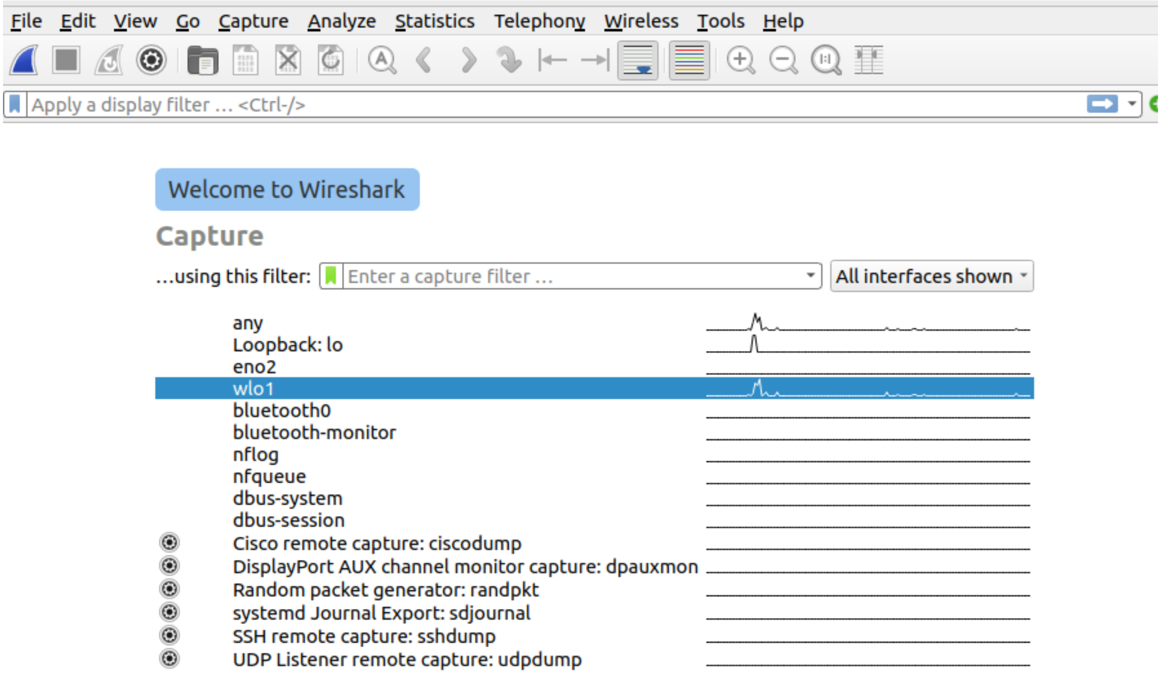
Wireshark Basics

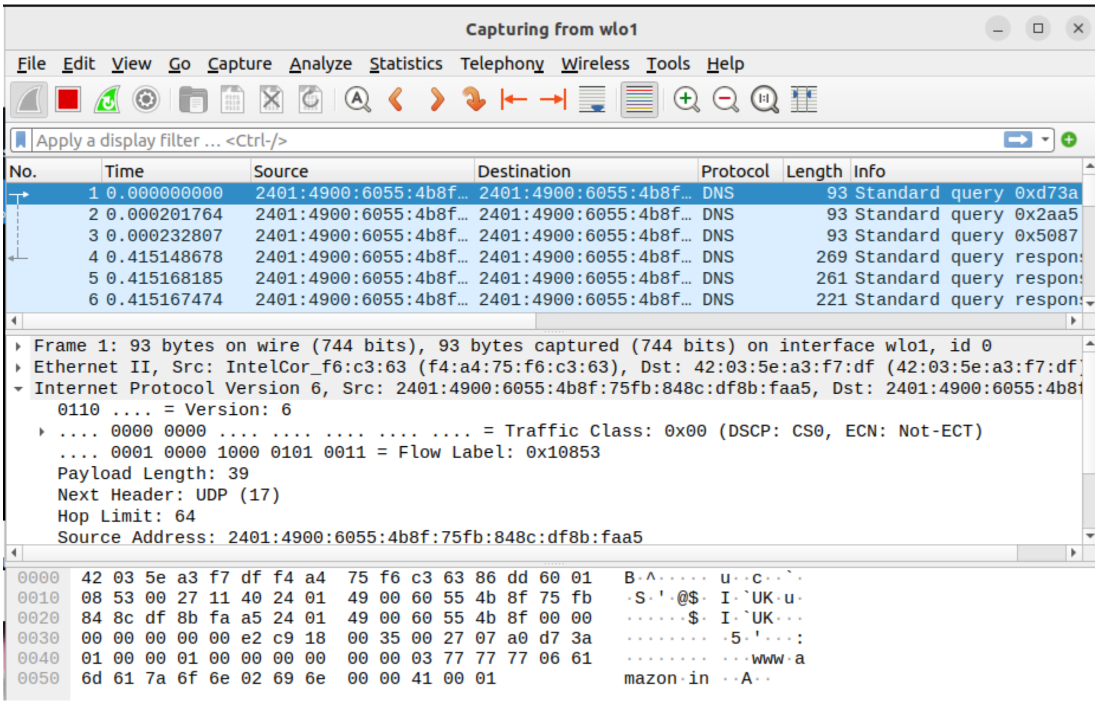
1.Start Wireshark and Select the Network Inteface to capture the packets


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown

any
Loopback: lo
eno2
wlo1
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump

WLO1 -Is my wireless inteface used for internet connection

2. Click Start Capturing and wireshark will diplay all packets captured in the interface.


Capturing from wlo1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	2401:4900:6055:4b8f…	2401:4900:6055:4b8f…	DNS	93	Standard query 0xd73a
2	0.000201764	2401:4900:6055:4b8f…	2401:4900:6055:4b8f…	DNS	93	Standard query 0x2aa5
3	0.000232807	2401:4900:6055:4b8f…	2401:4900:6055:4b8f…	DNS	93	Standard query 0x5087
4	0.415148678	2401:4900:6055:4b8f…	2401:4900:6055:4b8f…	DNS	269	Standard query respon:
5	0.415168185	2401:4900:6055:4b8f…	2401:4900:6055:4b8f…	DNS	261	Standard query respon:
6	0.415167474	2401:4900:6055:4b8f…	2401:4900:6055:4b8f…	DNS	221	Standard query respon:

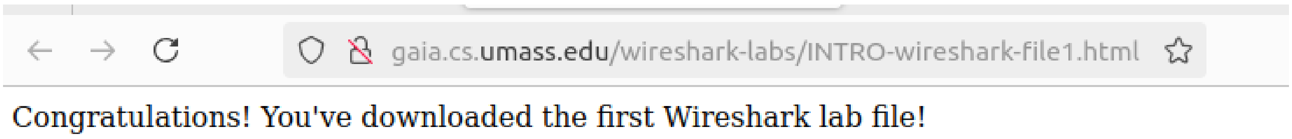
```
▸ Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface wlo1, id 0
▸ Ethernet II, Src: IntelCor_f6:c3:63 (f4:a4:75:f6:c3:63), Dst: 42:03:5e:a3:f7:df (42:03:5e:a3:f7:df)
▾ Internet Protocol Version 6, Src: 2401:4900:6055:4b8f:75fb:848c:df8b:faa5, Dst: 2401:4900:6055:4b8f
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0001 0000 1000 0101 0011 = Flow Label: 0x10853
    Payload Length: 39
    Next Header: UDP (17)
    Hop Limit: 64
    Source Address: 2401:4900:6055:4b8f:75fb:848c:df8b:faa5
```

```
0000  42 03 5e a3 f7 df f4 a4  75 f6 c3 63 86 dd 60 01   B·^·····  u··c··`·
0010  08 53 00 27 11 40 24 01  49 00 60 55 4b 8f 75 fb   ·S·'·@$·  I·`UK·u·
0020  84 8c df 8b fa a5 24 01  49 00 60 55 4b 8f 00 00   ······$·  I·`UK···
0030  00 00 00 00 00 e2 c9 18  00 35 00 27 07 a0 d7 3a   ········  ·5·'···:
0040  01 00 00 01 00 00 00 00  00 00 03 77 77 77 06 61   ········  ···www·a
0050  6d 61 7a 6f 6e 02 69 6e  00 00 41 00 01            mazon·in  ··A··
```

