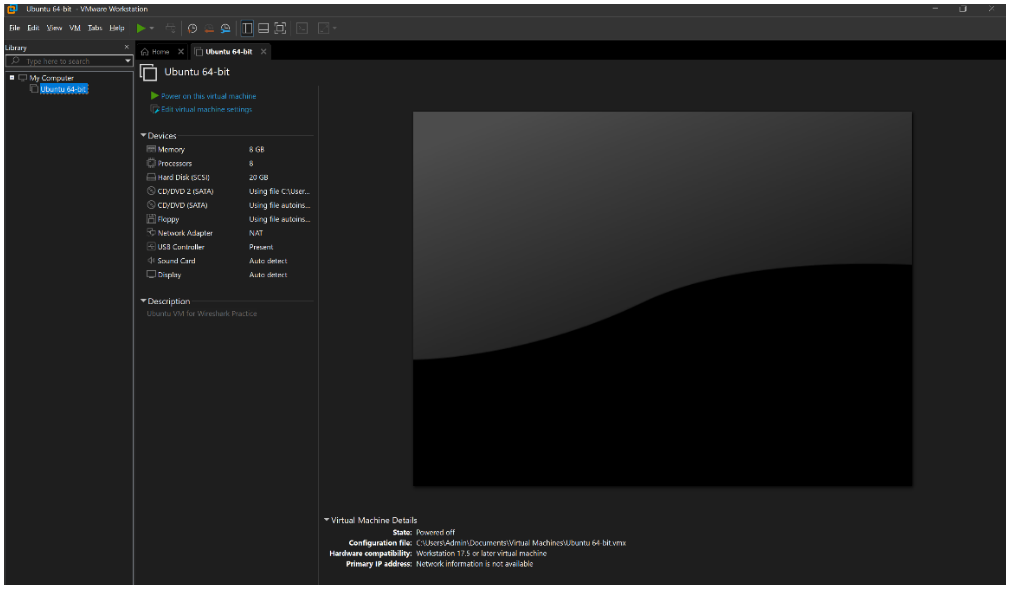
Wireshark Task 1:



Ubuntu 64-bit

Power on this virtual machine
Edit virtual machine settings

Devices

Memory	8 GB
Processors	8
Hard Disk (SCSI)	20 GB
CD/DVD 2 (SATA)	Using file C:\User...
CD/DVD (SATA)	Using file autoins...
Floppy	Using file autoins...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

