572.4 - Commercial Tools, Wireless, and Full-packet Hunting

[SMTP 4-23](#_Toc156246984)

[Overview & history 4](#_Toc156246985)

[M-acronyms 5](#_Toc156246986)

[MUA, MSA, MTA, MX, MDA 5](#_Toc156246987)

[Email message flow 6-8](#_Toc156246988)

[Common ports 9](#_Toc156246989)

[Basic transaction example 10-13](#_Toc156246990)

[SMTP evolutions 14](#_Toc156246991)

[MIME & Base64 15-17](#_Toc156246992)

[MIME Example 16-17](#_Toc156246993)

[Authentication 18-19](#_Toc156246994)

[Overview & history 18](#_Toc156246995)

[Examples 19](#_Toc156246996)

[Encryption 20-21](#_Toc156246997)

[Native TLS vs. STARTTLS 20](#_Toc156246998)

[STARTTLS example 21](#_Toc156246999)

[Unicode handling 22](#_Toc156247000)

[Investigative relevance 23](#_Toc156247001)

[Exfiltration 23](#_Toc156247002)

[Network Miner 25-35](#_Toc156247003)

[Overview 25](#_Toc156247004)

[Host profiling 29-30](#_Toc156247005)

[Image & credential extraction 31-32](#_Toc156247006)

[Use-cases 33](#_Toc156247007)

[CapLoader for large PCAPs 34-35](#_Toc156247008)

[Wireless Network Forensics 40-82](#_Toc156247009)

[Course scope 40](#_Toc156247010)

[Attack surface 41](#_Toc156247011)

[Modes 42-43](#_Toc156247012)

[Master & Managed 42](#_Toc156247013)

[Ad-Hoc & Monitor 43](#_Toc156247014)

[Basic Service Set (BSS) 44](#_Toc156247015)

[Extended Service Set (ESS) 45-46](#_Toc156247016)

[Legality 47](#_Toc156247017)

[Tools 48-57](#_Toc156247018)

[Required tools 48](#_Toc156247019)

[Alfa USB adapter 49](#_Toc156247020)

[802.11 analysers 50-51](#_Toc156247021)

[Wireshark 50](#_Toc156247022)

[Kismet 50](#_Toc156247023)

[NetSpot 50](#_Toc156247024)

[tcpdump 50](#_Toc156247025)

[inSSIDer 52-53](#_Toc156247026)

[Built-In macOS WiFi tools 54](#_Toc156247027)

[WiFi Controller software 55-57](#_Toc156247028)

[802.11 Frame 58-66](#_Toc156247029)

[Overview 58](#_Toc156247030)

[Frame types 59](#_Toc156247031)

[Management frame subtype 60](#_Toc156247032)

[Service Set Identifier (SSID) 61-62](#_Toc156247033)

[Control frame subtype 63](#_Toc156247034)

[Data frames 64](#_Toc156247035)

[Frame control fields (directionality) 65-66](#_Toc156247036)

[ToDS, FromDS 65-66](#_Toc156247037)

[Sniffing 67-71](#_Toc156247038)

[Managed mode sniffing 67-68](#_Toc156247039)

[RFMON sniffing – WPA2 69](#_Toc156247040)

[RFMON sniffing – No WPA/WEP 70-71](#_Toc156247041)

[Attacks 72-82](#_Toc156247042)

[Detection difficulties 72](#_Toc156247043)

[Main attacks overview 73](#_Toc156247044)

[WPA2 PSK attacks 74-75](#_Toc156247045)

[DOS: RF overload 76](#_Toc156247046)

[DOS: Deauth & RTS/CTS attacks 77-78](#_Toc156247047)

[Spotting DOS 79](#_Toc156247048)

[Evil twin attack 80-81](#_Toc156247049)

[Attacker staged approach 82](#_Toc156247050)

[Automated tools & libraries 84-102](#_Toc156247051)

[Overview & categories 84](#_Toc156247052)

[Popular libraries 85](#_Toc156247053)

[libpcap/npcap 85](#_Toc156247054)

[libnids 85](#_Toc156247055)

[tcpflow 86-88](#_Toc156247056)

[Overview 86](#_Toc156247057)

[Object extraction 87-88](#_Toc156247058)

[Scapy 89](#_Toc156247059)

[Dshell 90-91](#_Toc156247060)

[editcap 92](#_Toc156247061)

