Network traffic analysis introduction

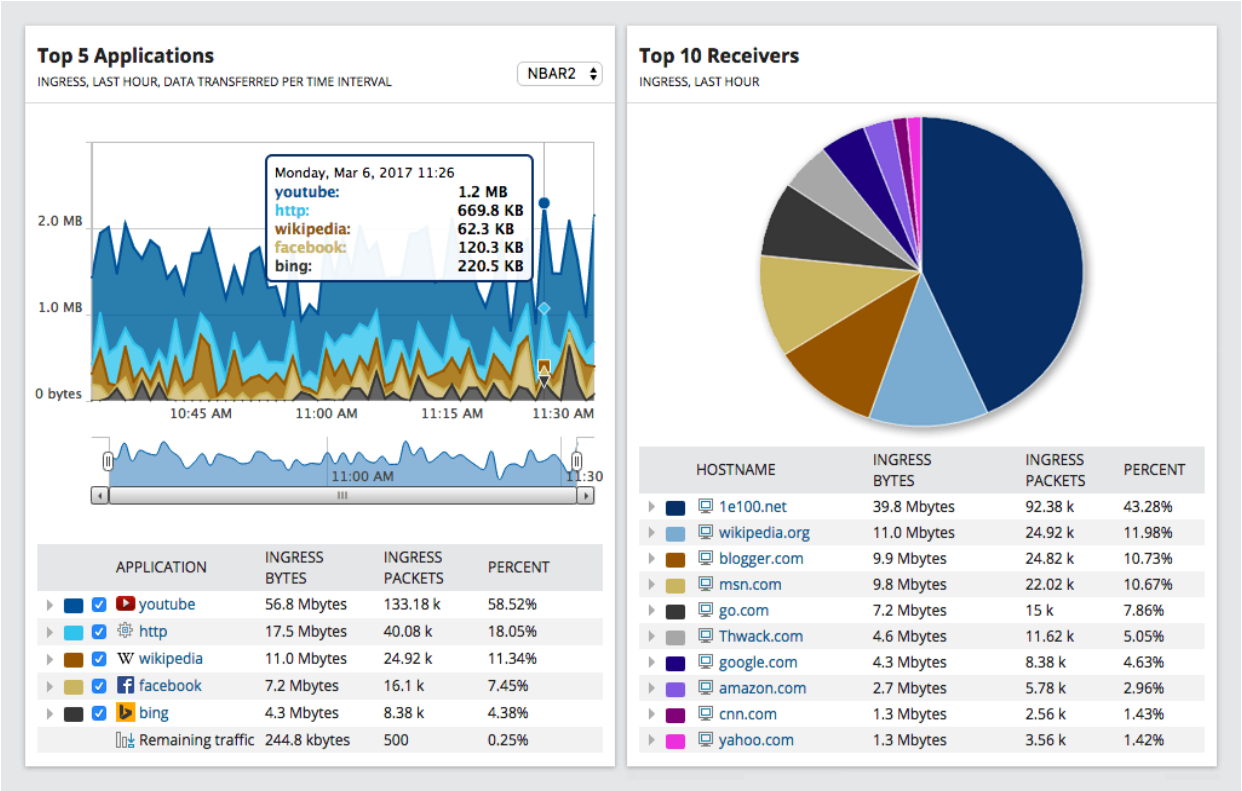
Serhii Zakharchenko

Agenda

- What is Network traffic analysis?
- Wireshark overview
- Traffic analysis samples

What is Network traffic analysis?

- Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.
- Common use cases for NTA include:
  - Collecting a real-time and historical record of what's happening on your network.
  - Detecting malware such as ransomware activity.
  - Modeling complex systems without the need for dedicated equipment.



NTA is a perfect tool for deep learning of computer network protocols and processes

List Of Network Traffic Analysis Tools

Tool name	Platform	Deployment	Free Trial	Price
Auvik	Web-based	Cloud-based	Available	Get a quote for Essentials & Performance plans.
SolarWinds Network Traffic Analysis Tool	Windows	On-premise	Available for 30 days.	It starts at $1036.
Paessler Network Analysis Tool	Windows	On-premises & Cloud-based.	Unlimited version 30 days	It starts at $1750 for 500 sensors. Free version: 100 Sensors
Wireshark	Windows, Mac, Linux, Solaris, etc.	On-premise.	--	Free
NetFort LANGuardian	Linux based OS.	On-premise.	Available for 30 days.	Get a quote.
Manage Engine NetFlow Analyzer	Windows and Linux	On-premise.	Available for 30 days.	Perpetual: It starts at $595. Subscription: It starts at $245.

Who Wireshark use?

Wireshark is a network packet analyzer. It presents captured packet data in as much detail as possible. Here are some reasons people use Wireshark:

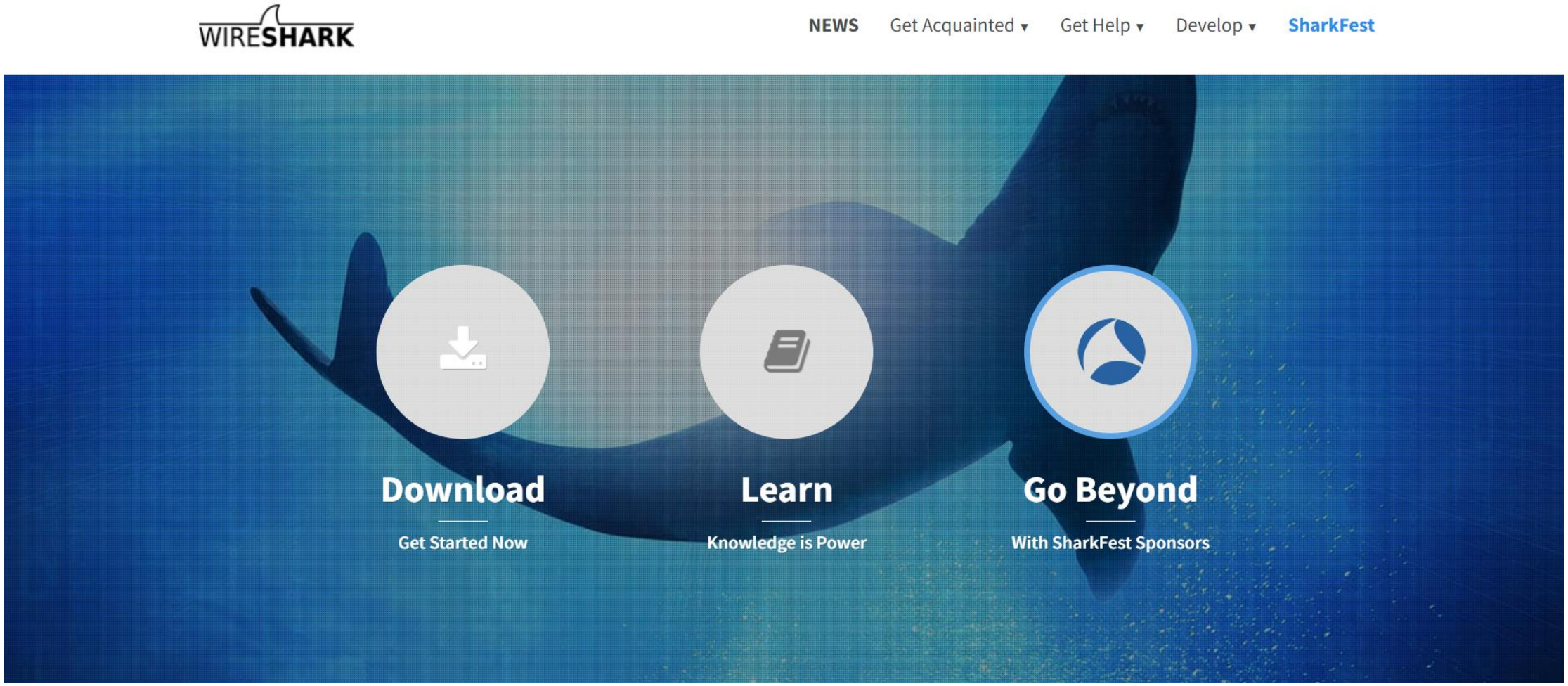
- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to **learn network protocol internals**

Some Wireshark features

- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

Where To Get Wireshark

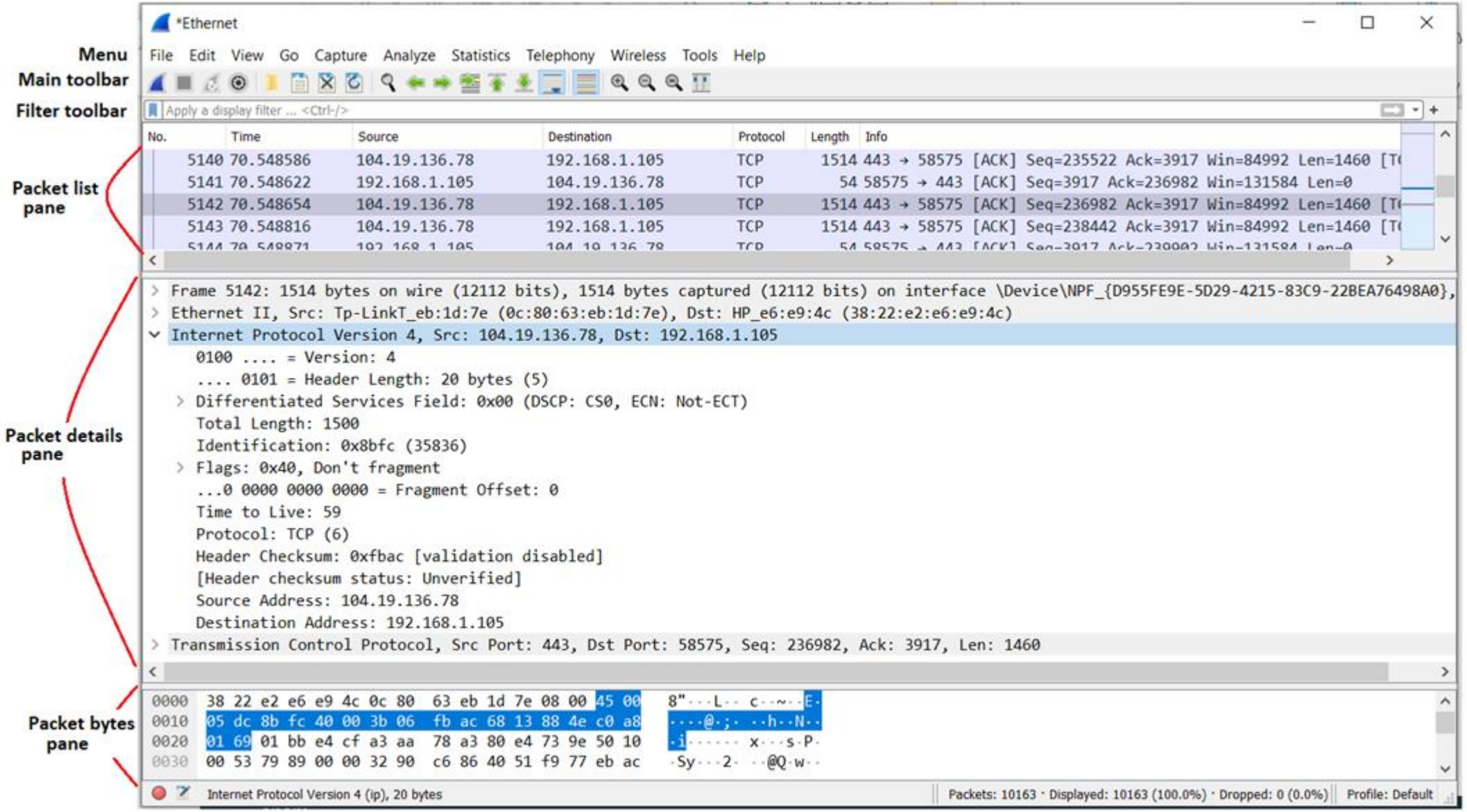
https://www.wireshark.org/



Wireshark main window

- The **menu** is used to start actions.
- The **main toolbar** provides quick access to frequently used items from the menu.
- The **filter toolbar** allows users to set display filters to filter which packets are displayed.
- The **packet list pane** displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.
- The **packet details pane** displays the packet selected in the packet list pane in more detail.
- The **packet bytes pane** displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.

Wireshark main window

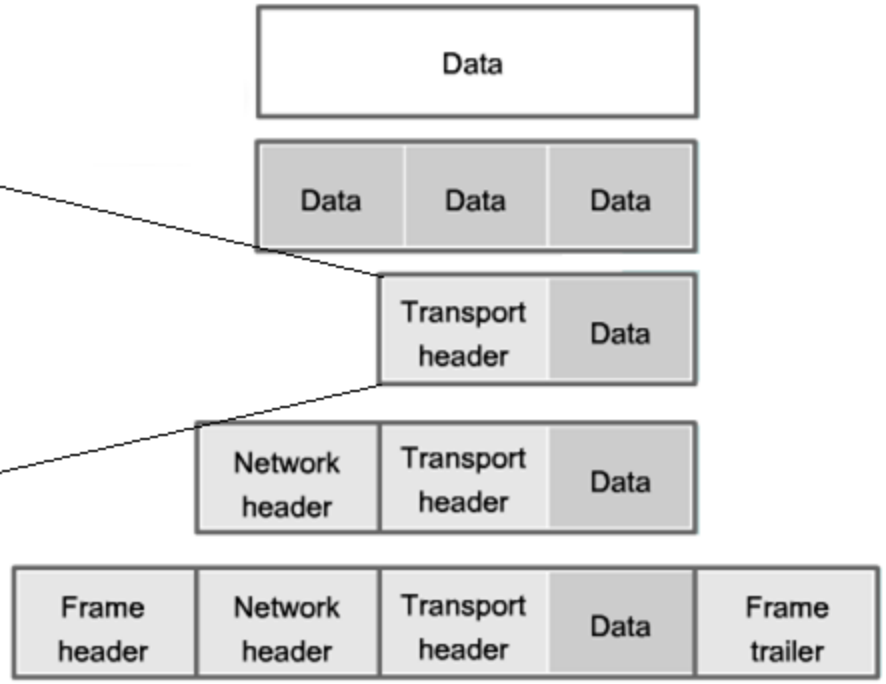


Few simple steps to begin traffic analysis

- Run the Wireshark program
- Choose the network interface for traffic capturing
- Choose and take on traffic capture filter (optional)
- Start traffic capturing
- Wait while the interesting traffic will have captured
- Stop traffic capturing
- Choose or create traffic review filter (optional)
- Find interesting packets
- Make an analysis of interesting packets

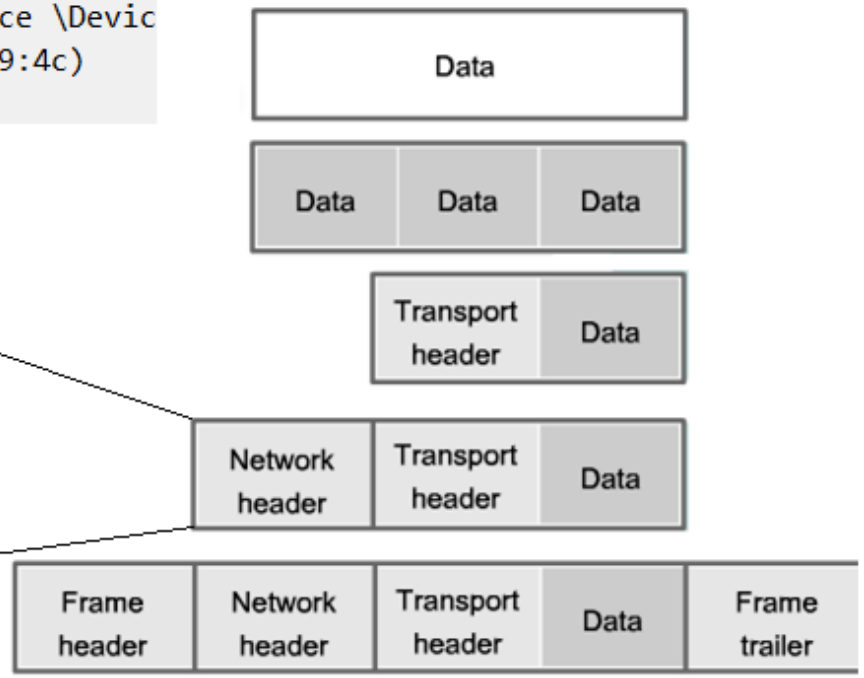
PDU header analysis. Transport layer

```
> Frame 5142: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Devic
> Ethernet II, Src: Tp-LinkT_eb:1d:7e (0c:80:63:eb:1d:7e), Dst: HP_e6:e9:4c (38:22:e2:e6:e9:4c)
> Internet Protocol Version 4, Src: 104.19.136.78, Dst: 192.168.1.105
v Transmission Control Protocol, Src Port: 443, Dst Port: 58575, Seq: 236982, Ack: 3917, Len: 1460
    Source Port: 443
    Destination Port: 58575
    [Stream index: 68]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 1460]
    Sequence Number: 236982    (relative sequence number)
    Sequence Number (raw): 2745858211
    [Next Sequence Number: 238442    (relative sequence number)]
    Acknowledgment Number: 3917    (relative ack number)
    Acknowledgment number (raw): 2162455454
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
    Window: 83
    [Calculated window size: 84992]
    [Window size scaling factor: 1024]
    Checksum: 0x7989 [unverified]
    [Checksum Status: Unverified]
```



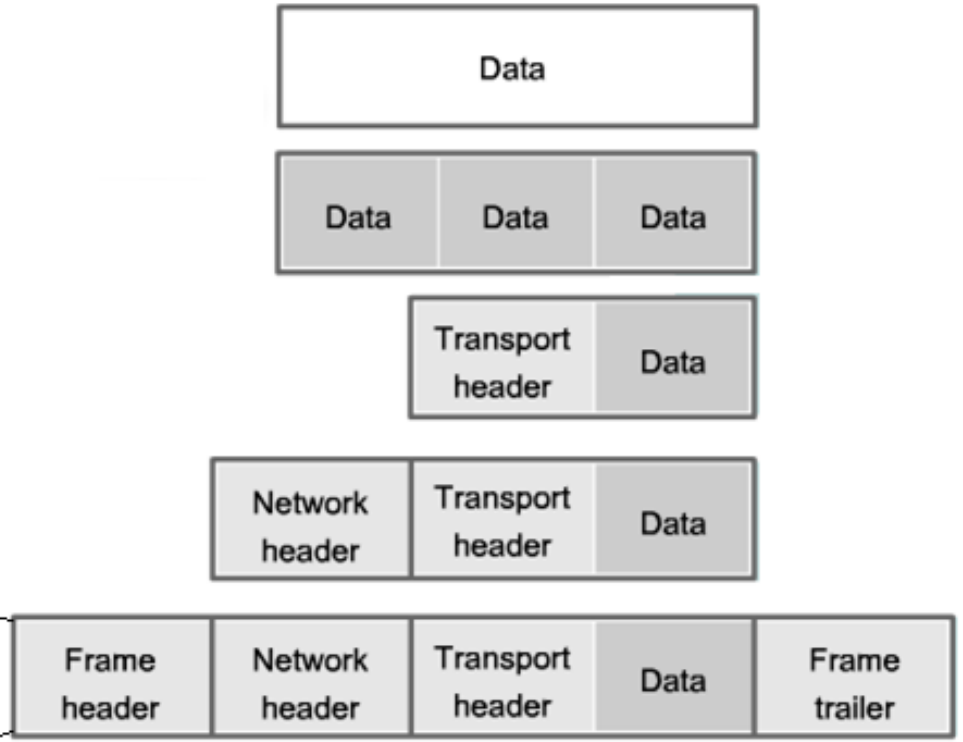
PDU header analysis. Network layer

```
> Frame 5142: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Devic
> Ethernet II, Src: Tp-LinkT_eb:1d:7e (0c:80:63:eb:1d:7e), Dst: HP_e6:e9:4c (38:22:e2:e6:e9:4c)
v Internet Protocol Version 4, Src: 104.19.136.78, Dst: 192.168.1.105
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x8bfc (35836)
  > Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 59
    Protocol: TCP (6)
    Header Checksum: 0xfbac [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 104.19.136.78
    Destination Address: 192.168.1.105
> Transmission Control Protocol, Src Port: 443, Dst Port: 58575, Seq: 236982, Ack: 3917, Len: 1460
```



PDU header analysis. Data link layer

```
> Frame 5142: 1514 bytes on wire (12112 bits), 1514 bytes captured (121
v Ethernet II, Src: Tp-LinkT_eb:1d:7e (0c:80:63:eb:1d:7e), Dst: HP_e6:e
  > Destination: HP_e6:e9:4c (38:22:e2:e6:e9:4c)
  > Source: Tp-LinkT_eb:1d:7e (0c:80:63:eb:1d:7e)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 104.19.136.78, Dst: 192.168.1.105
> Transmission Control Protocol, Src Port: 443, Dst Port: 58575, Seq: 2
```



Filtering Packets While Viewing

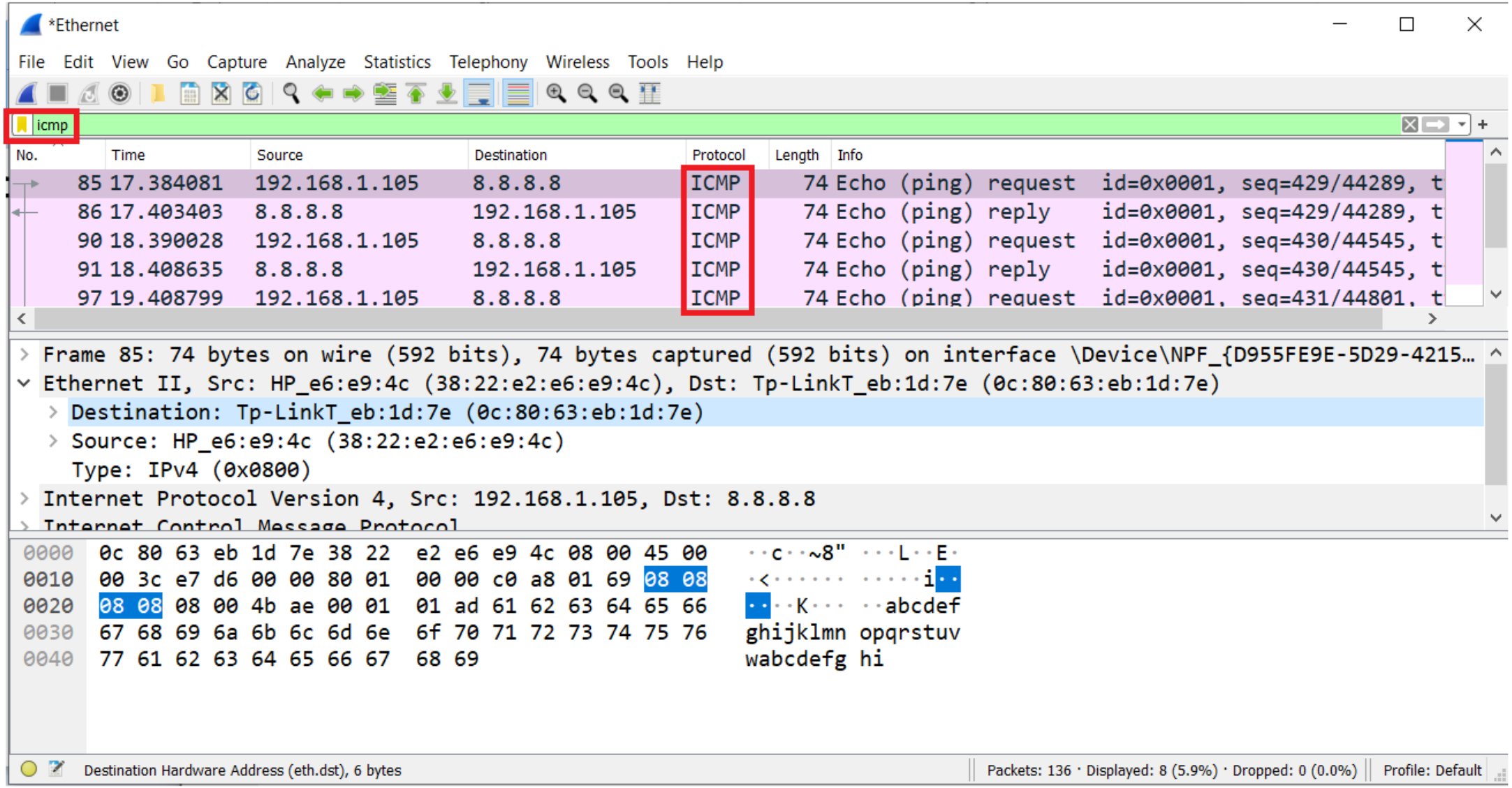
- Wireshark has two filtering languages: **capture** filters and **display** filters.
- Display filters allow you to concentrate on the packets you are interested in while hiding the currently uninteresting ones.
- They allow you to only display packets based on:
  - Protocol
  - The presence of a field
  - The values of fields
  - A comparison between fields
  - … and a lot more!

Analyze/Display Filters

Wireshark · Display Filters

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
No ARP	not arp
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
IPv4 only	ip
IPv4 address 192.0.2.1	ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!)	!(ip.addr == 192.0.2.1)
IPv6 only	ipv6
IPv6 address 2001:db8::1	ipv6.addr == 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	!(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP)	tcp.port == 80 || udp.port == 80
HTTP	http
No ARP and no DNS	not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and tcp.port not in {80, 25}
ICMP	icmp
IPv4 address 209.205.201.34	ip.addr == 209.205.201.34

ICMP Packets Filtering



TCP SYN Segments Filtering

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Length	Info
2	1.396295	192.168.1.105	52.184.217.37	TCP	66	53485 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 …
3	1.514425	52.184.217.37	192.168.1.105	TCP	66	443 → 53485 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1…

```
> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{D955FE9E-5D29-4215-83C9-2
> Ethernet II, Src: HP_e6:e9:4c (38:22:e2:e6:e9:4c), Dst: Tp-LinkT_eb:1d:7e (0c:80:63:eb:1d:7e)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 52.184.217.37
v Transmission Control Protocol, Src Port: 53485, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 53485
    Destination Port: 443
    [Stream index: 1]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 4033459805
```

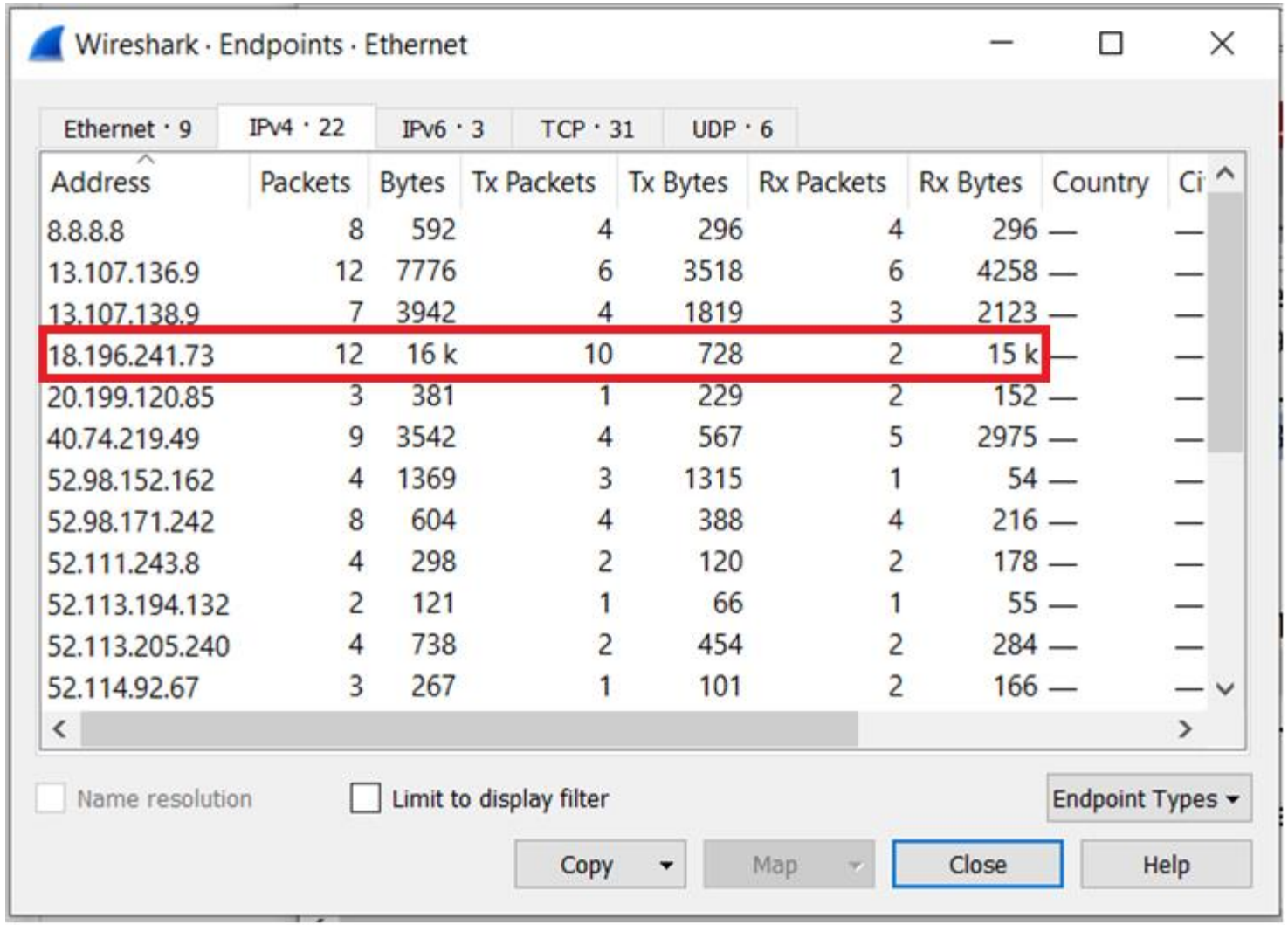
```
0000  0c 80 63 eb 1d 7e 38 22  e2 e6 e9 4c 08 00 45 00   ··c··~8"  ···L··E·
0010  00 34 86 a6 40 00 80 06  00 00 c0 a8 01 69 34 b8   ·4··@···  ·····i4·
0020  d9 25 d0 ed 01 bb f0 69  b6 5d 00 00 00 00 80 02   ·%····i·  ]******
0030  fa f0 d0 15 00 00 02 04  05 b4 01 03 03 08 01 01   ********  ********
0040  04 02                                              ··
```

Destination Port (tcp.dstport), 2 bytes | Packets: 136 · Displayed: 2 (1.5%) · Dropped: 0 (0.0%) | Profile: Default

Statistics

- Wireshark provides a wide range of network statistics which can be accessed via the **Statistics** menu.
- These statistics range from general information about the loaded capture file (like the number of captured packets), to statistics about specific protocols (e.g., statistics about the number of HTTP requests and responses captured).
- General statistics:
    - Capture File Properties about the capture file.
    - Protocol Hierarchy of the captured packets.
    - Conversations e.g., traffic between specific IP addresses.
    - Endpoints e.g., traffic to and from IP addresses.
    - I/O Graphs visualizing the number of packets (or similar) in time

Endpoints Statistics



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	Ci
8.8.8.8	8	592	4	296	4	296	—	—
13.107.136.9	12	7776	6	3518	6	4258	—	—
13.107.138.9	7	3942	4	1819	3	2123	—	—
18.196.241.73	12	16 k	10	728	2	15 k	—	—
20.199.120.85	3	381	1	229	2	152	—	—
40.74.219.49	9	3542	4	567	5	2975	—	—
52.98.152.162	4	1369	3	1315	1	54	—	—
52.98.171.242	8	604	4	388	4	216	—	—
52.111.243.8	4	298	2	120	2	178	—	—
52.113.194.132	2	121	1	66	1	55	—	—
52.113.205.240	4	738	2	454	2	284	—	—
52.114.92.67	3	267	1	101	2	166	—	—

Protocol Hierarchy Statistics

Wireshark · Protocol Hierarchy Statistics · Ethernet

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	136	100.0	52139	12 k	0	0	0
Ethernet	100.0	136	3.7	1904	451	0	0	0
Internet Protocol Version 6	3.7	5	0.4	200	47	0	0	0
User Datagram Protocol	2.2	3	0.0	24	5	0	0	0
Multicast Domain Name System	2.2	3	0.6	330	78	3	330	78
Internet Control Message Protocol v6	1.5	2	0.1	56	13	2	56	13
Internet Protocol Version 4	96.3	131	5.0	2632	624	0	0	0
User Datagram Protocol	21.3	29	0.4	232	55	0	0	0
Simple Service Discovery Protocol	19.1	26	15.3	8000	1897	26	8000	1897
Multicast Domain Name System	2.2	3	0.6	330	78	3	330	78
Transmission Control Protocol	66.9	91	72.7	37921	8995	50	6916	1640
Transport Layer Security	30.1	41	69.1	36026	8545	41	36026	8545
Internet Group Management Protocol	2.2	3	0.0	24	5	3	24	5
Internet Control Message Protocol	5.9	8	0.6	320	75	8	320	75

No display filter.

Close | Copy | Help