Digital Forensics for Enterprises Beyond Kali Linux

Navigate complex legal frameworks, ensure digital evidence admissibility, and establish robust forensics laboratory environments

Abhirup Guha

www.bpbonline.com

First Edition 2025

ISBN: 978-93-65895-902

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My father – ***Late Hriday Ranjan Guha***

My mom – ***Madhumita Guha***

My wife – ***Pampa Biswas Guha***

And my little star, my boy – ***Ishayu Guha***

About the Author

Abhirup Guha holds a Master of Business Administration in Information Technology from IBMR and a Bachelor of Computer Applications from NSEC College. He also holds a Certified Information Systems Security Professional (CISSP) certification from Charles Sturt University and several cybersecurity certifications from various universities worldwide.

As an accomplished cybersecurity expert, he is passionate about sharing his knowledge and skills with individuals and businesses to help them safeguard their digital assets against emerging cyber threats. With over 15+ years of experience in the industry, he has successfully trained professionals on various topics, including cyber forensics, mobile forensics, and cybersecurity.

Beyond the boardroom, he also serves as an Associate Cyber Security and Cyber Forensic Trainer at a reputed government body, where he delivers comprehensive training on forensic cloning, steganography, and digital evidence management. As a Lead Penetration Tester and Security Auditor at a reputed organization, he helped clients secure their digital infrastructure from a consistently evolving threat landscape.

About the Reviewer

Sanyam Jain is a distinguished Cloud Security Engineer and cybersecurity thought leader with a strong record of securing complex digital ecosystems and safeguarding critical infrastructure. With deep experience across cloud security, security operations, application security, compliance, and security automation, Sanyam has helped global organizations exceed their security objectives through forward-thinking strategies and cutting-edge technology.

His core technical proficiencies span network security, threat detection and response, container and Kubernetes security, data encryption, and identity/access control, with hands-on expertise across leading cloud platforms, including AWS, Azure, and Google Cloud. He brings a DevSecOps mindset to modern development pipelines, designing secure architectures, automating compliance, and embedding security at every layer of software delivery.

Sanyam's research on security vulnerabilities has earned international recognition, featured in Forbes, TechCrunch, ZDNet, Bleeping Computer, and 40+ other prominent publications. His work reflects a relentless drive to improve digital resilience globally.

Beyond the enterprise world, Sanyam actively gives back to the cybersecurity ecosystem. He serves as a Judge for the Globee® Awards for Cybersecurity and Disruptors (2025), Stratus Awards, and the Big Awards for Business, where he evaluates emerging technologies and cybersecurity innovations. He also contributes as a Mentor of Change with NITI Aayog, fostering grassroots innovation and leadership.

As a technical advisor to startups, Sanyam helps shape and secure early-stage ventures, guiding them on cloud architecture, secure coding practices, infrastructure hardening, and regulatory compliance to build defensible businesses from day one.

He contributes to global cybersecurity resilience through partnerships with NGOs like the GDI Foundation and CSIRT.Global, helping safeguard critical internet infrastructure. He's also a technical reviewer for key publications from Apress and BPB, strengthening community access to high-quality learning content.

Sanyam holds a Master's in Technology from BITS Pilani (with distinction) and is a Certified Kubernetes Administrator (CKA). He's mentored thousands of learners via platforms like Udacity, Rooman Technologies, and QwikSkills, empowering the next generation of cybersecurity professionals.

With a unique blend of technical depth, community leadership, and startup advisory, Sanyam Jain is not only defending the cloud but helping define its future.

Acknowledgement

I would like to express my sincere gratitude to all those who contributed to the completion of this book.

First and foremost, I extend my heartfelt appreciation to my family and students for their unwavering support and encouragement throughout this journey. Their love, support, and encouragement have been a constant source of motivation.

I am immensely grateful to BPB Publications for their guidance and expertise in bringing this book to fruition. Their support and assistance were invaluable in navigating the complexities of the publishing process.

I would also like to acknowledge the reviewers, technical experts, and editors who provided valuable feedback and contributed to the refinement of this manuscript. Their insights and suggestions have significantly enhanced the quality of the book.

