Linnéuniversitetet
Kalmar Växjö

Assignment 1

Computer networks

khaled Matar - km222uq

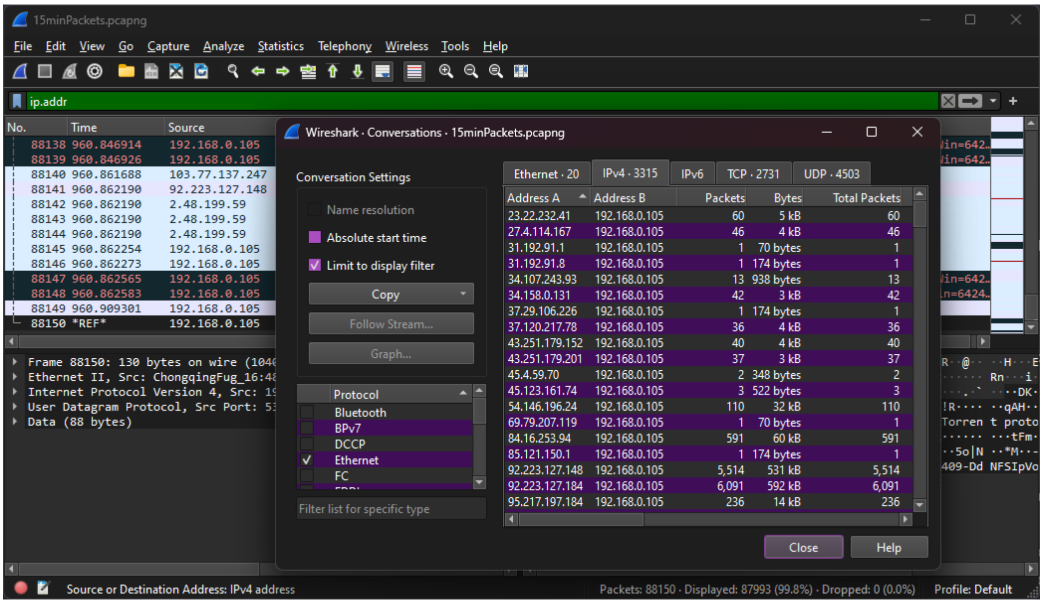
T1-1

TCP: Transmission control protocol is a very important and common protocol. It is a reliable, ordered and error-safe way of delivering streamed data over an IP network.

UDP: User datagram protocol is a communication protocol that is commonly used for transmitting short messages where speed is the main objective, unlike TCP it does not include error correction because it is less important.

Video streaming, phone calls, video calls and online gaming utilize this because the benefits of gaining speed and less delay is worth more than accuracy.

T1-2


15minPackets.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr
Wireshark · Conversations · 15minPackets.pcapng
Copy
Follow Stream...
Graph...
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
Filter list for specific type
Ethernet · 20
IPv4 · 3315
IPv6
TCP · 2731
UDP · 4503
Close
Help

```
No.   Time         Source
88138 960.846914   192.168.0.105
88139 960.846926   192.168.0.105
88140 960.861688   103.77.137.247
88141 960.862190   92.223.127.148
88142 960.862190   2.48.199.59
88143 960.862190   2.48.199.59
88144 960.862190   2.48.199.59
88145 960.862254   192.168.0.105
88146 960.862273   192.168.0.105
88147 960.862565   192.168.0.105
88148 960.862583   192.168.0.105
88149 960.909301   192.168.0.105
88150 *REF*        192.168.0.105

Frame 88150: 130 bytes on wire (1040
Ethernet II, Src: ChongqingFug_16:48
Internet Protocol Version 4, Src: 19
User Datagram Protocol, Src Port: 53
Data (88 bytes)
```

Conversation Settings

☐ Name resolution
☐ Absolute start time
☑ Limit to display filter

Address A	Address B	Packets	Bytes	Total Packets
23.22.232.41	192.168.0.105	60	5 kB	60
27.4.114.167	192.168.0.105	46	4 kB	46
31.192.91.1	192.168.0.105	1	70 bytes	1
31.192.91.8	192.168.0.105	1	174 bytes	1
34.107.243.93	192.168.0.105	13	938 bytes	13
34.158.0.131	192.168.0.105	42	3 kB	42
37.29.106.226	192.168.0.105	1	174 bytes	1
37.120.217.78	192.168.0.105	36	4 kB	36
43.251.179.152	192.168.0.105	40	4 kB	40
43.251.179.201	192.168.0.105	37	3 kB	37
45.4.59.70	192.168.0.105	2	348 bytes	2
45.123.161.74	192.168.0.105	3	522 bytes	3
54.146.196.24	192.168.0.105	110	32 kB	110
69.79.207.119	192.168.0.105	1	70 bytes	1
84.16.253.94	192.168.0.105	591	60 kB	591
85.121.150.1	192.168.0.105	1	174 bytes	1
92.223.127.148	192.168.0.105	5,514	531 kB	5,514
92.223.127.184	192.168.0.105	6,091	592 kB	6,091
95.217.197.184	192.168.0.105	236	14 kB	236

