James Gouveia

Professor Jun Dai

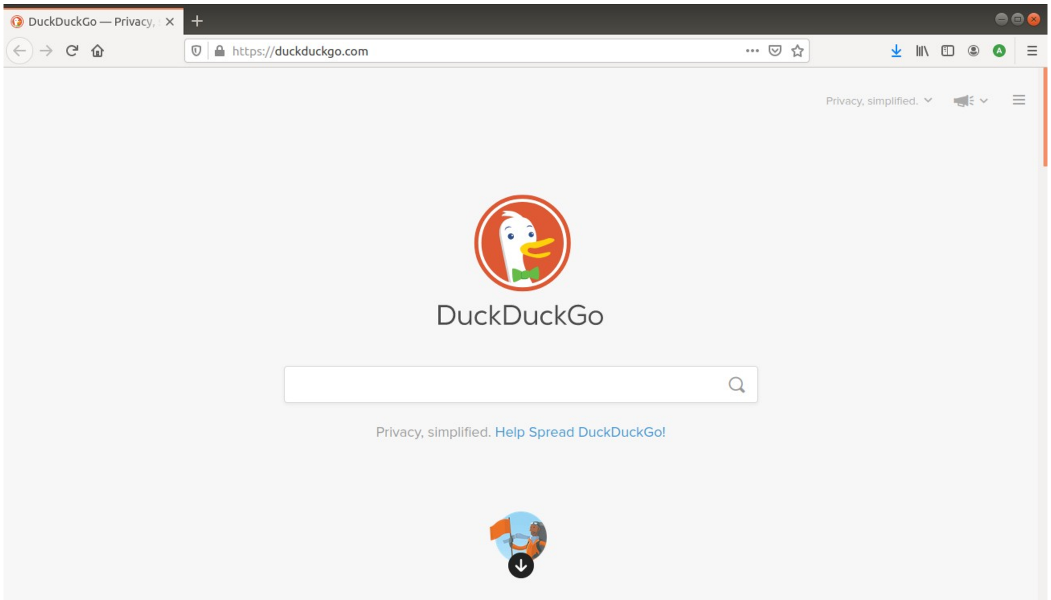
CSC138

03/21/2021

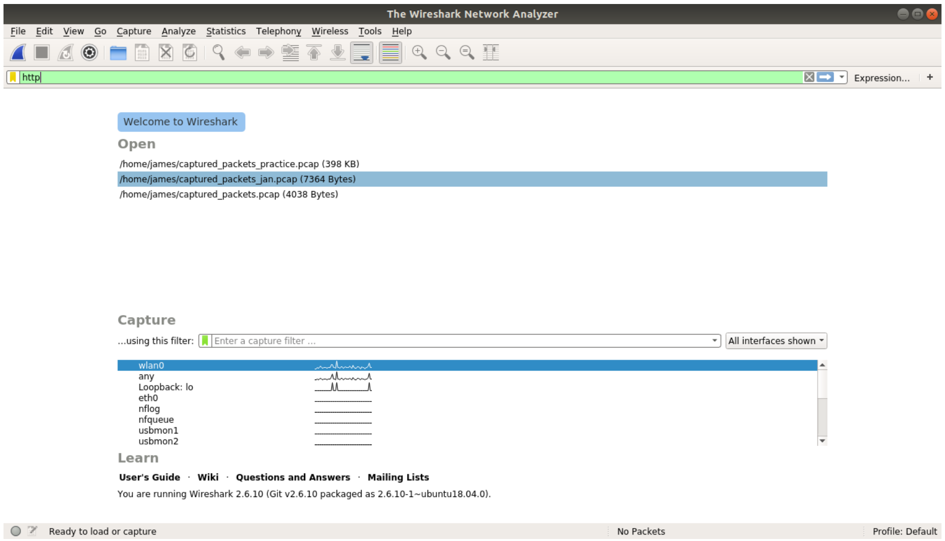
Wireshark Lab2

Lab Procedure 1:

1. Start up web browser



2. Start wire shark and type http into the display-filter


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Welcome to Wireshark
Open
Capture
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

http

/home/james/captured_packets_practice.pcap (398 KB)
/home/james/captured_packets_jan.pcap (7364 Bytes)
/home/james/captured_packets.pcap (4038 Bytes)

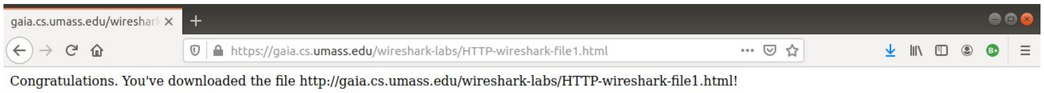
...using this filter: Enter a capture filter ...