3. Open the following link in browser and allow wireshark to capture the packets.

-http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

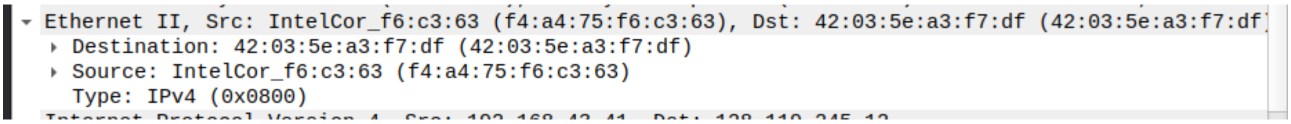
Response in Browser



Congratulations! You've downloaded the first Wireshark lab file!

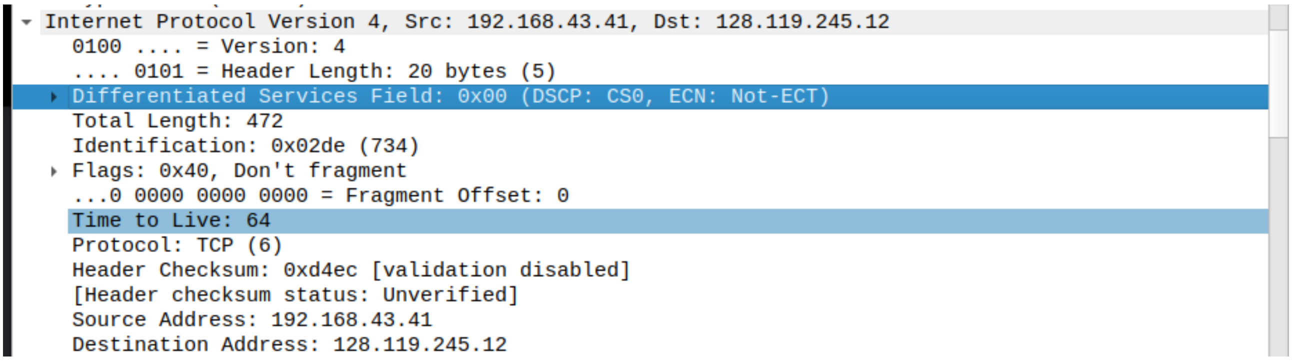
Request in Wireshark

3.1. Ethernet Details



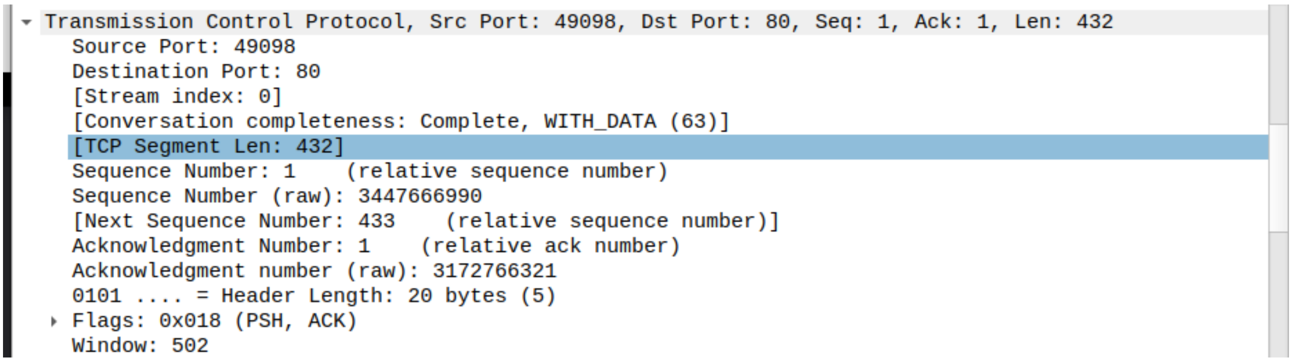
```
▾ Ethernet II, Src: IntelCor_f6:c3:63 (f4:a4:75:f6:c3:63), Dst: 42:03:5e:a3:f7:df (42:03:5e:a3:f7:df)
  ▸ Destination: 42:03:5e:a3:f7:df (42:03:5e:a3:f7:df)
  ▸ Source: IntelCor_f6:c3:63 (f4:a4:75:f6:c3:63)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.43.41, Dst: 128.119.245.12
```

3.2. IP Details



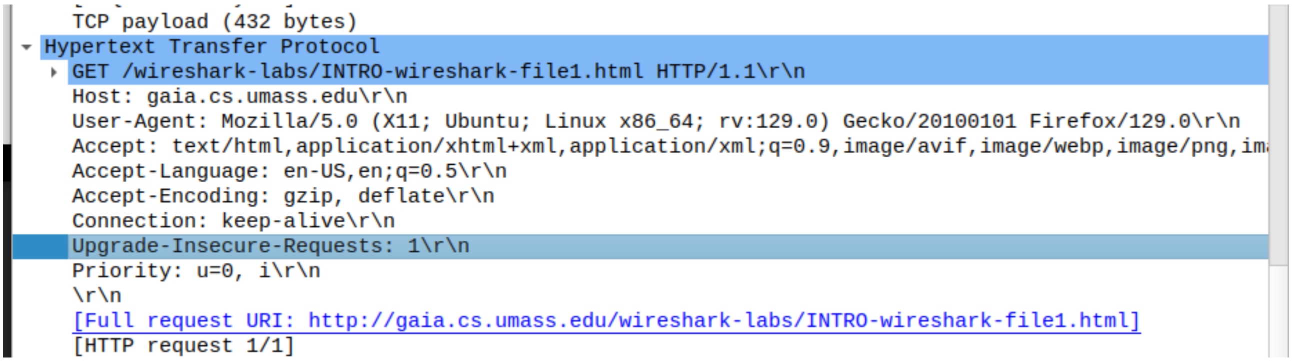
```
▾ Internet Protocol Version 4, Src: 192.168.43.41, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 472
    Identification: 0x02de (734)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xd4ec [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.41
    Destination Address: 128.119.245.12
```

3.3. TCP Details



```
▾ Transmission Control Protocol, Src Port: 49098, Dst Port: 80, Seq: 1, Ack: 1, Len: 432
    Source Port: 49098
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 432]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3447666990
    [Next Sequence Number: 433    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3172766321
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 502
```

