MISSION HACKERS

BANGLADESH

Assignment No-02

Assignment Title: Wireshark Packet Capture

Course Title: Cybersecurity & Ethical Hacking

Submitted by:

Name: Istiak Alam

Phone: 01765376101

Submission Date: 08-07-25

Lab Task Topic: Capturing and Analyzing HTTP Login Packets.

Submitted to:

MD Sha Jalal
Founder of Mission Hackers Bangladesh

□ What is Wireshark?

Wireshark is a network protocol analyzer that allows users to capture and analyze network traffic in detail. It is widely regarded as one of the most powerful tools for network troubleshooting, security analysis, and protocol development. Wireshark is free, open-source, and available on multiple platforms, including Windows, macOS, Linux.

□ Installing Wireshark on Kali Linux

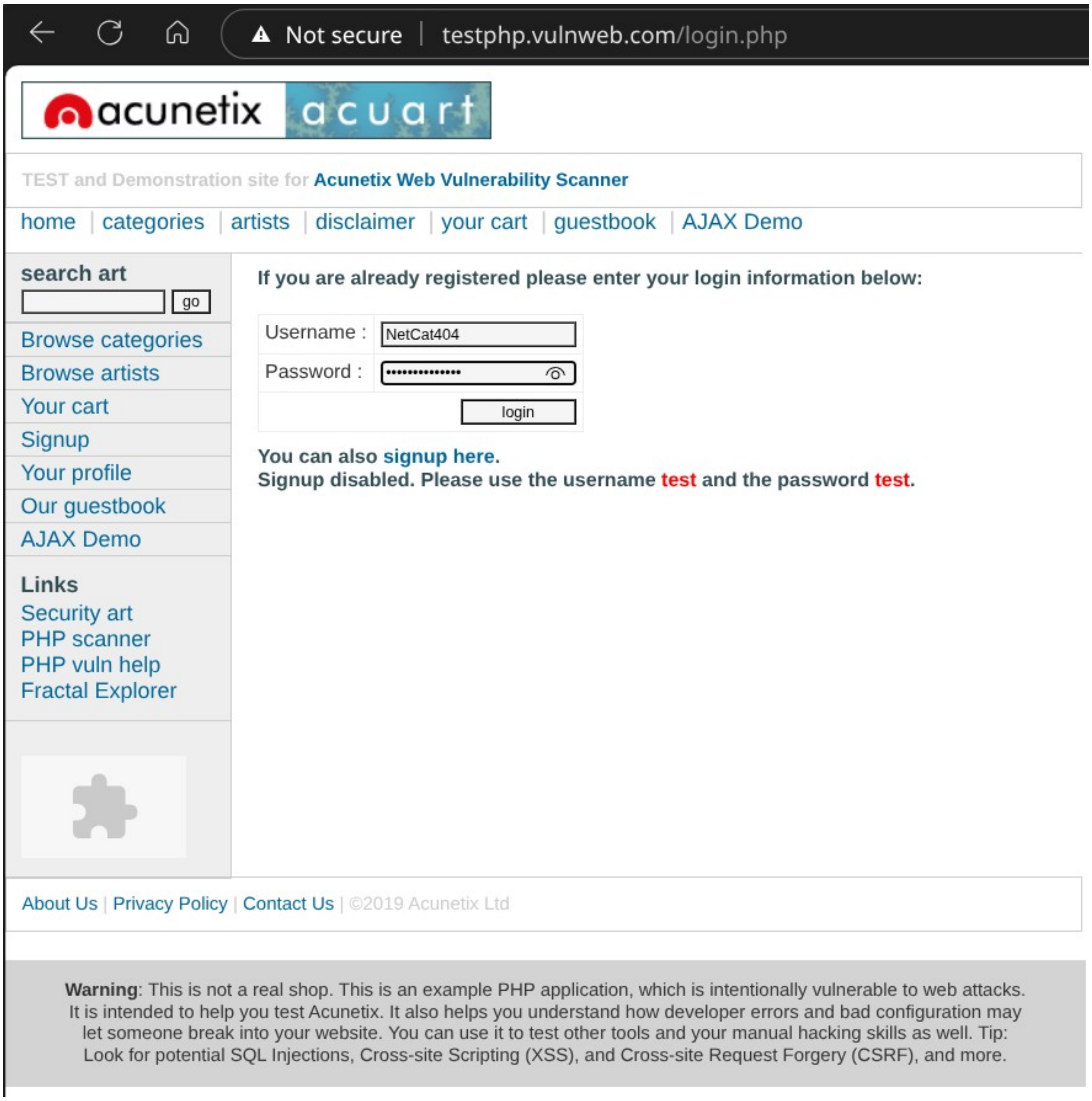
1. Open Terminal : ctrl+alt+t
2. By Default Wireshark is installed in Kali Linux
3. Check the Latest version in terminal :
   ```
   wireshark -version
   ```
4. If not installed, install with :
   ```
   sudo apt update
   sudo apt install wireshark -y
   ```
5. Launch Wireshark with : `sudo wireshark`

