

- 1) The three occurring protocols: TCP, SSDP and HTTP. (In addition: UDP, STP, DNS and MDNS)
- 2) Total delay: 0,154052 seconds.

```
[HTTP response 1/2]
[Time since request: 0.154051727 seconds]
```

- 3) The destination belongs to gaia.cs.umass.edu, the source is my internet address.

Source	Destination
192.168.1.174	128.119.245.12

- 4) OK:

Wireshark capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/INTRO-wireshark-file1.html. The packet details show the HTTP response status as '304 Not Modified'.

No.	Time	Source	Destination	Protocol	Length	Info
20	20:26:41,292437804	192.168.1.174	128.119.245.12	HTTP	587	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
24	20:26:41,342898337	128.119.245.12	192.168.1.174	HTTP	385	HTTP/1.1 304 Not Modified
26	20:26:41,995865340	192.168.1.174	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
27	20:26:42,115095943	128.119.245.12	192.168.1.174	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 24: 385 bytes on wire (2440 bits), 385 bytes captured (2440 bits) on interface 0
 Ethernet II, Src: AsustekC_11:90:b4 (60:45:cb:11:90:b4), Dst: IntelCor_a9:7f:1d (c8:f7:33:a9:7f:1d)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.174
 Transmission Control Protocol, Src Port: 80, Dst Port: 52450, Seq: 1, Ack: 522, Len: 239
 Hypertext Transfer Protocol
 HTTP/1.1 304 Not Modified
 Date: Mon, 21 Jan 2019 19:26:41 GMT
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3
 Connection: Keep-Alive
 Keep-Alive: timeout=5, max=100
 ETag: "51-57ff2654c6269"
 [HTTP response 1/2]
 [Time since request: 0.149362533 seconds]

Mark: In this screenshot, it did return “Not Modified” instead of “OK”. In a previous attempt, it did return “OK”. I ran wireshark with the sudo command and have given it superuser permissions, so it should work...

GET:

Wireshark capture showing HTTP traffic. The packet list shows a GET request for /wireshark-labs/INTRO-wireshark-file1.html. The packet details show the HTTP response status as '200 OK'.

No.	Time	Source	Destination	Protocol	Length	Info
20	20:26:41,292437804	192.168.1.174	128.119.245.12	HTTP	587	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
24	20:26:41,342898337	128.119.245.12	192.168.1.174	HTTP	385	HTTP/1.1 304 Not Modified
26	20:26:41,995865340	192.168.1.174	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
27	20:26:42,115095943	128.119.245.12	192.168.1.174	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 20: 587 bytes on wire (4696 bits), 587 bytes captured (4696 bits) on interface 0
 Ethernet II, Src: IntelCor_a9:7f:1d (c8:f7:33:a9:7f:1d), Dst: AsustekC_11:90:b4 (60:45:cb:11:90:b4)
 Internet Protocol Version 4, Src: 192.168.1.174, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 52450, Dst Port: 80, Seq: 1, Ack: 1, Len: 521
 Hypertext Transfer Protocol
 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
 Host: gaia.cs.umass.edu
 Connection: Keep-Alive
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36 Vivaldi/2.2.1388.37
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
 Accept-Encoding: gzip, deflate
 Accept-Language: en-US,en;q=0.9
 If-None-Match: "51-57ff2654c6269"
 [HTTP response 1/2]
 [Time since request: 0.149362533 seconds]