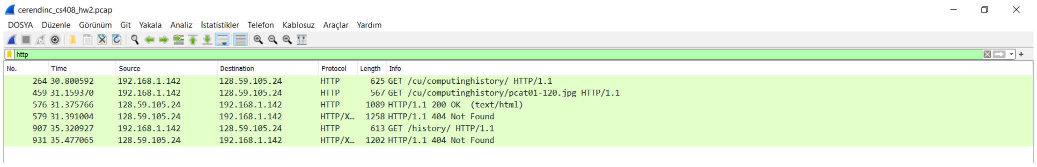
Ceren Dinç 28220

CS 408 HOMEWORK 2

Q1: What is the IP address of http://www.columbia.edu/cu/computinghistory/ website?

Answer:
From the screenshot below, destination of 1st line is the IP address of website.
128.59.105.24

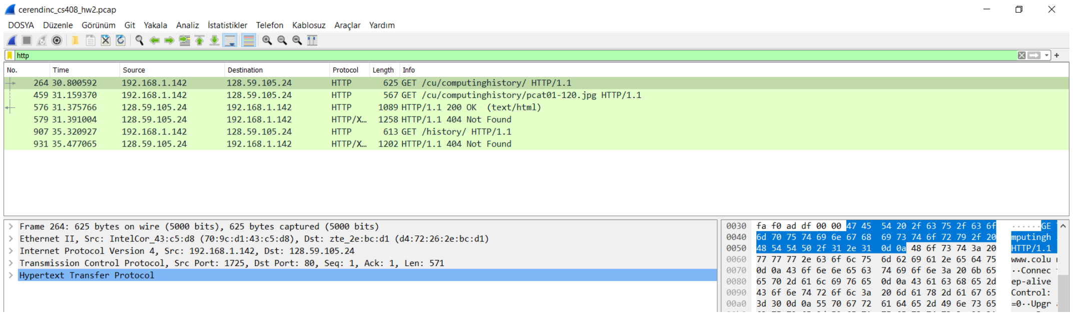


cerendinc_cs408_hw2.pcap
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
http

```
No.   Time       Source          Destination     Protocol Length Info
  264 30.800592  192.168.1.142   128.59.105.24   HTTP       625 GET /cu/computinghistory/ HTTP/1.1
  459 31.159370  192.168.1.142   128.59.105.24   HTTP       567 GET /cu/computinghistory/pcat01-120.jpg HTTP/1.1
  576 31.375766  128.59.105.24   192.168.1.142   HTTP      1089 HTTP/1.1 200 OK  (text/html)
  579 31.391004  128.59.105.24   192.168.1.142   HTTP/X…   1258 HTTP/1.1 404 Not Found
  907 35.320927  192.168.1.142   128.59.105.24   HTTP       613 GET /history/ HTTP/1.1
  931 35.477065  128.59.105.24   192.168.1.142   HTTP/X…   1202 HTTP/1.1 404 Not Found
```

Q2: What are the source port and destination port of the HTTP request used to get http://www.columbia.edu/cu/computinghistory/ ?

Answer:
From the screenshot below, source port & destination port of the HTTP request is written in Transmission Control Protocol part.
Source Port: 1725
Destination Port: 80



cerendinc_cs408_hw2.pcap
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
http

