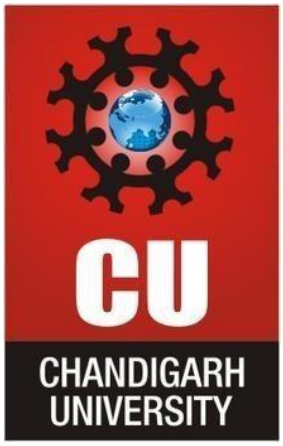
DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING

Discover. Learn. Empower.

CHANDIGARH UNIVERSITY
UNIVERSITY INSTITUTE OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING



Submitted By: Pranjal Kumar	**Submitted To:** Renuka Ratten
Subject Name	WEB AND MOBILE SECURITY LAB
Subject Code	20CSP-338
Branch	Computer Science
Semester	5th

DEPARTMENT OF
COMPUTER SCIENCE & ENGINEERING

CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

UNIVERSITY INSTITUTE OF ENGINEERING

Department of Computer Science & Engineering

Subject Name: WEB AND MOBILE SECURITY LAB

Subject Code: 20CSP-338

Submitted to: Renuka Ratten

Faculty name: Renuka Ratten

Submitted by: Pranjal Kumar

Name: Pranjal Kumar

UID: 20BCS3504

Section: 607

Group: B

Ex. No	List of Experiments	Date	Conduct (MM: 12)	Viva (MM: 10)	Record (MM: 8)	Total (MM: 30)	Remarks/Signature
1.1	Open any website on computer system and identify http packet on monitoring tool like Wireshark.	19/08/22					
1.2	Design a method to simulate the html injection and cross sites cripting to exploit the attackers	28/08/22					
1.3	Working of CSRF (cross site request forgery) attack/ Vulnerability.	16/09/22					
2.1	Design methods to break authentication schemes (SQL Injection Attack)**.**	04/09/22					
2.2							
2.3							
2.4							
3.1							

3.2							
3.3							

Experiment No 1

Aim: Open any website on computer system and identify http packet on monitoring tool like Wireshark

Objective: To analyse Http traffic

Software/Hardware Requirements: Windows 7 & above version

Tools to be used: Wireshark App

Introduction: Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.
The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related professional.

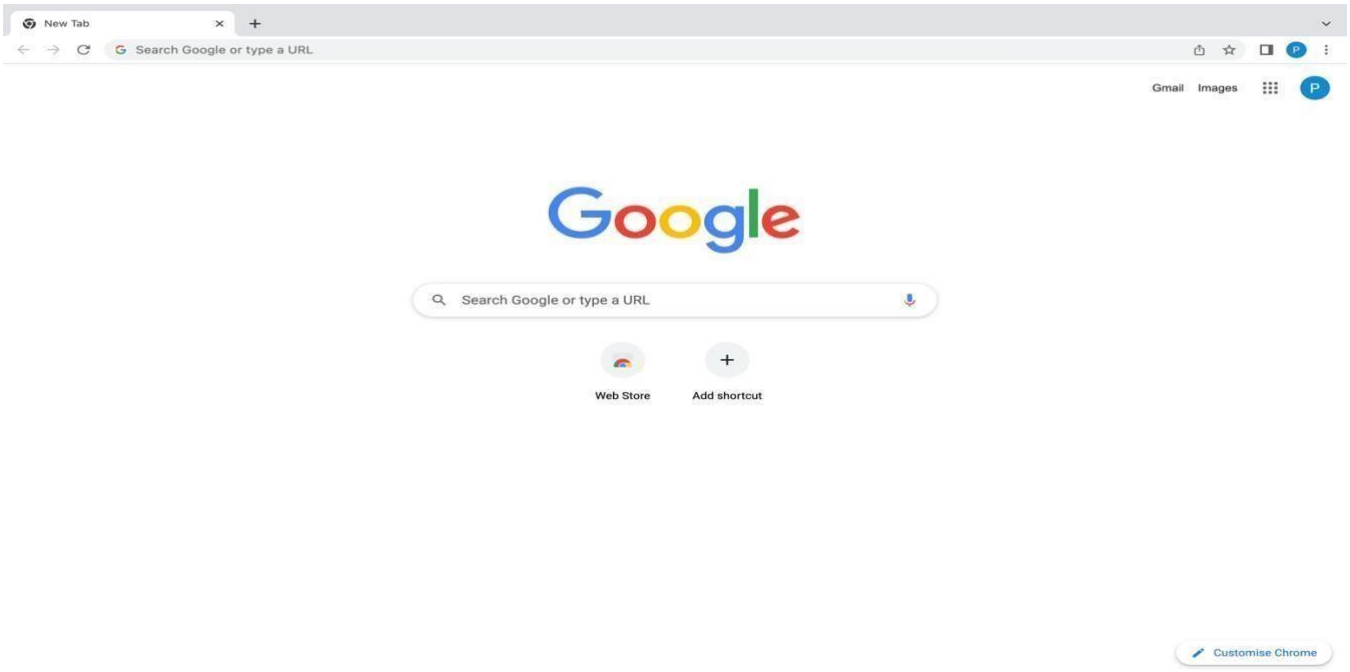
Steps/Method/Coding:

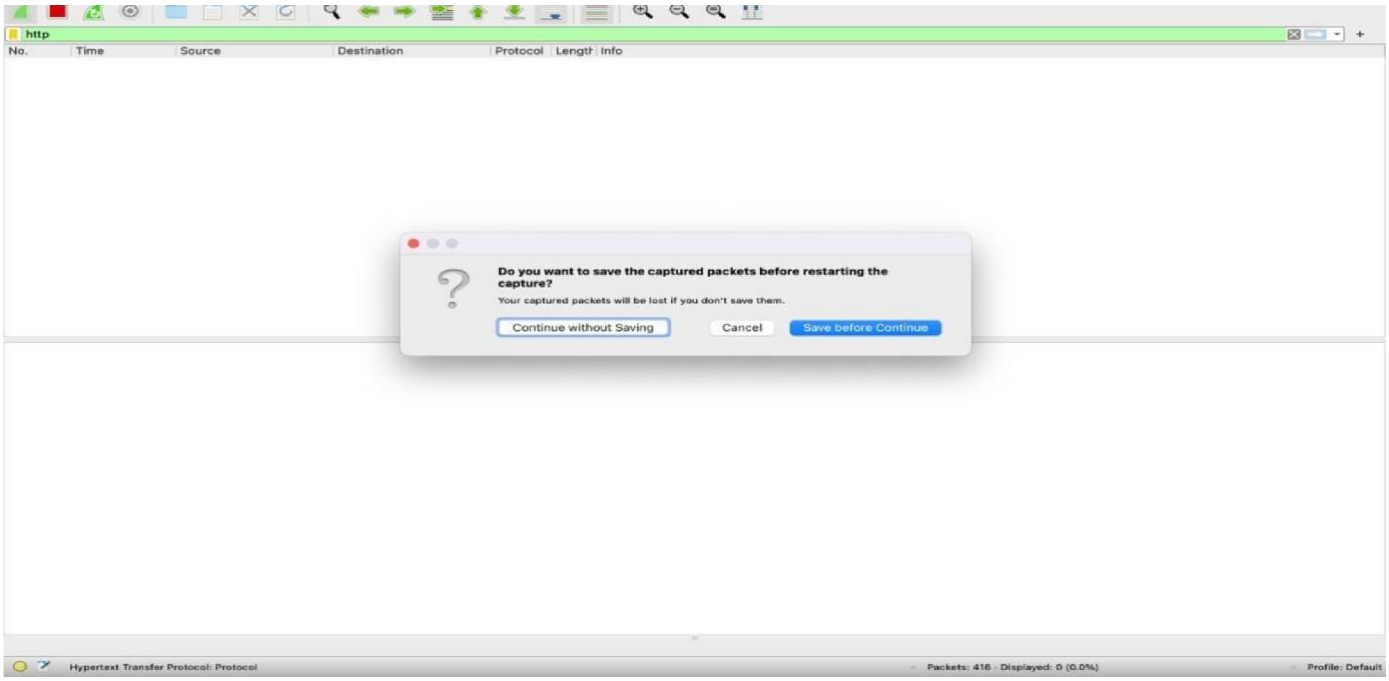
1. Install Wireshark.
2. Open your Internet browser.
3. Clear your browser cache.
4. Open Wireshark

