Index
1-3

Emsa Web Monitor, 3-28
End-to-end forensic investigation, 1-3
English laws, against child pornography, 11-25
Enterprise IP-Address Manager, 3-42, 3-43
Ephemeral, 6-4
Equal Protection Clause of 14th Amendment, 10-11
EtherApe, 2-24, 2-25
EtherDetect Packet Sniffer, 2-18–2-19
Ethernets
shared, 2-6–2-7
switched, 2-7
EtherScan Analyzer, 2-29
EtherSnopp, 2-35
eTrust Network Forensics, 2-39–2-41
EVE2 (Essay Verification Engine), 9-19, 9-21
EventLog Analyzer, 1-20–1-21
EventReporter, 1-20
Evidence
log files as, 1-3–1-8
looking for, 1-3
multiple logs as, 1-5
at physical layer, 2-6–2-7
eWebLog Analyzer, 3-23, 3-24
Exchange Message Tracking Center, 7-16, 7-17
Exploit-Me, 3-34

F
Fair Use Doctrine, 9-31–9-32
Falcove Web Vulnerability Scanner, 3-28
FINALEMAIL, 7-20
Financial Coalition Against Child Pornography (FCACP), 11-33
Firefox, 6-15, 6-16, 6-18, 6-22
Firewall Analyzer, 1-13–1-14, 1-15
Forensic Linguistics Institute, 9-22–9-23
Forensics, vs. router forensics, 4-5
Forensic Toolkit (FTK), 7-19–7-20
Fourteenth Amendment, 10-11
Fraggle attacks, 5-3–5-4
Friendly Pinger, 5-16–5-17
FTP compromises, 3-11
FTP logs, investigating, 3-11–3-12
FTP servers, investigating, 3-12

G
General Packet Radio Service (GPRS), 2-35–2-36
German laws, on sexual harassment, 10-12
GFI EventsManager, 1-15–1-17
Give Me Too, 2-33, 2-34
Glatt, 9-21
Gmail, viewing and copying e-mail headers in, 7-10–7-11
GPRS Network Sniffer-Nokia LIG, 2-35–2-36
Grab-a-Site, 6-18–6-19
Grooming, 6-3

H
Haihaisoft Media DRM Platform, 9-28
Hash-based IP tracebacks, 5-13
Hide Real IP, 3-40, 3-41
Hit-and-run attacks, 4-5
Honeypots, 8-5–8-6
Honeytokens, 8-5–8-6
Hong Kong laws, for intellectual property, 9-39
Hop-by-Hop IP traceback, 5-10–5-11
Hostile work environment harassment, 10-3–10-4
Hotmail, viewing and copying e-mail headers in, 7-10
HP Weblinspect, 3-30
HTTP Sniffer, 2-16, 2-18

I
ICMP traceback, 5-10
Identity theft, 7-8
ID Protect, 7-26
IDS (intrusion detection system), evidence gathering from, 2-10
IDS Policy Manager, 2-45, 2-46
IE HTTP Analyzer, 2-29
IISLogger, 1-8, 1-9
IIS logs, 1-5–1-6
investigating, 3-12
IMAP (Internet Message Access Protocol), 7-4
iMonitorPC, 8-17, 8-19
Impersonation attacks, 3-10
Indian laws
on sexual harassment, 10-12
for trademarks and copyright, 9-33–9-34
Industry self-regulation (ISP), 11-3
InfiniStream, 2-38–2-39, 2-40
Innocent Images National Initiative (IINI), 11-27–11-28
Insider threats, 8-3, 8-7
Intellectual property, 9-25–9-26, 9-39
IntelliProtector, 9-28, 9-29
Intermediate System to Intermediate System (IS-IS), 4-4
International Centre for Missing & Exploited Children (ICMEC), 11-31–11-33
Internet, role in child pornography, 11-3
Internet Assigned Numbers Authority (IANA), 6-6
Internet crimes
Internet forensics, 6-4
introduction, 6-2
investigation goals, 6-4
investigation steps, 6-4–6-8
investigation tools for, 6-8–6-27
types of, 6-2–6-3
Internet Crimes Against Children Task Force (ICAC), 11-28
Internet DNS spoofing (remote network), 2-8
Internet Service provider (ISP), 6-6
Internet Spy Filter, 8-12, 8-13
Internet Watch Foundation, 11-31
Intranet addressing, 2-2–2-3
Intranet DNS spoofing (local network), 2-8
Intrusion detection, 1-5, 3-15
Intrusion detection system (IDS), evidence gathering from, 2-10
Intrusion process, 1-2
IP2country, 3-46
IP addresses
examining the origin of, 7-16
Internet crimes and, 6-5–6-6
investigating, 3-16
locating, 5-15
IP Address Locator, 6-12, 6-13
IP.com, 9-24–9-25
IP Detective Suite, 3-40, 3-41
IPgrab, 2-32
IPHost Network Monitor, 5-17, 5-18
iProtectYou, 11-12–11-13
IPSec, 5-13