572.1 - Off the Disk and Onto the Wire

[Web Proxy Data](#_Toc156234297) 24-66

[Proxy servers](#_Toc156234298) 24-27

[Overview](#_Toc156234299) 24-25

[Proxy solutions overview](#_Toc156234300) 26

[Commercial vs. open-source](#_Toc156234301) 27

[Squid proxy](#_Toc156234302) 28-36

[Overview](#_Toc156234303) 28

[Configuration file](#_Toc156234304) 29

[access.log defaults](#_Toc156234305) 30

[Custom log format](#_Toc156234306) 31

[Squid log analysis](#_Toc156234307) 33-34

[calamaris, squidview…](#_Toc156234308) 33

[Raw analysis](#_Toc156234309) 34

[Converting UNIX timestamps](#_Toc156234310) 35

[Converting all timestamps](#_Toc156234311) 36

[Proxy log walkthrough example](#_Toc156234312) 37~64

[Intro](#_Toc156234313) 37

[Process](#_Toc156234314) 38

[Squid.conf file](#_Toc156234315) 39-41

[Squid access.log analysis](#_Toc156234316) 42-45

[Finding related activity](#_Toc156234317) 46-47

[Data dumping](#_Toc156234318) 48-49

[Timeline](#_Toc156234319) 50-51

[Carving](#_Toc156234320) 60-64

[Find objects by URL](#_Toc156234321) 60

[Railgrep objects](#_Toc156234322) 61

[Remove headers](#_Toc156234323) 62

[Identify file type](#_Toc156234324) 63

[Examine content](#_Toc156234325) 64

[Commercial proxy log analysis](#_Toc156234326) 52

[Web Proxy Cache](#_Toc156234327) 53~66

[Proxy Cache Extraction (Carving)](#_Toc156234328) 53

[Proxy Cache Configuration](#_Toc156234329) 54

[Squid cache file structure](#_Toc156234330) 55-56

[Squid cache objects](#_Toc156234331) 57-58

[Commercial proxy carving](#_Toc156234332) 66

[tcpdump & Wireshark](#_Toc156234333) 68-101

[tcpdump](#_Toc156234334) 68~80

[Overview](#_Toc156234335) 68

[tcpdump usage & pitfalls](#_Toc156234336) 73

[Useful tcpdump options](#_Toc156234337) 78

[tcpdump examples](#_Toc156234338) 79-80

[Wireshark](#_Toc156234339) 69~99

[Overview](#_Toc156234340) 69

[Interface](#_Toc156234341) 81-87

[Overview](#_Toc156234342) 81-83

[Layout and name resolution](#_Toc156234343) 84-85

[Timestamps & columns](#_Toc156234344) 86-87

[Display filters](#_Toc156234345) 88-96

[BPF vs. display filters](#_Toc156234346) 88-89

[Matching and contains](#_Toc156234347) 88-89

[Prepare vs. Apply](#_Toc156234348) 92-93

[DNS compression](#_Toc156234349) 92-93

[Syntax checking](#_Toc156234350) 94-96

[Follow stream](#_Toc156234351) 97-98

[Additional features](#_Toc156234352) 99

[Decode as](#_Toc156234353) 99

[Traffic capture](#_Toc156234354) 99

[PCAP file format](#_Toc156234355) 70-72

[Magic bytes, snaplen, link-type](#_Toc156234356) 70

[Packet/frame header](#_Toc156234357) 71

[PCAP vs. PCAPNG formats](#_Toc156234358) 72

[BPF primitives](#_Toc156234359) 74-77

[Overview](#_Toc156234360) 74

[Directionality, logical operators, helpful primitives](#_Toc156234361) 75-76

[Data reduction](#_Toc156234362) 77

[tshark](#_Toc156234363) 100-101

[Overview](#_Toc156234364) 100

[Usage](#_Toc156234365) 101

[Network Evidence Acquisition](#_Toc156234366) 110-132

[Where to start?](#_Toc156234367) 110

[Example: Phishing](#_Toc156234368) 111-112

[Evidence types](#_Toc156234369) 113-115

[PCAP files (libpcap, npcap)](#_Toc156234370) 113

