Capturing and Analyzing Network traffic with Wireshark

The objective of this work is to use Wireshark to capture network traffic, analyze the captured data, and identify patterns, anomalies or security threats.

Setup

I made sure I had the required permissions to record live traffic on my network interface before downloading and installing Wireshark on my PC using the given link.

Setting up Wireshark

I clicked the "start capturing packets" option to begin capturing after launching Wireshark and choosing WiFi as my network interface to observe.

Capturing Network Traffic

I perform network activities by browsing this site Testphp.vulnweb.com/login.php and I sent an email from my gmail. I stopped capturing after sufficient data had been collected.

Filter Capturing Traffic

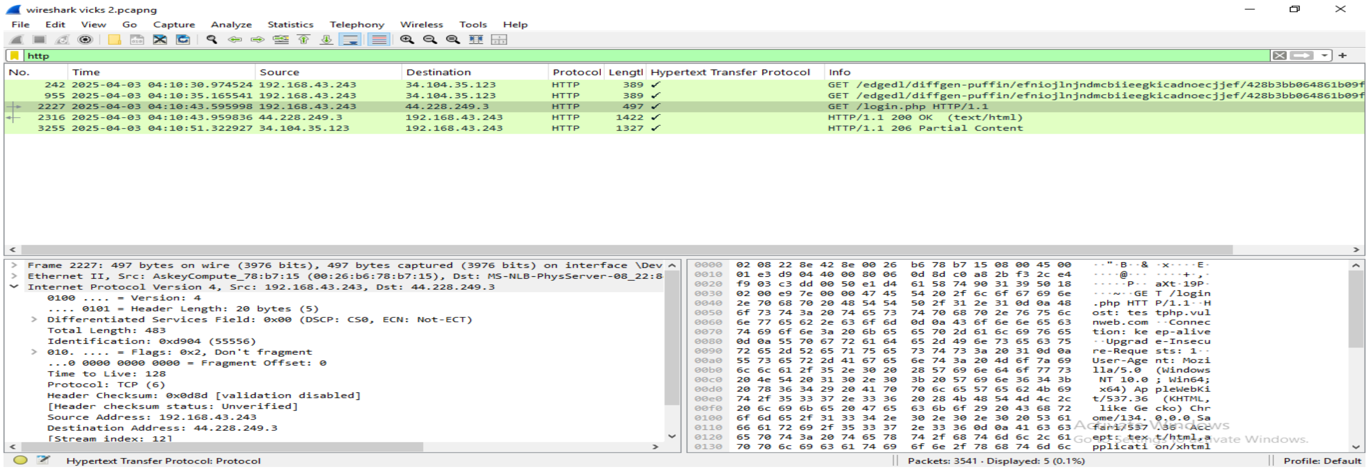
I used Wireshark to narrow down the data by using http - Display Http traffic.

Analyzing Packet Details

I analyzed the source and destination IP address of the website i downloaded which is:
Source IP address : 192.168.43.243 and **Destination IP address : 44.228.249.3**
I also analyze **HTTP** request which is:
Request method: GET
Request URL : /login.php
Request Version : HTTP/1.1
Host : Testphp.vulnwb.com\r\n
There were anomalies such as unencrypted data.

Identifying Security Concerns

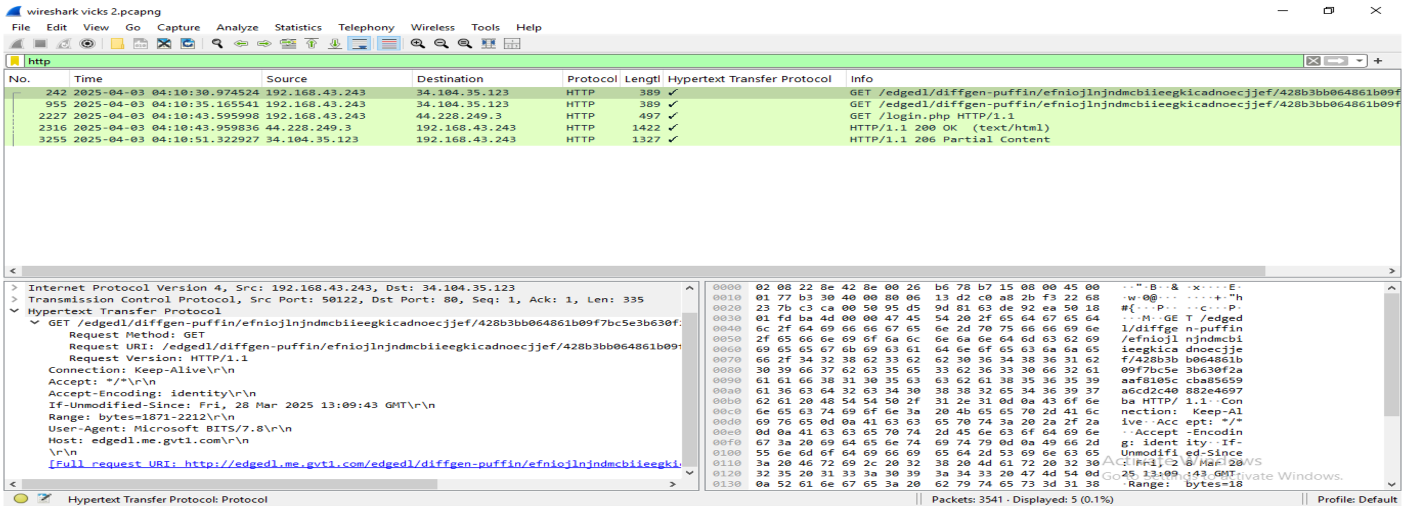
There was **unencrypted data** being transmitted.
There was no **Unexpected IP addresses** communicating with my network and there was no high volume of **traffic** that might indicate an attack.



```
No.   Time                       Source          Destination     Protocol Lengtl Hypertext Transfer Protocol Info
  242 2025-04-03 04:10:30.974524 192.168.43.243  34.104.35.123   HTTP      389  ✓                          GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/428b3bb064861b09f
  955 2025-04-03 04:10:35.165541 192.168.43.243  34.104.35.123   HTTP      389  ✓                          GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/428b3bb064861b09f
 2227 2025-04-03 04:10:43.595998 192.168.43.243  44.228.249.3    HTTP      497  ✓                          GET /login.php HTTP/1.1
 2316 2025-04-03 04:10:43.959836 44.228.249.3    192.168.43.243  HTTP     1422  ✓                          HTTP/1.1 200 OK  (text/html)
 3255 2025-04-03 04:10:51.322927 34.104.35.123   192.168.43.243  HTTP     1327  ✓                          HTTP/1.1 206 Partial Content
```

```
> Frame 2227: 497 bytes on wire (3976 bits), 497 bytes captured (3976 bits) on interface \Dev
> Ethernet II, Src: AskeyCompute_78:b7:15 (00:26:b6:78:b7:15), Dst: MS-NLB-PhysServer-08_22:8
v Internet Protocol Version 4, Src: 192.168.43.243, Dst: 44.228.249.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 483
    Identification: 0xd904 (55556)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0d8d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.243
    Destination Address: 44.228.249.3
    [Stream index: 12]
```

```
0000  02 08 22 8e 42 8e 00 26  b6 78 b7 15 08 00 45 00   ··"·B··& ·x····E·
0010  01 e3 d9 04 40 00 80 06  0d 8d c0 a8 2b f3 2c e4   ····@··· ····+·,·
0020  f9 03 c3 dd 00 50 e1 d4  61 58 74 90 31 39 50 18   ·····P·· aXt·19P·
0030  02 00 e9 7e 00 00 47 45  54 20 2f 6c 6f 67 69 6e   ···~··GE T /login
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0050  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0060  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··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 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ··Upgrad e-Insecu
0090  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1··
00a0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00b0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00c0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.0 ; Win64;
00d0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) Ap pleWebKi
00e0  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c   t/537.36  (KHTML,
00f0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 43 68 72    like Ge cko) Chr
0100  6f 6d 65 2f 31 33 34 2e  30 2e 30 2e 30 20 53 61   ome/134. 0.0.0 Sa
0110  66 61 72 69 2f 35 33 37  2e 33 36 0d 0a 41 63 63   fari/537 .36··Acc
0120  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
0130  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml
```



```
No.   Time                       Source          Destination     Protocol Lengtl Hypertext Transfer Protocol Info
  242 2025-04-03 04:10:30.974524 192.168.43.243  34.104.35.123   HTTP      389  ✓                          GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/428b3bb064861b09f
  955 2025-04-03 04:10:35.165541 192.168.43.243  34.104.35.123   HTTP      389  ✓                          GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/428b3bb064861b09f
 2227 2025-04-03 04:10:43.595998 192.168.43.243  44.228.249.3    HTTP      497  ✓                          GET /login.php HTTP/1.1
 2316 2025-04-03 04:10:43.959836 44.228.249.3    192.168.43.243  HTTP     1422  ✓                          HTTP/1.1 200 OK  (text/html)
 3255 2025-04-03 04:10:51.322927 34.104.35.123   192.168.43.243  HTTP     1327  ✓                          HTTP/1.1 206 Partial Content
```

```
> Internet Protocol Version 4, Src: 192.168.43.243, Dst: 34.104.35.123
> Transmission Control Protocol, Src Port: 50122, Dst Port: 80, Seq: 1, Ack: 1, Len: 335
v Hypertext Transfer Protocol
  v GET /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/428b3bb064861b09f7bc5e3b630f
      Request Method: GET
      Request URI: /edgedl/diffgen-puffin/efniojlnjndmcbiieegkicadnoecjjef/428b3bb064861b09
      Request Version: HTTP/1.1
    Connection: Keep-Alive\r\n
    Accept: */*\r\n
    Accept-Encoding: identity\r\n
    If-Unmodified-Since: Fri, 28 Mar 2025 13:09:43 GMT\r\n
    Range: bytes=1871-2212\r\n
    User-Agent: Microsoft BITS/7.8\r\n
    Host: edgedl.me.gvt1.com\r\n
    \r\n
    [Full request URI: http://edgedl.me.gvt1.com/edgedl/diffgen-puffin/efniojlnjndmcbiieegki
```

```
0000  02 08 22 8e 42 8e 00 26  b6 78 b7 15 08 00 45 00   ··"·B··& ·x····E·
0010  01 77 b3 30 40 00 80 06  13 d2 c0 a8 2b f3 22 68   ·w·0@··· ····+·"h
0020  23 7b c3 ca 00 50 95 d5  9d 81 63 de 92 ea 50 18   #{···P·· ··c···P·
0030  01 fd ba 4d 00 00 47 45  54 20 2f 65 64 67 65 64   ···M··GE T /edged
0040  6c 2f 64 69 66 66 67 65  6e 2d 70 75 66 66 69 6e   l/diffge n-puffin
0050  2f 65 66 6e 69 6f 6a 6c  6e 6a 6e 64 6d 63 62 69   /efniojl njndmcbi
0060  69 65 65 67 6b 69 63 61  64 6e 6f 65 63 6a 6a 65   ieegkica dnoecjje
0070  66 2f 34 32 38 62 33 62  62 30 36 34 38 36 31 62   f/428b3b b064861b
0080  30 39 66 37 62 63 35 65  33 62 36 33 30 66 32 61   09f7bc5e 3b630f2a
0090  61 61 66 38 31 30 35 63  63 62 61 38 35 36 35 39   aaf8105c cba85659
00a0  61 36 63 64 32 63 34 30  38 38 32 65 34 36 39 37   a6cd2c40 882e4697
00b0  62 61 20 48 54 54 50 2f  31 2e 31 0d 0a 43 6f 6e   ba HTTP/ 1.1··Con
00c0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
00d0  69 76 65 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   ive··Acc ept: */*
00e0  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
00f0  67 3a 20 69 64 65 6e 74  69 74 79 0d 0a 49 66 2d   g: ident ity··If-
0100  55 6e 6d 6f 64 69 66 69  65 64 2d 53 69 6e 63 65   Unmodifi ed-Since
0110  3a 20 46 72 69 2c 20 32  38 20 4d 61 72 20 32 30   : Fri, 2 8 Mar 20
0120  32 35 20 31 33 3a 30 39  3a 34 33 20 47 4d 54 0d   25 13:09 :43 GMT·
0130  0a 52 61 6e 67 65 3a 20  62 79 74 65 73 3d 31 38   ·Range:  bytes=18
```

Insights or Recommendations Based on my Observed Traffic Patterns

Upon analyzing my collected packet, I discovered they were unencrypted data transfer which is a serious security problem. Once data is unencrypted, it is susistible to a malware attack.

I recommend that we should always encrypt our data to avoid a potential malware attack or insider threat.