□ Capturing Packet From HTTP Login Page

We will now simulate capturing an HTTP login (not HTTPS). Since modern websites use HTTPS, we'll use a **demo HTTP login site** like: [Acunetix Web Vulnerability Scanner]()

1. Open Wireshark
2. Selecting active network interfaces such as: eth0, wlan0, lo
3. After selecting the interface it will start capturing
4. I will filter the capture in the top of the capture only HTTP
5. Everything is setup. Now browse to the HTTP login page.

6. The page link is : http://testphp.vulnweb.com/login.php



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

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

Username :	NetCat404
Password :	••••••••••••••

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

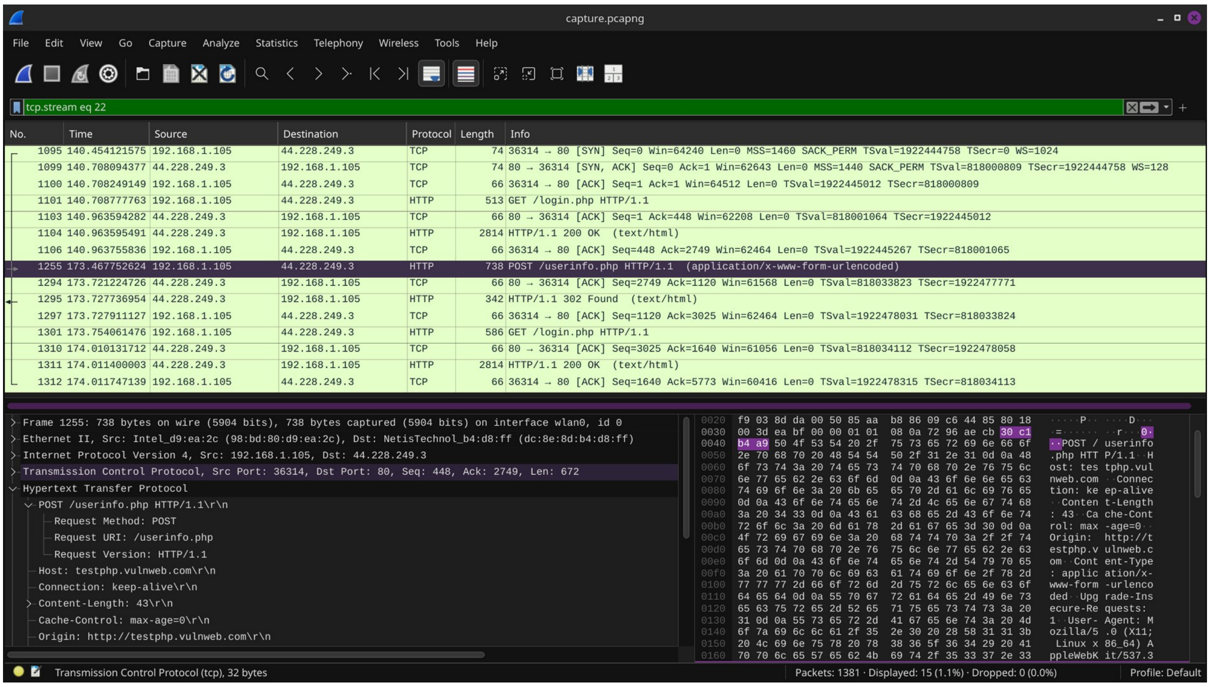
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Figure 1: Acunetix Vulnerability Scanner

