Cyber Forensics Up and Running

A hands-on guide to digital forensics tools and technique

Tarun Vashishth

www.bpbonline.com

Copyright © 2024 BPB Online

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor BPB Online or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

BPB Online has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, BPB Online cannot guarantee the accuracy of this information.

First published: 2024

Published by BPB Online
WeWork
119 Marylebone Road
London NW1 5PU

UK | UAE | INDIA | SINGAPORE

ISBN 978-93-55517-180

www.bpbonline.com

Dedicated to

In deep appreciation for my family — my grandparents, the sturdy pillars of our lineage, who laid the foundations of character and resilience; my parents, the unwavering backers of my dreams and my lighthouse to weather any storm; my aunts and uncles, the protective walls whose support forms a fortress of comfort and cheerleaders of my milestones. Not just my siblings, but my friends and co-conspirators, who have shared in every laugh and every challenge; and my wife, the true co-pilot in our life's adventures, and a steadfast companion on this remarkable odyssey.

About the Author

Tarun Vashishth, a seasoned professional in the field of cybersecurity, brings a wealth of hands-on experience and knowledge to his latest endeavor, ***Cyber Forensics Up and Running***. With an extensive career spanning renowned organizations such as McKinsey & Company, IAC, and Philips Electronics NA, Tarun has played pivotal roles in setting up enterprise security operations centers, has led incident response, and threat hunt teams, oversaw security engineering, set up and led automation teams in cyber security.

His professional journey is marked by achievements that include leading the engineering team as product manager to build and deliver a custom threat intel platform and SIEM, reporting bugs in a well-renowned EDR solution and in a phishing simulation platform, and leading the implementation of the custom incident case management system.

Tarun's relentless pursuit of learning cyber security started in 2011 by acquiring the knowledge and certificate of **Certified Ethical Hacker** (**CEH**) and then getting a master's degree in computer/cyber forensics and counters. He is also a recipient of the Sourcefire (now part of Cisco) student scholarship. He has acquired a couple of certificates and training from SANS, EC-Council, AWS, Microsoft, Splunk, CarbonBlack(now part of VMware), Agile Foundation, and Carnegie Mellon University.

About the Reviewer

Srikanth Addagatla is a certified and experienced cybersecurity professional with expertise in digital forensics, cyber defence, incident response, Security Operation Centre (SOC), hypothesis-based threat hunting, threat intelligence-driven proactive detection and monitoring, and malware analysis. He has a robust background working with various global organizations spanning multiple industries, including financial services, technology, healthcare, government, and data centres. He has a successful record of accomplishment of leading and conducting comprehensive forensic investigations into various incidents such as ransomware attacks, malware outbreaks, exploits, Business Email Compromise (BEC), and additional cyber threats. His ability to effectively determine the appropriate course of action has enabled him to mitigate risks and fortify defences against potential cyber threats, ensuring the security and integrity of the organizations he serves. He is a strong engineering professional who graduated with distinction in M.Tech focused on Computer Networks and Information Security. Additionally, he has obtained a Post Graduate Diploma specialized in Cyber Laws and IPR from the University of Hyderabad, along with other industry certifications and contributed content to a wide array of cybersecurity publications.

I would like to express my gratitude to my family and friends, whose unwavering understanding and support have been invaluable in every aspect of my life. A heartfelt thank you goes to my teachers and my peers for their continuous support throughout my cybersecurity journey. Last but not least, I extend my thanks to the cybersecurity community for their continuous sharing of knowledge and unwavering support in protecting and detecting threats within organizations.

Acknowledgement

The role of my family has been fundamental in the journey of bringing this book to fruition. Spanning nearly a year, filled with unexpected twists and turns, it was the support of my loved ones who not only saw me through but also made this process an unforgettable experience. The journey of writing this book has been as much an odyssey of personal growth as it has been a professional endeavor. It stands on the shoulders of many who have contributed to the foundations of learning and research that have shaped my career.

I owe a debt of gratitude to my teachers and professors, who have been the architects of my education. A special thank you to Professor Jim Jones, who not only gave me the opportunity to work alongside him on a research project but also challenged me to seek solutions independently. His lessons on relishing the pursuit of research have been invaluable. I extend my heartfelt appreciation to my advisors, sponsors, and managers. Their trust and belief in my potential provided me with opportunities crucial in honing my expertise in cybersecurity. They exposed me to complex problems and challenges, which allowed me to practice and apply my knowledge and instilled in me the problem-solving approach and confidence essential in compiling this book.

To the cybersecurity and digital forensics community: this book is a testament to the collective wisdom and spirit of sharing that defines our field. The access to community-driven materials in the early stages of my career was a beacon that guided my path from student to professional. To my colleagues, professionals, and researchers who generously share their knowledge and experiences, your contributions are the foundation of our community's growth and success. Finally, my heartfelt thanks go to the unsung heroes at BPB Publications. To the team members who have worked tirelessly behind the scenes, your dedication and meticulous attention to detail have been invaluable. This book is as much your creation as it is mine.

