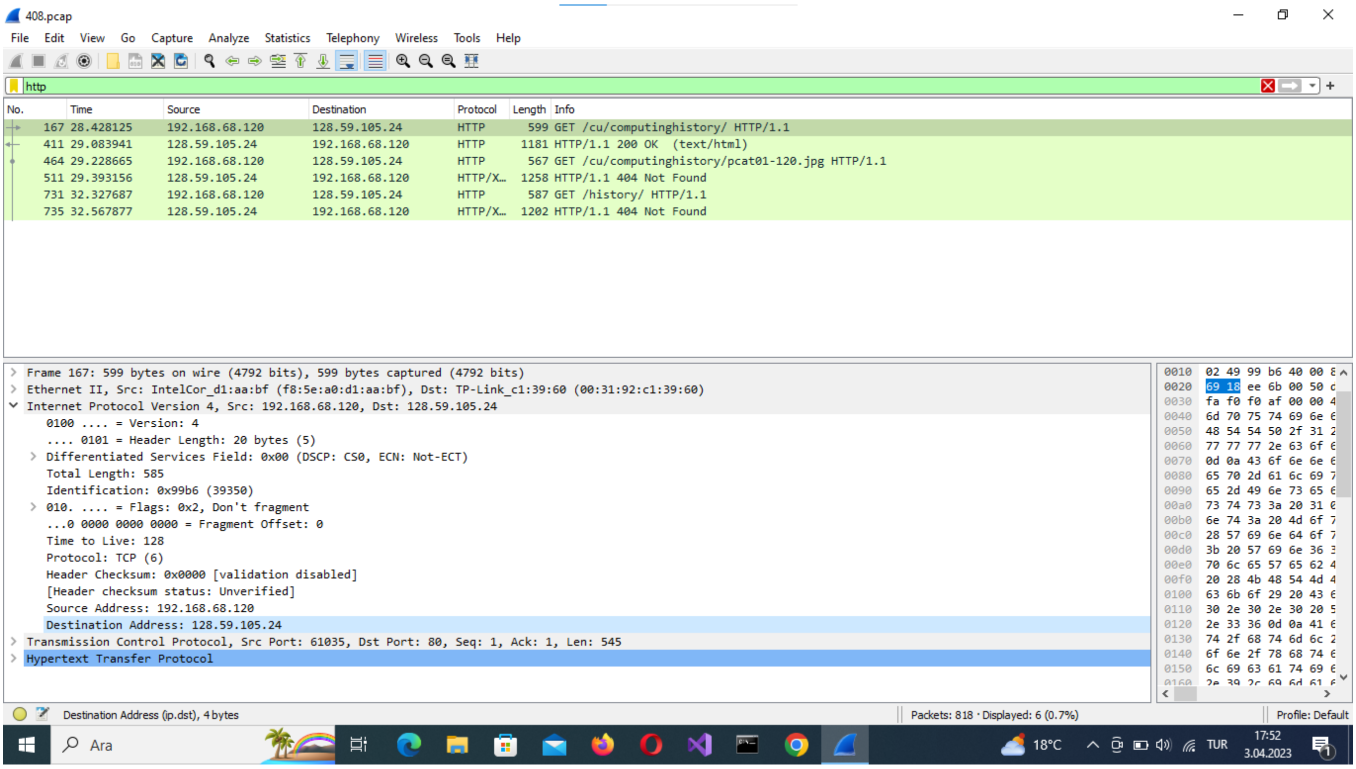
CS408 HW2

1)



408.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source           Destination      Protocol  Length  Info
  167 28.428125     192.168.68.120   128.59.105.24    HTTP        599   GET /cu/computinghistory/ HTTP/1.1
  411 29.083941     128.59.105.24    192.168.68.120   HTTP       1181   HTTP/1.1 200 OK  (text/html)
  464 29.228665     192.168.68.120   128.59.105.24    HTTP        567   GET /cu/computinghistory/pcat01-120.jpg HTTP/1.1
  511 29.393156     128.59.105.24    192.168.68.120   HTTP/X…    1258   HTTP/1.1 404 Not Found
  731 32.327687     192.168.68.120   128.59.105.24    HTTP        587   GET /history/ HTTP/1.1
  735 32.567877     128.59.105.24    192.168.68.120   HTTP/X…    1202   HTTP/1.1 404 Not Found
```

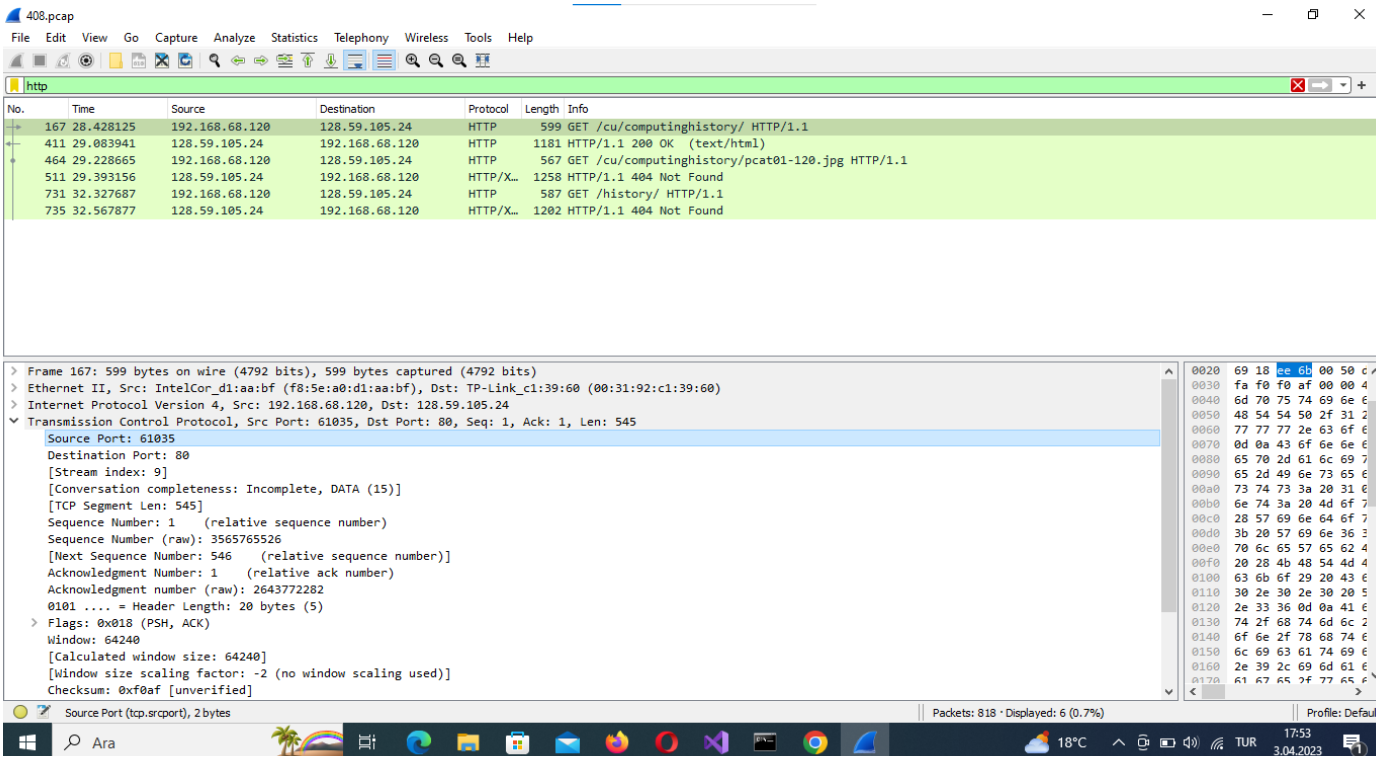
```
> Frame 167: 599 bytes on wire (4792 bits), 599 bytes captured (4792 bits)
> Ethernet II, Src: IntelCor_d1:aa:bf (f8:5e:a0:d1:aa:bf), Dst: TP-Link_c1:39:60 (00:31:92:c1:39:60)
v Internet Protocol Version 4, Src: 192.168.68.120, Dst: 128.59.105.24
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 585
    Identification: 0x99b6 (39350)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.68.120
    Destination Address: 128.59.105.24
> Transmission Control Protocol, Src Port: 61035, Dst Port: 80, Seq: 1, Ack: 1, Len: 545
> Hypertext Transfer Protocol
```