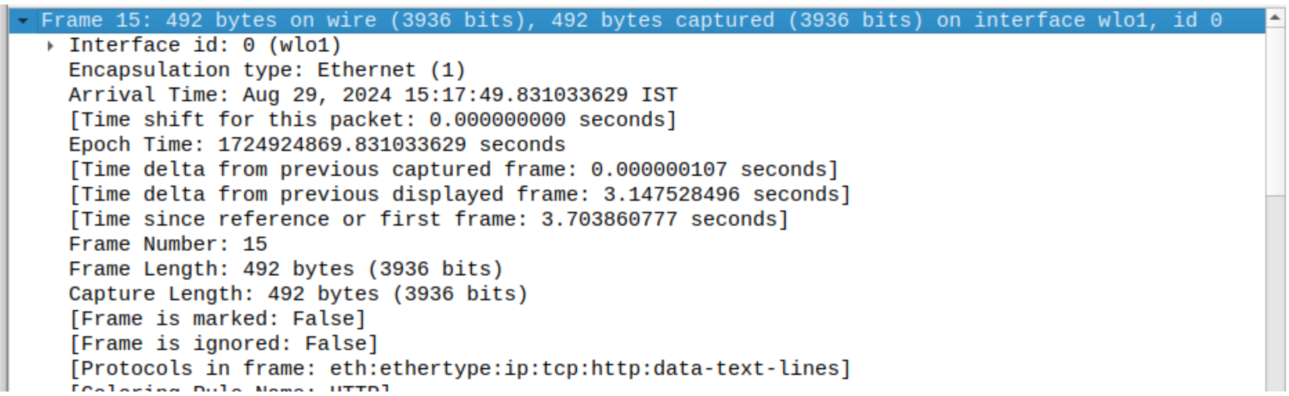
3.4. HTTP header Details



```
TCP payload (432 bytes)
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,im
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
```

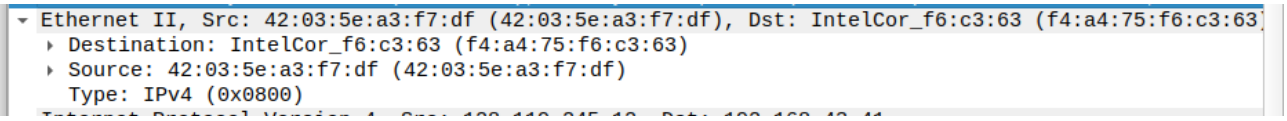
Response in Wireshark

1. Frame Details



```
▾ Frame 15: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface wlo1, id 0
  ▸ Interface id: 0 (wlo1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 29, 2024 15:17:49.831033629 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1724924869.831033629 seconds
    [Time delta from previous captured frame: 0.000000107 seconds]
    [Time delta from previous displayed frame: 3.147528496 seconds]
    [Time since reference or first frame: 3.703860777 seconds]
    Frame Number: 15
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
    [Coloring Rule Name: HTTP]
```

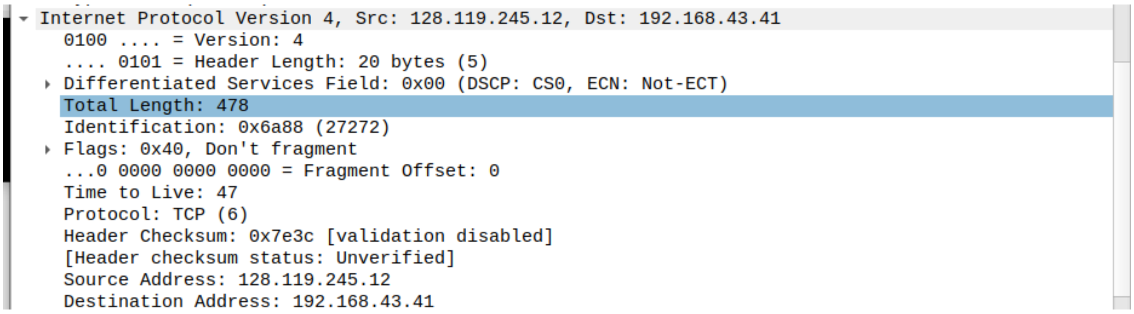
2. Ethernet Details



```
▾ Ethernet II, Src: 42:03:5e:a3:f7:df (42:03:5e:a3:f7:df), Dst: IntelCor_f6:c3:63 (f4:a4:75:f6:c3:63)
  ▸ Destination: IntelCor_f6:c3:63 (f4:a4:75:f6:c3:63)
  ▸ Source: 42:03:5e:a3:f7:df (42:03:5e:a3:f7:df)
    Type: IPv4 (0x0800)
```

