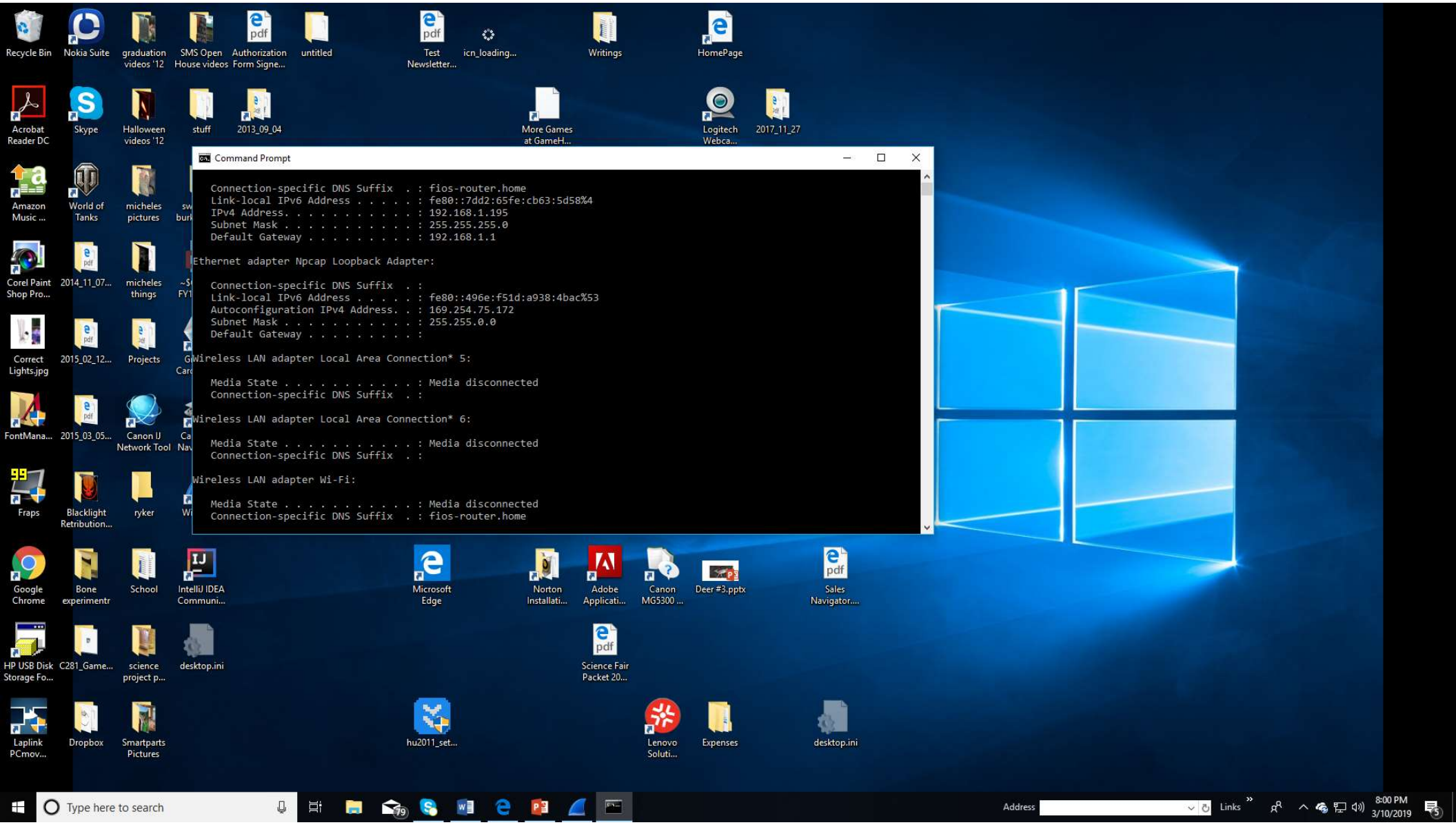