Source or Destination Address: IPv4 address

Packets: 88150 · Displayed: 87993 (99.8%) · Dropped: 0 (0.0%)   Profile: Default

IPv4: 3315
IPv6: 0

T1-3

UDP: Explained above

ICMP: Internet Control Message Protocol is a protocol used to send error messages by pinging and echoing the message back. Used for diagnosis purpose

DNS: Domain Name System used to convert human readble domains, ie www.google.com into an IP address. This is what enables any website to be accessed by the domain name.

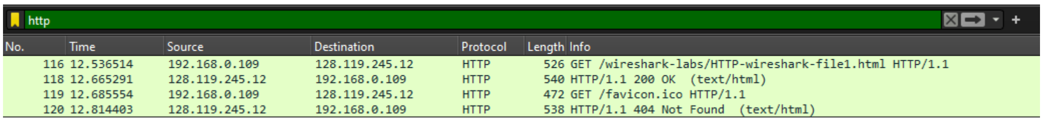
QUIC: Quick UDP Internet Connections is modern protocol developed by Google its designed to be a safer and quicker version of TCP connections.

SSDP: Simple Service Discovery Protocol is protocol for discovering and advertising services on a local network, often associated with universal plug and play (UPnP) devices like printers and media servers.

NBNS: NetBIOS Name Service is a protocol used by windows, it helps translate NetBIOS names into IP address allowing devices to communicate with each other.

Problem 2

T2-1



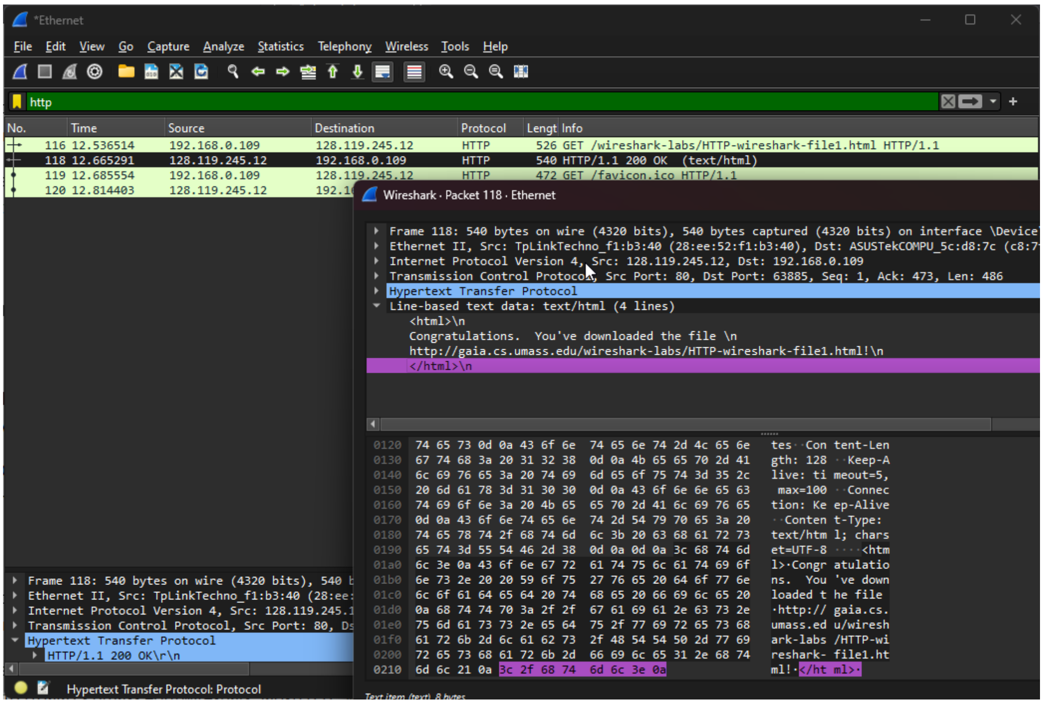
http

No.	Time	Source	Destination	Protocol	Length	Info
116	12.536514	192.168.0.109	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
118	12.665291	128.119.245.12	192.168.0.109	HTTP	540	HTTP/1.1 200 OK (text/html)
119	12.685554	192.168.0.109	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
120	12.814403	128.119.245.12	192.168.0.109	HTTP	538	HTTP/1.1 404 Not Found (text/html)

We can see that my ip, which is 192.168.0.109 is making a get request to 128.119.245.12 to download the file, we can see that in the info column.

