

AM.EN.P2CSN20020

1) Mapping the OSI layer into the wireshark that we see.

Wireshark network traffic capture showing an HTTP GET request to www.ieee.org. The packet list shows a GET request for / HTTP/1.1. The packet details show the full request URI and various headers. Annotations on the right map the OSI layers to the protocol components:

- Ethernet II is data link layer
- Internet Protocol is network layer
- Transmission Control Protocol is transport layer
- Hypertext Transfer Protocol is application layer

Frame 97: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits) on interface \Device\NPF\_{8DD29CF6-2337-4B28-9F1E-596458C8B67C}, id 0  
> Ethernet II, Src: IntelCor\_06:0b:53 (5c:87:9c:06:0b:53), Dst: Tp-LinkT\_64:16:70 (98:da:c4:64:16:70)  
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 184.24.152.23  
> Transmission Control Protocol, Src Port: 4730, Dst Port: 80, Seq: 1441, Ack: 1, Len: 340  
> [2 Reassembled TCP Segments (1780 bytes): #96(1440), #97(340)]  
> Hypertext Transfer Protocol  
 > GET / HTTP/1.1\r\n  
 Host: www.ieee.org\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/85.0.4183.121 Safari/537.36 Edg/85.0.564.63  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Accept-Language: en-US,en;q=0.9\r\n  
 [truncated]Cookie: \_\_gads=ID=ce43a609727115fa:T=1601289433:S=ALNI\_MZtF61s-JLvAtHCFqPEyp3eLGF\_sw; s\_ecid=MCMID%7C1088652463811608777021161604169\r\n  
 [Full request URI: http://www.ieee.org/]  
 [HTTP request 1/1]  
 [Response in frame: 142]

Frame (394 bytes) Reassembled TCP (1780 bytes)  
wireshark\_Wi-Fi\_20200928211403\_e18848.pcapng

Packets: 440 · Displayed: 4 (0.9%) Profile: Default

21:15 28-09-2020