5. Click on "Capture > Interfaces". A pop-up window will display.
6. You'll want to capture traffic that goes through your ethernet driver. Click on the `Start` button to capture traffic via this interface.
7. Visit the URL that you wanted to capture the traffic from.
8. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
9. After the traffic capture is stopped, please save the captured traffic into a *.pcap format file and attach it to your support ticket.

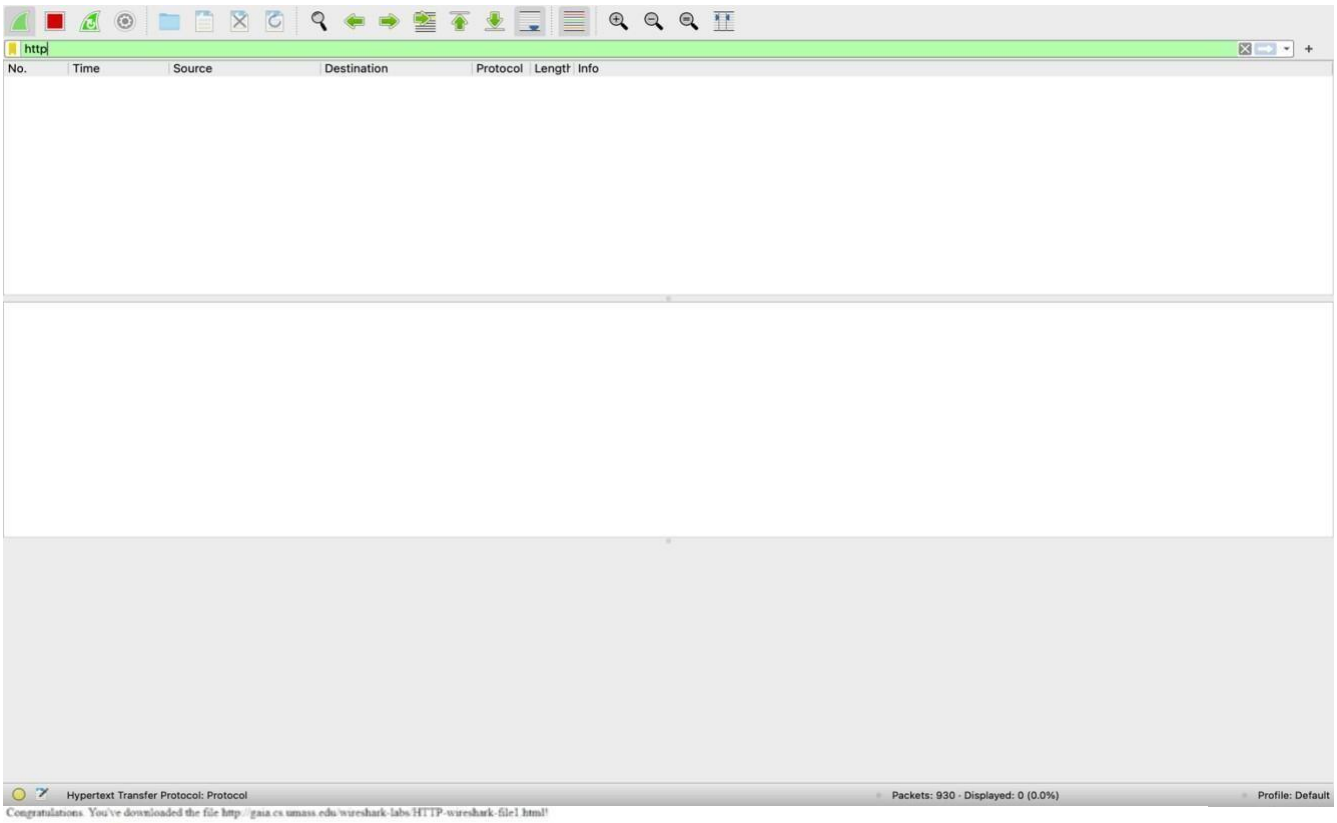
Output screenshot:

before doing any other activities I will clear the cache of my browser

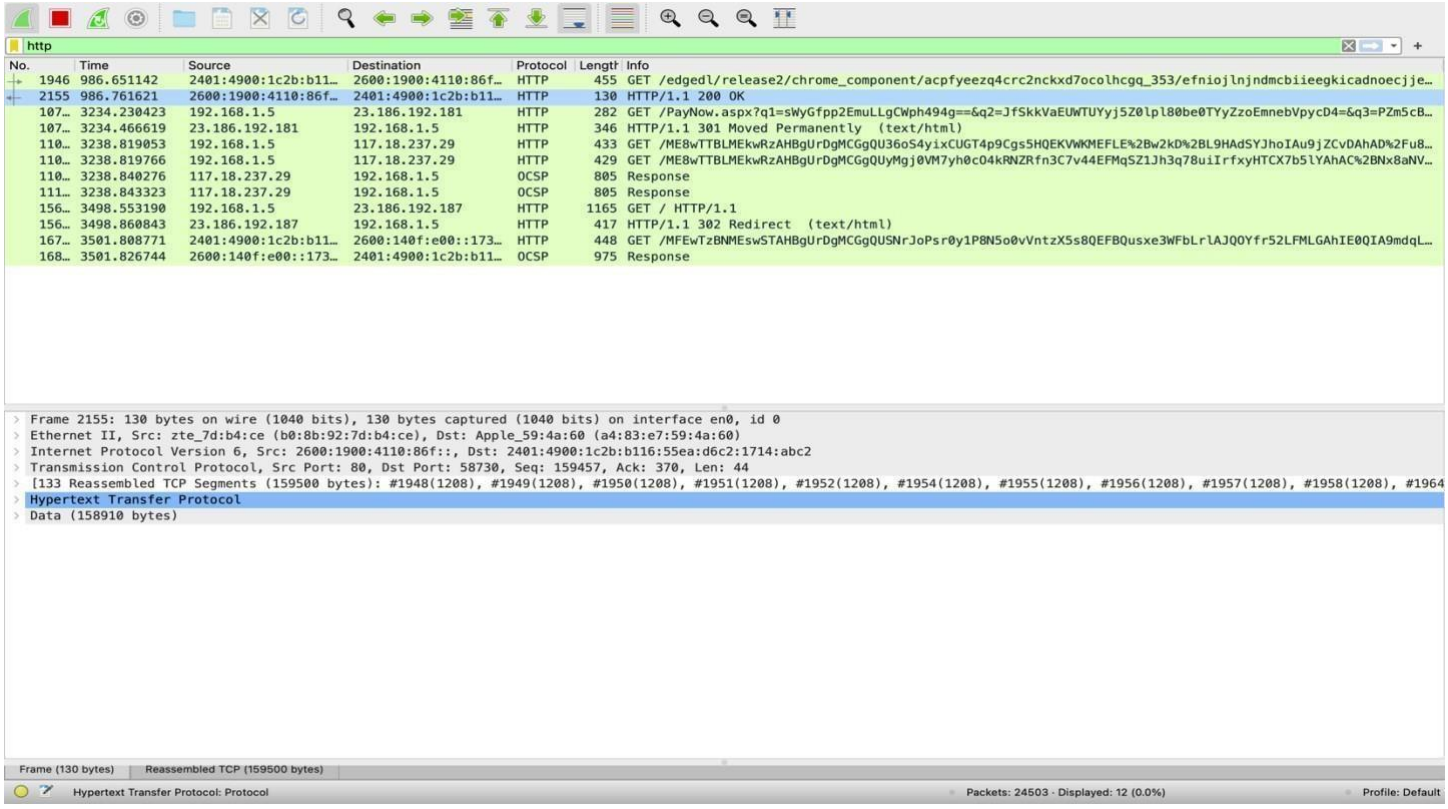


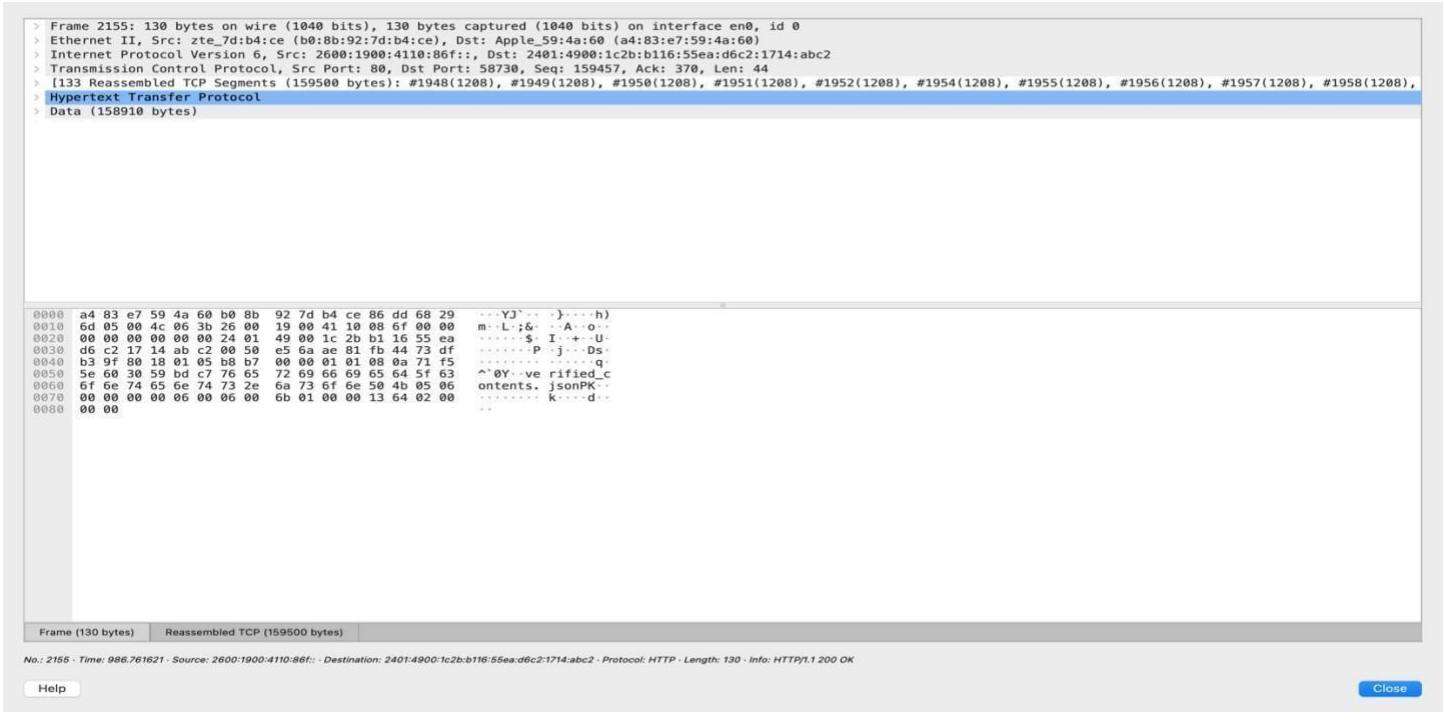


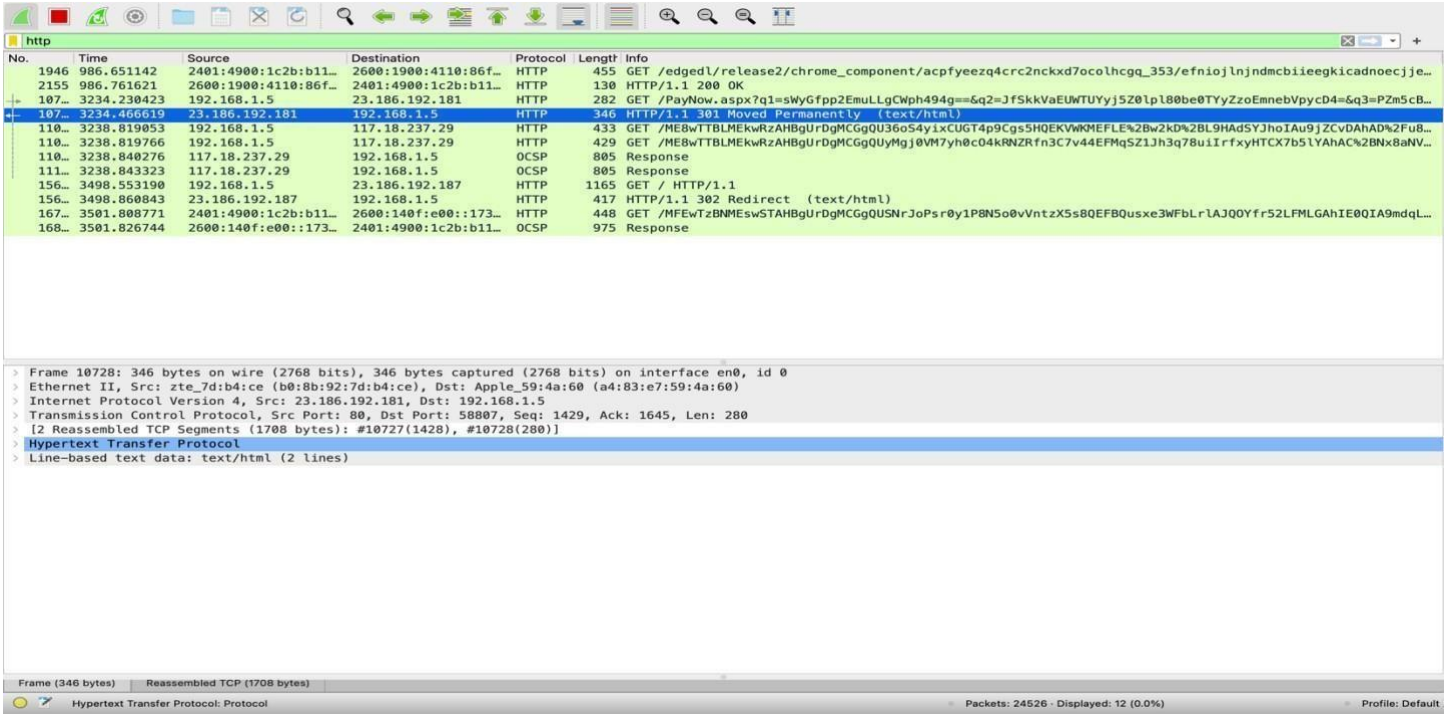
