Intro to

Network Forensics

TABLE OF CONTENTS

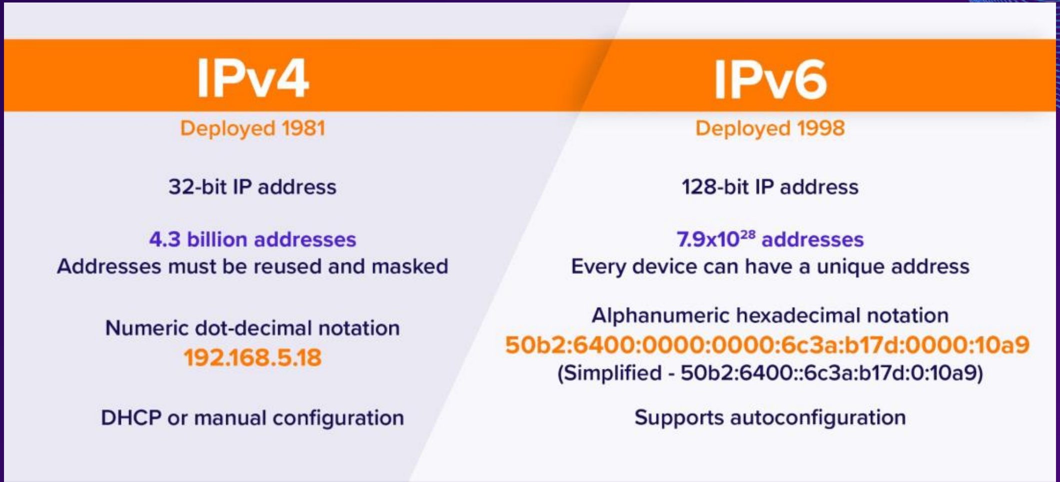
01 Network Basics

02 Wireshark Basics

03 CTF Example

Network Traffic

- The amount of data moving across a computer network at some point in time
- Usually stored in network traffic logs with .pcap or .pcapng file- programs like Wireshark can help analyze them
- IP Addresses- show the source and destination of the packet



IPv4	IPv6
Deployed 1981	Deployed 1998
32-bit IP address	128-bit IP address
4.3 billion addresses Addresses must be reused and masked	$7.9x10^{28}$ addresses Every device can have a unique address
Numeric dot-decimal notation 192.168.5.18	Alphanumeric hexadecimal notation 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration	Supports autoconfiguration

Network Basics

1. Private vs Public IP Addresses
192.168.0.0–192.168.255.255 (65,536 IP addresses)
172.16.0.0–172.31.255.255 (1,048,576 IP addresses)
10.0.0.0–10.255.255.255 (16,777,216 IP addresses)

2. Ports

Ports 0 to 1023 are Well-Known Ports.
Ports 1024 to 49151 are Registered Ports.
Ports 49152 to 65535 are Public Ports.

Network Basics

The port numbers in the range from 0 to 1023 are the well-known ports or system ports. They are used by system processes that provide widely used types of network services. On Unix-like operating systems, a process must execute with superuser privileges to be able to bind a network socket to an IP address using one of the well-known ports

The range of port numbers from 1024 to 49151 are the registered ports. They are assigned by IANA(Internet Assigned Numbers Authority) for specific service upon application by a requesting entity. On most systems, registered ports can be used without superuser privileges.

