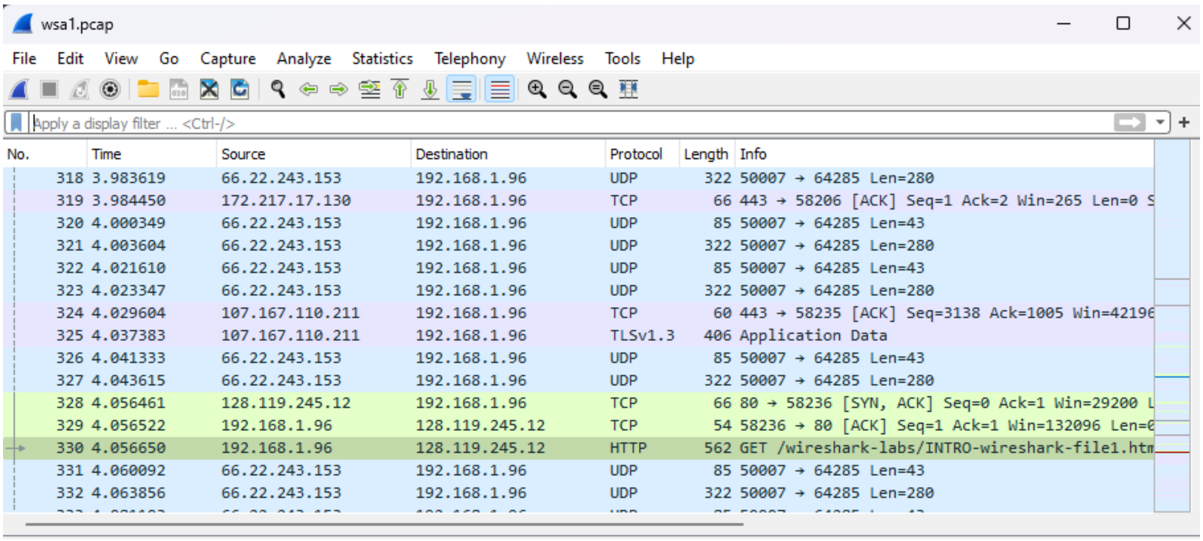
WSA1

2448025

1) TCP, HTTP, DNS, UDP, TLSv1.2



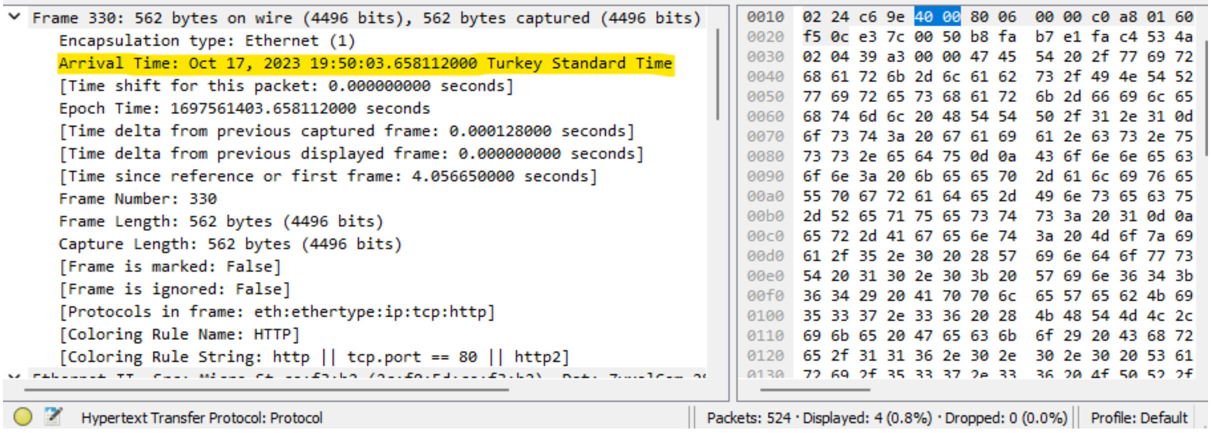
wsa1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source           Destination     Protocol Length Info
  318 3.983619  66.22.243.153    192.168.1.96    UDP       322 50007 → 64285 Len=280
  319 3.984450  172.217.17.130   192.168.1.96    TCP        66 443 → 58206 [ACK] Seq=1 Ack=2 Win=265 Len=0 S
  320 4.000349  66.22.243.153    192.168.1.96    UDP        85 50007 → 64285 Len=43
  321 4.003604  66.22.243.153    192.168.1.96    UDP       322 50007 → 64285 Len=280
  322 4.021610  66.22.243.153    192.168.1.96    UDP        85 50007 → 64285 Len=43
  323 4.023347  66.22.243.153    192.168.1.96    UDP       322 50007 → 64285 Len=280
  324 4.029604  107.167.110.211  192.168.1.96    TCP        60 443 → 58235 [ACK] Seq=3138 Ack=1005 Win=42196
  325 4.037383  107.167.110.211  192.168.1.96    TLSv1.3   406 Application Data
  326 4.041333  66.22.243.153    192.168.1.96    UDP        85 50007 → 64285 Len=43
  327 4.043615  66.22.243.153    192.168.1.96    UDP       322 50007 → 64285 Len=280
  328 4.056461  128.119.245.12   192.168.1.96    TCP        66 80 → 58236 [SYN, ACK] Seq=0 Ack=1 Win=29200 L
  329 4.056522  192.168.1.96     128.119.245.12  TCP        54 58236 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
  330 4.056650  192.168.1.96     128.119.245.12  HTTP      562 GET /wireshark-labs/INTRO-wireshark-file1.htm
  331 4.060092  66.22.243.153    192.168.1.96    UDP        85 50007 → 64285 Len=43
  332 4.063856  66.22.243.153    192.168.1.96    UDP       322 50007 → 64285 Len=280
```

2) 0.158

HTTP GET Message Arrival Time: Oct 17, 2023 19:50:03.658112000

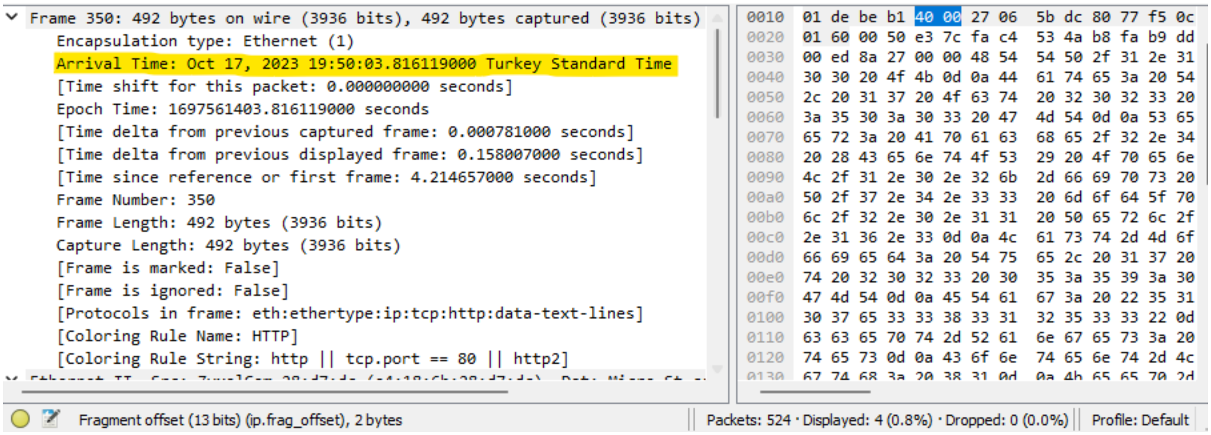
HTTP OK Reply Arrival Time: Oct 17, 2023 19:50:03.816119000



```
Frame 330: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 17, 2023 19:50:03.658112000 Turkey Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1697561403.658112000 seconds
    [Time delta from previous captured frame: 0.000128000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 4.056650000 seconds]
    Frame Number: 330
    Frame Length: 562 bytes (4496 bits)
    Capture Length: 562 bytes (4496 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

```
0010  02 24 c6 9e 40 00 80 06  00 00 c0 a8 01 60
0020  f5 0c e3 7c 00 50 b8 fa  b7 e1 fa c4 53 4a
0030  02 04 39 a3 00 00 47 45  54 20 2f 77 69 72
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72
0120  65 2f 31 31 36 2e 30 2e  30 2e 30 20 53 61
```

Hypertext Transfer Protocol: Protocol | Packets: 524 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

