

572.1- Off the Disk and Onto the Wire

Web Proxy Data.....24-66

Proxy servers 24-27

Overview24-25

Proxy solutions overview26

Commercial vs. open-source27

Squid proxy..... 28-36

Overview28

Configuration file29

access.log defaults30

Custom log format31

Squid log analysis33-34

calamaris, squidview...33

Raw analysis34

Converting UNIX timestamps35

Converting all timestamps36

Proxy log walkthrough example.....37~64

Intro37

Process38

Squid.conf file39-41

Squid access.log analysis42-45

Finding related activity.....46-47

Data dumping.....48-49

Timeline.....50-51

Carving60-64

Find objects by URL60

Railgrep objects.....61

Remove headers62

Identify file type63

Examine content64

Commercial proxy log analysis52

Web Proxy Cache53~66

Proxy Cache Extraction (Carving)53

Proxy Cache Configuration54

Squid cache file structure.....55-56

Squid cache objects57-58

Commercial proxy carving 66

tcpdump & Wireshark 68-101

tcpdump68~80

Overview 68

tcpdump usage & pitfalls 73

Useful tcpdump options 78

tcpdump examples 79-80

Wireshark69~99

Overview 69

Interface81-87

Overview.....81-83

Layout and name resolution84-85

Timestamps & columns86-87

Display filters88-96

BPF vs. display filters.....88-89

Matching and contains88-89

Prepare vs. Apply92-93

DNS compression.....92-93

Syntax checking94-96

Follow stream97-98

Additional features 99

Decode as99

Traffic capture99

PCAP file format 70-72

Magic bytes, snaplen, link-type 70

Packet/frame header 71

PCAP vs. PCAPNG formats 72

BPF primitives..... 74-77

Overview 74

Directionality, logical operators, helpful primitives
.....75-76

Data reduction 77

tshark..... 100-101

Overview 100

Usage 101

Network Evidence Acquisition..... 110-132

Where to start?	110
Example: Phishing	111-112
Evidence types	113-115
PCAP files (libpcap, npcap)	113
Netflow (IPFIX/IP flow)	114
Logs	115
Acquisition from switches	116-117
SPAN port/Port mirroring (software tap)	116-117
Acquisition from taps	118-119
Overview and options	118
Pros & cons	119
Internal Netflow Data	120
Infrastructure log sources	121
External log sources	122
Example evidence collection	123-126
Ideal case	123-124
Acceptable case	125
Worst/realistic case	126
Commercial solutions	127
Homegrown solutions	128
Collection platform design	129-130
Libraries (AF_INET vs. AF_PACKET)	129
What to capture?	129-130

Network Challenges & Opportunities 134-143

Overview	134
NAT (Network Address Translation)	135-136
Architecture	137-141
Encryption	137
Tunnels & VPN	138
Optimization	139
Wireless networks	140
Cloud	141
Everything-over-internet	142
Malware is network driven	143