```
0010  02 49 99 b6 40 00
0020  69 18 ee 6b 00 50
0030  fa f0 f0 af 00 00
0040  6d 70 75 74 69 6e
0050  48 54 54 50 2f 31
0060  77 77 77 2e 63 6f
0070  0d 0a 43 6f 6e 6e
0080  65 70 2d 61 6c 69
0090  65 2d 49 6e 73 65
00a0  73 74 73 3a 20 31
00b0  6e 74 3a 20 4d 6f
00c0  28 57 69 6e 64 6f
00d0  3b 20 57 69 6e 36
00e0  70 6c 65 57 65 62
00f0  20 28 4b 48 54 4d
0100  63 6b 6f 29 20 43
0110  30 2e 30 2e 30 20
0120  2e 33 36 0d 0a 41
0130  74 2f 68 74 6d 6c
0140  6f 6e 2f 78 68 74
0150  6c 69 63 61 74 69
```

Destination Address (ip.dst), 4 bytes
Packets: 818 · Displayed: 6 (0.7%)
Profile: Default
Ara
18°C
TUR
17:52
3.04.2023

Here as indicated in the region that is highlighted with the light blue color we may see the destination address. The destination address is the IP address of the website http://columbia.edu/cu/computinghistory/ so the IP address is 128.59.105.24

2)



408.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source           Destination      Protocol  Length  Info
  167 28.428125     192.168.68.120   128.59.105.24    HTTP        599   GET /cu/computinghistory/ HTTP/1.1
  411 29.083941     128.59.105.24    192.168.68.120   HTTP       1181   HTTP/1.1 200 OK  (text/html)
  464 29.228665     192.168.68.120   128.59.105.24    HTTP        567   GET /cu/computinghistory/pcat01-120.jpg HTTP/1.1
  511 29.393156     128.59.105.24    192.168.68.120   HTTP/X…    1258   HTTP/1.1 404 Not Found
  731 32.327687     192.168.68.120   128.59.105.24    HTTP        587   GET /history/ HTTP/1.1
  735 32.567877     128.59.105.24    192.168.68.120   HTTP/X…    1202   HTTP/1.1 404 Not Found
```

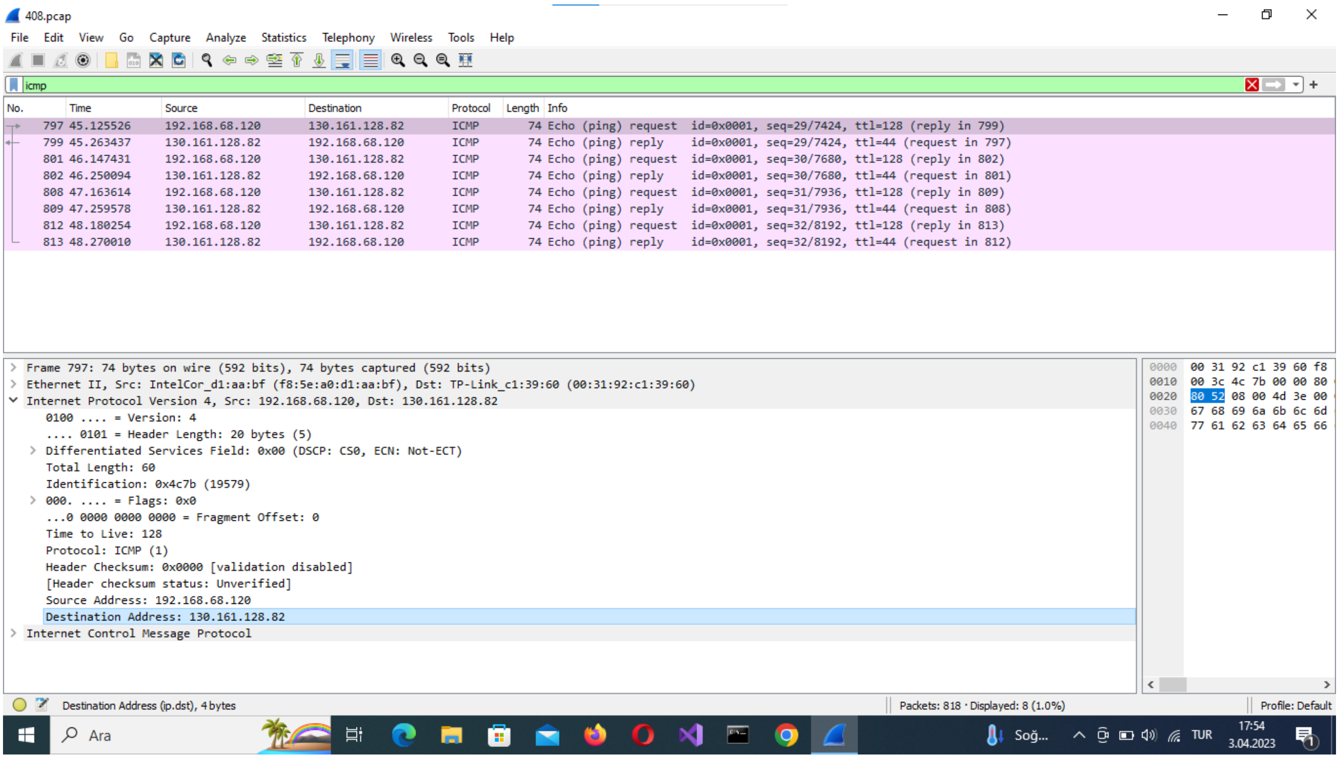
```
> Frame 167: 599 bytes on wire (4792 bits), 599 bytes captured (4792 bits)
> Ethernet II, Src: IntelCor_d1:aa:bf (f8:5e:a0:d1:aa:bf), Dst: TP-Link_c1:39:60 (00:31:92:c1:39:60)
> Internet Protocol Version 4, Src: 192.168.68.120, Dst: 128.59.105.24
v Transmission Control Protocol, Src Port: 61035, Dst Port: 80, Seq: 1, Ack: 1, Len: 545
    Source Port: 61035
    Destination Port: 80
    [Stream index: 9]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 545]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3565765526
    [Next Sequence Number: 546    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2643772282
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xf0af [unverified]
```

```
0020  69 18 ee 6b 00 50
0030  fa f0 f0 af 00 00
0040  6d 70 75 74 69 6e
0050  48 54 54 50 2f 31
0060  77 77 77 2e 63 6f
0070  0d 0a 43 6f 6e 6e
0080  65 70 2d 61 6c 69
0090  65 2d 49 6e 73 65
00a0  73 74 73 3a 20 31
00b0  6e 74 3a 20 4d 6f
00c0  28 57 69 6e 64 6f
00d0  3b 20 57 69 6e 36
00e0  70 6c 65 57 65 62
00f0  20 28 4b 48 54 4d
0100  63 6b 6f 29 20 43
0110  30 2e 30 2e 30 20
0120  2e 33 36 0d 0a 41
0130  74 2f 68 74 6d 6c
0140  6f 6e 2f 78 68 74
0150  6c 69 63 61 74 69
0160  2e 39 2c 69 6d 61
```