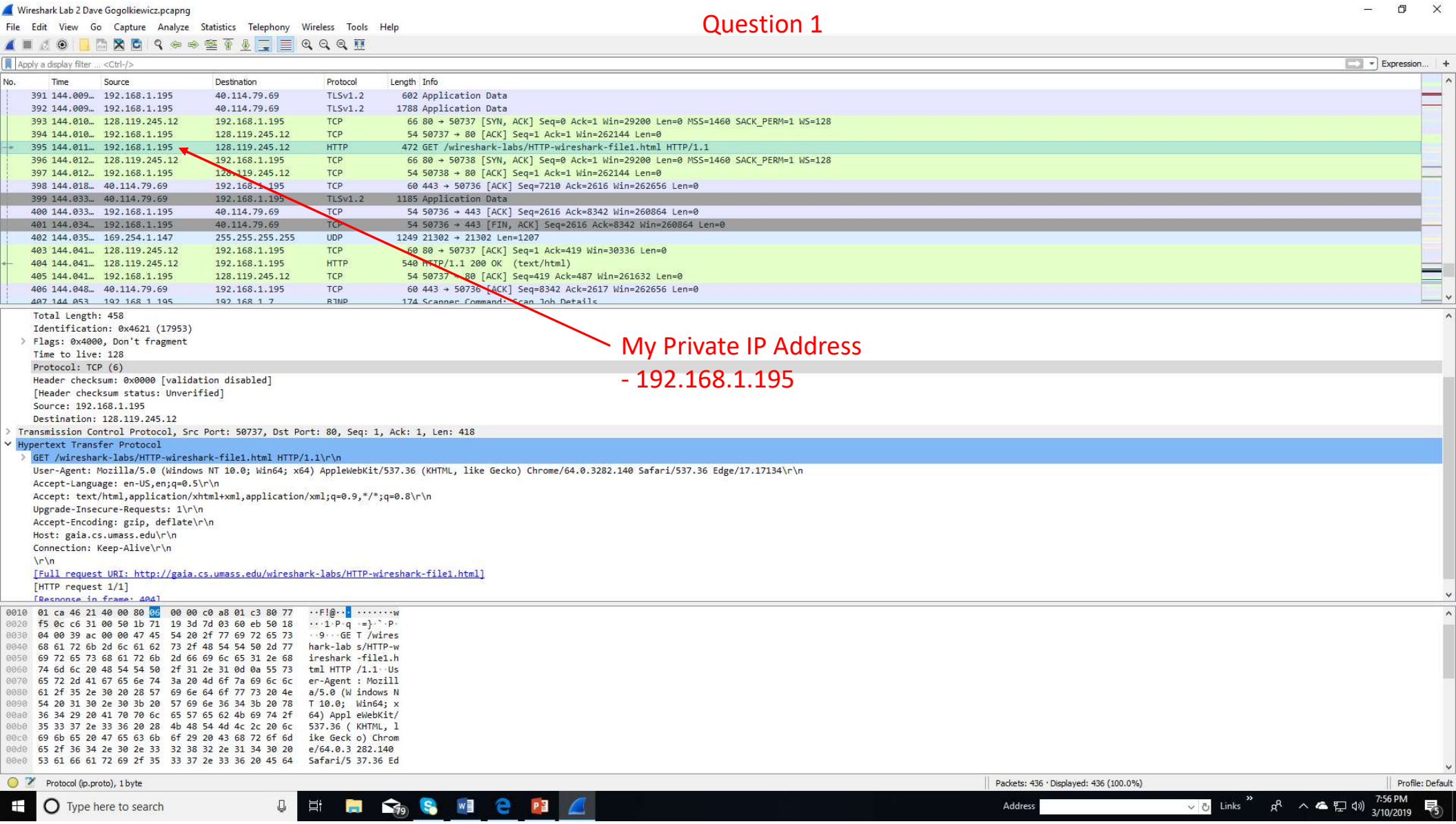
Wireshark Lab 4 - IP