Network Basics

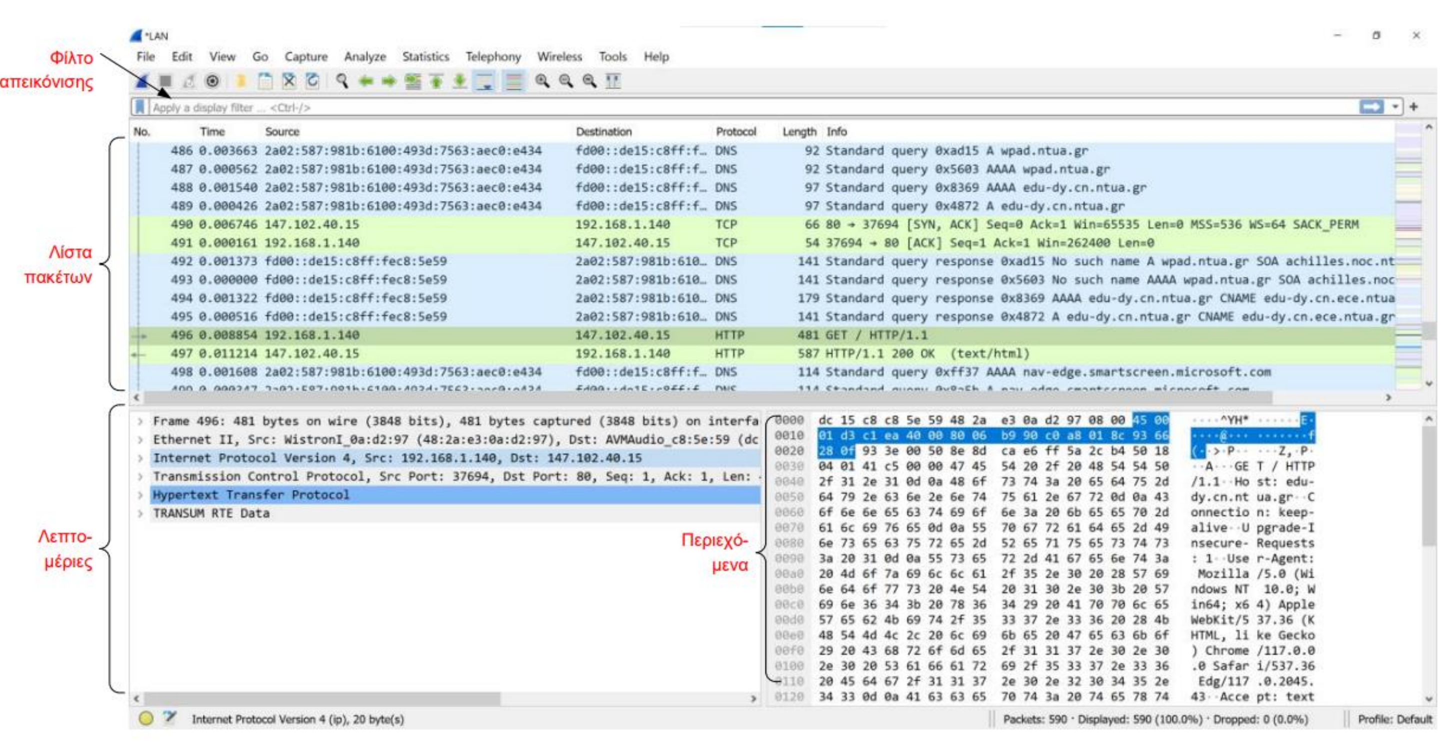
The range 49152–65535, 16.384 ports, contains dynamic or private ports that cannot be registered with IANA. This range is used for private or customized services, for temporary purposes, and for automatic allocation of ephemeral ports.

An ephemeral port is a communications endpoint (port) of a transport layer protocol of the Internet protocol suite that is used for only a short period of time for the duration of a communication session.

Network Basics

- **Ports 20 and 21:** File Transfer Protocol (FTP). FTP is for transferring files between a client and a server.
- **Port 20:** FTP data transfer
- **Port 21:** FTP control connection
- **Port 22:** Secure Shell (SSH). SSH is one of many tunneling protocols that create secure network connections.
- **Port 23:** Telnet
- **Port 25**: Historically, Simple Mail Transfer Protocol (SMTP). SMTP is used for email.
- **Port 53:** Domain Name System (DNS).
- **Port 80:** Hypertext Transfer Protocol (HTTP).
- **Port 88:** Kerberos
- **Port 443:** HTTP Secure (HTTPS).
- **Port 587:** Modern, secure SMTP that uses encryption.
- **Port 3389:** Remote Desktop Protocol (RDP). RDP enables users to remotely connect to their desktop computers from another device.

