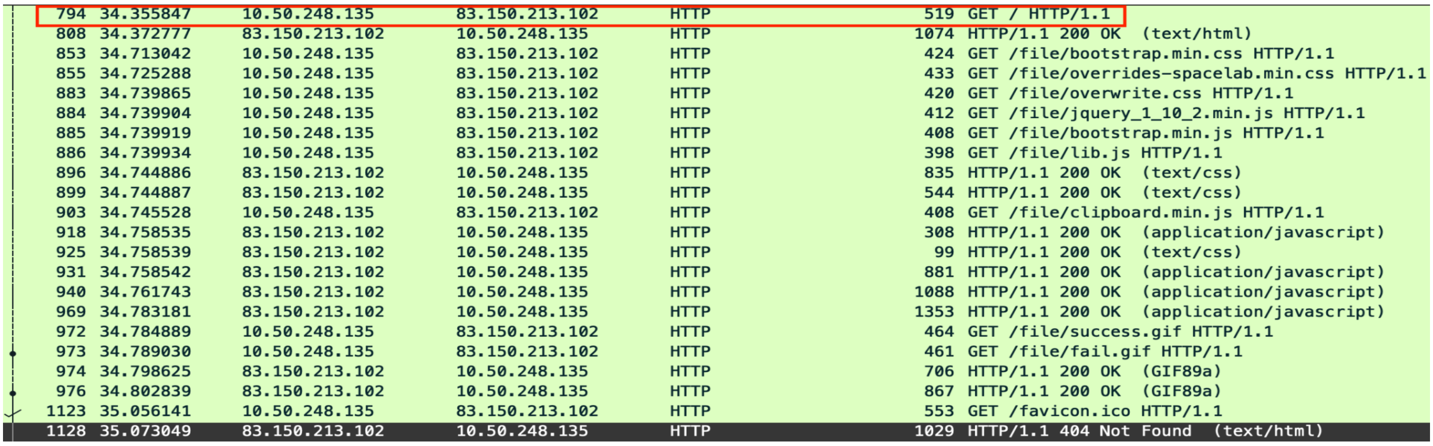
11/25/2022

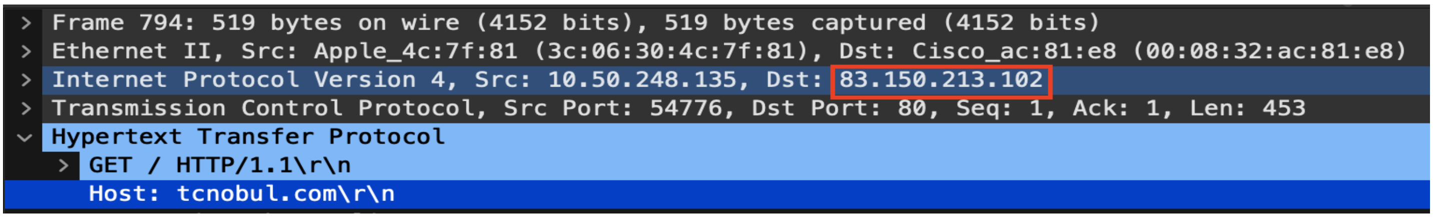
Fall 2022 - CS408 Assignment-2

Name: Muhammed Orhun Gale
ID: 26754

1) IP Address of http://tcnobul.com: 83.150.213.102



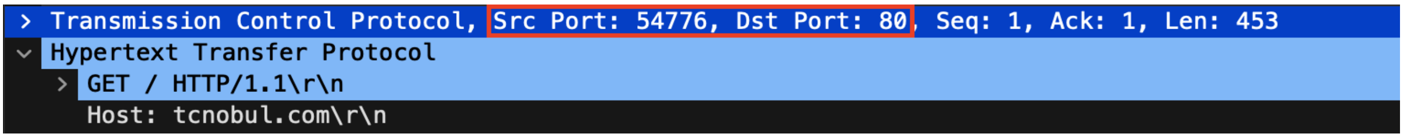
```
 794 34.355847   10.50.248.135    83.150.213.102   HTTP    519 GET / HTTP/1.1
 808 34.372777   83.150.213.102   10.50.248.135    HTTP   1074 HTTP/1.1 200 OK  (text/html)
 853 34.713042   10.50.248.135    83.150.213.102   HTTP    424 GET /file/bootstrap.min.css HTTP/1.1
 855 34.725288   10.50.248.135    83.150.213.102   HTTP    433 GET /file/overrides-spacelab.min.css HTTP/1.1
 883 34.739865   10.50.248.135    83.150.213.102   HTTP    420 GET /file/overwrite.css HTTP/1.1
 884 34.739904   10.50.248.135    83.150.213.102   HTTP    412 GET /file/jquery_1_10_2.min.js HTTP/1.1
 885 34.739919   10.50.248.135    83.150.213.102   HTTP    408 GET /file/bootstrap.min.js HTTP/1.1
 886 34.739934   10.50.248.135    83.150.213.102   HTTP    398 GET /file/lib.js HTTP/1.1
 896 34.744886   83.150.213.102   10.50.248.135    HTTP    835 HTTP/1.1 200 OK  (text/css)
 899 34.744887   83.150.213.102   10.50.248.135    HTTP    544 HTTP/1.1 200 OK  (text/css)
 903 34.745528   10.50.248.135    83.150.213.102   HTTP    408 GET /file/clipboard.min.js HTTP/1.1
 918 34.758535   83.150.213.102   10.50.248.135    HTTP    308 HTTP/1.1 200 OK  (application/javascript)
 925 34.758539   83.150.213.102   10.50.248.135    HTTP     99 HTTP/1.1 200 OK  (text/css)
 931 34.758542   83.150.213.102   10.50.248.135    HTTP    881 HTTP/1.1 200 OK  (application/javascript)
 940 34.761743   83.150.213.102   10.50.248.135    HTTP   1088 HTTP/1.1 200 OK  (application/javascript)
 969 34.783181   83.150.213.102   10.50.248.135    HTTP   1353 HTTP/1.1 200 OK  (application/javascript)
 972 34.784889   10.50.248.135    83.150.213.102   HTTP    464 GET /file/success.gif HTTP/1.1
 973 34.789030   10.50.248.135    83.150.213.102   HTTP    461 GET /file/fail.gif HTTP/1.1
 974 34.798625   83.150.213.102   10.50.248.135    HTTP    706 HTTP/1.1 200 OK  (GIF89a)
 976 34.802839   83.150.213.102   10.50.248.135    HTTP    867 HTTP/1.1 200 OK  (GIF89a)
1123 35.056141   10.50.248.135    83.150.213.102   HTTP    553 GET /favicon.ico HTTP/1.1
1128 35.073049   83.150.213.102   10.50.248.135    HTTP   1029 HTTP/1.1 404 Not Found  (text/html)
```



```
> Frame 794: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits)
> Ethernet II, Src: Apple_4c:7f:81 (3c:06:30:4c:7f:81), Dst: Cisco_ac:81:e8 (00:08:32:ac:81:e8)
> Internet Protocol Version 4, Src: 10.50.248.135, Dst: 83.150.213.102
> Transmission Control Protocol, Src Port: 54776, Dst Port: 80, Seq: 1, Ack: 1, Len: 453
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: tcnobul.com\r\n
```