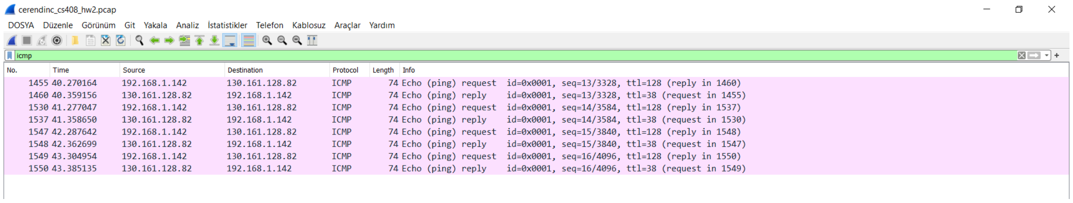
```
No.   Time       Source          Destination     Protocol Length Info
  264 30.800592  192.168.1.142   128.59.105.24   HTTP       625 GET /cu/computinghistory/ HTTP/1.1
  459 31.159370  192.168.1.142   128.59.105.24   HTTP       567 GET /cu/computinghistory/pcat01-120.jpg HTTP/1.1
  576 31.375766  128.59.105.24   192.168.1.142   HTTP      1089 HTTP/1.1 200 OK  (text/html)
  579 31.391004  128.59.105.24   192.168.1.142   HTTP/X…   1258 HTTP/1.1 404 Not Found
  907 35.320927  192.168.1.142   128.59.105.24   HTTP       613 GET /history/ HTTP/1.1
  931 35.477065  128.59.105.24   192.168.1.142   HTTP/X…   1202 HTTP/1.1 404 Not Found
```

```
> Frame 264: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits)
> Ethernet II, Src: IntelCor_43:c5:d8 (70:9c:d1:43:c5:d8), Dst: zte_2e:bc:d1 (d4:72:26:2e:bc:d1)
> Internet Protocol Version 4, Src: 192.168.1.142, Dst: 128.59.105.24
> Transmission Control Protocol, Src Port: 1725, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
> Hypertext Transfer Protocol
```

```
0030  fa f0 ad df 00 00 47 45  54 20 2f 63 75 2f 63 6f   ······GE
0040  6d 70 75 74 69 6e 67 68  69 73 74 6f 72 79 2f 20   mputingh
0050  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1
0060  77 77 77 2e 63 6f 6c 75  6d 62 69 61 2e 65 64 75   www.colu
0070  0d 0a 43 6f 6e 6e 65 63  74 69 6f 6e 3a 20 6b 65   ··Connec
0080  65 70 2d 61 6c 69 76 65  0d 0a 43 61 63 68 65 2d   ep-alive
0090  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:
00a0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65   =0··Upgr
```

Q3: What is the IP address of tudelft.nl domain?

Answer:
From the screenshot below, destination of ping request and source of ping reply shows IP address of tudelft.nl domain: **130.161.128.82**

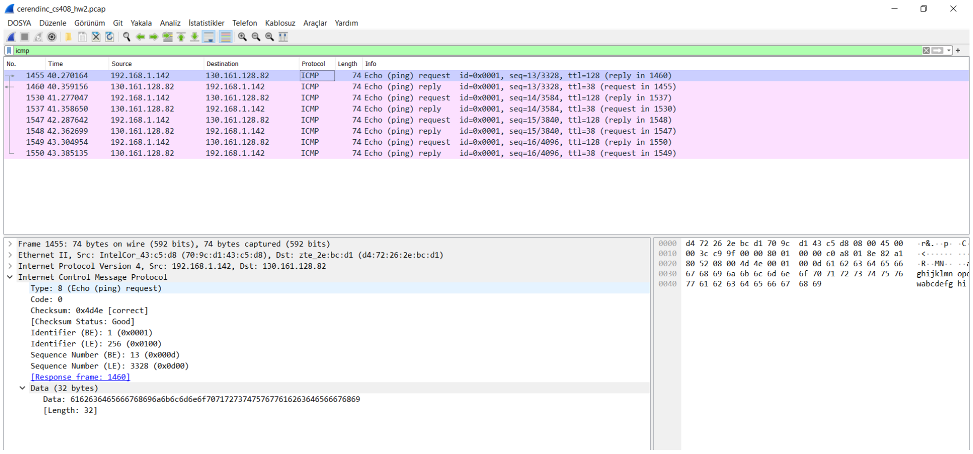


cerendinc_cs408_hw2.pcap
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
icmp

```
No.   Time       Source          Destination     Protocol Length Info
 1455 40.270164  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 1460)
 1460 40.359156  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=38 (request in 1455)
 1530 41.277047  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply in 1537)
 1537 41.358650  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=38 (request in 1530)
 1547 42.287642  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 1548)
 1548 42.362699  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=38 (request in 1547)
 1549 43.304954  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply in 1550)
 1550 43.385135  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=38 (request in 1549)
```

Q4: What are the type numbers of the ICMP Echo request and ICMP Echo reply (used for ping)?