Wireshark Basics


*LAN
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Φίλτο απεικόνισης

Λίστα πακέτων

Λεπτο-μέριες

Περιεχό-μενα

```
No.   Time     Source                                 Destination          Protocol  Length Info
  486 0.003663 2a02:587:981b:6100:493d:7563:aec0:e434 fd00::de15:c8ff:f… DNS         92 Standard query 0xad15 A wpad.ntua.gr
  487 0.000562 2a02:587:981b:6100:493d:7563:aec0:e434 fd00::de15:c8ff:f… DNS         92 Standard query 0x5603 AAAA wpad.ntua.gr
  488 0.001540 2a02:587:981b:6100:493d:7563:aec0:e434 fd00::de15:c8ff:f… DNS         97 Standard query 0x8369 AAAA edu-dy.cn.ntua.gr
  489 0.000426 2a02:587:981b:6100:493d:7563:aec0:e434 fd00::de15:c8ff:f… DNS         97 Standard query 0x4872 A edu-dy.cn.ntua.gr
  490 0.006746 147.102.40.15                          192.168.1.140       TCP         66 80 → 37694 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536 WS=64 SACK_PERM
  491 0.000161 192.168.1.140                          147.102.40.15       TCP         54 37694 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
  492 0.001373 fd00::de15:c8ff:fec8:5e59              2a02:587:981b:610… DNS        141 Standard query response 0xad15 No such name A wpad.ntua.gr SOA achilles.noc.nt
  493 0.000000 fd00::de15:c8ff:fec8:5e59              2a02:587:981b:610… DNS        141 Standard query response 0x5603 No such name AAAA wpad.ntua.gr SOA achilles.noc
  494 0.001322 fd00::de15:c8ff:fec8:5e59              2a02:587:981b:610… DNS        179 Standard query response 0x8369 AAAA edu-dy.cn.ntua.gr CNAME edu-dy.cn.ece.ntua
  495 0.000516 fd00::de15:c8ff:fec8:5e59              2a02:587:981b:610… DNS        141 Standard query response 0x4872 A edu-dy.cn.ntua.gr CNAME edu-dy.cn.ece.ntua.gr
  496 0.008854 192.168.1.140                          147.102.40.15       HTTP       481 GET / HTTP/1.1
  497 0.011214 147.102.40.15                          192.168.1.140       HTTP       587 HTTP/1.1 200 OK  (text/html)
  498 0.001608 2a02:587:981b:6100:493d:7563:aec0:e434 fd00::de15:c8ff:f… DNS        114 Standard query 0xff37 AAAA nav-edge.smartscreen.microsoft.com
```

```
> Frame 496: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interfa
> Ethernet II, Src: WistronI_0a:d2:97 (48:2a:e3:0a:d2:97), Dst: AVMAudio_c8:5e:59 (dc
> Internet Protocol Version 4, Src: 192.168.1.140, Dst: 147.102.40.15
> Transmission Control Protocol, Src Port: 37694, Dst Port: 80, Seq: 1, Ack: 1, Len:
> Hypertext Transfer Protocol
> TRANSUM RTE Data
```

```
0000  dc 15 c8 c8 5e 59 48 2a  e3 0a d2 97 08 00 45 00   ····^YH* ······E·
0010  01 d3 c1 ea 40 00 80 06  b9 90 c0 a8 01 8c 93 66   ····@··· ·······f
0020  28 0f 93 3e 00 50 8e 8d  ca e6 ff 5a 2c b4 50 18   (··>·P·· ···Z,·P·
0030  04 01 41 c5 00 00 47 45  54 20 2f 20 48 54 54 50   ··A···GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 65 64 75 2d   /1.1··Ho st: edu-
0050  64 79 2e 63 6e 2e 6e 74  75 61 2e 67 72 0d 0a 43   dy.cn.nt ua.gr··C
0060  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
0070  61 6c 69 76 65 0d 0a 55  70 67 72 61 64 65 2d 49   alive··U pgrade-I
0080  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
0090  3a 20 31 0d 0a 55 73 65  72 2d 41 67 65 6e 74 3a   : 1··Use r-Agent:
00a0  20 4d 6f 7a 69 6c 6c 61  2f 35 2e 30 20 28 57 69    Mozilla /5.0 (Wi
00b0  6e 64 6f 77 73 20 4e 54  20 31 30 2e 30 3b 20 57   ndows NT  10.0; W
00c0  69 6e 36 34 3b 20 78 36  34 29 20 41 70 70 6c 65   in64; x6 4) Apple
00d0  57 65 62 4b 69 74 2f 35  33 37 2e 33 36 20 28 4b   WebKit/5 37.36 (K
00e0  48 54 4d 4c 2c 20 6c 69  6b 65 20 47 65 63 6b 6f   HTML, li ke Gecko
00f0  29 20 43 68 72 6f 6d 65  2f 31 31 37 2e 30 2e 30   ) Chrome /117.0.0
0100  2e 30 20 53 61 66 61 72  69 2f 35 33 37 2e 33 36   .0 Safar i/537.36
0110  20 45 64 67 2f 31 31 37  2e 30 2e 32 30 34 35 2e    Edg/117 .0.2045.
0120  34 33 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   43··Acce pt: text
```

Internet Protocol Version 4 (ip), 20 byte(s) | Packets: 590 · Displayed: 590 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Image Source: ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ ΣΕΙΡΑ1

Wireshark Basics

Filters for IP Addresses

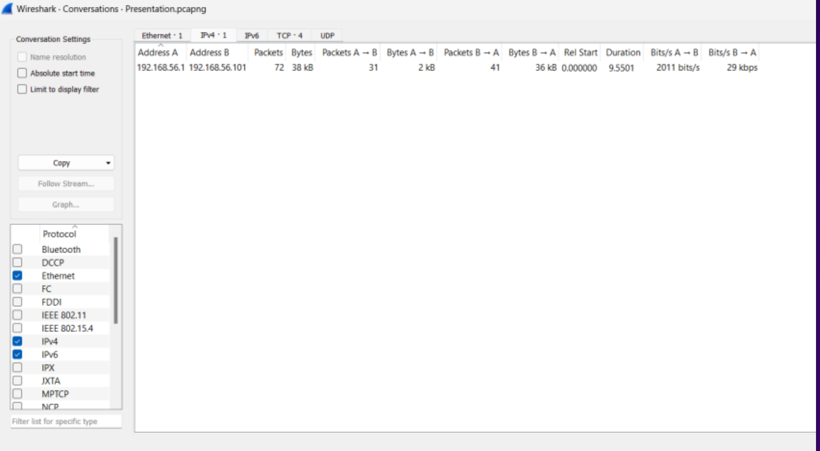
ip.addr == <IP address> — to find traffic of a particular IP Address
ip.src == <IP address> — to find traffic originating from particular IP Address
ip.dst == <IP address> —to find traffic pointed at a particular IP Address
ip.src == <IP address> and ip.dst == <IP address>
ip.src == <IP address> or ip.dst == <IP address>

Filters for Ports

tcp.port == 80, where 80 is port number
tcp.dstport == 80.
udp.port ==80
http — to filter traffic based on HTTP protocol
dns
http.request — when HTTP requests a file or resource, this filter can exclusively separate them out
http.request.method==GET

Wireshark Basics

Statistics-> Conversations



Wireshark - Conversations - Presentation.pcapng

Conversation Settings

- □ Name resolution
- □ Absolute start time
- □ Limit to display filter

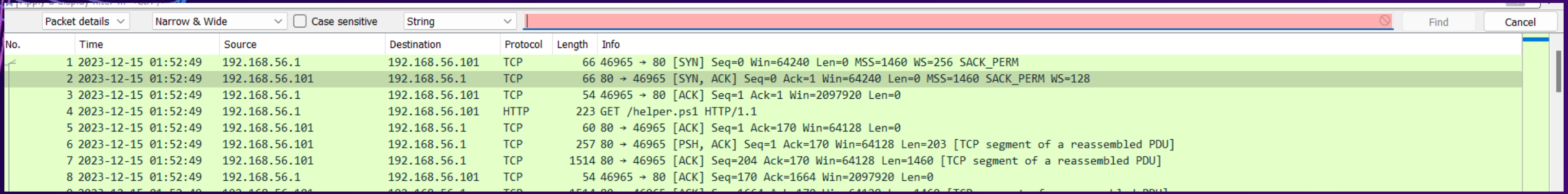
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.56.1	192.168.56.101	72	38 kB	31	2 kB	41	36 kB	0.000000	9.5501	2011 bits/s	29 kbps

	Protocol
□	Bluetooth
□	DCCP
☑	Ethernet
□	FC
□	FDDI
□	IEEE 802.11
□	IEEE 802.15.4
☑	IPv4
☑	IPv6
□	IPX
□	JXTA
□	MPTCP
□	NCP

Filter list for specific type

Wireshark Basics

Edit-> Find Packet
Ctrl+F



Packet details ⌄ | Narrow & Wide ⌄ | □ Case sensitive | String ⌄

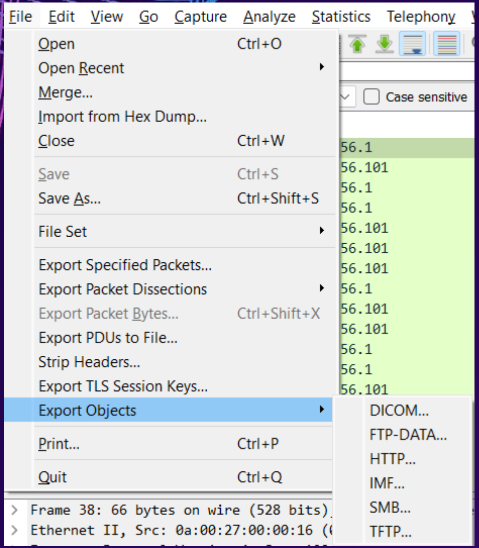
No.	Time	Source	Destination	Protocol	Length	Info
1	2023-12-15 01:52:49	192.168.56.1	192.168.56.101	TCP	66	46965 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	2023-12-15 01:52:49	192.168.56.101	192.168.56.1	TCP	66	80 → 46965 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
3	2023-12-15 01:52:49	192.168.56.1	192.168.56.101	TCP	54	46965 → 80 [ACK] Seq=1 Ack=1 Win=2097920 Len=0
4	2023-12-15 01:52:49	192.168.56.1	192.168.56.101	HTTP	223	GET /helper.ps1 HTTP/1.1
5	2023-12-15 01:52:49	192.168.56.101	192.168.56.1	TCP	60	80 → 46965 [ACK] Seq=1 Ack=170 Win=64128 Len=0
6	2023-12-15 01:52:49	192.168.56.101	192.168.56.1	TCP	257	80 → 46965 [PSH, ACK] Seq=1 Ack=170 Win=64128 Len=203 [TCP segment of a reassembled PDU]
7	2023-12-15 01:52:49	192.168.56.101	192.168.56.1	TCP	1514	80 → 46965 [ACK] Seq=204 Ack=170 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
8	2023-12-15 01:52:49	192.168.56.1	192.168.56.101	TCP	54	46965 → 80 [ACK] Seq=170 Ack=1664 Win=2097920 Len=0

Packet list->Info column
Packet details->Details section
Packet bytes->Contents section

Display filter
Hex Value
String
Regular Expression

Wireshark Basics

File->Export Objects



```
56.1
56.101
56.1
56.1
56.101
56.101
56.101
56.1
56.101
56.101
56.1
56.1
56.101
```

```
> Frame 38: 66 bytes on wire (528 bits)
> Ethernet II, Src: 0a:00:27:00:00:16 ((
```

DICOM->Digital Imaging and Communications in Medicine

HTTP-> http traffic

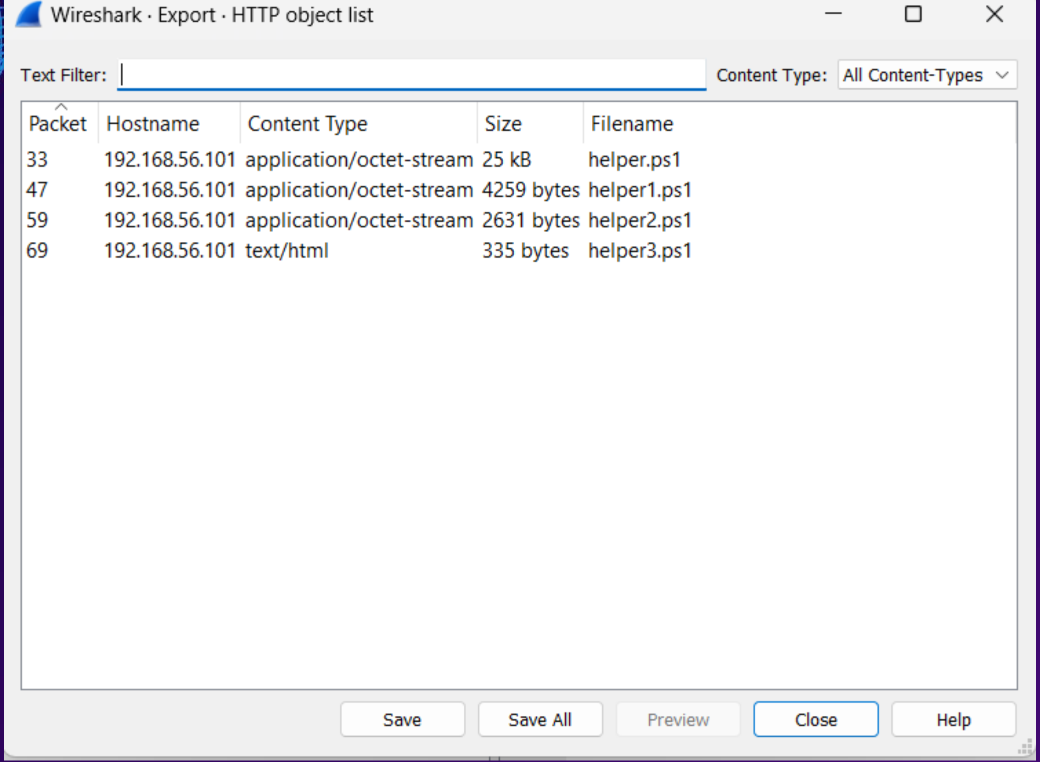
FTP-DATA-> ftp traffic

IMF->smtp traffic(Internet Message Format, .eml extension)

SMB-> smb traffic(Server Message Block)

TFTP-> tftp traffic(Trivial File Transfer Protocol)

Wireshark Basics

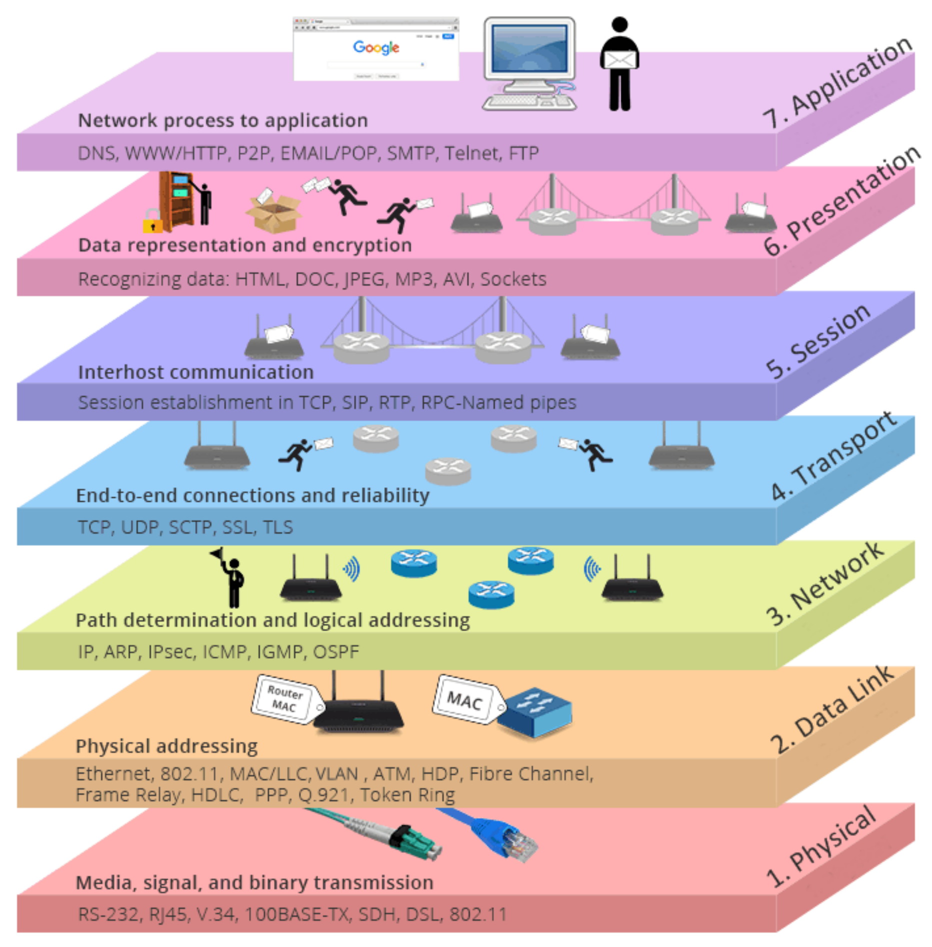


Text Filter:

Content Type: All Content-Types

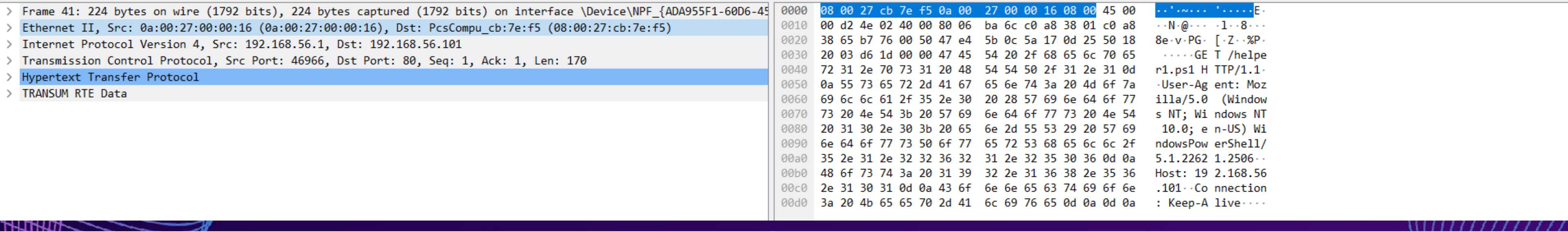
Packet	Hostname	Content Type	Size	Filename
33	192.168.56.101	application/octet-stream	25 kB	helper.ps1
47	192.168.56.101	application/octet-stream	4259 bytes	helper1.ps1
59	192.168.56.101	application/octet-stream	2631 bytes	helper2.ps1
69	192.168.56.101	text/html	335 bytes	helper3.ps1

Wireshark Basics



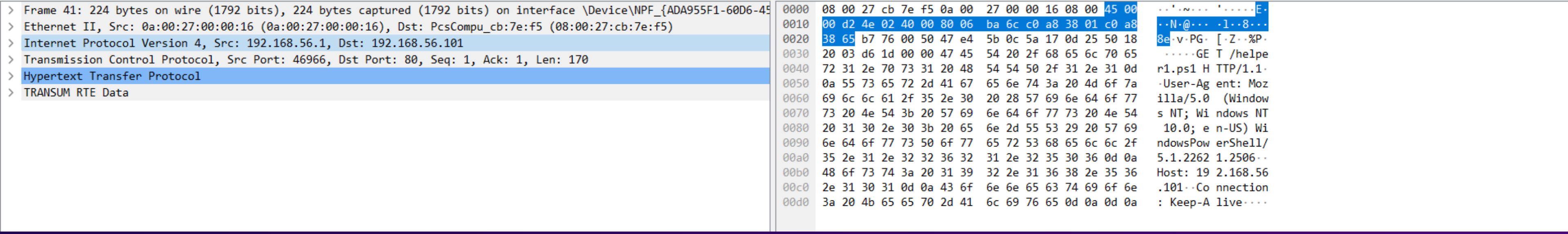
Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Wireshark Basics



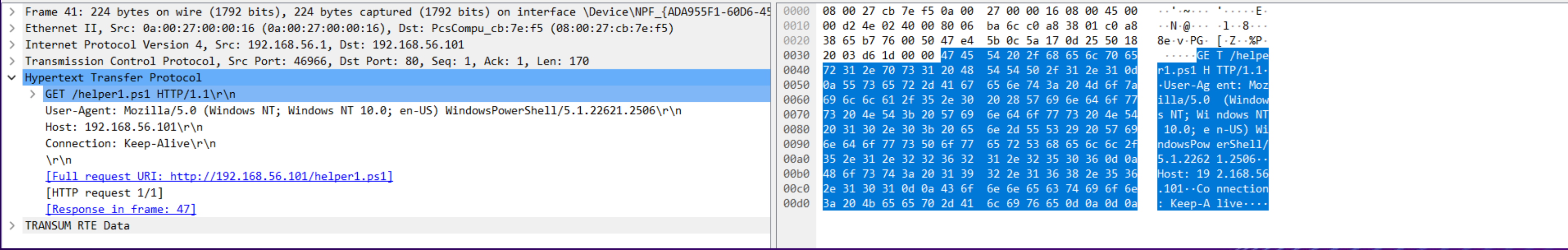
```
> Frame 41: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPF_{ADA955F1-60D6-45
> Ethernet II, Src: 0a:00:27:00:00:16 (0a:00:27:00:00:16), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
> Transmission Control Protocol, Src Port: 46966, Dst Port: 80, Seq: 1, Ack: 1, Len: 170
> Hypertext Transfer Protocol
> TRANSUM RTE Data
```

```
0000  08 00 27 cb 7e f5 0a 00  27 00 00 16 08 00 45 00   ··'·~··· '·····E·
0010  00 d2 4e 02 40 00 80 06  ba 6c c0 a8 38 01 c0 a8   ··N·@··· ·l··8···
0020  38 65 b7 76 00 50 47 e4  5b 0c 5a 17 0d 25 50 18   8e·v·PG· [·Z··%P·
0030  20 03 d6 1d 00 00 47 45  54 20 2f 68 65 6c 70 65    ·····GE T /helpe
0040  72 31 2e 70 73 31 20 48  54 54 50 2f 31 2e 31 0d   r1.ps1 H TTP/1.1·
0050  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0060  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0070  73 20 4e 54 3b 20 57 69  6e 64 6f 77 73 20 4e 54   s NT; Wi ndows NT
0080  20 31 30 2e 30 3b 20 65  6e 2d 55 53 29 20 57 69    10.0; e n-US) Wi
0090  6e 64 6f 77 73 50 6f 77  65 72 53 68 65 6c 6c 2f   ndowsPow erShell/
00a0  35 2e 31 2e 32 32 36 32  31 2e 32 35 30 36 0d 0a   5.1.2262 1.2506··
00b0  48 6f 73 74 3a 20 31 39  32 2e 31 36 38 2e 35 36   Host: 19 2.168.56
00c0  2e 31 30 31 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .101··Co nnection
00d0  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 0d 0a   : Keep-A live····
```



```
> Frame 41: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPF_{ADA955F1-60D6-45
> Ethernet II, Src: 0a:00:27:00:00:16 (0a:00:27:00:00:16), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
> Transmission Control Protocol, Src Port: 46966, Dst Port: 80, Seq: 1, Ack: 1, Len: 170
> Hypertext Transfer Protocol
> TRANSUM RTE Data
```

```
0000  08 00 27 cb 7e f5 0a 00  27 00 00 16 08 00 45 00   ··'·~··· '·····E·
0010  00 d2 4e 02 40 00 80 06  ba 6c c0 a8 38 01 c0 a8   ··N·@··· ·l··8···
0020  38 65 b7 76 00 50 47 e4  5b 0c 5a 17 0d 25 50 18   8e·v·PG· [·Z··%P·
0030  20 03 d6 1d 00 00 47 45  54 20 2f 68 65 6c 70 65    ·····GE T /helpe
0040  72 31 2e 70 73 31 20 48  54 54 50 2f 31 2e 31 0d   r1.ps1 H TTP/1.1·
0050  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0060  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0070  73 20 4e 54 3b 20 57 69  6e 64 6f 77 73 20 4e 54   s NT; Wi ndows NT
0080  20 31 30 2e 30 3b 20 65  6e 2d 55 53 29 20 57 69    10.0; e n-US) Wi
0090  6e 64 6f 77 73 50 6f 77  65 72 53 68 65 6c 6c 2f   ndowsPow erShell/
00a0  35 2e 31 2e 32 32 36 32  31 2e 32 35 30 36 0d 0a   5.1.2262 1.2506··
00b0  48 6f 73 74 3a 20 31 39  32 2e 31 36 38 2e 35 36   Host: 19 2.168.56
00c0  2e 31 30 31 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .101··Co nnection
00d0  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 0d 0a   : Keep-A live····
```



```
> Frame 41: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits) on interface \Device\NPF_{ADA955F1-60D6-45
> Ethernet II, Src: 0a:00:27:00:00:16 (0a:00:27:00:00:16), Dst: PcsCompu_cb:7e:f5 (08:00:27:cb:7e:f5)
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.101
> Transmission Control Protocol, Src Port: 46966, Dst Port: 80, Seq: 1, Ack: 1, Len: 170
v Hypertext Transfer Protocol
  > GET /helper1.ps1 HTTP/1.1\r\n
    User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.22621.2506\r\n
    Host: 192.168.56.101\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://192.168.56.101/helper1.ps1]
    [HTTP request 1/1]
    [Response in frame: 47]
> TRANSUM RTE Data
```

```
0000  08 00 27 cb 7e f5 0a 00  27 00 00 16 08 00 45 00   ··'·~··· '·····E·
0010  00 d2 4e 02 40 00 80 06  ba 6c c0 a8 38 01 c0 a8   ··N·@··· ·l··8···
0020  38 65 b7 76 00 50 47 e4  5b 0c 5a 17 0d 25 50 18   8e·v·PG· [·Z··%P·
0030  20 03 d6 1d 00 00 47 45  54 20 2f 68 65 6c 70 65    ·····GE T /helpe
0040  72 31 2e 70 73 31 20 48  54 54 50 2f 31 2e 31 0d   r1.ps1 H TTP/1.1·
0050  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
0060  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0070  73 20 4e 54 3b 20 57 69  6e 64 6f 77 73 20 4e 54   s NT; Wi ndows NT
0080  20 31 30 2e 30 3b 20 65  6e 2d 55 53 29 20 57 69    10.0; e n-US) Wi
0090  6e 64 6f 77 73 50 6f 77  65 72 53 68 65 6c 6c 2f   ndowsPow erShell/
00a0  35 2e 31 2e 32 32 36 32  31 2e 32 35 30 36 0d 0a   5.1.2262 1.2506··
00b0  48 6f 73 74 3a 20 31 39  32 2e 31 36 38 2e 35 36   Host: 19 2.168.56
00c0  2e 31 30 31 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   .101··Co nnection
00d0  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 0d 0a   : Keep-A live····
```

Useful material:

letsdefend.io
cyberdefenders.org
tryhackme.com->wireshark walkthroughs
hackthebox.com/sherlocks
enterprise.hackthebox -> Academy Lab Main

- Introduction to Networking
- Intro to Network Traffic Analysis

Thank you for your attention!