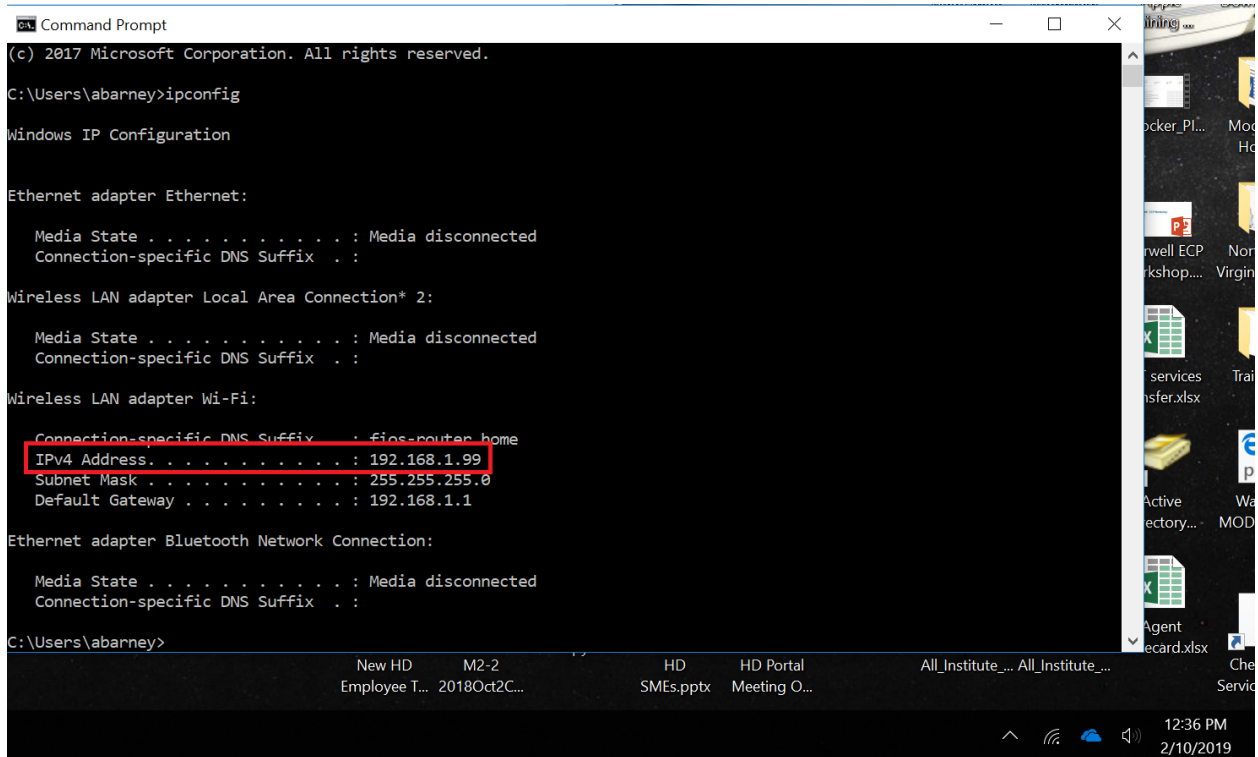


Wireshark Lab 2 - HTTP IT 520-A – Enterprise Infrastructure & Networks

My IP address: 192.167.1.99



```
Command Prompt
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Users\abarney>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : fics-router.home
    IPv4 Address. . . . . : 192.168.1.99
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\abarney>
```

1. Is your browser running HTTP version 1.0 or 1.1?
 - HTTP version 1.1

^Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
162	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	418	GET /wireshark-labs/HTTP-wireshark-file1.html H
164	2019-02-10 12:58:34	128.119.245.12	192.168.1.99	HTTP	540	HTTP/1.1 200 OK (text/html)
172	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
174	2019-02-10 12:58:35	128.119.245.12	192.168.1.99	HTTP	539	HTTP/1.1 404 Not Found (text/html)

<

0101 = Header Length: 20 bytes (5)

- > Flags: 0x018 (PSH, ACK)
- Window size value: 237
- [Calculated window size: 30336]
- [Window size scaling factor: 128]
- Checksum: 0xa742 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- > [SEQ/ACK analysis]
- > [Timestamps]
- TCP payload (486 bytes)

▼ Hypertext Transfer Protocol

- > HTTP/1.1 200 OK\r\n
- Date: Sun, 10 Feb 2019 17:58:35 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n
- Etag: "80-56184ba1f23f8"\r\n
- Accept-Ranges: bytes\r\n

1:09 PM
2/10/2019

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

- Last Modified Sun 10 Feb 2019 06:59:01 GMT/r/n

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
162	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	418	GET /wireshark-labs/HTTP-wireshark-file1
164	2019-02-10 12:58:34	128.119.245.12	192.168.1.99	HTTP	540	HTTP/1.1 200 OK (text/html)
172	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
174	2019-02-10 12:58:35	128.119.245.12	192.168.1.99	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```

<
> Frame 164: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: Verizon_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor_10:10:99 (14:ab:c5:10:10:99)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.99
> Transmission Control Protocol, Src Port: 80, Dst Port: 63060, Seq: 1, Ack: 365, Len: 486
▼ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 10 Feb 2019 17:58:35 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n
    Etag: "80-58184ba1f23f8"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\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
  
```

1:13 PM
2/10/2019

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

- 128.119.245.12

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
162	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	418	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
164	2019-02-10 12:58:34	128.119.245.12	192.168.1.99	HTTP	540	HTTP/1.1 200 OK (text/html)
172	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
174	2019-02-10 12:58:35	128.119.245.12	192.168.1.99	HTTP	539	HTTP/1.1 404 Not Found (text/html)

<

> Frame 164: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

> Ethernet II, Src: Verizon_e0:fe:66 (20:c0:47:e0:fe:66), Dst: IntelCor_10:10:99 (14:ab:c5:10:10:99)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.99

> Transmission Control Protocol, Src Port: 80, Dst Port: 63060, Seq: 1, Ack: 365, Len: 486

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Sun, 10 Feb 2019 17:58:35 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n

ETag: "80-58184ba1f23f8"\r\n

Accept-Ranges: bytes\r\n

> Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

1:17 PM
2/10/2019

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

- Accept-Language: en-US\r\n

Wireshark interface showing a packet capture of HTTP traffic. The packet list pane displays four packets, with packet 162 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
162	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	418	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
164	2019-02-10 12:58:34	128.119.245.12	192.168.1.99	HTTP	540	HTTP/1.1 200 OK (text/html)
172	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
174	2019-02-10 12:58:35	128.119.245.12	192.168.1.99	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Packet 162 details:

- Frame 162: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
- Ethernet II, Src: IntelCor_10:10:99 (14:ab:c5:10:10:99), Dst: Verizon_e0:fe:66 (20:c0:47:e0:fe:66)
- Internet Protocol Version 4, Src: 192.168.1.99, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 63060, Dst Port: 80, Seq: 1, Ack: 1, Len: 364
- Hypertext Transfer Protocol
 - GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /wireshark-labs/HTTP-wireshark-file1.html
 - Request Version: HTTP/1.1
 - Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
 - Accept-Language: en-US\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36 Edge/16.162
 - 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: 164]

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

- Sun, 10 Feb 2019 17:58:35 GMT\r\n

No.	Time	Source	Destination	Protocol	Length	Info
162	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	418	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
164	2019-02-10 12:58:34	128.119.245.12	192.168.1.99	HTTP	540	HTTP/1.1 200 OK (text/html)
172	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1.1
174	2019-02-10 12:58:35	128.119.245.12	192.168.1.99	HTTP	539	HTTP/1.1 404 Not Found (text/html)


```

[Next sequence number: 487 (relative sequence number)]
Acknowledgment number: 365 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xa742 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
  TCP payload (486 bytes)
  > Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      Date: Sun, 10 Feb 2019 17:58:35 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n
      ETag: "80-58184balf23f8"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\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: 0.030953000 seconds]
    [Request in frame: 162]
    File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
  
```

Full print of HTTP OK

Wireshark 2.10.0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

HTTP

No.	Time	Source	Destination	Protocol	Length	Info
162	2019-02-10 12:58:34	192.168.1.99	128.119.245.12	HTTP	418	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
164	2019-02-10 12:58:34	128.119.245.12	192.168.1.99	HTTP	540	HTTP/1.1 200 OK (text/html)

```

0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xa742 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
  TCP payload (486 bytes)
  > Hypertext Transfer Protocol
    > HTTP/1.1 200 OK\r\n
      [Expert Info [Chat/Sequence]: HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
      Date: Sun, 10 Feb 2019 17:58:35 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: Sun, 10 Feb 2019 06:59:01 GMT\r\n
      ETag: "80-58184balf23f8"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\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: 0.030953000 seconds]
    [Request in frame: 162]
    File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
  
```