Source Port (tcp.srcport), 2 bytes
Packets: 818 · Displayed: 6 (0.7%)
Profile: Defaul
Ara
18°C
TUR
17:53
3.04.2023

As seen in the screenshot the region that is highlighted in light blue indicates the source port which is 61035 and the line below is the destination port which is 80

3)



```
No.     Time           Source             Destination        Protocol  Length Info
    797 45.125526      192.168.68.120     130.161.128.82     ICMP        74 Echo (ping) request  id=0x0001, seq=29/7424, ttl=128 (reply in 799)
    799 45.263437      130.161.128.82     192.168.68.120     ICMP        74 Echo (ping) reply    id=0x0001, seq=29/7424, ttl=44 (request in 797)
    801 46.147431      192.168.68.120     130.161.128.82     ICMP        74 Echo (ping) request  id=0x0001, seq=30/7680, ttl=128 (reply in 802)
    802 46.250094      130.161.128.82     192.168.68.120     ICMP        74 Echo (ping) reply    id=0x0001, seq=30/7680, ttl=44 (request in 801)
    808 47.163614      192.168.68.120     130.161.128.82     ICMP        74 Echo (ping) request  id=0x0001, seq=31/7936, ttl=128 (reply in 809)
    809 47.259578      130.161.128.82     192.168.68.120     ICMP        74 Echo (ping) reply    id=0x0001, seq=31/7936, ttl=44 (request in 808)
    812 48.180254      192.168.68.120     130.161.128.82     ICMP        74 Echo (ping) request  id=0x0001, seq=32/8192, ttl=128 (reply in 813)
    813 48.270010      130.161.128.82     192.168.68.120     ICMP        74 Echo (ping) reply    id=0x0001, seq=32/8192, ttl=44 (request in 812)
```

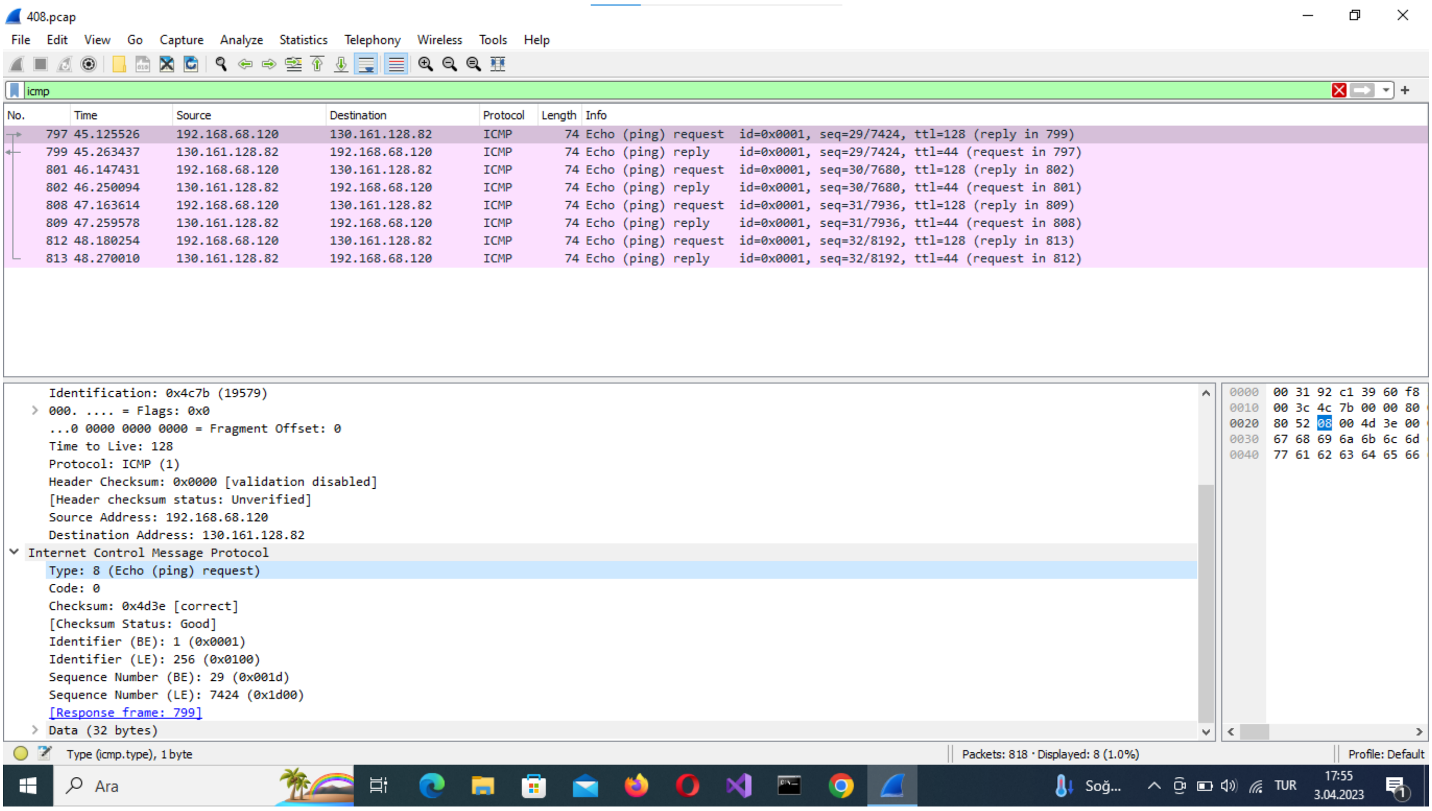
```
> Frame 797: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IntelCor_d1:aa:bf (f8:5e:a0:d1:aa:bf), Dst: TP-Link_c1:39:60 (00:31:92:c1:39:60)
v Internet Protocol Version 4, Src: 192.168.68.120, Dst: 130.161.128.82
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x4c7b (19579)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.68.120
    Destination Address: 130.161.128.82
> Internet Control Message Protocol
```

```
0000  00 31 92 c1 39 60 f8
0010  00 3c 4c 7b 00 00 80
0020  80 52 08 00 4d 3e 00
0030  67 68 69 6a 6b 6c 6d
0040  77 61 62 63 64 65 66
```

```
Destination Address (ip.dst), 4 bytes        Packets: 818 · Displayed: 8 (1.0%)        Profile: Default
```