wlan0
any
Loopback: lo
eth0
nflog
nfqueue
usbmon1
usbmon2

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

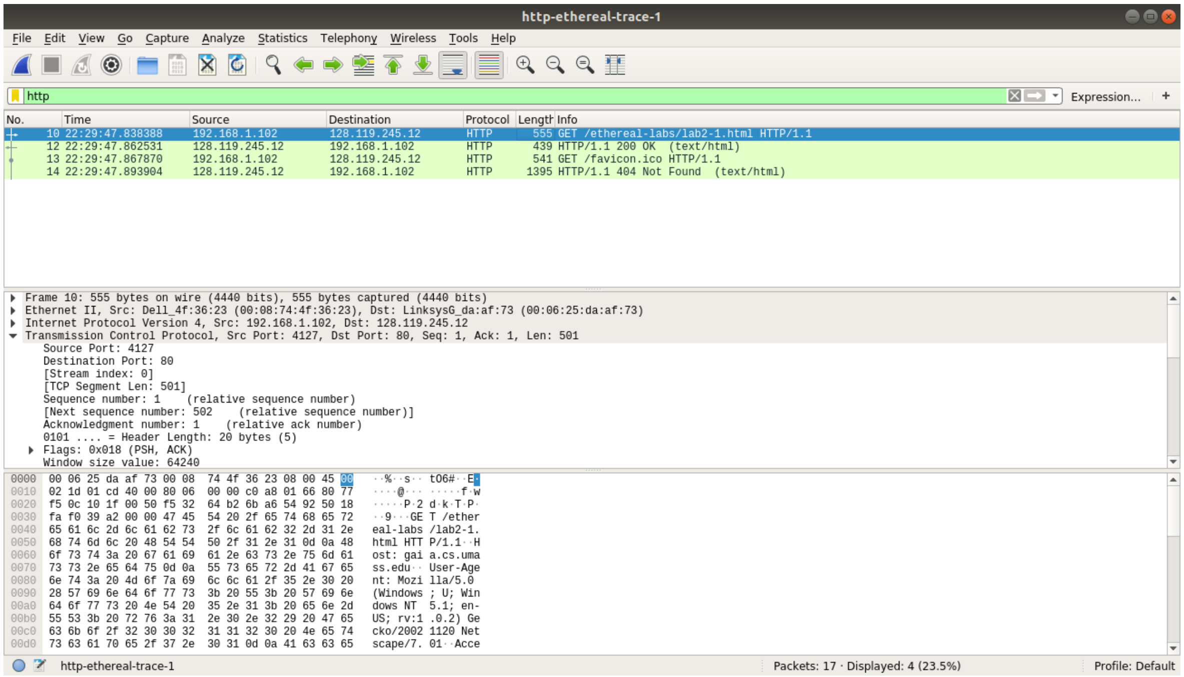
Ready to load or capture | No Packets | Profile: Default

3. Wait at least one minute and start packet capture


gaia.cs.umass.edu/wireshar
https://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

4. GET request


http-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

http

```
No.  Time             Source           Destination      Protocol Length Info
  10 22:29:47.838388  192.168.1.102    128.119.245.12   HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
  12 22:29:47.862531  128.119.245.12   192.168.1.102    HTTP      439 HTTP/1.1 200 OK  (text/html)
  13 22:29:47.867870  192.168.1.102    128.119.245.12   HTTP      541 GET /favicon.ico HTTP/1.1
  14 22:29:47.893904  128.119.245.12   192.168.1.102    HTTP     1395 HTTP/1.1 404 Not Found  (text/html)
```

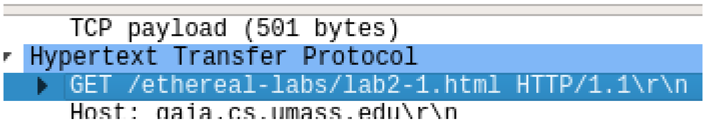
```
▸ Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
▸ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▸ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
    Source Port: 4127
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 501]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 502    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 64240
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  02 1d 01 cd 40 00 80 06  00 00 c0 a8 01 66 80 77   ····@··· ·····f·w
0020  f5 0c 10 1f 00 50 f5 32  64 b2 6b a6 54 92 50 18   ·····P·2 d·k·T·P·
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 6c 61 62 32 2d 31 2e   eal-labs /lab2-1.
0050  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0060  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0070  73 73 2e 65 64 75 0d 0a  55 73 65 72 2d 41 67 65   ss.edu·· User-Age
0080  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
0090  28 57 69 6e 64 6f 77 73  3b 20 55 3b 20 57 69 6e   (Windows ; U; Win
00a0  64 6f 77 73 20 4e 54 20  35 2e 31 3b 20 65 6e 2d   dows NT  5.1; en-
00b0  55 53 3b 20 72 76 3a 31  2e 30 2e 32 29 20 47 65   US; rv:1 .0.2) Ge
00c0  63 6b 6f 2f 32 30 30 32  31 31 32 30 20 4e 65 74   cko/2002 1120 Net
00d0  73 63 61 70 65 2f 37 2e  30 31 0d 0a 41 63 63 65   scape/7. 01··Acce
```

