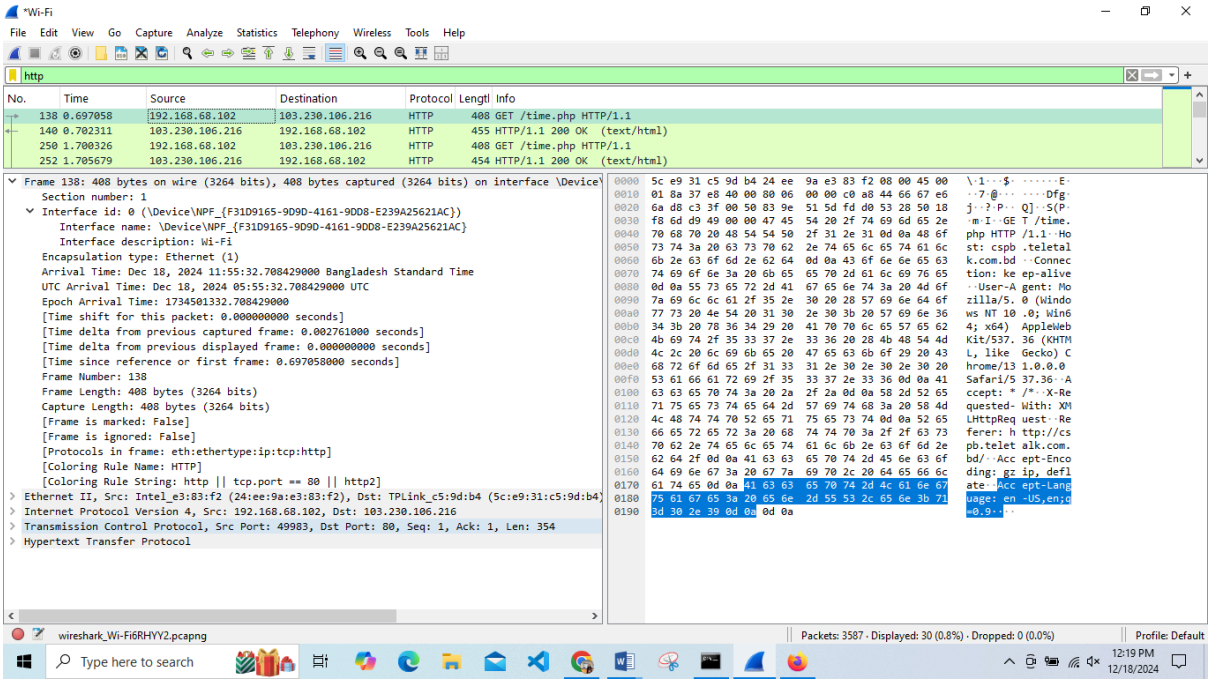
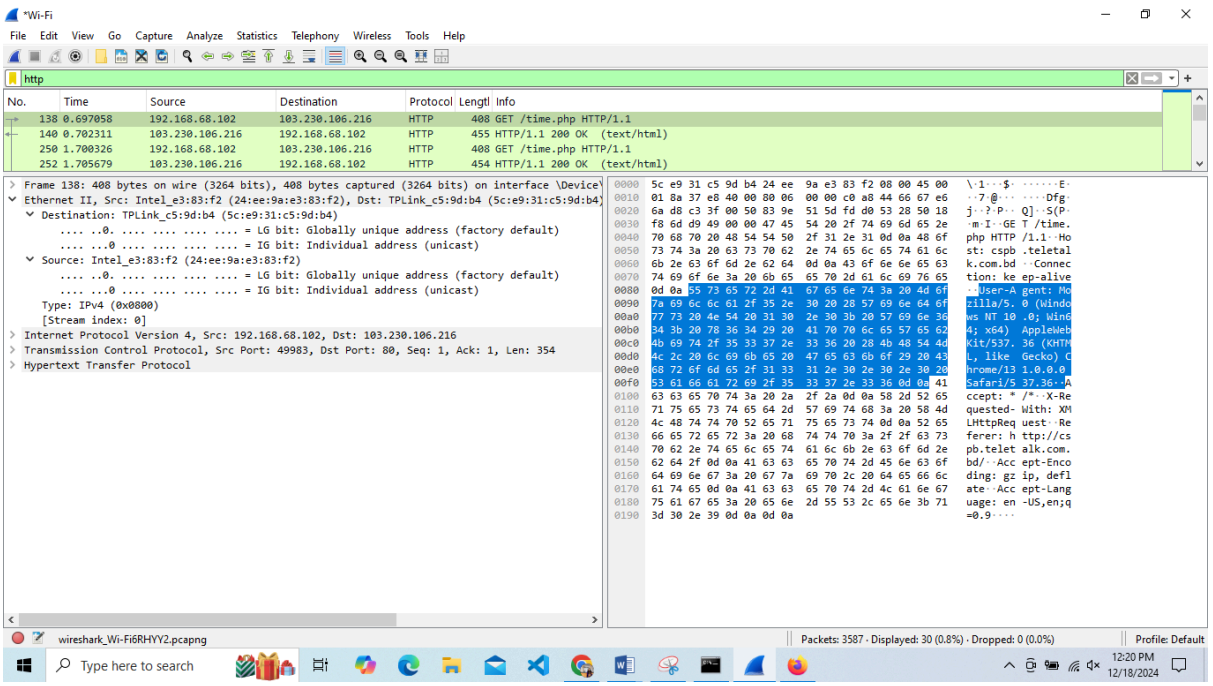