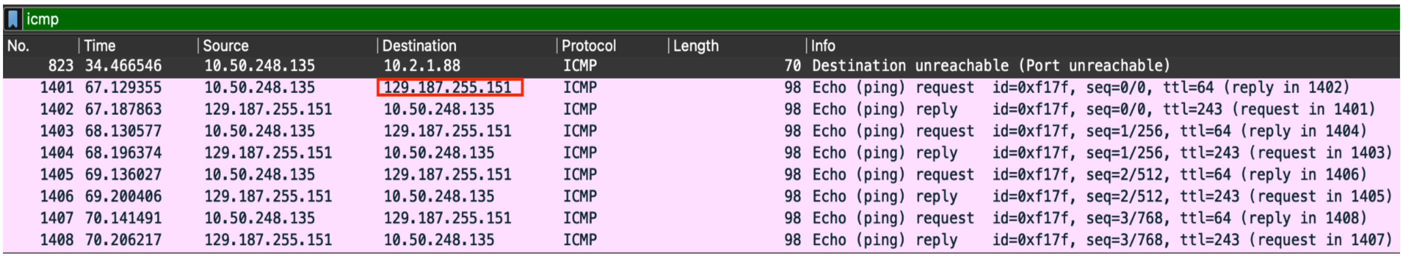
2) For GET http://tcnobul.com request:

Source port == 54776 – Destination port == 80



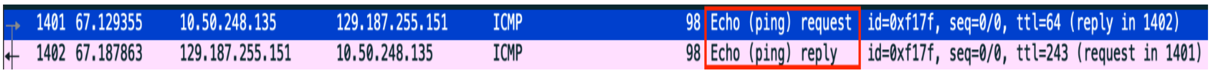
```
> Transmission Control Protocol, Src Port: 54776, Dst Port: 80, Seq: 1, Ack: 1, Len: 453
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: tcnobul.com\r\n
```