Again as described we may find the IP number by first searching icmp then again we may find the destination address which is the IP address of the tudelft.tu domain; IP address is 130.161.68.120

4)


408.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Ara
Soğ...
TUR
17:55
3.04.2023

icmp

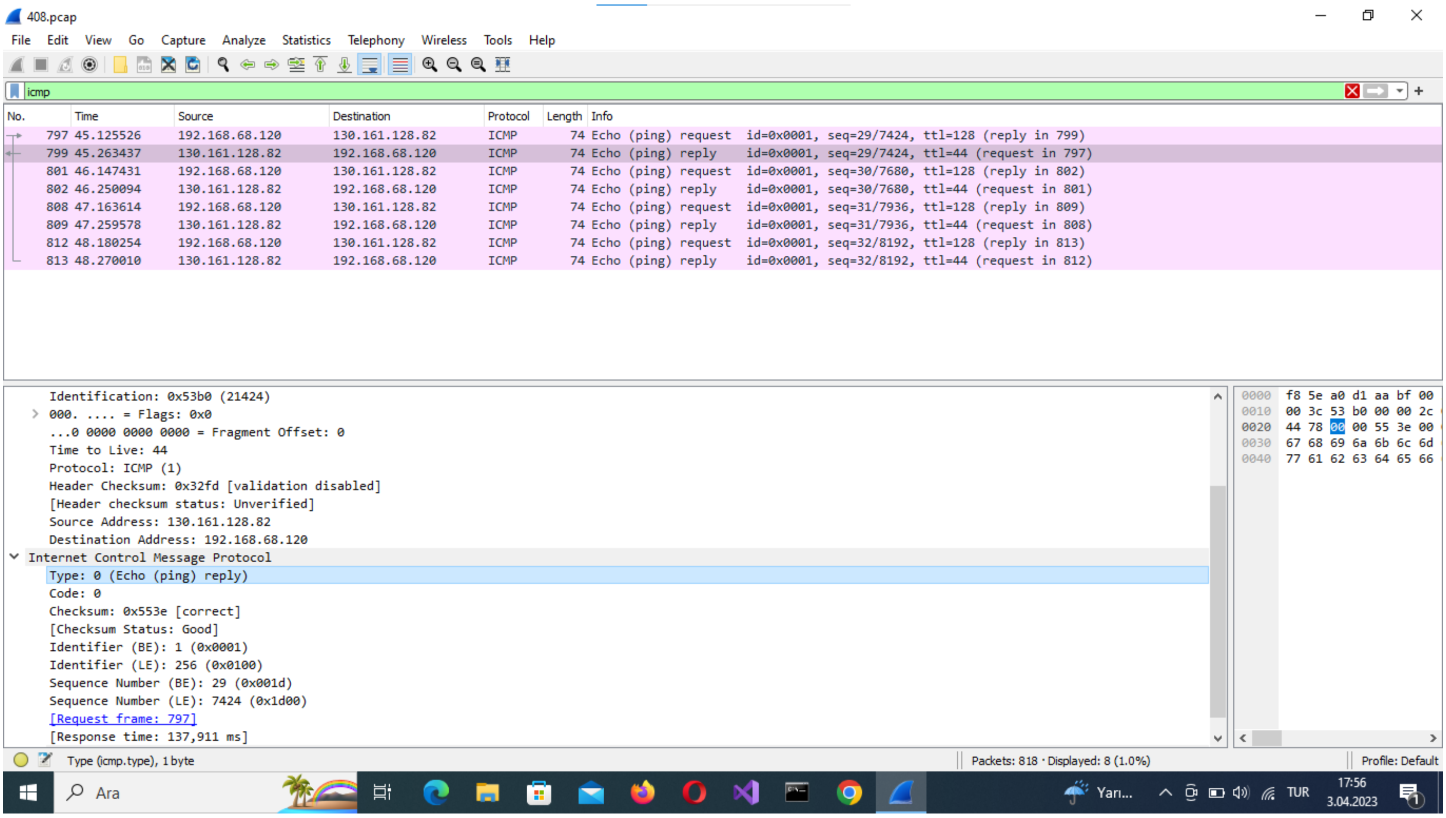
```
No.   Time       Source          Destination     Protocol Length Info
  797 45.125526  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=29/7424, ttl=128 (reply in 799)
  799 45.263437  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=29/7424, ttl=44 (request in 797)
  801 46.147431  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=30/7680, ttl=128 (reply in 802)
  802 46.250094  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=30/7680, ttl=44 (request in 801)
  808 47.163614  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=31/7936, ttl=128 (reply in 809)
  809 47.259578  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=31/7936, ttl=44 (request in 808)
  812 48.180254  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=32/8192, ttl=128 (reply in 813)
  813 48.270010  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=32/8192, ttl=44 (request in 812)
```

```
    Identification: 0x4c7b (19579)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.68.120
    Destination Address: 130.161.128.82
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d3e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 29 (0x001d)
    Sequence Number (LE): 7424 (0x1d00)
    [Response frame: 799]
  > Data (32 bytes)
```

```
0000  00 31 92 c1 39 60 f8
0010  00 3c 4c 7b 00 00 80
0020  80 52 08 00 4d 3e 00
0030  67 68 69 6a 6b 6c 6d
0040  77 61 62 63 64 65 66
```

Type (icmp.type), 1 byte | Packets: 818 · Displayed: 8 (1.0%) | Profile: Default

After selecting the request, below in the blue highlighted region we may see the type number of the request which is indicated as 8 (echo ping request)


408.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Ara
Yan...
TUR
17:56
3.04.2023

icmp

```
No.   Time       Source          Destination     Protocol Length Info
  797 45.125526  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=29/7424, ttl=128 (reply in 799)
  799 45.263437  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=29/7424, ttl=44 (request in 797)
  801 46.147431  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=30/7680, ttl=128 (reply in 802)
  802 46.250094  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=30/7680, ttl=44 (request in 801)
  808 47.163614  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=31/7936, ttl=128 (reply in 809)
  809 47.259578  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=31/7936, ttl=44 (request in 808)
  812 48.180254  192.168.68.120  130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=32/8192, ttl=128 (reply in 813)
  813 48.270010  130.161.128.82  192.168.68.120  ICMP       74 Echo (ping) reply    id=0x0001, seq=32/8192, ttl=44 (request in 812)
```

