

Joseph Kramer
CS 375 Into To Computer Networks
06-27-15

Lab 1

#1.

TCP, HTTP, QUIC, SSDP, DNS

#2.

Start Time: 17:37:22.429433000

End Time: 17:37:22.539245000

Difference = 00:00:00.109812000

#3

gaia.cs.umass.edu IP = 128.119.245.12

Joseph Kramer IP = 10.211.55.3

#4 (I had to print and then scan the printed document. Screen shots also included)

Scanned Get Message

mark-labs/INTRO-wireshark-file1.html HTTP/1.1

get

Frame 87: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 0
Ethernet II, Src: Parallel_2e:d2:0f (00:1c:42:2e:d2:0f), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)

Internet Protocol Version 4, Src: 10.211.55.3 (10.211.55.3), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 1329 (1329), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 301
Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, */*\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

Host: gaia.cs.umass.edu\r\n

DNT: 1\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 89]

Screen Shot Get Message

Local Area Connection [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	17:37:17.227184000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2	17:37:17.349678000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	181	M-SEARCH * HTTP/1.1
3	17:37:17.349827000	10.211.55.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4	17:37:17.350592000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	179	M-SEARCH * HTTP/1.1
5	17:37:17.350693000	10.211.55.3	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
21	17:37:20.348072000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	179	M-SEARCH * HTTP/1.1
22	17:37:20.348194000	10.211.55.3	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
23	17:37:20.348344000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	181	M-SEARCH * HTTP/1.1
24	17:37:20.348458000	10.211.55.3	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
25	17:37:21.205915000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	208	M-SEARCH * HTTP/1.1
31	17:37:21.283159000	10.211.55.3	191.234.5.80	HTTP	1011	GET /qsm1.aspx?query=http%3A%2F%2Fgaia.cs.umass.edu%2Fwireshark-labs%2FINTRO-wireshark-file1.html HTTP/1.1
50	17:37:21.365114000	191.234.5.80	10.211.55.3	HTTP	60	HTTP/1.1 200 OK
87	17:37:22.429438000	10.211.55.3	128.119.245.12	HTTP	355	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
89	17:37:22.539245000	128.119.245.12	10.211.55.3	HTTP	494	HTTP/1.1 200 OK (text/html)
95	17:37:22.686003000	10.211.55.3	128.119.245.12	HTTP	287	GET /Favicon.ico HTTP/1.1
100	17:37:22.778100000	128.119.245.12	10.211.55.3	HTTP	541	HTTP/1.1 404 Not Found (text/html)
148	17:37:23.359123000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	179	M-SEARCH * HTTP/1.1
149	17:37:23.359262000	10.211.55.3	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
150	17:37:23.359359000	fe80::b88e:2c9d:76eff02::c	fe80::b88e:2c9d:76eff02::c	SSDP	181	M-SEARCH * HTTP/1.1

Frame 87: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 0

Ethernet II, Src: Parallel_2e:d2:0f (00:1c:42:2e:d2:0f), Dst: Parallel_00:00:18 (00:1c:42:00:00:18)

Internet Protocol Version 4, Src: 10.211.55.3 (10.211.55.3), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 1329 (1329), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 301

Hypertext Transfer Protocol

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, */*\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

Host: gaia.cs.umass.edu\r\n

DNT: 1\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

[HTTP request 1/1]

[Response in frame: 89]

0000 00 1c 42 00 00 18 00 1c 42 2e d2 0f 08 00 45 00 ..B....B....E.

0010 01 55 71 03 40 00 80 06 00 00 0a d3 37 03 80 77 ..Uq.7..w

0020 f5 0c 05 31 00 50 cf e4 ec d6 c0 b6 23 ec 50 18 ...1.P.#.P.

0030 01 00 b8 a1 00 00 47 45 54 20 2f 77 69 72 65 73GE T /wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-

0050 77 60 73 65 72 69 61 72 68 74 66 60 66 65 21 7a ..wires-lab s/INTRO-

File: C:\Users\JOSEPH-1\AppData\Local\T... Packets: 196 - Displayed: 27 (13.8%) - Dropped: 0 (0.0%) Profile: Default

Scanned OK Message

OK

00 OK (text/html)

Frame 89: 494 bytes on wire (3952 bits), 494 bytes captured (3952 bits) on interface 0
Ethernet II, Src: Parallel_00:00:18 (00:1c:42:00:00:18), Dst: Parallel_2e:d2:0f (00:1c:42:2e:d2:0f)
Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.211.55.3 (10.211.55.3)
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1329 (1329), Seq: 1, Ack: 302, Len: 440

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sat, 27 Jun 2015 00:37:23 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: Fri, 26 Jun 2015 05:59:02 GMT\r\n

ETag: "51-519656fd25f91"\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 1/1]

[Time since request: 0.109812000 seconds]

[Request in frame: 87]

Line-based text data: text/html

Screen Shot OK Message

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. Below the menu is a toolbar with various icons for file operations, search, and analysis. The main window is divided into three panes:

- Filter:** Set to 'http'. Buttons for 'Expression...', 'Clear', 'Apply', and 'Save' are visible.
- Packet List:** A table showing captured packets. The selected packet is #89, an HTTP 200 OK response from 128.119.245.12 to 10.211.55.3.
- Packet Details:** A hierarchical view of the selected packet's structure, showing Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers.
- Packet Bytes:** A hex dump of the packet data at the bottom.

Packet #89 Details:

- Ethernet II:** Src: Parallel2e:d2:0f (00:1c:42:2e:d2:0f), Dst: Parallel00:00:18 (00:1c:42:00:00:18)
- Internet Protocol Version 4:** Src: 10.211.55.3 (10.211.55.3), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol:** Src Port: 1329 (1329), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 301
- Hypertext Transfer Protocol:**
 - GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 - Accept: text/html, application/xhtml+xml, */*
 - Accept-Language: en-US
 - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
 - Accept-Encoding: gzip, deflate
 - Host: gaia.cs.umass.edu
 - DNT: 1
 - Connection: Keep-Alive

Packet Bytes:

```
0000  00 1c 42 00 00 18 00 1c 42 2e d2 0f 08 00 45 00  ..B.... B....E.
0010  01 55 71 03 40 00 80 06 00 00 0a d3 37 03 80 77  .Uq.@....7..w
0020  f5 0c 05 31 00 50 cf e4 ec 06 c0 b6 23 ec 50 18  ...1.P...#.P.
0030  01 00 b8 a1 00 00 47 45 54 20 2f 77 69 72 65 73  ....GET/wires
0040  68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d  hark-lab s/INTRO-
0050  77 60 72 65 72 69 61 72 6b 2d 66 60 6c 65 31 7a  wireshark-fil1
```

The status bar at the bottom indicates: File: C:\Users\JOSEPH-1\AppData\Local\T... Packets: 196 - Displayed: 27 (13.8%) - Dropped: 0 (0.0%) Profile: Default.