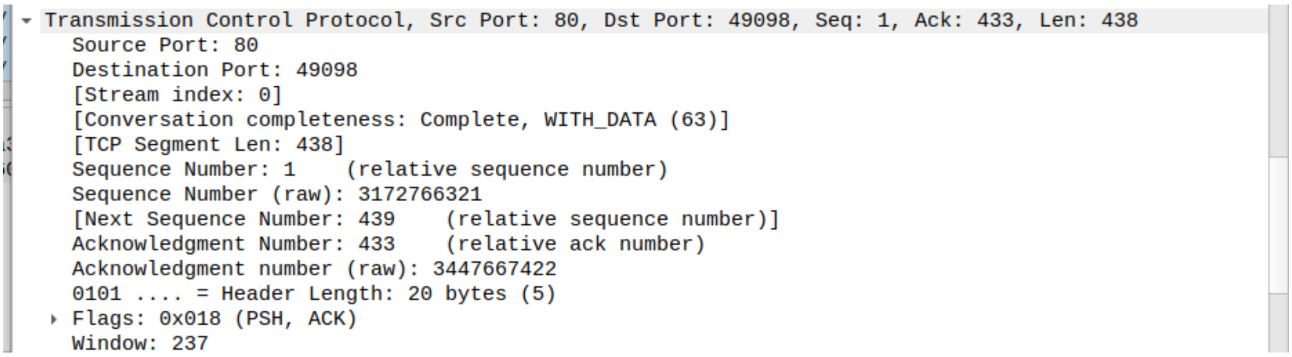
3 IP Details

4.



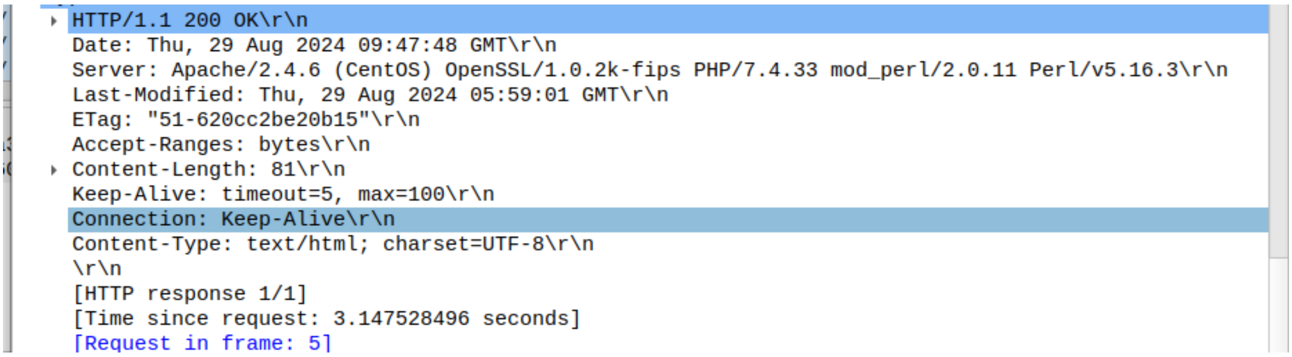
```
▾ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.43.41
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0x6a88 (27272)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 47
    Protocol: TCP (6)
    Header Checksum: 0x7e3c [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.43.41
```

TCP Details



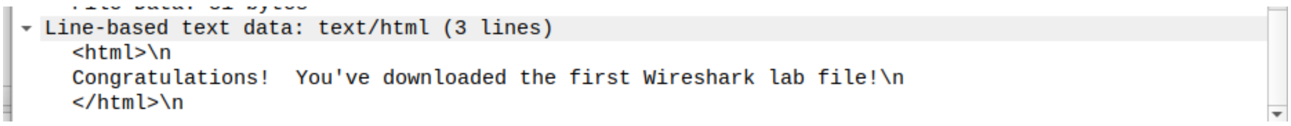
```
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 49098, Seq: 1, Ack: 433, Len: 438
    Source Port: 80
    Destination Port: 49098
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3172766321
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 433    (relative ack number)
    Acknowledgment number (raw): 3447667422
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x018 (PSH, ACK)
    Window: 237
```