Last but not least, I want to express my gratitude to the readers who have shown interest in my book. Your support and encouragement have been deeply appreciated.

Thank you to everyone who has played a part in making this book a reality.

Preface

Cybercrimes, data breaches, and online fraud are now daily headlines in today's times, thus triggering the need for professional digital forensics experts. This book is authored from the intersection of technological advancement and the urgent need for investigative skills in the digital space. This book seeks to provide a comprehensive and practical handbook for handling the complex world of digital evidence and cyber investigations.

The handbook on digital forensics is aimed at future practitioners and forensic analysts interested in learning more about digital investigations. The book progresses from simple concepts such as evidence handling and chain of custody to advanced concepts such as malware analysis, cloud forensics, and mobile device analysis. The book follows a step-by-step methodology based on case studies and industry needs. All the chapters are made readable, actionable, and relevant to today's legal and ethical standards.

The content of the handbook on digital forensics has been sourced from years of experience, research, and collaboration with law enforcement, legal, and cybersecurity professionals. It bridges the gap between practice and theory and encourages critical thinking and systematic problem-solving. Whether you are preparing for a certification exam, building internal incident response capacity, or working a case in the field, the advice in these pages will be your trusted guide.

I would like to extend my thanks to the authors who have shared their knowledge, and to the readers who strive to maintain the integrity and efficacy of digital investigations on a daily basis. My hope is that Handbook on Digital Forensics will enable you to reveal the truth concealed in data, and to do so with accuracy, professionalism, and purpose.

Chapter 1: Unveiling Digital Forensics - This chapter introduces major fields of digital forensics. Digital forensics is concerned with the application of scientifically established methods of collecting, gathering, authenticating, identifying, analysing, interpreting, recording, and presenting digital evidence. This digital evidence, gathered from electronic sources, is the foundation for re-creating the past or predicting potential unauthorized activity that can disrupt normal business operations.

Chapter 2: Role of Digital Forensics in Enterprises - The chapter will elucidate the very important role played by digital forensics in most business segments and industries. Organizations today are relying increasingly on digital infrastructure to store, process, and provide data, and hence, the significance of the role played by digital forensics in the

management of cybersecurity breaches is invaluable. Its strategic implementation allows organizations to create actionable intelligence that assists them in adjusting and improving their defenses based on the ever-evolving cyber threat landscape.

The ever-changing nature of cyber threats has made enterprise security an imperative with the inclusion of quality threat intelligence at the forefront. To properly address cybersecurity incidents, professional investigators need to utilize digital forensic methods with accuracy and consistency. Digital forensics in this regard is not just a response function but also a preemptive action in safeguarding organizational assets and processes.

Computer forensics has evolved from its initial function of investigating cybercrimes. Now, it has a more extensive function in the whole process of handling cybersecurity incidents. They range from the detection of threats and recovery of compromised data to legal compliance and regulation. Computer forensics has therefore emerged as a critical function in enterprise security measures.

The ongoing use of digital forensics in the digital era is aimed at validating a holistic application of cybersecurity. Not only does it provide for the investigation and containment of incidents, but it also ensures digital environment sustainability. As threat behavior changes in terms of sophistication, the need for forensic processes in safeguarding and maintaining trust in digital infrastructures is heightened.

Chapter 3: Expanse of Digital Forensics - Digital forensics has emerged from conventional computer forensics due to the increased dependency of contemporary businesses on a range of digital technologies. From a cybersecurity perspective, data on these digital devices is identified as digital evidence. The coverage of digital forensics today extends to various aspects of digital activity, both in hardware and network infrastructures. The digital revolution quickly pervades many business operations and hence incessantly highlights the importance of digital forensics. This is significantly propelled by the extensive application of internet technologies to facilitate business processes and address client needs. Digital forensics is also vital in incident response and compliance audits, both of which are essential for organizations to safeguard their reputation and hold a competitive advantage in their markets.