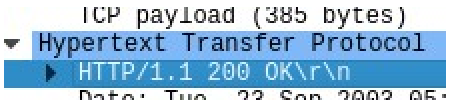
http-ethereal-trace-1 Packets: 17 · Displayed: 4 (23.5%) Profile: Default

Questions

1. Browser: HTTP Version 1.1 Server: HTTP Version 1.1

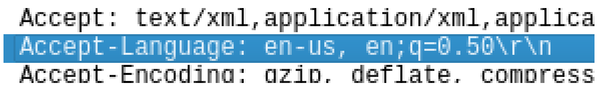


```
    TCP payload (501 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
```



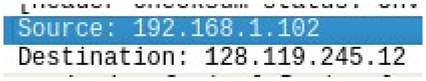
```
    TCP payload (385 bytes)
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:
```

2. American English



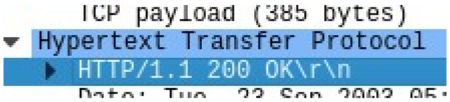
```
Accept: text/xml,application/xml,applica
Accept-Language: en-us, en;q=0.50\r\n
Accept-Encoding: gzip, deflate, compress
```

3. My computer IP: 192.168.1.102, Server IP: 128.119.245.12



```
Source: 192.168.1.102
Destination: 128.119.245.12
```

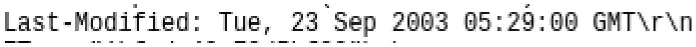
4. The status code returned: 200 ok



```
  TCP payload (385 bytes)
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
```

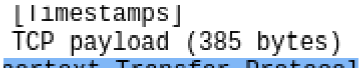
5. Last Modified: September 23, 2003

Please note I downloaded the packets from the book site to inspect hence the old date.



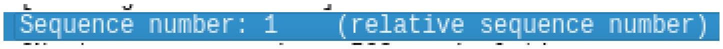
```
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
```

6. 385 bytes



```
[Timestamps]
TCP payload (385 bytes)
```

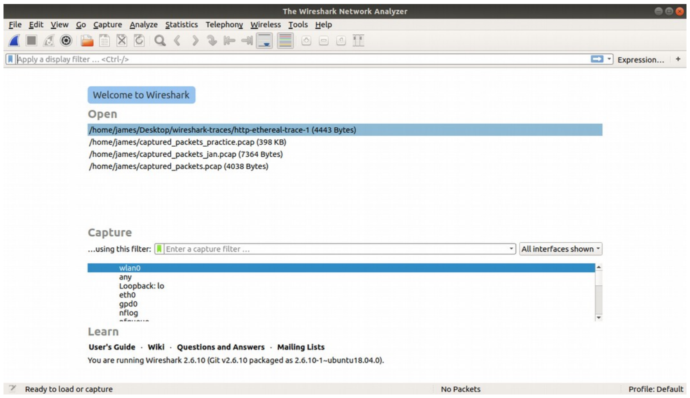
7. Sequence number



```
Sequence number: 1    (relative sequence number)
```

Lab Procedure 2:

1. Start Wireshark.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+
Welcome to Wireshark
Open
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

/home/james/Desktop/wireshark-traces/http-ethereal-trace-1 (4443 Bytes)
/home/james/captured_packets_practice.pcap (398 KB)
/home/james/captured_packets_jan.pcap (7364 Bytes)
/home/james/captured_packets.pcap (4038 Bytes)

…using this filter: Enter a capture filter … All interfaces shown

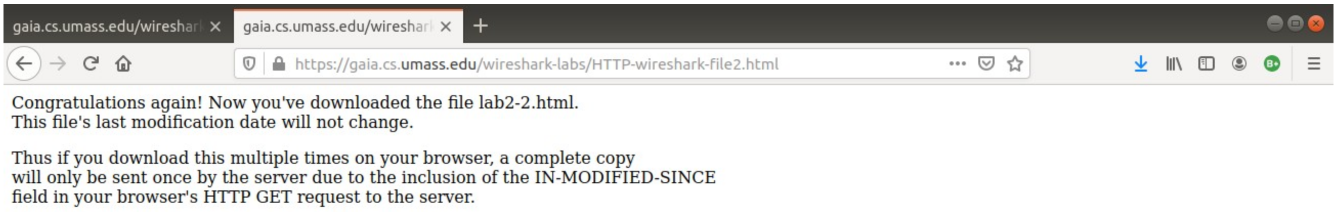
wlan0
any
Loopback: lo
eth0
gpd0
nflog

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Ready to load or capture | No Packets | Profile: Default

Continued Next Page

2. Open a browser and point it to http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

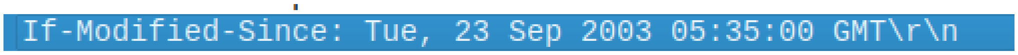

gaia.cs.umass.edu/wireshar ×
gaia.cs.umass.edu/wireshar ×
https://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