Preface

This book stands as a tribute to my grandparents, both maternal and paternal, reflecting their enduring legacy. Their belief in education and perseverance has always been a guiding light in my career, and deeply influenced interactions with aspiring cybersecurity enthusiasts and seasoned professionals alike.

I encountered two individuals at pivotal points in their careers: one, a student eager to enter the cybersecurity field, and the other, a cloud administrator aspiring to pivot to digital forensics. Their quest for practical, real-world knowledge underscored a void in available resources, especially in curated hands-on applied material. This gap in finding a single, comprehensive guide that could kick start their journey inspired this book, where I aim to curate knowledge and insights drawn from my education and career, offering a practical guide that addresses this critical gap.

Embarking on this journey, I sought to create a manual that is fundamentally practical, designed to serve not just as a reference but as a hands-on guide through the multifaceted world of digital forensics. The eleven chapters of this book are carefully crafted to guide readers from foundational concepts to the advanced techniques required in a professional setting.

From setting up your digital forensics lab to learning and practicing complex digital forensics concepts, tools, and techniques, this book is structured to build your understanding and skills progressively. As you delve into the realms of computer system and network forensics, legal frameworks, and emerging technological challenges, you will be guided by real-world scenarios and practical exercises that emulate the work of a digital forensics investigator.

The book's journey will take you through various facets of digital evidence, including volatile and non-volatile data, live forensics analysis, and the intricacies of file systems and Windows Registry analysis. You'll also explore browser forensics, anti-forensics techniques, and the constantly evolving landscape of cybersecurity challenges.

"Cyber Forensics Up and Running" is tailored for:

- Students who are eager to move beyond theoretical concepts to gain hands-on experience.
- IT professionals who wish to pivot into the digital forensics field.
- Security managers who aim to deepen their understanding to better support their teams.

This book is not just to be read; it is to be worked through, step by step, as a personal lab partner. *It is for those who are ready to engage with the content, and who are eager to follow a guide that is every bit as practical as it is informative***. *If you are not ready for this active learning journey, this book might not be the right fit for you*.** But if you are willing to embrace the labs and exercises contained within, this book will be a valuable ally on your journey.

Chapter 1: Introduction to Essential Concepts of Digital Forensics – This chapter lays the foundation for the entire book, introducing the basics of digital forensics, the types of cases commonly encountered, and the interplay between digital forensics and other cybersecurity fields. This chapter sets the stage for understanding the breadth and depth of digital forensics. Readers will gain a comprehensive view of the digital forensics landscape, setting the stage for more specialized topics in subsequent chapters.

Chapter 2: Digital Forensics Lab Setup – Here, we dive into the practical aspects of setting up a digital forensics' lab. The chapter discusses virtual machine environments, essential tools, and applications needed to create an effective lab setup.

Chapter 3: Data Collection: Volatile and Non-Volatile – The focus is on the critical task of data collection in digital forensics. The chapter distinguishes between volatile and non-volatile data, explaining their importance in forensic investigations. It elaborates on various methods and tools for data acquisition, such as FTK Imager and Linux Memory Extractor, providing practical knowledge for capturing crucial digital evidence. This chapter is pivotal in understanding the nuances of different data types and the best practices for their collection, which is a cornerstone of any forensic investigation.

Chapter 4: Forensics Analysis: Live Response – This chapter focuses on live forensics analysis, an increasingly important aspect of digital forensics in responding to incidents. It explains the significance of live analysis, the tools and techniques for volatile data collection, and the integration of digital forensics with incident response. This chapter is particularly relevant for those interested in understanding how to respond to live cyber incidents and the role of forensics in real-time scenarios. It provides the necessary insights for a comprehensive approach to incident response and digital forensics integration.

Chapter 5: File System and Log Analysis – Chapter 5 discusses techniques for analyzing key system components like the Master Boot Record and Master File Table, along with methods for file recovery and system log analysis. The chapter empowers readers to detect and retrieve subtle digital traces that could be pivotal in an investigation, showcasing the depth and detail required in forensic examinations.

Chapter 6: Windows Registry and Artifacts – The windows registry and artifacts chapter explores the in-depth exploration of the Windows Registry, a goldmine for forensic investigators. It teaches readers how to extract, analyze, and interpret data from the registry, providing insights into user activities and system configurations. This chapter is essential for understanding the wealth of information stored in the Windows Registry and how to use it effectively in digital forensic investigations.

Chapter 7: Network Data Collection and Analysis – In Chapter 7, the focus shifts to network forensics, a critical component of digital investigations. It covers the fundamentals of network data collection and analysis, including the use of tools like Wireshark and Tshark. This chapter provides foundational knowledge for conducting thorough network forensic investigations.

