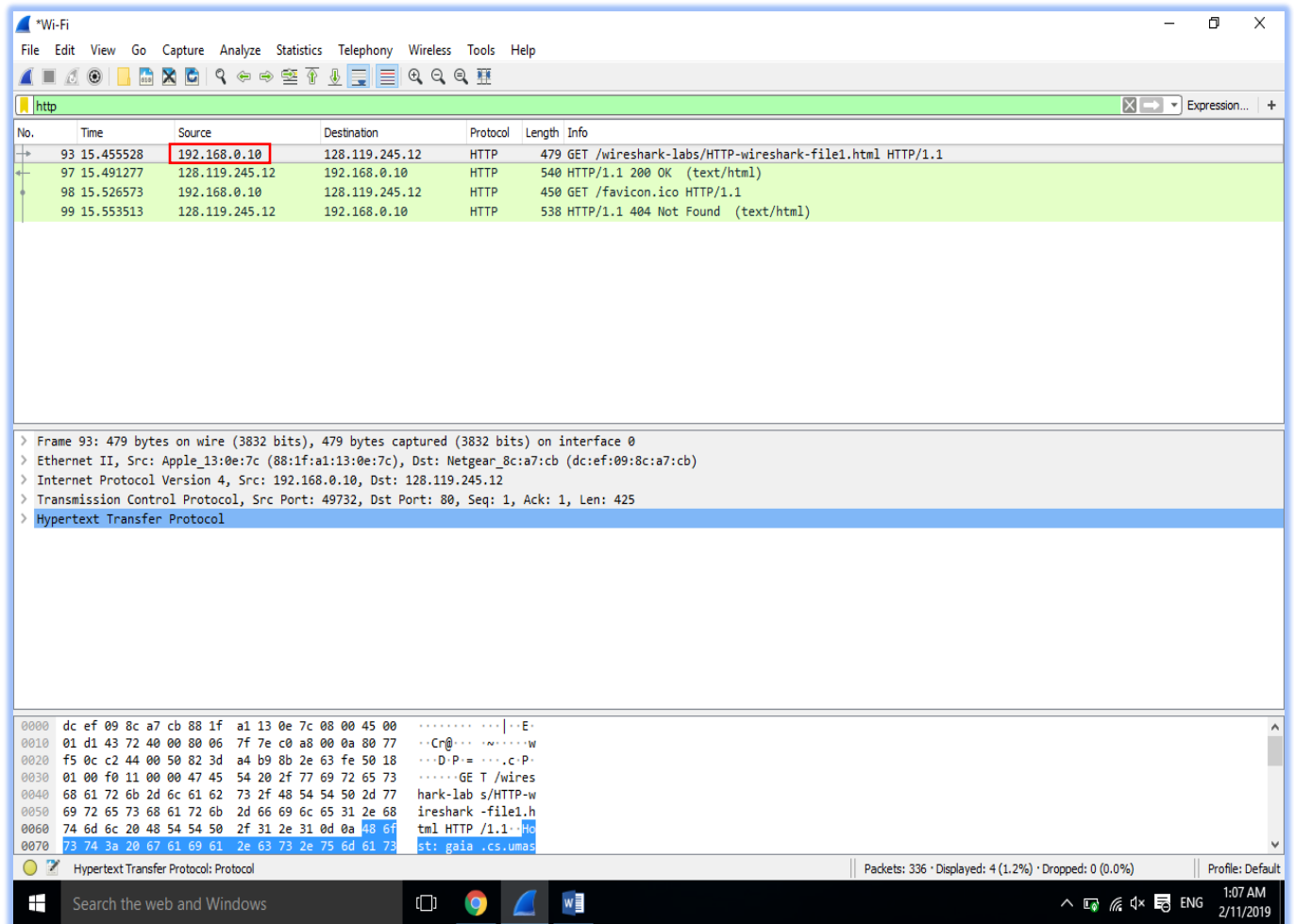


Abdullah Alrfeedi

IT-520

Lab #2

The IP address is (192.168.0.10).



1) Is your browser running HTTP version 1.0 or 1.1?

HTTP version 1.1

The image shows a Wireshark packet capture window titled "Wi-Fi". The main pane displays a list of captured packets. The first four packets are HTTP requests from 192.168.0.10 to 128.119.245.12. The second packet, at time 15.491277, is an "HTTP/1.1 200 OK" response, which is highlighted with a red box. The bottom pane shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4, and the Hypertext Transfer Protocol section. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
93	15.455528	192.168.0.10	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
97	15.491277	128.119.245.12	192.168.0.10	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15.526573	192.168.0.10	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
99	15.553513	128.119.245.12	192.168.0.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 93: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
> Ethernet II, Src: Apple_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb)
> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49732, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
> Hypertext Transfer Protocol

0000 dc ef 09 8c a7 cb 88 1f a1 13 0e 7c 08 00 45 00E
0010 01 d1 43 72 40 00 80 06 7f 7e c0 a8 00 0a 80 77 ..Cr@.....w
0020 f5 0c c2 44 00 50 82 3d a4 b9 8b 2e 63 fe 50 18 ...D-P=...c-P
0030 01 00 f0 11 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 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 48 6f tml HTTP /1.1-fo
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas

Hypertext Transfer Protocol: Protocol | Packets: 336 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%) | Profile: Default

Search the web and Windows | 1:24 AM 2/11/2019

2) When was the HTML file that you are retrieving last modified at the server?

Mon, 11 Feb 2019 06:04:01 GMT

The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list pane shows four packets. Packet 97 is an HTTP 200 OK response from 128.119.245.12 to 192.168.0.10. The packet details pane for packet 97 shows the following information:

- Frame 97: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
- Ethernet II, Src: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb), Dst: Apple_13:0e:7c (88:1f:a1:13:0e:7c)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.10
- Transmission Control Protocol, Src Port: 80, Dst Port: 49732, Seq: 1, Ack: 426, Len: 486
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Mon, 11 Feb 2019 06:04:19 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: Mon, 11 Feb 2019 06:04:01 GMT\r\n**
 - ETag: "80-58198133ef720"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 128\r\n
 - [Content length: 128]
 - Keep-Alive: timeout=5, max=100\r\n

The packet bytes pane shows the raw data of the packet, with the "Last-Modified" header highlighted in blue.

Search the web and Windows

Packets: 336 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%) Profile: Default

1:37 AM 2/11/2019

3) What is the IP address of the gaia.cs.umass.edu server?

128.119.245.12

The image shows a Wireshark packet capture window titled "Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A filter bar at the top shows "http". The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
93	15.455528	192.168.0.10	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
97	15.491277	128.119.245.12	192.168.0.10	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15.526573	192.168.0.10	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
99	15.553513	128.119.245.12	192.168.0.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for packet 93 shows the following structure:

- > Frame 93: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
- > Ethernet II, Src: Apple_13:0e:7c (88:1f:a1:13:0e:7c), Dst: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb)
- > Internet Protocol Version 4, Src: 192.168.0.10, Dst: 128.119.245.12
- > Transmission Control Protocol, Src Port: 49732, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
- > Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 dc ef 09 8c a7 cb 88 1f a1 13 0e 7c 08 00 45 00 .....E-
0010 01 d1 43 72 40 00 80 06 7f 7e c0 a8 00 0a 80 77 ..Cr@...w
0020 f5 0c c2 44 00 50 82 3d a4 b9 8b 2e 63 fe 50 18 ...D-P=...c-P
0030 01 00 f0 11 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 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 48 6f tml HTTP /1.1-fo
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umass
```

The status bar at the bottom indicates "Packets: 336 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%)". The system tray shows the time as 1:07 AM on 2/11/2019.

4) What languages does your browser indicate that it can accept to the server?

English-US Language.

The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list pane displays four packets. Packet 97 is an HTTP 200 OK response (text/html) from 128.119.245.12 to 192.168.0.10. Packet 98 is an HTTP GET request for /favicon.ico from 192.168.0.10 to 128.119.245.12. Packet 99 is an HTTP 404 Not Found response (text/html) from 128.119.245.12 to 192.168.0.10. The packet details pane for packet 98 shows the Hypertext Transfer Protocol section with the following fields: Host: gaia.cs.umass.edu, Connection: keep-alive, Upgrade-Insecure-Requests: 1, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8, Accept-Encoding: gzip, deflate, and **Accept-Language: en-US,en;q=0.9**. The packet bytes pane shows the raw data for the Accept-Language header: 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d 0a.

No.	Time	Source	Destination	Protocol	Length	Info
93	15.455528	192.168.0.10	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
97	15.491277	128.119.245.12	192.168.0.10	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15.526573	192.168.0.10	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
99	15.553513	128.119.245.12	192.168.0.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Hypertext Transfer Protocol

- GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
- Host: gaia.cs.umass.edu\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
- Accept-Encoding: gzip, deflate\r\n
- Accept-Language: en-US,en;q=0.9\r\n**
- \r\n
- [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
- [HTTP request 1/2]
- [Response in frame: 97]
- [Next request in frame: 98]

0160 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,application
0170 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0.9,image
0180 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,image/apng
0190 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 ,/*;q=0.8·Acce
01a0 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encoding: gzi
01b0 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 p, deflate·Acce
01c0 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-
01d0 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d 0a US,en;q= 0.9·...

HTTP Accept Language (http.accept_language), 33 bytes

Packets: 336 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%) Profile: Default

Search the web and Windows

1:49 AM
2/11/2019

5) When was the HTML file that you are retrieving created at the server?

Arrival Time: Feb 11, 2019 01:04:35 Eastern Slandered Time.

The image shows a Wireshark network traffic capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (Frame 93).

Packets List:

No.	Time	Source	Destination	Protocol	Length	Info
93	15.455528	192.168.0.10	128.119.245.12	HTTP	479	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
97	15.491277	128.119.245.12	192.168.0.10	HTTP	540	HTTP/1.1 200 OK (text/html)
98	15.526573	192.168.0.10	128.119.245.12	HTTP	450	GET /favicon.ico HTTP/1.1
99	15.553513	128.119.245.12	192.168.0.10	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 93 Details:

- Frame 93: 479 bytes on wire (3832 bits), 479 bytes captured (3832 bits) on interface 0
- Interface id: 0 (\Device\NPF_{311E61C6-4424-4D37-813C-AD9B3CAA2427})
- Interface name: \Device\NPF_{311E61C6-4424-4D37-813C-AD9B3CAA2427}
- Encapsulation type: Ethernet (1)
- Arrival Time: Feb 11, 2019 01:04:35.636849000 Eastern Standard Time**
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1549865075.636849000 seconds
- [Time delta from previous captured frame: 0.000174000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 15.455528000 seconds]
- Frame Number: 93
- Frame Length: 479 bytes (3832 bits)
- Capture Length: 479 bytes (3832 bits)
- [Frame is marked: False]

Packet Bytes:

```
0160 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e +xml,application
0170 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 /xml;q=0.9,image
0180 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,image/apng
0190 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 ,/*;q=0.8;Acce
01a0 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
01b0 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 p, defla te...Acce
01c0 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 6e 2d pt-Langu age: en-
01d0 55 93 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 0d 0a US,en;q= 0.9...
```

Status Bar: HTTP AcceptLanguage (http.accept_language), 33 bytes | Packets: 336 · Displayed: 4 (1.2%) · Dropped: 0 (0.0%) | Profile: Default

Taskbar: Search the web and Windows | 1:55 AM 2/11/2019

(A full print of the HTTP OK message)

```
No.      Time      Source      Destination      Protocol Length Info
 97 15.491277 128.119.245.12 192.168.0.10 HTTP 540 HTTP/1.1 200 OK (text/html)
Frame 97: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Interface id: 0 (\Device\NPF_{311E61C6-4424-4D37-813C-AD9B3CAA2427})
Interface name: \Device\NPF_{311E61C6-4424-4D37-813C-AD9B3CAA2427}
Encapsulation type: Ethernet (1)
Arrival Time: Feb 11, 2019 01:04:35.672598000 Eastern Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1549865075.672598000 seconds
[Time delta from previous captured frame: 0.006432000 seconds]
[Time delta from previous displayed frame: 0.035749000 seconds]
[Time since reference or first frame: 15.491277000 seconds]
Frame Number: 97
Frame Length: 540 bytes (4320 bits)
Capture Length: 540 bytes (4320 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb), Dst: Apple_13:0e:7c (88:1f:a1:13:0e:7c)
Destination: Apple_13:0e:7c (88:1f:a1:13:0e:7c)
Address: Apple_13:0e:7c (88:1f:a1:13:0e:7c)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0. .... = IG bit: Individual address (unicast)
Source: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb)
Address: Netgear_8c:a7:cb (dc:ef:09:8c:a7:cb)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.10
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
0010 00.. = Differentiated Services Codepoint: Class Selector 1 (8)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 526
Identification: 0x9414 (37908)
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: 47
Protocol: TCP (6)
Header checksum: 0x7f7f [validation disabled]
[Header checksum status: Unverified]
Source: 128.119.245.12
```

```
[Stream index: 4]
[TCP Segment Len: 486]
Sequence number: 1 (relative sequence number)
[Next sequence number: 487 (relative sequence number)]
Acknowledgment number: 426 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
 000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... = Congestion Window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 .... = Acknowledgment: Set
.... .... 1... = Push: Set
.... .... .0.. = Reset: Not set
.... .... ..0. = Syn: Not set
.... .... ...0 = Fin: Not set
[TCP Flags: .....AP...]
Window size value: 237
[Calculated window size: 60672]
[Window size scaling factor: 256]
Checksum: 0x50cd [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
  [iRTT: 0.027595000 seconds]
  [Bytes in flight: 486]
  [Bytes sent since last PSH flag: 486]
```

```
[Timestamps]
  [Time since first frame in this TCP stream: 0.063518000 seconds]
  [Time since previous frame in this TCP stream: 0.006432000 seconds]
TCP payload (486 bytes)
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
<html>\n
  Congratulations. You've downloaded the file \n
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```