5. HTTP header Details



```
  ▸ HTTP/1.1 200 OK\r\n
    Date: Thu, 29 Aug 2024 09:47:48 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: Thu, 29 Aug 2024 05:59:01 GMT\r\n
    ETag: "51-620cc2be20b15"\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: 3.147528496 seconds]
    [Request in frame: 5]
```

6. Data

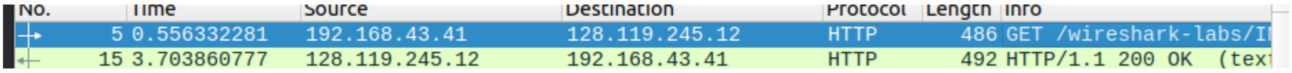


```
▾ Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

Questions Answers

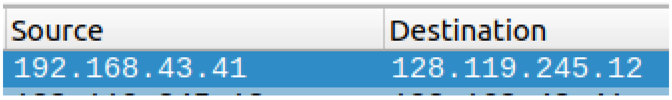
1. TCP

2. Request time – Response time



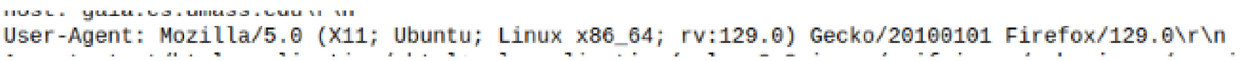
```
No.     Time          Source           Destination      Protocol  Length  Info
      5 0.556332281   192.168.43.41    128.119.245.12   HTTP         486  GET /wireshark-labs/I
     15 3.703860777   128.119.245.12   192.168.43.41    HTTP         492  HTTP/1.1 200 OK  (text
```

3. My ip= Source gaia.cs.umass.edu IP=Destination



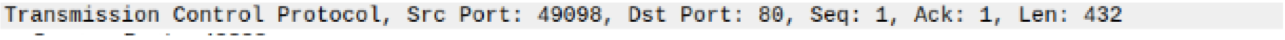
Source	Destination
192.168.43.41	128.119.245.12

4. User agent



```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0\r\n
```

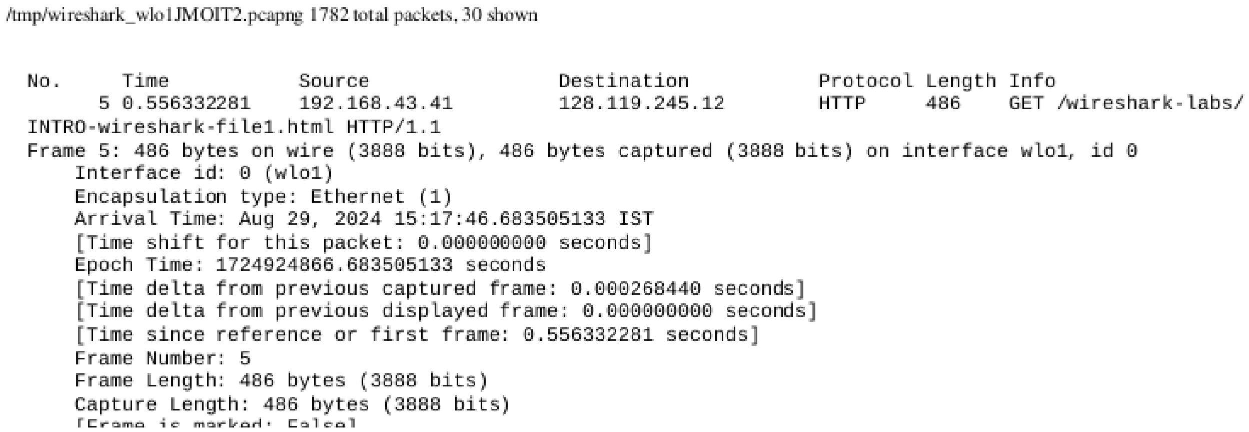
5. Destination Port