7. After fill up the form entering any dummy credentials like
   Username : Netcat404
   Password : Netarious725@3lsm#
8. Submit the form.
9. Go back to Wireshark and Stop the capturing packet by clicking the red square (Stop) button.

Saving the Capture file as capture.pcapng

Now, If we search for **post /userinfo.php** we can see there is a packet with the protocol of HTTP :


capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 22

No.   Time           Source          Destination     Protocol Length Info
1095 140.454121575 192.168.1.105   44.228.249.3    TCP        74 36314 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1922444758 TSecr=0 WS=1024
1099 140.708094377 44.228.249.3    192.168.1.105   TCP        74 80 → 36314 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1440 SACK_PERM TSval=818000809 TSecr=1922444758 WS=128
1100 140.708249149 192.168.1.105   44.228.249.3    TCP        66 36314 → 80 [ACK] Seq=1 Ack=1 Win=64512 Len=0 TSval=1922445012 TSecr=818000809
1101 140.708777763 192.168.1.105   44.228.249.3    HTTP      513 GET /login.php HTTP/1.1
1103 140.963594282 44.228.249.3    192.168.1.105   TCP        66 80 → 36314 [ACK] Seq=1 Ack=448 Win=62208 Len=0 TSval=818001064 TSecr=1922445012
1104 140.963595491 44.228.249.3    192.168.1.105   HTTP     2814 HTTP/1.1 200 OK  (text/html)
1106 140.963755836 192.168.1.105   44.228.249.3    TCP        66 36314 → 80 [ACK] Seq=448 Ack=2749 Win=62464 Len=0 TSval=1922445267 TSecr=818001065
1255 173.467752624 192.168.1.105   44.228.249.3    HTTP      738 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
