Index

Note: Page numbers followed by "f" and "b" indicate figures and boxes respectively.

A

Academic sites, 18
Addictomatic, 72
Addons
  buildwith, 48, 49f
  chat notification, 47
  Contactmonkey, 52
  follow.net, 49
  onetab, 50–51
  Project Naptha, 51
  Reveye, 51
  Riffle, 49–50, 50f
  salesloft, 51
  for security, 211
    HTTPS Everywhere, 212
    NoScript, 212
    WOT, 211, 211f
  shodan, 48
  Tineye, 51
  wappalyzer, 48
  whoworks.at, 50
  YouTube, 47
Adobe PhotoShop, 138–139
Advanced search techniques, 25
  Facebook, 25–26, 27f
  LinkedIn, 27–30, 27f
  site operator, 31
  Twitter, 30, 31f
Anonymity, 147
Anonymous network, 164
  I2P, 165–168, 166f
  Onion Router, 164–165, 165f
Antiviruses, 209
Application-based proxy
  JonDo, 153–156, 154f–155f
  Ultrasurf, 152–153, 153f
Application programming
      interface (API), 246
Autocomplete, 37–38

B

Betweenness, SNA
  bridges, 225
  defined, 222
  factors, 222, 222f
  gatekeeper/boundary spanners, 225
  isolate, 225–227, 225f–226f
  Liaison, 225
  network reach, 223–224
  nodes, role, 223
  star/hub, 224
Bing
  features, 85
  operators
    /, 85
    "", 85
    (), 86
    &, 86
    +, 85–87
    feed, 87, 87f
    filetype, 86
    ip, 86, 87f
    site, 86
Bitcoin, 272–274, 273f
BitLocker, 215, 215f
Black Hat mashup, 253–254
Boardreader, 73
Bookmark, 52
Browser, 52
  architecture, 34f
    browser engine, 35
    data persistence, 35–36
    error tolerance, 36
    javascript interpreter, 35
    networking, 35
    rendering engines, 35
    threads, 36
    UI backend, 35
    user interface, 35
  Chrome, 12
  Epic browser, 40
  features
    autocomplete, 37–38
    online and offline browsing, 36
    private browsing, 36–37, 37f
    proxy setup, 38
  Firefox, 12–13
  history of, 34
  operations, 33–34
Buildwith, 48, 49f
Business/company search, 59
  Glassdoor, 59–60, 60f
  LinkedIn, 59
  Zoominfo, 60

C

Carrot2, 72–73, 73f
CaseFile, 194–196, 195f–196f
CheckUsernames, 61
Chromium, 39
Clearweb, 169–170
Contactmonkey, 52
Content sharing websites, 17–18
Corporate websites, 17
Creepy
  applying filter, 104, 104f
  geolocation, 102
  Plug-in Configuration button, 102, 102f
  results, 103, 103f–104f
  search users, 102, 103f
Cryptography, 267
  asymmetric key, 268
  encoding, 268–269
  hashing, 268
  symmetric key, 267
Custom browsers, 46
  categories, 45–46
  Epic, 40
  FireCAT, 43–44
  HconSTF, 40–41
  Mantra, 41–43, 42f
  Oryon C, 44, 44f
  TOR bundle, 45
  Whitehat Aviator, 44–45
CyberGhost, 161–162, 162f

D

Darknet, 17
  I2P
    create own site, 180–183, 180f–183f
    download and install, 176
    forum, 178, 179f
    git, 177, 177f
    home, 176, 177f
    Id3nt, 179, 179f
    paste, 178, 178f
  Tor
    DuckDuckGo, 173, 173f
    files created, 175, 175f
    HiddenServicePort, 174–175
    Hidden Wiki, 172, 172f
    Silk Road, 174
    Torchan, 174, 174f
    Tor hidden service, 175f, 176
    Tor Wiki, 172, 173f
    XAMPP, 174
Darkweb, 170
Data encryption, 215–216, 215f
Data Encryption Standard (DES), 267
Data leakage protection (DLP), 145–146
  Doc Scrubber, 146
  geotags, 146
  MAT, 145
  MetaShield Protector, 145
  MyDLP, 145
  OpenDLP, 146
Data management/visualization
  and analysis tools
    CaseFile, 194–196, 195f–196f
    excel sheet, 190–191, 191f
    flowcharts, 192–193, 193f
    KeepNote, 197–198, 198f
    Lumify, 198–199, 199f
    MagicTree, 196–197, 197f
    Maltego, 193–194, 194f
    SQL databases, 191–192, 192f
    Xmind, 199–201, 200f
  data, 188
  information, 188
  intelligence, 188–190
DataMarket, 71
Data recovery/shredding, 269–270, 270f–271f
Deepweb. *See also* Darknet
  advantages, 171
  defined, 170
  disadvantages, 171
DiggityDownloads, 143
Doc Scrubber, 146
Domain name system (DNS), 5–6, 8
DuckDuckGo, 62, 62f

