Mastering Network Forensics

A practical approach to investigating and defending against network attacks

Nipun Jaswal

www.bpbonline.com

First Edition 2024

Copyright © BPB Publications, India

ISBN: 978-93-55516-916

All Rights Reserved. No part of this publication may be reproduced, distributed or transmitted in any form or by any means or stored in a database or retrieval system, without the prior written permission of the publisher with the exception to the program listings which may be entered, stored and executed in a computer system, but they can not be reproduced by the means of publication, photocopy, recording, or by any electronic and mechanical means.

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but 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.

To View Complete
BPB Publications Catalogue
Scan the QR Code:

www.bpbonline.com

Dedicated to

*To my son, my brightest joy, **Harwin***
This book is a tribute to your laughter, curiosity, and boundless love.
May its pages reflect the magic of our shared moments,
inspire your dreams, and embody the love that binds us.

About the Author

Nipun Jaswal is a highly experienced cybersecurity professional with a rich background of over 15 years in the field. He is renowned for his exceptional expertise in safeguarding the digital world. Nipun has represented India at prestigious global events such as the BRICS Summit and Future Skills, showcasing his exceptional skills and knowledge in cybersecurity. He has authored 11 Penetration Testing and Network Forensics books, further establishing his expertise in the field.

In addition to his remarkable contributions to the cybersecurity industry, Nipun is dedicated to imparting advanced cybersecurity knowledge and education to law enforcement agencies across the world. His passion and dedication to securing the ever-evolving digital landscape have earned him several prestigious awards, including Asia's Top 100 Power Leaders in Technology, Award of Excellence, and Tech Leadership award.

As a hardcore techie, Nipun has discovered and led the discovery of multiple zero-day exploits in Enterprise Software. Currently, he is serving as a Senior Director at Protiviti India, contributing his exceptional skills and knowledge to the organization. Nipun completed his Master's in Technology from LPU, which has further strengthened his technical expertise in cybersecurity.

Acknowledgement

I extend my heartfelt gratitude to the pillars of my life who have played an instrumental role in bringing this book to fruition. First and foremost, my beloved mother, Sumeet, whose unwavering support, love, and wisdom have been the bedrock of my journey. Her encouragement has been a constant source of inspiration, guiding me through the highs and lows of the creative process.

To my dear wife, Vandana, your unwavering belief in me and your endless patience during the long hours of writing are immeasurable treasures. Your encouragement has been my motivation and added an extra layer of warmth and purpose to this endeavor.

A special acknowledgment goes to BPB Publications for their exceptional guidance and expertise. Their commitment to excellence and their belief in the potential of this work have been pivotal in bringing this book to its final form. Their collaborative spirit and insightful feedback have shaped the narrative and enriched the content.

I am also grateful for the collaborative efforts of the reviewers, technical experts, and editors who participated in the extensive revision process. Your contributions have elevated the quality of this work and added depth to its substance.

A heartfelt thank you goes out to my colleagues and co-workers in the tech industry, especially the founders of Malware Traffic Analysis.

Last but certainly not least, I extend my thanks to the readers who have shown interest in my book. Your support, enthusiasm, and engagement have made this vision a reality. Your encouragement motivates me to continue sharing my thoughts and insights.

Preface

The need for robust and effective cybersecurity measures has become more critical as our dependence on digital networks grows, and so does the threat landscape that seeks to exploit vulnerabilities for malicious intent. In this era of interconnectedness, understanding and safeguarding our digital environments is paramount.

Mastering Network Forensics delves into the fascinating world of network forensics, an indispensable discipline in securing and investigating network-related incidents. The field of network forensics is dynamic and ever-evolving, presenting professionals and enthusiasts with constant challenges and opportunities to stay ahead of cyber threats.

This book provides a comprehensive and accessible guide to understanding network forensics's fundamental principles, methodologies, and advanced techniques. From cybersecurity practitioners to aspiring digital investigators, readers will find valuable insights into the nuances of network forensics. Real-world case studies and practical examples are interwoven throughout the book to illustrate the application of concepts in actual scenarios, allowing readers to bridge the gap between theory and practice.

The book covers topics like, network protocols, network traffic analysis, log analysis, and the intricacies of digital evidence gathering. It showcases how skilled investigators can use digital trails to identify perpetrators and understand their motives.