1294 173.721224726 44.228.249.3    192.168.1.105   TCP        66 80 → 36314 [ACK] Seq=2749 Ack=1120 Win=61568 Len=0 TSval=818033823 TSecr=1922477771
1295 173.727736954 44.228.249.3    192.168.1.105   HTTP      342 HTTP/1.1 302 Found  (text/html)
1297 173.727911127 192.168.1.105   44.228.249.3    TCP        66 36314 → 80 [ACK] Seq=1120 Ack=3025 Win=62464 Len=0 TSval=1922478031 TSecr=818033824
1301 173.754061476 192.168.1.105   44.228.249.3    HTTP      586 GET /login.php HTTP/1.1
1310 174.010131712 44.228.249.3    192.168.1.105   TCP        66 80 → 36314 [ACK] Seq=3025 Ack=1640 Win=61056 Len=0 TSval=818034112 TSecr=1922478058
1311 174.011400003 44.228.249.3    192.168.1.105   HTTP     2814 HTTP/1.1 200 OK  (text/html)
1312 174.011747139 192.168.1.105   44.228.249.3    TCP        66 36314 → 80 [ACK] Seq=1640 Ack=5773 Win=60416 Len=0 TSval=1922478315 TSecr=818034113
```

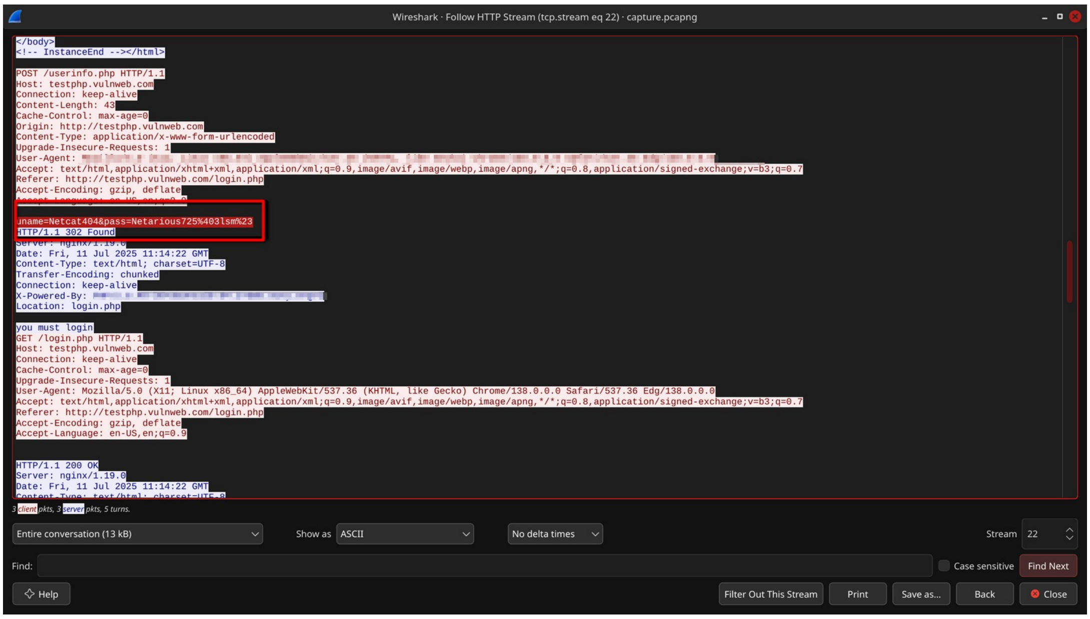
```
> Frame 1255: 738 bytes on wire (5904 bits), 738 bytes captured (5904 bits) on interface wlan0, id 0
> Ethernet II, Src: Intel_d9:ea:2c (98:bd:80:d9:ea:2c), Dst: NetisTechnol_b4:d8:ff (dc:8e:8d:b4:d8:ff)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 36314, Dst Port: 80, Seq: 448, Ack: 2749, Len: 672
v Hypertext Transfer Protocol
  v POST /userinfo.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /userinfo.php
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
  > Content-Length: 43\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
```