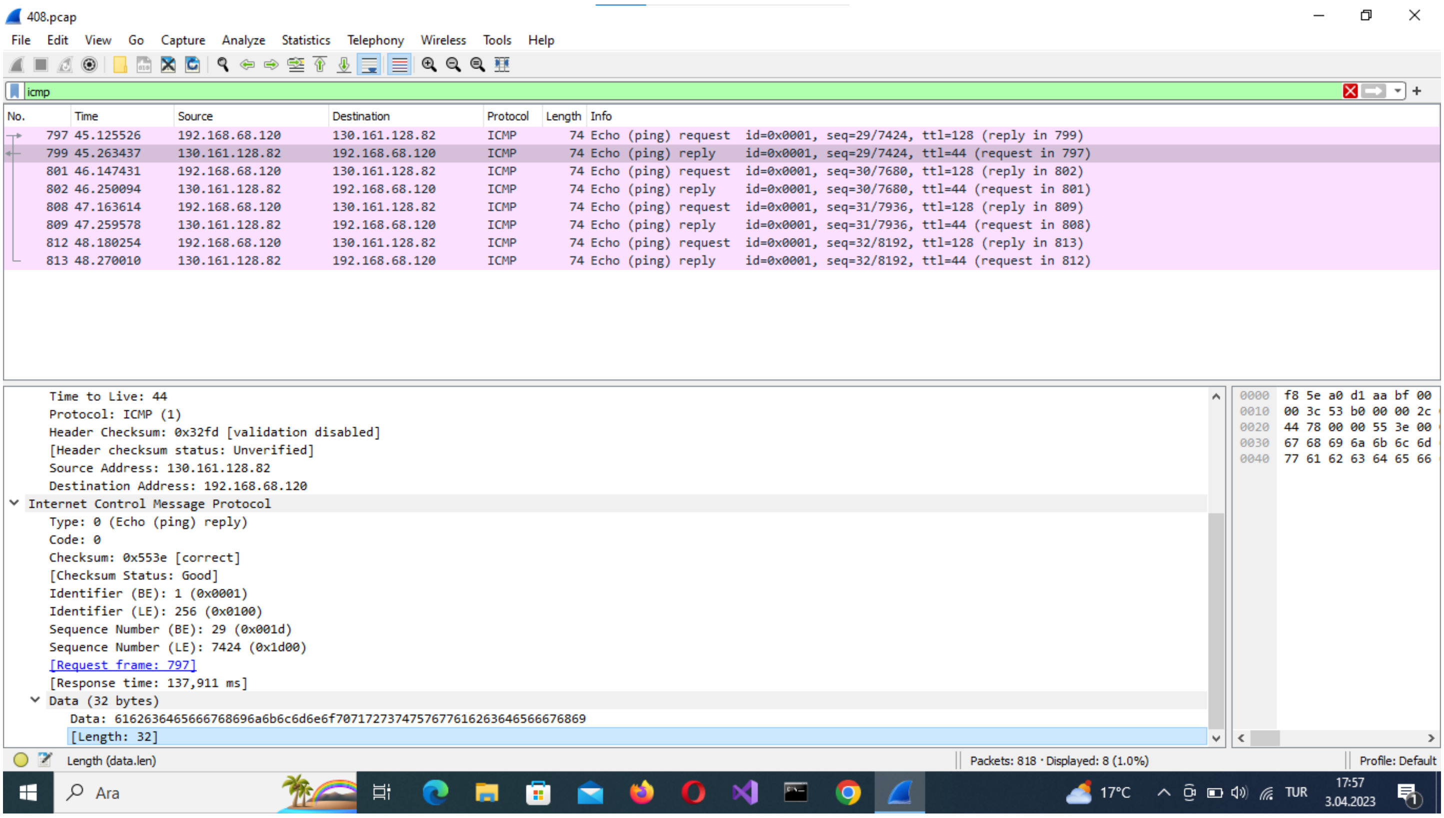
```
    Identification: 0x53b0 (21424)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 44
    Protocol: ICMP (1)
    Header Checksum: 0x32fd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 130.161.128.82
    Destination Address: 192.168.68.120
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x553e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 29 (0x001d)
    Sequence Number (LE): 7424 (0x1d00)
    [Request frame: 797]
    [Response time: 137,911 ms]
```

```
0000  f8 5e a0 d1 aa bf 00
0010  00 3c 53 b0 00 00 2c
0020  44 78 00 00 55 3e 00
0030  67 68 69 6a 6b 6c 6d
0040  77 61 62 63 64 65 66
```

Type (icmp.type), 1 byte | Packets: 818 · Displayed: 8 (1.0%) | Profile: Default

Similarly, if we want to know the type number of the reply, we simply select reply and then we may see the type number of the reply which is indicated as 0 (echo ping reply)

5)


408.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.  Time      Source          Destination     Protocol Length Info
797 45.125526  192.168.68.120  130.161.128.82  ICMP      74 Echo (ping) request  id=0x0001, seq=29/7424, ttl=128 (reply in 799)
799 45.263437  130.161.128.82  192.168.68.120  ICMP      74 Echo (ping) reply    id=0x0001, seq=29/7424, ttl=44 (request in 797)
801 46.147431  192.168.68.120  130.161.128.82  ICMP      74 Echo (ping) request  id=0x0001, seq=30/7680, ttl=128 (reply in 802)
802 46.250094  130.161.128.82  192.168.68.120  ICMP      74 Echo (ping) reply    id=0x0001, seq=30/7680, ttl=44 (request in 801)
808 47.163614  192.168.68.120  130.161.128.82  ICMP      74 Echo (ping) request  id=0x0001, seq=31/7936, ttl=128 (reply in 809)
809 47.259578  130.161.128.82  192.168.68.120  ICMP      74 Echo (ping) reply    id=0x0001, seq=31/7936, ttl=44 (request in 808)
812 48.180254  192.168.68.120  130.161.128.82  ICMP      74 Echo (ping) request  id=0x0001, seq=32/8192, ttl=128 (reply in 813)
813 48.270010  130.161.128.82  192.168.68.120  ICMP      74 Echo (ping) reply    id=0x0001, seq=32/8192, ttl=44 (request in 812)
```

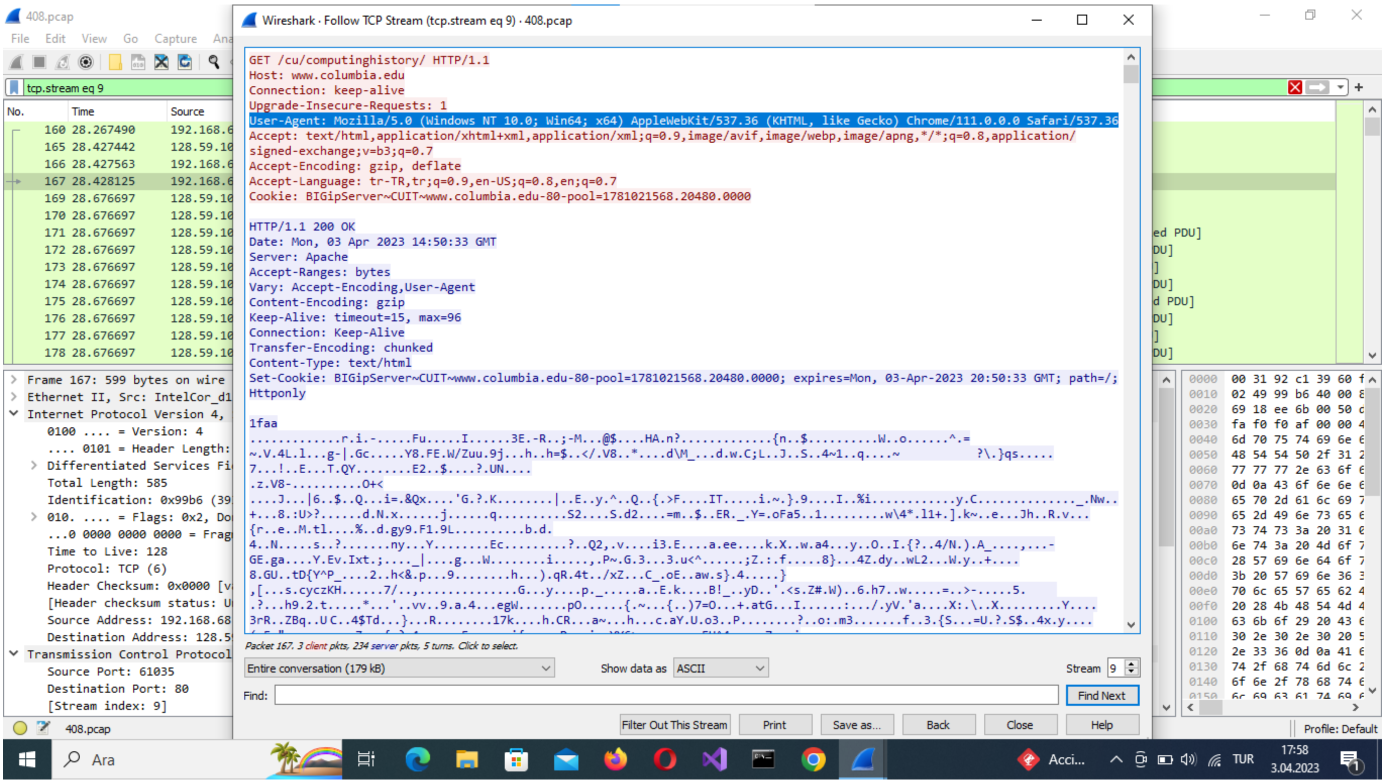
```
    Time to Live: 44
    Protocol: ICMP (1)
    Header Checksum: 0x32fd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 130.161.128.82
    Destination Address: 192.168.68.120
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x553e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 29 (0x001d)
    Sequence Number (LE): 7424 (0x1d00)
    [Request frame: 797]
    [Response time: 137,911 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  f8 5e a0 d1 aa bf 00
0010  00 3c 53 b0 00 00 2c
0020  44 78 00 00 55 3e 00
0030  67 68 69 6a 6b 6c 6d
0040  77 61 62 63 64 65 66
```

We may see the length of the data field of ICMP Echo reply packet from tudelft.nl; if we use the search bar to search for icmp, then select the reply package, finally inside the Data option we may see the length of the data (blue highlighted region) which is 32 bytes

6) id.addr == 192.105.59.24 && tcp.port == 1334 the first part of the filter before && is used to specify an IP address and the second part is used to provide a specific TCP port destination

7) The below blue highlighted region simply shows us the User Agent for the HTTP requests send by my browser, I have reached this page by; clicking Follow -> TCP Stream