Chapter 4: Tracing the Progression of Digital Forensics - The expanding role of digital transformation has been met with an equivalent expansion of cyberattacks and cybercrimes. These threats to security must be countered effectively through the strategic application of digital forensics. The diversification and sophistication of cybercrimes have, however, enhanced the complexity of forensic investigation. This necessitates the ongoing enhancement of digital forensics to keep up with the development of new technology. The

development in the field is now focused on the incorporation of new tools and approaches to forensic simplification. This chapter attempts to examine the development of digital forensics in countering the growing complexity of cybercrime investigation.

Chapter 5: Navigating Legal and Ethical Aspects of Digital Forensics - Value allocation to the digital forensics role in the current digital age requires its correct positioning within applicable legal and ethical standards. These standards are discussed in this chapter in the context of global digitalization, which has created the need to rely increasingly on different digital devices such as smartphones, laptops, and tablets. Instant response to cybercrime and accidents is warranted for protecting organizational assets and maintaining operational continuity. Nevertheless, current cyber attacks are increasingly sophisticated in nature, with malicious groups being behind them in most cases, with the intention to damage the reputation and credibility of firms operating in their own industry.

Chapter 6: Unfolding the Digital Forensics Process - The digital forensic analysis can take a long time, mainly due to the complexity of analyzing the digital devices utilized. This is due to the fact that the devices have a lot of diverse data. The data comes in various forms, in the modern digital age, including documents, emails, pictures, videos, log files, and encrypted files, all of which have to be analyzed in detail in a case of investigation.

Chapter 7: Beyond Kali Linux - Kali Linux is renowned in the field of digital forensics owing to its immense potential in penetration testing and cybersecurity evaluation. Its extensive set of built-in tools makes it a popular operating system among forensic experts. Forensic tools like Autopsy, Wireshark, and Volatility are integrated, and they are capable of performing detailed and efficient forensic analysis. Exclusive reliance on Kali Linux is limiting for cybercrime investigators because there is no single platform that can address all investigative hurdles. The rising popularity of Kali Linux in digital forensics is a reflection of the growing complexity of modern cybercrimes. The chapter continues to introduce a variety of forensic tools employed under varied investigative scenarios.

Chapter 8: Decoding Network Forensics - Modern organizations today are dependent on networks of interconnected digital devices to increase their efficiency and provide uninterrupted customer service. This dependence, however, tends to attract external assailants who attempt to compromise such systems. The opportunity, therefore, for digital forensic investigators to carry out thorough and methodical investigations of the device networks at cybercrime scenes is provided. Forensic investigators will perform different tasks like packet analysis, log examination, incident response, and attack reconstruction. As technology advances and the configuration of device networks within organizations gets more complex, forensic experts are required to resort to specialized tools to probe. Wireshark, Zeek, Snort, Splunk, Forensic Toolkit (FTK), and NetworkMiner are examples

of some tools that are very important for this line of inquiry. This chapter focuses on the field of network forensics and the current practices and standards in digital forensics.

Chapter 9: Demystifying Memory Forensics - Memory forensics is crucial to cybersecurity and digital forensics, for it allows investigators to analyze RAM, which is a type of volatile memory, in order to detect evidence of malicious activities. Unlike disk forensics, dealing with persistent storage, memory forensics affords a live view of the state of a system, revealing crucial details about active processes, open connections, encryption keys, and possibly even malware. This chapter discusses different aspects of memory forensics that demonstrate its worth to digital forensic investigators in providing valuable and necessary results for effective investigations.

Chapter 10: Exploring Mobile Device Forensics - Smartphones have become the object of choice for cyber adversaries due to growing dependence on them. These attacks begin on mobile devices, among many modern cybercrimes that target individuals. Following the rise of mobile forensics as an important branch of digital forensics, therefore, comes mobile forensics. Mainly, mobile forensics pertains to the area of digital forensics that concerns itself with the extraction, analysis, and presentation of data on mobile devices that include but are not limited to cell phones, smart tablets, and GPS units. It serves criminal investigations, cybersecurity, and corporate security equally. This chapter focuses on mobile forensics and the techniques and tools employed during evidence acquisition and analysis.