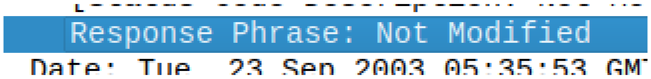
Questions

8. Yes



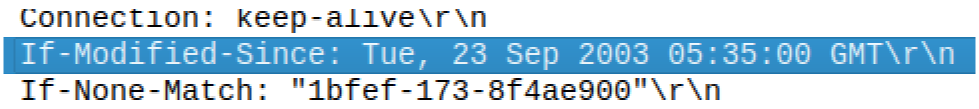
```
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
```

9. No, because the server responded with a not modified message.



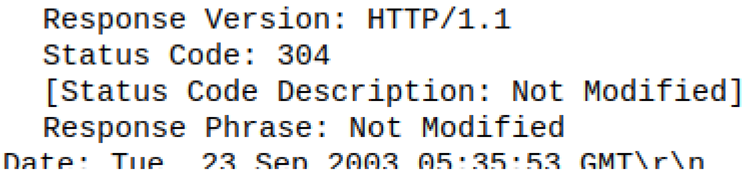
```
Response Phrase: Not Modified
Date: Tue, 23 Sep 2003 05:35:53 GM
```

10. Yes, the if modified since field indicates a if modified after September 23, 2003 then send the newer version.



```
Connection: keep-alive\r\n
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
If-None-Match: "1bfef-173-8f4ae900"\r\n
```

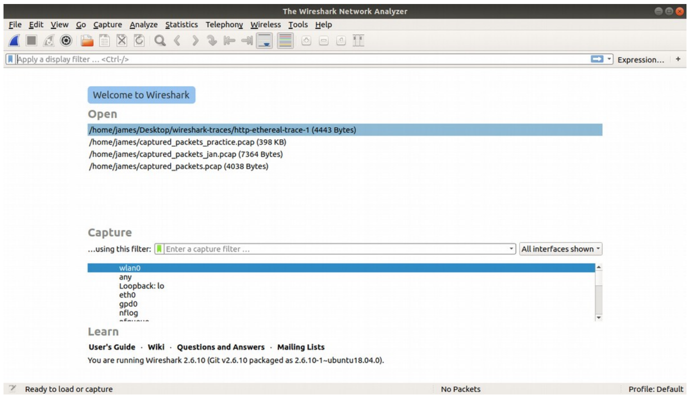
11. The server response code was 304 which is the code for not modified. The server did not return the contents of the file because the version of the file that is cached is the same as the version on the server. Since the two files are the same there is no need to request a new version and this results in less traffic traversing over the network.



```
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
```

Lab Procedure 3:

1. Clear your browsers cache and start Wireshark.



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

Welcome to Wireshark

Open

/home/james/Desktop/wireshark-traces/http-ethereal-trace-1 (4443 Bytes)
/home/james/captured_packets_practice.pcap (398 KB)
/home/james/captured_packets_jan.pcap (7364 Bytes)
/home/james/captured_packets.pcap (4038 Bytes)

Capture

…using this filter: Enter a capture filter … All interfaces shown

wlan0
any
Loopback: lo
eth0
gpd0
nflog

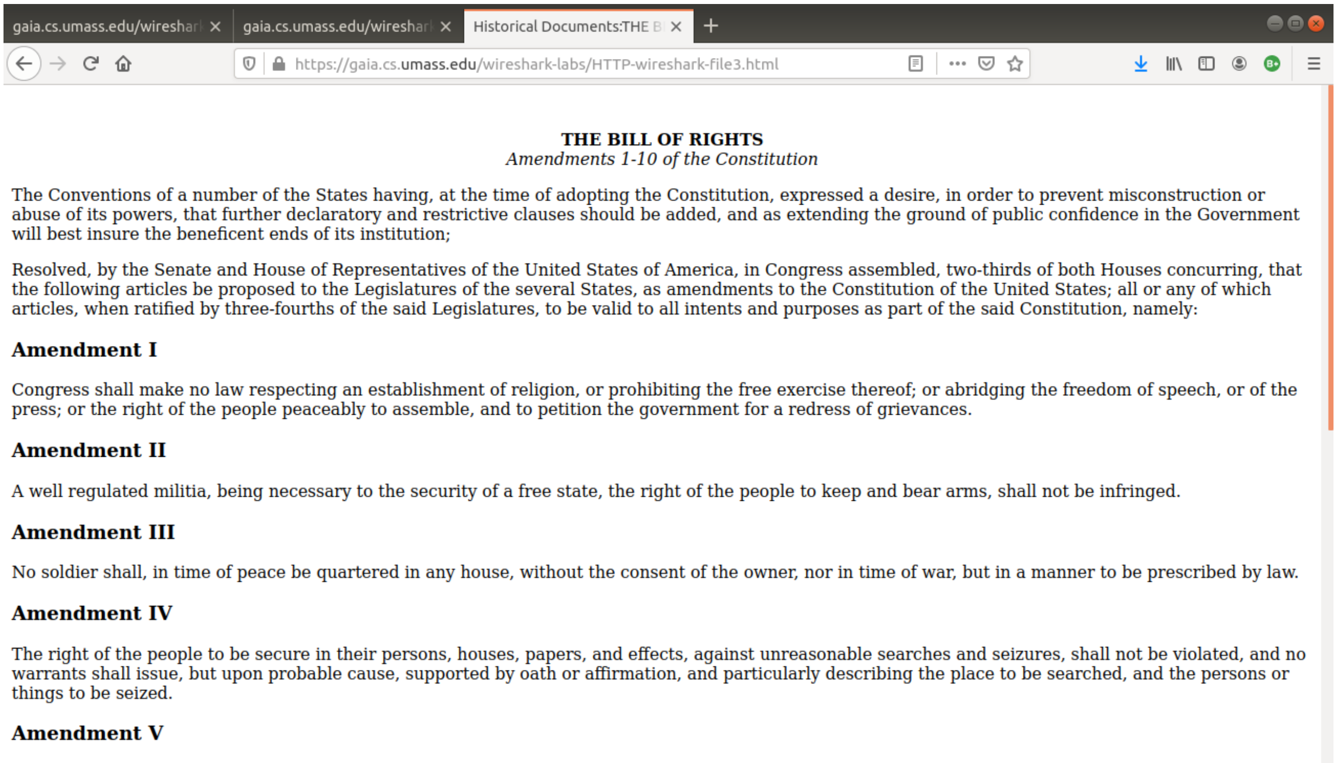
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Ready to load or capture No Packets Profile: Default

2. Point your browser to http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html



gaia.cs.umass.edu/wireshar
gaia.cs.umass.edu/wireshar
Historical Documents:THE B
https://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html

THE BILL OF RIGHTS
Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

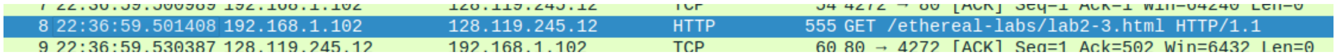
Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

Questions

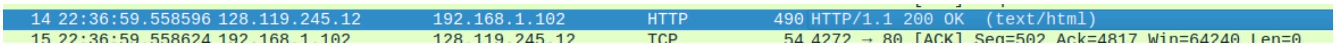
12. My browser sent 1 GET request. The GET request is number 8 on the Wireshark Trace.



```
 7 22:36:59.500989 192.168.1.102   128.119.245.12  TCP     54 4272 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 8 22:36:59.501408 192.168.1.102   128.119.245.12  HTTP   555 GET /ethereal-labs/lab2-3.html HTTP/1.1
 9 22:36:59.530387 128.119.245.12  192.168.1.102   TCP     60 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=0
```

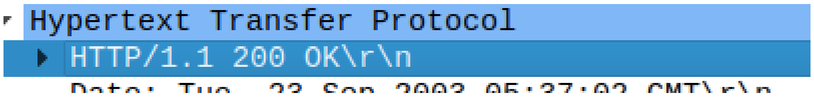
Continued Next Page

13. The response to the GET message is number 14 on the Wireshark trace.



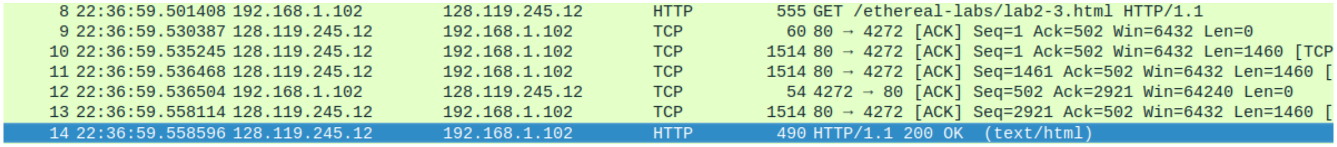
```
 14 22:36:59.558596 128.119.245.12        192.168.1.102        HTTP        490 HTTP/1.1 200 OK  (text/html)
 15 22:36:59.558624 192.168.1.102         128.119.245.12       TCP          54 4272 → 80 [ACK] Seq=502 Ack=4817 Win=64240 Len=0
```

14. The status code is 200 and the phrase is OK which corresponds to a successful transmission.



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:37:02 GMT\r\n
```

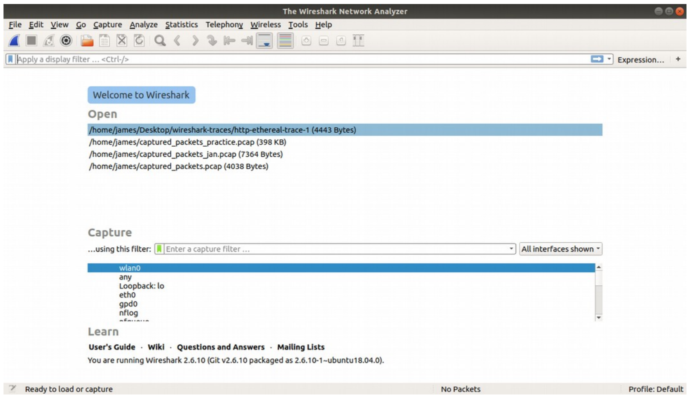
15. It took 6 data containing TCP packets in order to transmit the whole Bill of Rights text from the server to the client.