Chapter 8: Memory Forensics: Techniques and Tools – This chapter introduces readers to memory forensics, a specialized field within digital forensics. It discusses various tools and techniques for extracting and analyzing data from system memory, offering insights into the volatile aspects of digital evidence. Readers will learn about tools like Volatility, an essential tool for any forensic practitioner focusing on memory analysis.

Chapter 9: Browser and Email Forensics – In Chapter 9 of 'Cyber Forensics Up and Running,' we dive deep into the technical intricacies of Browser and Email Forensics. This chapter is your guide to the systematic examination of digital artifacts left behind by web browsers and emails. From dissecting browser architectures and analyzing artifacts to mastering email header analysis, we will cover the tools and knowledge necessary for digital forensic professionals to uncover crucial evidence.

Chapter 10: Advanced Forensics Tools, Commands and Methods – In Chapter 10 of 'Cyber Forensics Up and Running,' we delve into Advanced Forensics Tools and Methods. This chapter equips you with a toolbox of advanced techniques and methodologies to navigate complex digital investigations effectively. From command-line utilities to GUI-based tools, we explore the intricacies of forensic analysis. Additionally, we harness the power of Open-Source Intelligence (OSINT) to extract valuable insights. This chapter is your gateway to mastering the tools and methods that seasoned digital forensic professionals rely on to uncover critical evidence.

Chapter 11: Anti-Digital Forensics Techniques and Methods – We explore the concept of anti-forensics, dissecting its goals and techniques. From data hiding using tools like Steghide and StegDetect to encryption, data obfuscation, and data manipulation, we scrutinize the arsenal of techniques used by digital adversaries. Furthermore, we delve into the challenges faced by digital forensic practitioners in countering these anti-forensic tactics. This chapter equips you with the knowledge to recognize and respond to the covert methods employed to obstruct digital investigations, providing a vital perspective in the world of digital forensics.

The book aims to not only impart knowledge but also to inspire a deeper interest and understanding of the dynamic field of digital forensics. Whether you are a student, a professional in the field, or simply someone with a keen interest in digital forensics, this book offers valuable insights and practical knowledge to enhance your understanding of this essential aspect of cybersecurity.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/nk8madm

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Cyber-Forensics-Up-and-Running.
In case there's an update to the code, it will be updated on the existing GitHub repository.

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.

Did you know that BPB offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.bpbonline.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at :

business@bpbonline.com for more details.

At **www.bpbonline.com**, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on BPB books and eBooks.

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

Introduction to Essential Concepts of Digital Forensics

Introduction

Welcome to practical digital forensics. This book is your gateway to the world of digital investigation, offering a comprehensive guide to mastering this dynamic field. In a rapidly evolving digital landscape, the demand for skilled professionals in digital forensics has never been greater. The chapters are structured to equip you with the knowledge and tools necessary for success as a digital forensics investigator.

The first chapter serves as your gateway to the realm of digital forensics. It begins by defining digital forensics and discussing the types of cases that fall under its purview. Furthermore, it explores the relationship between digital forensics and other fields of cybersecurity, providing readers with a context for the role digital forensics plays in the broader security landscape. This chapter also delves into the modern technological growth of the past and reviews future technologies and digital forensics challenges in the modern tech era.

Additionally, you will learn about Locard's exchange principle, the different types and categories of digital evidence, and the techniques used to preserve evidence integrity, such as chain of custody, hashing algorithms, digital signatures, and write blockers. Finally, the chapter explains the differences between file carving and file recovery and covers time objects and their location on NTFS file systems.

Chapter 2, Digital Forensics Lab Setup, takes a practical approach, guiding you in setting up a virtual environment, mastering cloning and snapshots, and familiarizing you with essential tools like HxD, The Sleuth Kit, Autopsy, Volatility, and more.

Subsequent chapters explore volatile and non-volatile data, live forensics analysis, file systems, Windows Registry analysis, network forensics, memory forensics, browser forensics, and anti-forensics. Along this journey, you will gain the knowledge and skills to uncover hidden truths, identify suspicious activities, and make informed decisions in digital investigations.

This book is not just informative, but it is a practical resource designed to empower you with expertise in digital forensics. Each chapter builds on the last, deepening your understanding and hands-on experience. Join us on this journey of discovery, where each chapter reveals a new facet of digital investigation, and the possibilities are endless.

Structure

In this chapter, we will discuss the following topics:

- What is digital forensics?
- Types of cases in digital forensics
- Digital forensics and other fields of cybersecurity
- Digital and cyber technological growth
- The future of modern cyber world
- Modern technological explosion and its cyber security challenges
- Digital forensics challenges in the cyber modern era
- Phases of digital forensics
- What is data acquisition?
- Types of image formats
- Locard's exchange principle
- Types of digital evidence/data
- Categories of digital evidence
- Preserving digital evidence integrity
- File carving
- Digital forensics time objects - MAC(b)

Objectives

By the end of this chapter, readers will have a solid understanding of the key concepts and challenges involved in digital forensics, as well as the techniques used to preserve digital evidence integrity.