3) IP Address of tum.de: 129.187.255.151

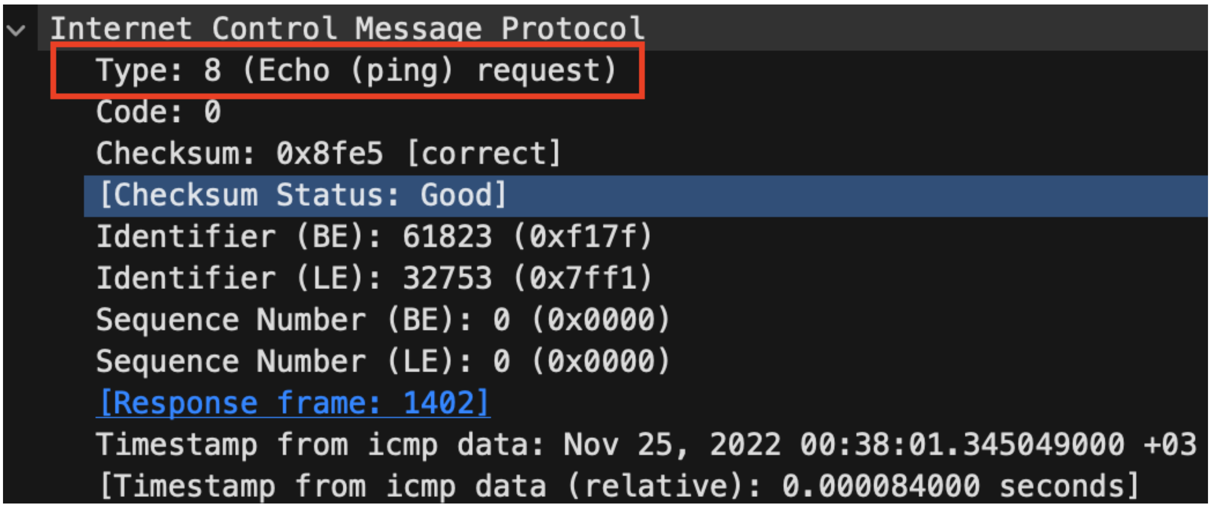


```
icmp
No.   Time        Source            Destination       Protocol  Length  Info
 823 34.466546   10.50.248.135     10.2.1.88         ICMP        70 Destination unreachable (Port unreachable)
1401 67.129355   10.50.248.135     129.187.255.151   ICMP        98 Echo (ping) request  id=0xf17f, seq=0/0, ttl=64 (reply in 1402)
1402 67.187863   129.187.255.151   10.50.248.135     ICMP        98 Echo (ping) reply    id=0xf17f, seq=0/0, ttl=243 (request in 1401)
1403 68.130577   10.50.248.135     129.187.255.151   ICMP        98 Echo (ping) request  id=0xf17f, seq=1/256, ttl=64 (reply in 1404)
1404 68.196374   129.187.255.151   10.50.248.135     ICMP        98 Echo (ping) reply    id=0xf17f, seq=1/256, ttl=243 (request in 1403)
1405 69.136027   10.50.248.135     129.187.255.151   ICMP        98 Echo (ping) request  id=0xf17f, seq=2/512, ttl=64 (reply in 1406)
1406 69.200406   129.187.255.151   10.50.248.135     ICMP        98 Echo (ping) reply    id=0xf17f, seq=2/512, ttl=243 (request in 1405)
1407 70.141491   10.50.248.135     129.187.255.151   ICMP        98 Echo (ping) request  id=0xf17f, seq=3/768, ttl=64 (reply in 1408)
1408 70.206217   129.187.255.151   10.50.248.135     ICMP        98 Echo (ping) reply    id=0xf17f, seq=3/768, ttl=243 (request in 1407)
```

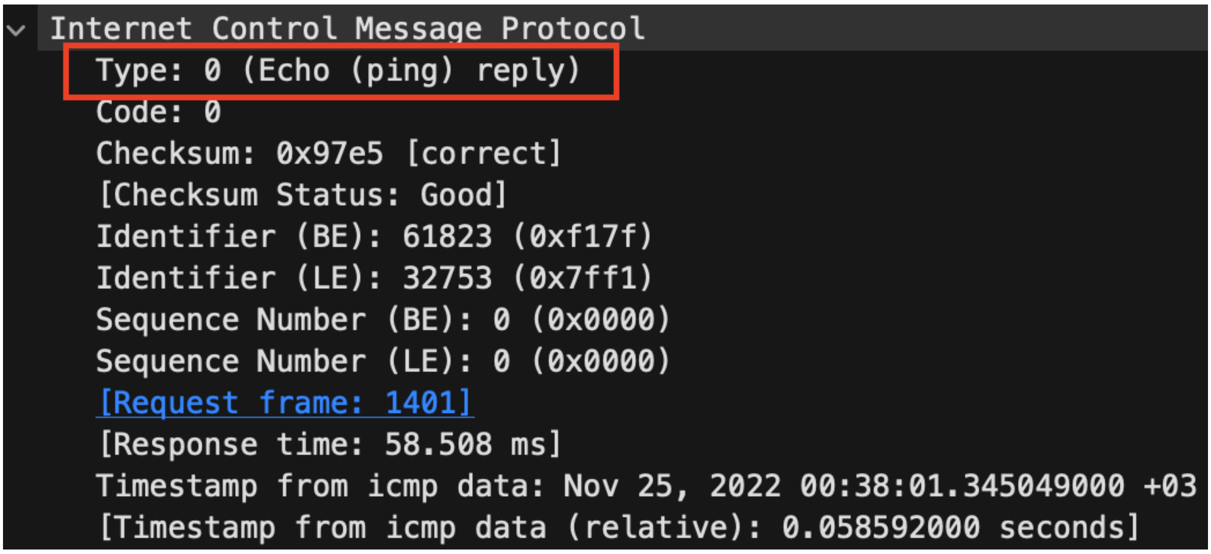
4) ICMP echo type number:
   Request: 8
   Reply   : 0



```
1401 67.129355   10.50.248.135    129.187.255.151  ICMP   98 Echo (ping) request  id=0xf17f, seq=0/0, ttl=64 (reply in 1402)
1402 67.187863   129.187.255.151  10.50.248.135    ICMP   98 Echo (ping) reply    id=0xf17f, seq=0/0, ttl=243 (request in 1401)
```

