the translation from a user-entered named destination, for example, web site www address, to its IP address such that the sending device may populate the destination IP address with the address corresponding to the entered domain name.

DNS is not only useful for Internet users but also for network administrators. By publishing name-to-IP address mappings in DNS, the administrator gains the freedom to change IP addresses as needed for network maintenance, service provider changes, or general renumbering without affecting how end users connect. I can map my www address to 192.0.2.55 today and change it to 198.51.100.23 tomorrow without affecting how users reach my website. Of course, I'd need to keep both addresses active for some time given the caching of the former mapping in various recursive servers that had queried for my address before I made the change.

This level of indirection is also useful when configuring Internet of things such as home appliances, smart cars, surveillance cameras, etc. that can connect to the Internet independently of user-initiated commands. Such connections may be initiated first by a DNS lookup of its configured web address, to which it connects to communicate a status update, alert, or other information. The thing's home website IP address may be changed as needed by changing its DNS entry in a manner similar to that just described.¹

¹ **Michael Dooley and Timothy Rooney**, DNS Security Management, First Edition, 2017 by The Institute of Electrical and Electronic Engineers, Inc. Published 2017 by John Wiley & Sons, Inc, p 17 18.

1.3.4.2 E-Mail Systems

E-mail is a term derived from the phrase electronic mail. Users can send and receive messages over an electronic communication system, such as the Internet. An e-mail system consists of both the servers that send and receive e-mails on the network and the e-mail clients that allow users to view and compose messages. An e-mail system works in the following way:

1. A user—let's call her Jane—composes a message using her mail user agent (MUA) and writes the e-mail address of her correspondent—Peter, in this example—and hits the Send button.
2. Jane's MUA formats the message in the Internet e-mail format and uses SMTP to send the message to the local mail transfer agent (MTA).
3. The MTA looks at the destination address provided in SMTP.
4. The MTA looks for this domain name in the Domain Name System to find the mail exchange servers accepting messages for Peter's domain.
5. The DNS server responds with a mail exchange record for Peter's domain.
6. Jane's SMTP server sends the message to the mail exchange server of Peter's domain.
7. Peter presses the Get Mail button in his MUA, which picks up the message using the Post Office Protocol (POP3). Peter then reads the message in his MUA.

A- E-Mail Client

An e-mail client, also known as a mail user agent (MUA), is a computer program for reading and sending e-mail. There are a number of standalone e-mail clients, including the following:

- Microsoft Outlook
- Microsoft Outlook Express
- Eudora
- Pegasus
- The Bat!
- Mozilla Thunderbird

There are also a number of Web-based e-mail clients, including the following:

- Hotmail
- Yahoo!
- Gmail¹

1.3.4.3 World Wide Web

We conclude this section with a review of HTTP and Hypertext Markup Language (HTML), technologies central to the WWW. HTTP is at the application layer of the OSI model. It uses TCP for transferring requests and responses between servers. A HTTP request consists of a header field and a body field. The most commonly used version of HTTP, version 1.1, requires three elements to be present in a request header: a verb, a path, and a host

¹ **EC-Council**, Computer Forensics Investigating Network Intrusions & Cyber Crime, Course Technology/Cengage Learning, 2010, USA, pp 236 237.

On the WWW, the HTTP response type is often TEXT/HTML, meaning that the requester should parse the content as a web page. This is a text format that is a dialect of the eXtensible Markup Language (XML). Web browsers specialize in sending and parsing HTTP requests and responses. They will generate a view on the user's screen based on this text. Within the text, browsers can find elements that trigger new HTTP requests, such references to pictures, scripting files, or style sheets. How the response should be presented to the user is determined using these style sheets, and scripts can generate subsequent requests, potentially adding more content to the original request.¹

1.3.5 MALWARE

Malware such as viruses, trojans, and ran somware are significant threats to internet users and likely will be for the foresee able future. As a result, it's important to arm yourself and your users with an antivirus solution that detects and removes malware. Additionally, keeping your endpoints up- to- date can prevent mal ware from infecting your network and in some cases provide more protection than an antivirus (AV) solution.²

1.3.5.1 Malware Attacks

This type of attack constitutes a significant portion of the overall cyber-attacks recorded. Malware stands for malicious software. Malware has a broad category of software that infects and exploits networks, servers, and end hosts in various ways.

