

Wireshark Lab 2 - HTTP

IT 520-A – Enterprise Infrastructure & Networks
Due Date: 09/17/18 (Handed in at the beginning of class)

Instructions:

1. Part 1: Start up your web browser.
2. 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).
3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>
5. Stop Wireshark packet capture.

Questions:

(For each of these questions, take a screenshot of Wireshark, and attach it to your answer).

1. Is your browser running HTTP version 1.0 or 1.1?
2. When was the HTML file that you are retrieving last modified at the server?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What languages (if any) does your browser indicate that it can accept to the server?
5. When was the HTML file that you are retrieving last modified at the server?

Don't forget to save your Wireshark Lab file.

Q#1



Source	Destination	Protocol	Length	Info
13 192.168.1.182	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
15 128.119.245.12	192.168.1.182	HTTP	540	HTTP/1.1 200 OK (text/html)
16 192.168.1.182	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
17 128.119.245.12	192.168.1.182	HTTP	538	HTTP/1.1 404 Not Found (text/html)

on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
telCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)
rsion 4, Src: 192.168.1.182, Dst: 128.119.245.12
Protocol, Src Port: 57095, Dst Port: 80, Seq: 1, Ack: 1, Len: 425

80

425]

1 (relative sequence number)

number: 426 (relative sequence number)]

number: 1 (relative ack number)

Length: 20 bytes (5)

, ACK)

: 68

size: 17408]

ing factor: 256]

5 00 e1 8c c5 a0 c6 08 00 45 00 H]6.....E.
3 80 06 75 5f c0 a8 01 b6 80 77 ..K.@...u_.....w
3 3f 70 40 55 3c b1 f8 aa 50 18P?p@U<...P.
3 47 45 54 20 2f 77 69 72 65 73 ..D/d..GE T /wires
3 61 62 73 2f 48 54 50 2d 77 hark-lab s/HTTP-w
1 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h



Lab 2.pcapng

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
------	------	------	----	---------	---------	------------	-----------	----------	-------	------

No.	Time	Source	Destination	Protocol	Length	Info
795	16:33:37.391687	128.119.245.12	192.168.1.182	HTTP	538	HTTP/1.1 404 Not Found (text/html)
793	16:33:37.367752	192.168.1.182	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
790	16:33:37.310915	128.119.245.12	192.168.1.182	HTTP	540	HTTP/1.1 200 OK (text/html)
787	16:33:37.286643	192.168.1.182	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

- ▼ Hypertext Transfer Protocol

✓ HTTP/1.1 200 OK\r\n

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Sun, 16 Sep 2018 20:33:38 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

Last-Modified: Sun, 16 Sep 2018 05:59:02 GMT\r\n

ETag: "80-575f6c0e49783"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

```
Keep-Alive: timeout=5, max=100\r\n
```

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

 $|r|n$

[HTTP response 1/2]

[Time since request: 0.024272000 seconds]

[Request in frame: 787]

[Next request in frame: 793]

0000	00	e1	8c	c5	a0	c6	48	5d	36	a8	f8	d6	08	00	45	00HJ	6.....E
0010	02	0e	53	b7	40	00	35	06	b8	50	80	77	f5	0c	c0	a8S@	5.....P.W

Frame is marked in the GUI (frame.marked)

Type here to search

Packets: 890 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)

Profile: Default

ENG 8:09 PM

TN 9/16/2018

Q.3



my computer IP
server IP

Source	Destination	Protocol	Length	Info
13 192.168.1.182	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
15 128.119.245.12	192.168.1.182	HTTP	540	HTTP/1.1 200 OK (text/html)
16 192.168.1.182	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
17 128.119.245.12	192.168.1.182	HTTP	538	HTTP/1.1 404 Not Found (text/html)

on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0

\Device\NPF_{32FF1456-3E0F-4D64-858E-B50969B7A4B9})

on: Ethernet (1)

16, 2018 16:33:37.286643000 Eastern Daylight Time

this packet: 0.000000000 seconds]

30017.286643000 seconds

previous captured frame: 0.000282000 seconds]

previous displayed frame: 0.000000000 seconds]

since or first frame: 121.885007000 seconds]

bytes (3832 bits)

79 bytes (3832 bits)

False]

: False]

me: eth:ethertype:ip:tcp:http]

me: HTTP]

ing: http || tcp.port == 80 || http2]

telCor_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon_a8:f8:d6 (48:5d:36:a8:f8:d6)

zon_a8:f8:d6 (48:5d:36:a8:f8:d6)

:5:a0:c6 (00:e1:8c:c5:a0:c6)

00 e1 8c c5 a0 c6 08 00 45 00 H]6... ..E.

tion 4 (ip), 20 bytes

search

[illegible]