**DESCRIPTION**

**Intensively hands-on training for real-world network forensics**

*Network Forensics* provides a uniquely practical guide for IT and law enforcement professionals seeking a deeper understanding of cybersecurity. This book is hands-on all the way—by dissecting packets, you gain fundamental knowledge that only comes from experience. Real packet captures and log files demonstrate network traffic investigation, and the learn-by-doing approach relates the essential skills that traditional forensics investigators may not have. From network packet analysis to host artifacts to log analysis and beyond, this book emphasizes the critical techniques that bring evidence to light.

Network forensics is a growing field, and is becoming increasingly central to law enforcement as cybercrime becomes more and more sophisticated. This book provides an unprecedented level of hands-on training to give investigators the skills they need.

- Investigate packet captures to examine network communications
- Locate host-based artifacts and analyze network logs
- Understand intrusion detection systems—and let them do the legwork
- Have the right architecture and systems in place ahead of an incident

Network data is always changing, and is never saved in one place; an investigator must understand how to examine data over time, which involves specialized skills that go above and beyond memory, mobile, or data forensics. Whether you're preparing for a security certification or just seeking deeper training for a law enforcement or IT role, you can only learn so much from concept; to thoroughly
understand something, you need to do it. Network Forensics provides intensive hands-on practice with direct translation to real-world application.

ABOUT THE AUTHOR

RIC MESSIER has been program director for various cyber-security and computer forensics programs at Champlain College. A veteran of the networking and computer security field since the early 1980s, he has worked at large Internet service providers and small software companies. He has been responsible for the development of numerous course materials, has served on incident response teams, and has been consulted on forensic investigations for large companies.

To purchase this product, please visit https://www.wiley.com/en-us/9781119328285