

Simran Shrestha

Professor Natalia Ermicioio

1. What is the Internet address of your computer?

> 10.8.20.196

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows a packet of 513 bytes on wire (4104 bits) captured on interface \Device\NPF_{DB803BE2-E17E-4B3C-BAC3-C6E100926EDF}, id 0. The packet details pane shows the structure of the HTTP request, including the version (4), header length (20 bytes), identification (0xfbed), flags (0x40), and destination address (128.119.245.12). The packet bytes pane shows the raw data of the request, including the GET method, the request URI, the host, and the user-agent.

No.	Time	Source	Destination	Protocol	Length	Info
877	10.855468	10.8.20.196	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
880	10.873942	128.119.245.12	10.8.20.196	HTTP	540	HTTP/1.1 200 OK (text/html)
884	10.920512	10.8.20.196	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
886	10.938805	128.119.245.12	10.8.20.196	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1176	13.476863	10.8.20.196	8.253.132.121	HTTP	366	GET /filestreamingservice/files/01ee126c-844f-4957-bb08-b42ece6e1138/pieceshash HTTP/1.1
1180	13.479551	8.253.132.121	10.8.20.196	HTTP	84	HTTP/1.1 200 OK
1213	13.510966	10.8.20.196	8.253.131.111	HTTP	471	GET /filestreamingservice/files/01ee126c-844f-4957-bb08-b42ece6e1138?P1=16147151636P2=4046P3=26P4=...
1216	13.512382	10.8.20.196	8.253.132.121	HTTP	471	GET /filestreamingservice/files/01ee126c-844f-4957-bb08-b42ece6e1138?P1=16147151636P2=4046P3=26P4=...
1219	13.514018	8.253.131.111	10.8.20.196	HTTP	417	HTTP/1.1 403 Forbidden (text/html)
1222	13.516113	8.253.132.121	10.8.20.196	HTTP	417	HTTP/1.1 403 Forbidden (text/html)
1355	13.965746	10.8.20.196	67.26.247.254	HTTP	487	GET /filestreamingservice/files/01ee126c-844f-4957-bb08-b42ece6e1138?P1=16315383536P2=4046P3=26P4=...
1358	13.966222	10.8.20.196	8.240.25.254	HTTP	487	GET /filestreamingservice/files/01ee126c-844f-4957-bb08-b42ece6e1138?P1=16315383536P2=4046P3=26P4=...
1361	13.969138	67.26.247.254	10.8.20.196	HTTP	1092	HTTP/1.1 206 Partial Content
1364	13.969795	8.240.25.254	10.8.20.196	HTTP	1092	HTTP/1.1 206 Partial Content
1365	13.972718	10.8.20.196	67.26.247.254	HTTP	501	GET /filestreamingservice/files/01ee126c-844f-4957-bb08-b42ece6e1138?P1=16315383536P2=4046P3=26P4=...

Frame 877: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF_{DB803BE2-E17E-4B3C-BAC3-C6E100926EDF}, id 0
Ethernet II, Src: Dell_17:24:5c (14:b3:1f:17:24:5c), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
Internet Protocol Version 4, Src: 10.8.20.196, Dst: 128.119.245.12
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 499
Identification: 0xfbed (64493)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x68c7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.8.20.196
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 52637, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
Hypertext Transfer Protocol

0000 00 2c c8 59 ec bf 14 b3 1f 17 24 5c 08 00 45 00 ..Y....\$...E
0010 01 f3 fb ed 40 00 80 06 68 c7 0a 08 14 c4 80 77 ...@...h...w
0020 f5 0c cd 9d 00 50 5a b9 9c 53 7f d7 88 bc 50 18PZ...S...P
0030 04 00 5c b0 00 00 47 45 54 20 2f 7f 69 72 65 73 ...\\...GE T/wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-Lab s/HTTP-w
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1- Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu :C onnectio
0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive-U

2. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

> TCP, ICMPv6, DNS

>

simran lab 1.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
883	10.915667	10.8.20.196	128.119.245.12	TCP	54	52637 → 80 [ACK] Seq=460 Ack=487 Win=261632 Len=0
884	10.920512	10.8.20.196	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
885	10.924653	10.8.20.196	107.20.229.191	TCP	54	49694 → 443 [ACK] Seq=12430 Ack=2851 Win=1020 Len=0
886	10.938805	128.119.245.12	10.8.20.196	HTTP	538	HTTP/1.1 404 Not Found (text/html)
887	10.979675	10.8.20.196	128.119.245.12	TCP	54	52637 → 80 [ACK] Seq=857 Ack=971 Win=261120 Len=0
888	11.069252	::	ff02::1:ff15:4db0	ICMPv6	78	Neighbor Solicitation for fe80::1945:aac9:9215:4db0
889	11.069485	fe80::1945:aac9:9215:4db0	ff02::1	ICMPv6	78	Neighbor Advertisement for fe80::1945:aac9:9215:4db0 (ovr)
890	11.256244	10.8.20.196	10.8.2.30	DNS	86	Standard query 0xf906 A vqualjlti.ad.marymount.edu
891	11.256249	10.8.20.196	10.8.2.30	DNS	92	Standard query 0xdb38 A lvqkhevifvmjxrw.ad.marymount.edu
892	11.256623	10.8.20.196	10.8.2.30	DNS	89	Standard query 0xf484 A diybrbgwjlph.ad.marymount.edu
893	11.257174	10.8.20.196	224.0.0.251	MDNS	75	Standard query 0x0000 A vqualjlti.local, "QM" question
894	11.257280	10.8.2.30	10.8.20.196	DNS	142	Standard query response 0xf906 No such name A vqualjlti.ad.marymount.edu SOA mc-ad-01.ad.marymount.edu
895	11.257443	10.8.2.30	10.8.20.196	DNS	148	Standard query response 0xdb38 No such name A lvqkhevifvmjxrw.ad.marymount.edu SOA mc-ad-01.ad.marymount.edu
896	11.257720	10.8.2.30	10.8.20.196	DNS	145	Standard query response 0xf484 No such name A diybrbgwjlph.ad.marymount.edu SOA mc-ad-02.ad.marymount.edu
897	11.257760	10.8.20.196	10.8.2.30	DNS	83	Standard query 0xd537 A vqualjlti.ad.marymount.edu

Frame 877: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF_{D8B03BE2-E17E-4B3C-BAC3-C6E100926EDF}, id 0

Ethernet II, Src: Dell_17:24:5c (14:b3:1f:17:24:5c), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)

Internet Protocol Version 4, Src: 10.8.20.196, Dst: 128.119.245.12

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 499
 Identification: 0xfbed (64493)
 Flags: 0x40, Don't fragment
 Fragment Offset: 0
 Time to Live: 128
 Protocol: TCP (6)
 Header Checksum: 0x68c7 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 10.8.20.196
 Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 52637, Dst Port: 80, Seq: 1, Ack: 1, Len: 459

Hypertext Transfer Protocol

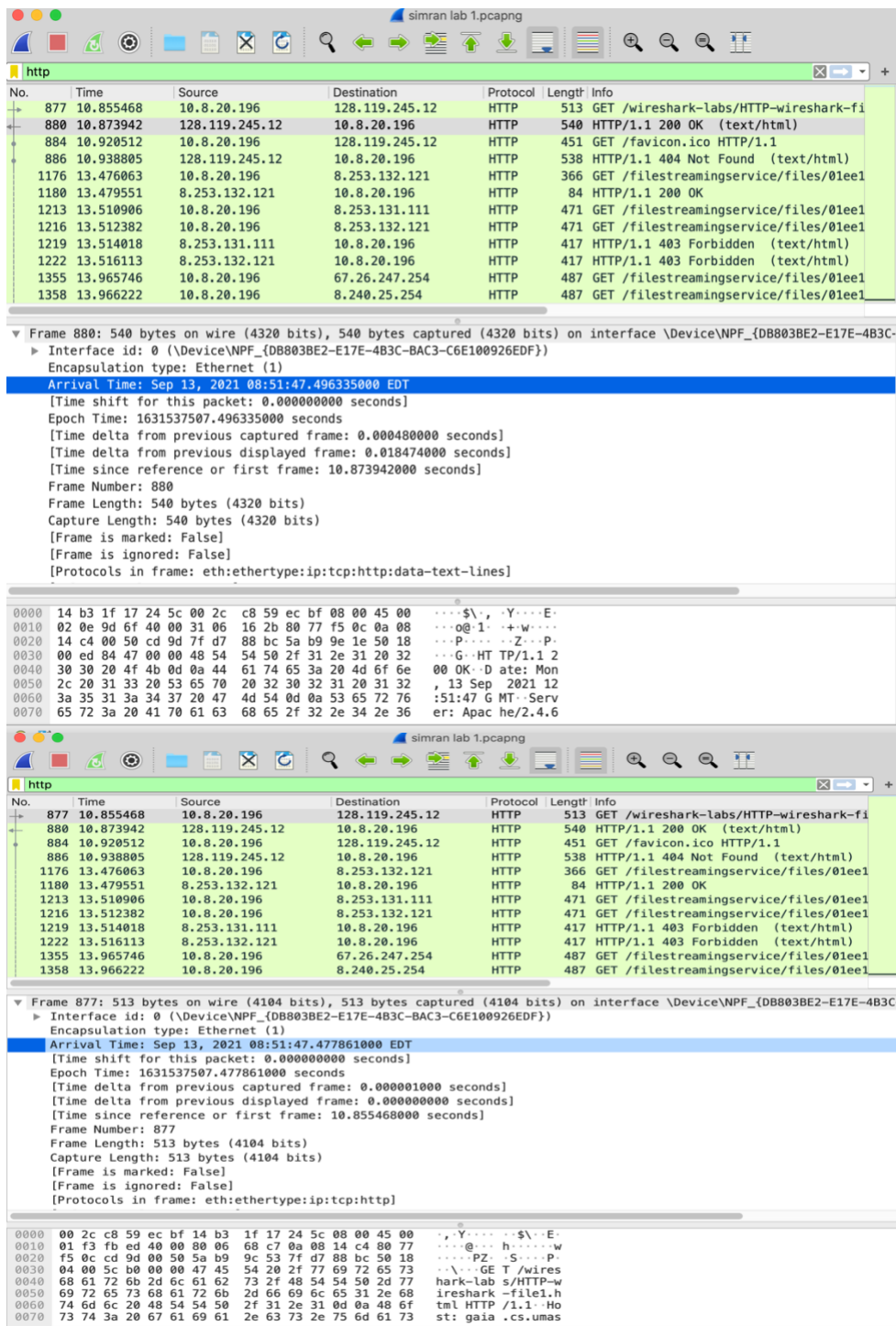
0000 00 2c c8 59 ec bf 14 b3 1f 17 24 5c 08 00 45 00 ..Y....\$.E.
 0010 01 f3 fb ed 40 00 06 68 c7 0a 08 14 c4 80 77 ...@...h.....
 0020 f5 0c cd 9d 00 50 5a b9 9c 53 7f d7 88 bc 50 18 ...PZ..S...P..
 0030 04 00 5c 00 00 47 45 54 20 2f 77 69 72 65 73 -\...GE T /wires
 0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w
 0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
 0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho
 0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
 0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 63 74 69 6f s.edu -C onnectio
 0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive- U

3. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packetlisting window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

> Arrival Time: Sep 13, 2021 08:51:47.477861000 EDT

Arrival Time: Sep 13, 2021 08:51:47.496335000 EDT

Difference : 0.496335000-0.477861000 = 0.018474 sec



The image shows two screenshots of the Wireshark network protocol analyzer. The top screenshot displays a packet list with 13 packets, where packet 880 (HTTP 200 OK) is selected. The packet details pane shows the arrival time as Sep 13, 2021 08:51:47.496335000 EDT and the frame length as 540 bytes (4320 bits). The packet bytes pane shows the raw data in hexadecimal and ASCII.

The bottom screenshot displays the same packet list, but packet 877 (HTTP 200 OK) is selected. The packet details pane shows the arrival time as Sep 13, 2021 08:51:47.477861000 EDT and the frame length as 513 bytes (4104 bits). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
877	10.855468	10.8.20.196	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-fi
880	10.873942	128.119.245.12	10.8.20.196	HTTP	540	HTTP/1.1 200 OK (text/html)
884	10.920512	10.8.20.196	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
886	10.938805	128.119.245.12	10.8.20.196	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1176	13.476063	10.8.20.196	8.253.132.121	HTTP	366	GET /filestreamingservice/files/01ee1
1180	13.479551	8.253.132.121	10.8.20.196	HTTP	84	HTTP/1.1 200 OK
1213	13.510906	10.8.20.196	8.253.131.111	HTTP	471	GET /filestreamingservice/files/01ee1
1216	13.512382	10.8.20.196	8.253.132.121	HTTP	471	GET /filestreamingservice/files/01ee1
1219	13.514018	8.253.131.111	10.8.20.196	HTTP	417	HTTP/1.1 403 Forbidden (text/html)
1222	13.516113	8.253.132.121	10.8.20.196	HTTP	417	HTTP/1.1 403 Forbidden (text/html)
1355	13.965746	10.8.20.196	67.26.247.254	HTTP	487	GET /filestreamingservice/files/01ee1
1358	13.966222	10.8.20.196	8.240.25.254	HTTP	487	GET /filestreamingservice/files/01ee1

4. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)?
 > 128.119.245.12

simran lab 1.pcapng

http

No.	Time	Source	Destination	Protocol	Length	Info
877	10.855468	10.8.20.196	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-fi
880	10.873942	128.119.245.12	10.8.20.196	HTTP	540	HTTP/1.1 200 OK (text/html)
884	10.920512	10.8.20.196	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
886	10.938805	128.119.245.12	10.8.20.196	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1176	13.476063	10.8.20.196	8.253.132.121	HTTP	366	GET /filestreamingservice/files/01ee1
1180	13.479551	8.253.132.121	10.8.20.196	HTTP	84	HTTP/1.1 200 OK
1213	13.510906	10.8.20.196	8.253.131.111	HTTP	471	GET /filestreamingservice/files/01ee1
1216	13.512382	10.8.20.196	8.253.132.121	HTTP	471	GET /filestreamingservice/files/01ee1
1219	13.514018	8.253.131.111	10.8.20.196	HTTP	417	HTTP/1.1 403 Forbidden (text/html)
1222	13.516113	8.253.132.121	10.8.20.196	HTTP	417	HTTP/1.1 403 Forbidden (text/html)
1355	13.965746	10.8.20.196	67.26.247.254	HTTP	487	GET /filestreamingservice/files/01ee1
1358	13.966222	10.8.20.196	8.240.25.254	HTTP	487	GET /filestreamingservice/files/01ee1

▼ Frame 877: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF_{DB803BE2-E17E-4B3C-BAC3-C6E100926EDF}

- Interface id: 0 (\Device\NPF_{DB803BE2-E17E-4B3C-BAC3-C6E100926EDF})
- Encapsulation type: Ethernet (1)
- Arrival Time: Sep 13, 2021 08:51:47.477861000 EDT
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1631537507.477861000 seconds
- [Time delta from previous captured frame: 0.000001000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 10.855468000 seconds]
- Frame Number: 877
- Frame Length: 513 bytes (4104 bits)
- Capture Length: 513 bytes (4104 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:tcp:http]

0000	00 2c c8 59 ec bf 14 b3 1f 17 24 5c 08 00 45 00	.,Y.... ..\$..E.
0010	01 f3 fb ed 40 00 80 06 68 c7 0a 08 14 c4 80 77	...@... h.....w
0020	f5 0c cd 9d 00 50 5a b9 9c 53 7f d7 88 bc 50 18PZ. .S....P.
0030	04 00 5c b0 00 00 47 45 54 20 2f 77 69 72 65 73	..\\...GE T /wires
0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77	hark-lab s/HTTP-w
0050	69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68	reshark -file1.h
0060	74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f	tml HTTP /1.1..Ho
0070	73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73	st: gaia .cs.umas

5. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.

/Users/simranshrestha/Downloads/simran lab 1.pcapng 36987 total packets, 197 shown

No.	Time	Source	Destination	Protocol	Length	Info
877	10.855468	10.8.20.196	128.119.245.12	HTTP	513	GET /

wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 877: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface
\\Device\\NPF_{DB803BE2-E17E-4B3C-BAC3-C6E100926EDF}, id 0
Ethernet II, Src: Dell_17:24:5c (14:b3:1f:17:24:5c), Dst: Cisco_59:ec:bf (00:2c:c8:59:ec:bf)
Internet Protocol Version 4, Src: 10.8.20.196, Dst: 128.119.245.12
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 499
Identification: 0xfbed (64493)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x68c7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.8.20.196
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 52637, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
Hypertext Transfer Protocol

/Users/simranshrestha/Downloads/simran lab 1.pcapng 36987 total packets, 197 shown

No.	Time	Source	Destination	Protocol	Length	Info
880	10.873942	128.119.245.12	10.8.20.196	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 880: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
\\Device\\NPF_{DB803BE2-E17E-4B3C-BAC3-C6E100926EDF}, id 0
Ethernet II, Src: Cisco_59:ec:bf (00:2c:c8:59:ec:bf), Dst: Dell_17:24:5c (14:b3:1f:17:24:5c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.20.196
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 526
Identification: 0x9d6f (40303)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 49
Protocol: TCP (6)
Header Checksum: 0x162b [validation disabled]
[Header checksum status: Unverified]
Source Address: 128.119.245.12
Destination Address: 10.8.20.196
Transmission Control Protocol, Src Port: 80, Dst Port: 52637, Seq: 1, Ack: 460, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)