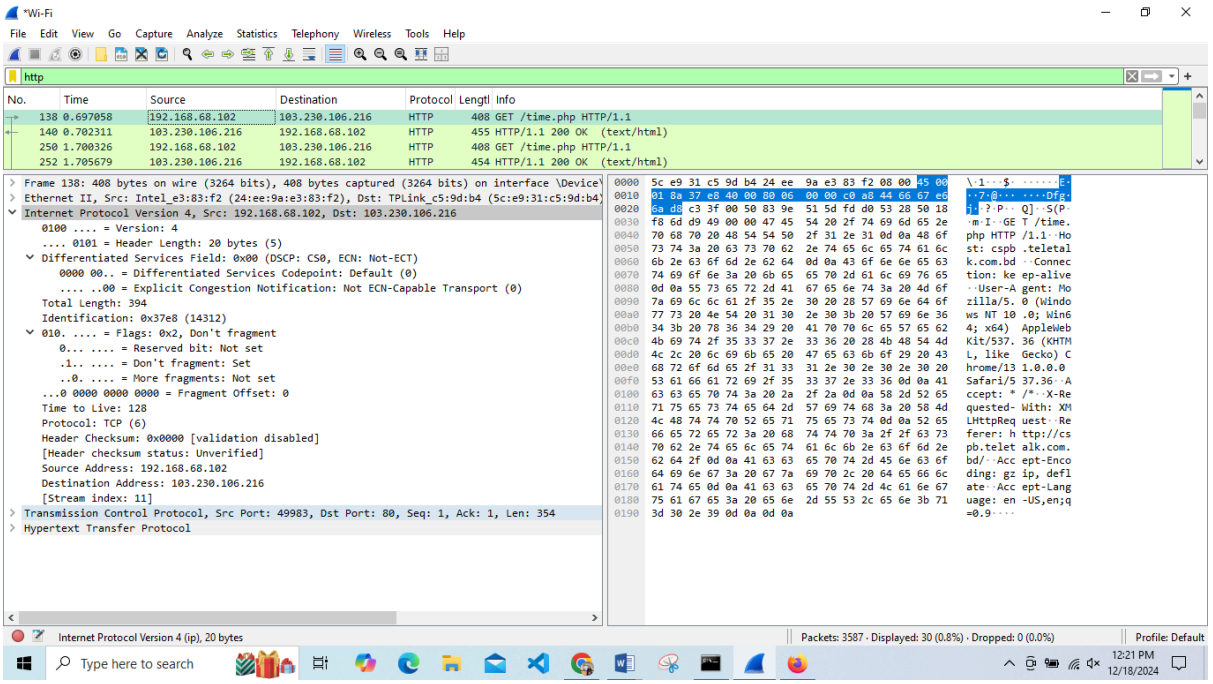
Request get:

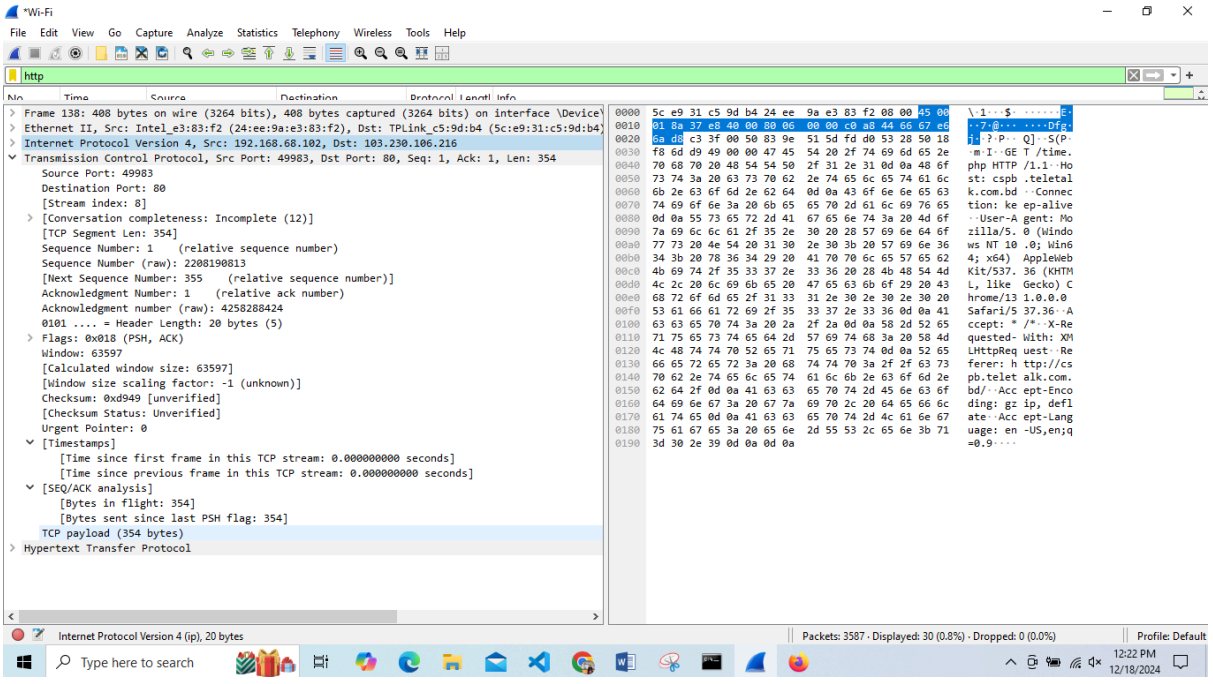
Source IP: 192.168.68.102

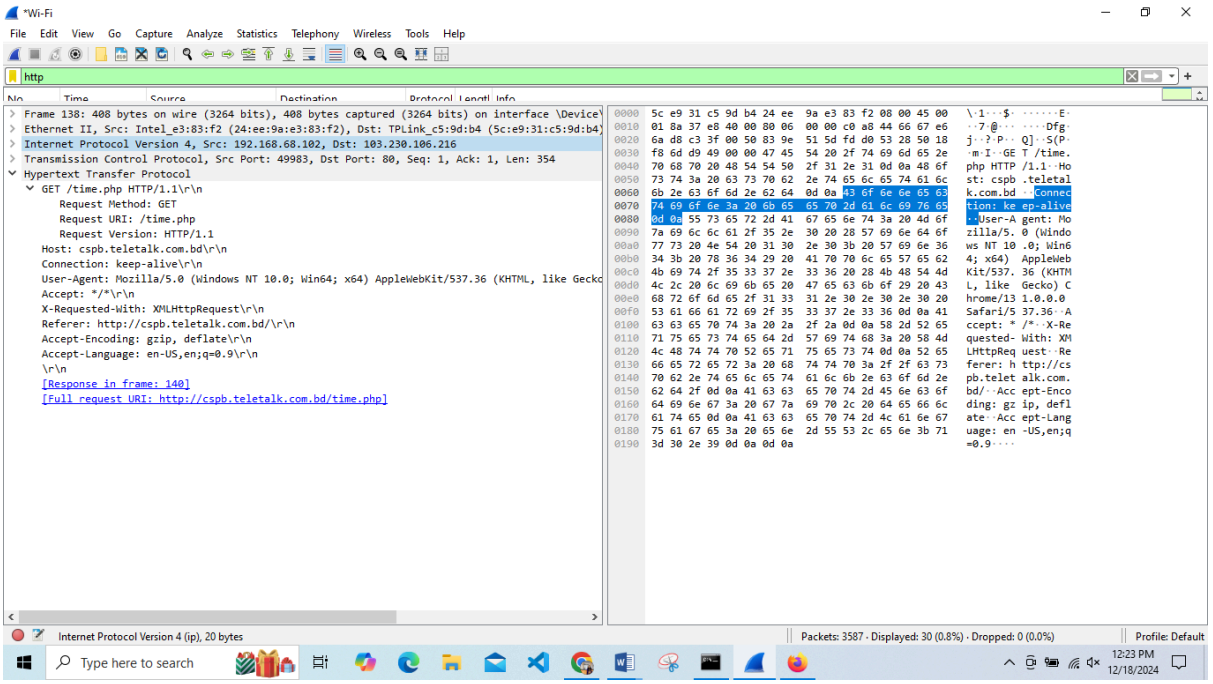
Destination IP: 103.230.106.216



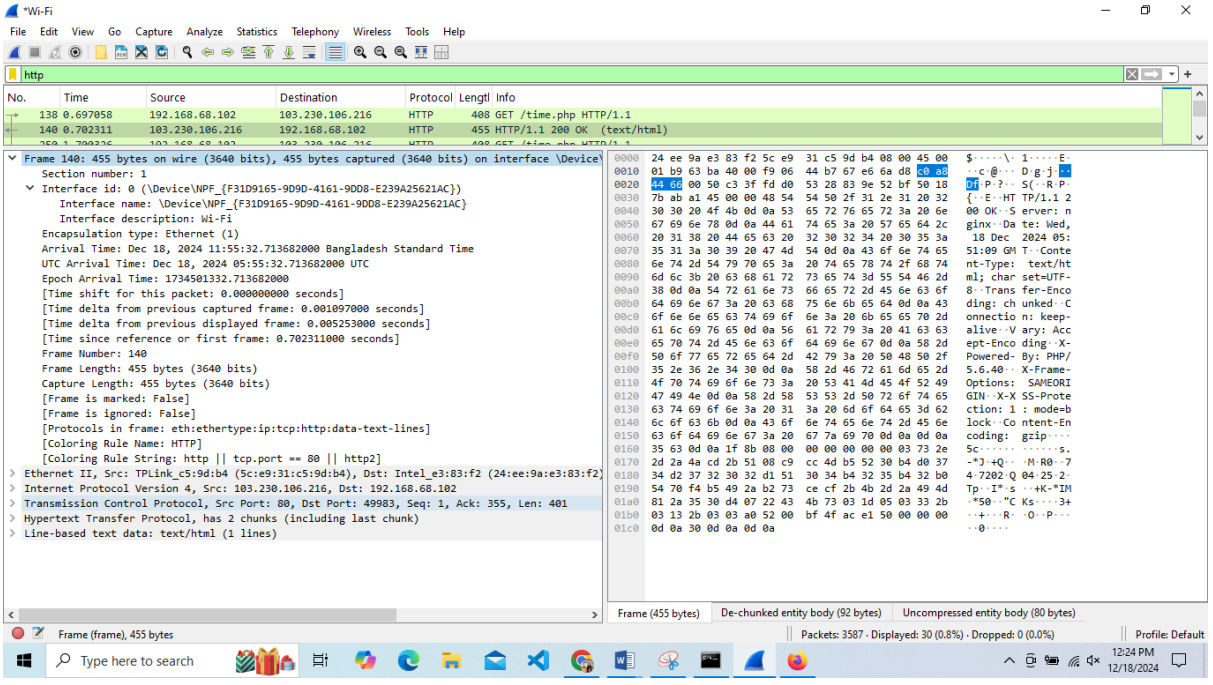


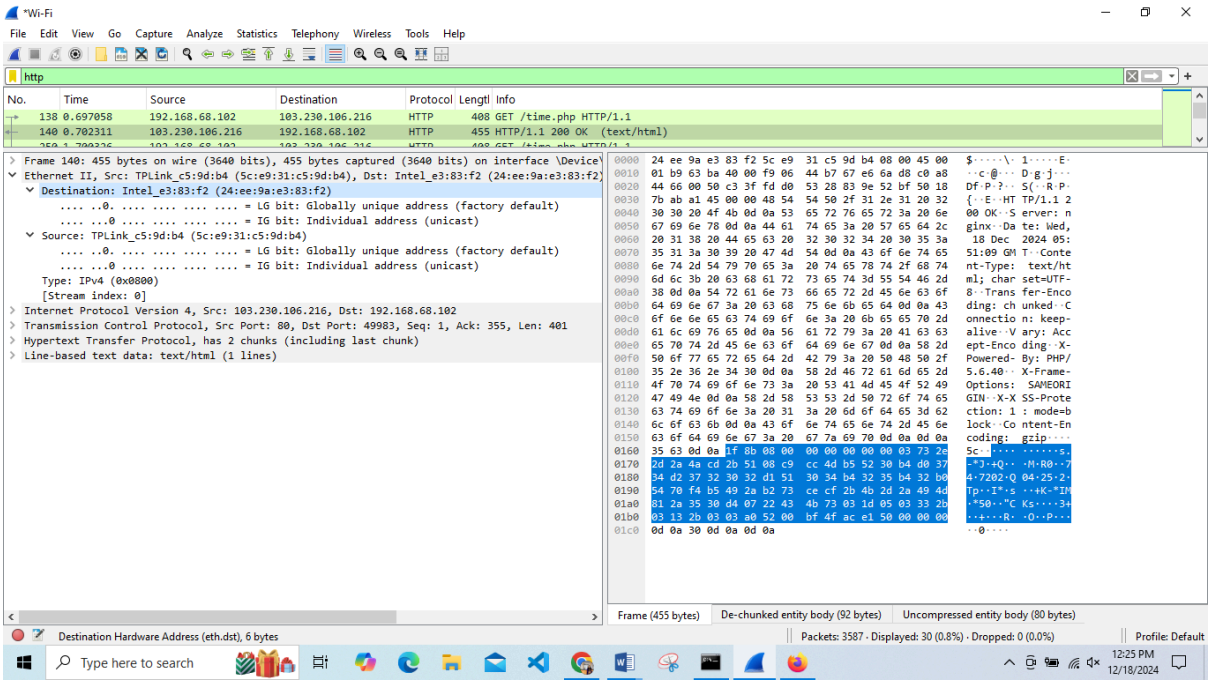

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengtl Info
138 0.697058 192.168.68.102 103.230.106.216 HTTP 408 GET /time.php HTTP/1.1
140 0.702311 103.230.106.216 192.168.68.102 HTTP 455 HTTP/1.1 200 OK (text/html)
250 1.700326 192.168.68.102 103.230.106.216 HTTP 408 GET /time.php HTTP/1.1
252 1.705679 103.230.106.216 192.168.68.102 HTTP 454 HTTP/1.1 200 OK (text/html)
Frame 138: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface \Device\
Ethernet II, Src: Intel_e3:83:f2 (24:ee:9a:e3:83:f2), Dst: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4)
Internet Protocol Version 4, Src: 192.168.68.102, Dst: 103.230.106.216
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 394
Identification: 0x37e8 (14312)
010. .... = Flags: 0x2, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...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: 192.168.68.102
Destination Address: 103.230.106.216
[Stream index: 11]
Transmission Control Protocol, Src Port: 49983, Dst Port: 80, Seq: 1, Ack: 1, Len: 354
Hypertext Transfer Protocol
0000 5c e9 31 c5 9d b4 24 ee 9a e3 83 f2 08 00 45 00 \·1···$· ·····E·
0010 01 8a 37 e8 40 00 80 06 00 00 c0 a8 44 66 67 e6 ··7·@··· ····Dfg·
0020 6a d8 c3 3f 00 50 83 9e 51 5d fd d0 53 28 50 18 j··?·P·· Q]··S(P·
0030 f8 6d d9 49 00 00 47 45 54 20 2f 74 69 6d 65 2e ·m·I··GE T /time.
0040 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f php HTTP /1.1··Ho
0050 73 74 3a 20 63 73 70 62 2e 74 65 6c 65 74 61 6c st: cspb .teletal
0060 6b 2e 63 6f 6d 2e 62 64 0d 0a 43 6f 6e 6e 65 63 k.com.bd ··Connec
0070 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
0080 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ··User-A gent: Mo
0090 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo
00a0 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 ws NT 10 .0; Win6
00b0 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4; x64) AppleWeb
00c0 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d Kit/537. 36 (KHTM
00d0 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 L, like Gecko) C
00e0 68 72 6f 6d 65 2f 31 33 31 2e 30 2e 30 2e 30 20 hrome/13 1.0.0.0
00f0 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36··A
0100 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 58 2d 52 65 ccept: * /*··X-Re
0110 71 75 65 73 74 65 64 2d 57 69 74 68 3a 20 58 4d quested- With: XM
0120 4c 48 74 74 70 52 65 71 75 65 73 74 0d 0a 52 65 LHttpReq uest··Re
0130 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 63 73 ferer: h ttp://cs
0140 70 62 2e 74 65 6c 65 74 61 6c 6b 2e 63 6f 6d 2e pb.telet alk.com.
0150 62 64 2f 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f bd/··Acc ept-Enco
0160 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
0170 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 ate··Acc ept-Lang
0180 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 uage: en -US,en;q
0190 3d 30 2e 39 0d 0a 0d 0a =0.9····
Internet Protocol Version 4 (ip), 20 bytes
Packets: 3587 · Displayed: 30 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
12:21 PM
12/18/2024

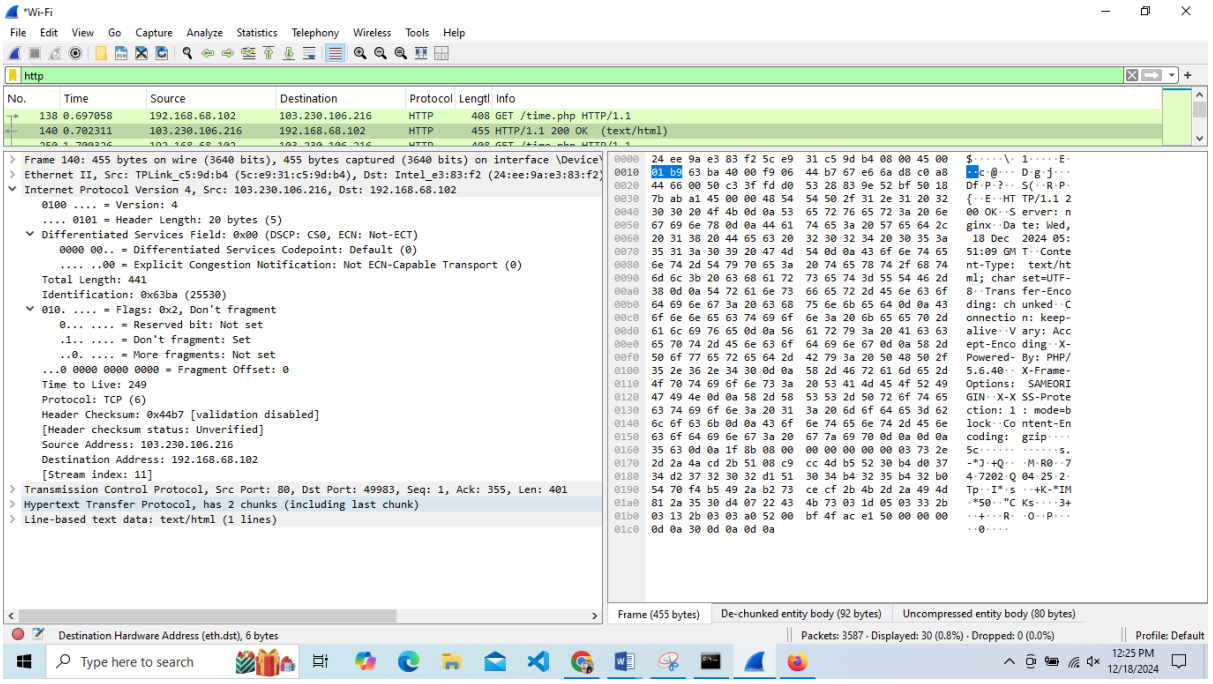

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame 138: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface \Device\
Ethernet II, Src: Intel_e3:83:f2 (24:ee:9a:e3:83:f2), Dst: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4)
Internet Protocol Version 4, Src: 192.168.68.102, Dst: 103.230.106.216
Transmission Control Protocol, Src Port: 49983, Dst Port: 80, Seq: 1, Ack: 1, Len: 354
Source Port: 49983
Destination Port: 80
[Stream index: 8]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 354]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2208190813
[Next Sequence Number: 355 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 4258288424
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 63597
[Calculated window size: 63597]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xd949 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]
[SEQ/ACK analysis]
[Bytes in flight: 354]
[Bytes sent since last PSH flag: 354]
TCP payload (354 bytes)
Hypertext Transfer Protocol
0000 5c e9 31 c5 9d b4 24 ee 9a e3 83 f2 08 00 45 00 \·1···$· ·····E·
0010 01 8a 37 e8 40 00 80 06 00 00 c0 a8 44 66 67 e6 ··7·@··· ····Dfg·
0020 6a d8 c3 3f 00 50 83 9e 51 5d fd d0 53 28 50 18 j··?·P·· Q]··S(P·
0030 f8 6d d9 49 00 00 47 45 54 20 2f 74 69 6d 65 2e ·m·I··GE T /time.
0040 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f php HTTP /1.1··Ho
0050 73 74 3a 20 63 73 70 62 2e 74 65 6c 65 74 61 6c st: cspb .teletal
0060 6b 2e 63 6f 6d 2e 62 64 0d 0a 43 6f 6e 6e 65 63 k.com.bd ··Connec
0070 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive
0080 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f ··User-A gent: Mo
0090 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f zilla/5. 0 (Windo
00a0 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 ws NT 10 .0; Win6
00b0 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4; x64) AppleWeb
00c0 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 54 4d Kit/537. 36 (KHTM
00d0 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 20 43 L, like Gecko) C
00e0 68 72 6f 6d 65 2f 31 33 31 2e 30 2e 30 2e 30 20 hrome/13 1.0.0.0
00f0 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36··A
0100 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 58 2d 52 65 ccept: * /*··X-Re
0110 71 75 65 73 74 65 64 2d 57 69 74 68 3a 20 58 4d quested- With: XM
0120 4c 48 74 74 70 52 65 71 75 65 73 74 0d 0a 52 65 LHttpReq uest··Re
0130 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 63 73 ferer: h ttp://cs
0140 70 62 2e 74 65 6c 65 74 61 6c 6b 2e 63 6f 6d 2e pb.telet alk.com.
0150 62 64 2f 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f bd/··Acc ept-Enco
0160 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c ding: gz ip, defl
0170 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 ate··Acc ept-Lang
0180 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 uage: en -US,en;q
0190 3d 30 2e 39 0d 0a 0d 0a =0.9····
Internet Protocol Version 4 (ip), 20 bytes
Packets: 3587 · Displayed: 30 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
12:22 PM
12/18/2024

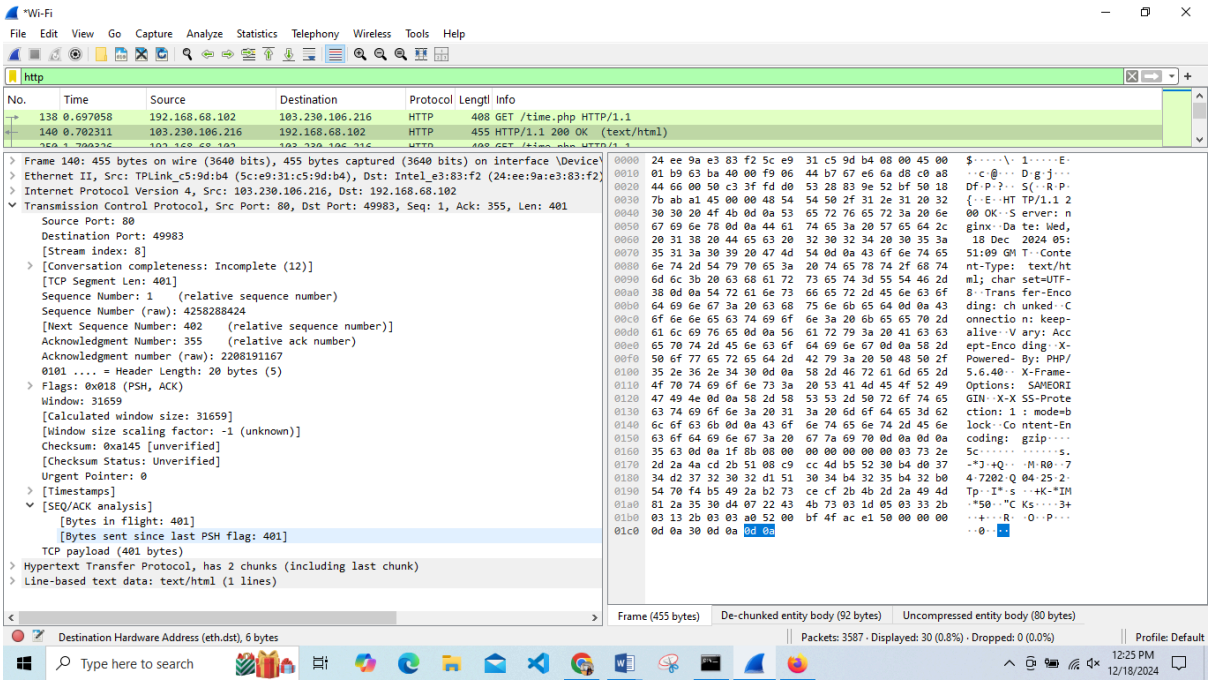

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame 138: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface \Device\
Ethernet II, Src: Intel_e3:83:f2 (24:ee:9a:e3:83:f2), Dst: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4)
Internet Protocol Version 4, Src: 192.168.68.102, Dst: 103.230.106.216
Transmission Control Protocol, Src Port: 49983, Dst Port: 80, Seq: 1, Ack: 1, Len: 354
Hypertext Transfer Protocol
GET /time.php HTTP/1.1\r\n
Request Method: GET
Request URI: /time.php
Request Version: HTTP/1.1
Host: cspb.teletalk.com.bd\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
Accept: */*\r\n
X-Requested-With: XMLHttpRequest\r\n
Referer: http://cspb.teletalk.com.bd/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Response in frame: 140]
[Full request URI: http://cspb.teletalk.com.bd/time.php]
Internet Protocol Version 4 (ip), 20 bytes
Packets: 3587 · Displayed: 30 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
12:23 PM
12/18/2024

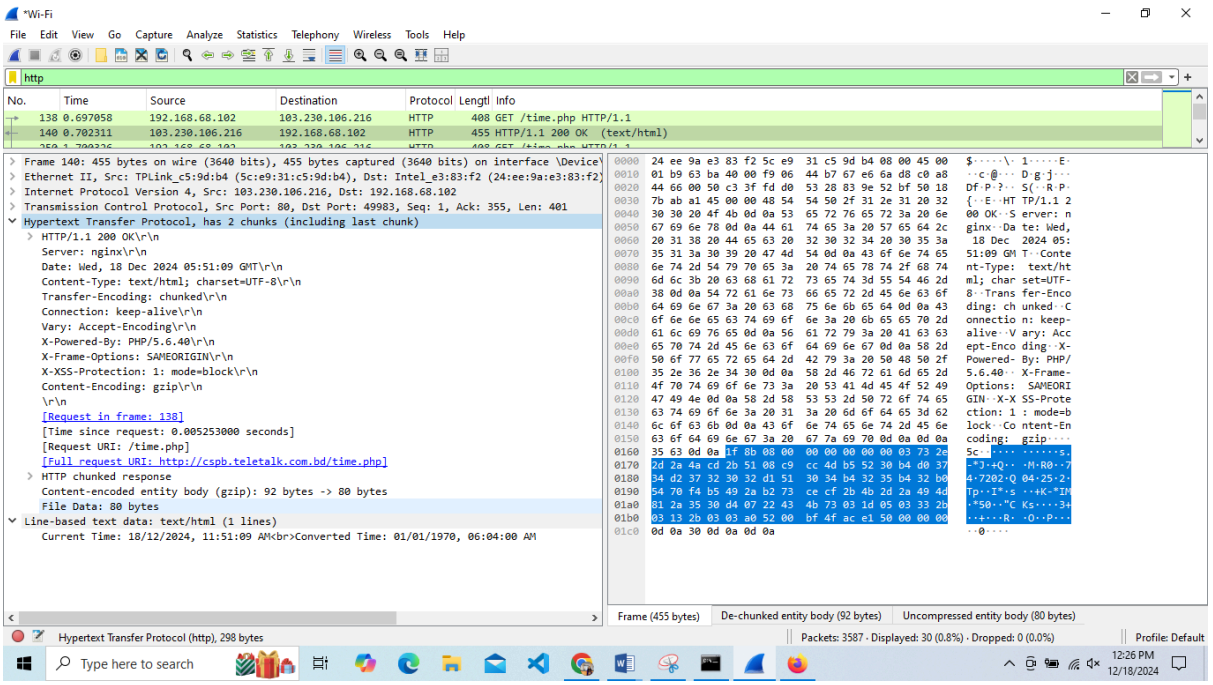
Response:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
138 0.697058 192.168.68.102 103.230.106.216 HTTP 408 GET /time.php HTTP/1.1
140 0.702311 103.230.106.216 192.168.68.102 HTTP 455 HTTP/1.1 200 OK (text/html)
Frame 140: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface \Device\
Section number: 1
Interface id: 0 (\Device\NPF_{F31D9165-9D9D-4161-9DD8-E239A25621AC})
Interface name: \Device\NPF_{F31D9165-9D9D-4161-9DD8-E239A25621AC}
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Dec 18, 2024 11:55:32.713682000 Bangladesh Standard Time
UTC Arrival Time: Dec 18, 2024 05:55:32.713682000 UTC
Epoch Arrival Time: 1734501332.713682000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.001097000 seconds]
[Time delta from previous displayed frame: 0.005253000 seconds]
[Time since reference or first frame: 0.702311000 seconds]
Frame Number: 140
Frame Length: 455 bytes (3640 bits)
Capture Length: 455 bytes (3640 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4), Dst: Intel_e3:83:f2 (24:ee:9a:e3:83:f2)
Internet Protocol Version 4, Src: 103.230.106.216, Dst: 192.168.68.102
Transmission Control Protocol, Src Port: 80, Dst Port: 49983, Seq: 1, Ack: 355, Len: 401
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
Line-based text data: text/html (1 lines)
Frame (455 bytes)
De-chunked entity body (92 bytes)
Uncompressed entity body (80 bytes)
Frame (frame), 455 bytes
Packets: 3587 · Displayed: 30 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
12:24 PM
12/18/2024


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengtl Info
138 0.697058 192.168.68.102 103.230.106.216 HTTP 408 GET /time.php HTTP/1.1
140 0.702311 103.230.106.216 192.168.68.102 HTTP 455 HTTP/1.1 200 OK (text/html)
Frame 140: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface \Device\
Ethernet II, Src: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4), Dst: Intel_e3:83:f2 (24:ee:9a:e3:83:f2)
Destination: Intel_e3:83:f2 (24:ee:9a:e3:83:f2)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 103.230.106.216, Dst: 192.168.68.102
Transmission Control Protocol, Src Port: 80, Dst Port: 49983, Seq: 1, Ack: 355, Len: 401
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
Line-based text data: text/html (1 lines)
Frame (455 bytes)
De-chunked entity body (92 bytes)
Uncompressed entity body (80 bytes)
Destination Hardware Address (eth.dst), 6 bytes
Packets: 3587 · Displayed: 30 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
12:25 PM
12/18/2024


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Lengtl Info
138 0.697058 192.168.68.102 103.230.106.216 HTTP 408 GET /time.php HTTP/1.1
140 0.702311 103.230.106.216 192.168.68.102 HTTP 455 HTTP/1.1 200 OK (text/html)
Frame 140: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface \Device\
Ethernet II, Src: TPLink_c5:9d:b4 (5c:e9:31:c5:9d:b4), Dst: Intel_e3:83:f2 (24:ee:9a:e3:83:f2)
Internet Protocol Version 4, Src: 103.230.106.216, Dst: 192.168.68.102
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 441
Identification: 0x63ba (25530)
010. .... = Flags: 0x2, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 249
Protocol: TCP (6)
Header Checksum: 0x44b7 [validation disabled]
[Header checksum status: Unverified]
Source Address: 103.230.106.216
Destination Address: 192.168.68.102
[Stream index: 11]
Transmission Control Protocol, Src Port: 80, Dst Port: 49983, Seq: 1, Ack: 355, Len: 401
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
Line-based text data: text/html (1 lines)
Frame (455 bytes)
De-chunked entity body (92 bytes)
Uncompressed entity body (80 bytes)
Destination Hardware Address (eth.dst), 6 bytes
Packets: 3587 · Displayed: 30 (0.8%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
12:25 PM
12/18/2024





Frame: Entire packet is captured by Wireshark.

Data Link Layer protocol: It is responsible for framing the packet for transmission over the physical network. Here it is Ethernet II.

Network Layer Protocol: Responsible for routing the packet across different networks. Here it is IPV4.

Transfer Layer Protocol: Providing reliable, ordered, and error-checked delivery of data. Here it is TCP.

Application Layer Protocol: Used for transmitting web pages and other data over the internet. Here it is HTTP.

HTTP is used to fetch resources, such as HTML documents. There will be two types of http messages. The 1st one is HTTP Request message & the 2nd one is HTTP Response messages. Get means request message. 200 OK means status code and status phase. \r\n means return and next line.