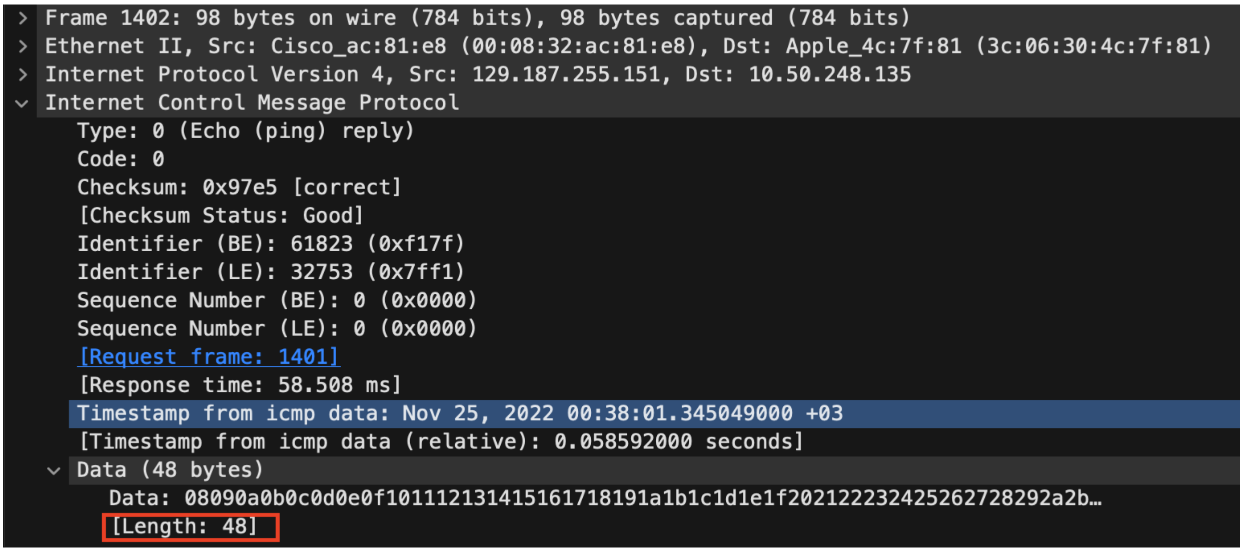


```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x8fe5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 61823 (0xf17f)
    Identifier (LE): 32753 (0x7ff1)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 1402]
    Timestamp from icmp data: Nov 25, 2022 00:38:01.345049000 +03
    [Timestamp from icmp data (relative): 0.000084000 seconds]
```



```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x97e5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 61823 (0xf17f)
    Identifier (LE): 32753 (0x7ff1)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Request frame: 1401]
    [Response time: 58.508 ms]
    Timestamp from icmp data: Nov 25, 2022 00:38:01.345049000 +03
    [Timestamp from icmp data (relative): 0.058592000 seconds]
```

5) 48

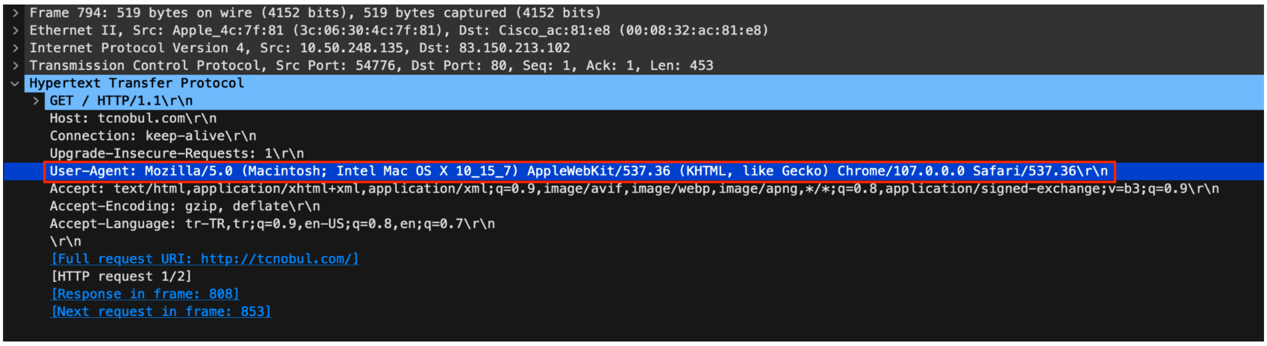


```
> Frame 1402: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Cisco_ac:81:e8 (00:08:32:ac:81:e8), Dst: Apple_4c:7f:81 (3c:06:30:4c:7f:81)
> Internet Protocol Version 4, Src: 129.187.255.151, Dst: 10.50.248.135
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x97e5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 61823 (0xf17f)
    Identifier (LE): 32753 (0x7ff1)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Request frame: 1401]
    [Response time: 58.508 ms]
    Timestamp from icmp data: Nov 25, 2022 00:38:01.345049000 +03
    [Timestamp from icmp data (relative): 0.058592000 seconds]
  v Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
```

6) ip.dst == 192.100.45.10 && tcp.dstport == 3040

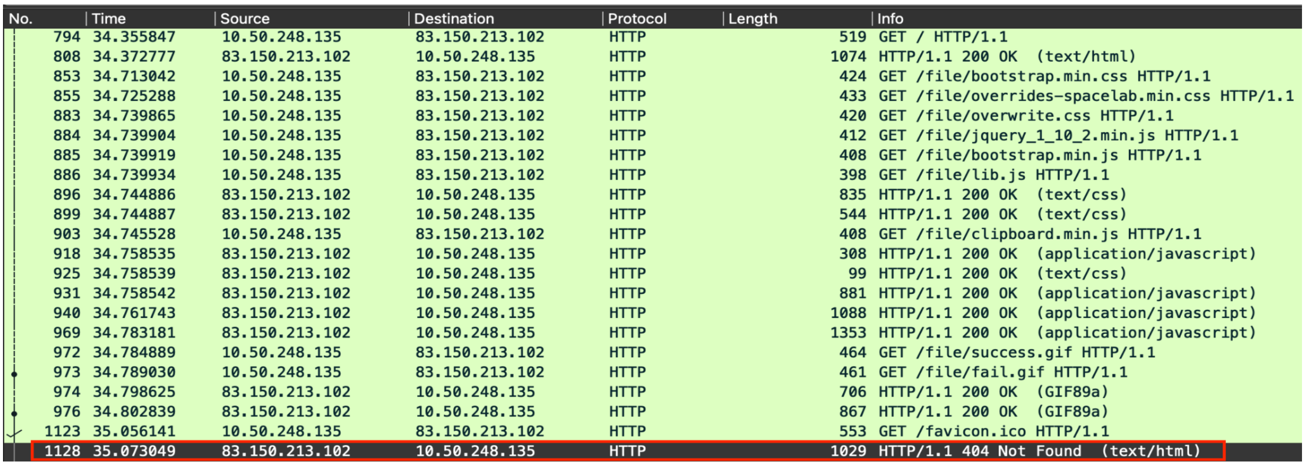
7) User-Agent header file:

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36

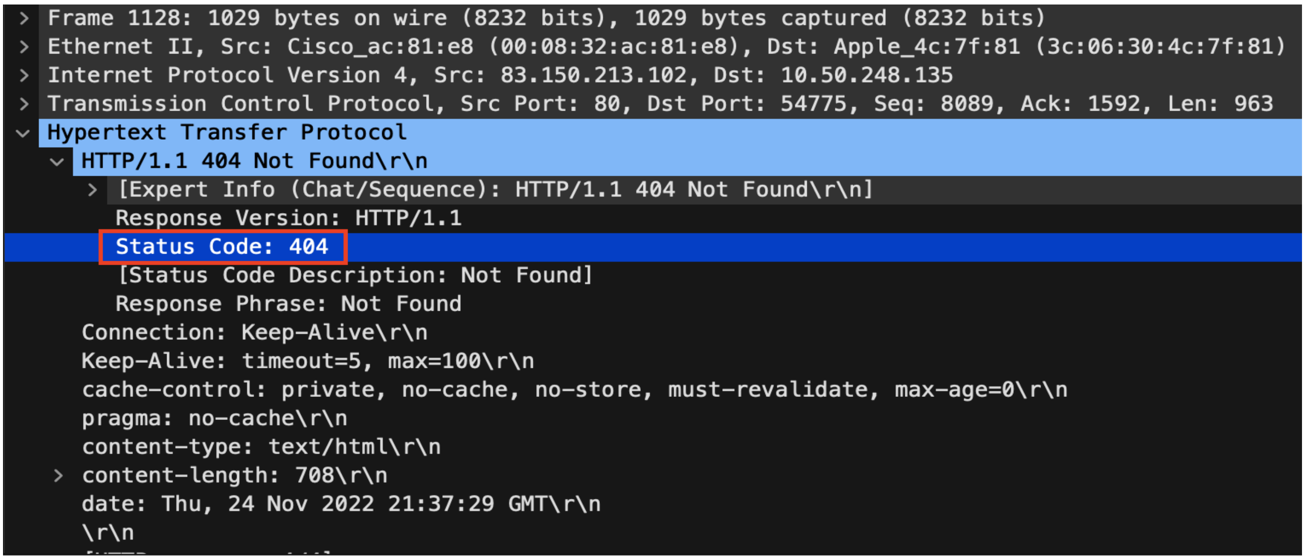


```
> Frame 794: 519 bytes on wire (4152 bits), 519 bytes captured (4152 bits)
> Ethernet II, Src: Apple_4c:7f:81 (3c:06:30:4c:7f:81), Dst: Cisco_ac:81:e8 (00:08:32:ac:81:e8)
> Internet Protocol Version 4, Src: 10.50.248.135, Dst: 83.150.213.102
> Transmission Control Protocol, Src Port: 54776, Dst Port: 80, Seq: 1, Ack: 1, Len: 453
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: tcnobul.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 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=0.9\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
    \r\n
    [Full request URI: http://tcnobul.com/]
    [HTTP request 1/2]
    [Response in frame: 808]
    [Next request in frame: 853]
```

8) content-length: 708\r\n
[Content length: 708]