[Netflow (IPFIX/IP flow)](#_Toc156234371) 114

[Logs](#_Toc156234372) 115

[Acquisition from switches](#_Toc156234373) 116-117

[SPAN port/Port mirroring (software tap)](#_Toc156234374) 116-117

[Acquisition from taps](#_Toc156234375) 118-119

[Overview and options](#_Toc156234376) 118

[Pros & cons](#_Toc156234377) 119

[Internal Netflow Data](#_Toc156234378) 120

[Infrastructure log sources](#_Toc156234379) 121

[External log sources](#_Toc156234380) 122

[Example evidence collection](#_Toc156234381) 123-126

[Ideal case](#_Toc156234382) 123-124

[Acceptable case](#_Toc156234383) 125

[Worst/realistic case](#_Toc156234384) 126

[Commercial solutions](#_Toc156234385) 127

[Homegrown solutions](#_Toc156234386) 128

[Collection platform design](#_Toc156234387) 129-130

[Libraries (AF\_INET vs. AF\_PACKET)](#_Toc156234388) 129

[What to capture?](#_Toc156234389) 129-130

[Network Challenges & Opportunities](#_Toc156234390) 134-143

[Overview](#_Toc156234391) 134

[NAT (Network Address Translation)](#_Toc156234392) 135-136

[Architecture](#_Toc156234393) 137-141

[Encryption](#_Toc156234394) 137

[Tunnels & VPN](#_Toc156234395) 138

[Optimization](#_Toc156234396) 139

[Wireless networks](#_Toc156234397) 140

[Cloud](#_Toc156234398) 141

[Everything-over-internet](#_Toc156234399) 142

[Malware is network driven](#_Toc156234400) 143

# Web Proxy Data 24-66

## Proxy servers 24-27

### Overview 24-25

### Proxy solutions overview 26

### Commercial vs. open-source 27

## Squid proxy 28-36

### Overview 28

### Configuration file 29

### access.log defaults 30

### Custom log format 31

### Squid log analysis 33-34

#### calamaris, squidview… 33

#### Raw analysis 34

#### Converting UNIX timestamps 35

#### Converting all timestamps 36

## Proxy log walkthrough example 37-51

### Intro 37

### Process 38

### Squid.conf file 39-41

### Squid access.log analysis 42-45

### Finding related activity 46-47

### Data dumping 48-49

### Timeline 50-51

### Carving 60-64

#### Find objects by URL 60

#### Railgrep objects 61

#### Remove headers 62

#### Identify file type 63

#### Examine content 64

## Commercial proxy log analysis 52

## Web Proxy Cache 53-58

### Proxy Cache Extraction (Carving) 53

### Proxy Cache Configuration 54

### Squid cache file structure 55-56

### Squid cache objects 57-58

### Commercial proxy carving 66

# tcpdump & Wireshark 68-101

## tcpdump 68~80

### Overview 68

### tcpdump usage & pitfalls 73

### Useful tcpdump options 78

### tcpdump examples 79-80

## Wireshark 69~

### Overview 69

### Interface 81-87

#### Overview 81-83

#### Layout and name resolution 84-85

#### Timestamps & columns 86-87

### Display filters 88-96

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

#### Matching and contains 88-89

#### Prepare vs. Apply 92-93

#### DNS compression 92-93

#### Syntax checking 94-96

### Follow stream 97-98

### Additional features 99

#### Decode as 99

#### Traffic capture 99

## PCAP file format 70-72

### Magic bytes, snaplen, link-type 70

### Packet/frame header 71

### PCAP vs. PCAPNG formats 72

## BPF primitives 74-

### 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