```
  8 22:36:59.501408 192.168.1.102     128.119.245.12     HTTP     555 GET /ethereal-labs/lab2-3.html HTTP/1.1
  9 22:36:59.530387 128.119.245.12    192.168.1.102      TCP       60 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=0
 10 22:36:59.535245 128.119.245.12    192.168.1.102      TCP     1514 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=1460 [TCP
 11 22:36:59.536468 128.119.245.12    192.168.1.102      TCP     1514 80 → 4272 [ACK] Seq=1461 Ack=502 Win=6432 Len=1460 [
 12 22:36:59.536504 192.168.1.102     128.119.245.12     TCP       54 4272 → 80 [ACK] Seq=502 Ack=2921 Win=64240 Len=0
 13 22:36:59.558114 128.119.245.12    192.168.1.102      TCP     1514 80 → 4272 [ACK] Seq=2921 Ack=502 Win=6432 Len=1460 [
 14 22:36:59.558596 128.119.245.12    192.168.1.102      HTTP     490 HTTP/1.1 200 OK  (text/html)
```

Lab Procedure 4:

1. Clear your browsers cache and start Wireshark.



/home/james/Desktop/wireshark-traces/http-ethereal-trace-1 (4443 Bytes)
/home/james/captured_packets_practice.pcap (398 KB)
/home/james/captured_packets_jan.pcap (7364 Bytes)
/home/james/captured_packets.pcap (4038 Bytes)

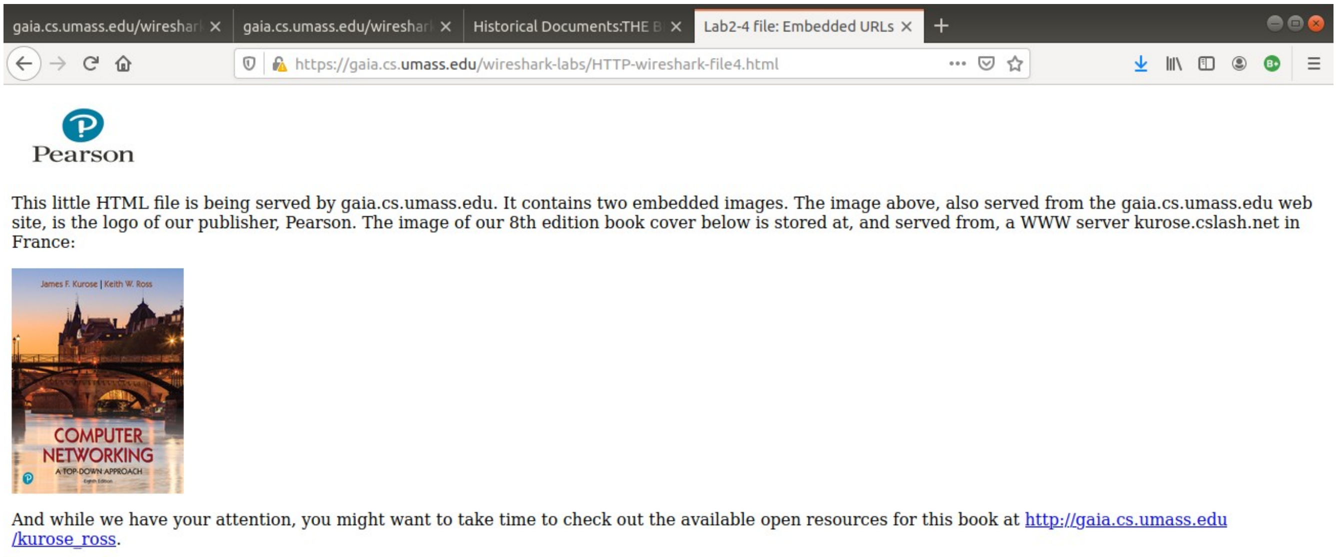
wlan0
any
Loopback: lo
eth0
gpd0
nflog

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Ready to load or capture | No Packets | Profile: Default

Continued Next Page

2. Point your browser to http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html.

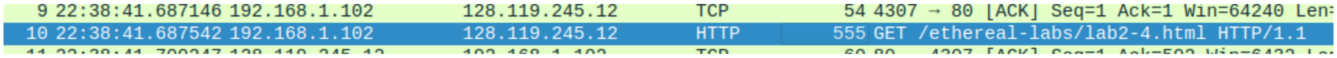

gaia.cs.umass.edu/wireshar
gaia.cs.umass.edu/wireshar
Historical Documents:THE B
Lab2-4 file: Embedded URLs
https://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
Pearson
James F. Kurose | Keith W. Ross
COMPUTER NETWORKING
A TOP-DOWN APPROACH

This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:

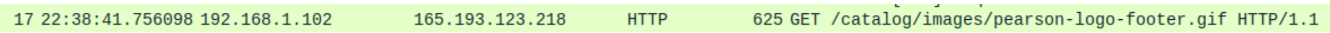
And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

Questions

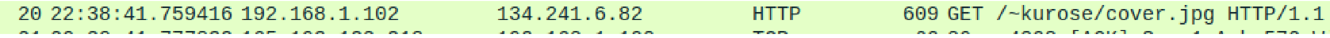
16. The browser sent 3 GET requests. Each GET request was pointed to a different IP address. Request 1 was pointed to 128.119.245.12. Request 2 was pointed to 165.193.123.218. Request 3 was pointed to 134.241.6.82.