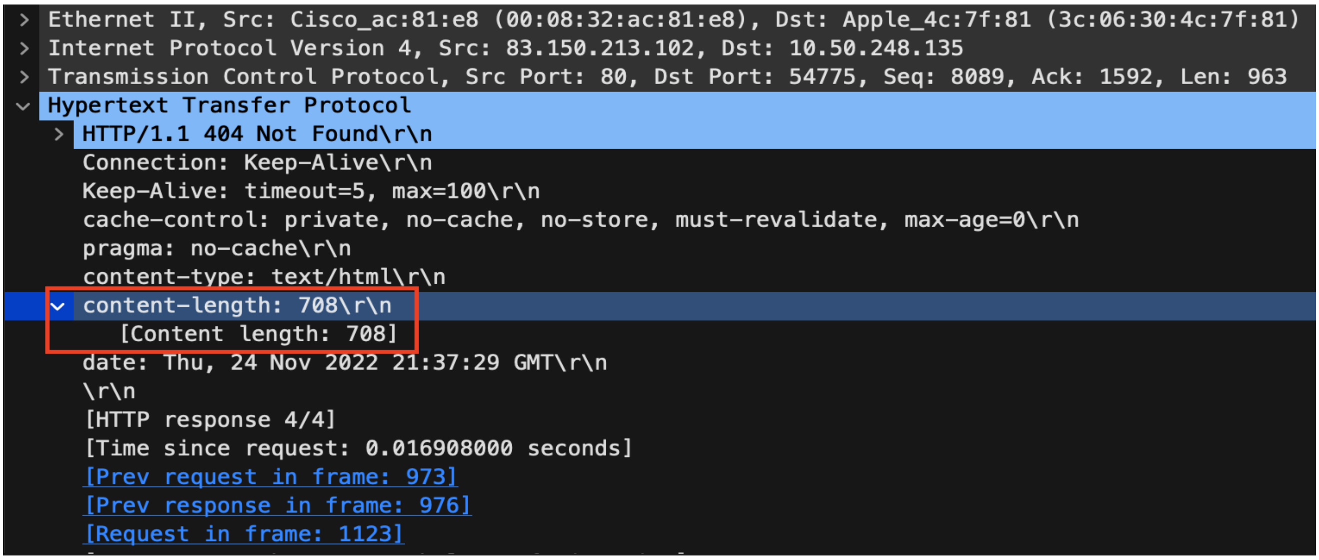


```
No.   Time       Source          Destination     Protocol   Length  Info
 794  34.355847  10.50.248.135   83.150.213.102  HTTP          519  GET / HTTP/1.1
 808  34.372777  83.150.213.102  10.50.248.135   HTTP         1074  HTTP/1.1 200 OK  (text/html)
 853  34.713042  10.50.248.135   83.150.213.102  HTTP          424  GET /file/bootstrap.min.css HTTP/1.1
 855  34.725288  10.50.248.135   83.150.213.102  HTTP          433  GET /file/overrides-spacelab.min.css HTTP/1.1
 883  34.739865  10.50.248.135   83.150.213.102  HTTP          420  GET /file/overwrite.css HTTP/1.1
 884  34.739904  10.50.248.135   83.150.213.102  HTTP          412  GET /file/jquery_1_10_2.min.js HTTP/1.1
 885  34.739919  10.50.248.135   83.150.213.102  HTTP          408  GET /file/bootstrap.min.js HTTP/1.1
 886  34.739934  10.50.248.135   83.150.213.102  HTTP          398  GET /file/lib.js HTTP/1.1
 896  34.744886  83.150.213.102  10.50.248.135   HTTP          835  HTTP/1.1 200 OK  (text/css)
 899  34.744887  83.150.213.102  10.50.248.135   HTTP          544  HTTP/1.1 200 OK  (text/css)
 903  34.745528  10.50.248.135   83.150.213.102  HTTP          408  GET /file/clipboard.min.js HTTP/1.1
 918  34.758535  83.150.213.102  10.50.248.135   HTTP          308  HTTP/1.1 200 OK  (application/javascript)
 925  34.758539  83.150.213.102  10.50.248.135   HTTP           99  HTTP/1.1 200 OK  (text/css)
 931  34.758542  83.150.213.102  10.50.248.135   HTTP          881  HTTP/1.1 200 OK  (application/javascript)
 940  34.761743  83.150.213.102  10.50.248.135   HTTP         1088  HTTP/1.1 200 OK  (application/javascript)
 969  34.783181  83.150.213.102  10.50.248.135   HTTP         1353  HTTP/1.1 200 OK  (application/javascript)
 972  34.784889  10.50.248.135   83.150.213.102  HTTP          464  GET /file/success.gif HTTP/1.1
 973  34.789030  10.50.248.135   83.150.213.102  HTTP          461  GET /file/fail.gif HTTP/1.1
 974  34.798625  83.150.213.102  10.50.248.135   HTTP          706  HTTP/1.1 200 OK  (GIF89a)
 976  34.802839  83.150.213.102  10.50.248.135   HTTP          867  HTTP/1.1 200 OK  (GIF89a)
1123  35.056141  10.50.248.135   83.150.213.102  HTTP          553  GET /favicon.ico HTTP/1.1
1128  35.073049  83.150.213.102  10.50.248.135   HTTP         1029  HTTP/1.1 404 Not Found  (text/html)
```



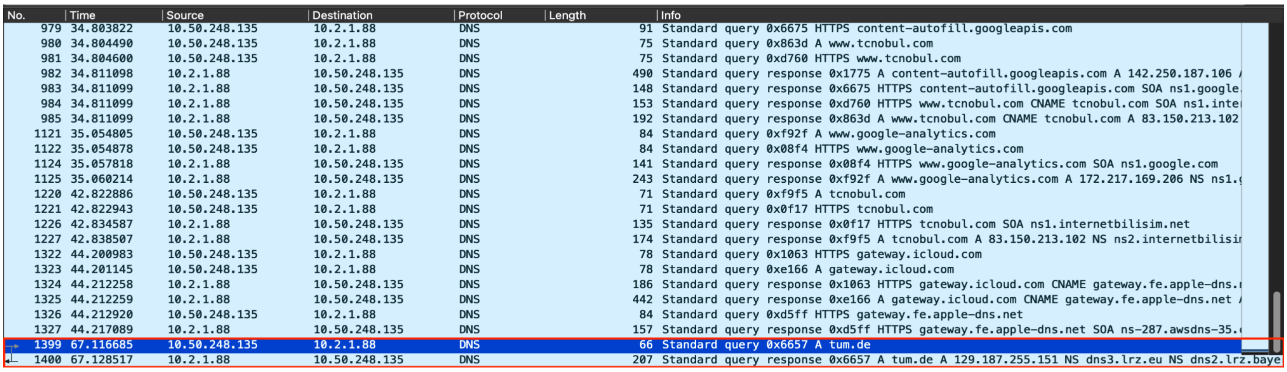
```
> Frame 1128: 1029 bytes on wire (8232 bits), 1029 bytes captured (8232 bits)
> Ethernet II, Src: Cisco_ac:81:e8 (00:08:32:ac:81:e8), Dst: Apple_4c:7f:81 (3c:06:30:4c:7f:81)
> Internet Protocol Version 4, Src: 83.150.213.102, Dst: 10.50.248.135
> Transmission Control Protocol, Src Port: 80, Dst Port: 54775, Seq: 8089, Ack: 1592, Len: 963
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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    cache-control: private, no-cache, no-store, must-revalidate, max-age=0\r\n
    pragma: no-cache\r\n
    content-type: text/html\r\n
  > content-length: 708\r\n
    date: Thu, 24 Nov 2022 21:37:29 GMT\r\n
    \r\n
```