Chapter 11: Deciphering Virtualization and Hypervisor Forensics - Virtualization means running more than one operating system inside one physical machine using hypervisors. It makes digital forensic investigations more complex. Investigating virtualized environments is complicated due to multiple factors such as shared resources, layered data storage, and live migration. All of these factors complicate the forensic process. Hence, knowledge of virtualization and hypervisor forensics is mandatory to overcome these challenges. Typical applications of virtualization are cloud computing, enterprise IT infrastructures, and cybersecurity sandboxes. This chapter examines how the effective interpretation of virtualization and hypervisor forensics is useful to digital forensic investigators in resolving cyberattacks more quickly.

Chapter 12: Integrating Incident Response with Digital Forensics - The organizations have been increasingly dependent on networks of digital devices, and at the same time, they are encountering a greater number of incidents of cybercrime. Complexity in incidents comes with a drastic need for highly sophisticated investigation procedures, as emphasized by the need for digital forensics. The combination of incident response (IR) and digital forensics leads to possession of a much broader and better-managed approach

to handling incidents of a security nature by organizations. This aids not only in the resolution of current problems but also in the collection of credible threat intelligence (TI) that will prevent similar incidents from occurring again in the future. The chapter will look into the linkages between incident response and digital forensics in regards to how they can be used to improve the overall actions toward any cybersecurity effort.

Chapter 13: Advanced Tactics in Digital Forensics - Advanced cyber attacks are highly evasive even for most forensic methods. It is fast becoming apparent that classical means cannot simply keep pace with the complexities introduced by advanced cyber threats, their encrypted data, and various anti-forensic techniques designed to hinder investigations. Advanced forensic techniques enable the extraction of hidden evidence and the analysis of complex cyber incidents, thereby helping to strengthen legal cases. The succeeding section shall showcase these advanced digital forensics techniques and their enhancement of the investigative art.

Chapter 14: Introduction to Digital Forensics in Industrial Control Systems - Digital transformation has a truly consequential impact on many critical areas such as energy, manufacturing, water supply, and transportation. With increased penetration of industrial control systems (ICS) into these sectors, these sectors become prone to cyber threats. This chapter discusses the aspects of digital forensics in a protection scheme for ICSes and critical infrastructural security. It examines the vulnerabilities in this area that lead to disruptions, which, if they harm the stakeholders involved, can result in severe repercussions across the vital sectors.

Chapter 15: Venturing into IoT Forensics - The rapid growth of the Internet of Things (IoT) has brought about a transformation in diverse industries, connecting billions of devices across healthcare, transportation, industrial systems, and smart cities. But there is a flip side to this general acceptance of IoT devices - the detection of security loopholes and new forensic challenges, which have made IoT forensics a prime area of interest in digital investigations. Unlike those of traditional computing systems, IoT ecosystems are a heterogeneous group of devices with diverse hardware, operating systems, and communication protocols. For this reason, investigators experience serious difficulties in data acquisition, evidence preservation, and forensic analysis. Furthermore, many IoT devices have limited storage and processing capabilities, which makes this transient data very difficult to analyze forensically. The chapter focuses on IoT forensics and supports the discussion on forensic issues, methods, legal issues, and real-world case studies. In addition, it will present a demonstration of best practices along with tools to perform forensic study inside smart environments so that whenever digital evidence from IoT devices, cloud services, and network logs is collected, it will be efficiently analyzed by forensic professionals.

Chapter 16: Setting Up Digital Forensics Labs and Tools - The establishment of a well-equipped digital forensics lab is important for investigations that are efficient, reliable, and hold space in a court of law. Such labs provide a conducive environment that allows forensic analysts to have access to tools, infrastructure, and security measures for analyzing digital evidence. The lab ensures that the integrity of the forensic investigation is preserved, the chain of custody remains intact, and legal standards are adhered to. Knowledge of the capability of tools and their limitations allows forensic professionals to select the most suitable analysis tool for any particular evidence pertaining to digital objects for an investigative situation. This chapter will give a practical, complete guide on how to establish digital forensics labs and select suitable tools for investigation.