```
0020  f9 03 8d da 00 50 85 aa  b8 86 09 c6 44 85 80 18   ·····P·· ····D···
0030  00 3d ea bf 00 00 01 01  08 0a 72 96 ae cb 30 c1   ·=······ ··r···0·
0040  b4 a9 50 4f 53 54 20 2f  75 73 65 72 69 6e 66 6f   ··POST / userinfo
0050  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0060  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0070  6e 77 65 62 2e 63 6f 6d  0d 0a 43 6f 6e 6e 65 63   nweb.com ··Connec
0080  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
0090  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
00a0  3a 20 34 33 0d 0a 43 61  63 68 65 2d 43 6f 6e 74   : 43··Ca che-Cont
00b0  72 6f 6c 3a 20 6d 61 78  2d 61 67 65 3d 30 0d 0a   rol: max -age=0··
00c0  4f 72 69 67 69 6e 3a 20  68 74 74 70 3a 2f 2f 74   Origin:  http://t
00d0  65 73 74 70 68 70 2e 76  75 6c 6e 77 65 62 2e 63   estphp.v ulnweb.c
00e0  6f 6d 0d 0a 43 6f 6e 74  65 6e 74 2d 54 79 70 65   om··Cont ent-Type
00f0  3a 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 78 2d   : applic ation/x-
0100  77 77 77 2d 66 6f 72 6d  2d 75 72 6c 65 6e 63 6f   www-form -urlenco
0110  64 65 64 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   ded··Upg rade-Ins
0120  65 63 75 72 65 2d 52 65  71 75 65 73 74 73 3a 20   ecure-Re quests: 
0130  31 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   1··User- Agent: M
0140  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0150  20 4c 69 6e 75 78 20 78  38 36 5f 36 34 29 20 41    Linux x 86_64) A
0160  70 70 6c 65 57 65 62 4b  69 74 2f 35 33 37 2e 33   ppleWebK it/537.3
```

Transmission Control Protocol (tcp), 32 bytes · Packets: 1381 · Displayed: 15 (1.1%) · Dropped: 0 (0.0%) · Profile: Default

Figure 2: Post Packet Captured

Under the Analyze click Follow and select TCP or HTTP Stream. Then the Username and the Password is visible unencrypted.


Wireshark · Follow HTTP Stream (tcp.stream eq 22) · capture.pcapng

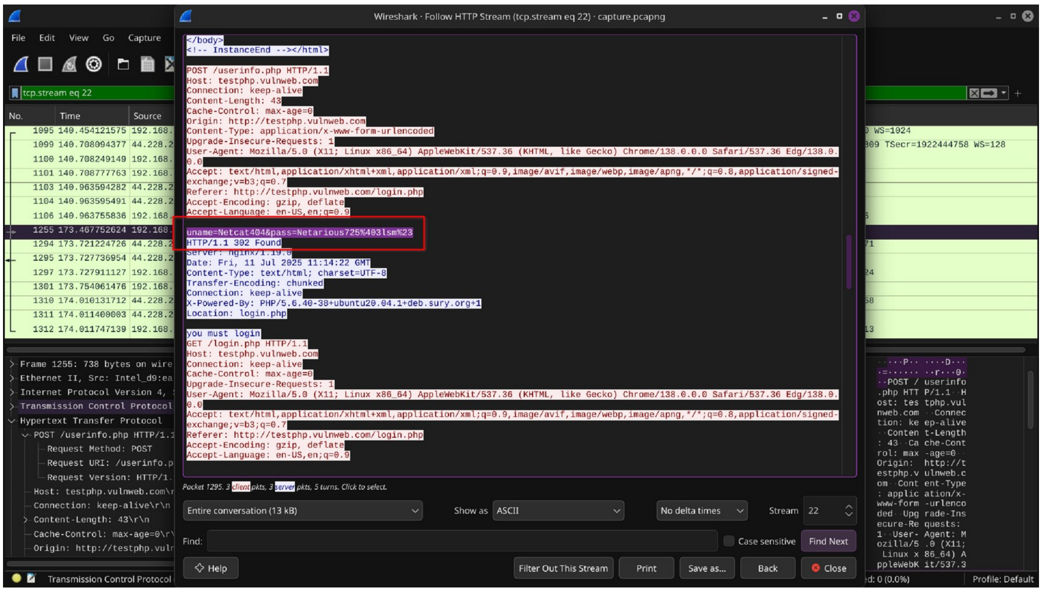
```
</body>
<!-- InstanceEnd --></html>