As the world becomes increasingly interconnected, the importance of network forensics cannot be overstated. This book endeavors to equip its readers with the knowledge and skills necessary to navigate the complex landscape of digital investigations, ultimately contributing to the collective effort to secure our digital future.

Embark on this journey into network forensics, and empower yourself with the tools to unravel the digital trails left behind in the vast expanse of cyberspace. Happy reading and secure computing!

Chapter 1: Foundations of Network Forensics – This chapter will discuss important topics related to network forensics. These include different types of network forensics, the methodology involved, the sources of evidence, the collection of source data, the setup of the environment for analysis, the use of TCPDump for packet listening and data reduction, the use of Wireshark for network analysis, and a case study on a suspicious web server. This chapter aims to comprehensively understand network forensics, including its methods and tools. By the end of this chapter, readers will have a clear understanding of network forensics.

Chapter 2: Protocols and Deep Packet Analysis – This chapter will explore the intricate world of computer networking. This chapter aims to provide a solid foundation by covering the OSI and TCP/IP models, packet structure, protocols, deep packet analysis, and case studies on protocol misuse and DDoS attacks. By the end of this chapter, you will have a comprehensive understanding of these key concepts and be better equipped to navigate the complex world of computer networking.

Chapter 3: Flow Analysis versus Packet Analysis – This chapter delves into the intriguing world of Flow analysis. It provides a detailed overview of Statistical Flow analysis, which involves examining network traffic data to detect patterns and trends. You will learn about Flow Records and FRP Systems, which are crucial for storing and managing Flow data. Additionally, you will gain insights into two commonly used methods of measuring Flow, Uniflow and Bitflow. You will also discover different Sensor deployment and flow analysis types, their applications, significance, and potential limitations. Furthermore, you will understand the potential limitations of Flow analysis and when to use full packet capturing instead. By the end of this chapter, you will have a comprehensive understanding of these topics, enabling you to apply them effectively in real-world situations.

Chapter 4: Conducting Log Analysis – This chapter provides an overview of log analysis and covers various related topics. You will learn how to extract essential fields from existing logs to assist you in performing quick analytics. The primary objective of this chapter is to introduce you to the process of obtaining forensic value from logs of any type. You will learn to investigate remote login attempts on SSH, examine web server attacks using Splunk, and scrutinize proxy logs. By the end of this chapter, you will have the necessary skills to investigate and parse various log formats, which can be beneficial in enhancing your understanding of log analysis.

Chapter 5: Wireless Forensics – The chapter provides in-depth knowledge and essential tools and techniques to the readers required to perform meticulous forensics on wireless networks such as Radio Frequencies (RF) and Wireless LANs. This chapter covers several key areas such as the fundamentals of Radio Frequency Monitoring, the 802.11 standard, evidence types in Wireless Local Area Networking, and analysis of other wireless attacks. This chapter aims to provide a comprehensive understanding of the technical aspects of wireless networks, including the protocols, standards, and communication channels. By learning and understanding these areas, readers will be equipped with the necessary skills and knowledge to investigate and analyze various wireless network incidents effectively.

Chapter 6: TLS Decryption and Visibility – In this chapter, readers will discover various techniques to decode SSL/TLS traffic which is generally concealed behind encryption. SSL/TLS encryption is a common tactic employed by several types of malware to circumvent network security devices. Thus, decrypting this communication can be a valuable aid in conducting investigations. The chapter also delves into various methods for decrypting SSL/TLS communication, such as utilizing pre-master secret keys and analyzing traffic using a proxy.

Chapter 7: Demystifying Covert Channels – In this chapter, we will explore various techniques for analyzing modern-day malware that utilizes legitimate services to establish hidden command and control channels. Our discussion will revolve around some essential topics that include detecting concealed communication channels through proxies, decrypting legitimate services traffic using MitmProxy, collecting attack details, identifying attack patterns, and detecting the misuse of DNS. By the end of this chapter, readers will be equipped with the necessary knowledge to analyze malware that employs legitimate services for covert communication effectively.

Chapter 8: Analyzing Exploit Kits – In this chapter, readers will be provided with valuable tips and techniques to effectively analyze exploit kits. This chapter will delve into several methods, such as network simulation, utilizing tools such as Security Onion, and manual extraction, to gather the essential analytics for detecting exploit kit infections. We will also cover crucial topics including the working mechanism of exploit kits, how to analyze an exploit kit infection, network forensics with Security Onion, extracting malicious payload, and using Fakenet-Ng to simulate a network. By the end of this chapter, readers will have a comprehensive understanding of how to analyze and detect exploit kit infections.

