

WIRESHARK

CPSC 441 - Tutorial 5

Winter 2018

WHAT IS **WIRESHARK**?

- **Wireshark** is a free and open source packet analyzer
- It is used for network troubleshooting, analysis, software and communication protocol development, and education.
- Originally named **Ethereal**, the project was renamed Wireshark in May 2006 due to trademark issues

FUNCTIONALITY

- Wireshark is very similar to tcpdump, but has a graphical front-end, and some integrated sorting and filtering options
- Data can be captured from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal version of the utility, TShark
- Data display can be refined using a display filter
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic

INSTALLATION

- Download Wireshark:

<http://www.wireshark.org/download.html>

Choose the appropriate version according to your operating system
For Windows, during the installation, agree to install WinPcap

- There is a good tutorial on how to capture data using WireShark:

<http://wiki.wireshark.org/CaptureSetup>

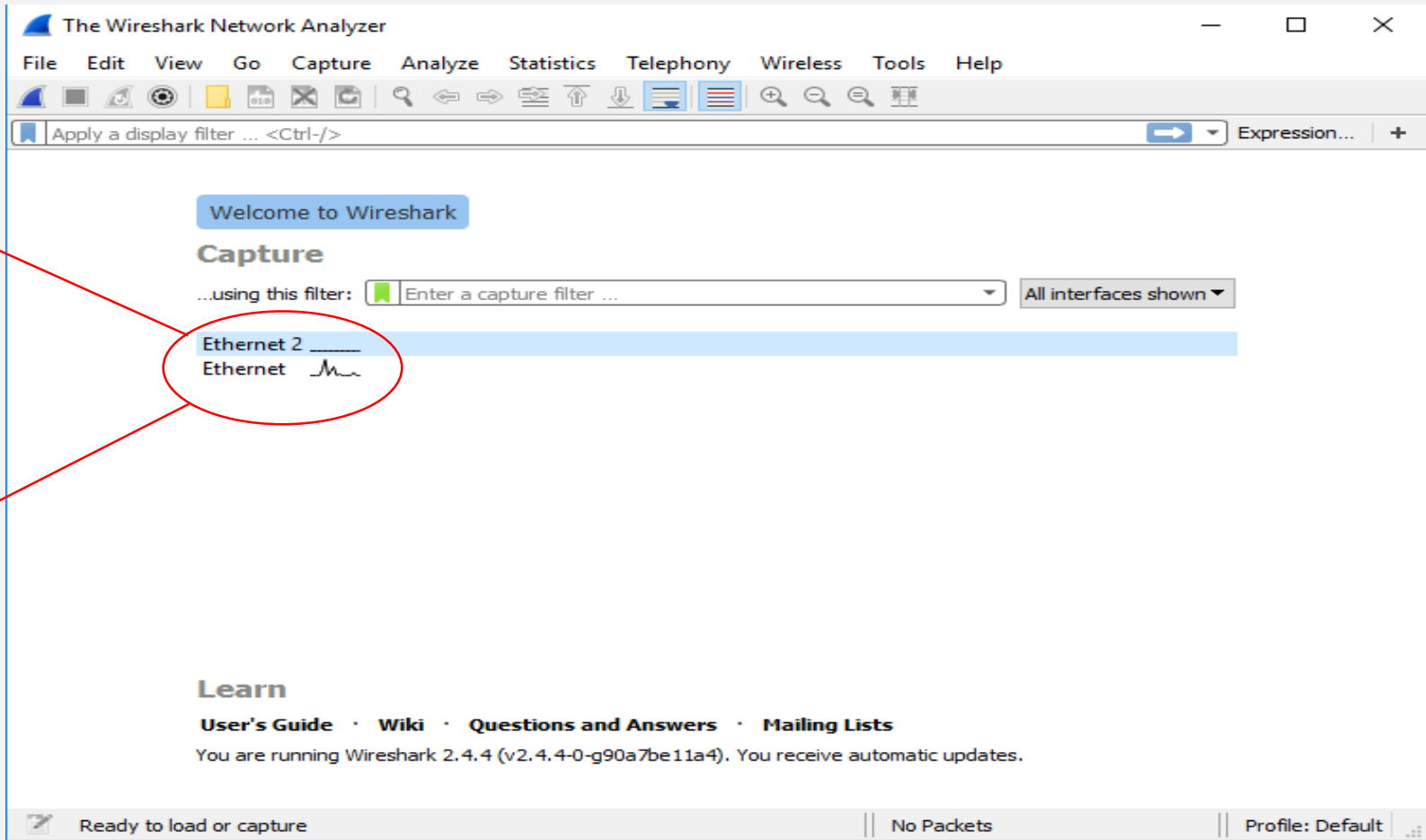
BEFORE CAPTURING

- Are you allowed to do this?
 - Ensure that you have permission to capture packets from the network you are connected with
 - Corporate policies or applicable laws may prohibit capturing data from the network
- General Setup
 - Operating system must support packet capturing, e.g. capture support is enabled
 - You must have sufficient privileges to capture packets, e.g. root / administrator privileges
 - Your computer's time and time zone settings should be correct



Available
Interfaces

Choose
the one
with traffic



START CAPTURING PACKETS

- After clicking on desired interface, Wireshark starts capturing packets

The screenshot displays the Wireshark interface with the 'Capturing from Ethernet' window open. The interface shows a list of captured packets and a detailed view of the first packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...
2	0.634647	172.17.14.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	0.682666	fe80::b583:39c3:e4f...	ff02::1:2	DHCPv6	165	Solicit XID: 0xd92aa6 C...
4	0.749053	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...
5	0.826584	172.17.14.47	172.17.12.110	SMB2	126	Tree Disconnect Request
6	0.826942	172.17.12.110	172.17.14.47	SMB2	126	Tree Disconnect Response
7	0.873383	172.17.14.47	172.17.12.110	TCP	54	56034 → 445 [ACK] Seq=7...

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
> Ethernet II, Src: Dell_7c:76:6a (00:26:b9:7c:76:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.17.14.28, Dst: 172.17.14.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service

```
0000  ff ff ff ff ff ff 00 26 b9 7c 76 6a 08 00 45 00  .....& .|vj..E.
0010  00 4e 53 0a 00 00 80 11 72 57 ac 11 0e 1c ac 11  .NS....rw.....
0020  0e ff 00 89 00 89 00 3a db 78 df 32 01 10 00 01  .....: .x.2....
0030  00 00 00 00 00 00 20 45 4d 45 50 45 48 45 4a 45  ..... E MEPEHEJE
0040  4f 45 46 45 4f 43 4f 44 48 46 41 45 4c 43 4f 45  OEFEOCOD HFAELCOE
0050  44 45 50 45 4e 41 41 00 00 20 00 01             DEPENAA. . .
```

Ethernet: <live capture in progress> | Packets: 30 · Displayed: 30 (100.0%) | Profile: Default

ANALYZE CAPTURED PACKETS

Time of capturing packet Source IP Destination IP Short description of packet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...
2	0.634647	172.17.14.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	0.682666	fe80::b583:39c3:e4f...	ff02::1:2	DHCPv6	165	Solicit XID: 0xd92aa6 C...
4	0.749053	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...
5	0.826584	172.17.14.47	172.17.12.110	SMB2	126	Tree Disconnect Request
6	0.826942	172.17.12.110	172.17.14.47	SMB2	126	Tree Disconnect Response
7	0.873383	172.17.14.47	172.17.12.110	TCP	54	56034 → 445 [ACK] Seq=7...
8	1.408862	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...

ANALYZE CAPTURED PACKETS

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...
2	0.634647	172.17.14.104	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	0.682666	fe80::b583:39c3:e4f...	ff02::1:2	DHCPv6	165	Solicit XID: 0xd92aa6 C...
4	0.749053	172.17.14.28	172.17.14.255	NBNS	92	Name query NB LOGINEN.7...
5	0.826584	172.17.14.47	172.17.12.110	SMB2	126	Tree Disconnect Request
6	0.826942	172.17.12.110	172.17.14.47	SMB2	126	Tree Disconnect Response
7	0.873383	172.17.14.47	172.17.12.110	TCP	54	56034 → 445 [ACK] Seq=7...

> Frame 7: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: Dell_dc:22:2d (34:17:eb:dc:22:2d), Dst: HewlettP_9d:62:00 (58:20:b1:9d:62:00)
> Internet Protocol Version 4, Src: 172.17.14.47, Dst: 172.17.12.110
> Transmission Control Protocol, Src Port: 56034, Dst Port: 445, Seq: 73, Ack: 73, Len: 0

Hierarchical View:

Frame
↓
Ethernet
↓
IP
↓
TCP

ANALYZE A HTTP REQUEST

The image shows a Wireshark window titled "*Ethernet" with a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The packet list pane shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
1088	63.398488	172.17.14.47	23.41.241.37	HTTP	894	GET /rd?cid=26xu0nx0k0&mkwid=sJiiJZmdk pcrid 237425676401 pmt e pkw...
1095	63.489927	23.41.241.37	172.17.14.47	HTTP	660	HTTP/1.1 302 Moved Temporarily
1108	63.600914	172.17.14.47	23.41.182.175	HTTP	721	GET /free-tools/response-time-viewer-for-wireshark?&CMP=KNC-TAD-GGL...

The packet details pane for packet 1088 shows the following structure:

- Frame 1088: 894 bytes on wire (7152 bits), 894 bytes captured (7152 bits) on interface 0
- Ethernet II, Src: Dell_dc:22:2d (34:17:eb:dc:22:2d), Dst: HewlettP_9d:62:00 (58:20:b1:9d:62:00)
- Internet Protocol Version 4, Src: 172.17.14.47, Dst: 23.41.241.37
- Transmission Control Protocol, Src Port: 64517, Dst Port: 80, Seq: 1, Ack: 1, Len: 840
- Hypertext Transfer Protocol
 - [truncated]GET /rd?cid=26xu0nx0k0&mkwid=sJiiJZmdk|pcrid|237425676401|pmt|e|pkw|wireshark|pdv|c&lp=http://www.solarwinds.com/free-tools/response-time
 - Host: tracker.marinsm.com\r\n
 - Connection: keep-alive\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - X-Chrome-UMA-Enabled: 1\r\n
 - X-Client-Data: CI62yQEIorbJAQjBtsk0CPqcygEIqZ3KAQioo8oB\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
 - Referer: https://www.google.ca/\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Language: en-US,en;q=0.9\r\n
 - Cookie: _msuuid=3bb431e5-64db-4b92-bc06-401f044688f8\r\n
 - \r\n
 - [Full request URI [truncated]: http://tracker.marinsm.com/rd?cid=26xu0nx0k0&mkwid=sJiiJZmdk|pcrid|237425676401|pmt|e|pkw|wireshark|pdv|c&lp=http://ww
 - [HTTP request 1/1]
 - [Response in frame: 1095]

The packet bytes pane shows the hex and ASCII representation of the first few bytes: 58 20 b1 9d 62 00 34 17 eb dc 22 2d 08 00 45 00 X ..b.4. .."-..E.

The status bar at the bottom indicates: wireshark_66DE2EF5-C836-4C02-A87F-7E165AAD13F6_20180127192634_a02608 | Packets: 3579 · Displayed: 4 (0.1%) | Profile: Default

PACKETS WITH STRANGE PROTOCOLS

QUIC:
Quick UDP
Internet
Connections

The image shows a Wireshark network traffic capture window titled "*Ethernet". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A display filter is set to "Apply a display filter ... <Ctrl-/>". The main pane displays a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets are color-coded: green for TCP, blue for HTTP, purple for DNS, and light blue for QUIC. Packet 1088 is highlighted in blue and selected. Below the packet list, the packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows a truncated GET request to tracker.marinsm.com. At the bottom, the packet bytes pane shows the hexadecimal and ASCII representation of the selected packet's data.

No.	Time	Source	Destination	Protocol	Length	Info
1087	63.398345	172.17.14.47	23.41.241.37	TCP	54	64516 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
1088	63.398488	172.17.14.47	23.41.241.37	HTTP	894	GET /rd?cid=26xu0nx0k0&mkwid=sJiiJZmdk pcrid 237425676401 pmt e pkw...
1089	63.399392	23.41.241.37	172.17.14.47	TCP	60	80 → 64517 [ACK] Seq=1 Ack=841 Win=934400 Len=0
1090	63.405220	172.217.3.174	172.17.14.47	QUIC	1392	Payload (Encrypted), PKN: 4
1091	63.406225	172.217.3.174	172.17.14.47	QUIC	1392	Payload (Encrypted), PKN: 4
1092	63.424535	HewlettP_57:40:38		LLDP_Multicast	LLDP	256 TTL = 120 System Name = elisalab System Description = HP J9728A 292...
1093	63.436432	23.41.241.37	172.17.14.47	TCP	60	[TCP Window Update] 80 → 64517 [ACK] Seq=1 Ack=841 Win=30880 Len=0
1094	63.458902	136.159.5.76	172.17.14.47	DNS	491	Standard query response 0xa23a A tracker.marinsm.com CNAME tracker...
1095	63.489927	23.41.241.37	172.17.14.47	HTTP	660	HTTP/1.1 302 Moved Temporarily
1096	63.491399	172.17.14.47	136.159.5.75	DNS	78	Standard query 0x27bf A www.solarwinds.com
1097	63.493344	172.217.3.174	172.17.14.47	QUIC	1392	Payload (Encrypted), PKN: 5
1098	63.493791	172.217.3.174	172.17.14.47	QUIC	1392	Payload (Encrypted), PKN: 5
1099	63.515865	172.17.14.47	136.159.5.76	DNS	78	Standard query 0x27bf A www.solarwinds.com
1100	63.529570	172.17.14.47	23.41.241.37	TCP	54	64517 → 80 [ACK] Seq=841 Ack=607 Win=65024 Len=0
1101	63.577772	136.159.5.75	172.17.14.47	DNS	489	Standard query response 0x27bf A www.solarwinds.com CNAME www.solar...
1102	63.578191	172.17.14.47	23.41.182.175	TCP	66	64518 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1103	63.578271	172.17.14.47	23.41.182.175	TCP	66	64519 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1104	63.600658	23.41.182.175	172.17.14.47	TCP	66	80 → 64518 [SYN, ACK] Seq=0 Ack=1 Win=28700 Len=0 MSS=1460 SACK_PER...

> Frame 1088: 894 bytes on wire (7152 bits), 894 bytes captured (7152 bits) on interface 0
> Ethernet II, Src: Dell_dc:22:2d (34:17:eb:dc:22:2d), Dst: HewlettP_9d:62:00 (58:20:b1:9d:62:00)
> Internet Protocol Version 4, Src: 172.17.14.47, Dst: 23.41.241.37
> Transmission Control Protocol, Src Port: 64517, Dst Port: 80, Seq: 1, Ack: 1, Len: 840
v Hypertext Transfer Protocol
> [truncated]GET /rd?cid=26xu0nx0k0&mkwid=sJiiJZmdk|pcrid|237425676401|pmt|e|pkw|wireshark|pdv|c&lp=http://www.solarwinds.com/free-tools/response-ti
Host: tracker.marinsm.com\r\n

0000 58 20 b1 9d 62 00 34 17 eb dc 22 2d 08 00 45 00 X..b.4. ."-..E.

Frame (frame), 894 bytes | Packets: 3579 · Displayed: 3579 (100.0%) · Dropped: 0 (0.0%) | Profile: Default



WIRESHARK FILTERS

- Wireshark has two types of filters:
 - Capture Filters
 - A powerful capture filter engine helps **remove unwanted packets** from a packet trace and only retrieve the packets of interest
 - Display Filters
 - Let you compare the fields within a protocol against a specific value, compare fields against other fields, and check the existence of specified fields or protocols

CAPTURE FILTER

The screenshot displays the Wireshark application window. The 'Capture' menu is circled in red. A dialog box titled 'Wireshark · Capture Interfaces' is open, showing a table of interfaces. The 'Ethernet' interface is selected and circled in red. Below the table, the 'Capture filter for selected interfaces' field contains the text 'tcp port http', which is also circled in red. The 'Start' button is highlighted in blue.

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor Mode	Capture Filter
Ethernet 2		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Ethernet		Ethernet	<input checked="" type="checkbox"/>	default	2	—	tcp port http

0000 ff ff ff ff ff ff 48 4d 7e b9 ff 16 08 00 45 00HM ~.....E.

wireshark_66DE2EF5-C836-4C02-A87F-7E165AAD13F6_20180127194746_a12208 | Packets: 977 · Displayed: 977 (100.0%) | Profile: Default

DISPLAY FILTER

The screenshot shows the Wireshark network protocol analyzer interface. The title bar reads "Capturing from Ethernet". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The display filter bar, located below the toolbar, contains the text "Apply a display filter ... <Ctrl-/>" and is circled in red. Below the filter bar is a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The table lists 10 packets, with packet 8 highlighted in black. Below the table, the packet details pane shows the structure of the first packet: Frame 1 (164 bytes on wire, 164 bytes captured on interface 0), Ethernet II (Src: Giga-Byt_c9:56:ec, Dst: IPv6mcast_01:00:02), Internet Protocol Version 6 (Src: fe80::2dc2:788d:2692:9e92, Dst: ff02::1:2), and User Datagram Protocol (Src Port: 546, Dst Port: 547). At the bottom, the packet bytes pane shows the hexadecimal and ASCII representation of the packet data.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::2dc2:788d:269...	ff02::1:2	DHCPv6	164	Solicit XID: 0xfbd802 CID: 000...
2	0.112554	172.17.14.47	74.125.28.188	TCP	55	60614 → 5228 [ACK] Seq=1 Ack=1...
3	0.134008	74.125.28.188	172.17.14.47	TCP	66	5228 → 60614 [ACK] Seq=1 Ack=2...
4	0.235534	172.17.14.101	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	0.832111	fe80::882f:c0d9:772...	ff02::1:2	DHCPv6	166	Solicit XID: 0x391248 CID: 000...
6	0.870912	172.17.14.47	172.17.12.110	NBSS	55	NBSS Continuation Message
7	0.871066	172.17.12.110	172.17.14.47	TCP	66	445 → 56034 [ACK] Seq=1 Ack=2 ...
8	0.895289	172.17.12.110	172.17.14.47	TCP	60	[TCP Keep-Alive] 445 → 56034 [...]
9	0.895315	172.17.14.47	172.17.12.110	TCP	66	[TCP Keep-Alive ACK] 56034 → 4...
10	2.003038	fe80::2dc2:788d:269...	ff02::1:2	DHCPv6	164	Solicit XID: 0xfbd802 CID: 000...

Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
Ethernet II, Src: Giga-Byt_c9:56:ec (50:e5:49:c9:56:ec), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
Internet Protocol Version 6, Src: fe80::2dc2:788d:2692:9e92, Dst: ff02::1:2
User Datagram Protocol, Src Port: 546, Dst Port: 547

0000 33 33 00 01 00 02 50 e5 49 c9 56 ec 86 dd 60 00 33...P. I.V...`
0010 00 00 00 6e 11 01 fe 80 00 00 00 00 00 00 2d c2 ...n...

Frame (frame), 164 bytes | Packets: 282 · Displayed: 282 (100.0%) | Profile: Default

DISPLAY FILTER EXAMPLE

The image shows the Wireshark network protocol analyzer interface. The display filter is set to `tcp.port == 80 || udp.port == 80`, which is highlighted with a red oval. The packet list pane shows several packets, with the first one (No. 3786) selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

`tcp.port == 80 || udp.port == 80` Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
3786	124.288732	172.17.14.47	34.204.112.229	TCP	66	64679 → 80 [SYN] Seq=0 Win=642...
3867	124.346886	34.204.112.229	172.17.14.47	TCP	66	80 → 64679 [SYN, ACK] Seq=0 Ac...
3869	124.346930	172.17.14.47	34.204.112.229	TCP	54	64679 → 80 [ACK] Seq=1 Ack=1 W...
3870	124.347015	172.17.14.47	34.204.112.229	HTTP	954	GET /master/?1=1&HASH=83ec&RED...
3872	124.347860	34.204.112.229	172.17.14.47	TCP	60	80 → 64679 [ACK] Seq=1 Ack=901...
4020	124.419284	34.204.112.229	172.17.14.47	TCP	60	[TCP Window Update] 80 → 64679...
4021	124.420773	34.204.112.229	172.17.14.47	HTTP	1169	HTTP/1.1 302 Found
4113	124.460181	172.17.14.47	54.85.54.13	TCP	66	64693 → 80 [SYN] Seq=0 Win=642...
4117	124.461311	172.17.14.47	34.204.112.229	TCP	54	64679 → 80 [ACK] Seq=901 Ack=1...
4258	124.523126	54.85.54.13	172.17.14.47	TCP	66	80 → 64693 [SYN, ACK] Seq=0 Ac...

> Frame 3786: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: Dell_dc:22:2d (34:17:eb:dc:22:2d), Dst: HewlettP_9d:62:00 (58:20:b1:9d:62:00)

> Internet Protocol Version 4, Src: 172.17.14.47, Dst: 34.204.112.229

> Transmission Control Protocol, Src Port: 64679, Dst Port: 80, Seq: 0, Len: 0

0000 58 20 b1 9d 62 00 34 17 eb dc 22 2d 08 00 45 00 X ..b.4. .."-..E.

0010 00 34 36 ba 40 00 80 06 00 00 ac 11 0e 2f 22 cc .46.@.../".

Frame (frame), 66 bytes | Packets: 10289 · Displayed: 16 (0.2%) | Profile: Default

FILTERS: COMPARISON OPERATORS AND LOGICAL EXPRESSIONS

The comparison operators can be expressed either through English-like abbreviations or through C-like symbols:

- eq, == Equal
- ne, != Not Equal
- gt, > Greater Than
- lt, < Less Than
- ge, >= Greater than or Equal to
- le, <= Less than or Equal to

Logical:

- and, && Logical AND
- or, || Logical OR
- not, ! Logical NOT

In display Filter:

- `tcp.port == 80` (`tcp.port eq 80`)
- `eth.addr == 00:00:5e:00:53:00`
- `tcp.port == 80 || udp.port == 80`
- `tcp.port == 80 && ip.src == 172.17.14.47`
- `http.request.version=="HTTP/1.1"`
- `tcp.dstport == 25`

In capture filter:

- `tcp port 80`
- `ip src host 136.159.5.20`
- `host 136.159.5.1`
(source/destination)
- `(src host 23.36.178.81 and not dst host 172.17.14.47) and tcp dst portrange 200-10000`

FILTERS: SLICE OPERATOR

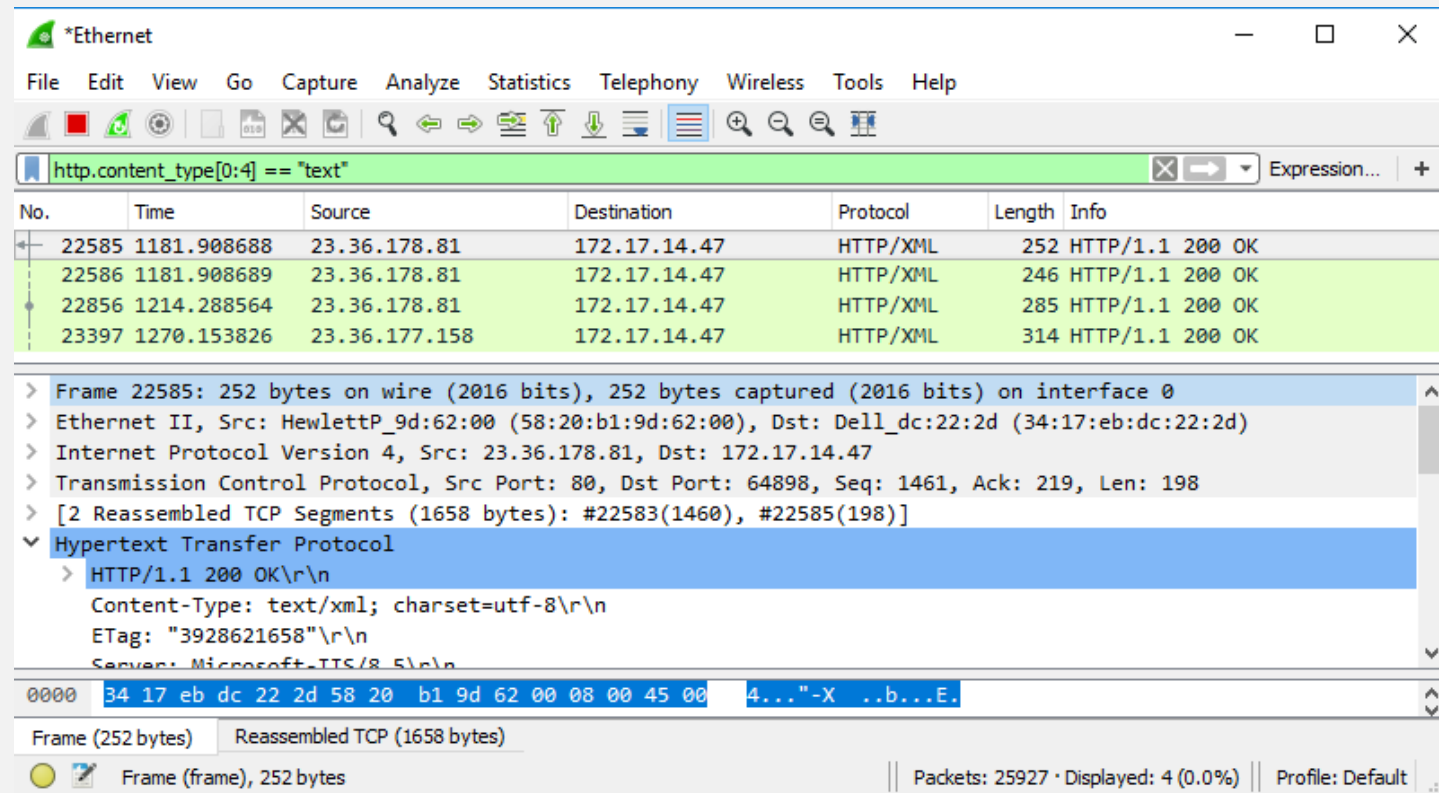
- You can take a slice of a field if the field is a text string or a byte array

For example, you can filter the HTTP header fields with the header “location” which indicates that redirection happens:

```
http.location[0:12]=  
="http://pages"
```

Another example:

```
http.content_type[0:4]  
=="text"
```



The screenshot shows the Wireshark interface with the filter `http.content_type[0:4] == "text"` applied. The packet list shows four HTTP/XML packets. The details pane for the selected packet (No. 22585) shows the following structure:

- Frame 22585: 252 bytes on wire (2016 bits), 252 bytes captured (2016 bits) on interface 0
- Ethernet II, Src: HewlettP_9d:62:00 (58:20:b1:9d:62:00), Dst: Dell_dc:22:2d (34:17:eb:dc:22:2d)
- Internet Protocol Version 4, Src: 23.36.178.81, Dst: 172.17.14.47
- Transmission Control Protocol, Src Port: 80, Dst Port: 64898, Seq: 1461, Ack: 219, Len: 198
- [2 Reassembled TCP Segments (1658 bytes): #22583(1460), #22585(198)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Content-Type: text/xml; charset=utf-8\r\n
 - ETag: "3928621658"\r\n
 - Server: Microsoft-IIS/8.5\r\n

The packet bytes pane shows the raw data: `0000 34 17 eb dc 22 2d 58 20 b1 9d 62 00 08 00 45 00 4...-X ..b...E.`

REFERENCES

- <https://en.wikipedia.org/wiki/Wireshark>
- <https://wiki.wireshark.org/>
- <https://www.wireshark.org/>