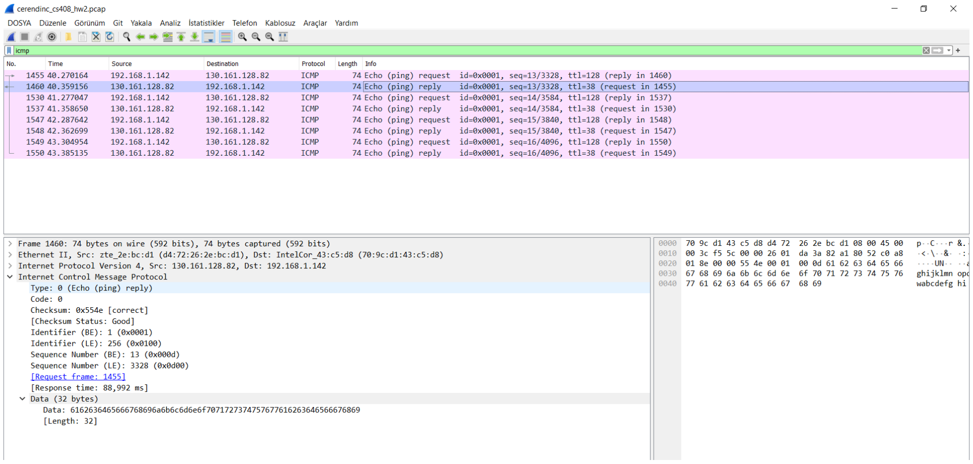
Answer:
In the Internet Control Message Protocol part:
1st screenshot below shows type number of ICMP Echo **request** for ping: **8**
2nd screenshot below shows type number of ICMP Echo **reply** for ping: **0**


cerendinc_cs408_hw2.pcap
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
icmp

```
No.   Time       Source          Destination     Protocol Length Info
 1455 40.270164  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 1460)
 1460 40.359156  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=38 (request in 1455)
 1530 41.277047  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply in 1537)
 1537 41.358650  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=38 (request in 1530)
 1547 42.287642  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 1548)
 1548 42.362699  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=38 (request in 1547)
 1549 43.304954  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply in 1550)
 1550 43.385135  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=38 (request in 1549)
```

```
> Frame 1455: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: IntelCor_43:c5:d8 (70:9c:d1:43:c5:d8), Dst: zte_2e:bc:d1 (d4:72:26:2e:bc:d1)
> Internet Protocol Version 4, Src: 192.168.1.142, Dst: 130.161.128.82
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d4e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
    [Response frame: 1460]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  d4 72 26 2e bc d1 70 9c  d1 43 c5 d8 08 00 45 00   ·r&.··p· ·C
0010  00 3c c9 9f 00 00 80 01  00 00 c0 a8 01 8e 82 a1   ·<······ ···
0020  80 52 08 00 4d 4e 00 01  00 0d 61 62 63 64 65 66   ·R··MN·· ··a
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opq
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```


cerendinc_cs408_hw2.pcap
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
icmp

```
No.   Time       Source          Destination     Protocol Length Info
 1455 40.270164  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 1460)
 1460 40.359156  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=38 (request in 1455)
 1530 41.277047  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=14/3584, ttl=128 (reply in 1537)
 1537 41.358650  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=14/3584, ttl=38 (request in 1530)
 1547 42.287642  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=15/3840, ttl=128 (reply in 1548)
 1548 42.362699  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=15/3840, ttl=38 (request in 1547)
 1549 43.304954  192.168.1.142   130.161.128.82  ICMP       74 Echo (ping) request  id=0x0001, seq=16/4096, ttl=128 (reply in 1550)
 1550 43.385135  130.161.128.82  192.168.1.142   ICMP       74 Echo (ping) reply    id=0x0001, seq=16/4096, ttl=38 (request in 1549)
```

```
> Frame 1460: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: zte_2e:bc:d1 (d4:72:26:2e:bc:d1), Dst: IntelCor_43:c5:d8 (70:9c:d1:43:c5:d8)
> Internet Protocol Version 4, Src: 130.161.128.82, Dst: 192.168.1.142
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x554e [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 13 (0x000d)
    Sequence Number (LE): 3328 (0x0d00)
    [Request frame: 1455]
    [Response time: 88,992 ms]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