Chapter 9: Automating Network Forensics – In this chapter, readers will learn about automating regular manual tasks using Python and LUA scripting. Key topics covered include parsing the Syslog format, IP reputation analysis, and writing dissectors for protocols using Lua. By the end of this chapter, readers will have a deeper understanding of how to automate tasks and streamline their workflow.

Chapter 10: Backtracking Malware – This chapter aims to provide readers with an overview of the latest malware and network techniques cybercriminals use. It will also explain how they misuse legitimate software like AnyDesk and TeamViewer for malicious purposes. This chapter focuses on two key topics - investigating traffic from popular command and control systems and investigating legitimate screen-sharing and remote control software such as TeamViewer and AnyDesk. By covering these topics, readers will understand these crucial issues comprehensively.

Chapter 11: Investigating Ransomware Attacks – In this chapter, we aim to enlighten the readers about the inner workings of different types of ransomware and how they impact computer networks. We will delve into various topics such as analyzing the notorious WannaCry ransomware, exploring ways to obtain decryption keys for ransomware, dissecting the GandCrab ransomware, presenting a case study of the REVIL ransomware attack on a bank, and highlighting crucial event IDs that aid in Windows network analysis. By the end of this chapter, readers will have a better understanding of the serious implications of ransomware and how to mitigate the risks associated with it.

Chapter 12: Investigating Command and Control Systems – In this chapter, the reader will gain knowledge about the most commonly used command and control systems, including the inner workings of Metasploit. Additionally, the reader will learn how to identify command-and-control traffic that originates from payloads and crucial indicators to detect it on the network. This chapter will also discuss the investigation of Metasploit Reverse Shells, Meterpreter Reverse Shell, and Meterpreter Stageless Reverse Shell. Overall, this chapter aims to provide a comprehensive understanding of different command and control systems and their investigation methods.

Chapter 13: Investigating Attacks on Email Servers – This chapter aims to provide practical knowledge on how to handle and examine evidence in the event of an attack on the email server. It will equip readers with the skills required to examine large data sets and identify key attack patterns using Splunk. The chapter will focus on critical attacks on exchange servers and help readers develop the ability to identify such attacks on the network quickly. Specifically, the chapter will cover the analysis of the ProxyLogon attack and how to investigate email authentication logs. By the end of this chapter, readers will have a better understanding of how to handle and investigate email server attacks, which will help them take appropriate actions to mitigate the impact of such attacks.

Chapter 14: Investigating Web Server Attacks – The purpose of this chapter is to provide readers with an understanding of the latest techniques used by attackers and gain a broader perspective on investigations. This includes exploring unconventional logs, such as those from a database, and enabling certain logs for forensic readiness. Throughout the chapter, we will delve into various topics such as Web Server Attack Analysis, Investigating Web Server Logs, Investigating Full Packet Captures, and Investigating database logs. By the end of this chapter, readers will have a deeper understanding of how to analyze and investigate attacks using advanced techniques and tools.

Code Bundle and Coloured Images

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

https://rebrand.ly/6xy33kj

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/Mastering-Network-Forensics.
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!

The VM for the book can be downloaded from
https://drive.google.com/file/d/1U8a5jkgKVwQM3FrqKh5lzMqRDTsh1XJT/view?usp=sharing

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

1. Foundations of Network Forensics 1

Introduction 1

Structure 2

Objectives 2

Types of network forensics 2

Network forensics investigation methodology 3

Evidence source types 5

Source data collection 8

Setting up the environment for analysis 10

Listening for Network Packets using TCPDump 11

Data Reduction Using TCPDump 16

Utilizing Wireshark for Network Analysis 17

Case study: Suspicious Web Server 22

Background 22

Conducting network forensics 22

Conducting log analysis 34

Conclusion 35

Multiple choice questions 36

Answers 37

Long questions 37

2. Protocols and Deep Packet Analysis 39

Introduction 39

Structure 39

The OSI model 40

The TCP/IP model 41

The Packet structure 42

The Internet Protocol Header 44

The Transmission Control Protocol Header 45

    The User Datagram Protocol Header *47*
  Case study: Curious case of protocol misuse 48
    The Internet Control Message Protocol (ICMP) *55*
  Deep Packet Inspection 56
    Censorship and DPI *57*
    SNI Block using DPI *60*
  Case study: Investigating Distributed Denial of service attacks 63
  Conclusion 71
  Multiple choice questions 72
    Answers *73*
  Long questions 73

