Moudle Alhousainan

Due Date: 09/17/18 (Handed in at the beginning of class)

- Wireshark Lab 2 HTTP

  Wedde with a restriction

  IT 520-A Enterprise Infrastracture & Manded in at the Due Date: 09/17/18 (Handed in at the Constitution)

  Recombility of the Constitution of the Constitut 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: <a href="http://gaia.cs.umass.edu/wireshark-">http://gaia.cs.umass.edu/wireshark-</a> labs/HTTP-wireshark-file1.html
  - 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.

-XX 479 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 538 HTTP/1.1 404 Not Found (text/html) 540 HTTP/1.1 200 OK (text/html) 450 GET /favicon.ico HTTP/1.1 Length Info Help Protocol HTTP Statistics Telephony Wireless Tools HTTP HTTP HTTP 1 ① ① 128.119.245.12 128.119.245.12 192.168.1.182 192.168.1.182 Destination 5 128.119.245.12 7 128.119.245.12 2 192.168.1.182 13 192.168.1.182 Capture Analyze 0 Source

telCor\_c5:a0:c6 (00:e1:8c:c5:a0:c6), Dst: Verizon\_a8:f8:d6 (48:5d:36:a8:f8:d6) on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0 Protocol, Src Port: 57095, Dst Port: 80, Seq: 1, Ack: 1, Len: 425 rsion 4, Src: 192.168.1.182, Dst: 128.119.245.12

425

(relative sequence number)] ( relative sequence number) nber: 426

(relative ack number) nber: 1

Length: 20 bytes (5)

ACK)

ing factor: 256] v size: 17408]

H]6.....E.

····P?p @U<···P. 8c c5 a0 c6 08 00 45 00 75 5f c0 a8 01 b6 80 77 40 55 3c b1 f8 aa 50 18 54 20 2f 77 69 72 65 73 3f 70 3 80 96

D/d GE T /wires hark-lab s/HTTP-w ireshark -file1.h 73 2f 48 54 54 50 2d 77 2d 66 69 6c 65 31 2e 68 47 45 61 62