```
408.pcap
tcp.stream eq 9

No.  Time       Source
160 28.267490  192.168.6
165 28.427442  128.59.10
166 28.427563  192.168.6
167 28.428125  192.168.6
169 28.676697  128.59.10
170 28.676697  128.59.10
171 28.676697  128.59.10
172 28.676697  128.59.10
173 28.676697  128.59.10
174 28.676697  128.59.10
175 28.676697  128.59.10
176 28.676697  128.59.10
177 28.676697  128.59.10
178 28.676697  128.59.10

> Frame 167: 599 bytes on wire
> Ethernet II, Src: IntelCor_d1
v Internet Protocol Version 4,
    0100 .... = Version: 4
    .... 0101 = Header Length:
  > Differentiated Services Fi
    Total Length: 585
    Identification: 0x99b6 (39
  > 010. .... = Flags: 0x2, Do
    ...0 0000 0000 0000 = Frag
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [v
    [Header checksum status: U
    Source Address: 192.168.68
    Destination Address: 128.5
v Transmission Control Protocol
    Source Port: 61035
    Destination Port: 80
    [Stream index: 9]
```

Wireshark · Follow TCP Stream (tcp.stream eq 9) · 408.pcap

```
GET /cu/computinghistory/ HTTP/1.1
Host: www.columbia.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/111.0.0.0 Safari/537.36
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
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1781021568.20480.0000

HTTP/1.1 200 OK
Date: Mon, 03 Apr 2023 14:50:33 GMT
Server: Apache
Accept-Ranges: bytes
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Keep-Alive: timeout=15, max=96
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
Set-Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1781021568.20480.0000; expires=Mon, 03-Apr-2023 20:50:33 GMT; path=/;
Httponly

1faa
............r.i.-.....Fu.....I......3E.-R..;-M...@$....HA.n?.............{n..$..........W..o......^.=
~.V.4L.l...g-|.Gc.....Y8.FE.W/Zuu.9j...h..h=$..</.V8..*....d\M_...d.w.C;L..J..S..4~1..q....~          ?\.}qs.....
7...!..E...T.QY........E2..$....?.UN....
.z.V8-..........O+<
....J...|6..$..Q...i=.&Qx....'G.?.K........|..E..y.^..Q..{.>F....IT.....i.~.}.9....I..%i...........y.C..............._.Nw..
+...8.:U>?......d.N.x......j......q..........S2....S.d2....=m..$..ER._.Y=.oFa5..1.........w\4*.l1+.].k~..e...Jh..R.v...
{r..e..M.tl....%..d.gy9.F1.9L..........b.d.
4..N.....s..?.......ny...Y........Ec.........?..Q2,.v....i3.E....a.ee....k.X..w.a4...y..O..I.{?..4/N.).A_....,...-
GE.ga....Y.Ev.Ixt.;...._|....g...W........i.....,.P~.G.3...3.u<^......;Z.:.f.....8}...4Z.dy..wL2...W.y..+....
8.GU..tD{Y^P_....2..h<&.p...9........h...).qR.4t../xZ...C_.oE..aw.s}.4.....}
,[...s.cyczKH......7/..,.............G...y....p._.....a..E.k....B!_..yD..'.<s.Z#.W)..6.h7..w.....=..>-.....5.
.?...h9.2.t.....*...'..vv..9.a.4...egW.......pO......{.~...{..)7=O...+.atG...I......:.../.yV.'a....X:.\..X.........Y....
3rR..ZBq..U C..4$Td...}...R........17k....h.CR...a~...h...c.aY.U.o3..P........?..o:.m3.......f..3.{S...=U.?.S$..4x.y....
```

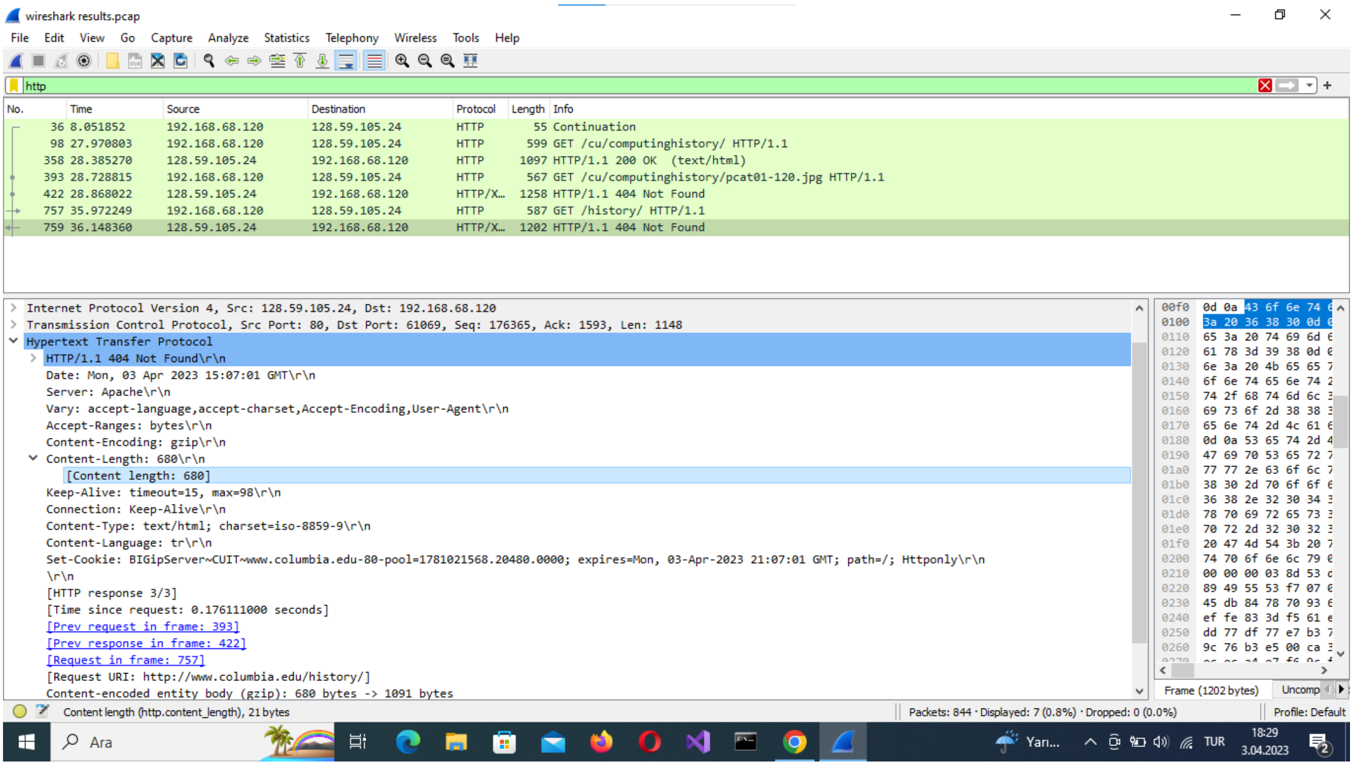
Packet 167. 3 client pkts, 234 server pkts, 5 turns. Click to select.

Entire conversation (179 kB) | Show data as ASCII | Stream 9

Find: | Find Next

