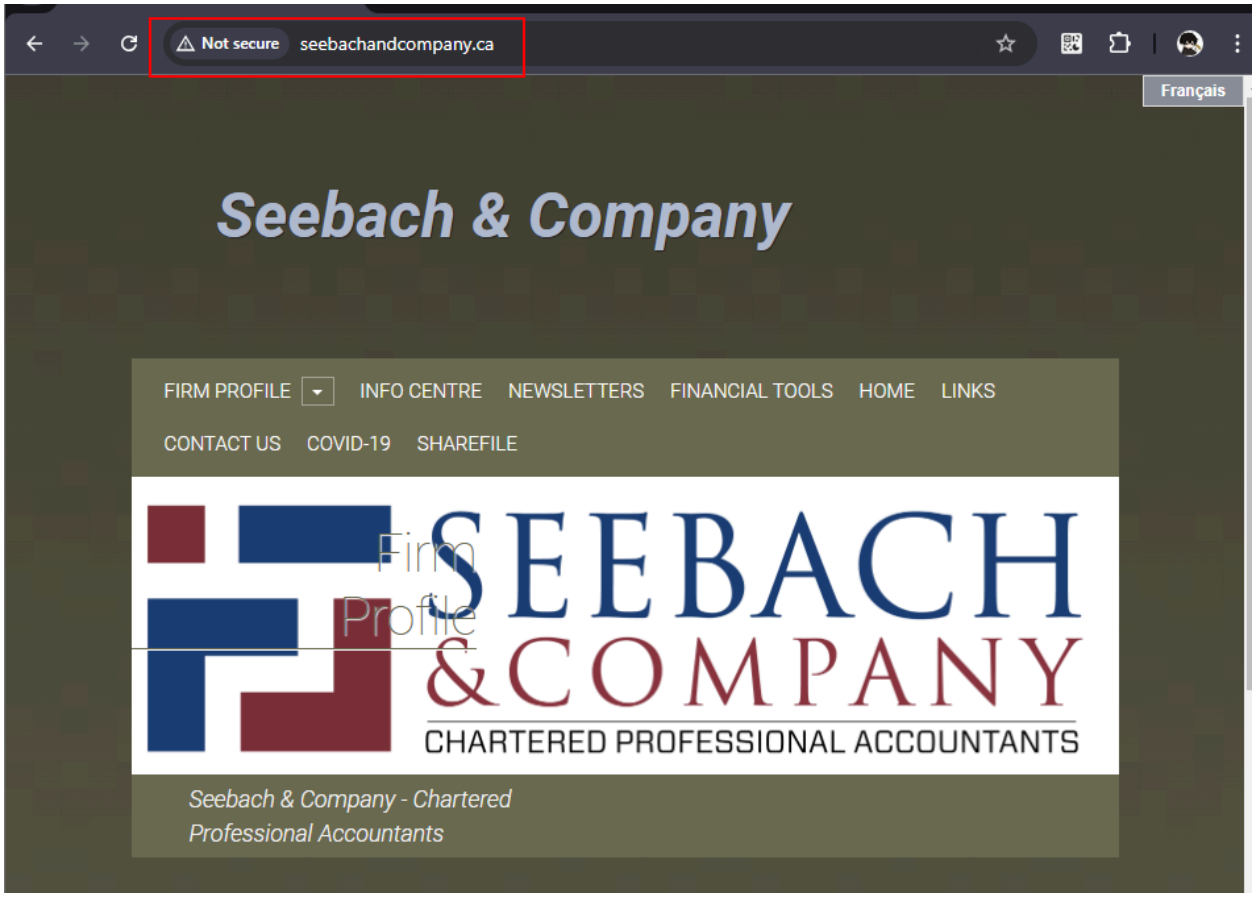
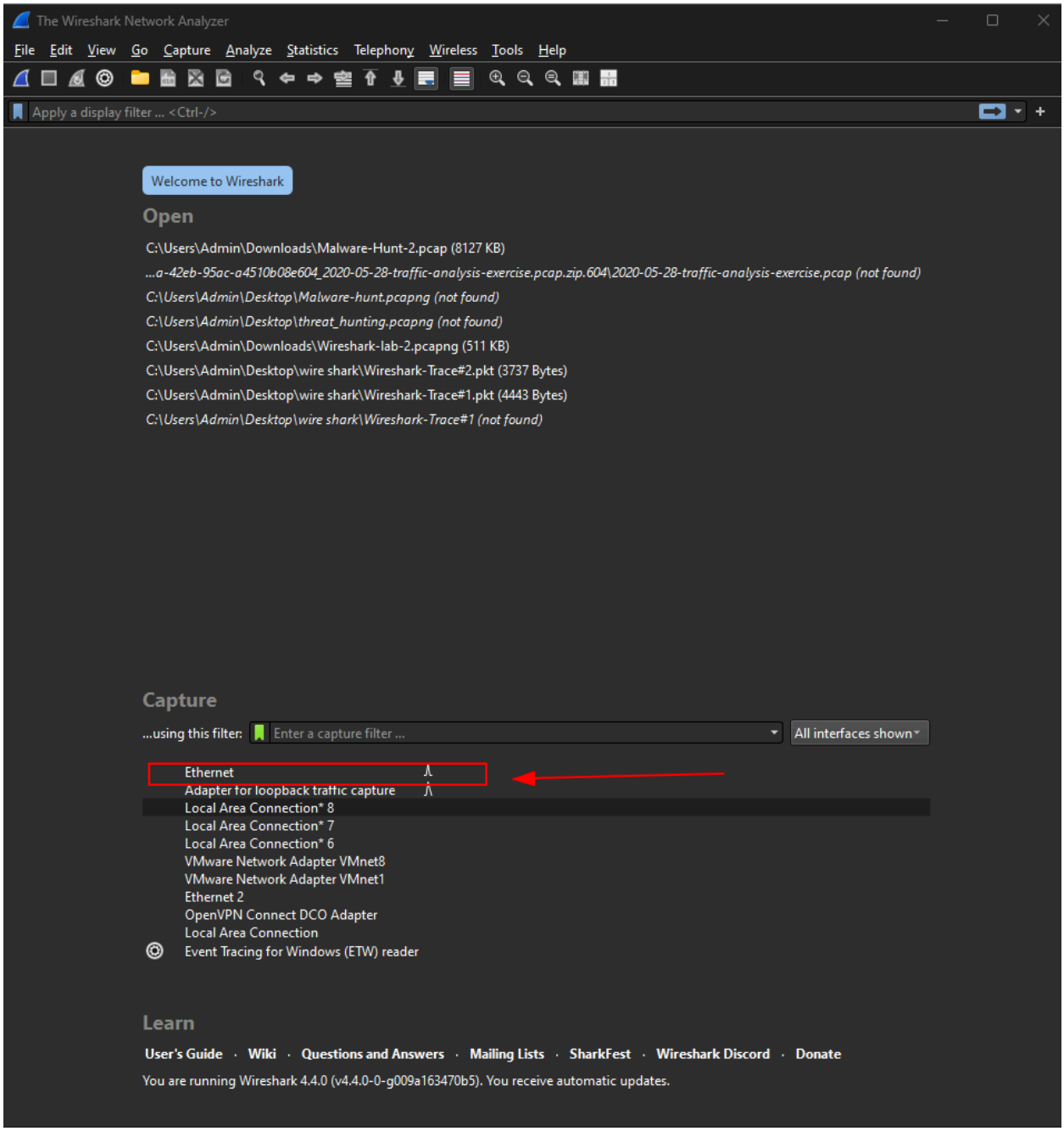
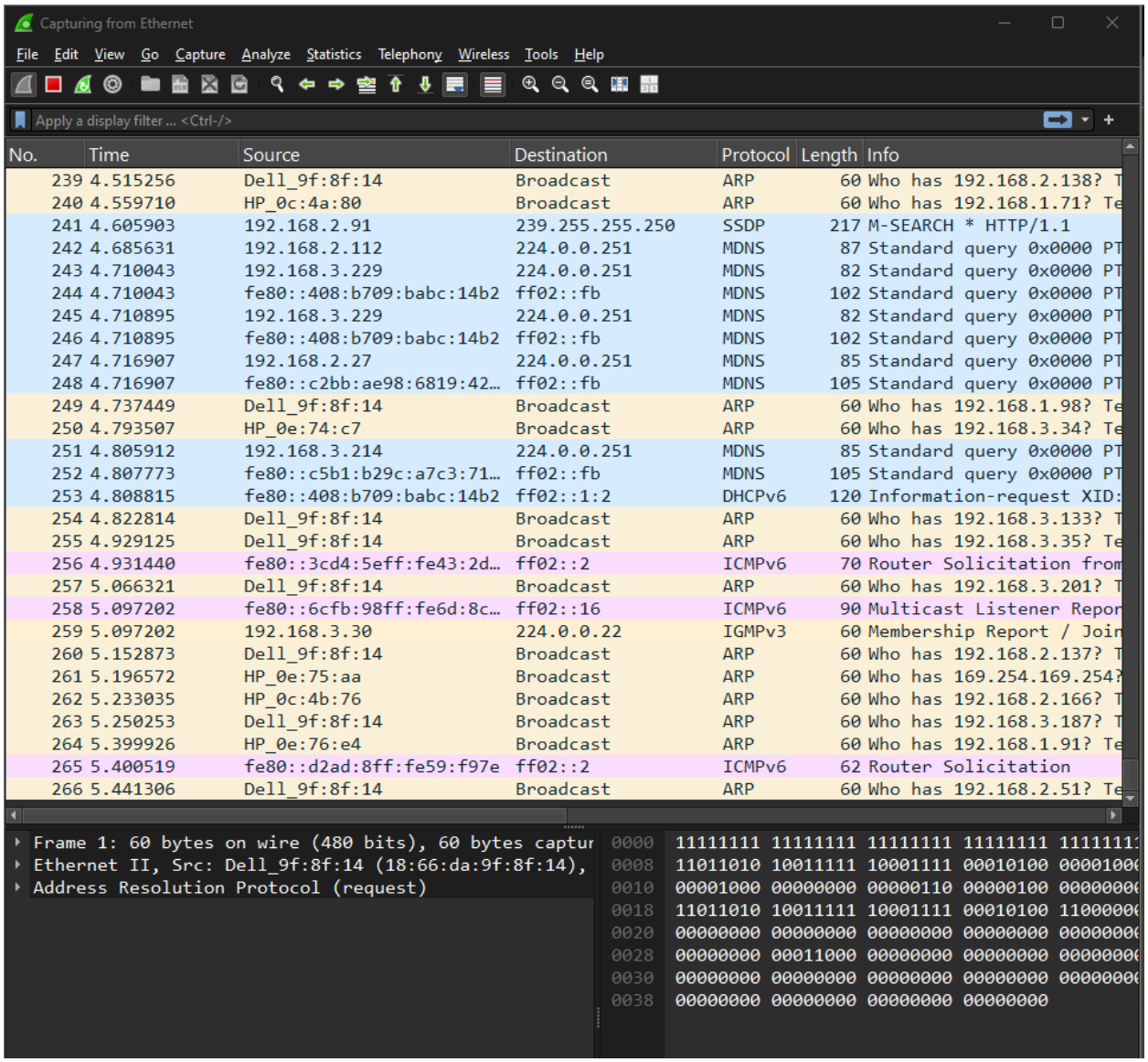
