Copyright Act (1968), 9-36–9-37
Copyright Management Business Law (4.2.2.3) (2000), 9-35

Copyrights
Australian laws for, 9-35–9-37
Belgian laws for, 9-39
Canadian laws for, 9-38
Chinese laws for, 9-38
enforcement of, 9-10–9-11
Indian laws for, 9-33–9-34
introduction, 9-1–9-2
Japanese laws for, 9-34–9-35
length of, 9-9–9-10
plagiarism, 9-11–9-23
South African laws for, 9-38
South Korean laws for, 9-39
status investigation, 9-9
U.K. laws for, 9-37–9-38
U.S. laws for, 9-30–9-33

Corporations
Corporate espionage
defenses against, 8-4–8-5
defined, 8-1–8-2
information sought by spies, 8-2–8-3
insider/outsider threat, 8-3
introduction, 8-1–8-2
motives behind, 8-2
prevention steps, 8-5–8-7
spying techniques, 8-3–8-4
threat due to aggregate of information, 8-3
CounterSpy, 8-16, 8-17
CounterStorm-1, 3-49
CountryWhois, 3-46
CPU utilization, for DoS attack detection, 5-9

Critical assets, 8-5
Cross-site request forgery (CSRF), 3–3–3-4
Cross-site scripting ( XSS) attacks, 3-2–3-3
Cryptographic interceptions, 3-9
Cyberbullying, 10-2
Cyberstalking, 10-6
Cybertip.ca, 11-36–11-37
CyberTipline, 11-33, 11-34
Cypriot laws, against child pornography, 11-24

Data link layer
evidence gathering from, 2-10
of main protocols, 2-4
of OSI model, 2-5
Data Recovery Wizard, 11-5, 11-6
DDoS attacks, 5-5–5-7
Deep Log Analyzer, 3-18–3-19
Denial-of-service (DoS) attacks, 4-4
DDoS attacks, 5-5–5-7
defined, 5-2
detection techniques, 5-8–5-9
indications of, 5-2
introduction, 5-2
investigating, 5-9–5-15
investigation challenges, 5-16
investigation tools for, 5-16–5-20
modes of, 5-7–5-8
types of, 5-2–5-4
DHCP database, evidence gathering from, 2-10
Digital evidence, 11-11
Digital Millennium Copyright Act (DMCA) (1998), 9-30–9-31
Digital rights management ( DRM), 9-26–9-29
Directory reversals, 3-9
Diskinternals Outlook Recovery, 7-22, 7-23
Distinct Network Monitor, 2-23
Distributed denial-of-service (DDoS) attacks, 5-5–5-7
DMZ protocol attacks, 3-7
DNS (Domain Name Service)
poisoning techniques, 2-7–2-9
Web page defacement using, 3-14
DNS root name servers, 6-7
Documentation, of evidence gathered on network, 2-45–2-46
Domain name infringement, 9-25
Domain Name System (DNS), Internet crimes and, 6-6–6-8
DoSHTTP, 5-20
dotDefender, 3-25, 3-26
Dupli Checker, 9-21, 9-22
Dynamic IP addresses, investigating, 3-16

E-mail
specialized forensic tools for, 7-17–7-26
tracing, 7-22–7-24
E-mail addresses, tracing, 6-22–6-25
E-mail crime
investigating, 7-8–7-17, 7-18, 7-19
overview, 7-4–7-7
RCW 19.190.020, 7-27
types of, 7-4–7-7
U.S. laws against (CAN-SPAM Act), 7-26–7-27
E-Mail Detective, 7-20
Email Dossier, 7-16
E-Mail Examiner by Paraben, 7-21, 7-22
E-mail headers
common, 7-13–7-15
examining, 7-11–7-15
“received”, 7-13
viewing and copying in AOL, 7-10
viewing and copying in Gmail, 7-10–7-11
viewing and copying in Hotmail, 7-10
viewing and copying in Microsoft Outlook, 7-9
viewing and copying in Yahoo! Mail, 7-11, 7-12
E-mails
chain messages, 7-8
copying messages, 7-9
examining messages, 7-9
investigating crimes and violations, 7-8–7-17, 7-18, 7-19
obtaining bit-by-bit image information, 7-9
online programs, 7-15
personal address book, 7-15
printing messages, 7-9
spoofing, 7-8
systems, 7-2–7-4
tracking and investigating crimes, 7-2
viewing and copying e-mail headers in AOL, 7-10
eMailTrackerPro, 7-24, 7-25
Employee-monitoring policies, writing guidelines, 8-19–8-20
Employee responsibilities, 10-7