```
 9 22:38:41.687146 192.168.1.102   128.119.245.12   TCP    54 4307 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=
10 22:38:41.687542 192.168.1.102   128.119.245.12   HTTP  555 GET /ethereal-labs/lab2-4.html HTTP/1.1
```

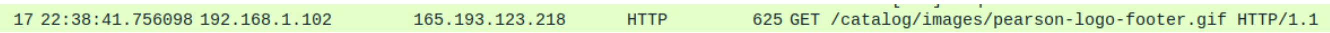


```
17 22:38:41.756098 192.168.1.102   165.193.123.218   HTTP   625 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
```

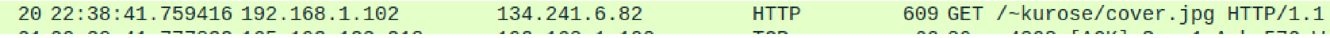


```
20 22:38:41.759416 192.168.1.102   134.241.6.82   HTTP   609 GET /~kurose/cover.jpg HTTP/1.1
```

17. The two images were downloaded serially. I can tell because the two GET messages were sent at different times.



```
17 22:38:41.756098 192.168.1.102   165.193.123.218   HTTP   625 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
```

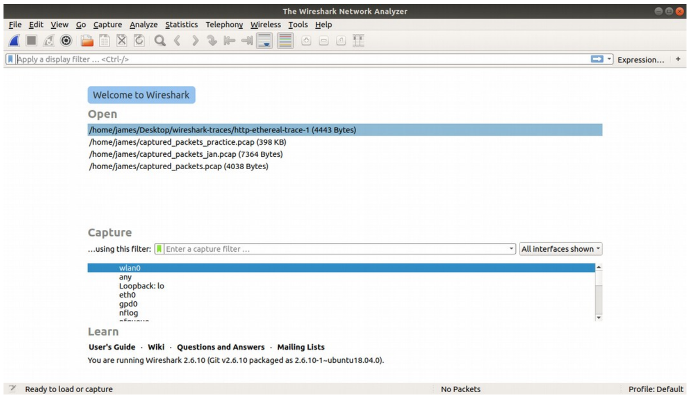