We then get an 200 OK response from the server, saying that the request is OK

T2-2


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Wireshark · Packet 118 · Ethernet

```
No.   Time        Source          Destination     Protocol Lengt Info
116 12.536514   192.168.0.109   128.119.245.12  HTTP     526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
118 12.665291   128.119.245.12  192.168.0.109   HTTP     540 HTTP/1.1 200 OK  (text/html)
119 12.685554   192.168.0.109   128.119.245.12  HTTP     472 GET /favicon.ico HTTP/1.1
120 12.814403   128.119.245.12  192.1
```

```
Frame 118: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device
Ethernet II, Src: TpLinkTechno_f1:b3:40 (28:ee:52:f1:b3:40), Dst: ASUSTekCOMPU_5c:d8:7c (c8:7
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.109
Transmission Control Protocol, Src Port: 80, Dst Port: 63885, Seq: 1, Ack: 473, Len: 486
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
```

```
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type:
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
01f0  61 72 6b 2d 6c 61 62 73  2f 48 54 54 50 2d 77 69   ark-labs /HTTP-wi
0200  72 65 73 68 61 72 6b 2d  66 69 6c 65 31 2e 68 74   reshark- file1.ht
0210  6d 6c 21 0a 3c 2f 68 74  6d 6c 3e 0a               ml!·</ht ml>·
```

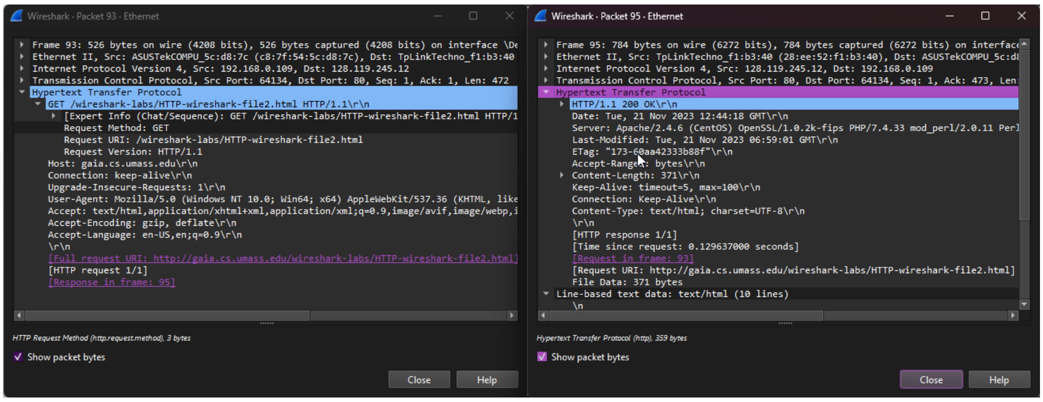
```
Frame 118: 540 bytes on wire (4320 bits), 540 b
Ethernet II, Src: TpLinkTechno_f1:b3:40 (28:ee:
Internet Protocol Version 4, Src: 128.119.245.1
Transmission Control Protocol, Src Port: 80, Ds
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
```

Hypertext Transfer Protocol: Protocol
Text item (text), 8 bytes

Examining the response, we can see the hypertext response, we can see that the response code is 200 that indicates “OK”; we can see the length of the bytes/bits being 540 bytes or 4320 bits.

Problem 3

T3-1



```
Frame 93: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \De
Ethernet II, Src: ASUSTekCOMPU_5c:d8:7c (c8:7f:54:5c:d8:7c), Dst: TpLinkTechno_f1:b3:40
Internet Protocol Version 4, Src: 192.168.0.109, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64134, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
  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
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  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-file2.html]
  [HTTP request 1/1]
  [Response in frame: 95]
```