and then I will open a link

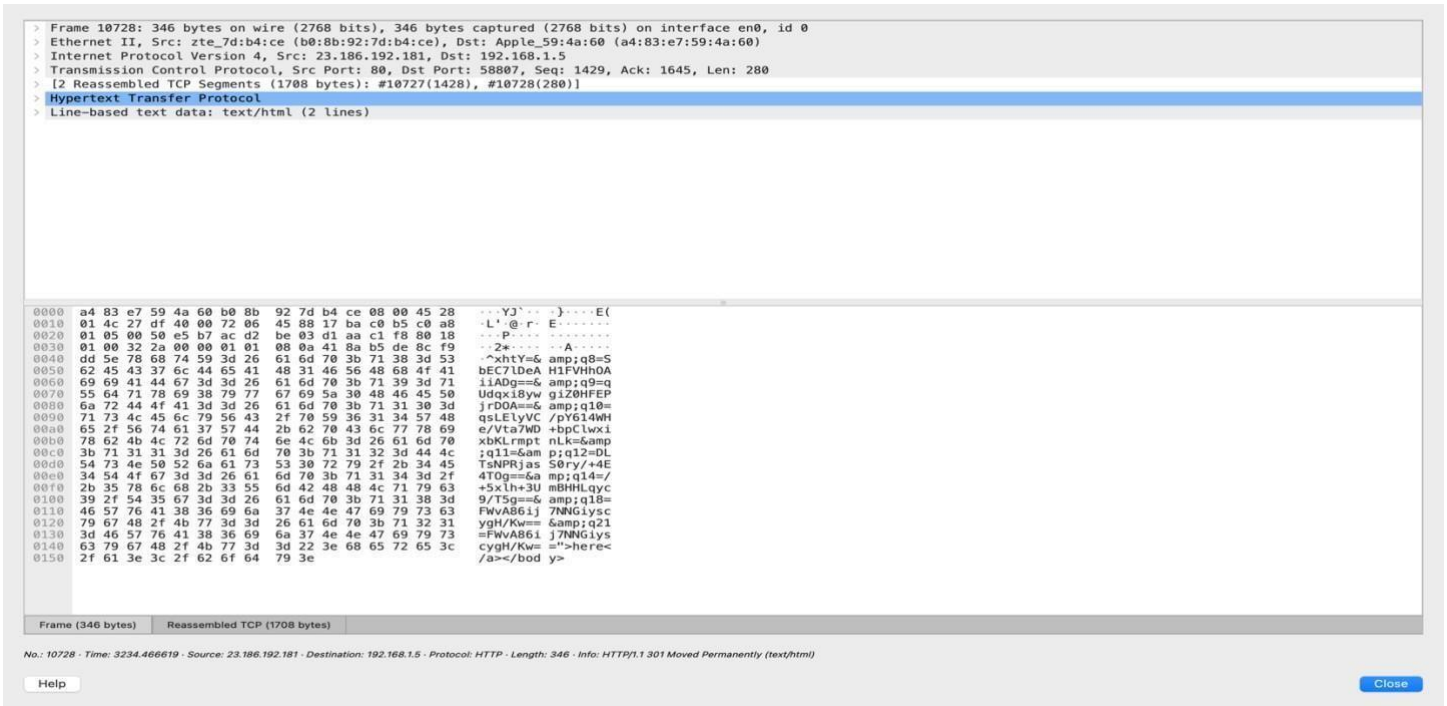


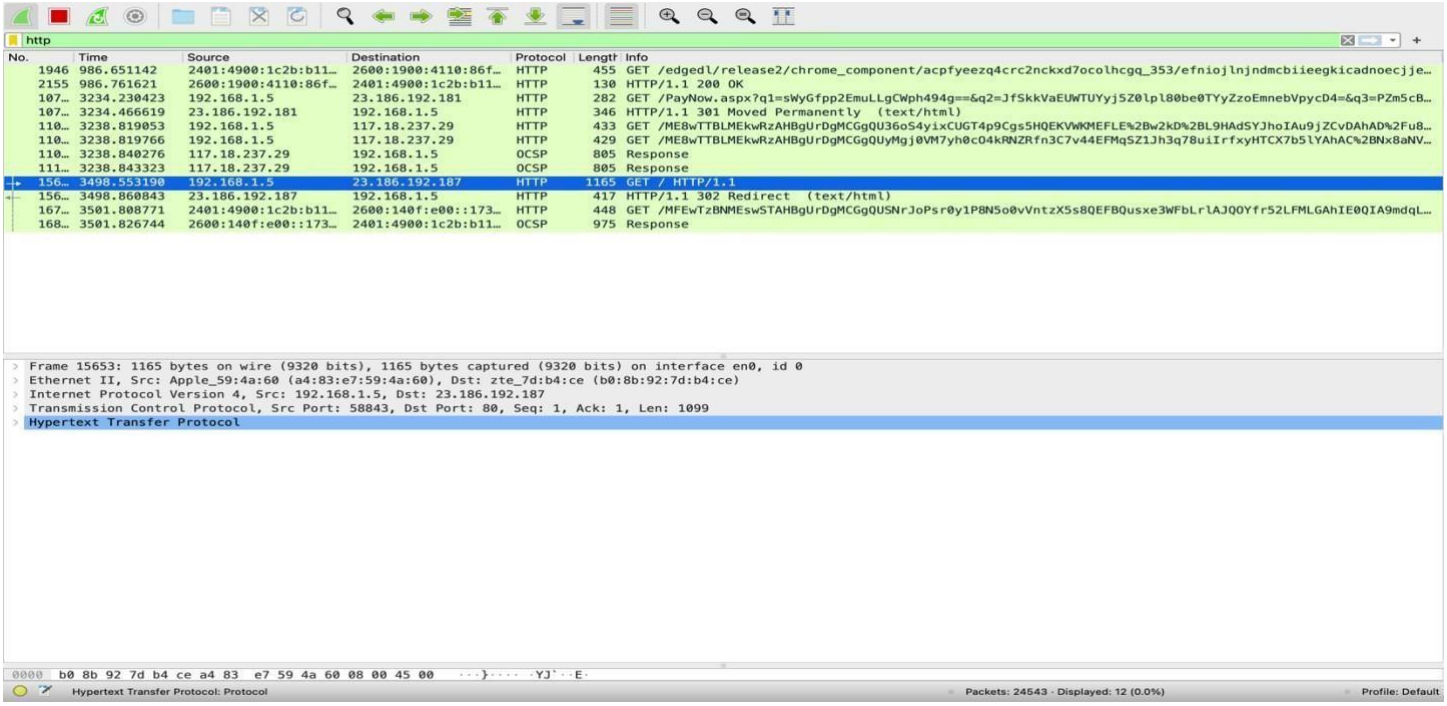
The link:
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