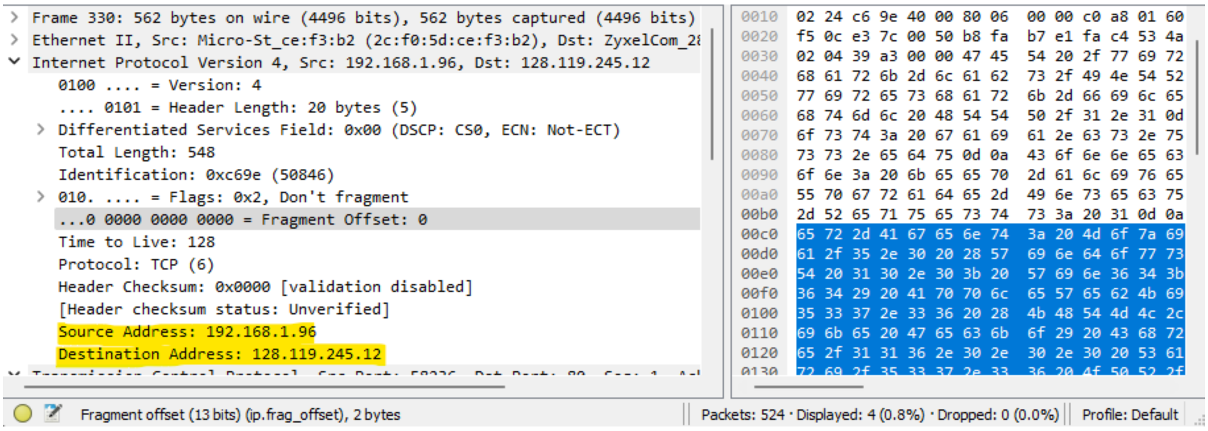


```
Frame 350: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 17, 2023 19:50:03.816119000 Turkey Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1697561403.816119000 seconds
    [Time delta from previous captured frame: 0.000781000 seconds]
    [Time delta from previous displayed frame: 0.158007000 seconds]
    [Time since reference or first frame: 4.214657000 seconds]
    Frame Number: 350
    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]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

```
0010  01 de be b1 40 00 27 06  5b dc 80 77 f5 0c
0020  01 60 00 50 e3 7c fa c4  53 4a b8 fa b9 dd
0030  00 ed 8a 27 00 00 48 54  54 50 2f 31 2e 31
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 54
0050  2c 20 31 37 20 4f 63 74  20 32 30 32 33 20
0060  3a 35 30 3a 30 33 20 47  4d 54 0d 0a 53 65
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f 70
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c 2f
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f
00d0  66 69 65 64 3a 20 54 75  65 2c 20 31 37 20
00e0  74 20 32 30 32 33 20 30  35 3a 35 39 3a 30
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 35 31
0100  30 37 65 33 33 38 33 31  32 35 33 33 22 0d
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c
```

Fragment offset (13 bits) (ip.frag_offset), 2 bytes | Packets: 524 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

3) Source Address: 192.168.1.96
Destination Address: 128.119.245.12

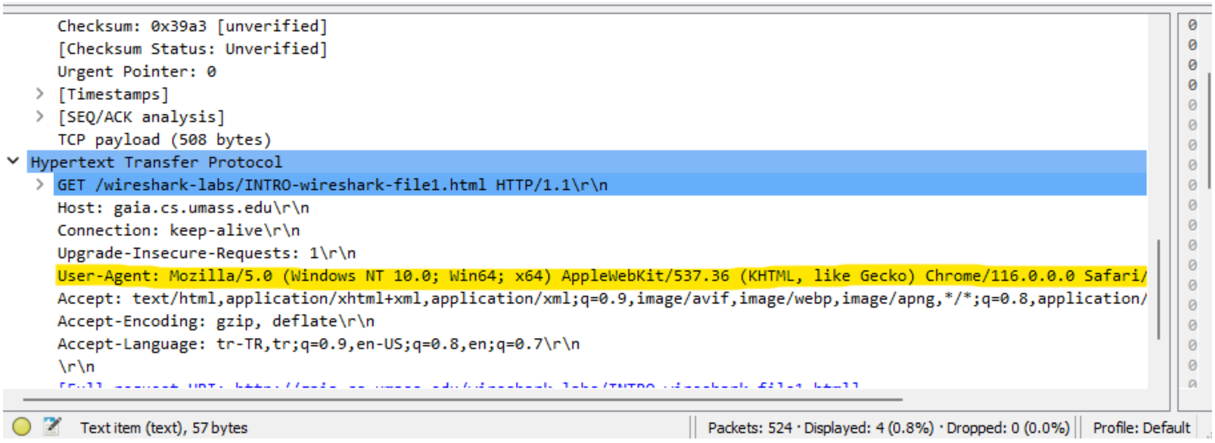