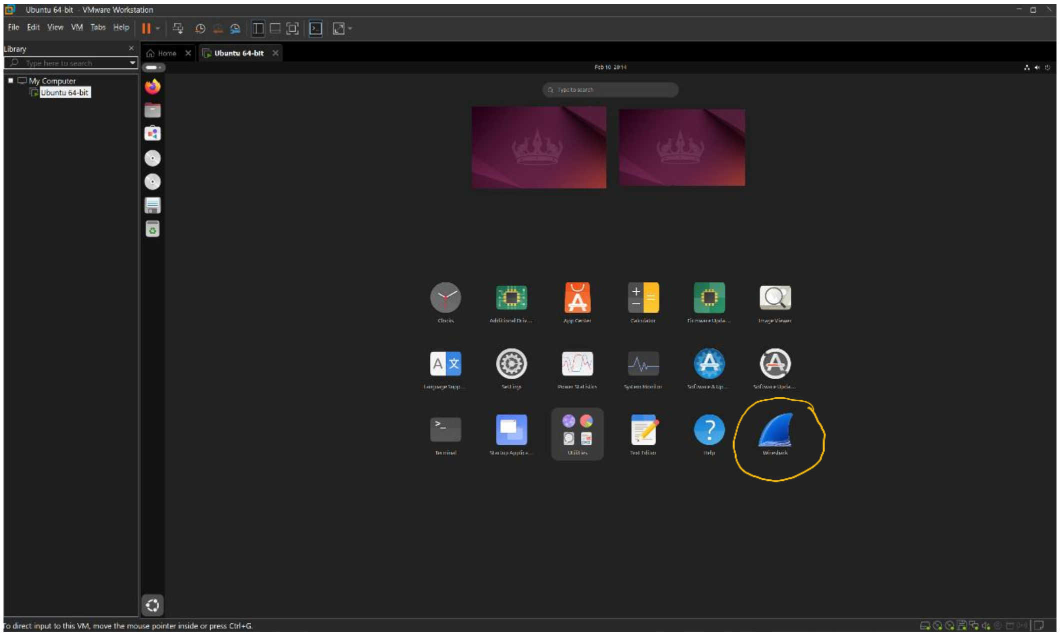
Ubuntu VM for Wireshark Practice

Virtual Machine Details

State: Powered off
Configuration file: C:\Users\Admin\Documents\Virtual Machines\Ubuntu 64-bit.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

Figure 1

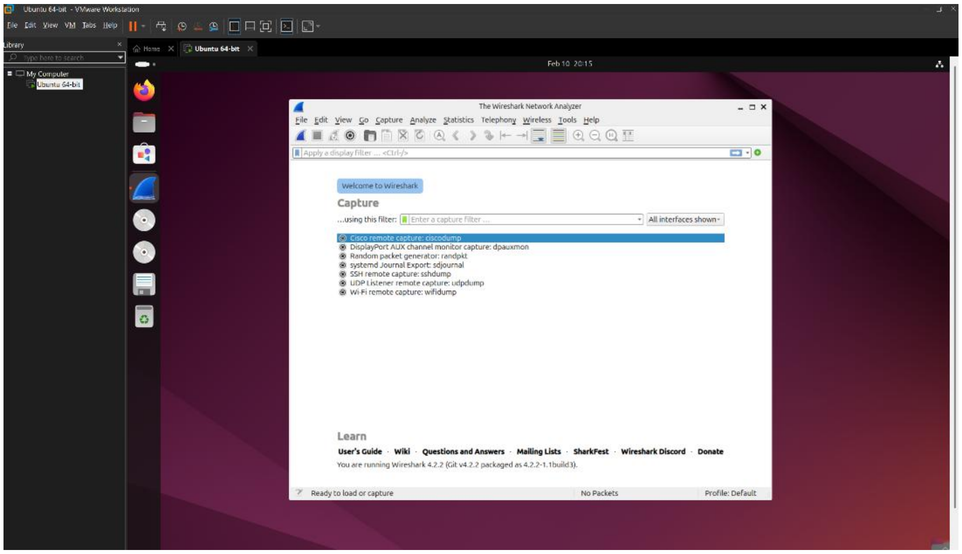
- In figure 1, I installed VMware Workstation, created the Ubuntu VM and provided it with 8 CPU cores, 8GB Memory and a 20GB Hard drive space



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Figure 2

- In figure 2, I installed Wireshark for packet capture circled in yellow.


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Ubuntu 64-bit
Home
Ubuntu 64-bit
Feb 10 20:15
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark

Capture

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

- 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

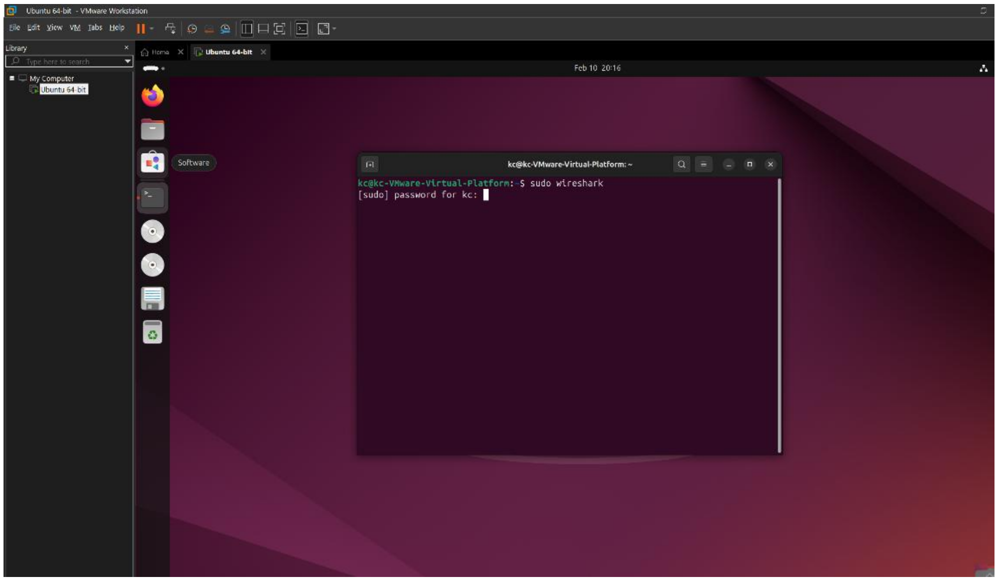
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1.1build3).

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

Figure 3

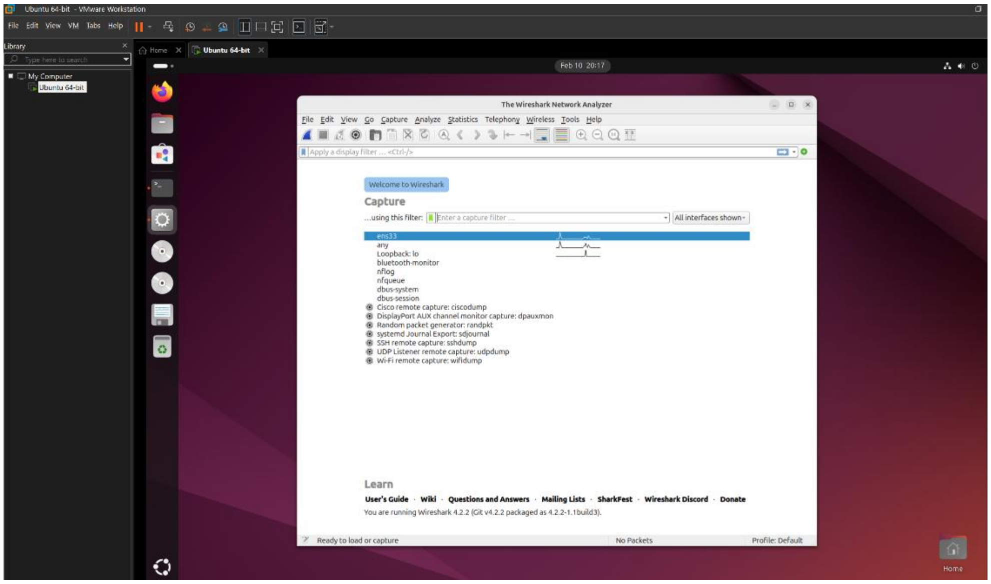
- In figure 3, Launching Wireshark without elevated privileges will not show my systems interfaces. It needs to be launched with Sudo privileges.


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Ubuntu 64-bit
Home
Ubuntu 64-bit
Feb 10 20:16
Software
kc@kc-VMware-Virtual-Platform: ~

```
kc@kc-VMware-Virtual-Platform:~$ sudo wireshark
[sudo] password for kc: 
```

Figure 4

- In figure 4, I launched Wireshark with Sudo privileges.


Ubuntu 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Ubuntu 64-bit
Home
Ubuntu 64-bit
Feb 10 20:17
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Home

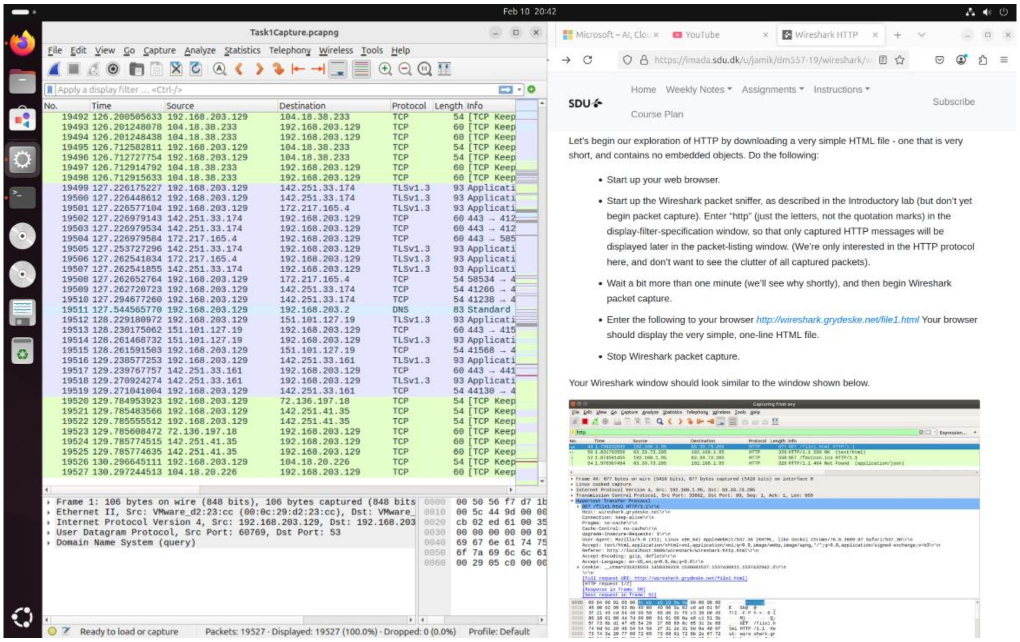
```
ens33
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
```

You are running Wireshark 4.2.2 (Git v4.2.2 packaged as 4.2.2-1.1build3).

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

Figure 5

- I selected ens33, as my interface to monitor traffic in figure 5.


Feb 10 20:42
Task1Capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Microsoft – AI, Clo
YouTube
Wireshark HTTP
https://imada.sdu.dk/u/jamik/dm557-19/wireshark/w
SDU
Home
Weekly Notes
Assignments
Instructions
Course Plan
Subscribe

```
No.   Time          Source          Destination     Protocol Length Info
19492 126.200505633 192.168.203.129 104.18.38.233   TCP      54 [TCP Keep
19493 126.201248078 104.18.38.233   192.168.203.129 TCP      60 [TCP Keep
19494 126.201248438 104.18.38.233   192.168.203.129 TCP      60 [TCP Keep
19495 126.712582811 192.168.203.129 104.18.38.233   TCP      54 [TCP Keep
19496 126.712727754 192.168.203.129 104.18.38.233   TCP      54 [TCP Keep
19497 126.712914792 104.18.38.233   192.168.203.129 TCP      60 [TCP Keep
19498 126.712915633 104.18.38.233   192.168.203.129 TCP      60 [TCP Keep
19499 127.226175227 192.168.203.129 142.251.33.174  TLSv1.3  93 Applicati
19500 127.226448612 192.168.203.129 142.251.33.174  TLSv1.3  93 Applicati
19501 127.226577104 192.168.203.129 172.217.165.4   TLSv1.3  93 Applicati
19502 127.226979143 142.251.33.174  192.168.203.129 TCP      60 443 → 412
19503 127.226979534 142.251.33.174  192.168.203.129 TCP      60 443 → 412
19504 127.226979584 172.217.165.4   192.168.203.129 TCP      60 443 → 585
19505 127.253727296 142.251.33.174  192.168.203.129 TLSv1.3  93 Applicati
19506 127.262541034 172.217.165.4   192.168.203.129 TLSv1.3  93 Applicati
19507 127.262541855 142.251.33.174  192.168.203.129 TLSv1.3  93 Applicati
19508 127.262652764 192.168.203.129 172.217.165.4   TCP      54 58534 → 4
19509 127.262720723 192.168.203.129 142.251.33.174  TCP      54 41266 → 4
19510 127.294677260 192.168.203.129 142.251.33.174  TCP      54 41238 → 4
19511 127.544565770 192.168.203.129 192.168.203.2   DNS      83 Standard
19512 128.229180972 192.168.203.129 151.101.127.19  TLSv1.3  93 Applicati
19513 128.230175062 151.101.127.19  192.168.203.129 TCP      60 443 → 415
19514 128.261468732 151.101.127.19  192.168.203.129 TLSv1.3  93 Applicati
19515 128.261591503 192.168.203.129 151.101.127.19  TCP      54 41568 → 4
19516 129.238577253 192.168.203.129 142.251.33.161  TLSv1.3  93 Applicati
19517 129.239767757 142.251.33.161  192.168.203.129 TCP      60 443 → 441
19518 129.270924274 142.251.33.161  192.168.203.129 TLSv1.3  93 Applicati
19519 129.271041004 192.168.203.129 142.251.33.161  TCP      54 44130 → 4
19520 129.784953923 192.168.203.129 72.136.197.18   TCP      54 [TCP Keep
19521 129.785483566 192.168.203.129 142.251.41.35   TCP      54 [TCP Keep
19522 129.785555512 192.168.203.129 142.251.41.35   TCP      54 [TCP Keep
19523 129.785608472 72.136.197.18   192.168.203.129 TCP      60 [TCP Keep
19524 129.785774515 142.251.41.35   192.168.203.129 TCP      60 [TCP Keep
19525 129.785774635 142.251.41.35   192.168.203.129 TCP      60 [TCP Keep
19526 130.296645111 192.168.203.129 104.18.20.226   TCP      54 [TCP Keep
19527 130.297244513 104.18.20.226   192.168.203.129 TCP      60 [TCP Keep

▸ Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits   0000  00 50 56 f7 d7 1b
▸ Ethernet II, Src: VMware_d2:23:cc (00:0c:29:d2:23:cc), Dst: VMware_   0010  00 5c 44 9d 00 00
▸ Internet Protocol Version 4, Src: 192.168.203.129, Dst: 192.168.203   0020  cb 02 ed 61 00 35
▸ User Datagram Protocol, Src Port: 60769, Dst Port: 53                 0030  00 00 00 00 00 01
▸ Domain Name System (query)                                            0040  69 67 6e 61 74 75
                                                                        0050  6f 7a 69 6c 6c 61
                                                                        0060  00 29 05 c0 00 00

Ready to load or capture   Packets: 19527 · Displayed: 19527 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

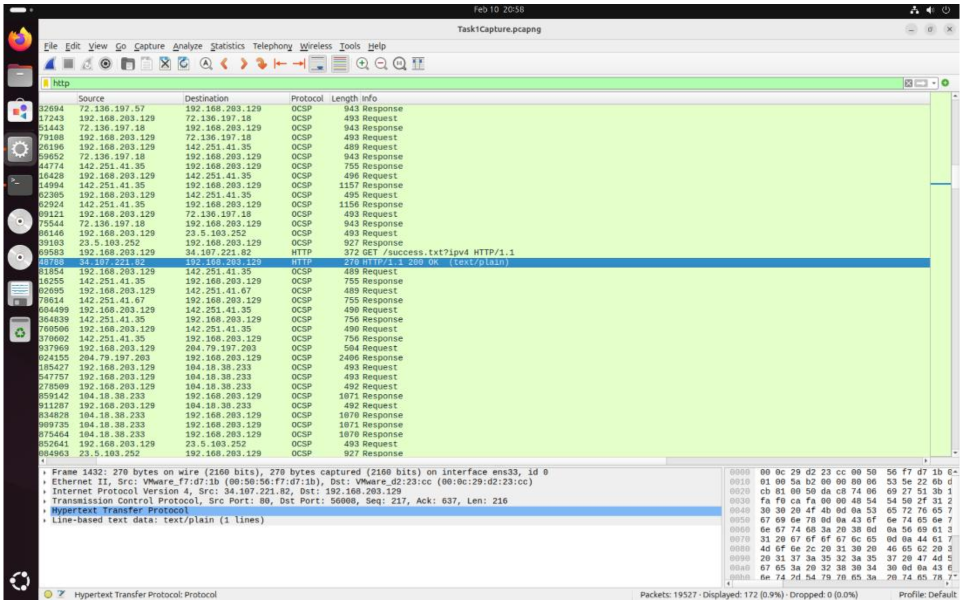
Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:

- Start up your web browser.
- Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
- Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
- Enter the following to your browser *http://wireshark.grydeske.net/file1.html* Your browser should display the very simple, one-line HTML file.
- Stop Wireshark packet capture.

Your Wireshark window should look similar to the window shown below.

Figure 6

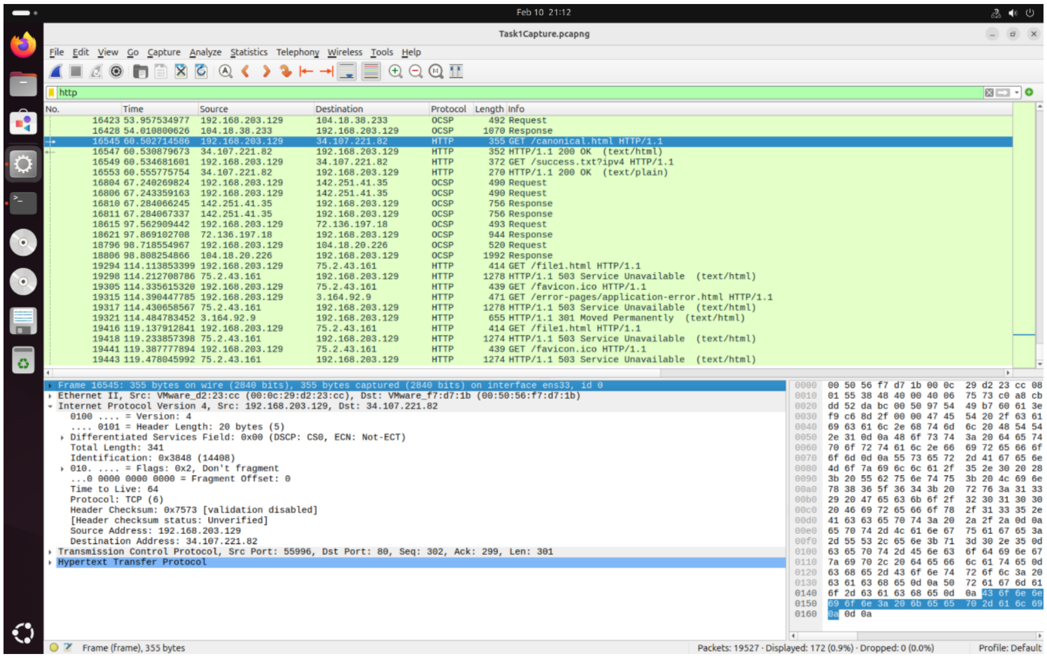
- Wireshark captured traffic packets running the TCP protocol, while browsing through various websites in figure 6.



```
Feb 10 20:58
Task1Capture.pcapng
http
        Source            Destination       Protocol Length Info
32694   72.136.197.57     192.168.203.129   OCSP      943 Response
17243   192.168.203.129   72.136.197.18     OCSP      493 Request
51443   72.136.197.18     192.168.203.129   OCSP      943 Response
79108   192.168.203.129   72.136.197.18     OCSP      493 Request
26196   192.168.203.129   142.251.41.35     OCSP      489 Request
59652   72.136.197.18     192.168.203.129   OCSP      943 Response
44774   142.251.41.35     192.168.203.129   OCSP      755 Response
16428   192.168.203.129   142.251.41.35     OCSP      496 Request
14994   142.251.41.35     192.168.203.129   OCSP     1157 Response
62305   192.168.203.129   142.251.41.35     OCSP      495 Request
62924   142.251.41.35     192.168.203.129   OCSP     1156 Response
09121   192.168.203.129   72.136.197.18     OCSP      493 Request
75544   72.136.197.18     192.168.203.129   OCSP      943 Response
86146   192.168.203.129   23.5.103.252      OCSP      493 Request
39103   23.5.103.252      192.168.203.129   OCSP      927 Response
69583   192.168.203.129   34.107.221.82     HTTP      372 GET /success.txt?ipv4 HTTP/1.1
48788   34.107.221.82     192.168.203.129   HTTP      270 HTTP/1.1 200 OK  (text/plain)
81854   192.168.203.129   142.251.41.35     OCSP      489 Request
16255   142.251.41.35     192.168.203.129   OCSP      755 Response
02695   192.168.203.129   142.251.41.67     OCSP      489 Request
78614   142.251.41.67     192.168.203.129   OCSP      755 Response
604499  192.168.203.129   142.251.41.35     OCSP      490 Request
364839  142.251.41.35     192.168.203.129   OCSP      756 Response
760506  192.168.203.129   142.251.41.35     OCSP      490 Request
370602  142.251.41.35     192.168.203.129   OCSP      756 Response
937969  192.168.203.129   204.79.197.203    OCSP      504 Request
024155  204.79.197.203    192.168.203.129   OCSP     2406 Response
185427  192.168.203.129   104.18.38.233     OCSP      493 Request
547757  192.168.203.129   104.18.38.233     OCSP      493 Request
278509  192.168.203.129   104.18.38.233     OCSP      492 Request
859142  104.18.38.233     192.168.203.129   OCSP     1071 Response
911287  192.168.203.129   104.18.38.233     OCSP      492 Request
834828  104.18.38.233     192.168.203.129   OCSP     1070 Response
909735  104.18.38.233     192.168.203.129   OCSP     1071 Response
875464  104.18.38.233     192.168.203.129   OCSP     1070 Response
852641  192.168.203.129   23.5.103.252      OCSP      493 Request
084963  23.5.103.252      192.168.203.129   OCSP      927 Response

▸ Frame 1432: 270 bytes on wire (2160 bits), 270 bytes captured (2160 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_f7:d7:1b (00:50:56:f7:d7:1b), Dst: VMware_d2:23:cc (00:0c:29:d2:23:cc)
▸ Internet Protocol Version 4, Src: 34.107.221.82, Dst: 192.168.203.129
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 56008, Seq: 217, Ack: 637, Len: 216
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/plain (1 lines)

0000  00 0c 29 d2 23 cc 00 50  56 f7 d7 1b 0
0010  01 00 5a b2 00 00 80 06  53 5e 22 6b d
0020  cb 81 00 50 da c8 74 06  69 27 51 3b 1
0030  fa f0 ca fa 00 00 48 54  54 50 2f 31 2
0040  30 30 20 4f 4b 0d 0a 53  65 72 76 65 7
0050  67 69 6e 78 0d 0a 43 6f  6e 74 65 6e 7
0060  6e 67 74 68 3a 20 38 0d  0a 56 69 61 3
0070  31 20 67 6f 6f 67 6c 65  0d 0a 44 61 7
0080  4d 6f 6e 2c 20 31 30 20  46 65 62 20 3
0090  20 31 37 3a 35 32 3a 35  37 20 47 4d 5
00a0  67 65 3a 20 32 38 30 34  30 0d 0a 43 6
00b0  6e 74 2d 54 79 70 65 3a  20 74 65 78 7

Hypertext Transfer Protocol: Protocol    Packets: 19527 · Displayed: 172 (0.9%) · Dropped: 0 (0.0%)    Profile: Default
```

Figure 7

- I saved my capture and filtered for http protocol in figure 7.



```
Feb 10 21:12
Task1Capture.pcapng
http
No.   Time              Source            Destination       Protocol Length Info
16423 53.957534977      192.168.203.129   104.18.38.233     OCSP      492 Request
16428 54.010800626      104.18.38.233     192.168.203.129   OCSP     1070 Response
16545 60.502714586      192.168.203.129   34.107.221.82     HTTP      355 GET /canonical.html HTTP/1.1
16547 60.530879673      34.107.221.82     192.168.203.129   HTTP      352 HTTP/1.1 200 OK  (text/html)
16549 60.534681601      192.168.203.129   34.107.221.82     HTTP      372 GET /success.txt?ipv4 HTTP/1.1
16553 60.555775754      34.107.221.82     192.168.203.129   HTTP      270 HTTP/1.1 200 OK  (text/plain)
16804 67.240269824      192.168.203.129   142.251.41.35     OCSP      490 Request
16806 67.243359163      192.168.203.129   142.251.41.35     OCSP      490 Request
16810 67.284066245      142.251.41.35     192.168.203.129   OCSP      756 Response
16811 67.284067337      142.251.41.35     192.168.203.129   OCSP      756 Response
18615 97.562909442      192.168.203.129   72.136.197.18     OCSP      493 Request
18621 97.869102708      72.136.197.18     192.168.203.129   OCSP      944 Response
18796 98.718554967      192.168.203.129   104.18.20.226     OCSP      520 Request
18806 98.808254866      104.18.20.226     192.168.203.129   OCSP     1992 Response
19294 114.113853399     192.168.203.129   75.2.43.161       HTTP      414 GET /file1.html HTTP/1.1
19298 114.212708786     75.2.43.161       192.168.203.129   HTTP     1278 HTTP/1.1 503 Service Unavailable  (text/html)
19305 114.335615320     192.168.203.129   75.2.43.161       HTTP      439 GET /favicon.ico HTTP/1.1
19315 114.390447785     192.168.203.129   3.164.92.9        HTTP      471 GET /error-pages/application-error.html HTTP/1.1
19317 114.430658567     75.2.43.161       192.168.203.129   HTTP     1278 HTTP/1.1 503 Service Unavailable  (text/html)
19321 114.484783452     3.164.92.9        192.168.203.129   HTTP      655 HTTP/1.1 301 Moved Permanently  (text/html)
19416 119.137912841     192.168.203.129   75.2.43.161       HTTP      414 GET /file1.html HTTP/1.1
19418 119.233857398     75.2.43.161       192.168.203.129   HTTP     1274 HTTP/1.1 503 Service Unavailable  (text/html)
19441 119.387777894     192.168.203.129   75.2.43.161       HTTP      439 GET /favicon.ico HTTP/1.1
19443 119.478045992     75.2.43.161       192.168.203.129   HTTP     1274 HTTP/1.1 503 Service Unavailable  (text/html)

▸ Frame 16545: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface ens33, id 0
▸ Ethernet II, Src: VMware_d2:23:cc (00:0c:29:d2:23:cc), Dst: VMware_f7:d7:1b (00:50:56:f7:d7:1b)
▾ Internet Protocol Version 4, Src: 192.168.203.129, Dst: 34.107.221.82
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 341
    Identification: 0x3848 (14408)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x7573 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.203.129
    Destination Address: 34.107.221.82
▸ Transmission Control Protocol, Src Port: 55996, Dst Port: 80, Seq: 302, Ack: 299, Len: 301
▸ Hypertext Transfer Protocol

0000  00 50 56 f7 d7 1b 00 0c  29 d2 23 cc 08
0010  01 55 38 48 40 00 40 06  75 73 c0 a8 cb
0020  dd 52 da bc 00 50 97 54  49 b7 60 61 3e
0030  f9 c6 8d 2f 00 00 47 45  54 20 2f 63 61
0040  69 63 61 6c 2e 68 74 6d  6c 20 48 54 54
0050  2e 31 0d 0a 48 6f 73 74  3a 20 64 65 74
0060  70 6f 72 74 61 6c 2e 66  69 72 65 66 6f
0070  6f 6d 0d 0a 55 73 65 72  2d 41 67 65 6e
0080  4d 6f 7a 69 6c 6c 61 2f  35 2e 30 20 28
0090  3b 20 55 62 75 6e 74 75  3b 20 4c 69 6e
00a0  78 38 36 5f 36 34 3b 20  72 76 3a 31 33
00b0  29 20 47 65 63 6b 6f 2f  32 30 31 30 30
00c0  20 46 69 72 65 66 6f 78  2f 31 33 35 2e
00d0  41 63 63 65 70 74 3a 20  2a 2f 2a 0d 0a
00e0  65 70 74 2d 4c 61 6e 67  75 61 67 65 3a
00f0  2d 55 53 2c 65 6e 3b 71  3d 30 2e 35 0d
0100  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67
0110  7a 69 70 2c 20 64 65 66  6c 61 74 65 0d
0120  63 68 65 2d 43 6f 6e 74  72 6f 6c 3a 20
0130  63 61 63 68 65 0d 0a 50  72 61 67 6d 61
0140  6f 2d 63 61 63 68 65 0d  0a 43 6f 6e 6e
0150  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69
0160  0a 0d 0a

Frame (frame), 355 bytes    Packets: 19527 · Displayed: 172 (0.9%) · Dropped: 0 (0.0%)    Profile: Default
```

- In figure 8, I observe that frame number 16545 has source Ip address: 192.168.203.129 (my ens33 interface) and destination address: 34.107.221.82 is a remote machine where GET method sent. It responded with an HTTP/1.1 200 OK message. The protocol used was TCP and the frame had a time to live of 64.