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 43
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=Netcat404&pass=Netarious725%403lsm%23
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Fri, 11 Jul 2025 11:14:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: [redacted]
Location: login.php

you must login
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 11 Jul 2025 11:14:22 GMT
Content-Type: text/html; charset=UTF-8
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (13 kB) · Show as: ASCII · No delta times · Stream: 22

Figure 3: Visible username & password

Now this is the process of Capturing Packet and get information from it….



Wireshark · Follow HTTP Stream (tcp.stream eq 22) · capture.pcapng
Packet 1295. 3 client pkts, 3 server pkts, 5 turns. Click to select.
Entire conversation (13 kB)
Show as ASCII
No delta times
Stream 22
Find:
Case sensitive
Find Next
Help
Filter Out This Stream
Print
Save as…
Back
Close

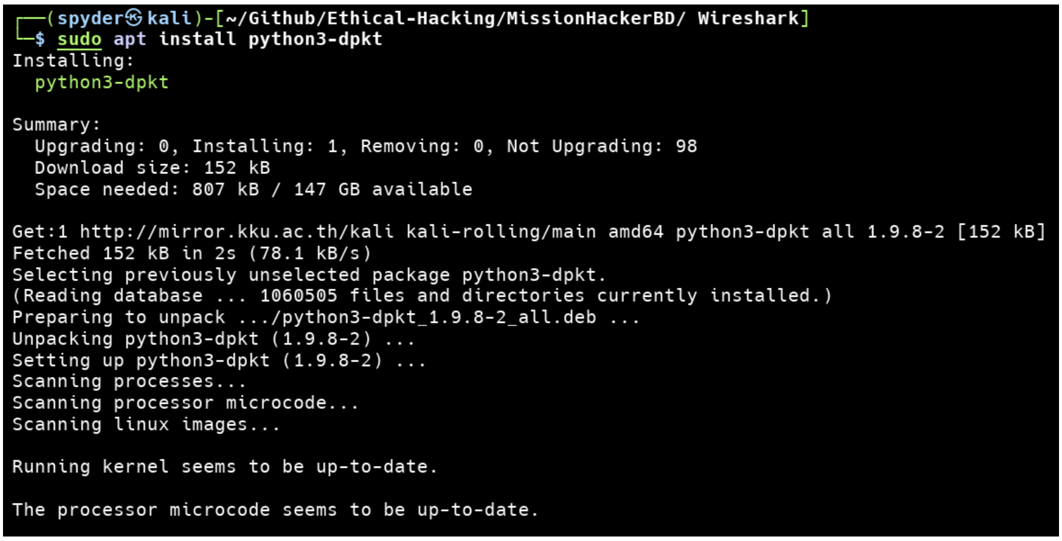
```
</body>
<!-- InstanceEnd --></html>

POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 43
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.
0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

uname=Netcat404&pass=Netarious725%403lsm%23
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Fri, 11 Jul 2025 11:14:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

you must login
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 Edg/138.0.
0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Figure 4: Visible information from captured packet

□ Analyses the Captured Packet Using Wanalyzer

We have the Captured file capture.pcapng in the folder. Now Following those step we can Analyze the data from the packet -

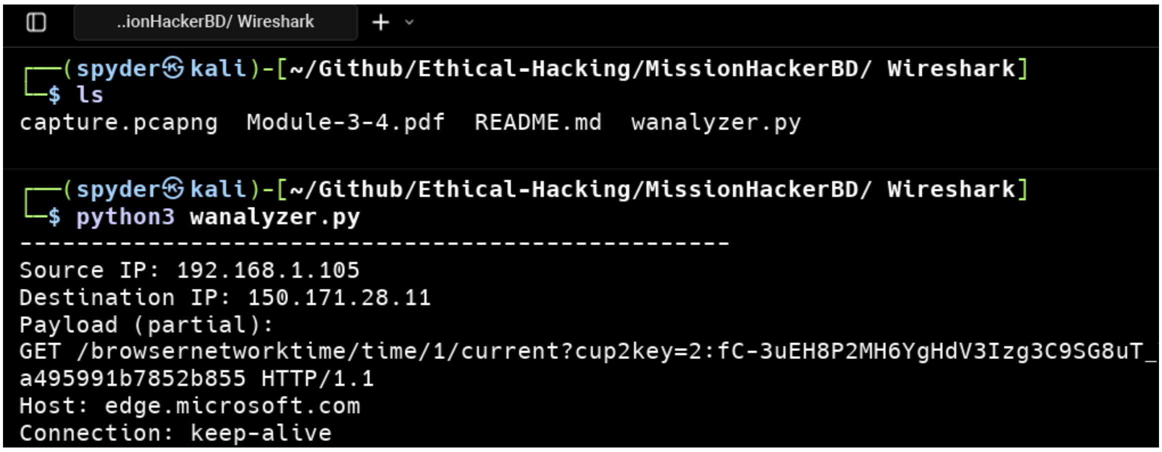
1. Open terminal in the working directory of that captured file.
2. For analyze the file we have to install some dependencies: python3-dpkt : **`sudo apt install python3-dpkt`**