Chapter 17: Advancing Your Career in Digital Forensics - Digital forensics is quickly changing its pace through technology innovations, increasing cyber threats, and gradually complicated legal issues. Organizations are more intensively concentrating on cybersecurity and digital investigations, so the demand for skilled professionals might increase in digital forensics. However, a successful career in this specialization was not an easy journey; it means building a solid technical foundation, gaining hands-on experience, and committing oneself to lifelong learning. Whether working for law enforcement, private security companies, governmental agencies, or corporate cybersecurity, professionals will always be on their toes with the latest tools, investigative methods, and legal requirements. Being equipped with industry certificates and having presented practical experience in forensic investigation may materially advance the career of an individual. In this sense, this chapter reviews interesting career avenues, critical skills and certifications, and trends in the industry as a guide for budding and mature professionals in taking their career advancements in digital forensics.

Chapter 18: Industry best practices in Digital Forensics - Digital forensics is fast-paced and multidimensional, and combines elements from cybersecurity, law enforcement, and corporate investigations. Rising cyber threats have made it more and more common for institutions to rely on digital forensics for evidence collection and increased security. Digital forensics foundation and growth show increasing dimensions in terms of application from simple file recovery techniques of the past to the most up-to-date techniques used today in analyzing cybercrimes and data breaches. The ever-growing digital footprint brought about by technologies such as cloud computing and IoT makes development even more complex. This chapter discusses industry best practices and considers career opportunities that exist in an ever-progressing digital forensics environment.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/mljjnju

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Unveiling Digital Forensics

Introduction

This chapter will cover digital forensics. Digital forensics is the use of scientifically derived and proven methods to preserve, collect, validate, identify, analyze, interpret, document, and present digital evidence derived from digital sources to facilitate or further reconstruct events or help anticipate unauthorized actions that can be disruptive to planned business operations.

Structure

The chapter covers the following topics:

- Understanding digital forensics
- Rules of computer forensics
- DFRWS investigative model
- Six A(s) of digital forensics
- Skills required for digital forensic investigator
- Digital evidence
- Types of digital forensics

- Digital forensic tools and their purposes
- Primary techniques of digital forensic analysis
- Incident response

Objectives

The objectives of this chapter are to develop a detailed understanding of digital forensics from the perspective of its role in modern-day crime investigation. We will also learn how to be aware of different skills that are required by digital forensic investigators to proceed with digital forensic investigation and develop a basic understanding of digital evidence from multiple perspectives, including legal considerations. We will also learn to acquire a preliminary understanding of incident management from the perspective of the digital world.

Understanding digital forensics

The progress of digital forensics Investigation conforms to different types, but primarily, the concerned principles and procedures remain the same, more or less. This relates to effective analysis of digital evidence to identify the root cause of a cybersecurity incident. The tendency of digital forensic investigators relates to resisting recurrences of cybersecurity incidents within the organizational environment. This leads to the overall success of a digital forensic investigation, relying on the expertise of associated investigators on the effective interpretation of data after using relevant information retrieval tools. The long-term experience of forensic investigators encourages them to select effective tools that can generate reliable results and thereby be considered as trustworthy for upcoming investigation procedures. Digital forensics gradually emerged as the Science of forensics combined with the art of investigation. The observed stages of digital forensics can be categorically represented as follows in *Figure 1.1*:

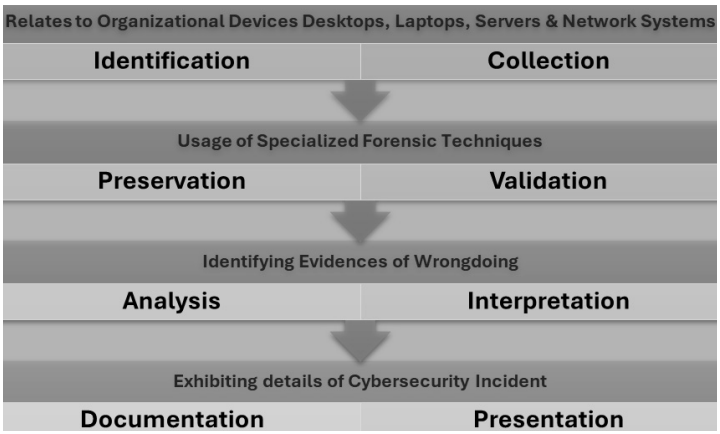

Figure 1.1: *Procedure of handling digital evidences in digital forensics*

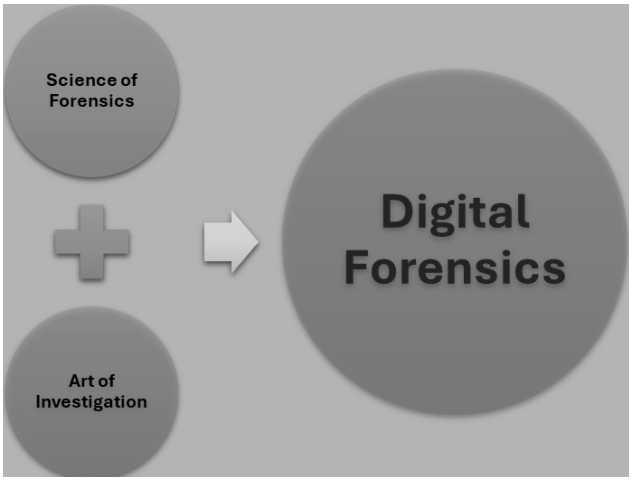

Figure 1.2: *Pillars of digital forensics*

Digital forensics is the combination of the science of applying appropriate methods and deductive reasoning to data, along with the art of interpreting this data to reconstruct an event as depicted in *Figure 1.2*.

The goal of conducting evidence analysis by investigators relates to finding the facts and thereby using them to reconstruct the true course of an event. The revelation of truth from a forensic investigation relates to discovering and exposing the remnants (traces) of the event left on the system. The remnants in forensic investigation are identified and referred to as artifacts or evidence during legal proceedings. The progress of simple tasks during the creation of artifacts apart from their cleaning that leaves additional artifacts.

Digital forensics investigators must apply the two tests for digital evidence for the aspect of survival in a court of law which includes authenticity and reliability. The importance of the authenticity test for digital evidence relates to uncovering its sources, as shown in the following *Figure 1.3*:

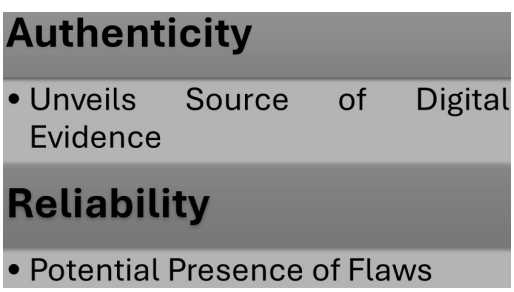

Figure 1.3: *Assessment of digital evidence*

Similarly, the importance of reliability for digital evidence relates to assessing the potential flaws present within it.

The detailed digital forensic investigation reveals the modes of attack that resulted in the occurrence of the incident. **These modes of attack are illustrated in** *Figure 1.4.* This includes insider attacks, implying a possible breach of trust from employees within an organization.

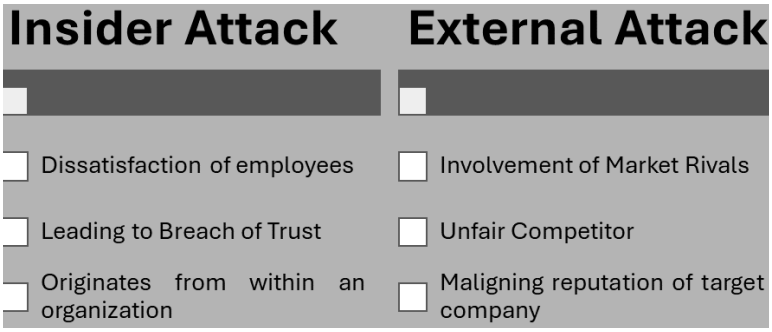

***Figure 1.4**: Modes of attack*

Otherwise, the occurrence of external attacks relates to hiring hackers by competitors to promote unhealthy market competition. The hired external hackers are instructed by competitors to target and destroy the reputation of their market rivals.

