CYBERTECH AWARENESS PROGRAM

CYBERSECURITY AWARENESS AND EDUCATIONAL OUT-REACH

BURLINGTON, VT

Wireshark

Network Scanner

@cybertechvt @cybertechvt cybertechvt.com

Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

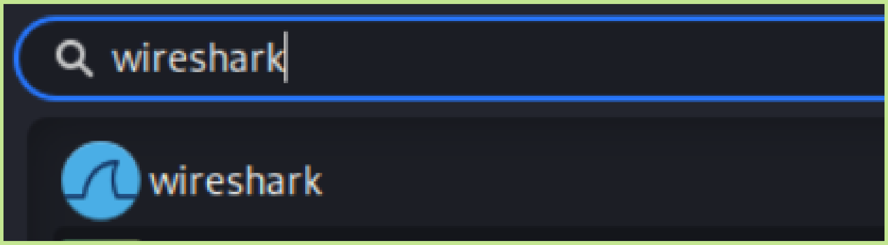
Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

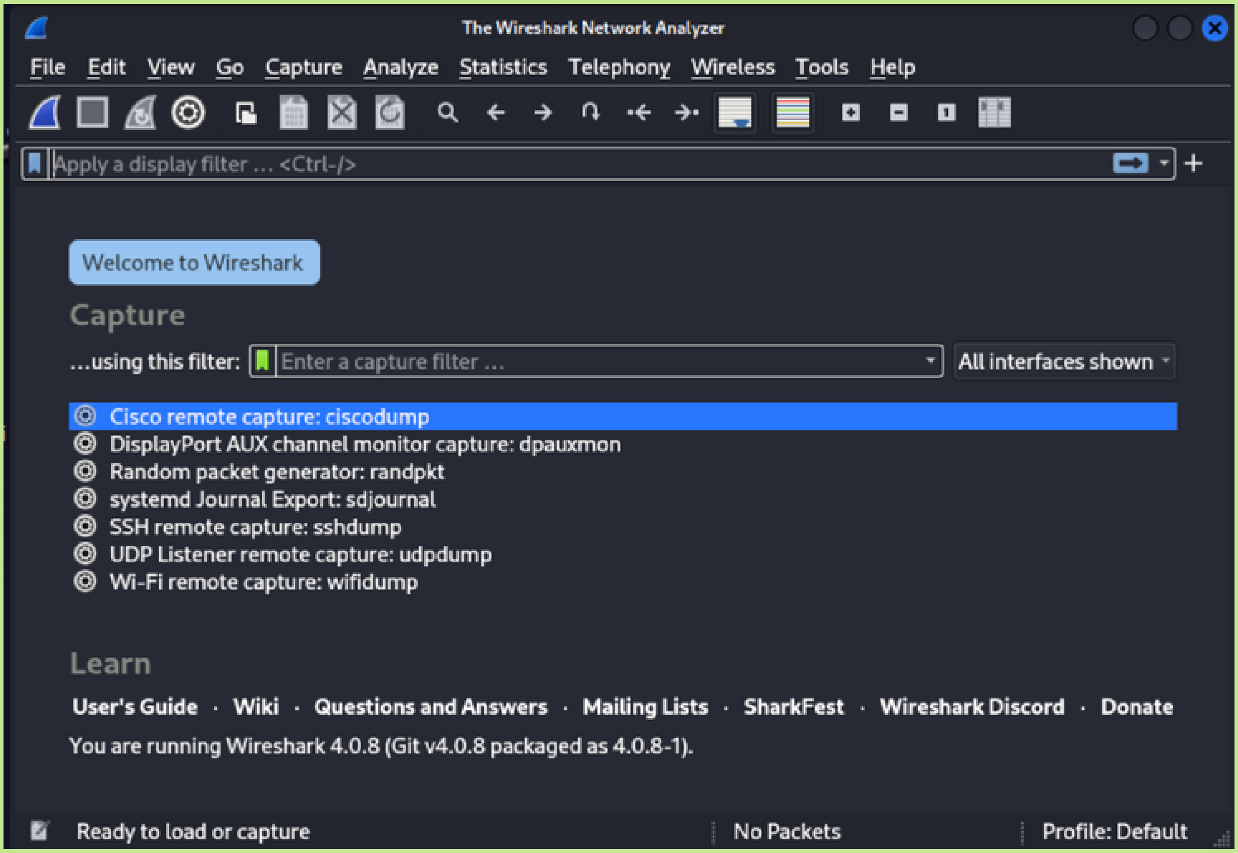
Wireshark is a tool for **capturing** and **analyzing data packets** as observed on a network.

How to Access Wireshark

Wireshark is an application on your desktop, so you can type in “Wireshark” in your terminal to access it, or you can click on the application itself.



wireshark



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Welcome to Wireshark
All interfaces shown

Apply a display filter … <Ctrl-/>

Capture

…using this filter: Enter a capture filter …

- Cisco remote capture: ciscodump
- DisplayPort AUX channel monitor capture: dpauxmon
- Random packet generator: randpkt
- systemd Journal Export: sdjournal
- SSH remote capture: sshdump
- UDP Listener remote capture: udpdump
- Wi-Fi remote capture: wifidump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

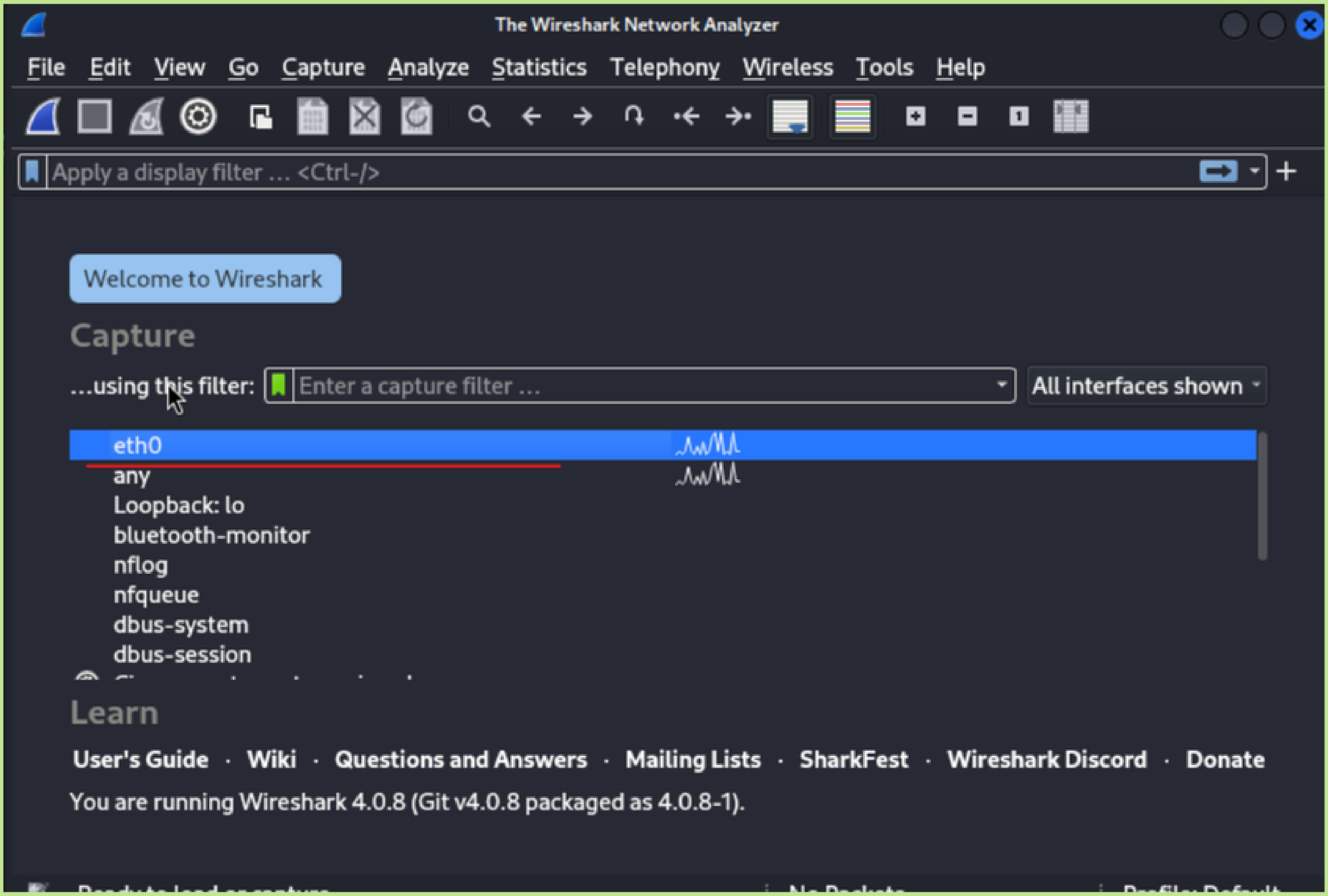
You are running Wireshark 4.0.8 (Git v4.0.8 packaged as 4.0.8-1).

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

This is the Wireshark Window that should pop up!

Running a Capture in Wireshark

When you run a capture in Wireshark you are scanning a network adapter to see what data and information is being sent and received.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

…using this filter: Enter a capture filter … All interfaces shown

eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session

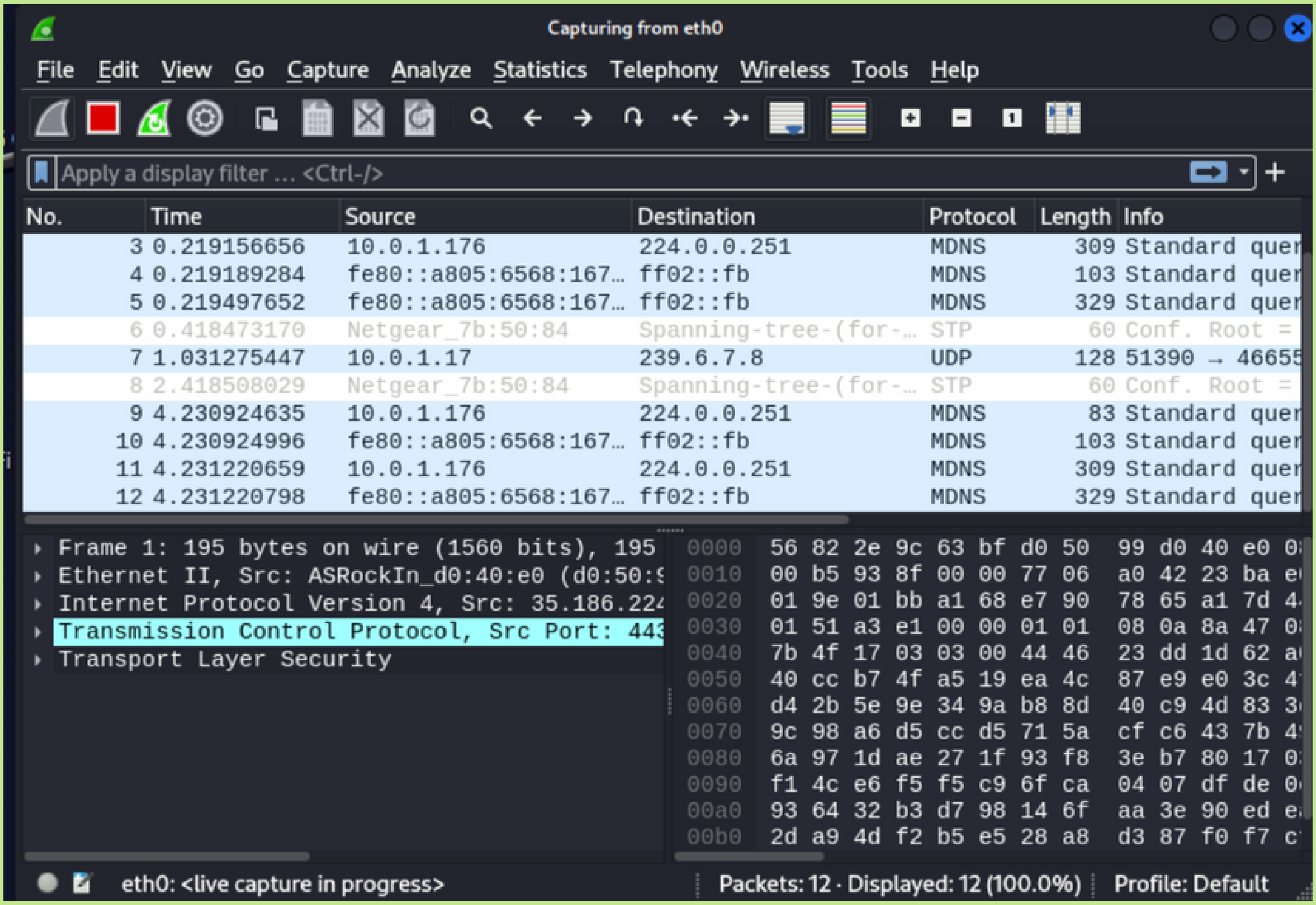
You are running Wireshark 4.0.8 (Git v4.0.8 packaged as 4.0.8-1).

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

Start by selecting the network adapter that you want to preform the capture on, in this case it will be done on “**eth0**”.

Running a Capture in Wireshark

Once you select your adapter, it should automatically start scanning the network and you should see the screen populate with data packet information!

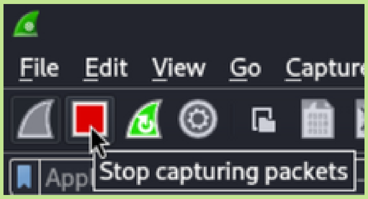

Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3	0.219156656	10.0.1.176	224.0.0.251	MDNS	309	Standard quer
4	0.219189284	fe80::a805:6568:167…	ff02::fb	MDNS	103	Standard quer
5	0.219497652	fe80::a805:6568:167…	ff02::fb	MDNS	329	Standard quer
6	0.418473170	Netgear_7b:50:84	Spanning-tree-(for-…	STP	60	Conf. Root =
7	1.031275447	10.0.1.17	239.6.7.8	UDP	128	51390 → 46655
8	2.418508029	Netgear_7b:50:84	Spanning-tree-(for-…	STP	60	Conf. Root =
9	4.230924635	10.0.1.176	224.0.0.251	MDNS	83	Standard quer
10	4.230924996	fe80::a805:6568:167…	ff02::fb	MDNS	103	Standard quer
11	4.231220659	10.0.1.176	224.0.0.251	MDNS	309	Standard quer
12	4.231220798	fe80::a805:6568:167…	ff02::fb	MDNS	329	Standard quer

```
› Frame 1: 195 bytes on wire (1560 bits), 195
› Ethernet II, Src: ASRockIn_d0:40:e0 (d0:50:9
› Internet Protocol Version 4, Src: 35.186.224
› Transmission Control Protocol, Src Port: 443
› Transport Layer Security
```

```
0000  56 82 2e 9c 63 bf d0 50  99 d0 40 e0 0
0010  00 b5 93 8f 00 00 77 06  a0 42 23 ba e
0020  01 9e 01 bb a1 68 e7 90  78 65 a1 7d 4
0030  01 51 a3 e1 00 00 01 01  08 0a 8a 47 0
0040  7b 4f 17 03 03 00 44 46  23 dd 1d 62 a
0050  40 cc b7 4f a5 19 ea 4c  87 e9 e0 3c 4
0060  d4 2b 5e 9e 34 9a b8 8d  40 c9 4d 83 3
0070  9c 98 a6 d5 cc d5 71 5a  cf c6 43 7b 4
0080  6a 97 1d ae 27 1f 93 f8  3e b7 80 17 0
0090  f1 4c e6 f5 f5 c9 6f ca  04 07 df de 0
00a0  93 64 32 b3 d7 98 14 6f  aa 3e 90 ed e
00b0  2d a9 4d f2 b5 e5 28 a8  d3 87 f0 f7 c
```

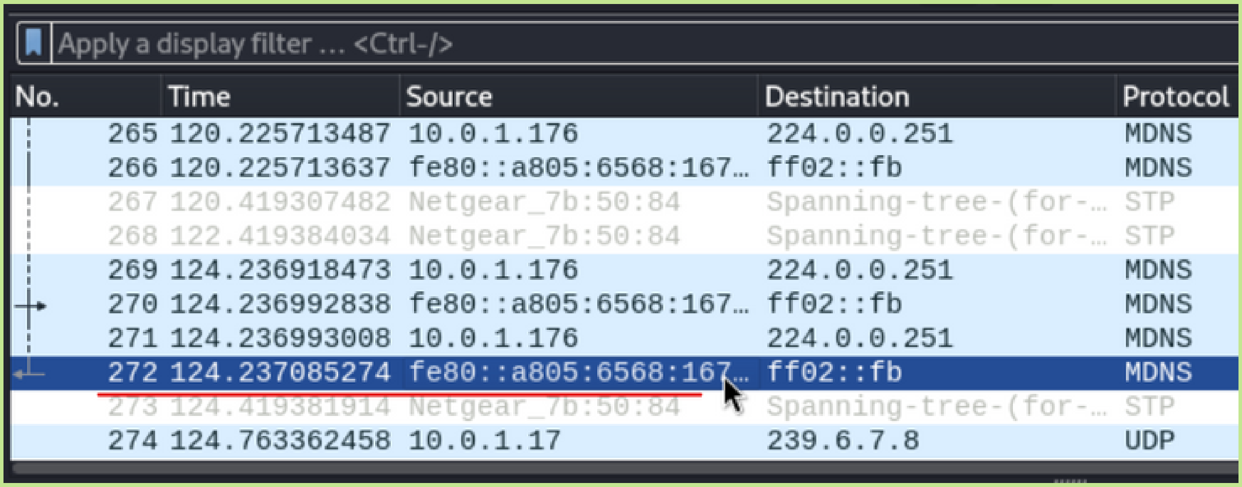
eth0: <live capture in progress> | Packets: 12 · Displayed: 12 (100.0%) | Profile: Default



You can stop the capture by pressing the red square in the top left corner.

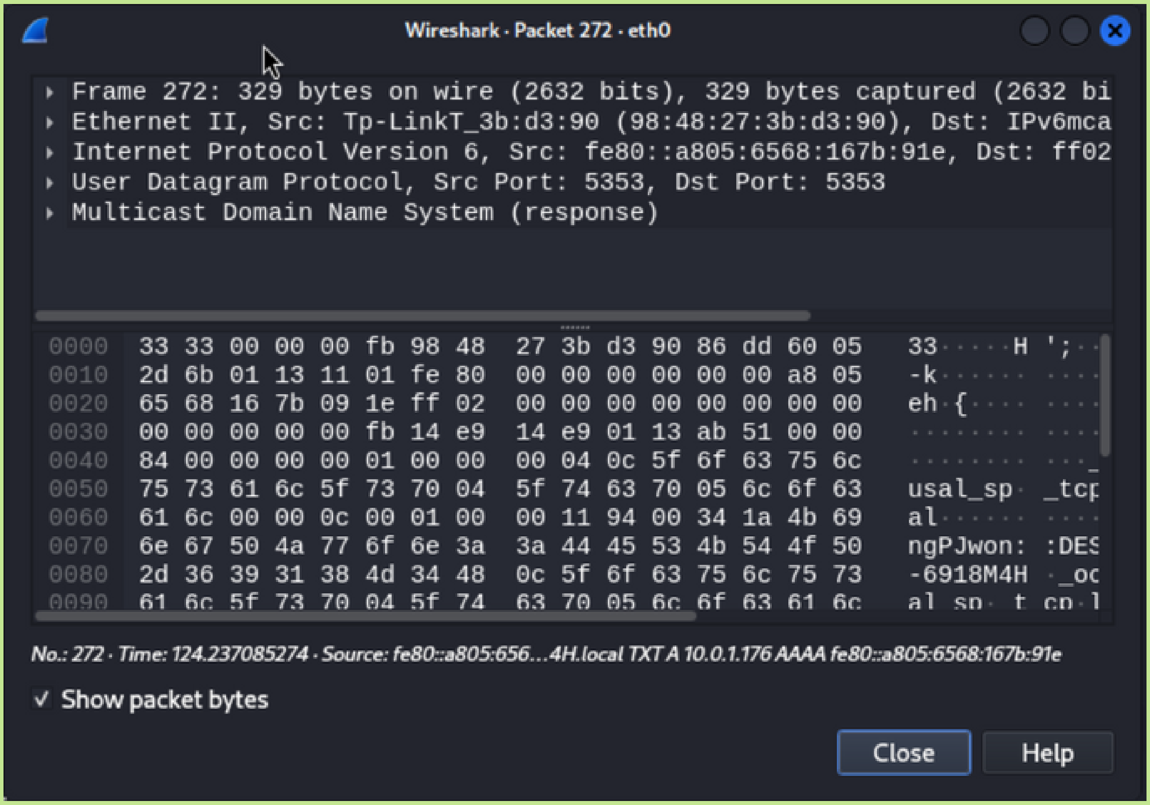
Running a Capture in Wireshark

If you click on any of the packets, you can see their information in more detail.



Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol
265	120.225713487	10.0.1.176	224.0.0.251	MDNS
266	120.225713637	fe80::a805:6568:167…	ff02::fb	MDNS
267	120.419307482	Netgear_7b:50:84	Spanning-tree-(for-…	STP
268	122.419384034	Netgear_7b:50:84	Spanning-tree-(for-…	STP
269	124.236918473	10.0.1.176	224.0.0.251	MDNS
270	124.236992838	fe80::a805:6568:167…	ff02::fb	MDNS
271	124.236993008	10.0.1.176	224.0.0.251	MDNS
272	124.237085274	fe80::a805:6568:167…	ff02::fb	MDNS
273	124.419381914	Netgear_7b:50:84	Spanning-tree-(for-…	STP
274	124.763362458	10.0.1.17	239.6.7.8	UDP



Wireshark · Packet 272 · eth0

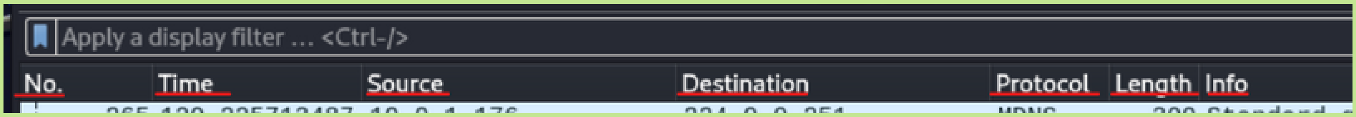
```
▸ Frame 272: 329 bytes on wire (2632 bits), 329 bytes captured (2632 bi
▸ Ethernet II, Src: Tp-LinkT_3b:d3:90 (98:48:27:3b:d3:90), Dst: IPv6mca
▸ Internet Protocol Version 6, Src: fe80::a805:6568:167b:91e, Dst: ff02
▸ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▸ Multicast Domain Name System (response)
```

```
0000  33 33 00 00 00 fb 98 48  27 3b d3 90 86 dd 60 05   33·····H ';··
0010  2d 6b 01 13 11 01 fe 80  00 00 00 00 00 00 a8 05   -k······ ····
0020  65 68 16 7b 09 1e ff 02  00 00 00 00 00 00 00 00   eh·{···· ····
0030  00 00 00 00 00 fb 14 e9  14 e9 01 13 ab 51 00 00   ········ ····
0040  84 00 00 00 00 01 00 00  00 04 0c 5f 6f 63 75 6c   ········ ···_
0050  75 73 61 6c 5f 73 70 04  5f 74 63 70 05 6c 6f 63   usal_sp· _tcp
0060  61 6c 00 00 0c 00 01 00  00 11 94 00 34 1a 4b 69   al······ ····
0070  6e 67 50 4a 77 6f 6e 3a  3a 44 45 53 4b 54 4f 50   ngPJwon: :DES
0080  2d 36 39 31 38 4d 34 48  0c 5f 6f 63 75 6c 75 73   -6918M4H ·_oc
0090  61 6c 5f 73 70 04 5f 74  63 70 05 6c 6f 63 61 6c   al_sp·_t cp·l
```

No.: 272 · Time: 124.237085274 · Source: fe80::a805:656…4H.local TXT A 10.0.1.176 AAAA fe80::a805:6568:167b:91e

Running a Capture in Wireshark

At the top of the window you should see all these packet information fields:



Number

- A number is assigned to each captured packet to create a viewable timeline of the communications captured

Time

- The time that has passed since the capture was started at the time that the packet was observed, Used to calculate time delta from previous captured or displayed frames. The time it took for each packet to go through as well as arrival time can be viewed for each individual packet.

Source

- Displays the IP address that each packet is coming from. To view this as the domain name, go to Edit > Preferences > Name Resolution > check off “Resolve network (IP) addresses”

Destination

- Displays the IP address that each packet is being sent to.

Protocol

- Displays the protocol (or type of packet) that is found within the packet signature. This is important information for filtering the packets.

Length

- Displays the size (in bytes) of the captured frame of the packet. For the length of the entire packet, go to Statistics > Packet Lengths

Info

- General information about the packet contents, which varies on the type of packet. On an unencrypted network this may include the data within the packets.

Additional Resources:

Kali Linux Wireshark Official Webpage:
https://www.kali.org/tools/wireshark/

How to Use Wireshark: Comprehensive Tutorial + Tips:
https://www.varonis.com/blog/how-to-use-wireshark

What Is Wireshark and How Is It Used?
https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

How to Use Wireshark: A Complete Tutorial:
https://www.lifewire.com/wireshark-tutorial-4143298

Learn Wireshark – Computer Networking Tutorial:
https://www.freecodecamp.org/news/learn-wireshark-computer-networking/