3. Flow Analysis versus Packet Analysis 75

  Introduction 75
  Structure 76
  Statistical Flow analysis 76
  Flow Record and FRP Systems 76
  Uniflow and BitFlow 77
  Types of Sensor deployment 78
  Flow analysis 80
    Generating IPFIX from PCAP *81*
    Analysis and Investigation of the IPFIX data *82*
    Identifying Scanning Activity using Silk *91*
  Conclusion 93
  Multiple choice questions 93
    Answers *94*
  Long questions 94

4. Conducting Log Analysis 95

  Introduction 95
  Structure 96
  Objectives 96
  Investigating Remote Login attempts on SSH 97

Investigating Web Server Attacks with Splunk 101
Investigating Proxy Logs 119
Conclusion 125
Multiple choice questions 125
    Answers 126
Long questions 126

5. Wireless Forensics 127

Introduction 127
Structure 127
Objectives 128
Basics of Radio Frequency Monitoring 128
    Using RTL-SDR for capturing Radio Frequencies 128
    Using RTL-SDR for frequency sweeping 130
The 802.11 standard 134
Evidence types in wireless local area networking 134
    Locating network and device details 137
    Analysing data transmitted through decryption 146
    Identifying a rogue access point: The evil twin attack 147
Other wireless attacks and their analysis 152
    Authentication and De-Authentication attacks 152
    Denial of Service 153
Conclusion 153
Multiple choice questions 153
    Answers 155
Long questions 155

6. TLS Decryption and Visibility 157

Introduction 157
Structure 157
Objectives 158
Techniques to decrypt SSL/TLS communication 158
    Decrypting SSL/TLS using pre master secret keys 158

Examining SSL/TLS traffic using proxy 163
Conclusion 171
Multiple choice questions 172
Answers 173
Long questions 173

7. Demystifying Covert Channels 175

Introduction 175
Structure 176
Objectives 176
Identifying covert communication using proxies 176
Using MitmProxy to decrypt Dropbox traffic 179
Using Dropbox API to gather attack details 182
Uncovering the attack pattern 185
Uncovering DNS misuse 193
Conclusion 198
Multiple choice questions 198
Answers 199
Long questions 199

8. Analyzing Exploit Kits 201

Introduction 201
Structure 201
Objectives 202
How exploit kits work 202
Analysis of an exploit kit infection 203
Network forensics with Security Onion 207
Extracting malicious payload 213
Using Fakenet-Ng to simulate a network 216
Conclusion 219
Multiple choice questions 219
Answers 220
Long questions 220

