

# 572.3 – NetFlow and File Access Protocols

## 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..... 55-74

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 .....	93-107
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