IT 520 –A – Enterprise Infrastructure & Networks

David Gogolkiewicz


Command Prompt
Connection-specific DNS Suffix . : fios-router.home
Link-local IPv6 Address . . . . . : fe80::7dd2:65fe:cb63:5d58%4
IPv4 Address. . . . . : 192.168.1.195
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
Ethernet adapter Npcap Loopback Adapter:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::496e:f51d:a938:4bac%53
Autoconfiguration IPv4 Address. . : 169.254.75.172
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
Wireless LAN adapter Local Area Connection* 5:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Local Area Connection* 6:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Wireless LAN adapter Wi-Fi:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : fios-router.home
Recycle Bin
Nokia Suite
graduation videos '12
SMS Open House videos
Authorization Form Signe...
untitled
Test Newsletter...
icn_loading...
Writings
HomePage
Acrobat Reader DC
Skype
Halloween videos '12
stuff
2013_09_04
More Games at GameH...
Logitech Webca...
2017_11_27
Amazon Music ...
World of Tanks
micheles pictures
Corel Paint Shop Pro...
2014_11_07...
micheles things
Correct Lights.jpg
2015_02_12...
Projects
FontMana...
2015_03_05...
Canon IJ Network Tool
Fraps
Blacklight Retribution...
ryker
Google Chrome
Bone experimentr
School
IntelliJ IDEA Communi...
Microsoft Edge
Norton Installati...
Adobe Applicati...
Canon MG5300 ...
Deer #3.pptx
Sales Navigator....
HP USB Disk Storage Fo...
C281_Game...
science project p...
desktop.ini
Science Fair Packet 20...
Laplink PCmov...
Dropbox
Smartparts Pictures
hu2011_set...
Lenovo Soluti...
Expenses
desktop.ini
Type here to search
Address
Links
8:00 PM
3/10/2019


Wireshark Lab 2 Dave Gogolkiewicz.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Question 1
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
391 144.009… 192.168.1.195 40.114.79.69 TLSv1.2 602 Application Data
392 144.009… 192.168.1.195 40.114.79.69 TLSv1.2 1788 Application Data
393 144.010… 128.119.245.12 192.168.1.195 TCP 66 80 → 50737 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
394 144.010… 192.168.1.195 128.119.245.12 TCP 54 50737 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
395 144.011… 192.168.1.195 128.119.245.12 HTTP 472 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
396 144.012… 128.119.245.12 192.168.1.195 TCP 66 80 → 50738 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
397 144.012… 192.168.1.195 128.119.245.12 TCP 54 50738 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
398 144.018… 40.114.79.69 192.168.1.195 TCP 60 443 → 50736 [ACK] Seq=7210 Ack=2616 Win=262656 Len=0
399 144.033… 40.114.79.69 192.168.1.195 TLSv1.2 1185 Application Data
400 144.033… 192.168.1.195 40.114.79.69 TCP 54 50736 → 443 [ACK] Seq=2616 Ack=8342 Win=260864 Len=0
401 144.034… 192.168.1.195 40.114.79.69 TCP 54 50736 → 443 [FIN, ACK] Seq=2616 Ack=8342 Win=260864 Len=0
402 144.035… 169.254.1.147 255.255.255.255 UDP 1249 21302 → 21302 Len=1207
403 144.041… 128.119.245.12 192.168.1.195 TCP 60 80 → 50737 [ACK] Seq=1 Ack=419 Win=30336 Len=0
404 144.041… 128.119.245.12 192.168.1.195 HTTP 540 HTTP/1.1 200 OK (text/html)
405 144.041… 192.168.1.195 128.119.245.12 TCP 54 50737 → 80 [ACK] Seq=419 Ack=487 Win=261632 Len=0
406 144.048… 40.114.79.69 192.168.1.195 TCP 60 443 → 50736 [ACK] Seq=8342 Ack=2617 Win=262656 Len=0
407 144.053… 192.168.1.195 192.168.1.7 BJNP 174 Scanner Command: Scan Job Details
Total Length: 458
Identification: 0x4621 (17953)
Flags: 0x4000, Don't fragment
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.195
Destination: 128.119.245.12
Transmission Control Protocol, Src Port: 50737, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 404]
My Private IP Address
- 192.168.1.195
0010 01 ca 46 21 40 00 80 06 00 00 c0 a8 01 c3 80 77 ··F!@··· ·······w
0020 f5 0c c6 31 00 50 1b 71 19 3d 7d 03 60 eb 50 18 ···1·P·q ·=}·`·P·
0030 04 00 39 ac 00 00 47 45 54 20 2f 77 69 72 65 73 ··9···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 55 73 tml HTTP /1.1··Us
0070 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
0080 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e a/5.0 (W indows N
0090 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 T 10.0; Win64; x
00a0 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 64) Appl eWebKit/
00b0 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l
00c0 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Geck o) Chrom
00d0 65 2f 36 34 2e 30 2e 33 32 38 32 2e 31 34 30 20 e/64.0.3 282.140
00e0 53 61 66 61 72 69 2f 35 33 37 2e 33 36 20 45 64 Safari/5 37.36 Ed
Protocol (ip.proto), 1 byte
Packets: 436 · Displayed: 436 (100.0%)
Profile: Default
Type here to search
Address
Links
7:56 PM
3/10/2019