9) HTTP Status Code: 404



```
> Ethernet II, Src: Cisco_ac:81:e8 (00:08:32:ac:81:e8), Dst: Apple_4c:7f:81 (3c:06:30:4c:7f:81)
> Internet Protocol Version 4, Src: 83.150.213.102, Dst: 10.50.248.135
> Transmission Control Protocol, Src Port: 80, Dst Port: 54775, Seq: 8089, Ack: 1592, Len: 963
v Hypertext Transfer Protocol
  > HTTP/1.1 404 Not Found\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    cache-control: private, no-cache, no-store, must-revalidate, max-age=0\r\n
    pragma: no-cache\r\n
    content-type: text/html\r\n
  v content-length: 708\r\n
      [Content length: 708]
    date: Thu, 24 Nov 2022 21:37:29 GMT\r\n
    \r\n
    [HTTP response 4/4]
    [Time since request: 0.016908000 seconds]
    [Prev request in frame: 973]
    [Prev response in frame: 976]
    [Request in frame: 1123]
```

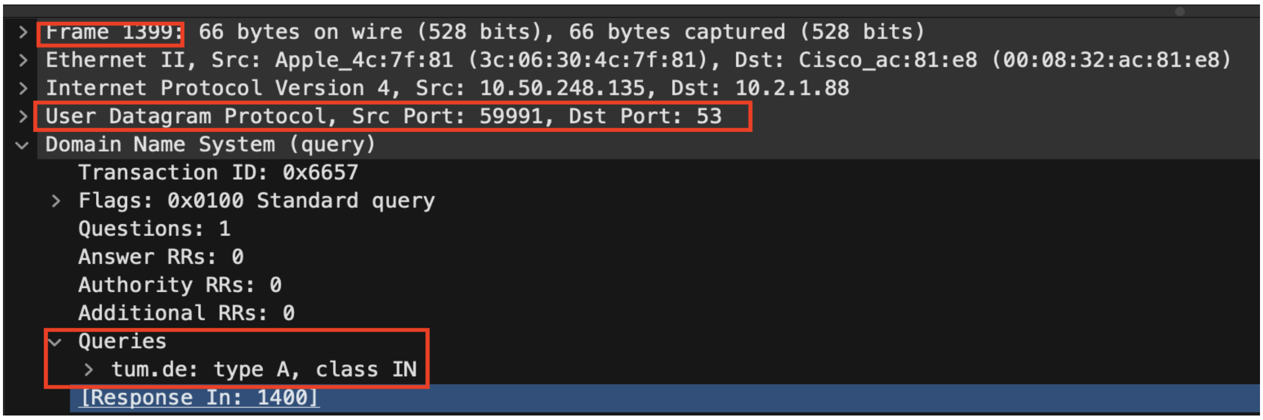
10)



