|  |  |
| --- | --- |
| PROTOCOL | EXPLANTION |
| ARP Address  Resolution  Protocol | A Protocol for connecting a dynamic [IP address](https://whatis.techtarget.com/definition/IP-address-Internet-Protocol-Address) to a permanent physical machine address in a LAN . The physical machine address called “MAC”. |
| ICMP Internet  Control  Message  Protocol | A supporting protocol and is used by networks devices like routers for sending error messages and operational information indicating success or failure when communicating with another [IP address](https://en.wikipedia.org/wiki/IP_address" \o "IP address). |
| LLMNR Link Local  Multicast  Name  Resolution | An DNS based protocol that works only on Microsoft OS that translates domain names of close computer( on the same LAN) with out the need of DNS server. |
| SMB Server Message Block | A [communication protocol](https://en.wikipedia.org/wiki/Communication_protocol) for providing [shared access](https://en.wikipedia.org/wiki/Shared_access) to [files](https://en.wikipedia.org/wiki/Computer_file) and [printers](https://en.wikipedia.org/wiki/Print_server) between [nodes](https://en.wikipedia.org/wiki/Node_(networking)) on a network |
| TLS Transport Layer Security | A protocol to provide privacy and encryption to data between two or more communicating computer applications which encrypt the data transferred |

2)The RTT 8.808- 9.183=0.375sec

3) the DNS of the lab server is gaia.cs.umass.edu  
the DNS of our computer is { ip=192.168.1.10, port =62177 }.  
c) WireShark displays the DNS protocol which provided informations for the two questions above.  
Information for the Source and Destination Domain name.

(4)

No. Time Source Destination Protocol Length Info

85 18:12:08.808197 192.168.1.10 128.119.245.12 HTTP 353 GET /ethereal-labs/INTRO-ethereal-file1.html HTTP/1.1

Frame 85: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface \Device\NPF\_{26EC4540-1904-473B-8DA8-4B081DB4C0EF}, id 0

Ethernet II, Src: HewlettP\_1a:2a:d8 (00:24:81:1a:2a:d8), Dst: Cisco\_ed:72:3e (00:17:59:ed:72:3e)

Internet Protocol Version 4, Src: 192.168.1.10, 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: 339

Identification: 0x0163 (355)

Flags: 0x40, 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: 192.168.1.10

Destination Address: 128.119.245.12

Transmission Control Protocol, Src Port: 62177, Dst Port: 80, Seq: 1, Ack: 1, Len: 299

Source Port: 62177

Destination Port: 80

[Stream index: 3]

[Conversation completeness: Complete, WITH\_DATA (31)]

[TCP Segment Len: 299]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2679433946

[Next Sequence Number: 300 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2594042444

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 256

[Calculated window size: 65536]

[Window size scaling factor: 256]

Checksum: 0x387c [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP payload (299 bytes)

Hypertext Transfer Protocol

GET /ethereal-labs/INTRO-ethereal-file1.html HTTP/1.1\r\n

Accept: text/html, application/xhtml+xml, \*/\*\r\n

Accept-Language: en-US\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

Host: gaia.cs.umass.edu\r\n

DNT: 1\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/INTRO-ethereal-file1.html]

[HTTP request 1/3]

[Response in frame: 90]

[Next request in frame: 92]

No. Time Source Destination Protocol Length Info

90 18:12:09.183448 128.119.245.12 192.168.1.10 HTTP 491 HTTP/1.1 200 OK (text/html)

Frame 90: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface \Device\NPF\_{26EC4540-1904-473B-8DA8-4B081DB4C0EF}, id 0

Ethernet II, Src: Cisco\_ed:72:3e (00:17:59:ed:72:3e), Dst: HewlettP\_1a:2a:d8 (00:24:81:1a:2a:d8)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x88 (DSCP: AF41, ECN: Not-ECT)

Total Length: 477

Identification: 0x6bc9 (27593)

Flags: 0x40, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 41

Protocol: TCP (6)

Header Checksum: 0xac93 [validation disabled]

[Header checksum status: Unverified]

Source Address: 128.119.245.12

Destination Address: 192.168.1.10

Transmission Control Protocol, Src Port: 80, Dst Port: 62177, Seq: 1, Ack: 300, Len: 437

Source Port: 80

Destination Port: 62177

[Stream index: 3]

[Conversation completeness: Complete, WITH\_DATA (31)]

[TCP Segment Len: 437]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 2594042444

[Next Sequence Number: 438 (relative sequence number)]

Acknowledgment Number: 300 (relative ack number)

Acknowledgment number (raw): 2679434245

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window: 237

[Calculated window size: 30336]

[Window size scaling factor: 128]

Checksum: 0x126c [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP payload (437 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 21 Nov 2021 16:11:37 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.25 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 21 Nov 2021 06:59:02 GMT\r\n

ETag: "50-5d1470b16784f"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 80\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 1/3]

[Time since request: 0.375251000 seconds]

[Request in frame: 85]

[Next request in frame: 92]

[Next response in frame: 104]

[Request URI: http://gaia.cs.umass.edu/ethereal-labs/INTRO-ethereal-file1.html]

File Data: 80 bytes

Line-based text data: text/html (3 lines)

5) The server and our computer runs on 1.1 .  
  
6)English US  
7) IP of the server : **128.119.245.12.** IP of our computer : **192.168.1.10**

8)OK 200.  
9) Last update of the HTML is :   
  
10) The number of bytes is :   
  
11)There is no change between the views.

12) conditional GET return 304 status code if nothing changed since the previous GET request.   
13) This was our first get request for ”file2” so the Data has to change, and we cannot compare the date of the last GET request , because as we said it is the first GET.  
14) The server sent us an text/html :  
Graphical user interface, text, application

Description automatically generated15)the date and time of the last file update from last Get.   
Graphical user interface, text, application, email

Description automatically generated



16)304 Not Modified , which means that the file has not change since the last Get request and the data received from CACHE and not from the server.  
the data from the server came as an html text and now we only get the requested file from the CACHE .

17)In the last trace the data transferred in on segment but in this on the data is to big so it spread into 4 segments.

18)We got 2 GET requests but on of them “Favicon”.  
19) 4 TCP segments   
Text

Description automatically generated  
20) OK 200.  
  
21)Each embedded object is from an outsource which means the browser need to send a GET request for each one  
of them.  
22) 3 GET request 1 for the site and 2 for embedded object.  
Text, application

Description automatically generated  
  
for destination :

23)The browser download the images serially, the two images were downloaded in different time .  
The browser used : HTTP1.1.

24)  
Text

Description automatically generated

25)   


26) the field authorization contains “gibberish” which means the information was encrypted.

one of the protocol which was used on the Packet-listing pane was  Transport secure layer and as we explained in the 1st question, this indicates that the information was encrypted.