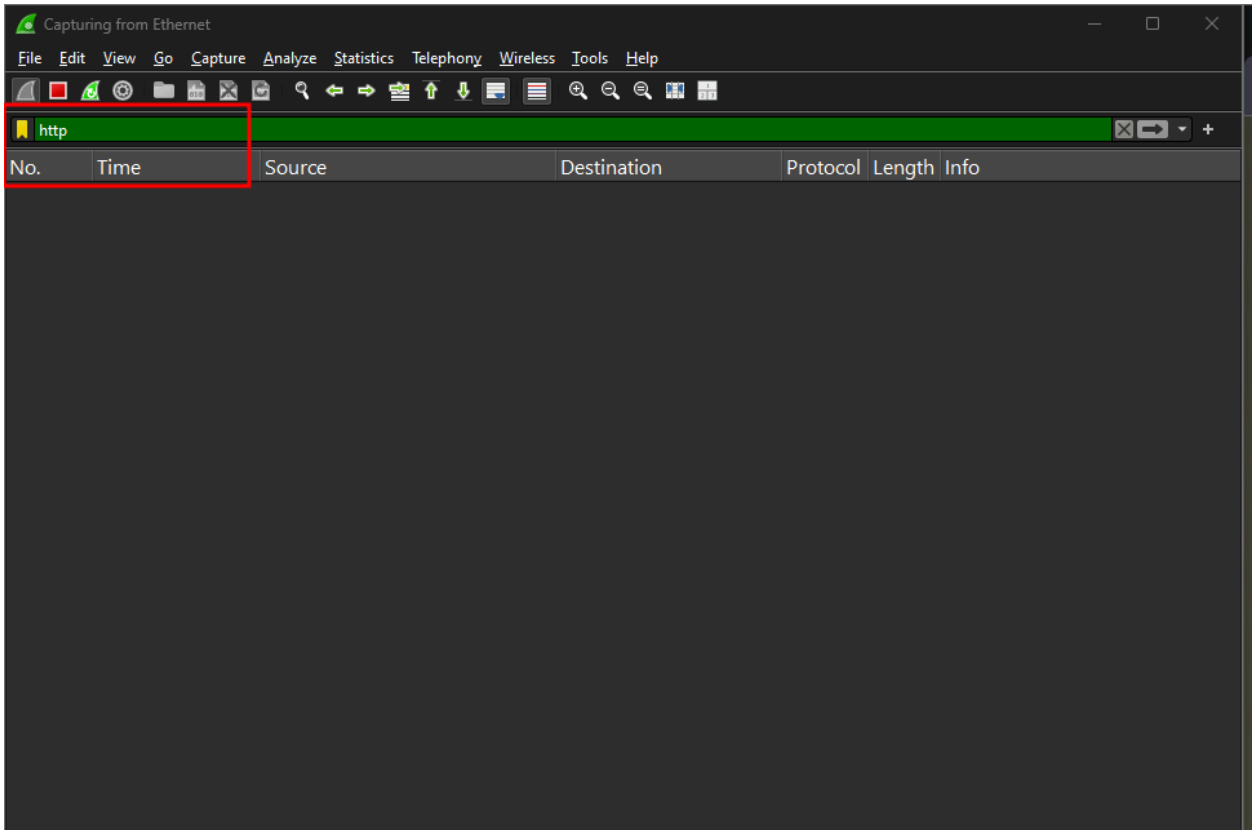
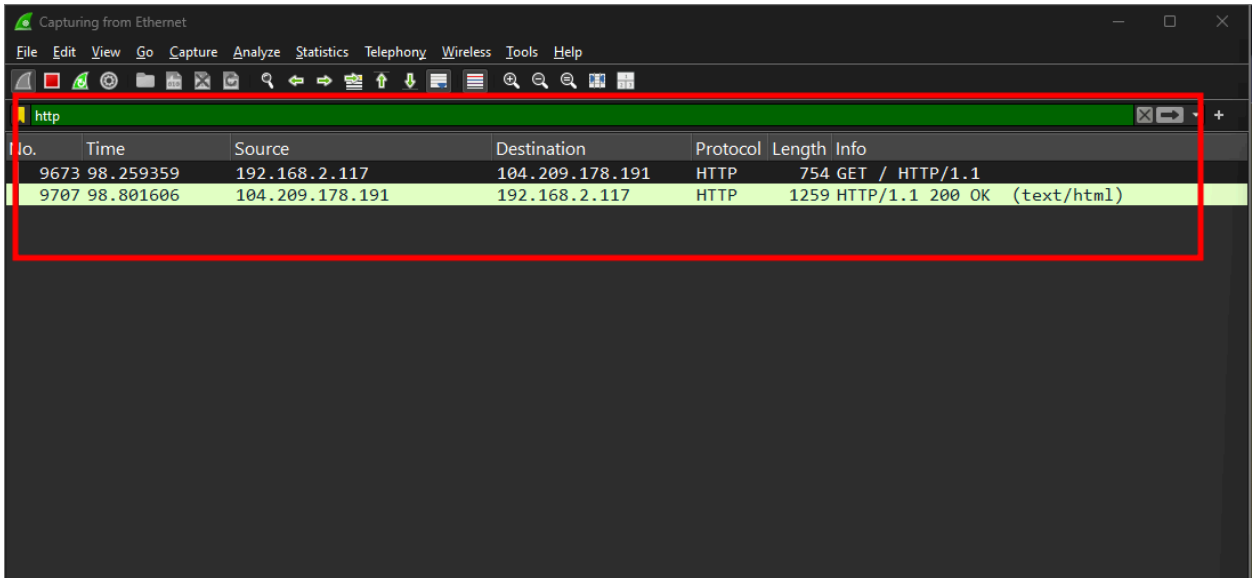
Name : Chetan Satone
Prn no. 008

