

Contents at a Glance

Introduction	xxi
1 Introduction to Network Forensics.....	1
2 Networking Basics.....	13
3 Host-Side Artifacts.....	53
4 Packet Capture and Analysis	81
5 Attack Types	113
6 Location Awareness.....	143
7 Preparing for Attacks.....	159
8 Intrusion Detection Systems	187
9 Using Firewall and Application Logs.....	211
10 Correlating Attacks	245
11 Network Scanning.....	265
12 Final Considerations	291
Index	319