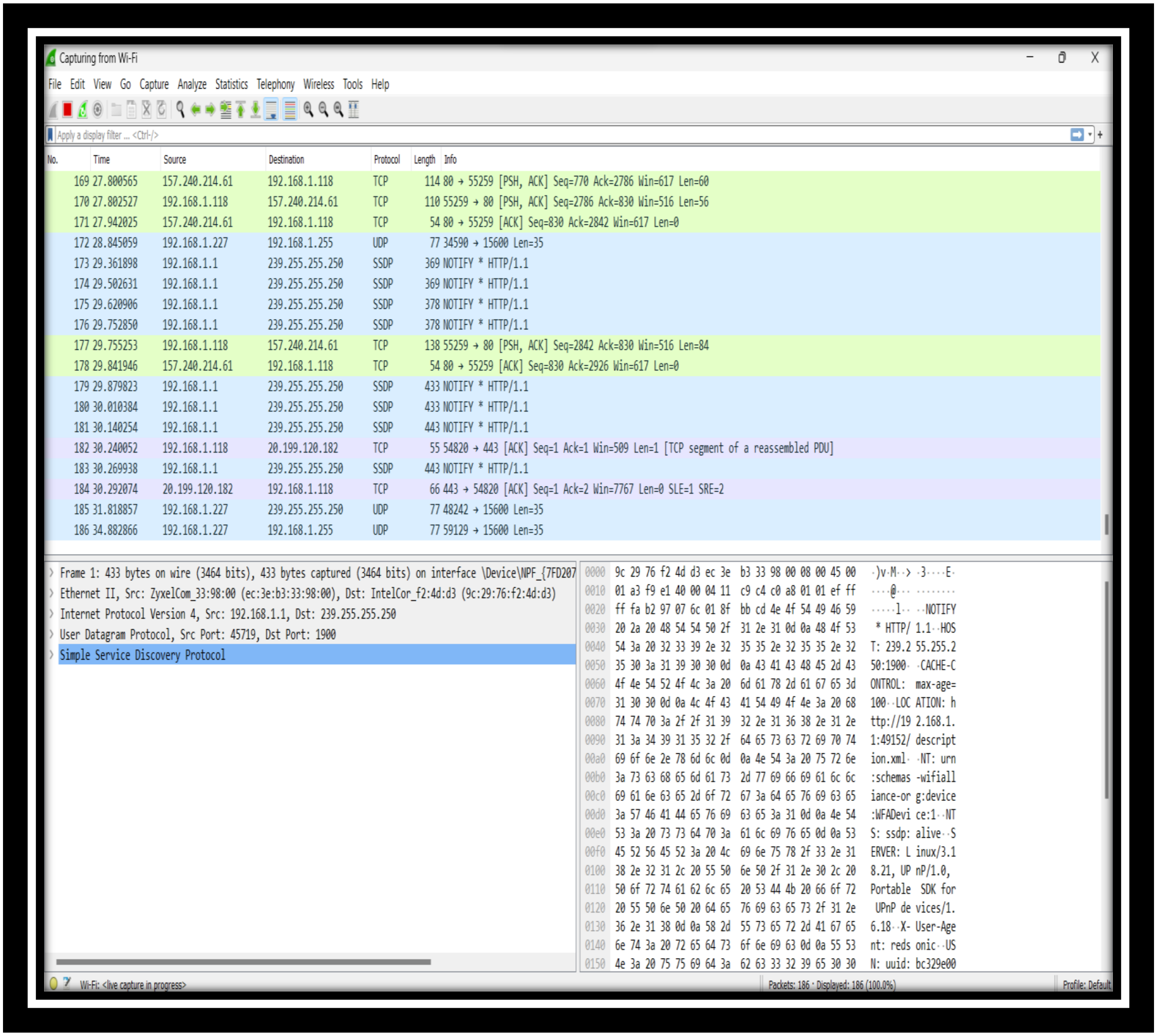
LAB 1

Name : Eslam Mostafa Mohamed

ID : 20p4797

1- TCP , UDP , SSDP


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

```
No.  Time       Source          Destination      Protocol Length Info
 169 27.800565  157.240.214.61  192.168.1.118    TCP      114 80 → 55259 [PSH, ACK] Seq=770 Ack=2786 Win=617 Len=60
 170 27.802527  192.168.1.118   157.240.214.61   TCP      110 55259 → 80 [PSH, ACK] Seq=2786 Ack=830 Win=516 Len=56
 171 27.942025  157.240.214.61  192.168.1.118    TCP       54 80 → 55259 [ACK] Seq=830 Ack=2842 Win=617 Len=0
 172 28.845059  192.168.1.227   192.168.1.255    UDP       77 34590 → 15600 Len=35
 173 29.361898  192.168.1.1     239.255.255.250  SSDP     369 NOTIFY * HTTP/1.1
 174 29.502631  192.168.1.1     239.255.255.250  SSDP     369 NOTIFY * HTTP/1.1
 175 29.620906  192.168.1.1     239.255.255.250  SSDP     378 NOTIFY * HTTP/1.1
 176 29.752850  192.168.1.1     239.255.255.250  SSDP     378 NOTIFY * HTTP/1.1