```
20 22:38:41.759416 192.168.1.102   134.241.6.82   HTTP   609 GET /~kurose/cover.jpg HTTP/1.1
```

Continued Next Page

Lab Procedure 5:

1. Clear your browsers cache and start Wireshark.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Welcome to Wireshark
Open
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
All interfaces shown
Profile: Default

/home/james/Desktop/wireshark-traces/http-ethereal-trace-1 (4443 Bytes)
/home/james/captured_packets_practice.pcap (398 KB)
/home/james/captured_packets_jan.pcap (7364 Bytes)
/home/james/captured_packets.pcap (4038 Bytes)

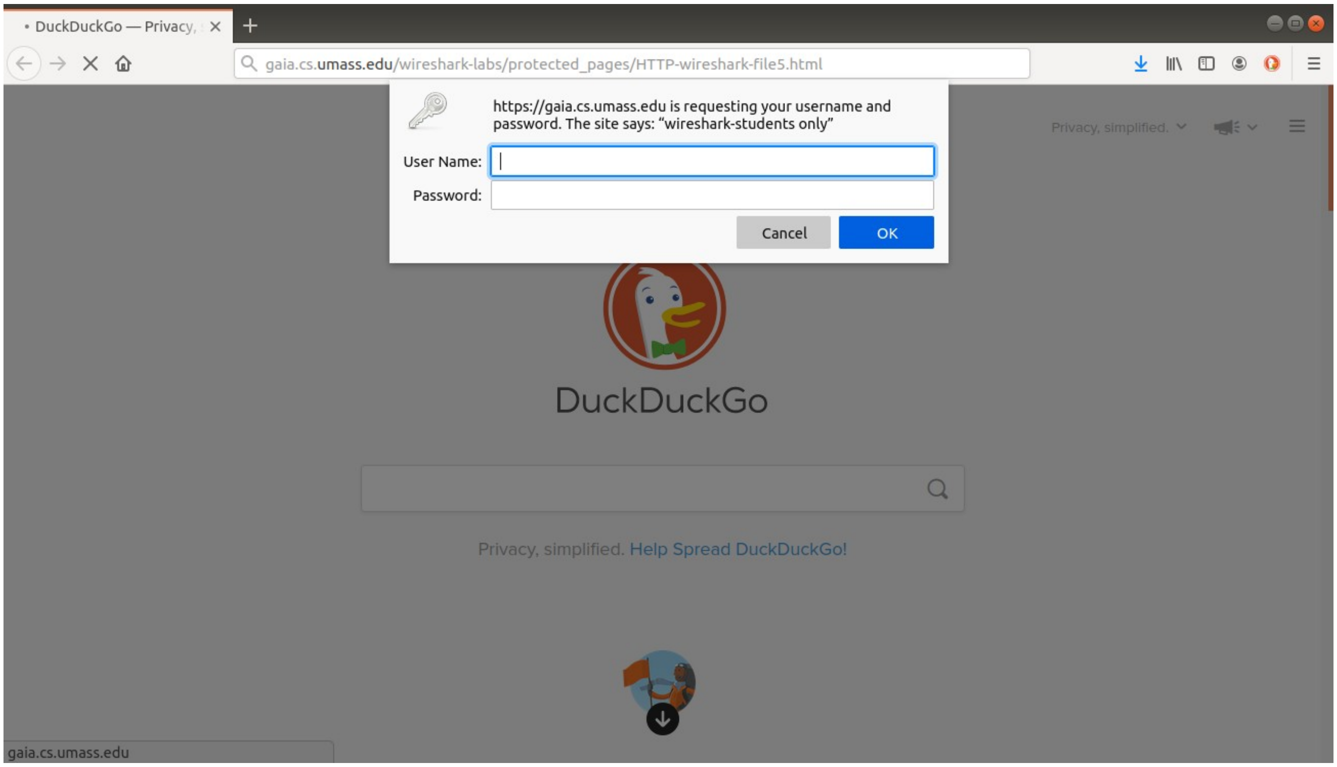
…using this filter: Enter a capture filter …

wlan0
any
Loopback: lo
eth0
gpd0
nflog

You are running Wireshark 2.6.10 (Git v2.6.10 packaged as 2.6.10-1~ubuntu18.04.0).

Ready to load or capture
No Packets

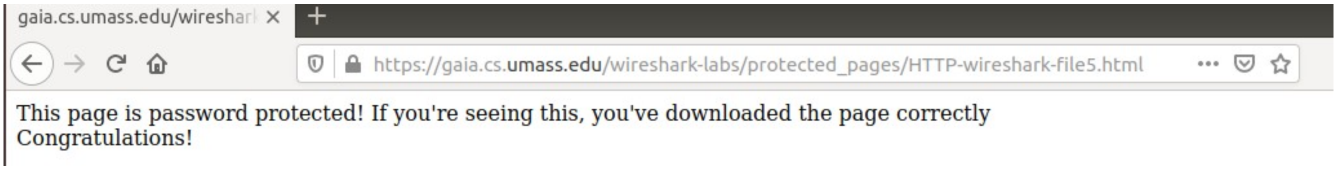
2. Point your browser to http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html.



gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

https://gaia.cs.umass.edu is requesting your username and password. The site says: “wireshark-students only”

User Name:
Password:



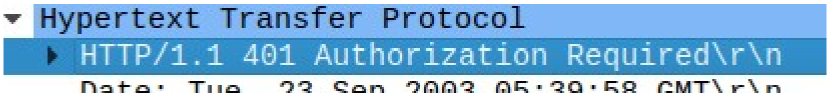
https://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!

Continued Next Page

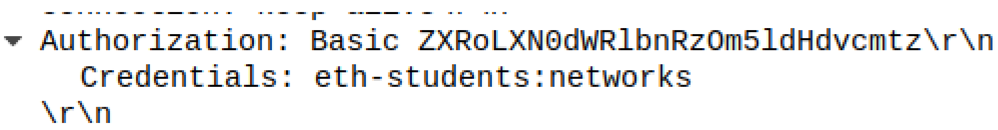
Questions

18. The server responded with code 401 and response phrase Authorization Required.



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 401 Authorization Required\r\n
    Date: Tue, 23 Sep 2003 05:39:58 GMT\r\n
```

19. The second GET message has a field titled Authorization which includes the password networks.



```
▾ Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n
    Credentials: eth-students:networks
  \r\n
```