Wireshark Lab 2 Dave Gogolkiewicz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 2

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
127	46.728328	198.91.36.196	192.168.1.195	TLSv1.2	171	Application Data
128	46.728400	192.168.1.195	198.91.36.196	TCP	54	50578 → 443 [ACK] Seq=1 Ack=586 Win=1018 Len=0
129	47.060074	192.168.1.1	239.255.255.250	SSDP	419	NOTIFY * HTTP/1.1
130	47.060403	192.168.1.1	239.255.255.250	SSDP	491	NOTIFY * HTTP/1.1
131	47.060644	192.168.1.1	239.255.255.250	SSDP	487	NOTIFY * HTTP/1.1
132	47.060646	192.168.1.1	239.255.255.250	SSDP	467	NOTIFY * HTTP/1.1
133	47.060972	192.168.1.1	239.255.255.250	SSDP	499	NOTIFY * HTTP/1.1
134	47.060973	192.168.1.1	239.255.255.250	SSDP	481	NOTIFY * HTTP/1.1
135	47.061242	192.168.1.1	239.255.255.250	SSDP	483	NOTIFY * HTTP/1.1
136	47.061243	192.168.1.1	239.255.255.250	SSDP	483	NOTIFY * HTTP/1.1
137	47.256805	54.236.106.22	192.168.1.195	HTTP	362	HTTP/1.1 504 Gateway Time-out (text/html)
138	47.257139	54.236.106.22	192.168.1.195	TCP	60	80 → 50733 [FIN, ACK] Seq=334 Ack=470 Win=30464 Len=0
139	47.257242	192.168.1.195	54.236.106.22	TCP	54	50733 → 80 [ACK] Seq=470 Ack=335 Win=65280 Len=0
140	47.257553	192.168.1.195	54.236.106.22	TCP	54	50733 → 80 [FIN, ACK] Seq=470 Ack=335 Win=65280 Len=0
141	47.271448	54.236.106.22	192.168.1.195	TCP	60	80 → 50733 [ACK] Seq=335 Ack=471 Win=30464 Len=0
142	47.391026	192.168.1.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
143	47.870268	192.168.1.195	BJNP	174	Scanner Command: Scan Job Details	

```
> Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
v Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 203
    Identification: 0x6bec (27628)
  v Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 2
    Protocol: UDP (17)
    Header checksum: 0x5a92 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.1
    Destination: 239.255.255.250
> User Datagram Protocol, Src Port: 60008, Dst Port: 1900
> Simple Service Discovery Protocol
```

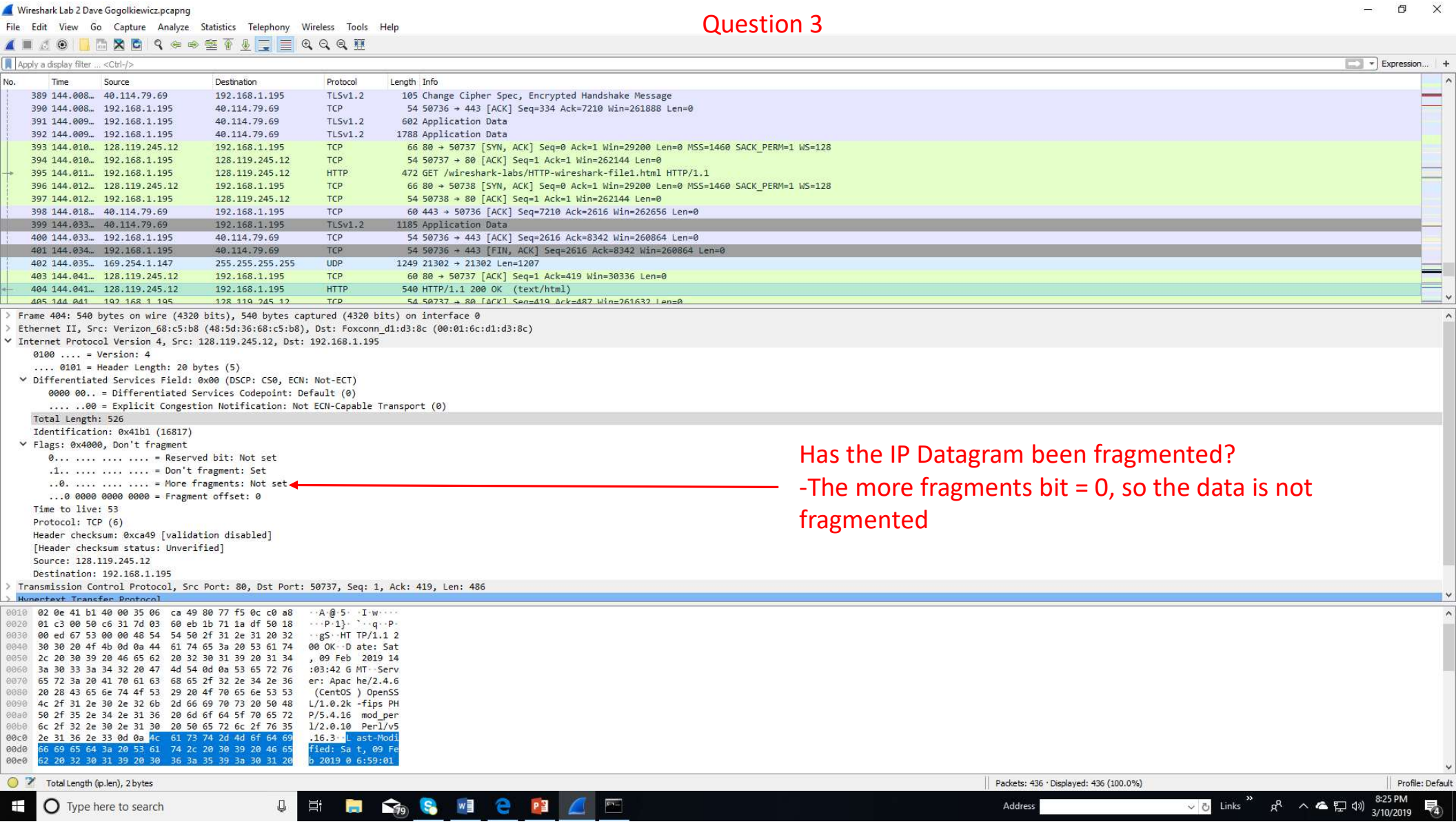
```
0000  01 00 5e 7f ff fa 48 5d  36 68 c5 b8 08 00 45 00   ··^···H] 6h····E·
0010  00 cb 6b ec 40 00 02 11  5a 92 c0 a8 01 01 ef ff   ··k·@··· Z·······
0020  ff fa ea 68 07 6c 00 b7  f7 59 4d 2d 53 45 41 52   ···h·l·· ·YM-SEAR
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d 0a 48   CH * HTT P/1.1··H
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32 35 35   OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e 3a 20   .250:190 0··MAN:
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72 22 0d   "ssdp:di scover"·
0070  0a 4d 58 3a 20 35 0d 0a  53 54 3a 20 73 73 64 70   ·MX: 5·· ST: ssdp
0080  3a 61 6c 6c 0d 0a 55 73  65 72 2d 41 67 65 6e 74   :all··Us er-Agent
0090  3a 20 4c 69 6e 75 78 2f  33 2e 31 34 20 55 70 6e   : Linux/ 3.14 Upn
00a0  70 2f 32 2e 30 20 62 68  72 2f 32 2e 30 0d 0a 43   p/2.0 bh r/2.0··C
00b0  50 46 4e 2e 55 50 4e 50  2e 4f 52 47 3a 20 47 72   PFN.UPNP .ORG: Gr
00c0  65 65 6e 77 61 76 65 20  63 6f 6e 74 72 6f 6c 20   eenwave  control
00d0  70 6f 69 6e 74 0d 0a 0d  0a                       point···· ·
```

What is the total length of the datagram?
-203 bytes

Total Length (ip.len), 2 bytes | Packets: 436 · Displayed: 436 (100.0%) | Profile: Default

Type here to search

Address Links 8:10 PM 3/10/2019


Wireshark Lab 2 Dave Gogolkiewicz.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Question 3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
389 144.008… 40.114.79.69 192.168.1.195 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
390 144.008… 192.168.1.195 40.114.79.69 TCP 54 50736 → 443 [ACK] Seq=334 Ack=7210 Win=261888 Len=0
391 144.009… 192.168.1.195 40.114.79.69 TLSv1.2 602 Application Data
392 144.009… 192.168.1.195 40.114.79.69 TLSv1.2 1788 Application Data
393 144.010… 128.119.245.12 192.168.1.195 TCP 66 80 → 50737 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
394 144.010… 192.168.1.195 128.119.245.12 TCP 54 50737 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
395 144.011… 192.168.1.195 128.119.245.12 HTTP 472 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
396 144.012… 128.119.245.12 192.168.1.195 TCP 66 80 → 50738 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
397 144.012… 192.168.1.195 128.119.245.12 TCP 54 50738 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
398 144.018… 40.114.79.69 192.168.1.195 TCP 60 443 → 50736 [ACK] Seq=7210 Ack=2616 Win=262656 Len=0
399 144.033… 40.114.79.69 192.168.1.195 TLSv1.2 1185 Application Data
400 144.033… 192.168.1.195 40.114.79.69 TCP 54 50736 → 443 [ACK] Seq=2616 Ack=8342 Win=260864 Len=0
401 144.034… 192.168.1.195 40.114.79.69 TCP 54 50736 → 443 [FIN, ACK] Seq=2616 Ack=8342 Win=260864 Len=0
402 144.035… 169.254.1.147 255.255.255.255 UDP 1249 21302 → 21302 Len=1207
403 144.041… 128.119.245.12 192.168.1.195 TCP 60 80 → 50737 [ACK] Seq=1 Ack=419 Win=30336 Len=0
404 144.041… 128.119.245.12 192.168.1.195 HTTP 540 HTTP/1.1 200 OK (text/html)
405 144.041… 192.168.1.195 128.119.245.12 TCP 54 50737 → 80 [ACK] Seq=419 Ack=487 Win=261632 Len=0
Frame 404: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.195
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 526
Identification: 0x41b1 (16817)
Flags: 0x4000, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 53
Protocol: TCP (6)
Header checksum: 0xca49 [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
Destination: 192.168.1.195
Transmission Control Protocol, Src Port: 80, Dst Port: 50737, Seq: 1, Ack: 419, Len: 486
Hypertext Transfer Protocol
0010 02 0e 41 b1 40 00 35 06 ca 49 80 77 f5 0c c0 a8 ··A·@·5· ·I·w····
0020 01 c3 00 50 c6 31 7d 03 60 eb 1b 71 1a df 50 18 ···P·1}· `··q··P·
0030 00 ed 67 53 00 00 48 54 54 50 2f 31 2e 31 20 32 ··gS··HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK··D ate: Sat
0050 2c 20 30 39 20 46 65 62 20 32 30 31 39 20 31 34 , 09 Feb 2019 14
0060 3a 30 33 3a 34 32 20 47 4d 54 0d 0a 53 65 72 76 :03:42 G MT··Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per
00b0 6c 2f 32 2e 30 2e 31 30 20 50 65 72 6c 2f 76 35 l/2.0.10 Perl/v5
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3··L ast-Modi
00d0 66 69 65 64 3a 20 53 61 74 2c 20 30 39 20 46 65 fied: Sa t, 09 Fe
00e0 62 20 32 30 31 39 20 30 36 3a 35 39 3a 30 31 20 b 2019 0 6:59:01
Has the IP Datagram been fragmented?
-The more fragments bit = 0, so the data is not fragmented
Total Length (ip.len), 2 bytes
Packets: 436 · Displayed: 436 (100.0%)
Profile: Default
Type here to search
Address
Links
8:25 PM
3/10/2019