 177 29.755253  192.168.1.118   157.240.214.61   TCP      138 55259 → 80 [PSH, ACK] Seq=2842 Ack=830 Win=516 Len=84
 178 29.841946  157.240.214.61  192.168.1.118    TCP       54 80 → 55259 [ACK] Seq=830 Ack=2926 Win=617 Len=0
 179 29.879823  192.168.1.1     239.255.255.250  SSDP     433 NOTIFY * HTTP/1.1
 180 30.010384  192.168.1.1     239.255.255.250  SSDP     433 NOTIFY * HTTP/1.1
 181 30.140254  192.168.1.1     239.255.255.250  SSDP     443 NOTIFY * HTTP/1.1
 182 30.240052  192.168.1.118   20.199.120.182   TCP       55 54820 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]
 183 30.269938  192.168.1.1     239.255.255.250  SSDP     443 NOTIFY * HTTP/1.1
 184 30.292074  20.199.120.182  192.168.1.118    TCP       66 443 → 54820 [ACK] Seq=1 Ack=2 Win=7767 Len=0 SLE=1 SRE=2
 185 31.818857  192.168.1.227   239.255.255.250  UDP       77 48242 → 15600 Len=35
 186 34.882866  192.168.1.227   192.168.1.255    UDP       77 59129 → 15600 Len=35
```