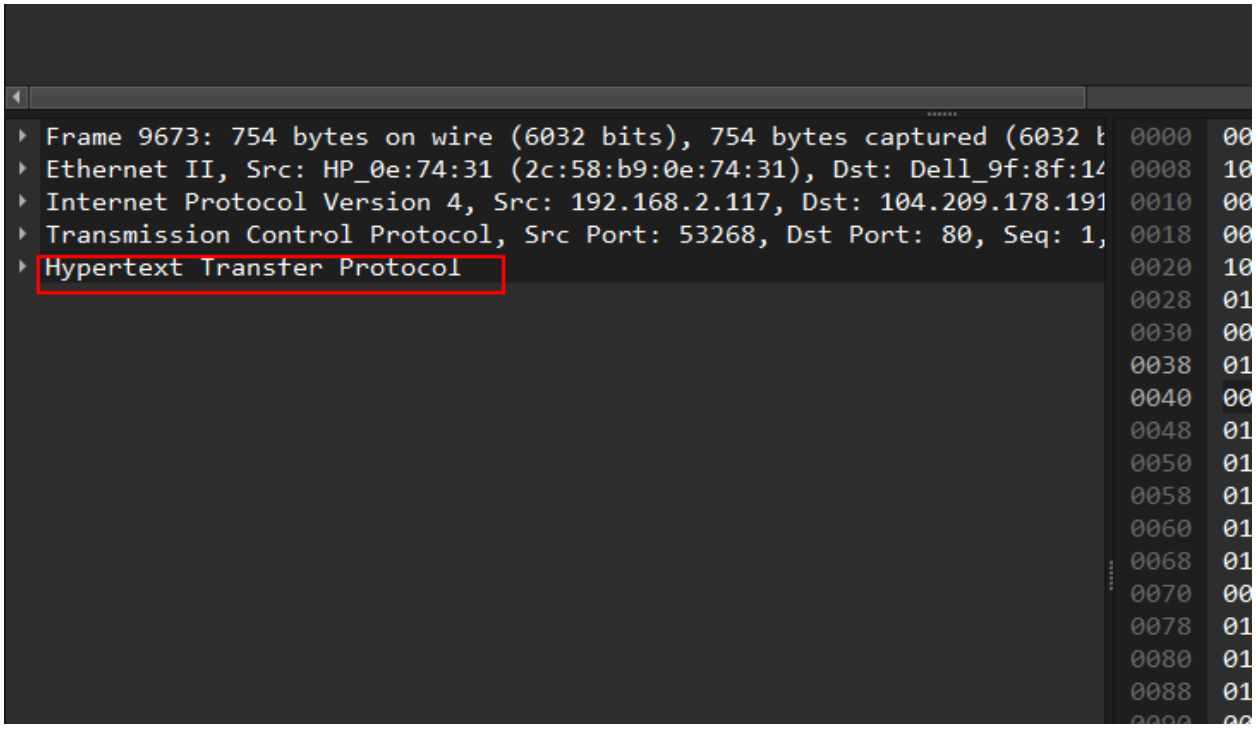


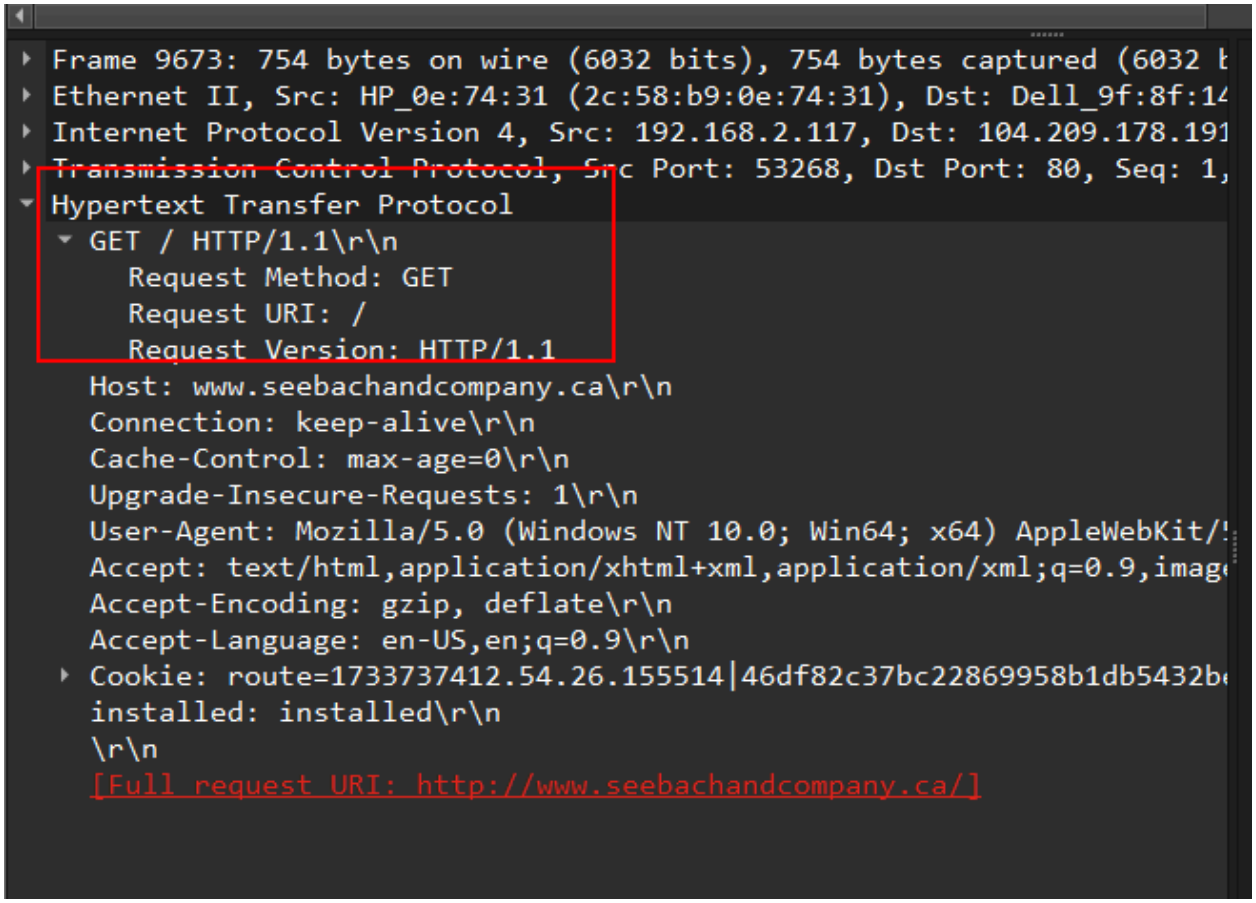

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
C:\Users\Admin\Downloads\Malware-Hunt-2.pcap (8127 KB)
...a-42eb-95ac-a4510b08e604_2020-05-28-traffic-analysis-exercise.pcap.zip.604\2020-05-28-traffic-analysis-exercise.pcap (not found)
C:\Users\Admin\Desktop\Malware-hunt.pcapng (not found)
C:\Users\Admin\Desktop\threat_hunting.pcapng (not found)
C:\Users\Admin\Downloads\Wireshark-lab-2.pcapng (511 KB)
C:\Users\Admin\Desktop\wire shark\Wireshark-Trace#2.pkt (3737 Bytes)
C:\Users\Admin\Desktop\wire shark\Wireshark-Trace#1.pkt (4443 Bytes)
C:\Users\Admin\Desktop\wire shark\Wireshark-Trace#1 (not found)
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Ethernet
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Ethernet 2
OpenVPN Connect DCO Adapter
Local Area Connection
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.0 (v4.4.0-0-g009a163470b5). You receive automatic updates.

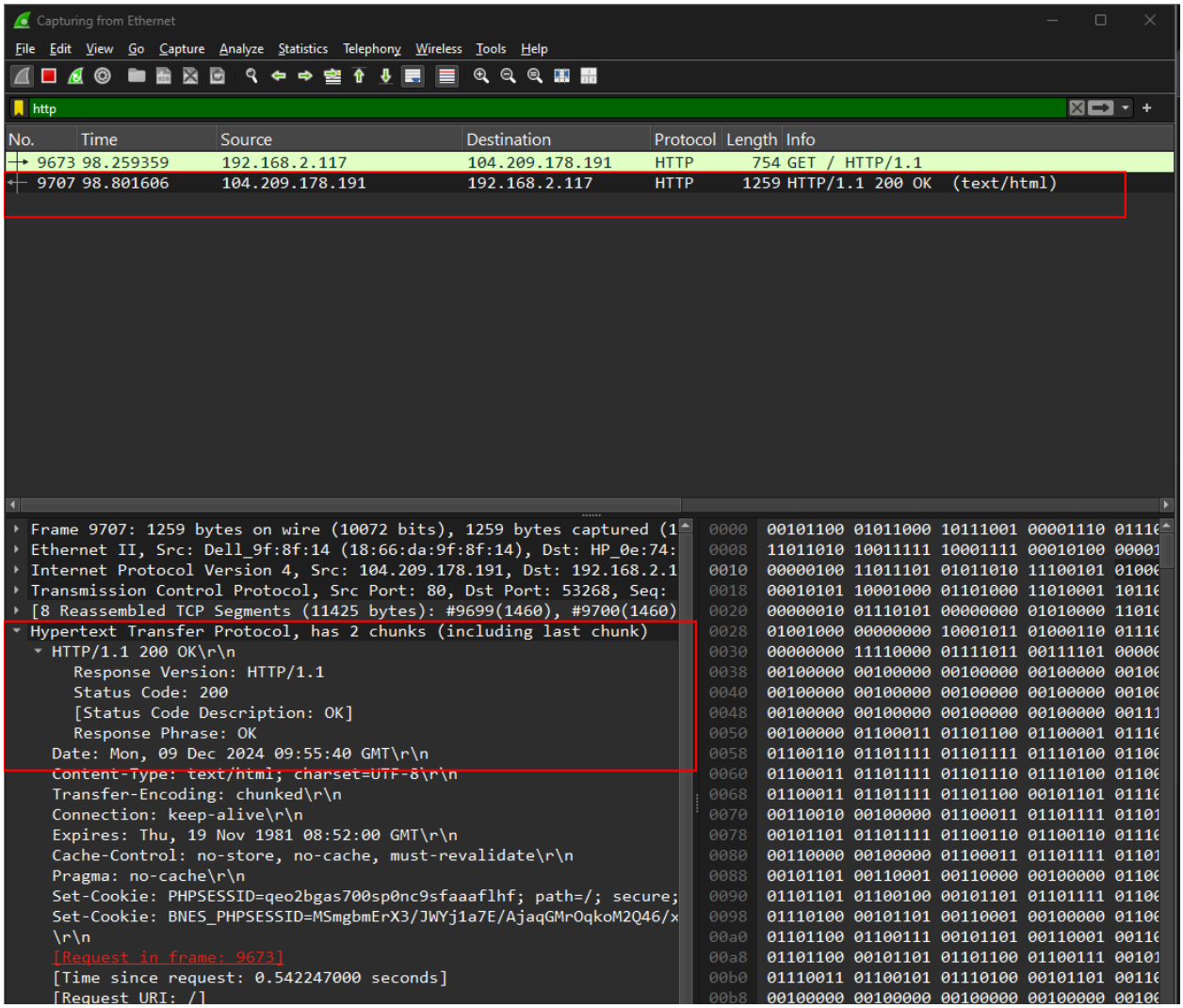

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
239 4.515256 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.2.138? T
240 4.559710 HP_0c:4a:80 Broadcast ARP 60 Who has 192.168.1.71? Te
241 4.605903 192.168.2.91 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
242 4.685631 192.168.2.112 224.0.0.251 MDNS 87 Standard query 0x0000 PT
243 4.710043 192.168.3.229 224.0.0.251 MDNS 82 Standard query 0x0000 PT
244 4.710043 fe80::408:b709:babc:14b2 ff02::fb MDNS 102 Standard query 0x0000 PT
245 4.710895 192.168.3.229 224.0.0.251 MDNS 82 Standard query 0x0000 PT
246 4.710895 fe80::408:b709:babc:14b2 ff02::fb MDNS 102 Standard query 0x0000 PT
247 4.716907 192.168.2.27 224.0.0.251 MDNS 85 Standard query 0x0000 PT
248 4.716907 fe80::c2bb:ae98:6819:42… ff02::fb MDNS 105 Standard query 0x0000 PT
249 4.737449 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.1.98? Te
250 4.793507 HP_0e:74:c7 Broadcast ARP 60 Who has 192.168.3.34? Te
251 4.805912 192.168.3.214 224.0.0.251 MDNS 85 Standard query 0x0000 PT
252 4.807773 fe80::c5b1:b29c:a7c3:71… ff02::fb MDNS 105 Standard query 0x0000 PT
253 4.808815 fe80::408:b709:babc:14b2 ff02::1:2 DHCPv6 120 Information-request XID:
254 4.822814 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.3.133? T
255 4.929125 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.3.35? Te
256 4.931440 fe80::3cd4:5eff:fe43:2d… ff02::2 ICMPv6 70 Router Solicitation from
257 5.066321 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.3.201? T
258 5.097202 fe80::6cfb:98ff:fe6d:8c… ff02::16 ICMPv6 90 Multicast Listener Repor
259 5.097202 192.168.3.30 224.0.0.22 IGMPv3 60 Membership Report / Join
260 5.152873 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.2.137? T
261 5.196572 HP_0e:75:aa Broadcast ARP 60 Who has 169.254.169.254?
262 5.233035 HP_0c:4b:76 Broadcast ARP 60 Who has 192.168.2.166? T
263 5.250253 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.3.187? T
264 5.399926 HP_0e:76:e4 Broadcast ARP 60 Who has 192.168.1.91? Te
265 5.400519 fe80::d2ad:8ff:fe59:f97e ff02::2 ICMPv6 62 Router Solicitation
266 5.441306 Dell_9f:8f:14 Broadcast ARP 60 Who has 192.168.2.51? Te
Frame 1: 60 bytes on wire (480 bits), 60 bytes captur
Ethernet II, Src: Dell_9f:8f:14 (18:66:da:9f:8f:14),
Address Resolution Protocol (request)
0000 11111111 11111111 11111111 11111111 1111111
0008 11011010 10011111 10001111 00010100 0000100
0010 00001000 00000000 00000110 00000100 0000000
0018 11011010 10011111 10001111 00010100 1100000
0020 00000000 00000000 00000000 00000000 0000000
0028 00000000 00011000 00000000 00000000 0000000
0030 00000000 00000000 00000000 00000000 0000000
0038 00000000 00000000 00000000 00000000

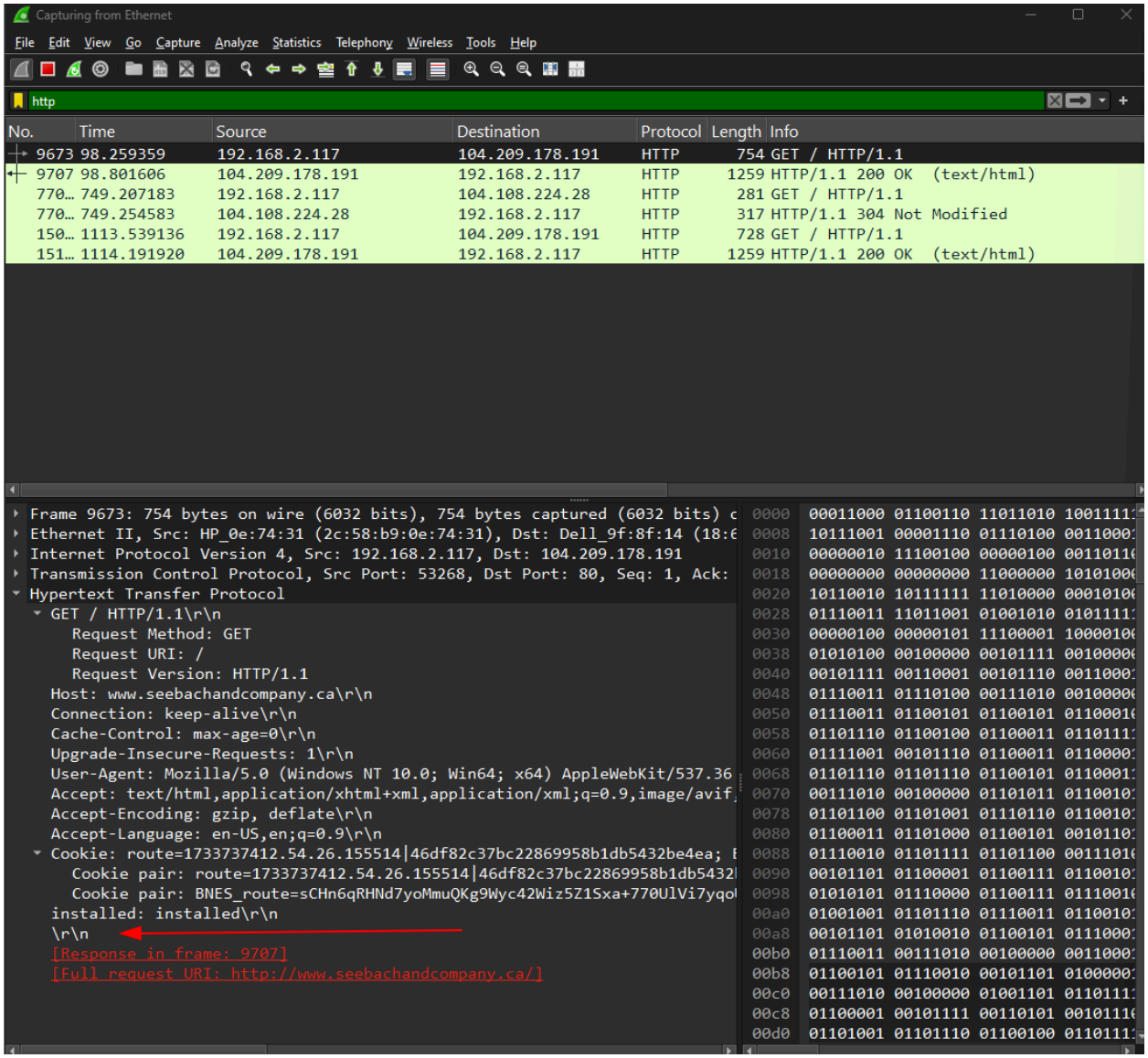

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info

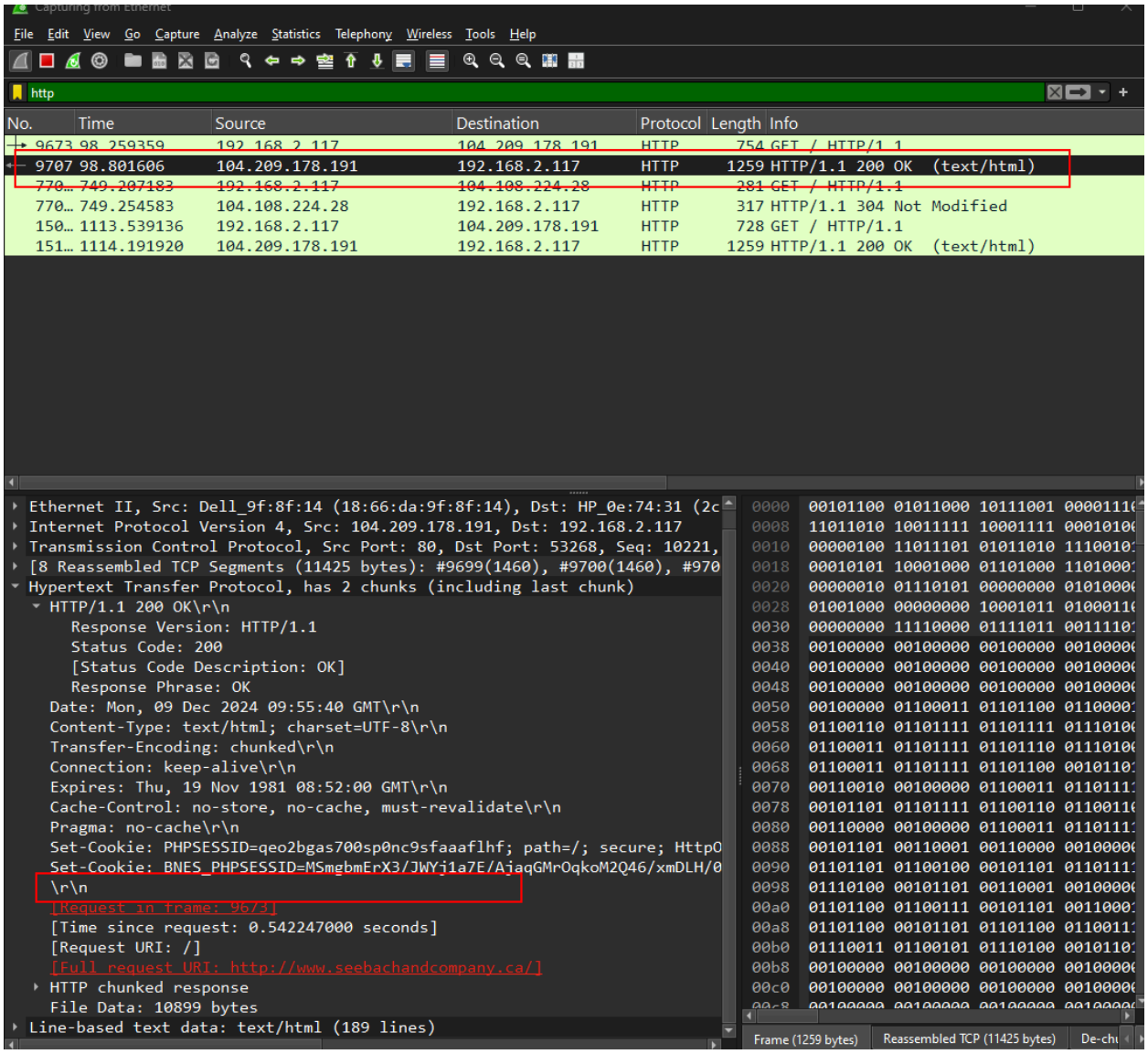

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9673 98.259359 192.168.2.117 104.209.178.191 HTTP 754 GET / HTTP/1.1
9707 98.801606 104.209.178.191 192.168.2.117 HTTP 1259 HTTP/1.1 200 OK (text/html)

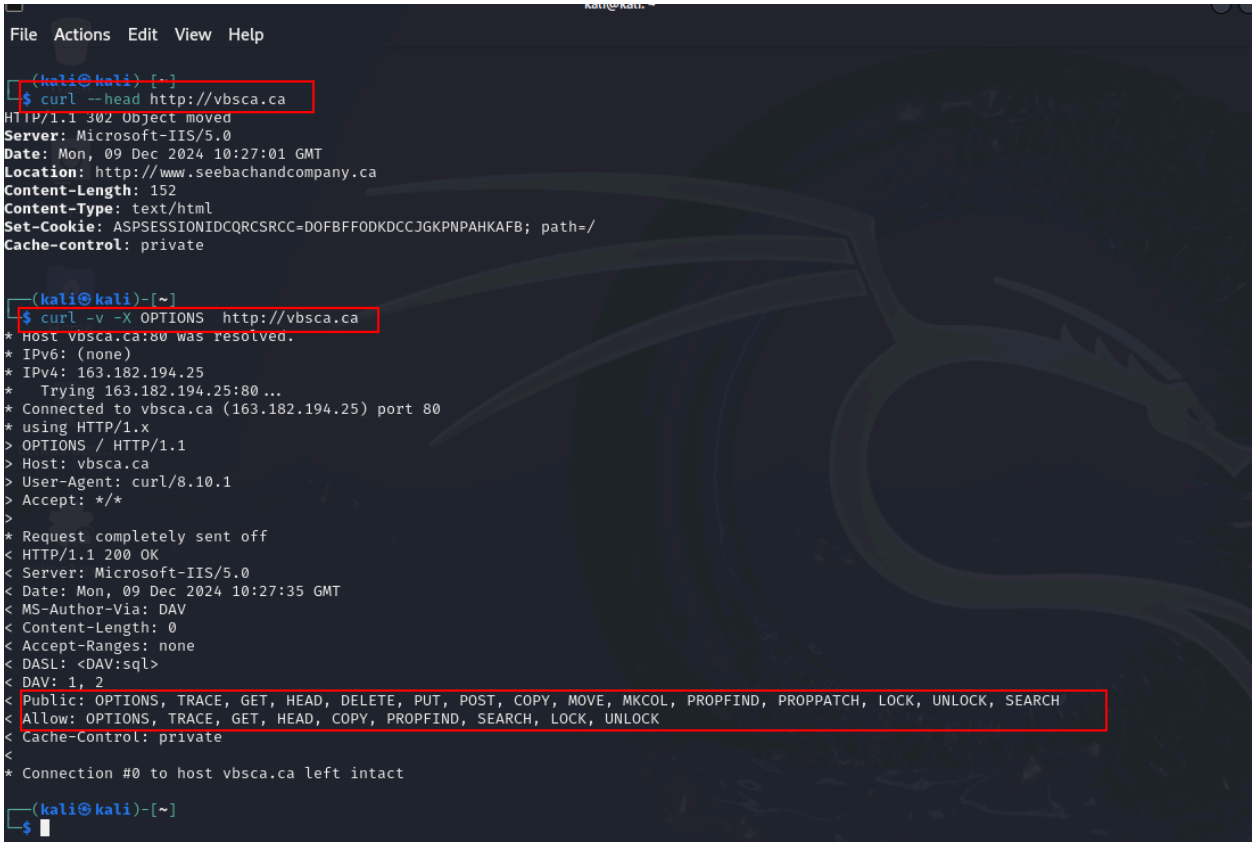

Frame 9673: 754 bytes on wire (6032 bits), 754 bytes captured (6032 b
Ethernet II, Src: HP_0e:74:31 (2c:58:b9:0e:74:31), Dst: Dell_9f:8f:14
Internet Protocol Version 4, Src: 192.168.2.117, Dst: 104.209.178.191
Transmission Control Protocol, Src Port: 53268, Dst Port: 80, Seq: 1,
Hypertext Transfer Protocol
0000 00
0008 10
0010 00
0018 00
0020 10
0028 01
0030 00
0038 01
0040 00
0048 01
0050 01
0058 01
0060 01
0068 01
0070 00
0078 01
0080 01
0088 01

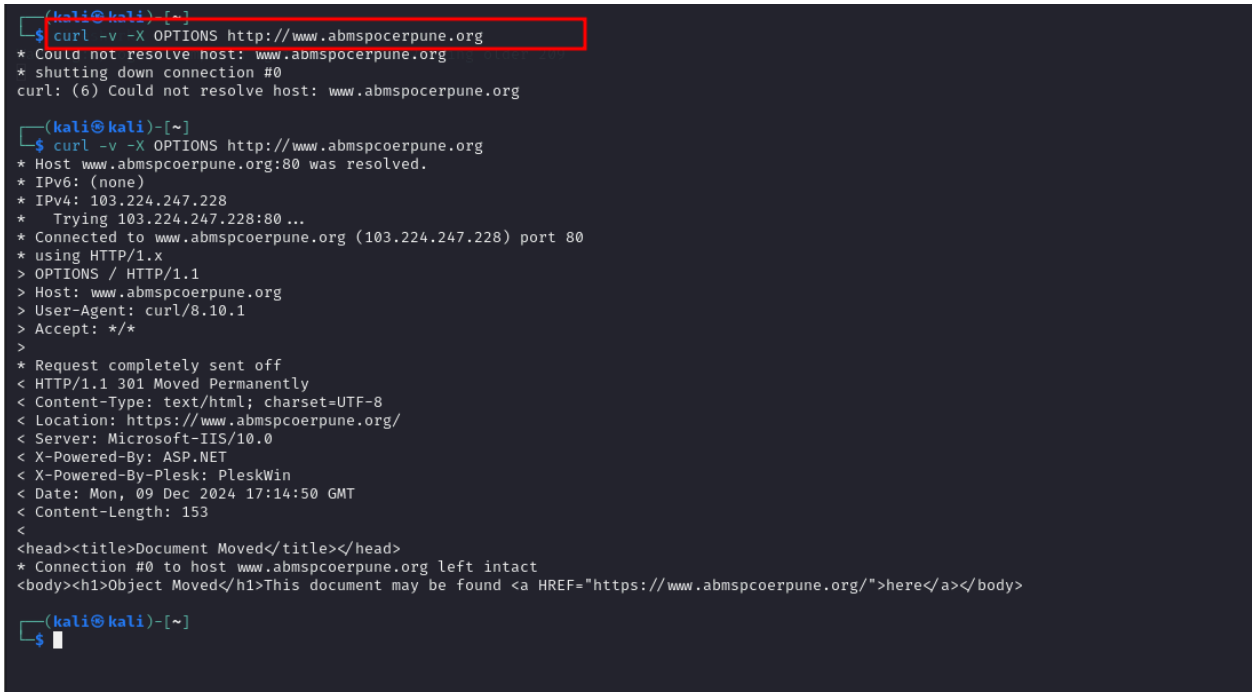

Frame 9673: 754 bytes on wire (6032 bits), 754 bytes captured (6032 b
Ethernet II, Src: HP_0e:74:31 (2c:58:b9:0e:74:31), Dst: Dell_9f:8f:14
Internet Protocol Version 4, Src: 192.168.2.117, Dst: 104.209.178.191
Transmission Control Protocol, Src Port: 53268, Dst Port: 80, Seq: 1,
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: www.seebachandcompany.ca\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Cookie: route=1733737412.54.26.155514|46df82c37bc22869958b1db5432b
installed: installed\r\n
\r\n
[Full request URI: http://www.seebachandcompany.ca/]


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9673 98.259359 192.168.2.117 104.209.178.191 HTTP 754 GET / HTTP/1.1
9707 98.801606 104.209.178.191 192.168.2.117 HTTP 1259 HTTP/1.1 200 OK (text/html)
Frame 9707: 1259 bytes on wire (10072 bits), 1259 bytes captured (1
Ethernet II, Src: Dell_9f:8f:14 (18:66:da:9f:8f:14), Dst: HP_0e:74:
Internet Protocol Version 4, Src: 104.209.178.191, Dst: 192.168.2.1
Transmission Control Protocol, Src Port: 80, Dst Port: 53268, Seq:
[8 Reassembled TCP Segments (11425 bytes): #9699(1460), #9700(1460)
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
HTTP/1.1 200 OK\r\n
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Mon, 09 Dec 2024 09:55:40 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate\r\n
Pragma: no-cache\r\n
Set-Cookie: PHPSESSID=qeo2bgas700sp0nc9sfaaaflhf; path=/; secure;
Set-Cookie: BNES_PHPSESSID=MSmgbmErX3/JWYj1a7E/AjaqGMrOqkoM2Q46/x
\r\n
[Request in frame: 9673]
[Time since request: 0.542247000 seconds]
[Request URI: /]
0000 00101100 01011000 10111001 00001110 0111
0008 11011010 10011111 10001111 00010100 0000
0010 00000100 11011101 01011010 11100101 0100
0018 00010101 10001000 01101000 11010001 1011
0020 00000010 01110101 00000000 01010000 1101
0028 01001000 00000000 10001011 01000110 0111
0030 00000000 11110000 01111011 00111101 0000
0038 00100000 00100000 00100000 00100000 0010
0040 00100000 00100000 00100000 00100000 0010
0048 00100000 00100000 00100000 00100000 0011
0050 00100000 01100011 01101100 01100001 0111
0058 01100110 01101111 01101111 01110100 0110
0060 01100011 01101111 01101110 01110100 0110
0068 01100011 01101111 01101100 00101101 0111
0070 00110010 00100000 01100011 01101111 0110
0078 00101101 01101111 01100110 01100110 0111
0080 00110000 00100000 01100011 01101111 0110
0088 00101101 00110001 00110000 00100000 0110
0090 01101101 01100100 00101101 01101111 0110
0098 01110100 00101101 00110001 00100000 0110
00a0 01101100 01100111 00101101 00110001 0011
00a8 01101100 00101101 01101100 01100111 0010
00b0 01110011 01100101 01110100 00101101 0011
00b8 00100000 00100000 00100000 00100000 0010


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9673 98.259359 192.168.2.117 104.209.178.191 HTTP 754 GET / HTTP/1.1
9707 98.801606 104.209.178.191 192.168.2.117 HTTP 1259 HTTP/1.1 200 OK (text/html)
770… 749.207183 192.168.2.117 104.108.224.28 HTTP 281 GET / HTTP/1.1
770… 749.254583 104.108.224.28 192.168.2.117 HTTP 317 HTTP/1.1 304 Not Modified
150… 1113.539136 192.168.2.117 104.209.178.191 HTTP 728 GET / HTTP/1.1
151… 1114.191920 104.209.178.191 192.168.2.117 HTTP 1259 HTTP/1.1 200 OK (text/html)
Frame 9673: 754 bytes on wire (6032 bits), 754 bytes captured (6032 bits) c
Ethernet II, Src: HP_0e:74:31 (2c:58:b9:0e:74:31), Dst: Dell_9f:8f:14 (18:6
Internet Protocol Version 4, Src: 192.168.2.117, Dst: 104.209.178.191
Transmission Control Protocol, Src Port: 53268, Dst Port: 80, Seq: 1, Ack:
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: www.seebachandcompany.ca\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Cookie: route=1733737412.54.26.155514|46df82c37bc22869958b1db5432be4ea; B
Cookie pair: route=1733737412.54.26.155514|46df82c37bc22869958b1db5432
Cookie pair: BNES_route=sCHn6qRHNd7yoMmuQKg9Wyc42Wiz5Z1Sxa+770UlVi7yqo
installed: installed\r\n
\r\n
[Response in frame: 9707]
[Full request URI: http://www.seebachandcompany.ca/]
0000 00011000 01100110 11011010 1001111
0008 10111001 00001110 01110100 0011000
0010 00000010 11100100 00000100 0011011
0018 00000000 00000000 11000000 1010100
0020 10110010 10111111 11010000 0001010
0028 01110011 11011001 01001010 0101111
0030 00000100 00000101 11100001 1000010
0038 01010100 00100000 00101111 0010000
0040 00101111 00110001 00101110 0011000
0048 01110011 01110100 00111010 0010000
0050 01110011 01100101 01100101 0110001
0058 01101110 01100100 01100011 0110111
0060 01111001 00101110 01100011 0110000
0068 01101110 01101110 01100101 0110001
0070 00111010 00100000 01101011 0110101
0078 01101100 01101001 01110110 0110101
0080 01100011 01101000 01100101 0010110
0088 01110010 01101111 01101100 0011101
0090 00101101 01100001 01100111 0110101
0098 01010101 01110000 01100111 0111001
00a0 01001001 01101110 01110011 0110101
00a8 00101101 01010010 01100101 0111000
00b0 01110011 00111010 00100000 0011000
00b8 01100101 01110010 00101101 0100000
00c0 00111010 00100000 01001101 0110111
00c8 01100001 00101111 00110101 0010111
00d0 01101001 01101110 01100100 0110111


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
9673 98.259359 192.168.2.117 104.209.178.191 HTTP 754 GET / HTTP/1.1
9707 98.801606 104.209.178.191 192.168.2.117 HTTP 1259 HTTP/1.1 200 OK (text/html)
770… 749.207183 192.168.2.117 104.108.224.28 HTTP 281 GET / HTTP/1.1
770… 749.254583 104.108.224.28 192.168.2.117 HTTP 317 HTTP/1.1 304 Not Modified
150… 1113.539136 192.168.2.117 104.209.178.191 HTTP 728 GET / HTTP/1.1
151… 1114.191920 104.209.178.191 192.168.2.117 HTTP 1259 HTTP/1.1 200 OK (text/html)
Ethernet II, Src: Dell_9f:8f:14 (18:66:da:9f:8f:14), Dst: HP_0e:74:31 (2c
Internet Protocol Version 4, Src: 104.209.178.191, Dst: 192.168.2.117
Transmission Control Protocol, Src Port: 80, Dst Port: 53268, Seq: 10221,
[8 Reassembled TCP Segments (11425 bytes): #9699(1460), #9700(1460), #970
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
HTTP/1.1 200 OK\r\n
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Mon, 09 Dec 2024 09:55:40 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate\r\n
Pragma: no-cache\r\n
Set-Cookie: PHPSESSID=qeo2bgas700sp0nc9sfaaaflhf; path=/; secure; HttpO
Set-Cookie: BNES_PHPSESSID=MSmgbmErX3/JWYj1a7E/AjaqGMrOqkoM2Q46/xmDLH/0
\r\n
[Request in frame: 9673]
[Time since request: 0.542247000 seconds]
[Request URI: /]
[Full request URI: http://www.seebachandcompany.ca/]
HTTP chunked response
File Data: 10899 bytes
Line-based text data: text/html (189 lines)
0000 00101100 01011000 10111001 00001110
0008 11011010 10011111 10001111 00010100
0010 00000100 11011101 01011010 11100101
0018 00010101 10001000 01101000 11010001
0020 00000010 01110101 00000000 01010000
0028 01001000 00000000 10001011 01000110
0030 00000000 11110000 01111011 00111101
0038 00100000 00100000 00100000 00100000
0040 00100000 00100000 00100000 00100000
0048 00100000 00100000 00100000 00100000
0050 00100000 01100011 01101100 01100001
0058 01100110 01101111 01101111 01110100
0060 01100011 01101111 01101110 01110100
0068 01100011 01101111 01101100 00101101
0070 00110010 00100000 01100011 01101111
0078 00101101 01101111 01100110 01100110
0080 00110000 00100000 01100011 01101111
0088 00101101 00110001 00110000 00100000
0090 01101101 01100100 00101101 01101111
0098 01110100 00101101 00110001 00100000
00a0 01101100 01100111 00101101 00110001
00a8 01101100 00101101 01101100 01100111
00b0 01110011 01100101 01110100 00101101
00b8 00100000 00100000 00100000 00100000
00c0 00100000 00100000 00100000 00100000
Frame (1259 bytes)
Reassembled TCP (11425 bytes)


File Actions Edit View Help
(kali㉿kali) [~]
$ curl --head http://vbsca.ca
HTTP/1.1 302 Object moved
Server: Microsoft-IIS/5.0
Date: Mon, 09 Dec 2024 10:27:01 GMT
Location: http://www.seebachandcompany.ca
Content-Length: 152
Content-Type: text/html
Set-Cookie: ASPSESSIONIDCQRCSRCC=DOFBFFODKDCCJGKPNPAHKAFB; path=/
Cache-control: private
(kali㉿kali)-[~]
$ curl -v -X OPTIONS http://vbsca.ca
* Host vbsca.ca:80 was resolved.
* IPv6: (none)
* IPv4: 163.182.194.25
* Trying 163.182.194.25:80 ...
* Connected to vbsca.ca (163.182.194.25) port 80
* using HTTP/1.x
> OPTIONS / HTTP/1.1
> Host: vbsca.ca
> User-Agent: curl/8.10.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Server: Microsoft-IIS/5.0
< Date: Mon, 09 Dec 2024 10:27:35 GMT
< MS-Author-Via: DAV
< Content-Length: 0
< Accept-Ranges: none
< DASL: <DAV:sql>
< DAV: 1, 2
< Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
< Allow: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
< Cache-Control: private
<
* Connection #0 to host vbsca.ca left intact
(kali㉿kali)-[~]
$


┌──(kali㉿kali)-[~]
└─$ curl -v -X OPTIONS http://www.abmspocerpune.org
* Could not resolve host: www.abmspocerpune.org
* shutting down connection #0
curl: (6) Could not resolve host: www.abmspocerpune.org
┌──(kali㉿kali)-[~]
└─$ curl -v -X OPTIONS http://www.abmspcoerpune.org
* Host www.abmspcoerpune.org:80 was resolved.
* IPv6: (none)
* IPv4: 103.224.247.228
*   Trying 103.224.247.228:80 ...
* Connected to www.abmspcoerpune.org (103.224.247.228) port 80
* using HTTP/1.x
> OPTIONS / HTTP/1.1
> Host: www.abmspcoerpune.org
> User-Agent: curl/8.10.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 301 Moved Permanently
< Content-Type: text/html; charset=UTF-8
< Location: https://www.abmspcoerpune.org/
< Server: Microsoft-IIS/10.0
< X-Powered-By: ASP.NET
< X-Powered-By-Plesk: PleskWin
< Date: Mon, 09 Dec 2024 17:14:50 GMT
< Content-Length: 153
<
<head><title>Document Moved</title></head>
* Connection #0 to host www.abmspcoerpune.org left intact
<body><h1>Object Moved</h1>This document may be found <a HREF="https://www.abmspcoerpune.org/">here</body>
┌──(kali㉿kali)-[~]
└─$