E

E-mail, 5
Email-Rapportive, 256
EmailSherlock, 60, 61f
Epic browser, 40
Error tolerance, 36
Excel sheet, 190–191, 191f
Exif Search, 136–137, 136f–137f

F

Facebook, 22, 25–26, 27f
Fingerprinting Organizations with Collected Archives (FOCA), 139–140, 140f
FireCAT, 42–44
Follow.net, 49
Freedom, 40–41
Freenet, 183–185, 183f–184f

G

Gecko, 35
Gephi
  Data Laboratory tab, 219, 219f
  installation, 218
  Overview tab, 218–219, 219f
  Preview tab, 220
Glassdoor, 59–60, 60f
Google
  operators
    -, 81
    .., 81
    “”, 81
    *, 81
    AND, 81
    allintext, 80
    allinurl, 79
    AROUND, 80–81
    cache, 82, 135f
    calculator, 83
    convertor, 83–84
    define, 80
    ext, 80
    filetype, 80
    info, 82
    intext, 79–80
    intitle, 80
    inurl, 79
    NOT, 81
    OR, 81
    related, 82
    site, 78–84, 79f
    time, 83
    weather, 83
  search categories, 78
Google+, 24–25
Google Chrome, 38–39
Google Hacking Database, 83–84, 84f
Google Translate, 149
Government sites, 19

H

Hachoir-metadata, 138–139
Hackerfox, 40–41
Hacking attempts, 208
Hard disk drive (HDD), 269
HaveIBeenPwned, 214, 214f, 256
Hello World program, 231, 231f
HconSTF, 40–41
Hideman, 163–164, 163f
HTTPS Everywhere, 212
HyperText Markup Language (HTML), 77

I

Id3nt, 179, 179f
ImageRaider, 70–71
Integrated database (IDB), 41
Intelligence
  definition, 188–189
  managing data, 189
  structured data, 190
Internet
  definition, 2
  history, 2
  working, 2
Internet Relay Chat (IRC), 271–272, 272f
Invisible Internet Project (I2P), 165–168, 166f
  create own site, 180–183, 180f–183f
  download and install, 176
  forum, 178, 179f
  git, 177, 177f
  home, 176, 177f
  Id3nt, 179, 179f
  paste, 178, 178f
IP address, 3–4
iPhone, 137–138
IRC. *See* Internet Relay Chat (IRC)
ivMeta, 137–138, 138f
Ixquick, 55, 55f

J

Jeffrey’s Exif Viewer, 134–136, 135f
JonDo, 153–156, 154f–155f
  installation, 154
  interface, 154, 154f
  running, 155, 155f
  test, 154, 155f
  Windows users, 153
JonDoFox, 153

K

KeepNote, 197–198, 198f
Keylogger, 206
Kngine, 63, 63f
KnowEm, 61

L

LinkedIn, 23, 27–30, 27f, 258
LittleSis, 57–58
Lumify, 198–199, 199f

M

MAC address, 5
MagicTree, 196–197, 197f

Maltego
  Collaboration, 127–128, 128f
  commercial version, 124
  community version, 124
  domain to E-mail, 129–130, 130f
  domain to website IP, 128–129, 129f
  entity, 124
  Investigate, 126
  machines, 125, 125f, 127
    Company Stalker, 263, 263f
    creating, 263–264, 264f
    HIBP local transform, 264
    MSL, 263
    output, 265, 265f
  Manage option, 126, 126f
  Organize option, 126, 126f
  person to website, 130–131, 131f
  transform, 124
Maltego scripting language (MSL), 263
Maltego Transforms, 245–251, 248f–250f
Malwares
  Keylogger, 206
  ransomwares, 206
  restricted sites, 205–206
  Trojan, 206
  virus, 206
Mamma search engines, 55–56
Mantra, 41–43, 42f
MarketVisual, 58, 58f
Media access control address, 5
Metadata
  creation of, 133–134
  extraction tools
    Exif Search, 136–137, 136f–137f
    FOCA, 139–140, 140f
    hachoir-metadata, 138–139
    ivMeta, 137–138, 138f
    Jeffrey's Exif Viewer, 134–136, 135f
    Metagoofil, 140–142, 141f–142f
  impact, 142–143
  removal/DLP tools, 145
    Doc Scrubber, 146
    geotags, 146
    MAT, 145
    MetaShield Protector, 145
    MyDLP, 145
    OpenDLP, 146
  Search Diggity, 143–145
Metadata anonymization toolkit (MAT), 145
Metagoofil, 140–142, 141f–142f
Meta search, 54
  Ixquick, 55, 55f
  Mamma, 55–56
  Polymeta, 54, 54f
MetaShield Protector, 145
Microsoft Baseline Security Analyzer (MBSA), 212, 213f
Mozilla Firefox, 38–39
MyDLP, 145