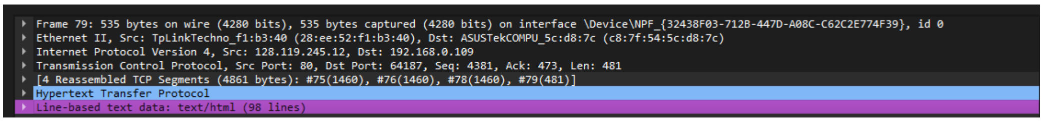
HTTP Request Method (http.request.method), 3 bytes
☑ Show packet bytes
Close
Help
Wireshark · Packet 95 · Ethernet

```
Frame 95: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface
Ethernet II, Src: TpLinkTechno_f1:b3:40 (28:ee:52:f1:b3:40), Dst: ASUSTekCOMPU_5c:d8
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.109
Transmission Control Protocol, Src Port: 80, Dst Port: 64134, Seq: 1, Ack: 473, Len:
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 21 Nov 2023 12:44:18 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl
  Last-Modified: Tue, 21 Nov 2023 06:59:01 GMT\r\n
  ETag: "173-60aa42333b88f"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\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: 0.129637000 seconds]
  [Request in frame: 93]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
Line-based text data: text/html (10 lines)
  \n
```

These are the two packets.

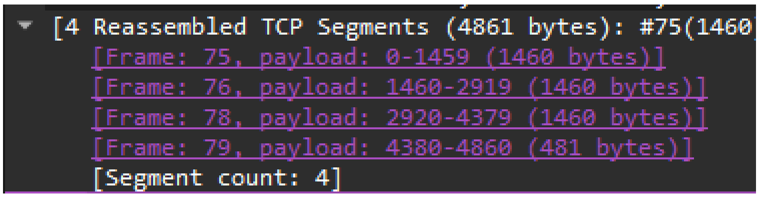
problem 4

T4-1



```
▸ Frame 79: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{32438F03-712B-447D-A08C-C62C2E774F39}, id 0
▸ Ethernet II, Src: TpLinkTechno_f1:b3:40 (28:ee:52:f1:b3:40), Dst: ASUSTekCOMPU_5c:d8:7c (c8:7f:54:5c:d8:7c)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.109
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 64187, Seq: 4381, Ack: 473, Len: 481
▸ [4 Reassembled TCP Segments (4861 bytes): #75(1460), #76(1460), #78(1460), #79(481)]
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (98 lines)
```

We can see that there is 4 reassembled TCp segments, lets unfold and see what has inside



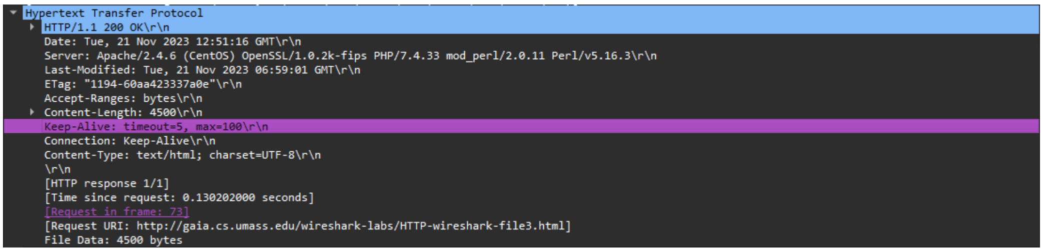
```
▾ [4 Reassembled TCP Segments (4861 bytes): #75(1460
      [Frame: 75, payload: 0-1459 (1460 bytes)]
      [Frame: 76, payload: 1460-2919 (1460 bytes)]
      [Frame: 78, payload: 2920-4379 (1460 bytes)]
      [Frame: 79, payload: 4380-4860 (481 bytes)]
      [Segment count: 4]
```

We can see that the browser only sends a maximum of 1460 bytes, so it had to send it in segments

T4-2

HTTP long polling relies on persistent TCP connections, with clients sending repeated long-polling requests to the server, allowing for real-time communication by keeping connections open and delivering updates when events occur. We can see that in wireshark because we are sending 4 packets back for the long file.

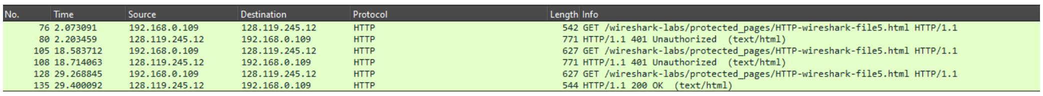
T4-3



```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 21 Nov 2023 12:51:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 21 Nov 2023 06:59:01 GMT\r\n
    ETag: "1194-60aa423337a0e"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 4500\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: 0.130202000 seconds]
    [Request in frame: 73]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
```

The response code is 200, implying that the server response and communication is OK