```
0000  00 31 92 c1 39 60 f
0010  02 49 99 b6 40 00 8
0020  69 18 ee 6b 00 50 c
0030  fa f0 f0 af 00 00 4
0040  6d 70 75 74 69 6e 6
0050  48 54 54 50 2f 31 2
0060  77 77 77 2e 63 6f 6
0070  0d 0a 43 6f 6e 6e 6
0080  65 70 2d 61 6c 69 7
0090  65 2d 49 6e 73 65 6
00a0  73 74 73 3a 20 31 0
00b0  6e 74 3a 20 4d 6f 7
00c0  28 57 69 6e 64 6f 7
00d0  3b 20 57 69 6e 36 3
00e0  70 6c 65 57 65 62 4
00f0  20 28 4b 48 54 4d 4
0100  63 6b 6f 29 20 43 6
0110  30 2e 30 2e 30 20 5
0120  2e 33 36 0d 0a 41 6
0130  74 2f 68 74 6d 6c 2
0140  6f 6e 2f 78 68 74 6
```

8) The content length is indicated in the light blue region which is stated as 680



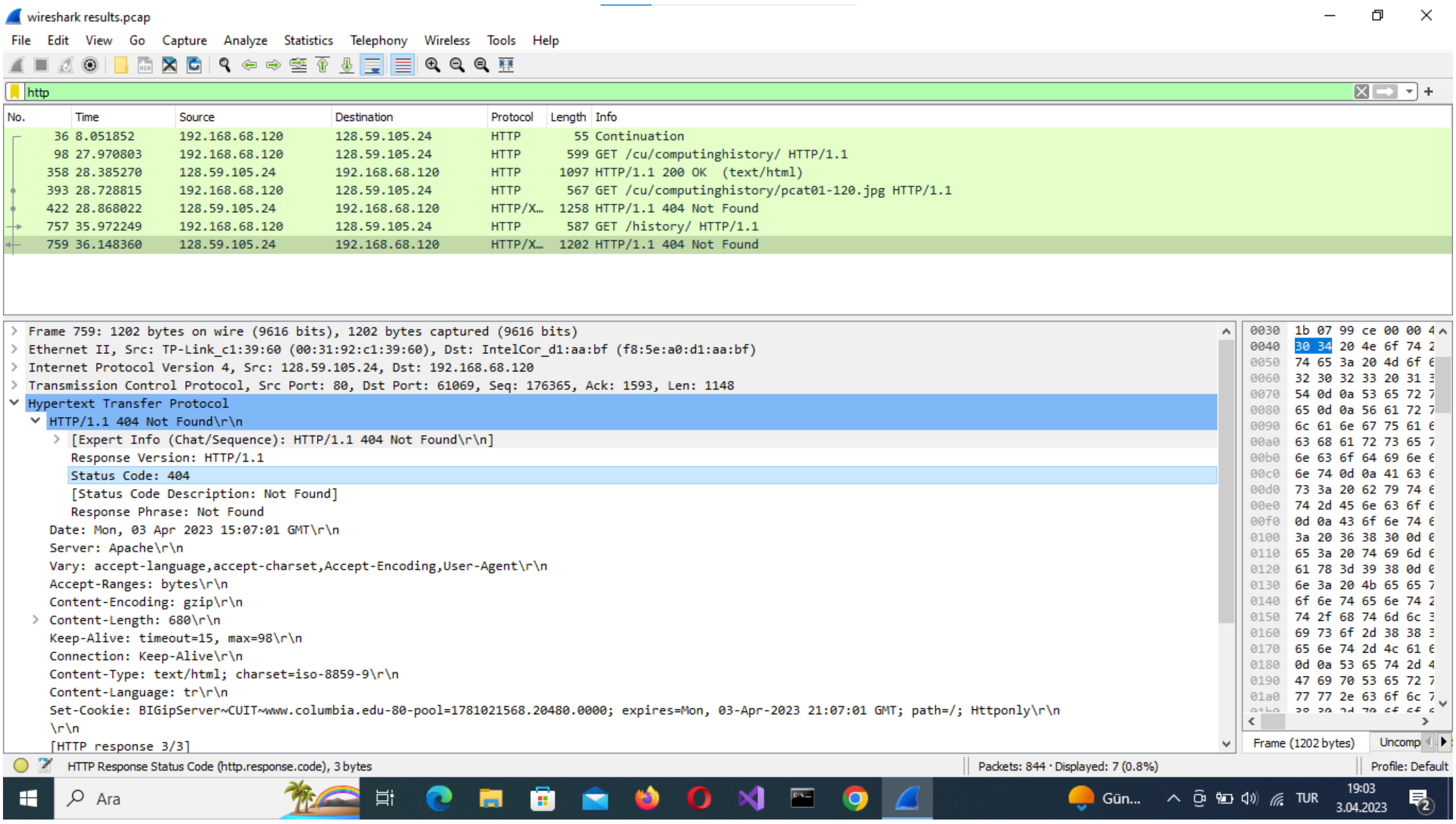
wireshark results.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.  Time        Source          Destination     Protocol  Length Info
 36  8.051852    192.168.68.120  128.59.105.24   HTTP        55 Continuation
 98  27.970803   192.168.68.120  128.59.105.24   HTTP       599 GET /cu/computinghistory/ HTTP/1.1
358  28.385270   128.59.105.24   192.168.68.120  HTTP      1097 HTTP/1.1 200 OK  (text/html)
393  28.728815   192.168.68.120  128.59.105.24   HTTP       567 GET /cu/computinghistory/pcat01-120.jpg HTTP/1.1
422  28.868022   128.59.105.24   192.168.68.120  HTTP/X…   1258 HTTP/1.1 404 Not Found
757  35.972249   192.168.68.120  128.59.105.24   HTTP       587 GET /history/ HTTP/1.1
759  36.148360   128.59.105.24   192.168.68.120  HTTP/X…   1202 HTTP/1.1 404 Not Found

> Internet Protocol Version 4, Src: 128.59.105.24, Dst: 192.168.68.120
> Transmission Control Protocol, Src Port: 80, Dst Port: 61069, Seq: 176365, Ack: 1593, Len: 1148
v Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Mon, 03 Apr 2023 15:07:01 GMT\r\n
    Server: Apache\r\n
    Vary: accept-language,accept-charset,Accept-Encoding,User-Agent\r\n
    Accept-Ranges: bytes\r\n
    Content-Encoding: gzip\r\n
  v Content-Length: 680\r\n
      [Content length: 680]
    Keep-Alive: timeout=15, max=98\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-9\r\n
    Content-Language: tr\r\n
    Set-Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1781021568.20480.0000; expires=Mon, 03-Apr-2023 21:07:01 GMT; path=/; Httponly\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.176111000 seconds]
    [Prev request in frame: 393]
    [Prev response in frame: 422]
    [Request in frame: 757]
    [Request URI: http://www.columbia.edu/history/]
    Content-encoded entity body (gzip): 680 bytes -> 1091 bytes

00f0  0d 0a 43 6f 6e 74 6
0100  3a 20 36 38 30 0d 0
0110  65 3a 20 74 69 6d 6
0120  61 78 3d 39 38 0d 0
0130  6e 3a 20 4b 65 65 7
0140  6f 6e 74 65 6e 74 2
0150  74 2f 68 74 6d 6c 3
0160  69 73 6f 2d 38 38 3
0170  65 6e 74 2d 4c 61 6
0180  0d 0a 53 65 74 2d 4
0190  47 69 70 53 65 72 7
01a0  77 77 2e 63 6f 6c 7
01b0  38 30 2d 70 6f 6f 6
01c0  36 38 2e 32 30 34 3
01d0  78 70 69 72 65 73 3
01e0  70 72 2d 32 30 32 3
01f0  20 47 4d 54 3b 20 7
0200  74 70 6f 6e 6c 79 0
0210  00 00 00 03 8d 53 d
0220  89 49 55 53 f7 07 0
0230  45 db 84 78 70 93 6
0240  ef fe 83 3d f5 61 e
0250  dd 77 df 77 e7 b3 7
0260  9c 76 b3 e5 00 ca 3
```