Virus, worms, and trojan horses: They enter a computing device through physical, Internet, emails, file attachments, and all possible digital transfer means. They infect the system, can encrypt or delete all data, and replicate and propagate to other computers by exploiting existing vulnerabilities. Sometimes, they can act like ransomware too.

Spyware, adware, keyloggers, and phishing: These types of malware aim at collecting sensitive information from the victim and don't cause much damage. They can replicate and propagate like viruses and worms through all possible means.³

Botnet and crypto miners: These types of malware use the computing resources of the victim system to cause DDoS-type attacks or earn money through crypto mining.

Ransomware: This type of malware after infecting the victim device or network demands ransom to not cause damage to the system. Every malware has its own way of communicating over the network and replicating. By monitoring the same Wireshark can detect malware communication signatures through packet capture. However, some of them can be extremely stealthy and may not communicate at all. Those are difficult to analyze through Wireshark.

¹ André Årnes, Op.cit., p 284.

² SETH ENOKA , CYBERSECURITY FOR SMALL NETWORKS: A NO-NONSENSE GUIDE FOR THE REASONABLY PARANOID, 2023, San Francisco, USA, p 117 .

³ Nagendra Kumar Nainar, Ashish Panda , Wireshark for Network Forensics, North Carolina, NC, USA, pp 232 233 234.

1.3.5.2 Prevention of Malware Attacks

Following a proper network and security hygiene will go a long way in preventing malware attacks.

Network and infrastructure should be beefed up with web security, good firewall, and intrusion detection and prevention policies. Multifactor authentication, endpoint security, and antivirus and antimalware tools should be deployed to protect the edge devices.

All devices should have updated software, and any known vulnerabilities should be patched at the earliest. Email, web, and cloud security protection mechanisms must be deployed.

Most malware attacks rely on social engineering and phishing techniques which trick the end user into clicking malicious links and opening malicious attachments. User education is important to prevent malware attacks through all such means.¹

1.4 Investigation Methods for Collecting Digital Evidence

Digital evidence is characterized by being sensitive; simply powering on a device or browsing its files may lead to changing the 'metadata' or unintentionally erasing evidence. Therefore, during the investigation and evidence seizure stage, the investigator must take into account all the complications encountered, whether at the digital crime scene or in the laboratory, and must expertly handle all stages with caution in order to preserve the digital evidence.

1.4.1 Investigation of Computers in Operation

In case of a blocked account, we request the entry of the defendant in it or the indication of the code, for our entry into the operating environment, by performing the following actions:

- ⇒ Control on the desktop of the PC and the applications that are running at that time.
- ⇒ Immediate disconnection of the device from the network, as there is a risk of remote management
- ⇒ Check recent-quick access or in the path
C:\Users\"username"\AppData\Roaming\Microsoft Windows\Recent.
- ⇒ Enable the view of hidden files and folders.
- ⇒ Control of the users who manage the specific computer (cmd: net users).
- ⇒ Control of devices that are on the local network. (e.g. maintaining a local file server).

¹ Nagendra Kumar Nainar, Ashish Panda , Idem.

⇒ Check for the installation date of the operating system (cmd: systeminfo, focusing on OriginalDate). ⇒ Special investigation on a computer in operation.

⇒ Control of installed programs (control panel or explorer).

⇒ Check for installed virtual machines.

⇒ Check for encrypted files (containers) or entire partitions (hard disk drive) and corresponding programs to encrypt them. In case they are found, especially if they were found decrypted, it is absolutely necessary to export or create the Memory.dmp or minidump file for the subsequent possible decryption of the container by the forensic laboratories of the police authorities.¹

⇒ Check for the connection history of portable usb devices, in the system registry, by typing in the search regedit or with windows+R, in the path: H LOCAL

MACHINE/SYSTEM/CURRENTCONTROLSET/ENUM/USBTO R.

⇒ Check the Appdata folder for programs, records that interest us.