What is digital forensics?

Digital forensics is the process of using scientific methods to collect, preserve, analyze, and present digital evidence in a court of law in a legally permissible manner. It is a branch of forensic science that deals with recovering and investigating digital data to help law enforcement agencies, businesses, and individuals understand and use digital proof to solve crimes and disputes.

Types of cases in digital forensics

Digital forensics experts have to deal with various types of cases. Let us see a few examples in this section.

Computer crime

Digital forensics analysts may be called upon to investigate crimes committed using a computer or other digital device. It could include hacking, identity theft, data exfiltration, sabotage, etc.

For example, a financial institution suspects that an employee has been using a compromised credit card to make fraudulent purchases online. Digital forensics investigators would be called to examine the individual's computer and other digital devices to determine how the credit card information was obtained. They would analyze the individual's browsing history, email, and other electronic communications to look for any signs of phishing attempts or other social engineering methods that could have been used to obtain the credit card information. They would also examine the individual's computer for malware or potentially malicious software that could have been used to steal credit card information.

Corporate espionage and intellectual property theft

Digital forensics experts investigate intellectual property theft, such as the theft of trade secrets, copyrighted material, and corporate espionage cases.

For example, an employee at a company is suspected of stealing sensitive information from the company's digital assets. Digital forensics investigators would be brought in to examine the employee's computer and any other devices they may have used to access the company's network. They would use specialized software to analyze the computer's hard drive, looking for signs of data exfiltration, such as large amounts of data transferred to external devices or cloud storage services. They would also examine the employee's internet browsing history, email, and other electronic communications to determine whether the employee had any motive or intent to steal the information.

Financial fraud and embezzlement

Digital forensics experts assist financial forensics experts in collecting digital evidence, such as financial records and emails, identifying fraud, and helping prosecute criminals.

Electronic discovery

Digital forensics analysts would assist in identifying and collecting electronically stored information relevant to a legal case.

Human trafficking and drug crimes

Digital forensics experts assist by analyzing digital evidence, such as text messages and social media posts, to help identify suspects and build a case.

Child exploitation

Digital forensics analysts also help investigate child exploitation cases. They would use specialized software to search the computer's hard drive for images and videos of child pornography. They would also examine the suspect's internet browsing history, email, and other electronic communications, to determine whether the suspect had been actively searching for or distributing child pornography. They may also look for further evidence, such as chat logs or other communications related to child pornography.

Murder

Digital forensics experts would assist in investigating murder cases. They may be called upon to analyze digital evidence, such as cell phone records, social media posts, and GPS data, to help identify suspects and build a case.

Terrorism

Digital forensics experts may be called to investigate digital evidence related to terrorism activities by analyzing in-line communication and to identify individuals or groups involved in promoting or planning terrorist activities by analyzing emails, social media posts, chat groups, and applications to help identify the suspect.

In conclusion, digital forensics play a critical role in investigating digital crimes and can be used to uncover and present evidence in various cases. In each scenario, the digital forensics investigator must use a combination of technical expertise and legal knowledge to conduct a thorough and legally admissible investigation.

Digital forensics and other fields of cybersecurity

The tools, techniques, and methods used in digital forensics can be directly applied to other fields of cyber security like malware investigation, incident response, and E-discovery. It allows investigators to collect, preserve, and analyze digital evidence to uncover the truth behind cybercrime, security breaches, and other cyber and digital incidents. This section will discuss how digital forensics is used in these fields and provide detailed examples to illustrate the process.

Malware investigation and digital forensics overlap

First, let us begin with the question: *what is malware?*

Malware, or malicious software, is a type of software designed to harm or exploit computer systems. Digital forensics play a vital role in investigating malware incidents by allowing investigators to identify the origin and spread of the malware, as well as the damage it has caused.

For example, when a company detects malware on its network, a digital forensic investigator is called to examine the infected systems. The investigator would first make an image of the hard drive of the affected computer, allowing them to safely analyze the system without altering any evidence. Then, they would then use specialized software tools to analyze the malware, such as identifying the type of malware, how it entered the system, and its intended purpose.

The investigator would also look at the system's logs to determine when the malware was first introduced and track its spread throughout the network. This information is critical in identifying the source and scope of the attack and devising a strategy to respond and recover from the incident.

Once the investigation is complete, the investigator will provide a detailed report of their findings, which can be used to prosecute the attackers and help the company improve its security measures to prevent future attacks. Examples of tools and techniques that can be used in malware investigation are: