

Lab 1: Wireshark

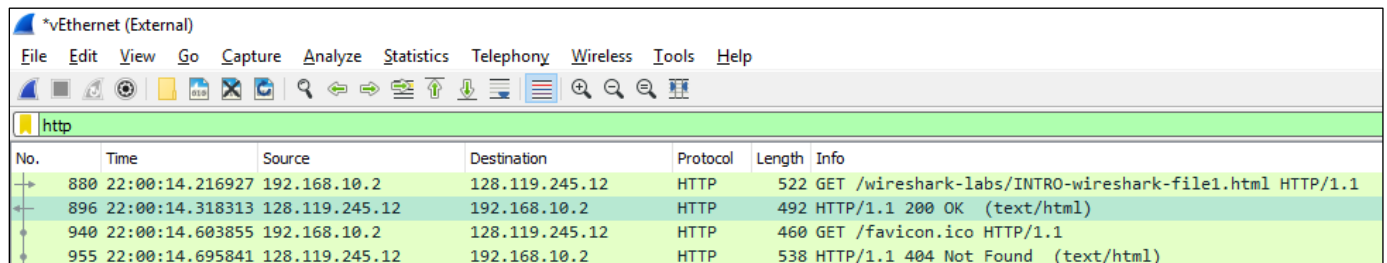
- 1) List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

HTTP, DNS, TCP

- 2) 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 packet listing 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*.)

22:00:14.318313 – 22:00:14.216926 = 0.101386 sec

It took 0.101386 sec from when the HTTP GET message was sent until the HTTP OK reply was received.



No.	Time	Source	Destination	Protocol	Length	Info
880	22:00:14.216927	192.168.10.2	128.119.245.12	HTTP	522	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
896	22:00:14.318313	128.119.245.12	192.168.10.2	HTTP	492	HTTP/1.1 200 OK (text/html)
940	22:00:14.603855	192.168.10.2	128.119.245.12	HTTP	460	GET /favicon.ico HTTP/1.1
955	22:00:14.695841	128.119.245.12	192.168.10.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- 3) What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the Internet address of your computer?

The internet address of gaia.cs.umass.edu is 128.119.245.12, which is the destination IP address.
The internet address of my computer is 192.168.10.2, which is the source IP address.

*vEthernet (External)						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
http						
No.	Time	Source	Destination	Protocol	Length	Info
880	22:00:14.216927	192.168.10.2	128.119.245.12	HTTP	522	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
896	22:00:14.318313	128.119.245.12	192.168.10.2	HTTP	492	HTTP/1.1 200 OK (text/html)
940	22:00:14.603855	192.168.10.2	128.119.245.12	HTTP	460	GET /favicon.ico HTTP/1.1
955	22:00:14.695841	128.119.245.12	192.168.10.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 880: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a), Dst: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08)
> Internet Protocol Version 4, Src: 192.168.10.2, 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: 508
Identification: 0x6d8e (28046)
> Flags: 0x4000, Don't fragment
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.10.2
Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 11422, Dst Port: 80, Seq: 1, Ack: 1, Len: 468
> Hypertext Transfer Protocol

- 4) Screenshot the two HTTP messages (GET and OK) referred to in question 2 above. Make sure to include all pertinent information in the screenshot (Time field, Internet addresses, etc). Paste these screenshots into your lab report.

*vEthernet (External)

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

http

No.	Time	Source	Destination	Protocol	Length	Info
880	22:00:14.216927	192.168.10.2	128.119.245.12	HTTP	522	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
896	22:00:14.318313	128.119.245.12	192.168.10.2	HTTP	492	HTTP/1.1 200 OK (text/html)
940	22:00:14.603855	192.168.10.2	128.119.245.12	HTTP	460	GET /favicon.ico HTTP/1.1
955	22:00:14.695841	128.119.245.12	192.168.10.2	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 955: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface 0
> Ethernet II, Src: AsustekC_c6:cb:08 (1c:b7:2c:c6:cb:08), Dst: Tp-LinkT_61:1c:8a (18:d6:c7:61:1c:8a)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.10.2
> Transmission Control Protocol, Src Port: 80, Dst Port: 11422, Seq: 439, Ack: 875, Len: 484

Hypertext Transfer Protocol

HTTP/1.1 404 Not Found\r\n

Date: Sun, 22 Sep 2019 05:00:14 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Content-Length: 209\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n
[HTTP response 2/2]
[Time since request: 0.091986000 seconds]
[\[Prev request in frame: 880\]](#)
[\[Prev response in frame: 896\]](#)
[\[Request in frame: 940\]](#)
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 209 bytes

> Line-based text data: text/html (7 lines)

0030	00 f5 e4 a2 00 00 48 54 54 50 2f 31 2e 31 20 34HT TP/1.1 4
0040	30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 44 61	04 Not F ound..Da
0050	74 65 3a 20 53 75 6e 2c 20 32 32 20 53 65 70 20	te: Sun, 22 Sep
0060	32 30 31 39 20 30 35 3a 30 30 3a 31 34 20 47 4d	2019 05: 00:14 GM
0070	54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68	T..Serve r: Apach
0080	65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29	e/2.4.6 (CentOS)
0090	20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 32 6b 2d	OpenSSL /1.0.2k-
00a0	66 69 70 73 20 50 48 50 2f 35 2e 34 2e 31 36 20	fips PHP /5.4.16
00b0	6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 31 30 20	mod_perl /2.0.10
00c0	50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 0a 43 6f	Perl/v5. 16.3..Co
00d0	6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 32 30	ntent-Le ngth: 20
00e0	39 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 74	9..Keep- Alive: t
00f0	69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 39 39	imeout=5 , max=99
0100	0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65	..Connec tion: Ke
0110	65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e	ep-Alive ..Conten
0120	74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d	t-Type: text/htm
0130	6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38	l; chars et=iso-8
0140	38 35 39 2d 31 0d 0a 0d 0a 3c 21 44 4f 43 54 59	859-1... <!DOCTYPE
0150	50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22	PE HTML PUBLIC "
0160	2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d	-//IETF/ /DTD HTM

Text item (text), 24 bytes