No.	Time	Source	Destination	Protocol	Length	Info
979	34.803822	10.50.248.135	10.2.1.88	DNS	91	Standard query 0x6675 HTTPS content-autofill.googleapis.com
980	34.804490	10.50.248.135	10.2.1.88	DNS	75	Standard query 0x863d A www.tcnobul.com
981	34.804600	10.50.248.135	10.2.1.88	DNS	75	Standard query 0xd760 HTTPS www.tcnobul.com
982	34.811098	10.2.1.88	10.50.248.135	DNS	490	Standard query response 0x1775 A content-autofill.googleapis.com A 142.250.187.106
983	34.811099	10.2.1.88	10.50.248.135	DNS	148	Standard query response 0x6675 HTTPS content-autofill.googleapis.com SOA ns1.google.
984	34.811099	10.2.1.88	10.50.248.135	DNS	153	Standard query response 0xd760 HTTPS www.tcnobul.com CNAME tcnobul.com SOA ns1.inte
985	34.811099	10.2.1.88	10.50.248.135	DNS	192	Standard query response 0x863d A www.tcnobul.com CNAME tcnobul.com A 83.150.213.102
1121	35.054805	10.50.248.135	10.2.1.88	DNS	84	Standard query 0xf92f A www.google-analytics.com
1122	35.054878	10.50.248.135	10.2.1.88	DNS	84	Standard query 0x08f4 HTTPS www.google-analytics.com
1124	35.057818	10.2.1.88	10.50.248.135	DNS	141	Standard query response 0x08f4 HTTPS www.google-analytics.com SOA ns1.google.com
1125	35.060214	10.2.1.88	10.50.248.135	DNS	243	Standard query response 0xf92f A www.google-analytics.com A 172.217.169.206 NS ns1.
1220	42.822886	10.50.248.135	10.2.1.88	DNS	71	Standard query 0xf9f5 A tcnobul.com
1221	42.822943	10.50.248.135	10.2.1.88	DNS	71	Standard query 0x0f17 HTTPS tcnobul.com
1226	42.834587	10.2.1.88	10.50.248.135	DNS	135	Standard query response 0x0f17 HTTPS tcnobul.com SOA ns1.internetbilisim.net
1227	42.838507	10.2.1.88	10.50.248.135	DNS	174	Standard query response 0xf9f5 A tcnobul.com A 83.150.213.102 NS ns2.internetbilisi
1322	44.200983	10.50.248.135	10.2.1.88	DNS	78	Standard query 0x1063 HTTPS gateway.icloud.com
1323	44.201145	10.50.248.135	10.2.1.88	DNS	78	Standard query 0xe166 A gateway.icloud.com
1324	44.212258	10.2.1.88	10.50.248.135	DNS	186	Standard query response 0x1063 HTTPS gateway.icloud.com CNAME gateway.fe.apple-dns.
1325	44.212259	10.2.1.88	10.50.248.135	DNS	442	Standard query response 0xe166 A gateway.icloud.com CNAME gateway.fe.apple-dns.net
1326	44.212920	10.50.248.135	10.2.1.88	DNS	84	Standard query 0xd5ff HTTPS gateway.fe.apple-dns.net
1327	44.217089	10.2.1.88	10.50.248.135	DNS	157	Standard query response 0xd5ff HTTPS gateway.fe.apple-dns.net SOA ns-287.awsdns-35.
1399	67.116685	10.50.248.135	10.2.1.88	DNS	66	Standard query 0x6657 A tum.de
1400	67.128517	10.2.1.88	10.50.248.135	DNS	207	Standard query response 0x6657 A tum.de A 129.187.255.151 NS dns3.lrz.eu NS dns2.lrz.baye

Query:

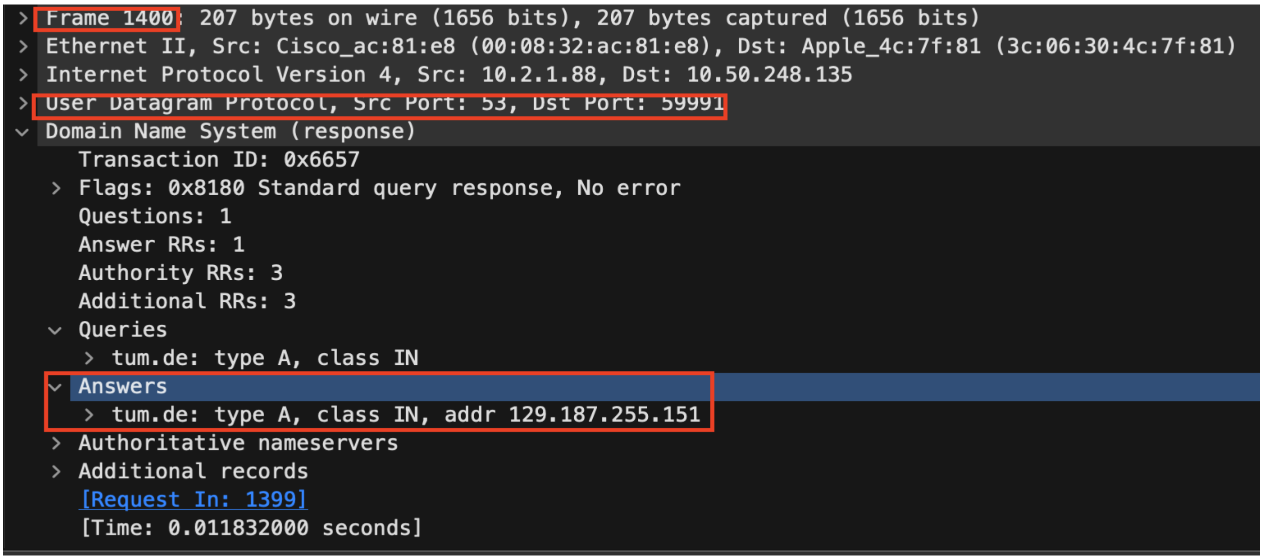
tum.de: type A, class IN
No: 1399
Sent over: UDP



```
> Frame 1399: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Apple_4c:7f:81 (3c:06:30:4c:7f:81), Dst: Cisco_ac:81:e8 (00:08:32:ac:81:e8)
> Internet Protocol Version 4, Src: 10.50.248.135, Dst: 10.2.1.88
> User Datagram Protocol, Src Port: 59991, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x6657
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > tum.de: type A, class IN
    [Response In: 1400]
```

Response:

tum.de: type A, class IN, addr 129.187.255.151
No: 1400
Sent over: UDP



```
> Frame 1400: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits)
> Ethernet II, Src: Cisco_ac:81:e8 (00:08:32:ac:81:e8), Dst: Apple_4c:7f:81 (3c:06:30:4c:7f:81)
> Internet Protocol Version 4, Src: 10.2.1.88, Dst: 10.50.248.135
> User Datagram Protocol, Src Port: 53, Dst Port: 59991
v Domain Name System (response)
    Transaction ID: 0x6657
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 3
  v Queries
    > tum.de: type A, class IN
  v Answers
    > tum.de: type A, class IN, addr 129.187.255.151
  > Authoritative nameservers
  > Additional records
    [Request In: 1399]
    [Time: 0.011832000 seconds]
```