⇒ Control in folders related to reception, e.g. in p2p programs. Shared folders, incoming

⇒ General search with keywords that interest us. For example, in cases of child pornography, one of the words is PTHC.

⇒ More general search for file types by writing for example *.jpg, *.mp4, *.avi, *.flv.

⇒ Control, given that there is a decree that defines it in communication programs, browser history, email accounts, social media, cloud services, credentials in accounts by browsers, otherwise a superficial search is carried out on data related to external contact information, e.g. photos, installers.

⇒ Control of installed programs (control panel or explorer).

⇒ Check for installed virtual machines.

⇒ Check for encrypted files (containers) or entire partitions (hard disk drive) and corresponding programs to encrypt them. In case they are found, especially if they were found decrypted. the export or creation of the Memory.dmp or minidump file is absolutely required for the subsequent possible decryption of the container by the Forensic Service of the Law Enforcement Authorities.

¹ **ISO/IEC 27037:2012**, is an international standard that provides guidelines for the identification, collection, acquisition, and preservation of digital evidence, with a particular focus on the roles of Digital Evidence First Responders (DEFR) and Digital Evidence Specialists (DES). The standard was developed by ISO and IEC to ensure that evidence remains intact by following strict procedures.

1.4.2 Special Investigation on Mobile Phone in Operation

⇒ Turn on airplane mode.

⇒ App list overview and Photo/video gallery control.

⇒ Check the settings for linked accounts (google etc) on the device as well as the storage space (if it has a microSD buttoned)

⇒ Removing a device lock (or recording it in cases where it is not advisable to remove it, * Second Space)

⇒ Checking every application that is of interest to the case (e.g. facebook/gmail and their linked accounts and their content in case there is a privacy waiver)

⇒ Check the files stored on the device with the file manager (videos/photos plus other files and folders of interest)¹

⇒ If the illegal material is not detected, while there are strong indications that the phone is involved in the illegal activity, check for special hiding applications (eg Ar Lock, Hide it pro) or e.g. on Xiaomi devices with MIUI which are popular, Second Space (be careful when removing a lock on a Xiaomi device, the second space is deleted, as if there is no lock it is not functional).²

1.4.3 Crimes and Potential Evidence

The following crimes may involve the use of a computer or other electronic media; listed below are the crimes and potential evidence which may be recovered.

Computer Fraud Investigations:

- | | |
|-------------------------------------|-------------------------------|
| - Account data from online auctions | - Credit card data |
| - Accounting software and files | - Databases |
| - Address books | - Digital camera software |
| - Calendar | - E-mail, notes and letters |
| - Chat Logs | - Financial and asset records |
| -Customer information | |

Child Abuse and Pornography Investigations:

- | | |
|------------|--------------------------|
| -Chat logs | -Digital camera software |
|------------|--------------------------|

¹ ISO/IEC 27037:2012, p 20 .

² ISO/IEC 27037:2012, Idem.

- E-mails, notes and letters
- Internet activity logs
- User created directory and file names
- Graphic editing and viewing software which classify images

- Games
- Movie files
- Images

Network Intrusion Investigations:

- Address books
- E-mails, notes and letters
- Malware
- Configuration files
- Executable programs
- Cache information¹
- Internet activity logs usernames and passwords
- Website history
- Source code
- Random Access Memory (RAM)
- Internet protocol address
- Internet chat logs
- Registry information
- Network connections

Homicide Investigations :

- Address books
- Financial asset records
- Legal documents and wills
- Address books
- E-mails, notes and letters
- Telephone records
- Photo of victim/suspect
- E-mails, notes and letters
- Internet activity logs
- Medical records
- Diaries
- Financial asset records
- Maps
- Trophy photos

Domestic Violence Investigations:

- Adress Books
- Daireies
- E-Mails, notes and letters
- Financial asset records
- Telephone records

¹ **U.S. Departments of Homeland Security**, United States Secret Service, Best Practices for Seizing Electronic Evidence, V4.2, A Pocket Guide for First Responders, p 14.