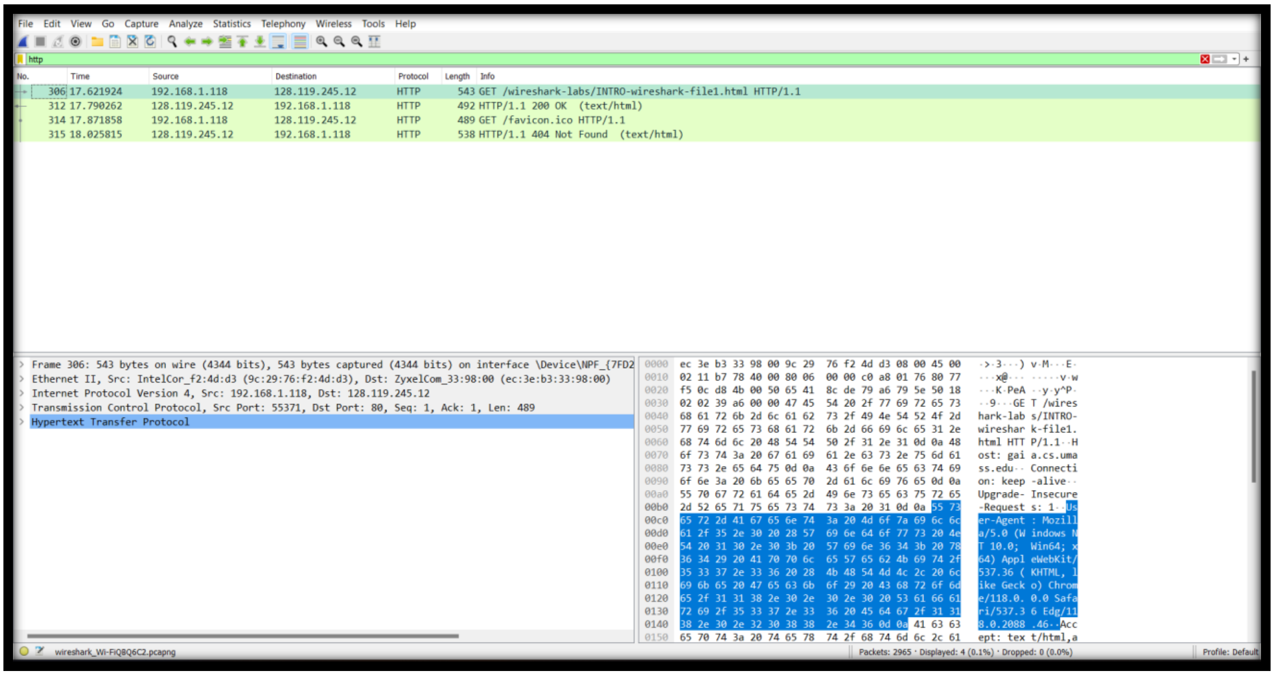
```
> Frame 1: 433 bytes on wire (3464 bits), 433 bytes captured (3464 bits) on interface \Device\NPF_{7FD207
> Ethernet II, Src: ZyxelCom_33:98:00 (ec:3e:b3:33:98:00), Dst: IntelCor_f2:4d:d3 (9c:29:76:f2:4d:d3)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 45719, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  9c 29 76 f2 4d d3 ec 3e  b3 33 98 00 08 00 45 00   ·)v·M··> ·3····E·
0010  01 a3 f9 e1 40 00 04 11  c9 c4 c0 a8 01 01 ef ff   ····@··· ········
0020  ff fa b2 97 07 6c 01 8f  bb cd 4e 4f 54 49 46 59   ·····l·· ··NOTIFY
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 4f 53    * HTTP/ 1.1··HOS
0040  54 3a 20 32 33 39 2e 32  35 35 2e 32 35 35 2e 32   T: 239.2 55.255.2
0050  35 30 3a 31 39 30 30 0d  0a 43 41 43 48 45 2d 43   50:1900· ·CACHE-C
0060  4f 4e 54 52 4f 4c 3a 20  6d 61 78 2d 61 67 65 3d   ONTROL:  max-age=
0070  31 30 30 0d 0a 4c 4f 43  41 54 49 4f 4e 3a 20 68   100··LOC ATION: h
0080  74 74 70 3a 2f 2f 31 39  32 2e 31 36 38 2e 31 2e   ttp://19 2.168.1.
0090  31 3a 34 39 31 35 32 2f  64 65 73 63 72 69 70 74   1:49152/ descript
00a0  69 6f 6e 2e 78 6d 6c 0d  0a 4e 54 3a 20 75 72 6e   ion.xml· ·NT: urn
00b0  3a 73 63 68 65 6d 61 73  2d 77 69 66 69 61 6c 6c   :schemas -wifiall
00c0  69 61 6e 63 65 2d 6f 72  67 3a 64 65 76 69 63 65   iance-or g:device
00d0  3a 57 46 41 44 65 76 69  63 65 3a 31 0d 0a 4e 54   :WFADevi ce:1··NT
00e0  53 3a 20 73 73 64 70 3a  61 6c 69 76 65 0d 0a 53   S: ssdp: alive··S
00f0  45 52 56 45 52 3a 20 4c  69 6e 75 78 2f 33 2e 31   ERVER: L inux/3.1
0100  38 2e 32 31 2c 20 55 50  6e 50 2f 31 2e 30 2c 20   8.21, UP nP/1.0,
0110  50 6f 72 74 61 62 6c 65  20 53 44 4b 20 66 6f 72   Portable  SDK for
0120  20 55 50 6e 50 20 64 65  76 69 63 65 73 2f 31 2e    UPnP de vices/1.
0130  36 2e 31 38 0d 0a 58 2d  55 73 65 72 2d 41 67 65   6.18··X- User-Age
0140  6e 74 3a 20 72 65 64 73  6f 6e 69 63 0d 0a 55 53   nt: reds onic··US
0150  4e 3a 20 75 75 69 64 3a  62 63 33 32 39 65 30 30   N: uuid: bc329e00
```

