Index

IP Sniffer, 2-30, 2-31
Iris Network Traffic Analyzer, 2-19–2-20, 2-21
IS-IS (Intermediate System to Intermediate System), 4-4
iThenticate, 9-20, 9-21

Japanese laws
against child pornography, 11-24
for trademarks and copyright, 9-34–9-35

JavaScript, 6-17–6-18
JPlag, 9-15

keepNI, 3-31–3-32
Kiwi Syslog Daemon, 1-12, 1-13

LAN addressing, 2-2
LAND attacks, 5-3
Lanham (Trademark) Act, 9-31–9-32
LanWhols, 3-45
Link Logger, 4-17–4-18
Linux, process accounting, 1-18–1-19
Local area network (LAN), 2-2
LOCIS, 9-9, 9-10
LockLizard, 9-28, 9-29
Log files
authenticity of, 1-7
as evidence, 1-3–1-8
missing, 1-7
multiple, 1-5
tampering with, 3-8
Log-input, tracing with, 5-14
Logs, investigating
introduction, 1-2
log files as evidence, 1-3–1-8
tools for, 1-8–1-21
LoPe, 7-24, 7-25

MaxTec Network Analyzer, 2-23, 2-24
MAC (Media Access Control) address, 2-2
Mail bombing, 7-6–7-7
MailDetective, 7-16–7-17, 7-18
Mail storm, 7-7
Mail user agent (MUA), 7-2
Malaysia, 11-23

Mail user agent (MUA), 7-2
Malaysian penal code, on sexual harassment, 10-12
Mapper, 3-32
McAfee Visual Trace, 3-37, 3-38
Media Access Control (MAC) address, 2-2
Michigan laws, against child pornography, 11-23
Microsoft Log Parser, 1-12–1-13, 1-14
Microsoft Outlook, 7-15
viewing and copying e-mail headers in, 7-9
Moles, detecting, 8-6
Monitoring, 8-6
Multiple logs, 1-5
My Offline Browser, 6-19–6-20

Nagios, 2-33
National Center for Missing & Exploited Children (NCMEC), 11-33
NeoTrace (McAfee Visual Trace), 6-25, 6-26
NetGEAR router logs, 4-13–4-14, 4-15
NetInterceptor, 2-12, 2-13
NetResident, 2-38
NetScan Tools, 6-26, 6-27
NetSetMan, 2-21–2-22
Netspionage, 8-7
NetVizor, 8-11
NetWitness, 2-37
Network Abuse Clearinghouse, 7-5
Network E-Mail Examiner by Paraben, 7-22
Network forensics
data analysis, 1-2
date-to-end, 1-3
introduction, 1-2
invasion process, 1-2–1-3
looking for evidence, 1-3
NTP, 1-21–1-28
Network Intrusion Detection System (NIDS), for DoS attack detection, 5-9
Network interface card (NIC), 2-2
Network layer
of main protocols, 2-4
of OSI model, 2-5–2-6

Network Probe, 2-43
Network protocols, overview, 2-3–2-5
Network Time Protocol (NTP), 1-21–1-27
Network traffic
data link layer of OSI model, 2-5
dDNS poisoning techniques, 2-7–2-9
documenting evidence, 2-45–2-46
evidence gathering at data link layer-
DHCP database, 2-10
evidence gathering at physical layer,
2-6–2-7
evidence gathering from ARP table, 2-9
evidence gathering from IPS, 2-10
introduction, 2-2
investigation tools for, 2-10–2-45
network addressing, 2-2–2-3
network layer of OSI model, 2-5–2-6
OSI reference model, 2-3
physical layer of OSI model, 2-5
protocols overview, 2-3–2-5
reasons for investigating, 2-6
reconstructing evidence for investigation,
2-46–2-47
transport layer of OSI model, 2-6
types of attacks, 2-6
Nic (network interface card), 2-2
NIDS (Network Intrusion Detection System),
for DoS attack detection, 5-9
Nmap, 5-16
Nokia LIG, 2-35–2-36
Nslookup, 3-34, 3-36, 6-8–6-9
N-Stalker, 3-33
N-Stealth, 3-23, 3-24
ntop, 2-24, 2-25
NTP (Network Time Protocol), 1-21–1-27
NTsyslog, 1-19–1-20
Nuke attacks, 5-4

ODBC logging, 1-8
OmniPeek, 2-19
Online Copyright Infringement Liability Limitation Act, 9-32–9-33
OOB attacks, 5-4
Open Shortest Path First (OSPF), 4-4