Content length (http.content_length), 21 bytes | Packets: 844 · Displayed: 7 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

9) The HTTP status code of HTTP response for http://columbia.edu/history/ is 404 as indicated in the light blue region and we know that 4XX type of errors indicates a client error.



wireshark results.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time        Source          Destination     Protocol  Length Info
    36 8.051852    192.168.68.120  128.59.105.24   HTTP        55 Continuation
    98 27.970803   192.168.68.120  128.59.105.24   HTTP       599 GET /cu/computinghistory/ HTTP/1.1
   358 28.385270   128.59.105.24   192.168.68.120  HTTP      1097 HTTP/1.1 200 OK  (text/html)
   393 28.728815   192.168.68.120  128.59.105.24   HTTP       567 GET /cu/computinghistory/pcat01-120.jpg HTTP/1.1
   422 28.868022   128.59.105.24   192.168.68.120  HTTP/X…   1258 HTTP/1.1 404 Not Found
   757 35.972249   192.168.68.120  128.59.105.24   HTTP       587 GET /history/ HTTP/1.1
   759 36.148360   128.59.105.24   192.168.68.120  HTTP/X…   1202 HTTP/1.1 404 Not Found
```

```
> Frame 759: 1202 bytes on wire (9616 bits), 1202 bytes captured (9616 bits)
> Ethernet II, Src: TP-Link_c1:39:60 (00:31:92:c1:39:60), Dst: IntelCor_d1:aa:bf (f8:5e:a0:d1:aa:bf)
> Internet Protocol Version 4, Src: 128.59.105.24, Dst: 192.168.68.120
> Transmission Control Protocol, Src Port: 80, Dst Port: 61069, Seq: 176365, Ack: 1593, Len: 1148
v Hypertext Transfer Protocol
  v HTTP/1.1 404 Not Found\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 404 Not Found\r\n]
      Response Version: HTTP/1.1
      Status Code: 404
      [Status Code Description: Not Found]
      Response Phrase: Not Found
    Date: Mon, 03 Apr 2023 15:07:01 GMT\r\n
    Server: Apache\r\n
    Vary: accept-language,accept-charset,Accept-Encoding,User-Agent\r\n
    Accept-Ranges: bytes\r\n
    Content-Encoding: gzip\r\n
  > Content-Length: 680\r\n
    Keep-Alive: timeout=15, max=98\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-9\r\n
    Content-Language: tr\r\n
    Set-Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1781021568.20480.0000; expires=Mon, 03-Apr-2023 21:07:01 GMT; path=/; Httponly\r\n
    \r\n
    [HTTP response 3/3]
```

```
0030  1b 07 99 ce 00 00 4
0040  30 34 20 4e 6f 74 2
0050  74 65 3a 20 4d 6f 6
0060  32 30 32 33 20 31 3
0070  54 0d 0a 53 65 72 7
0080  65 0d 0a 56 61 72 7
0090  6c 61 6e 67 75 61 6
00a0  63 68 61 72 73 65 7
00b0  6e 63 6f 64 69 6e 6
00c0  6e 74 0d 0a 41 63 6
00d0  73 3a 20 62 79 74 6
00e0  74 2d 45 6e 63 6f 6
00f0  0d 0a 43 6f 6e 74 6
0100  3a 20 36 38 30 0d 0
0110  65 3a 20 74 69 6d 6
0120  61 78 3d 39 38 0d 0
0130  6e 3a 20 4b 65 65 7
0140  6f 6e 74 65 6e 74 2
0150  74 2f 68 74 6d 6c 3
0160  69 73 6f 2d 38 38 3
0170  65 6e 74 2d 4c 61 6
0180  0d 0a 53 65 74 2d 4
0190  47 69 70 53 65 72 7
01a0  77 77 2e 63 6f 6c 7
```

HTTP Response Status Code (http.response.code), 3 bytes

Packets: 844 · Displayed: 7 (0.8%)

Profile: Default

Zeynep Kurtuluş
29045