Man-in-the-Middle (MITM) by using WIERSHARK

Introduction:

➢ What is MITM Attack ?

A Man-in-the-Middle (MITM) attack occurs when an attacker intercepts communication between two parties to steal, modify, or monitor data without their knowledge.

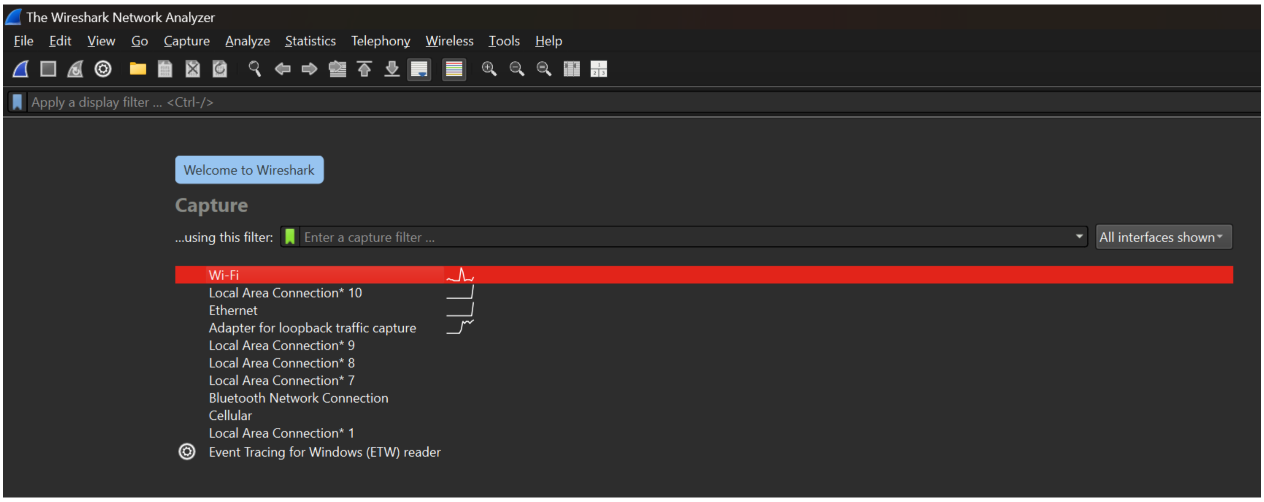
➢ How does MITM Work ?

1. The attacker positions themselves between the victim and the network.
2. The victim unknowingly communicates through the attacker's system.
3. If the communication is unencrypted (HTTP), the attacker can read and modify the data.
4. This can lead to credential theft, session hijacking, or data manipulation.

Step-by-step Process for MITM Attack:

Step-01: Set up Wireshark

1. Open Wireshark.
2. Select the network interface (e.g, wifi option)
3. Double click on it for open , when it open it start caturing the packets.

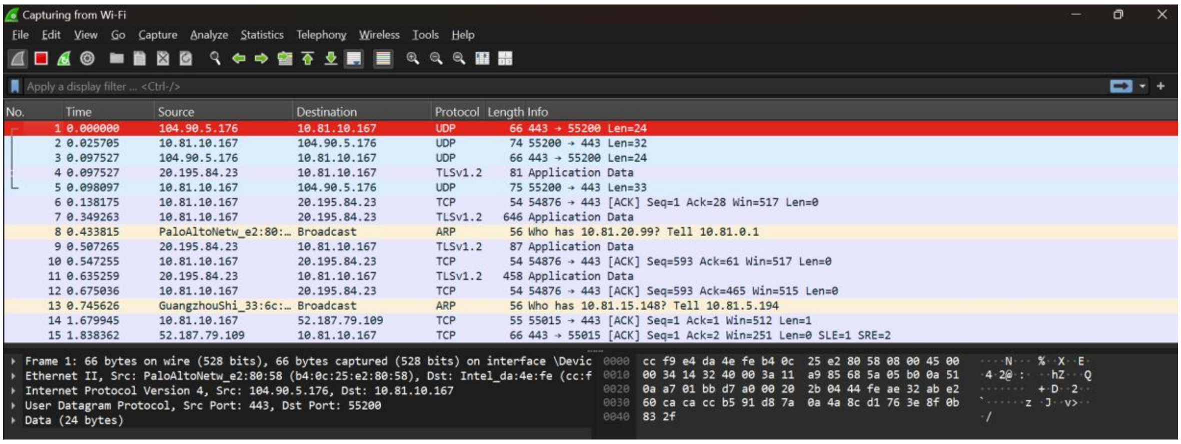


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

- Wi-Fi
- Local Area Connection* 10
- Ethernet
- Adapter for loopback traffic capture
- Local Area Connection* 9
- Local Area Connection* 8
- Local Area Connection* 7
- Bluetooth Network Connection
- Cellular
- Local Area Connection* 1
- Event Tracing for Windows (ETW) reader



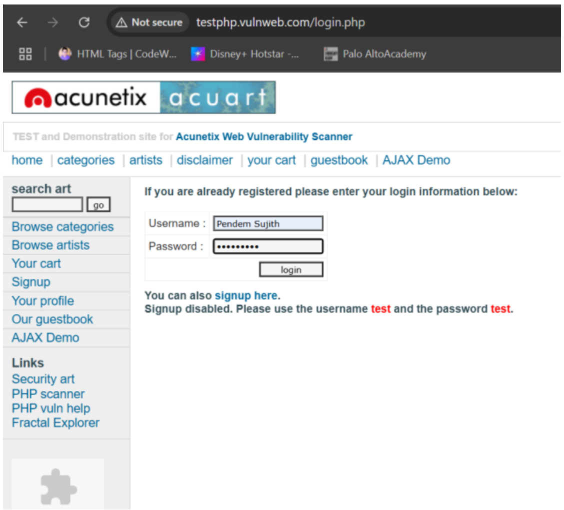
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source               Destination    Protocol Length Info
   1 0.000000  104.90.5.176         10.81.10.167   UDP       66 443 → 55200 Len=24
   2 0.025705  10.81.10.167         104.90.5.176   UDP       74 55200 → 443 Len=32
   3 0.097527  104.90.5.176         10.81.10.167   UDP       66 443 → 55200 Len=24
   4 0.097527  20.195.84.23         10.81.10.167   TLSv1.2   81 Application Data
   5 0.098097  10.81.10.167         104.90.5.176   UDP       75 55200 → 443 Len=33
   6 0.138175  10.81.10.167         20.195.84.23   TCP       54 54876 → 443 [ACK] Seq=1 Ack=28 Win=517 Len=0
   7 0.349263  10.81.10.167         20.195.84.23   TLSv1.2  646 Application Data
   8 0.433815  PaloAltoNetw_e2:80:… Broadcast      ARP       56 Who has 10.81.20.99? Tell 10.81.0.1
   9 0.507265  20.195.84.23         10.81.10.167   TLSv1.2   87 Application Data
  10 0.547255  10.81.10.167         20.195.84.23   TCP       54 54876 → 443 [ACK] Seq=593 Ack=61 Win=517 Len=0
  11 0.635259  20.195.84.23         10.81.10.167   TLSv1.2  458 Application Data
  12 0.675036  10.81.10.167         20.195.84.23   TCP       54 54876 → 443 [ACK] Seq=593 Ack=465 Win=515 Len=0
  13 0.745626  GuangzhouShi_33:6c:… Broadcast      ARP       56 Who has 10.81.15.148? Tell 10.81.5.194
  14 1.679945  10.81.10.167         52.187.79.109  TCP       55 55015 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1
  15 1.838362  52.187.79.109        10.81.10.167   TCP       66 443 → 55015 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2

› Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devic
› Ethernet II, Src: PaloAltoNetw_e2:80:58 (b4:0c:25:e2:80:58), Dst: Intel_da:4e:fe (cc:f
› Internet Protocol Version 4, Src: 104.90.5.176, Dst: 10.81.10.167
› User Datagram Protocol, Src Port: 443, Dst Port: 55200
› Data (24 bytes)

0000  cc f9 e4 da 4e fe b4 0c  25 e2 80 58 08 00 45 00   ····N··· %··X··E·
0010  00 34 14 32 40 00 3a 11  a9 85 68 5a 05 b0 0a 51   ·4·2@·:· ··hZ···Q
0020  0a a7 01 bb d7 a0 00 20  2b 04 44 fe ae 32 ab e2   ········ +·D··2··
0030  60 ca ca cc b5 91 d8 7a  0a 4a 8c d1 76 3e 8f 0b   `······z ·J··v>··
0040  83 2f                                              ·/
```

Step-02: Now go to chrome browser and search for “vulnweb login page”, here the login page will open and fill the details and click on login.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [go]

- Browse categories
- Browse artists
- Your cart
- Signup
- Your profile
- Our guestbook
- AJAX Demo

Links

- Security art
- PHP scanner
- PHP vuln help
- Fractal Explorer

If you are already registered please enter your login information below:

Username : Pendem Sujith

Password : ••••••••••

[login]

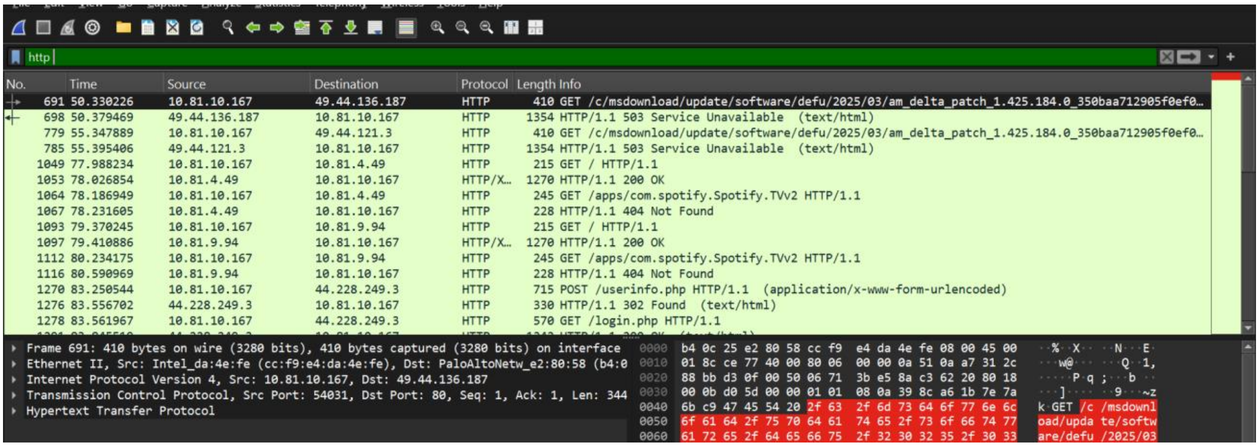
You can also signup here.
Signup disabled. Please use the username test and the password test.

Step-03: In step-03 now go to wireshark in these all the packages loading one by one which are connected with wifi it shows that packages, then stop the loding package.

Step-04: In step-04 now we have find our login website in from all packages for that we use filter.

- In filter search for “http”. It filters all the http websites.

- In these filter we have go to info in info search for “POST”, because the website is under post then we get our website package.

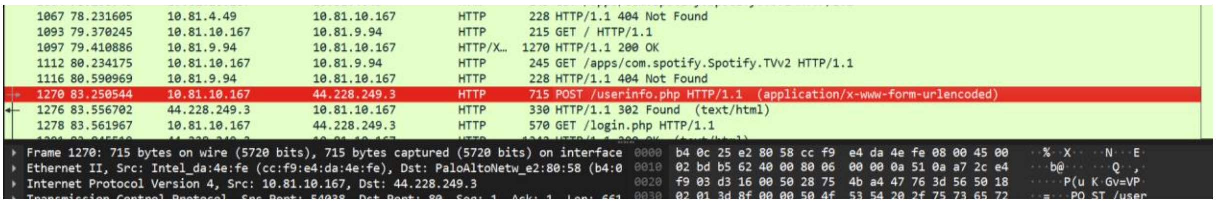


```
http

No.    Time       Source          Destination     Protocol Length Info
  691 50.330226   10.81.10.167    49.44.136.187   HTTP      410 GET /c/msdownload/update/software/defu/2025/03/am_delta_patch_1.425.184.0_350baa712905f0ef0…
  698 50.379469   49.44.136.187   10.81.10.167    HTTP     1354 HTTP/1.1 503 Service Unavailable  (text/html)
  779 55.347889   10.81.10.167    49.44.121.3     HTTP      410 GET /c/msdownload/update/software/defu/2025/03/am_delta_patch_1.425.184.0_350baa712905f0ef0…
  785 55.395406   49.44.121.3     10.81.10.167    HTTP     1354 HTTP/1.1 503 Service Unavailable  (text/html)
 1049 77.988234   10.81.10.167    10.81.4.49      HTTP      215 GET / HTTP/1.1
 1053 78.026854   10.81.4.49      10.81.10.167    HTTP/X…  1270 HTTP/1.1 200 OK
 1064 78.186949   10.81.10.167    10.81.4.49      HTTP      245 GET /apps/com.spotify.Spotify.TVv2 HTTP/1.1
 1067 78.231605   10.81.4.49      10.81.10.167    HTTP      228 HTTP/1.1 404 Not Found
 1093 79.370245   10.81.10.167    10.81.9.94      HTTP      215 GET / HTTP/1.1
 1097 79.410886   10.81.9.94      10.81.10.167    HTTP/X…  1270 HTTP/1.1 200 OK
 1112 80.234175   10.81.10.167    10.81.9.94      HTTP      245 GET /apps/com.spotify.Spotify.TVv2 HTTP/1.1
 1116 80.590969   10.81.9.94      10.81.10.167    HTTP      228 HTTP/1.1 404 Not Found
 1270 83.250544   10.81.10.167    44.228.249.3    HTTP      715 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 1276 83.556702   44.228.249.3    10.81.10.167    HTTP      330 HTTP/1.1 302 Found  (text/html)
 1278 83.561967   10.81.10.167    44.228.249.3    HTTP      570 GET /login.php HTTP/1.1

> Frame 691: 410 bytes on wire (3280 bits), 410 bytes captured (3280 bits) on interface
> Ethernet II, Src: Intel_da:4e:fe (cc:f9:e4:da:4e:fe), Dst: PaloAltoNetw_e2:80:58 (b4:0
> Internet Protocol Version 4, Src: 10.81.10.167, Dst: 49.44.136.187
> Transmission Control Protocol, Src Port: 54031, Dst Port: 80, Seq: 1, Ack: 1, Len: 344
> Hypertext Transfer Protocol

0000  b4 0c 25 e2 80 58 cc f9  e4 da 4e fe 08 00 45 00   ··%··X·· ··N···E·
0010  01 8c ce 77 40 00 80 06  00 00 0a 51 0a a7 31 2c   ···w@··· ···Q··1,
0020  88 bb d3 0f 00 50 06 71  3b e5 8a c3 62 20 80 18   ·····P·q ;···b ··
0030  00 0b d0 5d 00 00 01 01  08 0a 39 8c a6 1b 7e 7a   ···]···· ··9···~z
0040  6b c9 47 45 54 20 2f 63  2f 6d 73 64 6f 77 6e 6c   k·GET /c /msdownl
0050  6f 61 64 2f 75 70 64 61  74 65 2f 73 6f 66 74 77   oad/upda te/softw
0060  61 72 65 2f 64 65 66 75  2f 32 30 32 35 2f 30 33   are/defu /2025/03
```



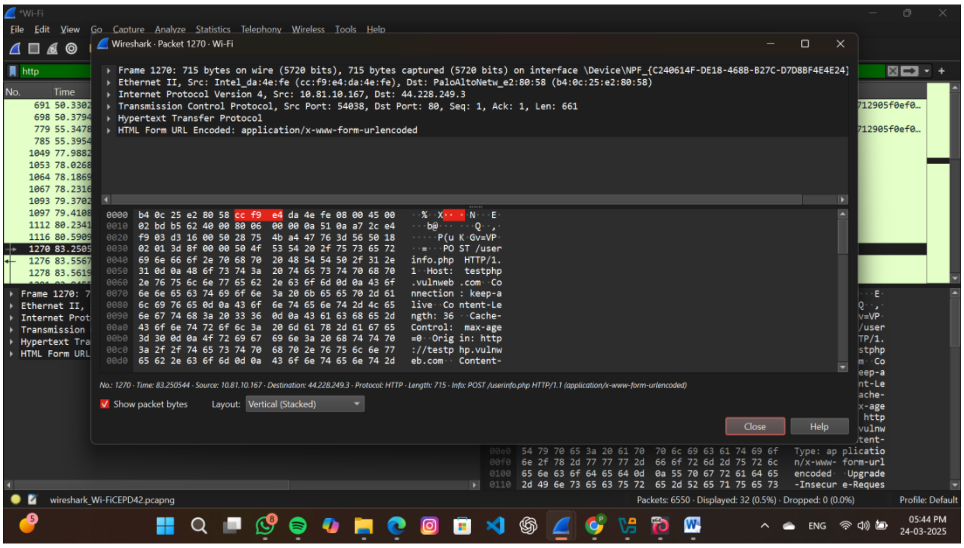
```
 1067 78.231605   10.81.4.49      10.81.10.167    HTTP      228 HTTP/1.1 404 Not Found
 1093 79.370245   10.81.10.167    10.81.9.94      HTTP      215 GET / HTTP/1.1
 1097 79.410886   10.81.9.94      10.81.10.167    HTTP/X…  1270 HTTP/1.1 200 OK
 1112 80.234175   10.81.10.167    10.81.9.94      HTTP      245 GET /apps/com.spotify.Spotify.TVv2 HTTP/1.1
 1116 80.590969   10.81.9.94      10.81.10.167    HTTP      228 HTTP/1.1 404 Not Found
 1270 83.250544   10.81.10.167    44.228.249.3    HTTP      715 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 1276 83.556702   44.228.249.3    10.81.10.167    HTTP      330 HTTP/1.1 302 Found  (text/html)
 1278 83.561967   10.81.10.167    44.228.249.3    HTTP      570 GET /login.php HTTP/1.1

> Frame 1270: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface
> Ethernet II, Src: Intel_da:4e:fe (cc:f9:e4:da:4e:fe), Dst: PaloAltoNetw_e2:80:58 (b4:0
> Internet Protocol Version 4, Src: 10.81.10.167, Dst: 44.228.249.3

0000  b4 0c 25 e2 80 58 cc f9  e4 da 4e fe 08 00 45 00   ··%··X·· ··N···E·
0010  02 bd b5 62 40 00 80 06  00 00 0a 51 0a a7 2c e4   ···b@··· ···Q··,·
0020  f9 03 d3 16 00 50 28 75  4b a4 47 76 3d 56 50 18   ·····P(u K·Gv=VP·
```

- That red part is our website login credentials package then double click on it then it will open.

- After opening in these we can see the login credentials with username and password.



Wireshark · Packet 1270 · Wi-Fi

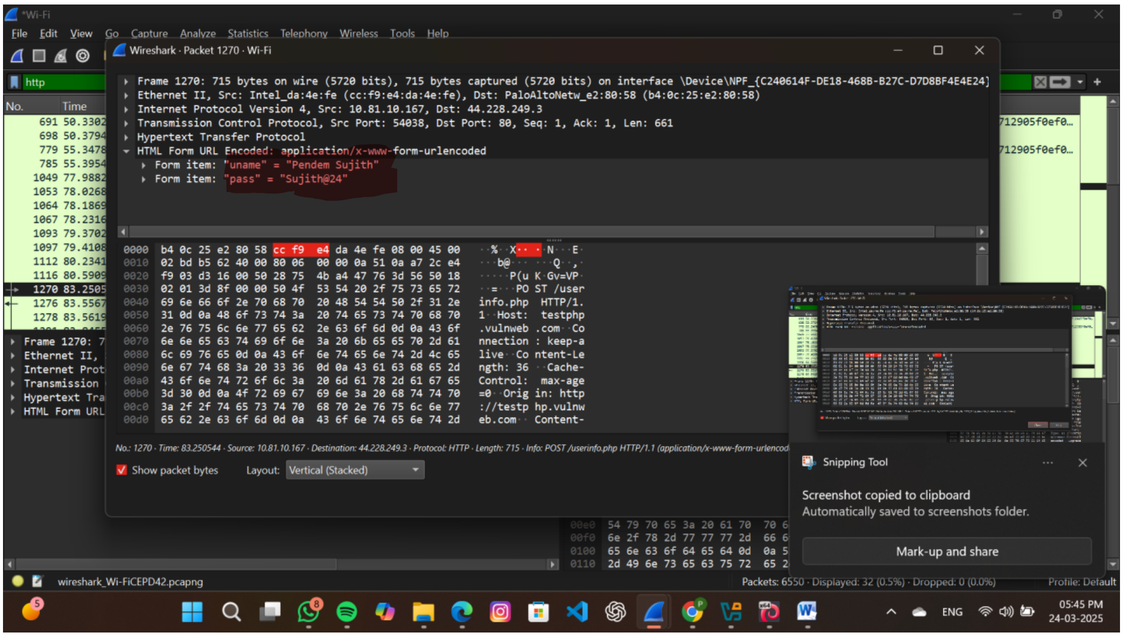
```
Frame 1270: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Device\NPF_{C240614F-DE18-468B-B27C-D7D8BF4E4E24}
Ethernet II, Src: Intel_da:4e:fe (cc:f9:e4:da:4e:fe), Dst: PaloAltoNetw_e2:80:58 (b4:0c:25:e2:80:58)
Internet Protocol Version 4, Src: 10.81.10.167, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54038, Dst Port: 80, Seq: 1, Ack: 1, Len: 661
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  b4 0c 25 e2 80 58 cc f9  e4 da 4e fe 08 00 45 00   ··%··X·· ··N···E·
0010  02 bd b5 62 40 00 80 06  00 00 0a 51 0a a7 2c e4   ···b@··· ···Q··,·
0020  f9 03 d3 16 00 50 28 75  4b a4 47 76 3d 56 50 18   ·····P(u K·Gv=VP·
0030  02 01 3d 8f 00 00 50 4f  53 54 20 2f 75 73 65 72   ··=···PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 33 36  0d 0a 43 61 63 68 65 2d   ngth: 36 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
```

No.: 1270 · Time: 83.250544 · Source: 10.81.10.167 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 715 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

☑ Show packet bytes   Layout: Vertical (Stacked)

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Close
Help
wireshark_Wi-FiCEPD42.pcapng
Packets: 6550 · Displayed: 32 (0.5%) · Dropped: 0 (0.0%)
Profile: Default
ENG
05:44 PM
24-03-2025



Wireshark · Packet 1270 · Wi-Fi

```
Frame 1270: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Device\NPF_{C240614F-DE18-468B-B27C-D7D8BF4E4E24}
Ethernet II, Src: Intel_da:4e:fe (cc:f9:e4:da:4e:fe), Dst: PaloAltoNetw_e2:80:58 (b4:0c:25:e2:80:58)
Internet Protocol Version 4, Src: 10.81.10.167, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54038, Dst Port: 80, Seq: 1, Ack: 1, Len: 661
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "uname" = "Pendem Sujith"
  Form item: "pass" = "Sujith@24"
```

```
0000  b4 0c 25 e2 80 58 cc f9  e4 da 4e fe 08 00 45 00   ··%··X·· ··N···E·
0010  02 bd b5 62 40 00 80 06  00 00 0a 51 0a a7 2c e4   ···b@··· ···Q··,·
0020  f9 03 d3 16 00 50 28 75  4b a4 47 76 3d 56 50 18   ·····P(u K·Gv=VP·
0030  02 01 3d 8f 00 00 50 4f  53 54 20 2f 75 73 65 72   ··=···PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 33 36  0d 0a 43 61 63 68 65 2d   ngth: 36 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
```

No.: 1270 · Time: 83.250544 · Source: 10.81.10.167 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 715 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencod

☑ Show packet bytes   Layout: Vertical (Stacked)

Snipping Tool

Screenshot copied to clipboard
Automatically saved to screenshots folder.

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Mark-up and share
wireshark_Wi-FiCEPD42.pcapng
Packets: 6550 · Displayed: 32 (0.5%) · Dropped: 0 (0.0%)
Profile: Default
ENG
05:45 PM
24-03-2025