Wi-Fi: <live capture in progress>   Packets: 186 · Displayed: 186 (100.0%)   Profile: Default

2- the time taken is 0.168338

17.790262 – 17.621924 = 0.168338



```
http
```

```
No.     Time       Source          Destination     Protocol Length Info
    306 17.621924  192.168.1.118   128.119.245.12  HTTP     543 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    312 17.790262  128.119.245.12  192.168.1.118   HTTP     492 HTTP/1.1 200 OK  (text/html)
    314 17.871858  192.168.1.118   128.119.245.12  HTTP     489 GET /favicon.ico HTTP/1.1
    315 18.025815  128.119.245.12  192.168.1.118   HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 306: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{7FD2
> Ethernet II, Src: IntelCor_f2:4d:d3 (9c:29:76:f2:4d:d3), Dst: ZyxelCom_33:98:00 (ec:3e:b3:33:98:00)
> Internet Protocol Version 4, Src: 192.168.1.118, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 55371, Dst Port: 80, Seq: 1, Ack: 1, Len: 489
> Hypertext Transfer Protocol
```

```
0000  ec 3e b3 33 98 00 9c 29  76 f2 4d d3 08 00 45 00   ·>·3···) v·M···E·
0010  02 11 b7 78 40 00 80 06  00 00 c0 a8 01 76 80 77   ···x@··· ·····v·w
0020  f5 0c d8 4b 00 50 65 41  8c de 79 a6 79 5e 50 18   ···K·PeA ··y·y^P·
0030  02 02 39 a6 00 00 47 45  54 20 2f 77 69 72 65 73   ··9···GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54 52 4f 2d   hark-lab s/INTRO-
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c 65 31 2e   wireshar k-file1.
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b 69 74 2f   64) Appl eWebKit/
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c 2c 20 6c   537.36 ( KHTML, l
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68 72 6f 6d   ike Geck o) Chrom
0120  65 2f 31 31 38 2e 30 2e  30 2e 30 20 53 61 66 61   e/118.0. 0.0 Safa
0130  72 69 2f 35 33 37 2e 33  36 20 45 64 67 2f 31 31   ri/537.3 6 Edg/11
0140  38 2e 30 2e 32 30 38 38  2e 34 36 0d 0a 41 63 63   8.0.2088 .46··Acc
0150  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
```