Wireshark Lab 2 Dave Gogolkiewicz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 4

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
389	144.008…	40.114.79.69	192.168.1.195	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
390	144.008…	192.168.1.195	40.114.79.69	TCP	54	50736 → 443 [ACK] Seq=334 Ack=7210 Win=261888 Len=0
391	144.009…	192.168.1.195	40.114.79.69	TLSv1.2	602	Application Data
392	144.009…	192.168.1.195	40.114.79.69	TLSv1.2	1788	Application Data
393	144.010…	128.119.245.12	192.168.1.195	TCP	66	80 → 50737 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
394	144.010…	192.168.1.195	128.119.245.12	TCP	54	50737 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
395	144.011…	192.168.1.195	128.119.245.12	HTTP	472	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
396	144.012…	128.119.245.12	192.168.1.195	TCP	66	80 → 50738 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
397	144.012…	192.168.1.195	128.119.245.12	TCP	54	50738 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
398	144.018…	40.114.79.69	192.168.1.195	TCP	60	443 → 50736 [ACK] Seq=7210 Ack=2616 Win=262656 Len=0
399	144.033…	40.114.79.69	192.168.1.195	TLSv1.2	1185	Application Data
400	144.033…	192.168.1.195	40.114.79.69	TCP	54	50736 → 443 [ACK] Seq=2616 Ack=8342 Win=260864 Len=0
401	144.034…	192.168.1.195	40.114.79.69	TCP	54	50736 → 443 [FIN, ACK] Seq=2616 Ack=8342 Win=260864 Len=0
402	144.035…	169.254.1.147	255.255.255.255	UDP	1249	21302 → 21302 Len=1207
403	144.041…	128.119.245.12	192.168.1.195	TCP	60	80 → 50737 [ACK] Seq=1 Ack=419 Win=30336 Len=0
404	144.041…	128.119.245.12	192.168.1.195	HTTP	540	HTTP/1.1 200 OK (text/html)
405	144.041…	192.168.1.195	128.119.245.12	TCP	54	50737 → 80 [ACK] Seq=419 Ack=487 Win=261632 Len=0

```
> Frame 395: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface 0
> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
v Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 458
    Identification: 0x4621 (17953)
  v Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.195
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 50737, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
> Hypertext Transfer Protocol
```

How many bytes are in the IP header?
- 20 bytes

```
0000  48 5d 36 68 c5 b8 00 01  6c d1 d3 8c 08 00 45 00   H]6h···· l·····E·
0010  01 ca 46 21 40 00 80 06  00 00 c0 a8 01 c3 80 77   ··F!@··· ·······w
0020  f5 0c c6 31 00 50 1b 71  19 3d 7d 03 60 eb 50 18   ···1·P·q ·=}·`·P·
0030  04 00 39 ac 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···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 55 73   tml HTTP /1.1··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
0090  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00a0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
00b0  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
00c0  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
00d0  65 2f 36 34 2e 30 2e 33  32 38 32 2e 31 34 30 20   e/64.0.3 282.140
```

Header Length (ip.hdr_len), 1 byte | Packets: 436 · Displayed: 436 (100.0%) | Profile: Default

Type here to search

Address Links 8:28 PM 3/10/2019

Wireshark Lab 2 Dave Gogolkiewicz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Question 5

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
389	144.008…	40.114.79.69	192.168.1.195	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
390	144.008…	192.168.1.195	40.114.79.69	TCP	54	50736 → 443 [ACK] Seq=334 Ack=7210 Win=261888 Len=0
391	144.009…	192.168.1.195	40.114.79.69	TLSv1.2	602	Application Data
392	144.009…	192.168.1.195	40.114.79.69	TLSv1.2	1788	Application Data
393	144.010…	128.119.245.12	192.168.1.195	TCP	66	80 → 50737 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
394	144.010…	192.168.1.195	128.119.245.12	TCP	54	50737 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
395	144.011…	192.168.1.195	128.119.245.12	HTTP	472	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
396	144.012…	128.119.245.12	192.168.1.195	TCP	66	80 → 50738 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
397	144.012…	192.168.1.195	128.119.245.12	TCP	54	50738 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
398	144.018…	40.114.79.69	192.168.1.195	TCP	60	443 → 50736 [ACK] Seq=7210 Ack=2616 Win=262656 Len=0
399	144.033…	40.114.79.69	192.168.1.195	TLSv1.2	1185	Application Data
400	144.033…	192.168.1.195	40.114.79.69	TCP	54	50736 → 443 [ACK] Seq=2616 Ack=8342 Win=260864 Len=0
401	144.034…	192.168.1.195	40.114.79.69	TCP	54	50736 → 443 [FIN, ACK] Seq=2616 Ack=8342 Win=260864 Len=0
402	144.035…	169.254.1.147	255.255.255.255	UDP	1249	21302 → 21302 Len=1207
403	144.041…	128.119.245.12	192.168.1.195	TCP	60	80 → 50737 [ACK] Seq=1 Ack=419 Win=30336 Len=0
404	144.041…	128.119.245.12	192.168.1.195	HTTP	540	HTTP/1.1 200 OK (text/html)
405	144.041…	192.168.1.195	128.119.245.12	TCP	54	50737 → 80 [ACK] Seq=419 Ack=487 Win=261632 Len=0

```
> Frame 395: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits) on interface 0
> Ethernet II, Src: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c), Dst: Verizon_68:c5:b8 (48:5d:36:68:c5:b8)
v Internet Protocol Version 4, Src: 192.168.1.195, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 458
    Identification: 0x4621 (17953)
  v Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.195
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 50737, Dst Port: 80, Seq: 1, Ack: 1, Len: 418
> Hypertext Transfer Protocol
```

How many bytes are in the payload of the IP datagram?
- 438 bytes. There are 20 bytes in the IP header, and 458 bytes total length, this gives 438 bytes in the payload.

```
0000  48 5d 36 68 c5 b8 00 01  6c d1 d3 8c 08 00 45 00   H]6h···· l·····E·
0010  01 ca 46 21 40 00 80 06  00 00 c0 a8 01 c3 80 77   ··F!@··· ·······w
0020  f5 0c c6 31 00 50 1b 71  19 3d 7d 03 60 eb 50 18   ···1·P·q ·=}·`·P·
0030  04 00 39 ac 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···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 55 73   tml HTTP /1.1··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
0090  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00a0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
00b0  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
00c0  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
00d0  65 2f 36 34 2e 30 2e 33  32 38 32 2e 31 34 30 20   e/64.0.3 282.140
```

Header Length (ip.hdr_len), 1 byte | Packets: 436 · Displayed: 436 (100.0%) | Profile: Default

Type here to search

Address Links 8:30 PM 3/10/2019

C:\Users\dgogo\OneDrive\Masters\Computer Networking Course\Wireshark Lab 2 Dave Gogolkiewicz.pcapng 436 total packets, 7 shown

```
No.     Time           Source                Destination           Protocol Length Info
    404 144.041870     128.119.245.12        192.168.1.195         HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 404: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: Verizon_68:c5:b8 (48:5d:36:68:c5:b8), Dst: Foxconn_d1:d3:8c (00:01:6c:d1:d3:8c)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.195
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 526
    Identification: 0x41b1 (16817)
    Flags: 0x4000, Don't fragment
        0... .... .... .... = Reserved bit: Not set
        .1.. .... .... .... = Don't fragment: Set
        ..0. .... .... .... = More fragments: Not set
        ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 53
    Protocol: TCP (6)
    Header checksum: 0xca49 [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.195
Transmission Control Protocol, Src Port: 80, Dst Port: 50737, Seq: 1, Ack: 419, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```