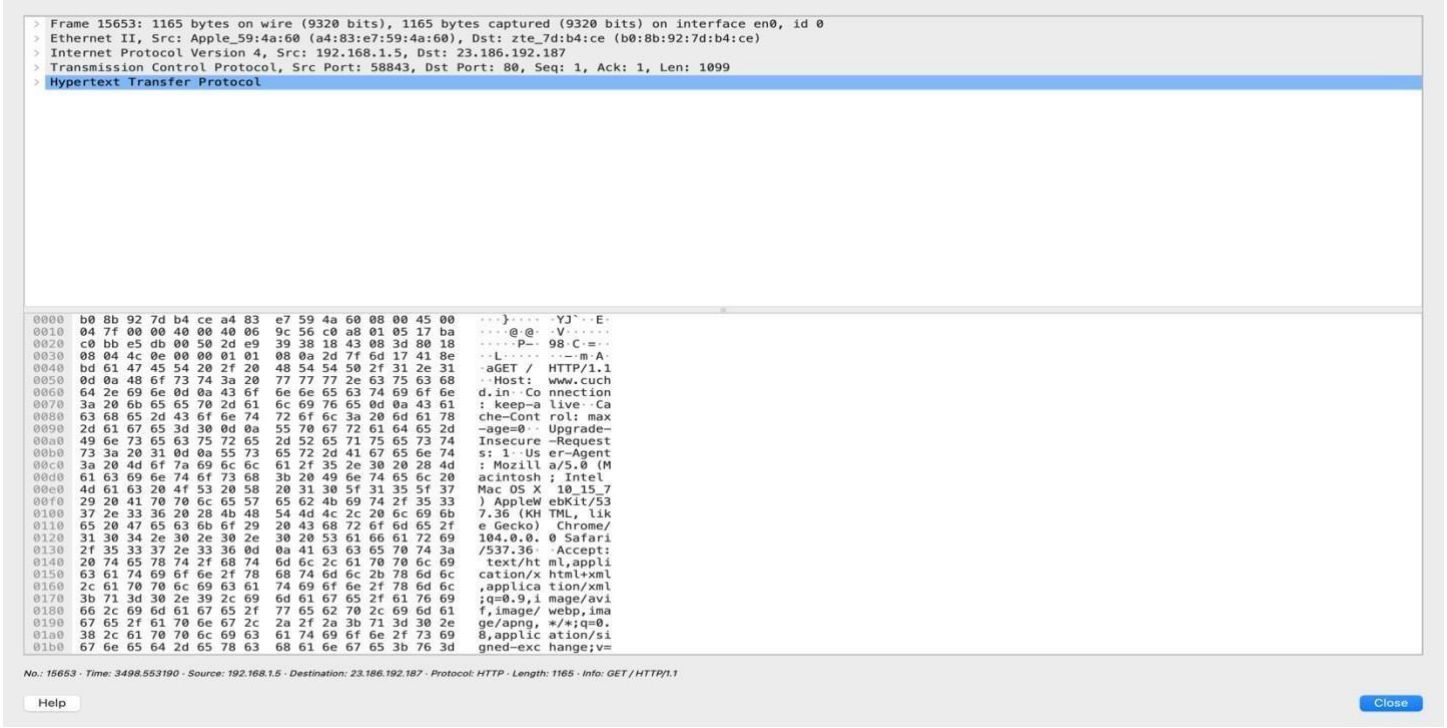

http
No. Time Source Destination Protocol Length Info
1946 986.651142 2401:4900:1c2b:b11… 2600:1900:4110:86f… HTTP 455 GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7ocolhcgq_353/efniojlnjndmcbiieegkicadnoecjje…
2155 986.761621 2600:1900:4110:86f… 2401:4900:1c2b:b11… HTTP 130 HTTP/1.1 200 OK
107… 3234.230423 192.168.1.5 23.186.192.181 HTTP 282 GET /PayNow.aspx?q1=sWyGfpp2EmuLLgCWph494g==&q2=JfSkkVaEUWTUYyj5Z0lpl80be0TYyZzoEmnebVpycD4=&q3=PZm5cB…
107… 3234.466619 23.186.192.181 192.168.1.5 HTTP 346 HTTP/1.1 301 Moved Permanently (text/html)
110… 3238.819053 192.168.1.5 117.18.237.29 HTTP 433 GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQU36oS4yixCUGT4p9Cgs5HQEKVWKMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAD%2Fu8…
110… 3238.819766 192.168.1.5 117.18.237.29 HTTP 429 GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQUyMgj0VM7yh0cO4kRNZRfn3C7v44EFMqSZ1Jh3q78uiIrfxyHTCX7b5lYAhAC%2BNx8aNV…
110… 3238.840276 117.18.237.29 192.168.1.5 OCSP 805 Response
111… 3238.843323 117.18.237.29 192.168.1.5 OCSP 805 Response
156… 3498.553190 192.168.1.5 23.186.192.187 HTTP 1165 GET / HTTP/1.1
156… 3498.860843 23.186.192.187 192.168.1.5 HTTP 417 HTTP/1.1 302 Redirect (text/html)
167… 3501.808771 2401:4900:1c2b:b11… 2600:140f:e00::173… HTTP 448 GET /MFEwTzBNMEswSTAHBgUrDgMCGgQUSNrJoPsr0y1P8N5o0vVntzX5s8QEFBQusxe3WFbLrlAJQOYfr52LFMLGAhIE0QIA9mdqL…
168… 3501.826744 2600:140f:e00::173… 2401:4900:1c2b:b11… OCSP 975 Response
Frame 2155: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface en0, id 0
Ethernet II, Src: zte_7d:b4:ce (b0:8b:92:7d:b4:ce), Dst: Apple_59:4a:60 (a4:83:e7:59:4a:60)
Internet Protocol Version 6, Src: 2600:1900:4110:86f::, Dst: 2401:4900:1c2b:b116:55ea:d6c2:1714:abc2
Transmission Control Protocol, Src Port: 80, Dst Port: 58730, Seq: 159457, Ack: 370, Len: 44
[133 Reassembled TCP Segments (159500 bytes): #1948(1208), #1949(1208), #1950(1208), #1951(1208), #1952(1208), #1954(1208), #1955(1208), #1956(1208), #1957(1208), #1958(1208), #1964
Hypertext Transfer Protocol
Data (158910 bytes)
Frame (130 bytes)
Reassembled TCP (159500 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 24503 · Displayed: 12 (0.0%)
Profile: Default