9. Automating Network Forensics ... 221

Introduction ... 221

Structure ... 221

Objectives ... 222

Parsing the Syslog format ... 222

Decompressing GZ compressed Logs ... 223

Writing a parser for firewall log files ... 224

IP reputation analysis ... 227

Writing dissectors for protocols in Lua ... 231

Conclusion ... 237

Multiple choice questions ... 238

Answers ... 239

Long questions ... 240

10. Backtracking Malware ... 241

Introduction ... 241

Structure ... 241

Objectives ... 242

Investigating Cobalt Strike Encrypted traffic ... 242

Decrypting Cobalt Strike Encrypted Traffic Using Leaked Keys ... 248

Investigating TeamViewer and AnyDesk ... 255

Proactive monitoring of TeamViewer Sessions ... 257

Investigating AnyDesk sessions ... 258

Conclusion ... 261

Multiple choice questions ... 261

Answers ... 262

Long questions ... 262

11. Investigating Ransomware Attacks ... 263

Introduction ... 263

Structure ... 264

Objectives ... 264

Analysis of WannaCry ransomware ... 264

Capturing ransomware keys for decryption 267

PyLocky ransomware key Recovery 267

Recovering Keys for Hidden Tear ransomware 268

Analyzing GandCrab ransomware 271

Case Study: REVIL ransomware at a Bank 276

Network evidence from Windows Event logs 278

Conclusion 281

Multiple choice questions 281

Answers 282

Long questions 282

12. Investigating Command and Control Systems 283

Introduction 283

Structure 283

Objectives 284

Investigating Metasploit Reverse Shell 284

Investigating Meterpreter Reverse Shell 297

Investigating Meterpreter Stageless Reverse Shell 300

Conclusion 305

Multiple choice questions 305

Answers 306

Long questions 306

13. Investigating Attacks on Email Servers 307

Introduction 307

Objectives 307

Structure 308

Analysis of ProxyLogon attack 308

Investigating ProxyLogon attack 308

Investigating Email authentication logs 317

Conclusion 325

Multiple choice questions 325

Answers 326

Long questions 326

14. Investigating Web Server Attacks **327**

Introduction 327

Structure 327

Objectives 328

Web Server attack analysis........ 328

Investigating Web Server logs........ *328*

Investigating Full Packet Captures for Web Server Traffic........ *335*

Investigating MySQL logs........ *345*

Conclusion 346

Multiple choice questions 346

Answers........ *347*

Long questions 347

Index **349-353**

CHAPTER 1

Foundations of Network Forensics

Introduction

Network forensics was coined to facilitate forensic analysis over the network, regardless of the network type. Network forensics is a sub-branch of digital forensics. The focus is on network evidence such as network traffic, protocols, and logs, to accomplish monitoring, collecting information, establishing root cause analysis, simulating malware behavior, and intrusion detection. We can also call network forensics a branch of digital forensics studying data in motion. While traditional digital forensics cover the imaging and analysis of the media drives and memory in a phased manner, network forensics deals with more volatile and dynamic information. You may ask why there is a need for network forensics or what are the primary applications of it? Since we primarily deal with network-based evidence, network forensics has become particularly helpful in investigating data theft, suspicious connections, DDOS attacks, and network leakage investigation. Considering the present challenges with the rising number of data thefts, **Business Email Compromise** (**BEC**), and ransomware attacks, network forensics can be utilized proactively and passively.

Structure

In this chapter, we will cover the following key topics:

- Types of network forensics
  - o Network forensics investigation methodology
  - o Evidence source types
  - o Source data collection
- Setting up the environment for analysis
  - o Listening for Network Packets using TCPDump
  - o Data Reduction using TCPDump
  - o Utilising Wireshark for Network Analysis
- Case study: Suspicious Web Server
  - o Background
  - o Conducting network forensics
  - o Conducting log analysis

Objectives

By the end of this chapter, the reader will gain knowledge about forensic methodology, type of network evidence and their sources. We will also see how to perform packet analysis using `tcpdump` and Wireshark, and conduct basic log analysis as well. Finally, we will discuss a case study and apply knowledge learned to the analysis of a **Packet Capture** (**PCAP**) file.

Types of network forensics

As discussed, network forensics can be distinguished into two specific activity types: proactive and passive. The proactive approach to network forensics can sometimes be referred to as continuous threat hunting and incident response. In contrast, the latter can be considered post-incident or reactive detection and response.

The proactive approach requires applying new intelligence sources to the existing data, whereas the reactive/passive course examines existing data to better understand what went wrong and how. For example, consider a scenario where XYZ Bank actively monitors its network for threats. The team responsible for monitoring the network has subscribed to multiple threat intelligence feeds that provide vital details such as IP, domains, email addresses, file names, and the hash values that are found to be suspicious/malicious.

The team at XYZ Bank applies all these feeds to their monitoring system and analyzes if something from the threat feed matches with the data sent or received from their network. We call this activity proactive as there may not be an imminent threat, but the team at XYZ bank continuously searches for it.

Consider another scenario where ABC Bank does not have a threat hunting team and faced a ransomware attack that compromised 50 of their machines, including their Antivirus server. The ABC bank establishes an internal forensic team to figure out the root cause of the infection or hires third-party forensic services professionals to figure out the cause. The ABC bank further shares all the details around the incident, such as logs and network capture files, among other evidence, with the forensic subject matter experts to aid the activity. A professional forensicator who analyses the incident, figures out a vulnerable **Virtual Private Network** (**VPN**) service, and establishes the validity of the server running the VPN service contracting other systems within the network. In his report, he mentions the root cause being a vulnerable VPN service, and credential reuse within the network, and pens down recommendations to update the outdated services, based on which the ABC bank implements the recommendation within their network. The scenario we just discussed outlines a reactive response to the incident.