```
┌──(spyder㉿kali)-[~/Github/Ethical-Hacking/MissionHackerBD/ Wireshark]
└─$ sudo apt install python3-dpkt
Installing:
  python3-dpkt

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 98
  Download size: 152 kB
  Space needed: 807 kB / 147 GB available

Get:1 http://mirror.kku.ac.th/kali kali-rolling/main amd64 python3-dpkt all 1.9.8-2 [152 kB]
Fetched 152 kB in 2s (78.1 kB/s)
Selecting previously unselected package python3-dpkt.
(Reading database ... 1060505 files and directories currently installed.)
Preparing to unpack .../python3-dpkt_1.9.8-2_all.deb ...
Unpacking python3-dpkt (1.9.8-2) ...
Setting up python3-dpkt (1.9.8-2) ...
Scanning processes...
Scanning processor microcode...
Scanning linux images...

Running kernel seems to be up-to-date.

The processor microcode seems to be up-to-date.
```

Figure 5: Installing Dependencies

3. After install all the dependencies, now we can use Wanalyzer by the command : python3 wanalyzer.py



```
┌──(spyder㉿kali)-[~/Github/Ethical-Hacking/MissionHackerBD/ Wireshark]
└─$ ls
capture.pcapng  Module-3-4.pdf  README.md  wanalyzer.py

┌──(spyder㉿kali)-[~/Github/Ethical-Hacking/MissionHackerBD/ Wireshark]
└─$ python3 wanalyzer.py
--------------------------------------------------
Source IP: 192.168.1.105
Destination IP: 150.171.28.11
Payload (partial):
GET /browsernetworktime/time/1/current?cup2key=2:fC-3uEH8P2MH6YgHdV3Izg3C9SG8uT_
a495991b7852b855 HTTP/1.1
Host: edge.microsoft.com
Connection: keep-alive
```

Figure 6: Running Wanalyzer

4. As we can see the analyze report of the captured file :

```
┌──(spyder㉿kali)-[~/Github/Ethical-Hacking/MissionHackerBD/ Wireshark]
└─$ python3 wanalyzer.py
-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 192.168.1.105
Destination IP: 150.171.28.11
Payload (partial):
GET /browsernetworktime/time/1/current?
cup2key=2:fC-3uEH8P2MH6YgHdV3Izg3C9SG8uT_YQu4eX-
UjgI8&cup2hreq=e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
HTTP/1.1
Host: edge.microsoft.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Sec-Mesh-Client-Edge-Version: 138.0.3351.77
Sec-Mesh-Client-Edge-Channel: stable
Sec-Mesh-Client-OS: Linux
Sec-Mesh-Client-OS-Version: 6.12.33+kali-amd64
Sec-Mesh-Client-Arch: x86_64
Sec-Mesh-Client-WebView: 0
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
Accept-Encoding: gzip, deflate


-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 150.171.28.11
Destination IP: 192.168.1.105
Payload (partial):
HTTP/1.1 200 OK
Cache-Control: no-store, must-revalidate, no-cache, max-age=0
```

```
Pragma: no-cache
Content-Length: 100
Content-Type: application/json
Content-Encoding: gzip
Expires: Mon, 01 Jan 1990 00:00:00 GMT
X-Frame-Options: sameorigin
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
x-cup-server-proof:
304602210088C3BCDE3A07314D789D55A3160993C6BA46929568D8D28B4B78584482ABFCC0022100F32
CDCE3859EC2834AEBA04B2A4B3F41FB0A611C5D102F6A10244A3610229EE4:e3b0c44298fc1c149afbf
4c8996fb92427ae41e4649b934ca495991b7852b855
Content-Disposition: attachment; filename='json.txt'
X-Cache: CONFIG_NOCACHE
X-MSEdge-Ref: Ref A: 168A7D530C664CF99F26A3140AA1B4BD Ref B: SIN30EDGE0509 Ref C:
2025-07-11T11:12:13Z
Date: Fri, 11 Jul 2025 11:12:13 GMT

