

Wireshark

CPSC 441 - TUTORIAL 4

RACHEL MCLEAN

WINTER 2020

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

Sources of data:

- Live network connection
- File of already-captured trace

Different types of live networks, including :

- Ethernet (LAN)
- IEEE 802.11 (WLAN)
- loopback

Redefining displayed data with 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

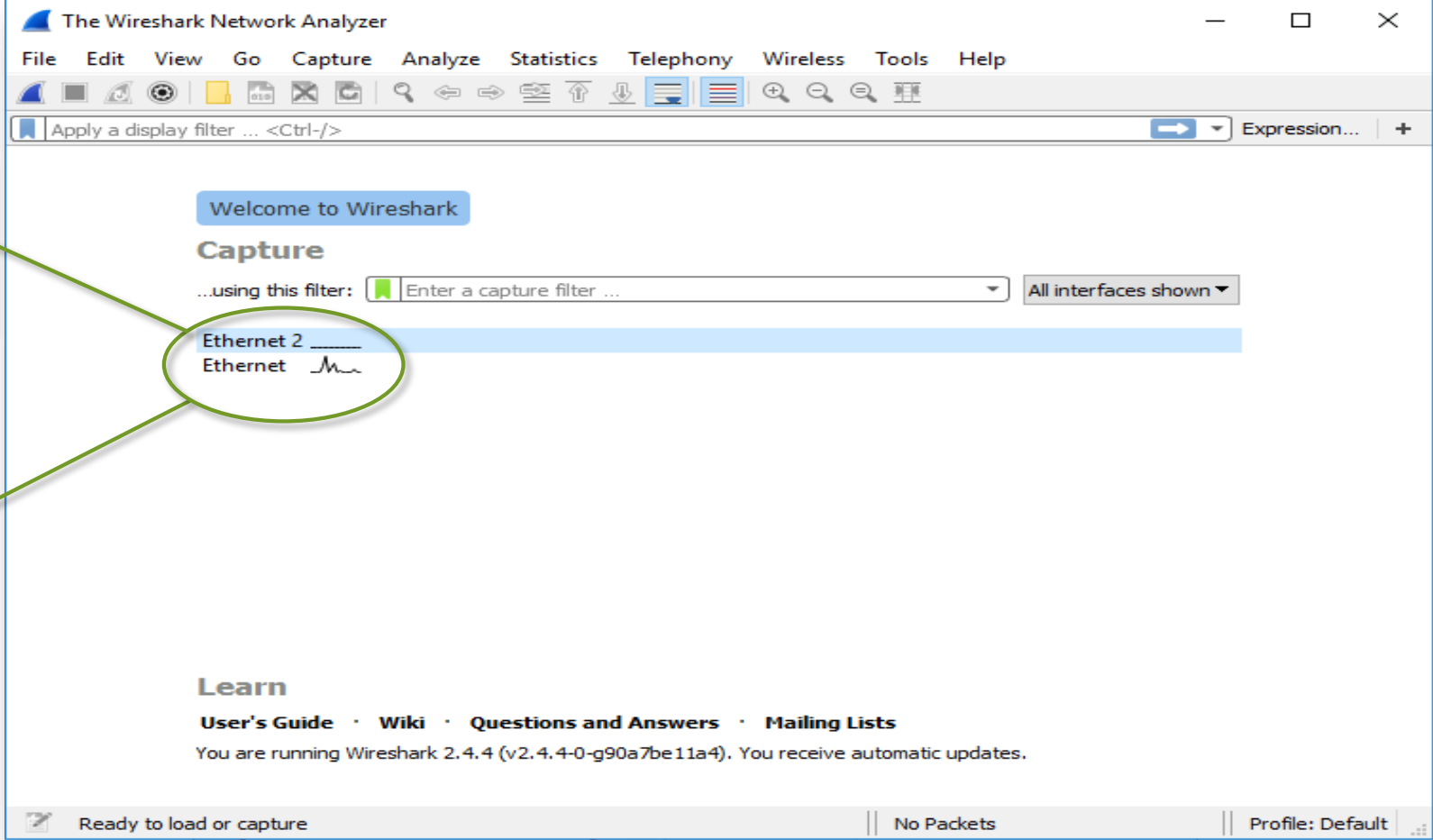
Are you allowed to do this?

- 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

Choosing network interface



The screenshot shows the Wireshark Network Analyzer interface. The 'Capture' section is active, displaying a list of available network interfaces. The interface 'Ethernet 2' is highlighted with a blue bar. A green oval highlights the 'Ethernet 2' entry, with a line pointing to a green box labeled 'Choose the one with traffic'. Another green box labeled 'Available Interfaces' has a line pointing to the list of interfaces.

Available Interfaces

Choose the one with traffic

Welcome to Wireshark

Capture

...using this filter: All interfaces shown

Ethernet 2
Ethernet

Learn

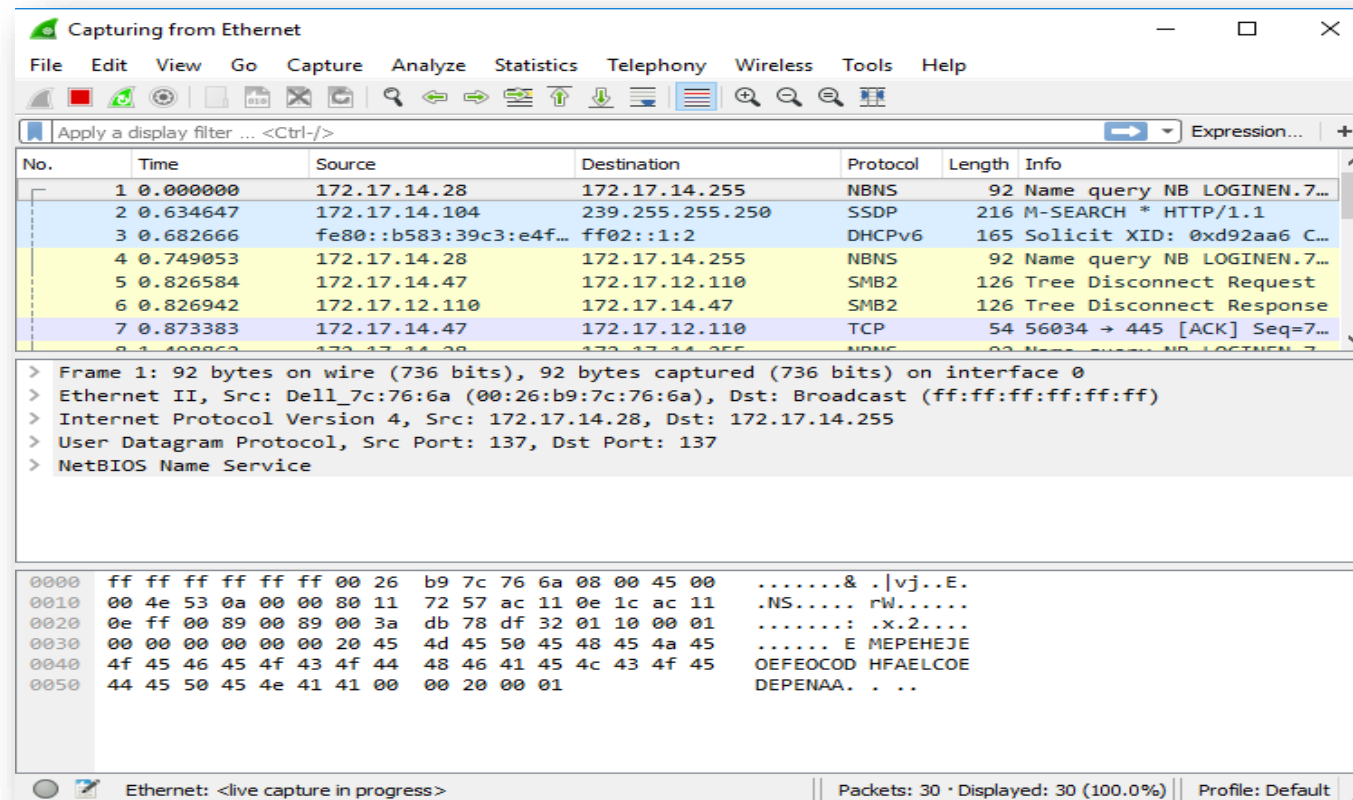
[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

You are running Wireshark 2.4.4 (v2.4.4-0-g90a7be11a4). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Start capturing packets

After clicking on desired interface, Wireshark starts capturing packets



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

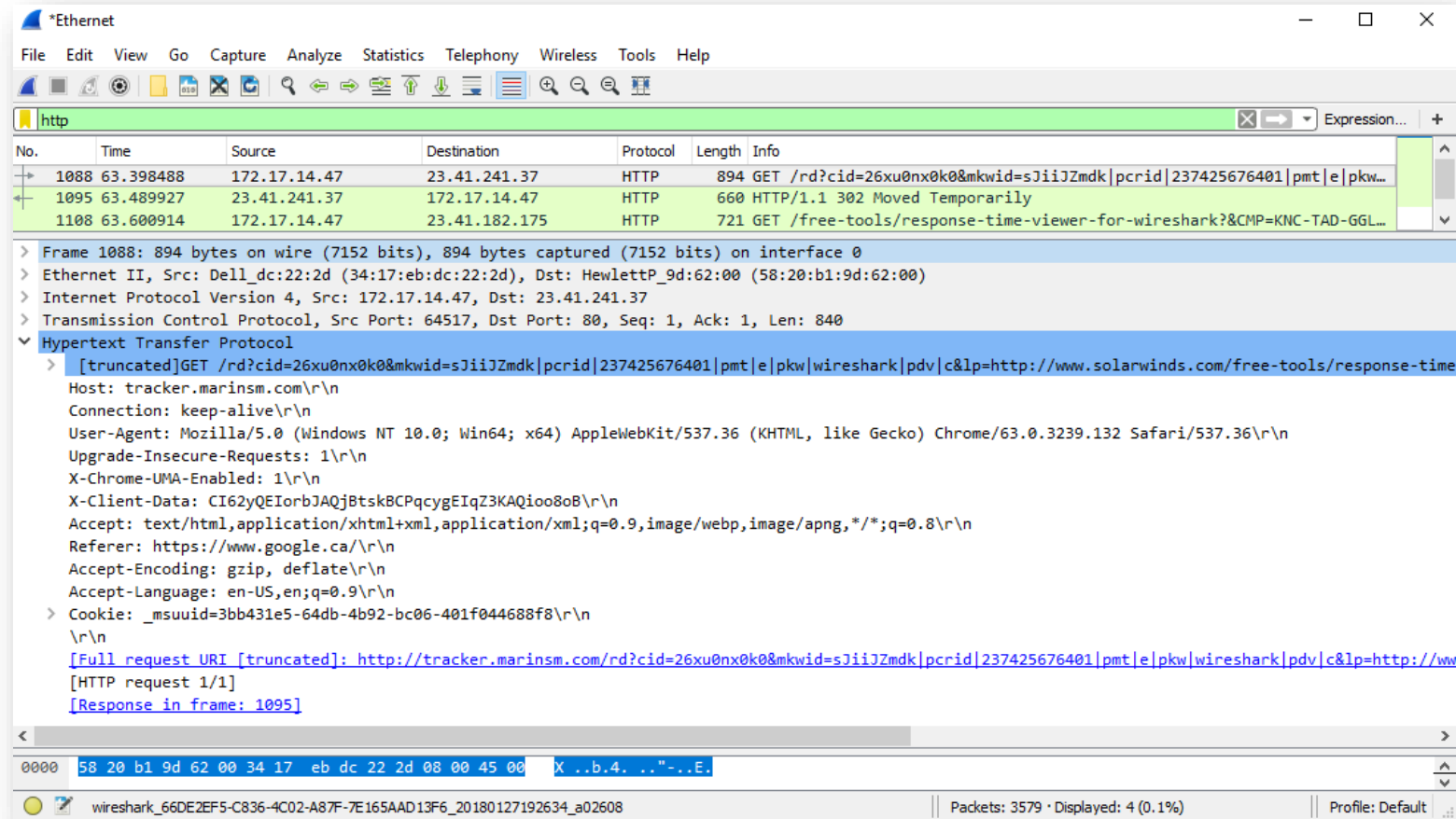
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|-----------------|----------|--------|----------------------------|
| 1 | 0.000000 | 172.17.14.28 | 172.17.14.255 | NBNS | 92 | Name query NB LOGINEN.7... |
| 2 | 0.634647 | 172.17.14.104 | 239.255.255.250 | 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... |
| 8 | 1.408863 | 172.17.14.28 | 172.17.14.255 | NBNS | 92 | Name query NB LOGINEN.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 an HTTP Request



The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for packet capture and analysis. The main display area is divided into three panes:

- Packet List:** Shows a list of captured packets. The selected packet is 1095, an HTTP GET request from 172.17.14.47 to 23.41.241.37.
- Packet Details:** Provides a hierarchical view of the selected packet's structure. It shows the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol (HTTP) section. The HTTP section is expanded, revealing the request line, host, connection, user-agent, and other headers.
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII format.

The selected packet (1095) is an HTTP GET request. The details pane shows the following information:

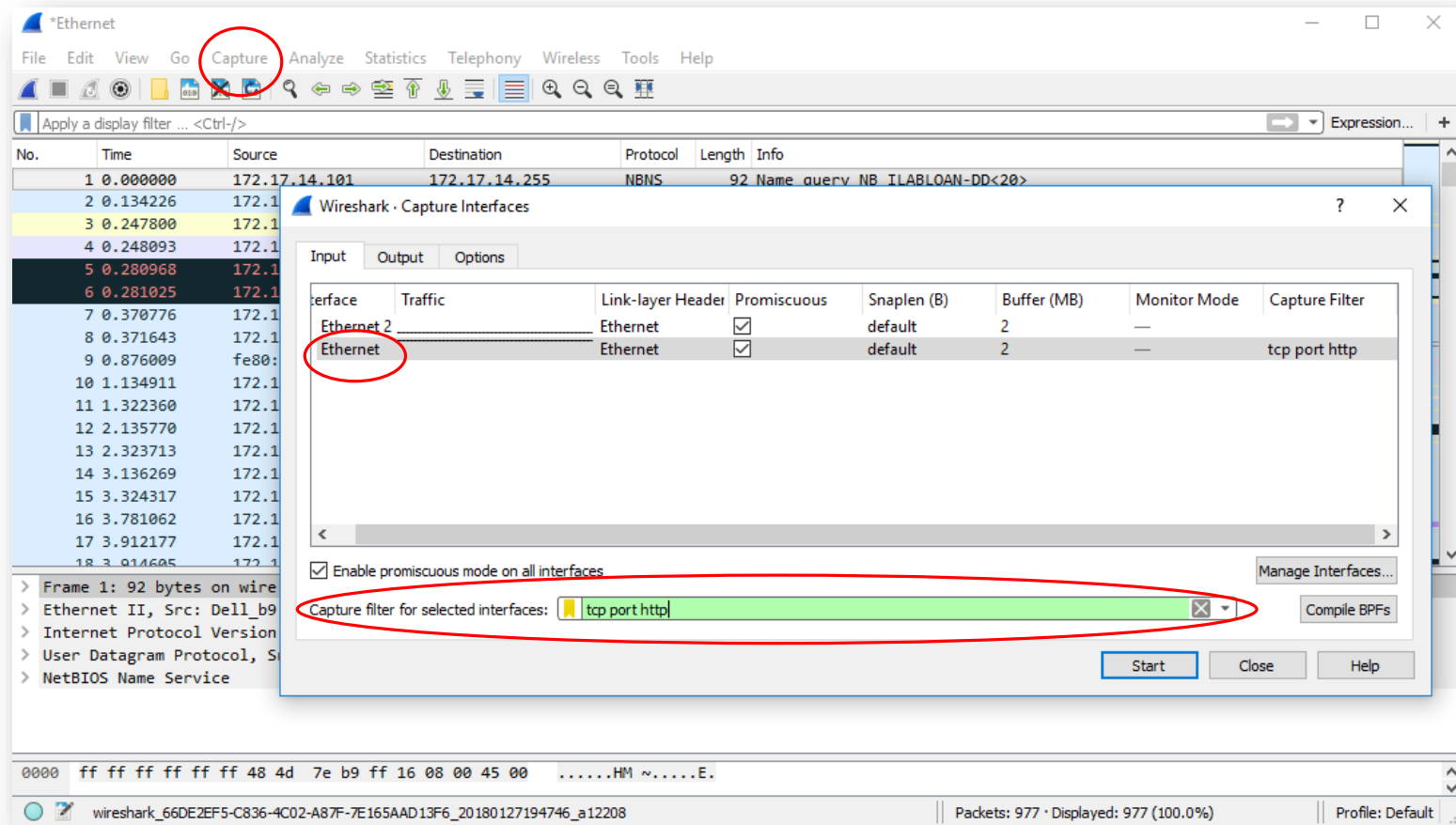
- Frame 1088: 894 bytes on wire (7152 bits), 894 bytes captured (7152 bits) on interface 0
- Ethernet II, Src: Dell_dc:22:2d (34:17:eb:dc:22:2d), Dst: HewlettP_9d:62:00 (58:20:b1:9d:62:00)
- Internet Protocol Version 4, Src: 172.17.14.47, Dst: 23.41.241.37
- Transmission Control Protocol, Src Port: 64517, 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-viewer-for-wireshark?&CMP=KNC-TAD-GGL...
 - 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: CI62yQEiorbJAQjBtskBCPqcygEIqZ3KAQioo8oB\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://www...
 - [HTTP request 1/1]
 - [Response in frame: 1095]

The bottom status bar shows the file name: wireshark_66DE2EF5-C836-4C02-A87F-7E165AAD13F6_20180127192634_a02608. It also indicates that 3579 packets are displayed, with 4 (0.1%) shown in the current view. The profile is set to Default.

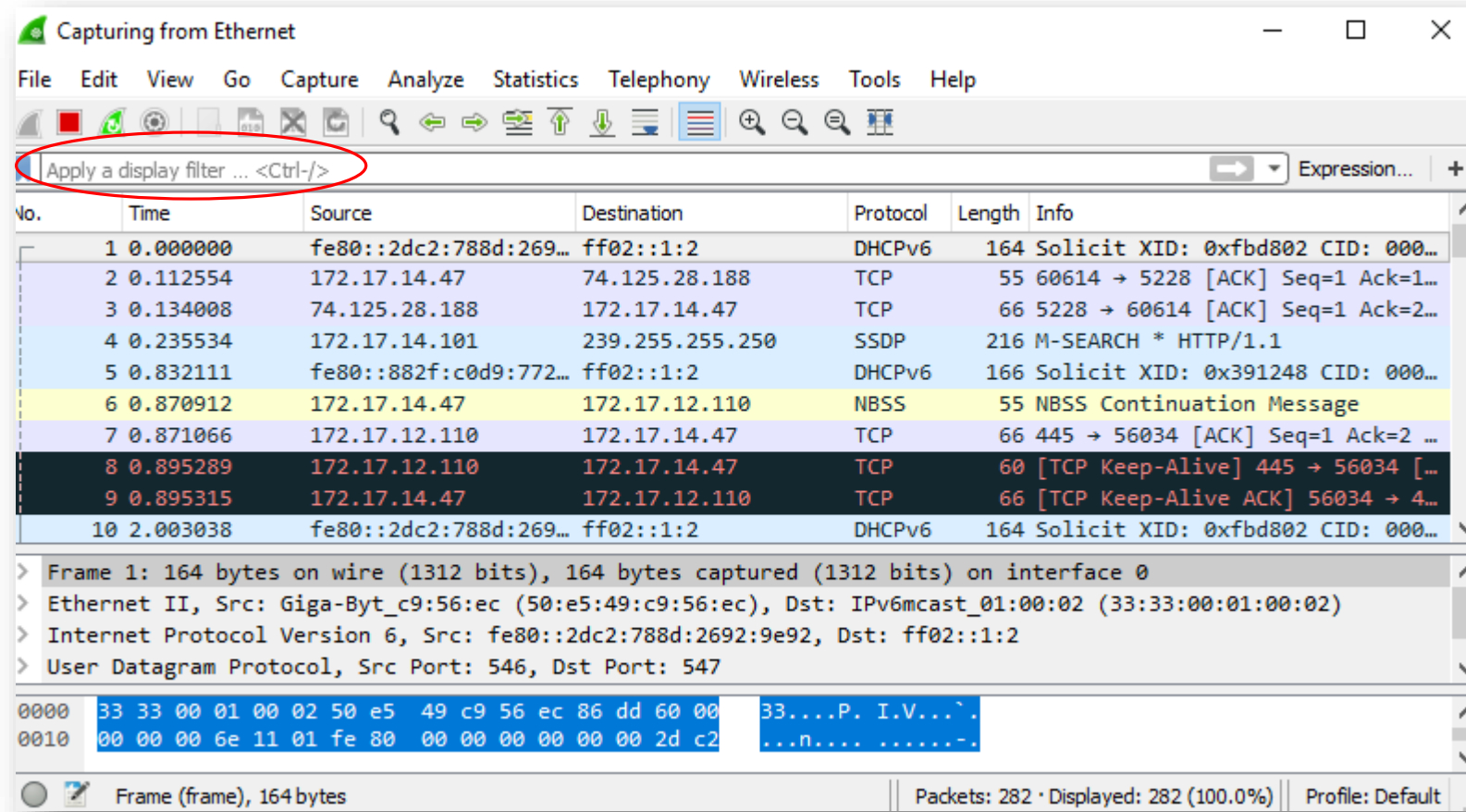
Wireshark Filters

- Capture Filters
 - Removes unwanted packets from a packet trace and only retrieve the packets of interest
- Display Filters
 - Hides unwanted packets based on your filter definition

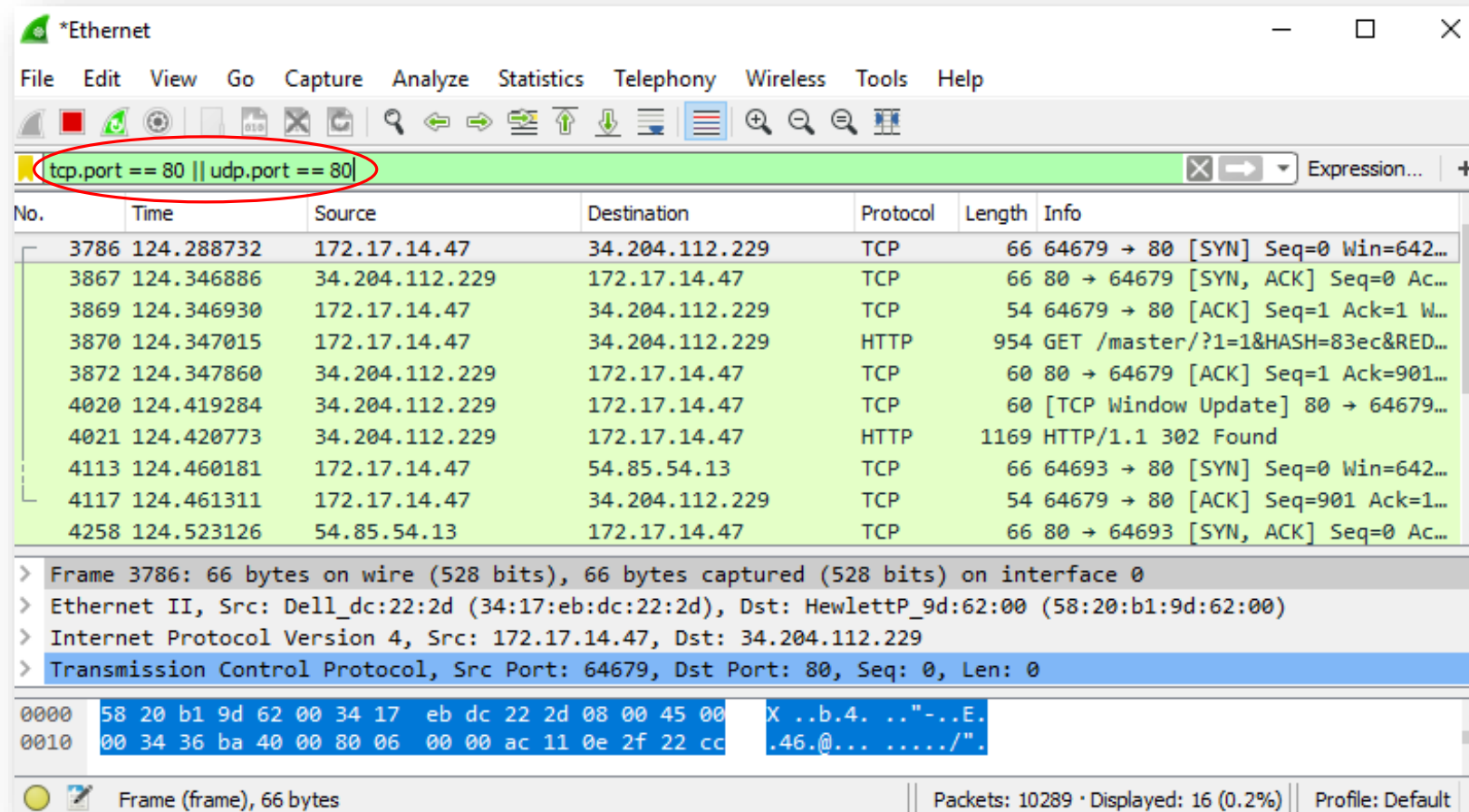
Capture Filter



Display Filter



Display Filter Example



The screenshot shows the Wireshark network protocol analyzer interface. The title bar indicates the capture is on the '*Ethernet' interface. 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 at the top shows the filter `tcp.port == 80 || udp.port == 80`, which is circled in red. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The first packet (No. 3786) is selected, and its details are shown in the lower pane. The details pane shows the following information:

- 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

The packet list shows the following data:

| 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... |

The bottom status bar shows: Frame (frame), 66 bytes | Packets: 10289 · Displayed: 16 (0.2%) | Profile: Default

Filter Examples

The operators are similar to programming languages:

- `==` Equal
- `!=` Not Equal
- `>` Greater Than
- `<` Less Than
- `>=` Greater than or Equal to
- `<=` Less than or Equal to
- `&&` Logical AND
- `||` Logical OR
- `!` Logical NOT

In display filter:

- `tcp.port == 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:
 - `http.location[0:12] == "http://pages"`
 - `http.content_type[0:4] == "text"`
 - `http.host` contains `"pages.cpsc"`

References

<https://en.wikipedia.org/wiki/Wireshark>

<https://wiki.wireshark.org/>

<https://www.wireshark.org/>