572.3 - NetFlow and File Access Protocols

[NetFlow](#_Toc156243681) 4-27

[Full-packet doesn’t scale](#_Toc156243682) 4

[Overview](#_Toc156243683) 5

[Forensic use-cases](#_Toc156243684) 6

[Versions & history](#_Toc156243685) 7

[Implementations](#_Toc156243686) 8

[NetFlow Architecture](#_Toc156243687) 9-10

[NetFlow UDP & SCTP](#_Toc156243688) 11

[NetFlow V5](#_Toc156243689) 12-13

[Header & flow record](#_Toc156243690) 12-13

[NetFlow V9](#_Toc156243691) 12-13

[Header & template record](#_Toc156243692) 14

[Data record & Content Types](#_Toc156243693) 15

[Identifying collection points](#_Toc156243694) 16-18

[NetFlow exporter basics](#_Toc156243695) 19

[Analyst interface](#_Toc156243696) 20

[Storage and format options](#_Toc156243697) 21-22

[Lack of content](#_Toc156243698) 23

[Encryption 24](#_Toc156243699)

[Multi-use protocols 25](#_Toc156243700)

[Encrypted traffic 26-27](#_Toc156243701)

[Open-source flow tools 28-50](#_Toc156243702)

[nfcapd/nfpcapd 28-29](#_Toc156243703)

[nfdump 30-42](#_Toc156243704)

[Overview 30](#_Toc156243705)

[Input 31](#_Toc156243706)

[Filters 32](#_Toc156243707)

[Output 33-35](#_Toc156243708)

[Example scenarios 36-38](#_Toc156243709)

[C2 UDP/8765 36](#_Toc156243710)

[Autonomous Systems (AS) 37-38](#_Toc156243711)

[Aggregating flows (-a, -A) 39-40](#_Toc156243712)

[TopN statistics (-s, -n) 41-42](#_Toc156243713)

[SOF-ELK 43-50](#_Toc156243714)

[Overview 43](#_Toc156243715)

[Loading flow data (nfcapd, cloud, Zeek, live) 44](#_Toc156243716)

[NetFlow Dashboard 45-50](#_Toc156243717)

[FTP 55-74](#_Toc156243718)

[Overview & history 55-56](#_Toc156243719)

[Basics (channels overview) 57](#_Toc156243720)

[Active FTP 58-60](#_Toc156243721)

[Active FTP visualized 58](#_Toc156243722)

[PORT Command 59](#_Toc156243723)

[Shortcomings 60](#_Toc156243724)

[Passive FTP 60-62](#_Toc156243725)

[Explanation 60](#_Toc156243726)

[Passive FTP visualized 61](#_Toc156243727)

[Extended Passive FTP 62](#_Toc156243728)

[Capturing FTP 63](#_Toc156243729)

[Analyzing FTP 64-74](#_Toc156243730)

[Overview 64](#_Toc156243731)

[Automated tools overview 65](#_Toc156243732)

[File extraction with Wireshark 66-74](#_Toc156243733)

[Microsoft file sharing protocols 79-108](#_Toc156243734)

[Forensic relevance 79](#_Toc156243735)

[Windows Architecture 80](#_Toc156243736)

[Expected protocols 81-82](#_Toc156243737)

[Outlook-to-exchange email traffic 83](#_Toc156243738)

[0x45 XOR 83](#_Toc156243739)

[SMB versions 84-88](#_Toc156243740)

[Release dates 84](#_Toc156243741)

[Version comparison 85](#_Toc156243742)

[Identifying clients by SMB version 86](#_Toc156243743)

[Who else uses what version? 87](#_Toc156243744)

[Key changes with SMB3 (encryption) 88](#_Toc156243745)

[SMB analysis 89-108](#_Toc156243746)

[Forensic goals 89](#_Toc156243747)

[Commons adversary behavior 90](#_Toc156243748)

[Filter & review SMB 91](#_Toc156243749)

[SMB2/3 commands overview 92](#_Toc156243750)

[Typical SMB2/3 session 93-107](#_Toc156243751)

[Overview 93](#_Toc156243752)

[Protocol negotiation (NEGOTIATE) 94-95](#_Toc156243753)

[Session established (SESSION\_SETUP) 96-97](#_Toc156243754)

[Access services (TREE\_CONNECT) 98](#_Toc156243755)

[Directory navigation (CREATE) 99-100](#_Toc156243756)

[Directory listing (QUERY\_DIRECTORY) 101-102](#_Toc156243757)

[Opening files (CREATE) 103-104](#_Toc156243758)

[Read from a file (READ/WRITE) 105-106](#_Toc156243759)

[Close file (CLOSE) 107](#_Toc156243760)

[Disconnect tree (TREE\_DISCONNECT) 107](#_Toc156243761)

[Logoff (LOGOFF) 107](#_Toc156243762)

[Behavioral attack indicators (IOCs) 108](#_Toc156243763)

# NetFlow 4-27

## Full-packet doesn’t scale 4

## Overview 5

## Forensic use-cases 6

## Versions & history 7

## Implementations 8

## NetFlow Architecture 9-10

## NetFlow UDP & SCTP 11

## NetFlow V5 12-13

### Header & flow record 12-13

## NetFlow V9 12-13

### Header & template record 14

### Data record & Content Types 15

## Identifying collection points 16-18

## NetFlow exporter basics 19

## Analyst interface 20

## Storage and format options 21-22

## Lack of content 23

## Encryption 24

### Multi-use protocols 25

### Encrypted traffic 26-27

# Open-source flow tools 28-50

## nfcapd/nfpcapd 28-29

## nfdump 30-42

### Overview 30

### Input 31

### Filters 32

### Output 33-35

### Example scenarios 36-38

#### C2 UDP/8765 36

#### Autonomous Systems (AS) 37-38

### Aggregating flows (-a, -A) 39-40

### TopN statistics (-s, -n) 41-42

## SOF-ELK 43-50

### Overview 43

### Loading flow data (nfcapd, cloud, Zeek, live) 44

### NetFlow Dashboard 45-50

# FTP 55-

## Overview & history 55-56

## Basics (channels overview) 57

## Active FTP 58-60

### Active FTP visualized 58

### PORT Command 59

### Shortcomings 60

## Passive FTP 60-62

### Explanation 60

### Passive FTP visualized 61

### Extended Passive FTP 62

## Capturing FTP 63

## Analyzing FTP 64-74

### Overview 64

### Automated tools overview 65

### File extraction with Wireshark 66-74

# Microsoft file sharing protocols 79-108

## Forensic relevance 79

## Windows Architecture 80

## Expected protocols 81-82

## Outlook-to-exchange email traffic 83

### 0x45 XOR 83

## SMB versions 84-88

### Release dates 84

### Version comparison 85

### Identifying clients by SMB version 86

### Who else uses what version? 87

### Key changes with SMB3 (encryption) 88

## SMB analysis 89-108

### Forensic goals 89

### Commons adversary behavior 90

### Filter & review SMB 91

### SMB2/3 commands overview 92

### Typical SMB2/3 session 93-

#### Overview 93

#### Protocol negotiation (NEGOTIATE) 94-95

#### Session established (SESSION\_SETUP) 96-97

#### Access services (TREE\_CONNECT) 98

#### Directory navigation (CREATE) 99-100

#### Directory listing (QUERY\_DIRECTORY) 101-102

#### Opening files (CREATE) 103-104

#### Read from a file (READ/WRITE) 105-106

#### Close file (CLOSE) 107

#### Disconnect tree (TREE\_DISCONNECT) 107

#### Logoff (LOGOFF) 107

### Behavioral attack indicators (IOCs) 108