```
Transmission Control Protocol, Src Port: 49098, Dst Port: 80, Seq: 1, Ack: 1, Len: 432
```

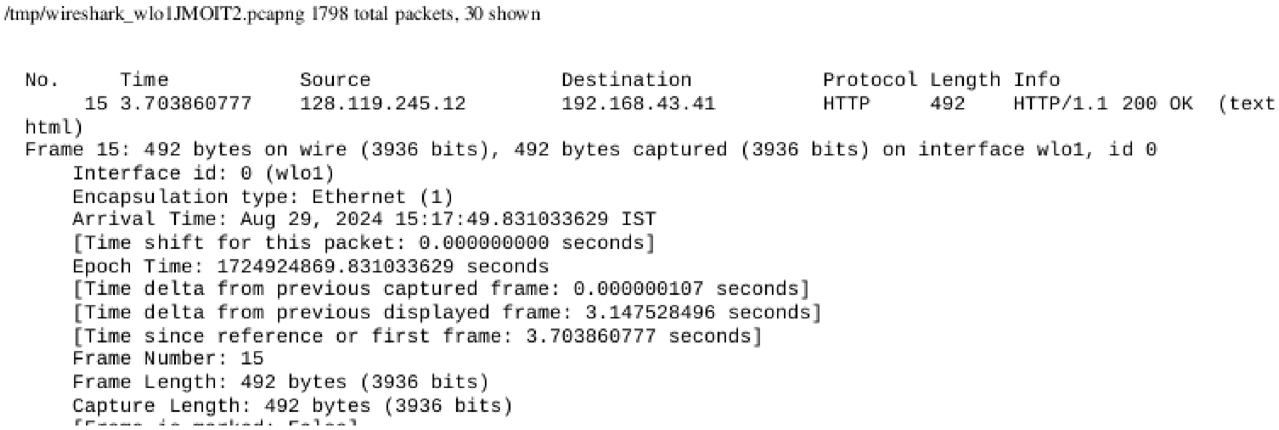
ds

6. HTTP GET request and OK response



/tmp/wireshark_wlo1JMOIT2.pcapng 1782 total packets, 30 shown

```
No.     Time           Source                Destination           Protocol Length Info
      5 0.556332281    192.168.43.41         128.119.245.12        HTTP     486    GET /wireshark-labs/
INTRO-wireshark-file1.html HTTP/1.1
Frame 5: 486 bytes on wire (3888 bits), 486 bytes captured (3888 bits) on interface wlo1, id 0
    Interface id: 0 (wlo1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 29, 2024 15:17:46.683505133 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1724924866.683505133 seconds
    [Time delta from previous captured frame: 0.000268440 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.556332281 seconds]
    Frame Number: 5
    Frame Length: 486 bytes (3888 bits)
    Capture Length: 486 bytes (3888 bits)
    [Frame is marked: False]
```



/tmp/wireshark_wlo1JMOIT2.pcapng 1798 total packets, 30 shown

```
No.     Time           Source                Destination           Protocol Length Info
     15 3.703860777    128.119.245.12        192.168.43.41         HTTP     492    HTTP/1.1 200 OK  (text
html)
Frame 15: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface wlo1, id 0
    Interface id: 0 (wlo1)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 29, 2024 15:17:49.831033629 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1724924869.831033629 seconds
    [Time delta from previous captured frame: 0.000000107 seconds]
    [Time delta from previous displayed frame: 3.147528496 seconds]
    [Time since reference or first frame: 3.703860777 seconds]
    Frame Number: 15
    Frame Length: 492 bytes (3936 bits)
    Capture Length: 492 bytes (3936 bits)
    [Frame is marked: False]
```