Financial Fraud and Counterfeiting Investigations:

- | | |
|-----------------------------------|-------------------------------|
| -Address books | -Calendar |
| -Currency Images | -Check and money order images |
| -Customer information | -Databases |
| -E-mails, notes and letters | -False identification |
| -Financial asset records | -Images of signatures |
| -Internet activity logs | -On-line banking software |
| -Counterfeit currency images | -Bank logs |
| -Credit card numbers ¹ | |

E-Mail Threats, Harassment and Stalking Investigations:

- | | |
|-----------------------------|---------------------------|
| -Address books | - Diaries |
| -E-mails, notes and letters | - Financial asset records |
| -Images | - Internet activity logs |
| -Legal document | - Telephone records |
| -Victim background research | -Maps to victim locations |

Narcotics Investigations:

- | | |
|-----------------------------|--------------------------|
| -Address books | - Calendar |
| -Databases | - Drug recipes |
| -E-mails, notes and letters | - False ID |
| -Financial asset records | - Internet activity logs |
| -Prescription form images | |

Software Piracy Investigations:

- | | |
|--------------------------|------------------------------|
| -Chat logs | - Torrents |
| -Video and audio files | - E-mails, notes and letters |
| -Software serial numbers | -File sharing web sites |

¹ U.S. Departments of Homeland Security, Op.cit.,pp 14 15.

- Contains copyrighted media
- Image files of software certificates
- Internet activity logs which classify copyrighted software
- Software cracking utilities
- User created directories and file names

Telecommunication Fraud Investigations:

- Cloning software
- Electronic serial numbers
- E-mails, notes, and letters
- Internet activity logs¹
- Customer database records
- Mobile identification numbers
- Financial asset records

Identity Theft Investigations:

- Hardware and Software Tools
- Backdrops
- Credit card reader / writer
- Embosser
- Scanner software
- Internet activity logs
- Birth certificates
- Digital photo images
- Electronic signatures
- Counterfeit insurance documents
- Negotiable Instruments
- Cashier's checks
- Counterfeit court documents
- Counterfeit loan documents
- Money orders
- Internet Activity Related to ID Theft
- E-mail and forum postings
- Deleted documents
- On-line orders
- On-line trading information
- Identification Templates
- Check cashing cards
- Driver's licenses
- Counterfeit vehicle registrations
- Social security cards
- Business checks
- Credit card numbers
- Counterfeit gift certificates
- Counterfeit sales receipts
- Personal checks²

¹ U.S. Departments of Homeland Security, Idem.

² U.S. Departments of Homeland Security, Op,cit., p 15.

1.4.4 Investigative Tools

Cybercrime investigation tools include tons of utilities, counting on the techniques you're using and therefore the phase you're transiting. However, know that the majority of those tools are dedicated to the forensic analysis of knowledge once you've got the evidence in hand.

There are thousands of tools for every sort of cybercrime

- The Sleuth Kit
- Autopsy
- X-Ways Forensics
- Digital Forensics Framework
- Oxygen Forensic Detective
- F-Response
- Open Computer Forensics Architecture
- Bulk Extractor
- EnCase
- Computer Online Forensic Evidence Extractor (COFEE)
- ExifTool¹
- Forensic Toolkit
- Volatility
- SurfaceBrowser™.
- Foremost
- WindowsSCOPE
- Xplico.
- Paladin
- FAW
- Internet Evidence Finder (IEF).
- NFI Defraser
- NetworkMiner
- MAGNET RAM Capture.
- ProDiscover Forensics
- WinAudit
- Mandiant's Memoryze™.

1.4.5 Role of Forensic Expert in Crime Investigation

A Forensic Expert plays a vital role in crime investigation by identifying the computer the crime was targeted and the tools used in carrying out the attack. He will identify and gather the evidence, build a suitable chain of custody of the evidence, recover data from the system, duplicate and generate a hash, maybe an MD5 or SHA1 to check to authenticity and integrity of the recovered data.

The forensic analyst must analyze the data in a forensically sound manner and must evaluate all evidence and write a report and present it to the jury, can act as an expert witness in a case.

The key role therefore of a Forensic expert in crime investigation can be summarized as follows.

1. Identifying the Crime
2. Gathering the evidence
3. Building a chain of custody
4. Analyzing the Evidence
5. Presenting the Evidence

¹ **ROBERT KAMARGI**, Cyber Forensics, n.p, no pub, pp 347 to 396.