```
> Frame 330: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
> Ethernet II, Src: Micro-St_ce:f3:b2 (2c:f0:5d:ce:f3:b2), Dst: ZyxelCom_28
v Internet Protocol Version 4, Src: 192.168.1.96, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 548
    Identification: 0xc69e (50846)
  > 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: 192.168.1.96
    Destination Address: 128.119.245.12
v Transmission Control Protocol, Src Port: 58236, Dst Port: 80, Seq: 1, Ack
```

```
0010  02 24 c6 9e 40 00 80 06  00 00 c0 a8 01 60
0020  f5 0c e3 7c 00 50 b8 fa  b7 e1 fa c4 53 4a
0030  02 04 39 a3 00 00 47 45  54 20 2f 77 69 72
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72
0120  65 2f 31 31 36 2e 30 2e  30 2e 30 20 53 61
0130  72 69 2f 35 33 37 2e 33  36 20 4f 50 52 2f
```

Fragment offset (13 bits) (ip.frag_offset), 2 bytes | Packets: 524 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

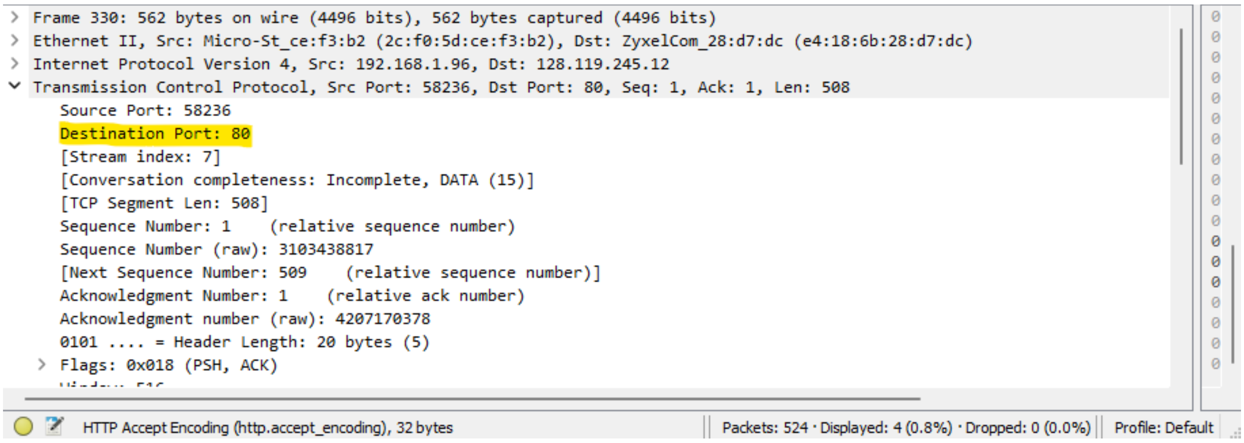
4) User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 OPR/102.0.0.0



```
    Checksum: 0x39a3 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (508 bytes)
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    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 Gecko) Chrome/116.0.0.0 Safari/
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
    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://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

Text item (text), 57 bytes | Packets: 524 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) | Profile: Default

5) Destination Port: 80



```
> Frame 330: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits)
> Ethernet II, Src: Micro-St_ce:f3:b2 (2c:f0:5d:ce:f3:b2), Dst: ZyxelCom_28:d7:dc (e4:18:6b:28:d7:dc)
> Internet Protocol Version 4, Src: 192.168.1.96, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 58236, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
    Source Port: 58236
    Destination Port: 80
    [Stream index: 7]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 508]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3103438817
    [Next Sequence Number: 509    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 4207170378
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 516
```

HTTP Accept Encoding (http.accept_encoding), 32 bytes | Packets: 524 · Displayed: 4 (0.8%) · Dropped: 0 (0.0%) | Profile: Default