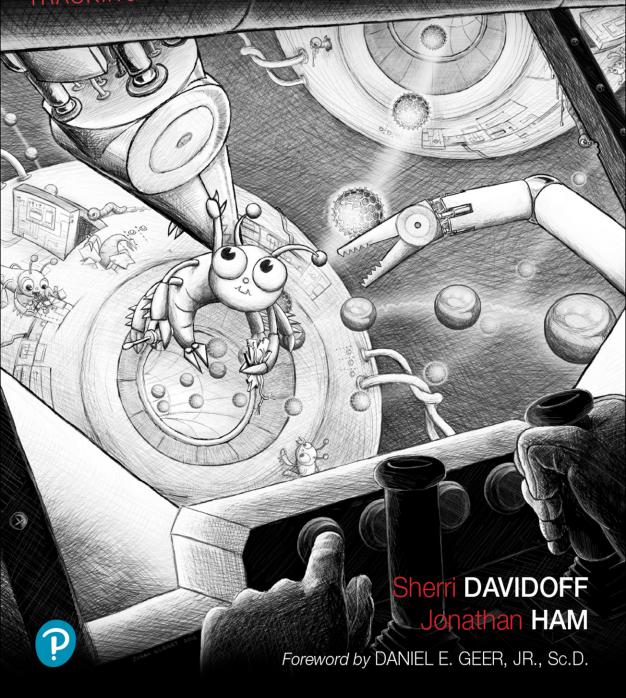


# Network Forensics TRACKING HACKERS THROUGH CYBERSPACE



### Network Forensics

## Network Forensics: Tracking Hackers through Cyberspace

#### **Table of Contents**

_	•					
•	•	$\overline{}$	١.		$\overline{}$	"
		( )	١.	•	_	

Half Title

Title Page

Copyright Page

Contents

**Foreword** 

#### **Preface**

- 0.1 The Changing Landscape
- 0.2 Organization
  - 0.2.1 Part I, Foundation
  - 0.2.2 Part II, Traffic Analysis
  - 0.2.3 Part III, Network Devices and Servers
  - 0.2.4 Part IV, Advanced Topics
- 0.3 Tools
- 0.4 Case Studies
- 0.5 Errata
- 0.6 Final Notes

Acknowledgments

About the Authors

Part I: Foundation

Chapter 1 Practical Investigative Strategies

1.1 Real-World Cases



#### **Table of Contents**

- 1.2 Footprints
- 1.3 Concepts in Digital Evidence
- 1.4 Challenges Relating to Network Evidence
- 1.5 Network Forensics Investigative Methodology (OSCAR)
- 1.6 Conclusion

#### Chapter 2 Technical Fundamentals

- 2.1 Sources of Network-Based Evidence
- 2.2 Principles of Internetworking
- 2.3 Internet Protocol Suite
- 2.4 Conclusion

#### **Chapter 3 Evidence Acquisition**

- 3.1 Physical Interception
- 3.2 Traffic Acquisition Software
- 3.3 Active Acquisition
- 3.4 Conclusion

#### Part II: Traffic Analysis

#### Chapter 4 Packet Analysis

- 4.1 Protocol Analysis
- 4.2 Packet Analysis
- 4.3 Flow Analysis
- 4.4 Higher-Layer Traffic Analysis
- 4.5 Conclusion
- 4.6 Case Study: Anns Rendezvous

#### Chapter 5 Statistical Flow Analysis

- 5.1 Process Overview
- 5.2 Sensors
- 5.3 Flow Record Export Protocols
- 5.4 Collection and Aggregation
- 5.5 Analysis
- 5.6 Conclusion



#### **Table of Contents**

5.7 Case Study: The Curious Mr. X

#### Chapter 6 Wireless: Network Forensics Unplugged

- 6.1 The IEEE Layer 2 Protocol Series
- 6.2 Wireless Access Points (WAPs)
- 6.3 Wireless Traffic Capture and Analysis
- 6.4 Common Attacks
- 6.5 Locating Wireless Devices
- 6.6 Conclusion
- 6.7 Case Study: HackMe, Inc.

#### Chapter 7 Network Intrusion Detection and Analysis

- 7.1 Why Investigate NIDS/NIPS?
- 7.2 Typical NIDS/NIPS Functionality
- 7.3 Modes of Detection
- 7.4 Types of NIDS/NIPSs
- 7.5 NIDS/NIPS Evidence Acquisition
- 7.6 Comprehensive Packet Logging
- 7.7 Snort
- 7.8 Conclusion
- 7.9 Case Study: InterOptic Saves the Planet (Part 1 of 2)

#### Part III: Network Devices and Servers

#### Chapter 8 Event Log Aggregation, Correlation, and Analysis

- 8.1 Sources of Logs
- 8.2 Network Log Architecture
- 8.3 Collecting and Analyzing Evidence
- 8.4 Conclusion
- 8.5 Case Study: Lone Sh4rks Revenge

#### Chapter 9 Switches, Routers, and Firewalls

- 9.1 Storage Media
- 9.2 Switches
- 9.3 Routers



#### **Table of Contents**

- 9.4 Firewalls
- 9.5 Interfaces
- 9.6 Logging
- 9.7 Conclusion
- 9.8 Case Study: Anns Coffee Ring

#### Chapter 10 Web Proxies

- 10.1 Why Investigate Web Proxies?
- 10.2 Web Proxy Functionality
- 10.3 Evidence
- 10.4 Squid
- 10.5 Web Proxy Analysis
- 10.6 Encrypted Web Traffic
- 10.7 Conclusion
- 10.8 Case Study: InterOptic Saves the Planet (Part 2 of 2)

#### Part IV: Advanced Topics

#### Chapter 11 Network Tunneling

- 11.1 Tunneling for Functionality
- 11.2 Tunneling for Confidentiality
- 11.3 Covert Tunneling
- 11.4 Conclusion
- 11.5 Case Study: Ann Tunnels Underground

#### Chapter 12 Malware Forensics

- 12.1 Trends in Malware Evolution
- 12.2 Network Behavior of Malware
- 12.3 The Future of Malware and Network Forensics
- 12.4 Case Study: Anns Aurora

#### Afterword

#### Index