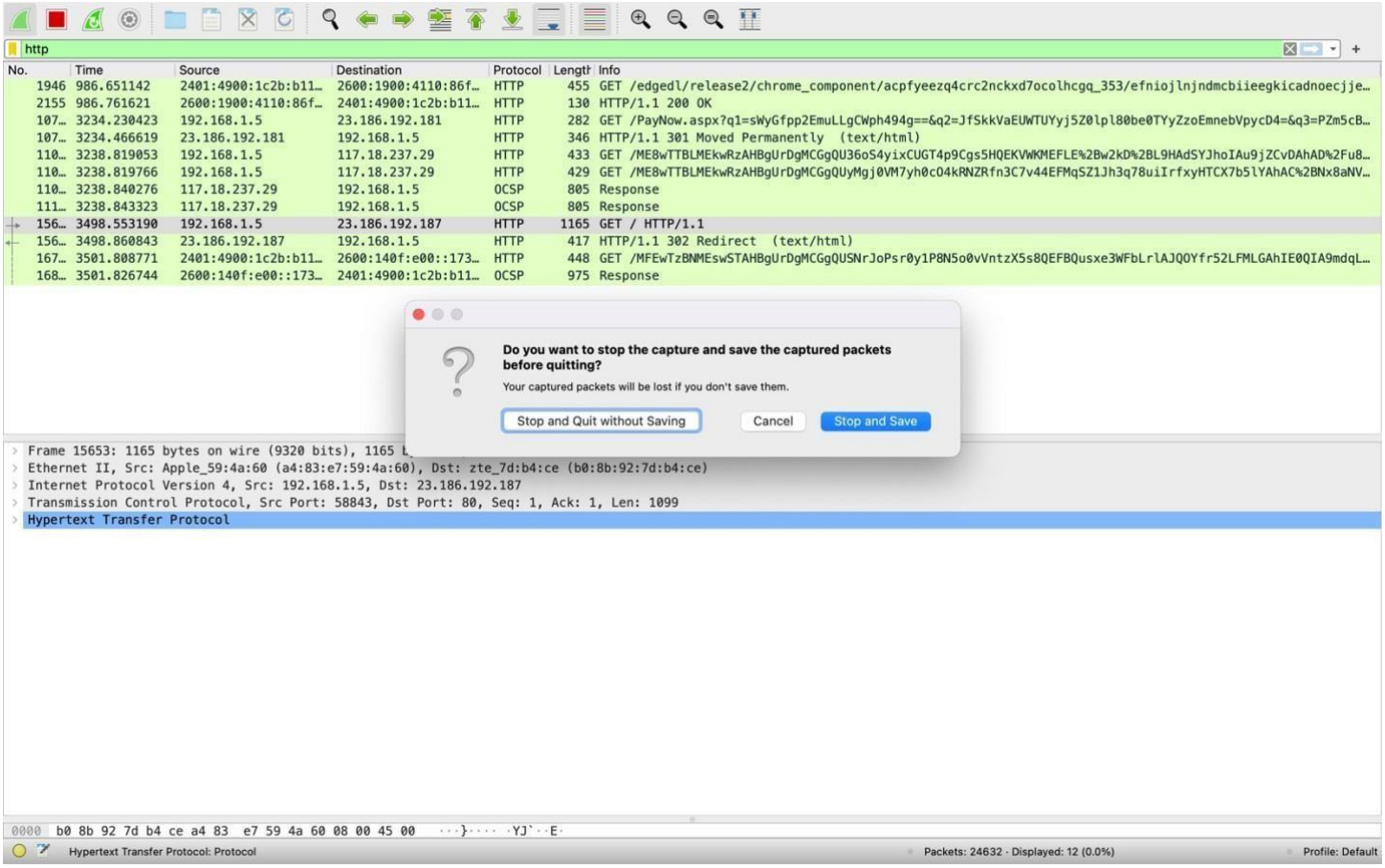

Frame 2155: 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits) on interface en0, id 0
Ethernet II, Src: zte_7d:b4:ce (b0:8b:92:7d:b4:ce), Dst: Apple_59:4a:60 (a4:83:e7:59:4a:60)
Internet Protocol Version 6, Src: 2600:1900:4110:86f::, Dst: 2401:4900:1c2b:b116:55ea:d6c2:1714:abc2
Transmission Control Protocol, Src Port: 80, Dst Port: 58730, Seq: 159457, Ack: 370, Len: 44
[133 Reassembled TCP Segments (159500 bytes): #1948(1208), #1949(1208), #1950(1208), #1951(1208), #1952(1208), #1954(1208), #1955(1208), #1956(1208), #1957(1208), #1958(1208),
Hypertext Transfer Protocol
Data (158910 bytes)
0000 a4 83 e7 59 4a 60 b0 8b 92 7d b4 ce 86 dd 68 29
0010 6d 05 00 4c 06 3b 26 00 19 00 41 10 08 6f 00 00
0020 00 00 00 00 00 00 24 01 49 00 1c 2b b1 16 55 ea
0030 d6 c2 17 14 ab c2 00 50 e5 6a ae 81 fb 44 73 df
0040 b3 9f 80 18 01 05 b8 b7 00 00 01 01 08 0a 71 f5
0050 5e 60 30 59 bd c7 76 65 72 69 66 69 65 64 5f 63
0060 6f 6e 74 65 6e 74 73 2e 6a 73 6f 6e 50 4b 05 06
0070 00 00 00 00 06 00 06 00 6b 01 00 00 13 64 02 00
0080 00 00
Frame (130 bytes)
Reassembled TCP (159500 bytes)
No.: 2155 · Time: 986.761621 · Source: 2600:1900:4110:86f:: · Destination: 2401:4900:1c2b:b116:55ea:d6c2:1714:abc2 · Protocol: HTTP · Length: 130 · Info: HTTP/1.1 200 OK
Help
Close


http
No. Time Source Destination Protocol Lengt Info
1946 986.651142 2401:4900:1c2b:b11… 2600:1900:4110:86f… HTTP 455 GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7ocolhcgq_353/efniojlnjndmcbiieegkicadnoecjje…
2155 986.761621 2600:1900:4110:86f… 2401:4900:1c2b:b11… HTTP 130 HTTP/1.1 200 OK
107… 3234.230423 192.168.1.5 23.186.192.181 HTTP 282 GET /PayNow.aspx?q1=sWyGfpp2EmuLLgCWph494g==&q2=JfSkkVaEUWTUYyj5Z0lpl80be0TYyZzoEmnebVpycD4=&q3=PZm5cB…
107… 3234.466619 23.186.192.181 192.168.1.5 HTTP 346 HTTP/1.1 301 Moved Permanently (text/html)
110… 3238.819053 192.168.1.5 117.18.237.29 HTTP 433 GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQU36oS4yixCUGT4p9Cgs5HQEKVWKMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAD%2Fu8…
110… 3238.819766 192.168.1.5 117.18.237.29 HTTP 429 GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQUyMgj0VM7yh0cO4kRNZRfn3C7v44EFMqSZ1Jh3q78uiIrfxyHTCX7b5lYAhAC%2BNx8aNV…
110… 3238.840276 117.18.237.29 192.168.1.5 OCSP 805 Response
111… 3238.843323 117.18.237.29 192.168.1.5 OCSP 805 Response
156… 3498.553190 192.168.1.5 23.186.192.187 HTTP 1165 GET / HTTP/1.1
156… 3498.860843 23.186.192.187 192.168.1.5 HTTP 417 HTTP/1.1 302 Redirect (text/html)
167… 3501.808771 2401:4900:1c2b:b11… 2600:140f:e00::173… HTTP 448 GET /MFEwTzBNMEswSTAHBgUrDgMCGgQUSNrJoPsr0y1P8N5o0vVntzX5s8QEFBQusxe3WFbLrlAJQOYfr52LFMLGAhIE0QIA9mdqL…
168… 3501.826744 2600:140f:e00::173… 2401:4900:1c2b:b11… OCSP 975 Response