[ngrep 93](#_Toc156247062)

[tcpstat & tcpdstat 94-97](#_Toc156247063)

[Overview 94-95](#_Toc156247064)

[gnuplot visualization 96-97](#_Toc156247065)

[ntopng 98-100](#_Toc156247066)

[tcpextract 101-102](#_Toc156247067)

[Arkime 106-129](#_Toc156247068)

[Overview 107-108](#_Toc156247069)

[Components (Capture, Elastic, Viewer) 108](#_Toc156247070)

[Architecture 109-110](#_Toc156247071)

[Limitations 111](#_Toc156247072)

[Processing PCAP files 112](#_Toc156247073)

[Filtering/querying 113-115](#_Toc156247074)

[Fields 113-114](#_Toc156247075)

[Examples 115](#_Toc156247076)

[Viewer walkthrough 116-125](#_Toc156247077)

[Sessions & rows 116-117](#_Toc156247078)

[Sessions inspection 118-119](#_Toc156247079)

[Uncompress: Extracting files 120-121](#_Toc156247080)

[Connections tab 122-123](#_Toc156247081)

[Hunts tab 124-125](#_Toc156247082)

[Native enrichment 126](#_Toc156247083)

[WISE – other enrichments 127](#_Toc156247084)

[Integrated CyberChef 128-129](#_Toc156247085)

# SMTP 4-23

## Overview & history 4

## M-acronyms 5

### MUA, MSA, MTA, MX, MDA 5

## Email message flow 6-8

## Common ports 9

## Basic transaction example 10-13

## SMTP evolutions 14

## MIME & Base64 15-17

### MIME Example 16-17

## Authentication 18-19

### Overview & history 18

### Examples 19

## Encryption 20-21

### Native TLS vs. STARTTLS 20

### STARTTLS example 21

## Unicode handling 22

## Investigative relevance 23

### Exfiltration 23

# Network Miner 25-35

## Overview 25

## Host profiling 29-30

## Image & credential extraction 31-32

## Use-cases 33

## CapLoader for large PCAPs 34-35

# Wireless Network Forensics 40-82

## Course scope 40

## Attack surface 41

## Modes 42-43

### Master & Managed 42

### Ad-Hoc & Monitor 43

## Basic Service Set (BSS) 44

## Extended Service Set (ESS) 45-46

## Legality 47

## Tools 48-57

### Required tools 48

### Alfa USB adapter 49

### 802.11 analysers 50-51

#### Wireshark 50

#### Kismet 50

#### NetSpot 50

#### tcpdump 50

### inSSIDer 52-53

### Built-In macOS WiFi tools 54

### WiFi Controller software 55-57

## 802.11 Frame 58-66

### Overview 58

### Frame types 59

### Management frame subtype 60

### Service Set Identifier (SSID) 61-62

### Control frame subtype 63

### Data frames 64

### Frame control fields (directionality) 65-66

#### ToDS, FromDS 65-66

## Sniffing 67-71

### Managed mode sniffing 67-68

### RFMON sniffing – WPA2 69

### RFMON sniffing – No WPA/WEP 70-71

## Attacks 72-82

### Detection difficulties 72

### Main attacks overview 73

### WPA2 PSK attacks 74-75

### DOS: RF overload 76

### DOS: Deauth & RTS/CTS attacks 77-78

### Spotting DOS 79

### Evil twin attack 80-81

### Attacker staged approach 82

# Automated tools & libraries 84-102

## Overview & categories 84

## Popular libraries 85

### libpcap/npcap 85

### libnids 85

## tcpflow 86-88

### Overview 86

### Object extraction 87-88

## Scapy 89

## Dshell 90-91

## editcap 92

## ngrep 93

## tcpstat & tcpdstat 94-97

### Overview 94-95

### gnuplot visualization 96-97

## ntopng 98-100

## tcpextract 101-102

# Arkime 106-129

## Overview 107-108

### Components (Capture, Elastic, Viewer) 108

## Architecture 109-110

## Limitations 111

## Processing PCAP files 112

## Filtering/querying 113-115

### Fields 113-114

### Examples 115

## Viewer walkthrough 116-125

### Sessions & rows 116-117

### Sessions inspection 118-119

### Uncompress: Extracting files 120-121

### Connections tab 122-123

### Hunts tab 124-125

## Native enrichment 126

## WISE – other enrichments 127

## Integrated CyberChef 128-129