N

Namechk, 61
NerdyData, 66–67, 67f
News sites, 17
NoScript, 212

O

Ohloh code, 67
Omgili, 73
Onetab, 50–51
.onion domain websites, 174
Onion Router, 164–165, 165f
Online anonymity
  IP address, 147–148
  proxy
    Google Translate, 149, 150f
    page opened inside, 150, 151f
    types of, 151
    whatismyipaddress, 149, 150f
  VPN, 161
    CyberGhost, 161–162, 162f
    Hideman, 163–164, 163f
Online scams/frauds, 207–208, 207f
Online security
  addons, 211
    HTTPS Everywhere, 212
    NoScript, 212
    WOT, 211, 211f
  antiviruses, 209
  data encryption, 215–216, 215f
  hacking attempts, 208
  jailbroken iPhone, 204–205
  malwares
    Keylogger, 206
    ransomwares, 206
    restricted sites, 205–206
    Trojan, 206
    virus, 206
  operating system update, 210–211
  password policy, 213–214, 214f
  password reset, 204–205
  phishing, 207, 210
  scams and frauds, 207–208, 207f, 210
  shoulder surfing, 208–209

social engineering, 209, 215
spam message, 203–204
tools, 212–213, 213f
weak passwords, 208
OpenDLP, 146
Open source intelligence (OSINT)
academic sites, 18
content sharing websites, 17–18
corporate websites, 17
demo, 255
government sites, 19
news sites, 17
public sources, 16b
search engines, 16–17
tools and techniques, 101
Creepy, 102–104
Maltego, 124–131
Recon-ng, 113–121
Search Diggity, 110–113
Shodan, 107–110
TheHarvester, 105–107
Yahoo Pipes, 121–124
WEBINT, 16
weblogs/blogs, 18–19, 18f
Operating system
basic hardwares, 10
Linux, 11
Mac, 11
Windows, 10–11
Oryon C, 44, 44f
OSINT. *See* Open source intelligence (OSINT)

P

PeekYou, 57
People search, 56
LittleSis, 57–58
MarketVisual, 58, 58f
PeekYou, 57
Pipl, 56–57, 57f
Spokeo, 56
TheyRule, 58–59
Yasni, 57
Phishing, 207
Pipl, 56–57, 57f
Polymeta, 54, 54f
Ports, 4
Prime, 40–41
Private browsing, 36–37, 37f
Private IP address, 4
Programming language
Java, 11–12
Python, 12
Project Naptha, 51
Protocol, 4–5
Proxy
application-based proxy
JonDo, 153–156, 154f–155f
Ultrasurf, 152–153, 153f
Google Translate, 149, 150f
page opened inside, 150, 151f
set up, 160–161, 160f
in Chrome, 38
in Firefox, 38
web-based proxy, 156
anonymouse.org, 156–158, 156f–157f
Boomproxy.com, 159–160
FilterBypass, 159, 159f
Zend2, 158–159, 158f
whatismyipaddress, 149, 150f
Public IP address, 4
Python, 230
classes, 239–240
common mistakes, 243–245, 244f
data types, 232–235, 232f–234f
functions, 239
Hello World program, 231, 231f
identifiers, 232
indentation, 235–238
installation, 230
Maltego Transforms, 245–251, 248f–250f
modes, 230–231
modules, 238–239
programming *vs.* scripting, 229–230
resource, 251–252
user input, 242–243
working with files
os, 241
re, 241
sys, 241
urllib2, 242

R

Ransomwares, 206
Raw browsers, 38–40
Recon-ng, 118f
commands, 114b, 115
installation, 114
LinkedIn, 119
modules, 115, 115b, 116f–118f
penetration testing, 120
physical tracking, 119–120
PunkSpider in progress, 120, 121f
Rendering engines, 35

Reverse image search, 69
  Google images, 70, 70f
  ImageRaider, 70–71
  TinEye, 70
Reverse username/e-mail search, 60
  CheckUsernames, 61
  EmailSherlock, 60, 61f
  Facebook, 61
  KnowEm, 61
  Namechk, 61
Reveye, 51
Riffle, 49–50, 50f
Robots, 17
Robtex, 68