Rules of computer forensics

A good forensic investigator should always abide by specific rules to lead a fruitful forensic investigation procedure, as illustrated in *Figure 1.5*. These include proceeding with the due investigation with duplicate images of evidence instead of the original evidence. This is crucial in terms of refraining from tampering with the digital evidence. This is because the loss of integrity by digital evidence can lead to losing its admissibility in the Court of Law. Furthermore, digital evidence tends to be crucial for crimes in the modern-day digital world. The effective preservation of original digital evidence and thereby using only its image for the investigation procedure is essential to maintain the overall integrity of the evidence. This is because using only the image of digital evidence resists frequent handling of evidence and thereby avoids the possible occurrence of integrity loss.

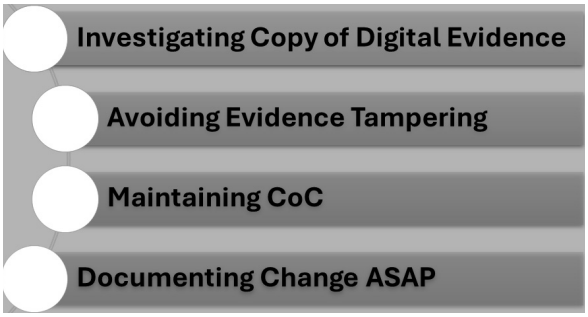

***Figure 1.5:** Best practices of digital forensics investigation*

The rules for leading forensic investigations further include preparing a duly filled-out **Chain of Custody** (**CoC**) to encourage careful handling of evidence. The importance of maintaining the CoC of Evidence relates to timely documenting changes in evidence during an investigation. This is in addition to implying in the Court of Law that the digital evidence has been handled with due care during the phase of investigation. The importance of these rules for investigation relates to increasing the overall value and defensibility of the concerned case. The detailed documentation of a digital forensic investigation, carried out by a designated team of investigators, is crucial for its verification by another team of investigators, as per the direction of the Court of Law in the future, if needed for the benefit of the case. The forensic investigators are required to face a complex landscape of laws and regulations, and this requires them to meticulously document the details of digital evidence investigation.

DFRWS investigative model

This is a standardized investigative model for the progress of digital forensic investigations, consisting of multiple stages. The uniqueness of this model relates to considering individual digital devices to be a digital crime scene for investigators. The relevant stages of this model are listed as follows, as well as illustrated in *Figure 1.6*.

- **Identification:** The basis of Forensic Sciences is based on the Exchange Principle of Locard, which relates to the exchange of traces. The modern digital world resembles the combination of two systems that result in their exchanging traces. For instance, if an individual browses a website, the web server or web application firewall may record the individual's IP address within a collection log. This principle can guide the identification of potential sources of evidence during an incident. E.g., identifying the root cause of a malware infection requires starting with an analysis of the infected system by searching the firewall connection or proxy logs for any outbound traffic from the infected system to external IP addresses. This may reveal the C2 Server.
- **Preservation**: This subsequent phase, after evidence identification, relates to safeguarding it from any modification or deletion. This is done by enabling the controls to protect the potential evidence, e.g., log files, from removal or modification. Considering the host systems, such as desktops, isolate the potential digital evidence from the rest of the network, either through physical or logical controls, or through network access controls, etc. It is critical that the users not be allowed to access a suspect system to prevent deliberate or inadvertent integrity tampering of evidence. The required preservation of evidence in virtual systems is achieved through snapshotting systems, cloning the system, and saving on non-volatile storage.
- **Collection (media)**: The investigators initiate the actual process of digital evidence acquisition, and during this phase, consider the volatility of the evidence. Considering the network equipment, this could include active connections or log