Problem 5

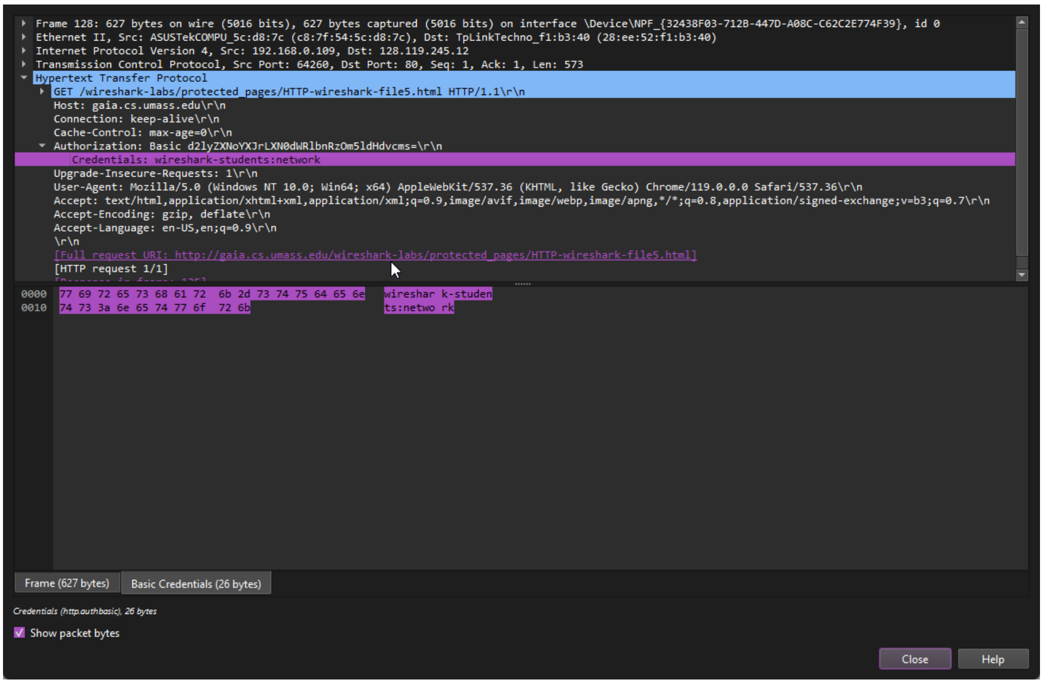


```
No.  Time       Source          Destination     Protocol  Length Info
  76 2.073091   192.168.0.109   128.119.245.12  HTTP         542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  80 2.203459   128.119.245.12  192.168.0.109   HTTP         771 HTTP/1.1 401 Unauthorized  (text/html)
 105 18.583712  192.168.0.109   128.119.245.12  HTTP         627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 108 18.714063  128.119.245.12  192.168.0.109   HTTP         771 HTTP/1.1 401 Unauthorized  (text/html)
 128 29.268845  192.168.0.109   128.119.245.12  HTTP         627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 135 29.400092  128.119.245.12  192.168.0.109   HTTP         544 HTTP/1.1 200 OK  (text/html)
```

I first wrote in the credentials incorrectly, we can see that the HTTp response was Unauthorized for that one.

I then put in the correct credentials and got a 200 OK response, lets investigate more

After opening the GET packet we can observe that the username and password are not secure at all, and can actually be viewed directly in the packet

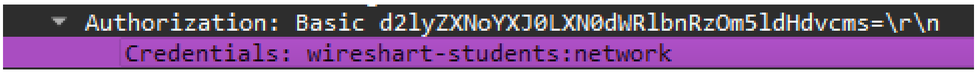


```
> Frame 128: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{32438F03-712B-447D-A08C-C62C2E774F39}, id 0
> Ethernet II, Src: ASUSTekCOMPU_5c:d8:7c (c8:7f:54:5c:d8:7c), Dst: TpLinkTechno_f1:b3:40 (28:ee:52:f1:b3:40)
> Internet Protocol Version 4, Src: 192.168.0.109, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64260, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\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/protected_pages/HTTP-wireshark-file5.html]
    [HTTP request 1/1]

0000  77 69 72 65 73 68 61 72  6b 2d 73 74 75 64 65 6e   wireshar k-studen
0010  74 73 3a 6e 65 74 77 6f  72 6b                     ts:netwo rk
```

Frame (627 bytes)
Basic Credentials (26 bytes)
Credentials (http.authbasic), 26 bytes
☑ Show packet bytes
Close
Help

We can even see my typo in the first packet



```
v Authorization: Basic d2lyZXNoYXJ0LXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshart-students:network
```