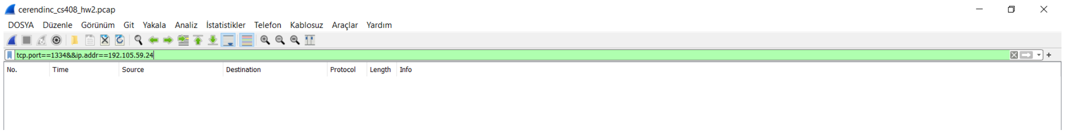
```
0000  70 9c d1 43 c5 d8 d4 72  26 2e bc d1 08 00 45 00   p··C···r &.
0010  00 3c f5 5c 00 00 26 01  da 3a 82 a1 80 52 c0 a8   ·<·\··&· ·:
0020  01 8e 00 00 55 4e 00 01  00 0d 61 62 63 64 65 66   ····UN·· ··a
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opq
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Q5: What is the length of the Data field of ICMP Echo reply packet from tudelft.nl?

Answer:
Can be seen in the 4th question, 2nd screenshot.
Length of the data field of ICMP Echo reply packet: **32 bytes**

Q6: Write a Wireshark filter for showing packets with source IP address 192.105.59.24 and TCP destination port 1334?

Answer:
tcp.port == 1334 && ip.addr == 192.105.59.24



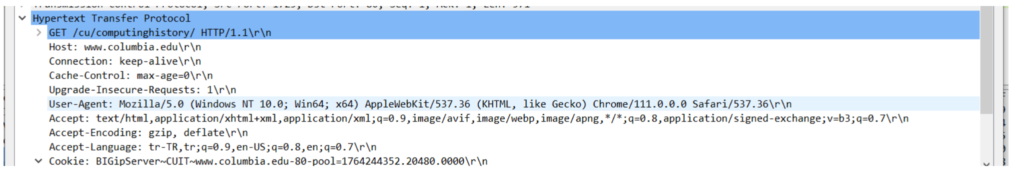
cerendinc_cs408_hw2.pcap
DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

```
tcp.port==1334&&ip.addr==192.105.59.24
```

```
No.   Time   Source   Destination   Protocol   Length   Info
```

Q7: What is the value of the User-Agent header field of HTTP requests sent by your browser?

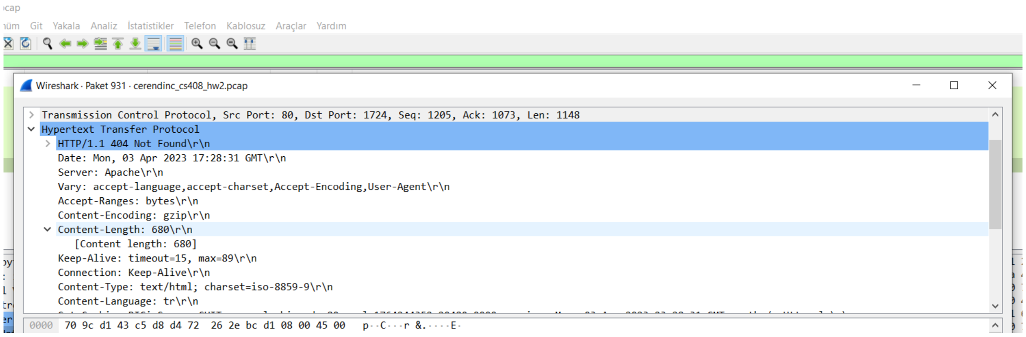
Answer:
From the screenshot below, User-Agent header field of HTTP requests sent by my browser
is shown in Hypertext Transfer Protocol part.
I used Chrome/111.0.0.0



```
v Hypertext Transfer Protocol
  > GET /cu/computinghistory/ HTTP/1.1\r\n
    Host: www.columbia.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    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\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: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  v Cookie: BIGipServer~CUIT~www.columbia.edu-80-pool=1764244352.20480.0000\r\n
```

Q8: What is the Content Length header field of HTTP response for http://www.columbia.edu/history/ ?

Answer:
From screenshot below, Content-Length is seen in Hypertext Transfer Protocol part:
Content-Length: **680**



ıcap
ıüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım
Wireshark · Paket 931 · cerendinc_cs408_hw2.pcap

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 1724, Seq: 1205, Ack: 1073, Len: 1148
v Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Date: Mon, 03 Apr 2023 17:28:31 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=89\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-9\r\n
    Content-Language: tr\r\n

0000  70 9c d1 43 c5 d8 d4 72  26 2e bc d1 08 00 45 00   p··C···r &.····E·
```

Q9: What is the HTTP Status Code of HTTP response for http://www.columbia.edu/history/ ?

Answer:
From the screenshot in 8th question, HTTP Status Code: **404**