S

Salesloft, 51
Search Diggity, 143–145
  basic requirement, 110
  interface, 110, 110f
  NotInMyBackyard, 112, 112f
  scan-Bing tab, 111, 112f
  scan-Google tab, 111, 111f
  Shodan scan, 112, 113f
Search engine optimization (SEO), 78
Search engines, 53. *See also specific search engines*
Secunia PSI, 211
Semantic search
  DuckDuckGo, 62, 62f
  Kngine, 63, 63f
Server, 7
Shodan, 48, 68–69, 69f
  banners, 107
  filters, 107, 108f
  popular searches, 107, 108f
  results for query "port:21 country:in,", 109, 109f
  results for query "webcam,", 108–109, 109f
Shoulder surfing, 208–209
Silk Road, 174
Small web format (SWF), 84
SNA. *See* Social network analysis (SNA)
Social media intelligence (SOCMINT), 20
Social media search, 63
  SocialMention, 63–64, 64f
  Social Searcher, 64–65
SocialMention, 63–64, 64f
Social network analysis (SNA)
  edges, 218
    betweenness, 222–227, 222f
    directed edges, 221
    ranking, 222
    type, 221
    undirected edges, 221
    weight, 221
  Gephi
    Data Laboratory tab, 219, 219f
    installation, 218
    Overview tab, 218–219, 219f
    Preview tab, 220
  network, 218
  nodes, 217, 220
Social network websites, 21f
  Facebook, 22
  features, 21b
  Google+, 24–25
  LinkedIn, 23
  Twitter, 24
Social Searcher, 64–65
SOCMINT. *See* Social media intelligence (SOCMINT)
Source code search, 66–67
  NerdyData, 66–67, 67f
  Ohloh code, 67
Spiders, 17
Spokeo, 56
SQL databases, 191–192, 192f
Storage devices, 269
Surface web, 17

T

Tape drives, 269
TheHarvester
  in action, 105, 105f
  HTML results, 105, 106f
  sources, 106–107
TheyRule, 58–59
Tineye, 51, 70
Top level domains (TLDs), 5–6, 6b
Topsy, 65, 65f
Tor, 164–165, 165f
  DuckDuckGo, 173, 173f
  files created, 175, 175f
  HiddenServicePort, 174–175
  Hidden Wiki, 172, 172f
  Silk Road, 174
  Torchan, 174, 174f
  Tor hidden service, 175f, 176
  Tor Wiki, 172, 173f
  XAMPP, 174
TOR bundle, 45
Torchan, 174, 174f
Trendsmap, 66
Trojan, 206

Truecaller, 74–75
Tweetbeep, 66
Twitter, 24, 30, 31f
  Topsy, 65, 65f
  Trendsmap, 66
  Tweetbeep, 66
  Twiangulate, 66

U

Ultrasurf, 152–153, 153f
Uniform resource locator (URL), 6–8

V

Virtualization, classifications, 7–8
Virtual private network (VPN), 161
  CyberGhost, 161–162, 162f
  Hideman, 163–164, 163f
Virtual world, 19
Virus, 206
Vital Information Resources Under Seize, 206

W

Wappalyzer, 48
WayBack Machine, 69
W3dt, 68
Weak passwords, 208
Web 2.0, 19–20
Web 3.0, 32
Web-based proxy, 156
  anonymouse.org, 156–158, 156f–157f
  Boomproxy.com, 159–160
  FilterBypass, 159, 159f
  Zend2, 158–159, 158f
Web browser, 7
WEBINT, 16
WebKit, 35
Weblogs/blogs, 18–19, 18f
Web of trust (WOT), 211, 211f
Web search engine, 7
Whitehat Aviator, 44–45
Whois, 68
Whoworks.at, 50
Wise Data Recovery, 270, 270f
WolframAlpha, 71–72, 72f
World Wide Web (WWW)
  vs. internet, 3
  media types, 3

X

Xmind, 199–201, 200f

Y

Yahoo
  contents, 88
  operators
    -, 88
    +, 88–90
    define, 89
    intitle, 89–90, 90f
    link, 88–89, 89f
    OR, 88
    site, 88
Yahoo Pipes, 121–124, 123f
Yandex, 90
  defined, 90
  operators, 91
    /, 94
    !, 92–93
    !!, 93
    “”, 93–94
    (), 93, 93f
    *, 94
    &, 91
    &&, 91
    +, 90–99
    ~, 91
    <<, 94
    Cat, 98–99
    date, 96–97
    domain, 97
    host, 96
    inurl, 95
    lang, 97–98
    mime:filetype, 95–96, 95f
    /number, 91–92
    rhost, 96
    site, 96
    title, 94–95
    url, 95
Yasni, 57

Z

Zend2, 158–159, 158f
Zoominfo, 60