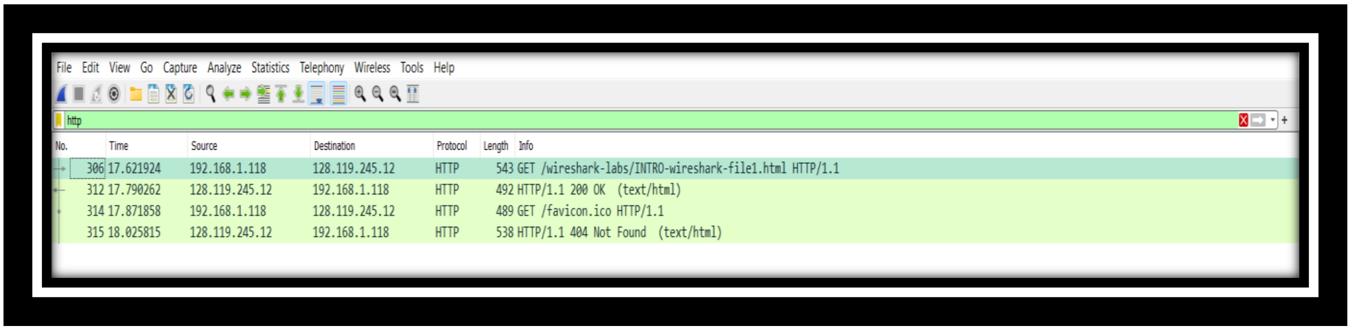
wireshark_Wi-FiQ8Q6C2.pcapng

Packets: 2965 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

3-the Internet address

Source and destination

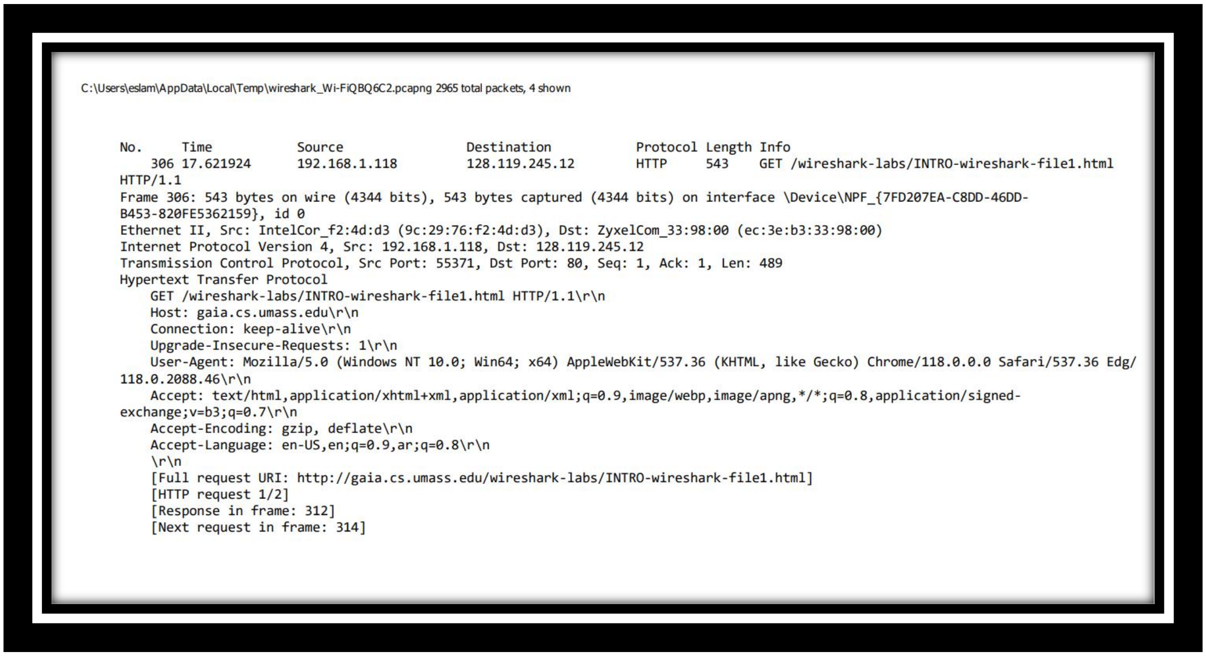


http

No.	Time	Source	Destination	Protocol	Length	Info
306	17.621924	192.168.1.118	128.119.245.12	HTTP	543	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
312	17.790262	128.119.245.12	192.168.1.118	HTTP	492	HTTP/1.1 200 OK (text/html)
314	17.871858	192.168.1.118	128.119.245.12	HTTP	489	GET /favicon.ico HTTP/1.1
315	18.025815	128.119.245.12	192.168.1.118	HTTP	538	HTTP/1.1 404 Not Found (text/html)

4-

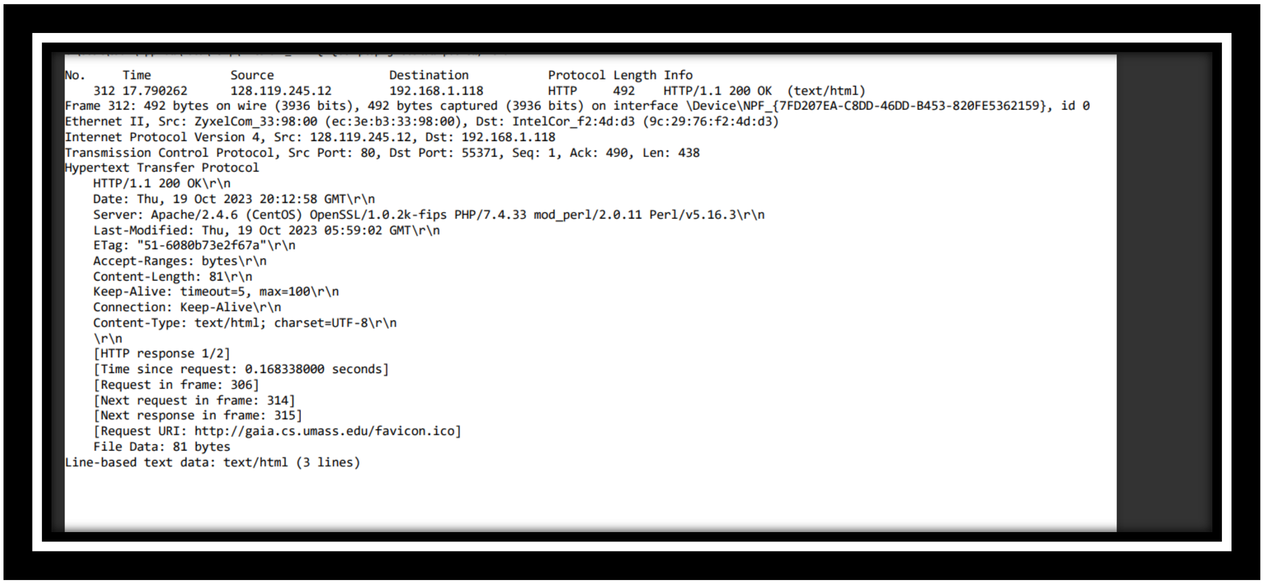
Get



C:\Users\eslam\AppData\Local\Temp\wireshark_Wi-FiQBQ6C2.pcapng 2965 total packets, 4 shown

```
No.     Time           Source                Destination           Protocol Length Info
    306 17.621924      192.168.1.118         128.119.245.12        HTTP     543    GET /wireshark-labs/INTRO-wireshark-file1.html 
HTTP/1.1
Frame 306: 543 bytes on wire (4344 bits), 543 bytes captured (4344 bits) on interface \Device\NPF_{7FD207EA-C8DD-46DD-
B453-820FE5362159}, id 0
Ethernet II, Src: IntelCor_f2:4d:d3 (9c:29:76:f2:4d:d3), Dst: ZyxelCom_33:98:00 (ec:3e:b3:33:98:00)
Internet Protocol Version 4, Src: 192.168.1.118, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55371, Dst Port: 80, Seq: 1, Ack: 1, Len: 489
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/118.0.0.0 Safari/537.36 Edg/
118.0.2088.46\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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: en-US,en;q=0.9,ar;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 312]
    [Next request in frame: 314]
```

OK



```
No.     Time           Source                Destination           Protocol Length Info
    312 17.790262      128.119.245.12        192.168.1.118         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 312: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{7FD207EA-C8DD-46DD-B453-820FE5362159}, id 0
Ethernet II, Src: ZyxelCom_33:98:00 (ec:3e:b3:33:98:00), Dst: IntelCor_f2:4d:d3 (9c:29:76:f2:4d:d3)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.118
Transmission Control Protocol, Src Port: 80, Dst Port: 55371, Seq: 1, Ack: 490, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Thu, 19 Oct 2023 20:12:58 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, 19 Oct 2023 05:59:02 GMT\r\n
    ETag: "51-6080b73e2f67a"\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 1/2]
    [Time since request: 0.168338000 seconds]
    [Request in frame: 306]
    [Next request in frame: 314]
    [Next response in frame: 315]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```