6. Testifying

As a forensics examiner you are not to make decision as to guilty or innocent, you are only there to present the fact and let the Judges decide. A forensic examiner must maintain professional integrity and impartiality. As an examiner you can answer the following and more questions using forensic investigations.¹

¹ **ROBERT KAMARGI** , Ibid,pp 397 398 .

Summary

This Chapter presents the procedural and technical framework followed for handling digital evidence to ensure its integrity and legal admissibility before judicial authorities. We pointed out the dual challenge represented by the necessity of comprehensive access to data to extract evidence, while strictly adhering to the protection of the right to privacy as a fundamental right of litigants. Furthermore, the procedures to be followed when working with an electronic device were mentioned, along with the most important tools used for the examination, tracking, and analysis of the key data, images, files, and devices under investigation.

General Conclusion

This study concludes that the digital crime scene will remain an evolving field, open to new challenges as science advances. This reality necessitates that researchers and legislators continuously pursue development and innovation to protect justice in the digital age.

The research has yielded several key findings, most notably:

- **The Nature of Digital Evidence:** Its fragile nature and extreme sensitivity to the surrounding environment mean that a simple technical error can result in the loss of the evidence's legal admissibility.
- **Technical Inspection:** Visual inspection is no longer sufficient; reliance on digital forensic tools has become a necessity to ensure the integrity of data.
- **The Urgent Need for Legislative Development:** Laws must be updated to keep pace with rapid technological surges and the widespread expansion of cybercrime. This includes crimes against national or private corporate systems, as well as social media crimes such as fraud, money laundering, online gambling, and the proliferation of electronic games that facilitate criminal activities, account hacking, and the spreading of malicious viruses for illegal use.
- **Individual Security Awareness:** This is the most crucial element in preventing cyberattacks and protecting private life. This is especially true for individuals in sensitive positions, as any error could allow access to an entire institutional system via Social Engineering, enabling criminals to infiltrate and deploy malware to gain total control.

Recommendations

Based on the findings, we propose the following recommendations:

- **Technical Training:** Necessity of technical training for judges, officers, and lawyers to understand electronic systems, ensuring the issuance of logical and appropriate judicial rulings.

Infrastructure: The necessity of acquiring high-quality servers with large storage and processing capacities.

- **Child Protection:** Protecting children from electronic games that involve grooming, harassment, and the exploitation of their vulnerability.
- **Content Regulation:** Strictly banning pornographic material in Algeria.
- **The necessity of tightening oversight on online gambling platforms and enforcing a total ban on them.**
- **Public Awareness:** Expanding and intensifying guidance for the general public regarding safety and the proper use of electronic devices.
- **Legislative Reform:** Improving and amending laws to match technological developments; applying traditional legal articles to cybercrimes often reveals a "legislative poverty" in this field.
- **Telecommunications Security:** Requiring mobile operators (Djezzy, Ooredoo, Mobilis) to change default PIN codes on GSM SIM cards to protect phone lines from hacking, as universal codes (0000) pose a security risk.
- **Router Security:** Necessity of changing default passwords for Algeria Telecom fiber optic routers, as their simple algorithms facilitate unauthorized access by cybercriminals.
- **Data Privacy:** Exercising caution when accepting "Cookies" on websites, as they can act as a gateway to personal data.
- **Specialized Expertise:** Establishing independent centers dedicated to conducting specialized electronic forensic expertise.

Bibliography

References

English Referencess:

1. **Prashant Mali** ,Cyber law& Cybercrimes , Foreword by Justice Rajesh Tandon EX-chairman cyber regulations apellate Tribunal of India , First Edition 2012.
2. **André Årnes**, Digital forensics, Norwegian University of technology and science, Norway, 2018.
3. **BrianD. Carrier, M.S. and Eugene H. Spafford,Ph.D**, Defining Event Reconstruction of Digital Crime Scenes, J forensic Sci, Nov.2004, Vol.49, No. 6.
4. **Charles J.Brooks,et al** , CYBERSECURITY ESSENTIALS, 2018, CANADA .
5. **Conference of International Investigators (CII 2021)**, General principles for digital evidence.
6. **EC-Council**, Computer Forensics Investigating Network Intrusions & Cyber Crime, Course Technology/Cengage Learning, 2010, USA.
7. **Elizabeth Ozioma Edward, Joseph A. Ojeniyi**, A Systematic literature review on digital evidence admissibility: methodology, challenges, and research directions, ICECCO 2019, Department of cybersecurity science Federal University of technology minna, Nigeria.
8. **Eoghan Casey**, Digital Evidence and computer crime : Forensic Science, Computers, and the Internet, Second Edition, 2004, USA.
9. **Eoghan Casey**, Digital Evidence and computer crime, third edition, Maryland,USA, 2011.
10. **Fernando Molina Granja, Glen D. Rodríguez Rafael**, The preservation of digital evidence and its admissibility in the court, J. Electronic Security and Digital Forensics, vol. 9, No. 1, 2017, Peru.
11. **Gerard Johansen**, Digital Forensic and Incident Response, Birmingham,UK, 2017.
12. **Graeme Horsman**, Digital evidence and the crime scene , School of health and life sciences, Teesside University, Middlesbrough, Tees Valley, United Kingdom, science&justice 61 (2021) 761-770.
13. **INTERPOL**, Guidlines For Digital Forensics First responders, march 2021.

14. **ISO/IEC 27037:2012**, is an international standard that provides guidelines for the identification, collection, acquisition, and preservation of digital evidence, with a particular focus on the roles of Digital Evidence First Responders (DEFR) and Digital Evidence Specialists (DES). The standard was developed by ISO and IEC to ensure that evidence remains intact by following strict procedures.
15. **K. Loughheed**, A Border Gateway Protocol (BGP), Network Working Group, T.J. Watson Research Center, IBM Corp, June 1998.
16. **Larry Daniel, Lars Daniel**, Digital Forensics For Legal Professionals, 2012,USA.
17. **M. Bas Seyyar, Z.J.M.H Geradts**, Privacy impact assessment in large-scale digital forensic investigations, Forensic Science International: Digital Investigation, university of Groningen, PO Box 72, 9700 AB Groningen, Netherlands, 17 January 2020.
18. **Michael Dooley and Timothy Rooney**, DNS Security Management, First Edition, 2017 by The Institute of Electrical and Electronic Engineers, Inc. Published 2017 by John Wiley & Sons, Inc.
19. **Nagendra Kumar Nainar, Ashish Panda** , Wireshark for Network Forensics, North Carolina, NC, USA.
20. **Pat Dalton**, The Internet: A Primer, INFORMATION BRIEF, Minnesota House of Representatives, Research Department, October 1998.
21. **Perry Xiao**, Designing Embedded Systems and the internet of things (IoT) with the ARM Mbed, London south Bank University, first edition, 2018, UK.
22. **Peter Mell, Timothy Grance**, The NIST Definition of Cloud Computing, Special publication 800-145, september 2011, USA.
23. **Ric Messier**, NETWORK FORENSICS, 2017, Canada .
24. **Robert C. Newman**, Computer Forensics, Evidence Collection and Management, 2007 By Taylor & Francis Group, USA, P 109.
25. **ROBERT KAMARGI**, Cyber Forensics, n.p, no pub.

26. **SETH ENOKA** , CYBERSECURITY FOR SMALL NETWORKS: A NO-NONSENSE GUIDE FOR THE REASONABLY PARANOID, 2023, San Francisco, USA.
27. **T.Janarthanan, et al**, IOT Forensics: An Overview of the Current Issue and Challenges, Sheffield Hallam University, Sheffield, England .
28. **U.S.Departments of Homeland Security**, United States Secret Service, Best Practices for Seizing Electronic Evidence, V4.2, A Pocket Guide for First Responders.
29. **Vibha Soni**, IOT for Beginners, FIRST EDITION, 2022, India.
30. **Vivek Kale**, Creating Smart Enterprises, 2018, New York, USA.

French References:

1. **Loi n° 25-14** du 9 Safar 1447 correspondant au 3 août 2025 portant code de procédure pénale, JOURNAL OFFICIEL DE LA REPUBLIQUE ALGERIENNE N° 54, 13 août 2025, Art 114-116.
2. **Loi n° 09-04** du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relative la prévention et à la lutte contre les infraction liées aux technologies de l'information et de la communication, JOURNAL OFFICIEL DE LA REPUBLIQUE ALGERIENNE N° 47, 16 août 2009.

Arabic References :

1. **ايت حمودة كاهنة**، البحث و التحري الجنائي في مسرح الجريمة الالكترونية ، جامعة حسنية بن بوعلي، الشلف ، مجلة الفكر القانوني و السياسي، المجلد السابع العدد الاول (2023) ، تاريخ نشر المقال 2023/05/15.
2. **براهيمي جمال**، التحقيق الجنائي في الجرائم الالكترونية، اطروحة نيل شهادة الدكتوراه، جامعة مولود معمري - تيزي وزو، الجزائر.
3. **صهيب سهيل غازي زامل**، البحث و التحري عن الدليل الالكتروني في المسائل الجزائية، دراسة مقارنة ، اطروحة الحصول على شهادة الدكتوراه، كلية الحقوق و العلوم السياسية، جامعة وهران 2، الجزائر.
4. **عائشة بن قارة مصطفى**، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دراسة مقارنة، رسالة ماجستير، كلية الاسكندرية، مصر، 2009.

Contents

Dedication

Acknowledgments

Abstract

المخلص

List Of Acronyms

INTRODUCTION.....1-2-3

CHAPTER ONE: The Theoretical and Technical Framework of The Digital Crime Scene

1.1 The Legal and Technical Definition of The Digital Crime Scene.....	5
1.1.1 The Legal Definition of The Digital Crime Scene.....	6
1.1.2 The Technical definition of The Digital crime scene	7
1.2 Types of Digital Environments	8
1.2.1 The Internet of Things (IOT)	8
1.2.2 Protocols.....	8
1.2.3 Network Servers	10
1.2.4 Metadata.....	11
1.2.5 Cloud Computing	13
1.3 The Legal Admissibility of Digital Evidence.....	14
1.3.1 Definition of Digital Evidence.....	14
1.3.2 Need for the admissibility of digital evidence.....	15
1.3.3 Increasing Awareness of Digital Evidence	15
1.3.4 Admissibility.....	16
1.3.5 Authenticity and Reliability	17
1.3.6 Casey's Certainty Scale	17
1.3.7 Best Evidence	18
1.3.8 Scientific Evidence	18
1.3.9 The probative value of digital evidence under Algerian legislation	19
1.4 Challenges in digital crime scene	20

1.4.1 challenges in digital forensics	20
1.4.2 Challenging Aspects of Digital Evidence	26
Summary.....	29

CHAPTER TWO : Operational Procedures in The Digital Crime Scene

1.1 Privacy in the search and investigation of Digital Evidence	31
1.1.1 Characteristics of Electronic Evidence:	32
1.1.2 Functional Characteristics of Electronic Evidence:	32
1.1.3 Assessment of the risks to the rights and freedoms of data subjects	33
1.1.4 The measures envisaged to address the risks.....	35
1.1.5 Discussion of principles relating to processing of personal data in law enforcement sector	37
1.2 The Digital Forensic Process	38
1.2.1 Identification	38
1.2.2 Preservation	39
1.2.3 The collection.....	39
1.2.4 Examination.....	41
1.2.5 Analysis	41
1.2.6 Presentation	41
1.3 Internet Forensics.....	42
1.3.1 Network Devices	42
1.3.2 Layers of Network Abstraction	43
1.3.3 The Internet.....	44
1.3.4 Common Applications.....	46
1.3.5 MALWARE	48
1.4 Investigation Methods for Collecting Digital Evidence.....	49
1.4.1 Investigation of Computers in Operation	49
1.4.2 Special Investigation on Mobile Phone in Operation.....	51
1.4.3 Crimes and Potential Evidence	51
1.4.4 Investigative Tools.....	55
1.4.5 Role of Forensic Expert in Crime Investigation	55
Summary.....	56
General Conclusion	58
Bibliography	60