3E0F-4D64-858E-B50969B7A4B9\_20180916163133\_a11184.pcapng



search









0





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





100

S# 2

ille: Defai	Lab 2.pcapng							10	×
Time Source 12 (25.33.7) 2016 State 12 (25.24.2) 12 (25.12.2) 12 (25.13.2) 2016 State 11 (25.24.12.2) 12 (25.24.12.2)	iew Go Capture Analyze	Telephony			d				
The   Section   Protect   Length   Le	* * * * * * * * * * * * * * * * * * *	⊕*	1						
Time   Percent Line	http						X		+
939 16:33:37:325667 123.113.245.12  939 16:33:37.34667 123.113.255.12  939 16:33:37.34667 123.113.255.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.34667 132.113.245.12  939 16:33:37.3467 132.113.245  1181113.245.12  1181113.24	Time	Destination	-A		ength Infe				
939 16:33:37. 2395.12 23.13 2455.12 HTPP 549 GET /Adreshark-filed.html HTP/1.1 200 (text/html)   787 16:33:37. 2395.12 123.13 245.12 HTTP 540 HTP/1.1 200 (text/html)   787 16:33:37. 2395.13 123.13 245.12 HTTP 540 HTP/1.1 200 (text/html)   787 16:33:37. 2395.13 123.13 245.12 HTTP 540 HTP/1.1 200 (text/html)   787 16:33:37. 2395.13 123.13	795 16:33:37.391687 128.119.245.12	192.168.1.182	H	TP	538 HT	TP/1.1 404 Not F.	ound (text/html)		
18.2   16.3   18.3   19.3   18.3   19.3   18.3   19.3   18.3   19.3   18.3   19.3   18.3   19.3   18.3   19.3   18.3   19.3   19.3   18.3   19.3	793 16:33:37.367752 192.168.1.182	128.119.245.12		TP	450 GE	/favicon.ico H	ПР/1.1		
######################################	790 16:33:37.310915 128.119.245.12	192.168.1.182	H	TP	540 HT	P/1.1 200 OK (	text/html)		
######################################	787 16:33:37.286643 192.168.1.182	128.119.245.12		dT.	479 GE	/wireshark-lab	s/HTTP-wireshark-file1.html HTTP/1.1		
######################################	Hypertext Transfer Protocol								
Expert Info (chat/Sequence): HTTP/1.1 200 OK\r\n]   Response Version: HTTP/1.1 200 OFFER Sequence Seq	→ HTTP/1.1 200 OK\r\n								
Response Version: HTTP/1.1 Status Code: 200 (Status Code: 200 Response Phrase: 0K Response Version: 16 Sep 2018 0S:59:92 GNT\n\n\n Response Phrase: 0K Response VII Response VI	<pre>\ [Expert Info (Chat/Sequence): HTTP/1</pre>	1.1 200 OK\r\n]							
Status Code: 2006   Status Code Description: 0K    Response Phrase: Na. 16 Sep 2018 20:33:36 GMT\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	Response Version: HTTP/1.1								
[Status Code Description: OK] Response Phrase: OK Response LOGIN Respon	Status Code: 200								
Response Phrase: 0K  Babter Sun, 16 Sep 2018 20:33:38 GMT\n\n  Bast-Modifical Sun, 16 Sep 2018 95:55:02 GMT\n\n  Bast-Modifical Sun, 16 Sep 2018 95:55:02 GMT\n\n  Elag: "28-575fc6e49793"\n\n  Flag: "28-575fc6e49793"\n\n  Content-Type: text/html; charset-UFF-8\n\n  Connection: Keep-Alive'\n\n  Connection: Keep-Alive'\n\n  Content-Type: text/html; charset-UFF-8\n\n  Flam: 22-272000 seconds]  [HIP response 1/2]  [Him since request: 0.224272000 seconds]  [Him response 1/2]  [Him since request: 1 frame: 793]  [Hext request: 1 frame: 793]  [Mext request: 1 frame: 794]  [Mext request: 1 frame: 794]  [Mext request: 1 frame: 794]  [Mext reques	[Status Code Description: OK]	1							
Date: Sun, 16 Sep 2018 2013:38 GMT\n\n  Server. Abache/2.4.6 (CentOS) OpenSSL/1.0.2.0.10 Perl/V5.16.3\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n  Accept-Ranges: bytes\n\n  Accept-Ranges: bytes\n\n  Accept-Ran	Response Phrase: OK								
Server: Apacha/2.4.6 (centoS) OpenSSI/1.0.2k-fips PHP/5.4.16 mod_perl/V5.16.3k\n     Last-Modfied: Sin, 16 Sep 2018 05:59:02 GMT\n\n     Last-Modfied: Sin, 16 Sep 2018 05:59:02 GMT\n\n     Etga: "Ba-575f60e49783"\n\n     Etga: "Ba-575f60e49783"\n\n     Content-Length: 128\n\n     Content-Length: 128\n\n     Content-Length: 128\n\n     Content-Length: 128\n\n     Content-Type: text/html; charset=UTF-8\n\n     Content-Type: text/html; charset=U	Date: Sun, 16 Sep 2018 20:33:38 GMT\r\	ln							
Last-Modified: Sun, 16 Sep 2018 05:59:02 GMT\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\	Server: Apache/2.4.6 (CentOS) OpenSSL/	1.0.2k-fips PHP/5	.4.16 mod	per1/.	2.9.10 P	er1/v5.16.3/r/n			
### ETag: "88-575f60849783"\r\n Accept.Ranges: bytes/r\n Accept.Ranges: bytes/r\n Content.Length: 128\r\n Connection: Keep-Alive\r\n Content.Type: text/html; charset=UTF-8\r\n Content.Type=UTF-8\r\n Content.Type=UTF-8\	Last-Modified: Sun, 16 Sep 2018 05:59:	:02 GMT/r/n							
Accept-Ranges: bytes\r\n Content-Length: 128\r\n Content-Length: 128\r\n Content-Length: 128\r\n Content-Length: 128\r\n Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive\r\n Connection: Keep-Alive\r\n Connection: Keep-Alive\r\n Connection: Keep-Alive\r\n IHTP response 1/2] [HITP response 1/2] [Filme since request: 0.04272000 seconds] [Filme since request: 0.04477200 seconds] [Filme since request: 0.044772000 seconds] [Filme since request: 0.044772000 seconds] [Filme since request: 0.044772000 seconds] [Filme since request: 0.04472000 seconds] [Filme since request: 0.044772000 seconds] [F	ETag: "80-575f6c0e49783"\r\n								
Content-Length: 128\r\n  Keep-Alive: timeout=5, max=100\r\n  Connection: Keep-Alive: timeout=5, max=100\r\n  Content-Type: text/html; charset=UTF-8\r\n  Content-Type: text/html  Conten	Accept-Ranges: bytes/r\n								
Keep-Alive: timeout=5, max=100\r\n         Connection: Keep-Alive\r\n         Connection: Keep-Alive\r\n         Connection: Keep-Alive\r\n         Content-Type: text/html; charset=UTF-8\r\n         (hTP         Image: Content-Type: text/html; charset=UTF-8\r\n         (hTP         Image: Content-Type: text/html; charset=UTF-8\r\n         (hTP         Image: Content-Type: text/html; charset=UTF-8\r\n	<pre>Content-Length: 128\r\n</pre>								
Connection: Keep-Alive\r\n Content-Type: text/html; charset=UTF-8\r\n Content-Type: text/html Content-Type: text/	Keep-Alive: timeout=5, max=100/r/n								
Content-Type: text/html; charset=UTF-8\r\n  r\n	Connection: Keep-Alive\r\n								
[HTTP response 1/2]	Content-Type: text/html; charset=UTF-8	3/11/11							Ī
[HTTP response 1/2] [Time since request: 0.024272000 seconds] [Time since request: 0.024272000 seconds] [Next request in frame: 787] [Next request in frame: 787] [Next request in frame: 783]  00 e1 8c c5 a0 c6 48 5d 36 a8 f8 d6 08 00 45 00 00 00 00 00 00 00 00 00 00 00 00 00	\r\n								
[Time since request: 0.024272000 seconds] [Request in frame: 787] [Next request in frame: 787] [Next request in frame: 783]  00 e1 8c c5 a0 c6 48 5d 36 a8 f8 d6 08 00 45 00 c0 a8S.@.5. P.W  Profile: Defan: Packets: 890 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)  Frame is marked in the GUI (frame.marked)	[HTTP response 1/2]								
Request in frame: 787]   Next request in frame: 793]   OB e1 8c c5 a0 c6 48 5d 36 a8 f8 d6 08 00 45 00 c0 a8	[Time since request: 0.024272000 second	[spi							
Next request in frame: 793	[Request in frame: 787]								
60 e1 8c c5 a0 c6 48 5d 36 a8 f8 d6 08 60 45 00	[Next request in frame: 793]								>
Frame is marked in the GUI (frame.marked)  Packets: 890 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)	00 e1 8c c5 a0 c6 48 5d 02 0e 53 b7 40 00 35 06		H] 6	· · · · · · · · · · · · · · · · · · ·					<>
							Packets: 890 · Displayed: 4 (0.4%) · Dropped: 0 (0.0%)		: Defau

9

479 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1 540 HTTP/1.1 200 OK (text/html) 450 GET /favicon.ico HTTP/1.1 Length Info Help Protocol Tools HTTP HTTP HTTP Wireless 1 0 128.119.245.12 128.119.245.12 ⊕" 192.168.1.182 Telephony Destination Statistics 5 128.119.245.12 3 192, 168, 1, 182 2 192.168.1.182 Capture Analyze Source

538 HTTP/1.1 404 Not Found (text/html)

HTTP

192.168.1.182

7 128.119.245.12

on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0 Device\NPF\_{32FF1456-3E0F-4D64-858E-B50969B7A4B9})

3: Ethernet (1)

16, 2018 16:33:37.286643000 Eastern Daylight Time

is packet: 0.00000000 seconds]

30017.286643000 seconds

previous captured frame: 0.000282000 seconds]

previous displayed frame: 0.00000000 seconds]

ence or first frame: 121.885007000 seconds]

bytes (3832 bits)

79 bytes (3832 bits)

False

: False

ne: eth:ethertype:ip:tcp:http]

ne: 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)

8c c5 a0 c6 08 00 45 00

00 e1

H]6....E.

sion 4 (ip), 20 bytes

search



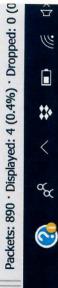






0





100

