Vlad Predovic

CS 372

7/3/2016

Lab 1

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

   HTTP , SSDP, QUIC

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*.)

   20:59:19.171977 → .105306 seconds
   20:59:19.277283

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?

   My Computer: 10.0.0.244 WWWnet.cs.umass.edu: 128.119.245.12

4. 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.

```
C:\Users\User\AppData\Local\Temp\wireshark_pcapng_D4DE60C9-7D7D-4B39-A28B-2BC06E2640F6_20160629203941_a12976 30519 total packets, 100 shown
30428 20:59:19.277283 128.119.245.12 10.0.0.244 HTTP 494 HTTP/1.1 200 OK (text/html)
Frame 30428: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0
Ethernet II, Src: 4a:1d:70:63:ca:5c (4a:1d:70:63:ca:5c), Dst: IntelCor_bf:b4:36 (5c:e0:c5:bf:b4:36)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.244
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 61583 (61583), Seq: 1, Ack: 440, Len: 440
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Thu, 30 Jun 2016 03:59:17 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
Last-Modified: Wed, 29 Jun 2016 05:59:01 GMT\r\n
ETag: "51-53664733a9fb5"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\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: 0.105306000 seconds]
[Request in frame: 30421]
[Next request in frame: 30438]
[Next response in frame: 30441]
Line-based text data: text/html
```

```
30421 20:59:19.171977 10.0.0.244 128.119.245.12 HTTP 493 GET /wireshark-labs/INTRO-wireshark-Frame 30421: 493 bytes on
wire (3944 bits), 493 bytes captured (3944 bits) on interface 0 file1.html HTTP/1.1 EInthteerrnneett IPIr,o tSocrco:l IVenrtesilCono
r4_,b f:Sbr4c:: 316 0(.05.c0:.e024:4c,5 :Dbfs:t:b 41:2368).,1 19D.s2t4: 5.41a2:1d:70:63:ca:5c (4a:1d:70:63:ca:5c)
HTryapenrsmteisxst iTonr aCnosfnetrr oPl rPortooctooclol, Src Port: 61583 (61583), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 439
GHEoTs t/: wgiareias.hacrs.k-ulmaabsss./IeNdTuR\Or-\nwireshark-file1.html HTTP/1.1\r\n CUopgnnraecdet-iIonn:s eckeuerep--
Raeliquvee\srt\s:n 1\r\n AUcsceer-pAt:g entet:x t/Mhotzimll,laa/p5p.l0i c(aWtiinodn/owxhs tNmTl +1x0m.l,0;a pWpOlWi6c4a)t
iAonp/plxemWl;ebq=K0i.t/9,53i7m.a3g6e /(wKeHbTp,M*L,/ *;liq=k0e .8G\ecr\kno) Chrome/51.0.2704.103 Safari/537.36\r\n
AAcccceepptt--ELancngoduaigneg:: egnz-iUp,S ,deen;flq=a0t.e,8 ,esds-c4h1\9r;\nq=0.6,es;q=0.4\r\n [\Fr\ulnl request URI:
http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html] [[HRTeTsPp onreseq ueins t f1r/a2m]e: 30428] [Next request in
frame: 30438]
```