Frame 10728: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface en0, id 0
Ethernet II, Src: zte_7d:b4:ce (b0:8b:92:7d:b4:ce), Dst: Apple_59:4a:60 (a4:83:e7:59:4a:60)
Internet Protocol Version 4, Src: 23.186.192.181, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 58807, Seq: 1429, Ack: 1645, Len: 280
[2 Reassembled TCP Segments (1708 bytes): #10727(1428), #10728(280)]
Hypertext Transfer Protocol
Line-based text data: text/html (2 lines)
Frame (346 bytes)
Reassembled TCP (1708 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 24526 · Displayed: 12 (0.0%)
Profile: Default


Frame 10728: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface en0, id 0
Ethernet II, Src: zte_7d:b4:ce (b0:8b:92:7d:b4:ce), Dst: Apple_59:4a:60 (a4:83:e7:59:4a:60)
Internet Protocol Version 4, Src: 23.186.192.181, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 58807, Seq: 1429, Ack: 1645, Len: 280
[2 Reassembled TCP Segments (1708 bytes): #10727(1428), #10728(280)]
Hypertext Transfer Protocol
Line-based text data: text/html (2 lines)
0000 a4 83 e7 59 4a 60 b0 8b 92 7d b4 ce 08 00 45 28 ···YJ`·· ·}····E(
0010 01 4c 27 df 40 00 72 06 45 88 17 ba c0 b5 c0 a8 ·L'·@·r· E·······
0020 01 05 00 50 e5 b7 ac d2 be 03 d1 aa c1 f8 80 18 ···P···· ········
0030 01 00 32 2a 00 00 01 01 08 0a 41 8a b5 de 8c f9 ··2*···· ··A·····
0040 dd 5e 78 68 74 59 3d 26 61 6d 70 3b 71 38 3d 53 ·^xhtY=& amp;q8=S
0050 62 45 43 37 6c 44 65 41 48 31 46 56 48 68 4f 41 bEC7lDeA H1FVHhOA
0060 69 69 41 44 67 3d 3d 26 61 6d 70 3b 71 39 3d 71 iiADg==& amp;q9=q
0070 55 64 71 78 69 38 79 77 67 69 5a 30 48 46 45 50 Udqxi8yw giZ0HFEP
0080 6a 72 44 4f 41 3d 3d 26 61 6d 70 3b 71 31 30 3d jrDOA==& amp;q10=
0090 71 73 4c 45 6c 79 56 43 2f 70 59 36 31 34 57 48 qsLElyVC /pY614WH
00a0 65 2f 56 74 61 37 57 44 2b 62 70 43 6c 77 78 69 e/Vta7WD +bpClwxi
00b0 78 62 4b 4c 72 6d 70 74 6e 4c 6b 3d 26 61 6d 70 xbKLrmpt nLk=&amp
00c0 3b 71 31 31 3d 26 61 6d 70 3b 71 31 32 3d 44 4c ;q11=&am p;q12=DL
00d0 54 73 4e 50 52 6a 61 73 53 30 72 79 2f 2b 34 45 TsNPRjas S0ry/+4E
00e0 34 54 4f 67 3d 3d 26 61 6d 70 3b 71 31 34 3d 2f 4TOg==&a mp;q14=/
00f0 2b 35 78 6c 68 2b 33 55 6d 42 48 48 4c 71 79 63 +5xlh+3U mBHHLqyc
0100 39 2f 54 35 67 3d 3d 26 61 6d 70 3b 71 31 38 3d 9/T5g==& amp;q18=
0110 46 57 76 41 38 36 69 6a 37 4e 4e 47 69 79 73 63 FWvA86ij 7NNGiysc
0120 79 67 48 2f 4b 77 3d 3d 26 61 6d 70 3b 71 32 31 ygH/Kw== &q21
0130 3d 46 57 76 41 38 36 69 6a 37 4e 4e 47 69 79 73 =FWvA86i j7NNGiys
0140 63 79 67 48 2f 4b 77 3d 3d 22 3e 68 65 72 65 3c cygH/Kw= =">here<
0150 2f 61 3e 3c 2f 62 6f 64 79 3e /a></bod y>
Frame (346 bytes)
Reassembled TCP (1708 bytes)
No.: 10728 · Time: 3234.466619 · Source: 23.186.192.181 · Destination: 192.168.1.5 · Protocol: HTTP · Length: 346 · Info: HTTP/1.1 301 Moved Permanently (text/html)
Help
Close


http
No. Time Source Destination Protocol Lengt Info
1946 986.651142 2401:4900:1c2b:b11… 2600:1900:4110:86f… HTTP 455 GET /edgedl/release2/chrome_component/acpfyeezq4crc2nckxd7ocolhcgq_353/efniojlnjndmcbiieegkicadnoecjje…
2155 986.761621 2600:1900:4110:86f… 2401:4900:1c2b:b11… HTTP 130 HTTP/1.1 200 OK
107… 3234.230423 192.168.1.5 23.186.192.181 HTTP 282 GET /PayNow.aspx?q1=sWyGfpp2EmuLLgCWph494g==&q2=JfSkkVaEUWTUYyj5Z0lpl80be0TYyZzoEmnebVpycD4=&q3=PZm5cB…
107… 3234.466619 23.186.192.181 192.168.1.5 HTTP 346 HTTP/1.1 301 Moved Permanently (text/html)
110… 3238.819053 192.168.1.5 117.18.237.29 HTTP 433 GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQU36oS4yixCUGT4p9Cgs5HQEKVWKMEFLE%2Bw2kD%2BL9HAdSYJhoIAu9jZCvDAhAD%2Fu8…
110… 3238.819766 192.168.1.5 117.18.237.29 HTTP 429 GET /ME8wTTBLMEkwRzAHBgUrDgMCGgQUyMgj0VM7yh0cO4kRNZRfn3C7v44EFMqSZ1Jh3q78uiIrfxyHTCX7b5lYAhAC%2BNx8aNV…
110… 3238.840276 117.18.237.29 192.168.1.5 OCSP 805 Response
111… 3238.843323 117.18.237.29 192.168.1.5 OCSP 805 Response
156… 3498.553190 192.168.1.5 23.186.192.187 HTTP 1165 GET / HTTP/1.1
156… 3498.860843 23.186.192.187 192.168.1.5 HTTP 417 HTTP/1.1 302 Redirect (text/html)
167… 3501.808771 2401:4900:1c2b:b11… 2600:140f:e00::173… HTTP 448 GET /MFEwTzBNMEswSTAHBgUrDgMCGgQUSNrJoPsr0y1P8N5o0vVntzX5s8QEFBQusxe3WFbLrlAJQOYfr52LFMLGAhIE0QIA9mdqL…
168… 3501.826744 2600:140f:e00::173… 2401:4900:1c2b:b11… OCSP 975 Response
Frame 15653: 1165 bytes on wire (9320 bits), 1165 bytes captured (9320 bits) on interface en0, id 0
Ethernet II, Src: Apple_59:4a:60 (a4:83:e7:59:4a:60), Dst: zte_7d:b4:ce (b0:8b:92:7d:b4:ce)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 23.186.192.187
Transmission Control Protocol, Src Port: 58843, Dst Port: 80, Seq: 1, Ack: 1, Len: 1099
Hypertext Transfer Protocol
0000 b0 8b 92 7d b4 ce a4 83 e7 59 4a 60 08 00 45 00 ···}····· ·YJ`··E·
Hypertext Transfer Protocol: Protocol
Packets: 24543 · Displayed: 12 (0.0%)
Profile: Default


Frame 15653: 1165 bytes on wire (9320 bits), 1165 bytes captured (9320 bits) on interface en0, id 0
Ethernet II, Src: Apple_59:4a:60 (a4:83:e7:59:4a:60), Dst: zte_7d:b4:ce (b0:8b:92:7d:b4:ce)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 23.186.192.187
Transmission Control Protocol, Src Port: 58843, Dst Port: 80, Seq: 1, Ack: 1, Len: 1099
Hypertext Transfer Protocol
0000 b0 8b 92 7d b4 ce a4 83 e7 59 4a 60 08 00 45 00 ···}····· ·YJ`··E·
0010 04 7f 00 00 40 00 40 06 9c 56 c0 a8 01 05 17 ba ····@·@· ·V·····
0020 c0 bb e5 db 00 50 2d e9 39 38 18 43 08 3d 80 18 ·····P-· 98·C·=··
0030 08 04 4c 0e 00 00 01 01 08 0a 2d 7f 6d 17 41 8e ··L····· ··-·m·A·
0040 bd 61 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 ·aGET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 63 75 63 68 ··Host: www.cuch
0060 64 2e 69 6e 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e d.in··Co nnection
0070 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 61 : keep-a live··Ca
0080 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 che-Cont rol: max
0090 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65 2d -age=0·· Upgrade-
00a0 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 Insecure -Request
00b0 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 s: 1··Us er-Agent
00c0 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 4d : Mozill a/5.0 (M
00d0 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 65 6c 20 acintosh ; Intel
00e0 4d 61 63 20 4f 53 20 58 20 31 30 5f 31 35 5f 37 Mac OS X 10_15_7
00f0 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33) AppleW ebKit/53
0100 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 7.36 (KH TML, lik
0110 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f e Gecko) Chrome/
0120 31 30 34 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 104.0.0. 0 Safari
0130 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a /537.36· ·Accept:
0140 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/ht ml,appli
0150 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/x html+xml
0160 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applica tion/xml
0170 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 ;q=0.9,i mage/avi
0180 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 f,image/ webp,ima
0190 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e ge/apng, */*;q=0.
01a0 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 8,applic ation/si
01b0 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d gned-exc hange;v=
No.: 15653 · Time: 3498.553190 · Source: 192.168.1.5 · Destination: 23.186.192.187 · Protocol: HTTP · Length: 1165 · Info: GET / HTTP/1.1
Help
Close



Learning Outcomes:

Identify requests (from client) and response packets. Find HTTP version, response code/phrase, requested file (including size). Observe single small file (e.g., simple html file) request/response behaviour and the request/response behaviour for a file that has already been received. Observe how a larger file is sent in multiple segments Observe multi-file (e.g., web page with image) request/response behaviour. Observe request/response behaviour for a page that needs authentication.

Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1			
2			
3			
4			