Throughout the book, we will discuss passive and proactive approaches in detail. Also, it is better to approach network forensics with a defined methodology as it specifies goals in a clear manner.

Network forensics investigation methodology

The forensic investigators should follow a defined path throughout the network forensic exercise, to harvest accurate and meaningful results. The **OSCAR** framework contains **Obtain**, **Strategize**, **Collect**, **Analyze** and **Report** Phases in a systematic setting, to define a standard methodology for network forensics, as shown in *Figure 1.1*:

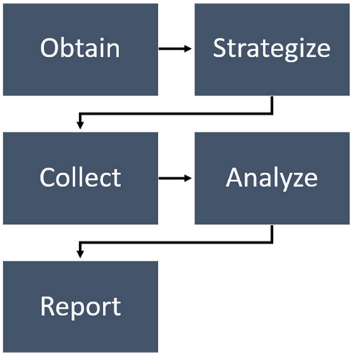

Figure 1.1: *O.S.C.A.R Methodology in Forensics*

The use of the OSCAR framework ensures consistency in the results. So, let us drill into the following phases of OSCAR, to understand them at a grassroots level:

- **Obtain**: Finding out as much information about the incident and discussing goals for the network forensic exercise, are the primary goals of this phase. Once an incident takes place, a few key details become equally important such as Date and Time, Systems and endpoints affected, Presence of Logs, a narrative from the client's IT team, and the steps taken to contain evidence and ensure continuity of business. This phase answers the 'What' and 'Where' part of the incident.
- **Strategize**: The blueprint/plan of the investigation is to be devised in this phase. Most network forensic cases differ in terms of steps taken by the attacker unless a similar attacker group is encountered. When such incidents occur, most IT teams become disoriented and may lose sight of vital evidence to be contained and preserved. Therefore, forensic investigators need to guide the client's team and work backward from the incident. For example, in the case of ransomware infection, the first step is to preserve event logs from the machine after being isolated on the network. The event logs can reveal who connected to the system and from where. It is also essential not to blatantly ask for anything and everything regarding log files. In the example we just discussed, the first step was to obtain event logs and determine who connected to the system and its IP address. Then, we ask the IT teams to provide the IP address details to know whose system got connected to the infected host from within the network. Next, we can repeat the steps until an end is reached and may choose to start the investigation on the 'first patient' (the first system to get compromised). Therefore, we are asking what is necessary and not everything available. Hence, planning and strategizing become essential. Additionally, keep the following points in mind while strategizing the forensic exercise:
    - Define clear goals and timelines for the investigation.
    - Think of the sources of evidence.
    - Plan timely updates for the client.
- **Collect**: In this phase, we will acquire the evidence as per the plan defined in the previous phase. Collection of the evidence requires us to document all the systems that were accessed and used; capture and save the data streams to the hard drive, and collect logs from servers, applications, proxies, and firewalls. The best practices for evidence collection include:

  - Create copies of the evidence and generate cryptographic hashes for verifiability.
  - Work on copies of data instead of the original evidence.
  - Use commercial and industry-standard tools.
  - Document all your actions and steps taken.
- **Analyze**: The most critical phase includes making sense of the data, deriving a story behind the incident, and determining what happened and caused it. This is the phase where you start working on evidence by using automated and manual techniques and industry's leading forensic tools to correlate data from numerous sources, formulate a timeline of events, eliminate sinkholes, and derive working theories with supporting evidence. The book focuses primarily on this particular phase of the OSCAR framework, as the rest of the phases are easy to grasp and generally age with real-world experience.
- **Report**: The reporting phase is also one of the most crucial phases of an investigation as your reports would be read by CEOs, CFOs, CISOs, Jury, Insurance, Legal teams, and many others. It is vital that the produced report is in a layman's language and easy to follow, and should be well understood by people with no technical expertise. The report should begin with executive summaries followed by technical findings backed by technical evidence.

Getting to know about the OSCAR methodology, let us see which source of evidence we will deal with, in a typical network forensic exercise in the next section.

Evidence source types

To carry out network forensics, we as investigators must deal with multiple data sources such as network capture files, logs, and sometimes even executables. Let us understand the three basic types of source data types for investigation:

- **Log Files (LF)**: The most crucial data type. Log files can unveil the majority of the attacks, help understand the attack patterns, and contain platform or application-centric items to characterize activities observed. The following *Figure 1.2* is an example of an IIS web server log file: