

53y3fkqnku2rcxwaa6np5iuvdmi2ydblnxvqtpeu6rz6vhgvlpa.us-east1-c.resources.bumper-boats-00.services.qwiklabs.com/Myrtille...

sample.pcap

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

tcp contains "curl"

No.	Time	Source	Destination	Protocol	Length	Info
67	18.034291	172.21.224.2	142.250.1.139	HTTP	151	GET / HTTP/1.1
148	42.369093	172.21.224.2	142.250.1.102	HTTP	151	GET / HTTP/1.1

▼ Frame 67: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 23, 2022 12:38:34.622216000 Greenwich Standard Time
UTC Arrival Time: Nov 23, 2022 12:38:34.622216000 UTC
Epoch Arrival Time: 1669207114.622216000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000053000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 18.034291000 seconds]
Frame Number: 67
Frame Length: 151 bytes (1208 bits)
Capture Length: 151 bytes (1208 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:00:00:00:00)
> Internet Protocol Version 4, Src: 172.21.224.2, Dst: 142.250.1.139
> Transmission Control Protocol, Src Port: 49652, Dst Port: 80, Seq: 1, Ack: 1, Len: 85
> Hypertext Transfer Protocol

0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00 45 00 B.....B.....E.
0010 00 89 e4 aa 40 00 40 06 39 27 ac 15 e0 02 8e fa@..@ 9'.....
0020 01 8b c1 f4 00 50 cb 6b 93 a1 60 64 ec 24 80 18P.k...`d.\$..
0030 01 ff 1d 19 00 00 01 01 08 0a a7 23 85 7e f2 92#.....
0040 4f b2 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0-GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 6f 70 65 6e 73 6f 75 72 ..Host: opensour
0060 63 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 0d 0a 55 ce.googl e.com..U
0070 73 65 72 2d 41 67 65 6e 74 3a 20 63 75 72 6c 2f ser-Agen t: curl/
0080 37 2e 37 34 2e 30 0d 0a 41 63 63 65 70 74 3a 20 7.74.0.. Accept:
0090 2a 2f 2a 0d 0a 0d 0a */*.....

sample.pcapPackets: 200 · Displayed: 2 (1.0%)Profile: Default

cloudskillsboost.google/focuses/41916618?parent=lti_session&parent=lti_session

Exemplar: Analyze your first packet with Wireshark

End Lab00:39:15

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked.
[Learn more.](#)
Windows VM

6. Enter the following filter to select TCP packet data that contains specific text data.

tcp contains "curl"

7. Press **ENTER** or click the **Apply display filter** icon in the filter text box.

This filters to packets containing web requests made with the `curl` command in this sample packet capture file.

Conclusion

Great work!

You now have practical experience using Wireshark to

- open saved packet capture files,
- view high-level packet data, and
- use filters to inspect detailed packet data.

This is an important milestone on your journey toward understanding how to use network packet analysis tools to examine network traffic!

Lab instructions and tasks

Activity overview

Scenario

Task 1. Explore data with Wireshark

Task 2. Apply a basic Wireshark filter and inspect a packet

Task 3. Use filters to select packets

Task 4. Use filters to explore DNS packets

Task 5. Use filters to explore TCP packets

Conclusion

End your lab