-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 192.168.1.105
Destination IP: 44.228.249.3
Payload (partial):
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 44.228.249.3
Destination IP: 192.168.1.105
Payload (partial):
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 11 Jul 2025 11:13:49 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

9b4
Xms6
7MPIdQm;nمIHę"^Y(3iGX>7?qstn~=:gQ$'?8浑VWIr>ذJkQ,@YrKRyuTJ1(lMy56
83Y3+MŭH.i9}\ŠXAS6U!~n- DFS^8/332[HsU[Qn<44:OY^rmMQW/^GP`S/
                                               iyV   9!vVJY$qIH8;,/b)PiQiDB >'F^e6=
            F)`3%
                     r_'M'\Ʋ′
я|o戮m/ s'OU
`KYj 藹 c?EhIS[qB[/[(yҲ'_{aMO7o
                             9H\o: d3″,lysOrVSj/b)o xt)_̽9; `9pps${IxgQD'!
G2U&lo\H#Jk:b.@Q>G<3j8ax8Rm8#C9!.)=M("<oka W4r>cFi$
                                              2SF^4z~xpU2it1^4z8qfDjiWp_'pd-
U=U`bP5slJVaV.dc[KAd>DA    W~oT'c_zz 礁^9;4<wi4<<Fz&%guUbj'O9;)O_l҅\[il

                                                                      zha!
M^q93ᓄw)s04+jF@ӂ
c3<z7?=Kk}ҷT
g

wj      GR)9AodzN9ĽrK8!\PPj`9Qy+vPU
}#P"BlxDՈ ?-_|A\*T1~Fh=Cu-u+ѧLUACf7~jllĜwho,릒 ANe
                MS@%H#a.)C|7m6W-qOZ&<C1?)H' @@A.6%@ȶN;@AI3pQ]u

M~.◌xḰ,tbEῳL3*;tشV/˥vk]F\tO|rg?CV'[}=mXo?t'-F4bs̑-#w]}}8!uↄt;NS<P
cTq_$                                             F
     &J"t J$
[nV(/EDhx&uk]~ƙy(%P6T]Q)\4a^a]<8;\\a>__xGf5p95pb!ϐiĔï|!3D2)tl
?9Aûx4j!C/||l[*\)z<q6/tB                                     <;|vQ
                        ;h(x6o7ZaLo;S3^1∸lq44=N\$tue\{|Ah<>3a34?ܼZ.x/ˏB2vI1VV
                                                                             F2⸮
j"vhcUܼIk6
1&aQ)hxΨyDYыо;:lmf\I6RjeK<r|7
N/2e)nK
       ū
1&L\&a-l`ԉ
          <x@ᨩк>:7FCs^J|)P9+`VZ+mL꞉OS9k<+V
                                                jˠ   &CiI4'X%VF>J<Ḫ̈UlF#
aoP3v1p+Xlᷝg/HDẔ9W3;>lC{3Г
0


-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 192.168.1.105
Destination IP: 44.228.249.3
Payload (partial):
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 43
Cache-Control: max-age=0
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

uname=Netcat404&pass=Netarious725%403lsm%23

```
-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 44.228.249.3
Destination IP: 192.168.1.105
Payload (partial):
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Fri, 11 Jul 2025 11:14:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

e
you must login
0


-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 192.168.1.105
Destination IP: 44.228.249.3
Payload (partial):
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36 Edg/138.0.0.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
Source IP: 44.228.249.3
Destination IP: 192.168.1.105
Payload (partial):
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 11 Jul 2025 11:14:22 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
```

```
###[ Ethernet ]###
  dst       = dc:8e:8d:b4:d8:ff
  src       = 98:bd:80:d9:ea:2c
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 60
     id        = 52425
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x1221
     src       = 192.168.1.105
     dst       = 103.62.50.130
     \options   \
###[ TCP ]###
        sport     = 57578
        dport     = 6464
        seq       = 1881558653
        ack       = 0
        dataofs   = 10
        reserved  = 0
        flags     = S
        window    = 64240
        chksum    = 0x5c00
        urgptr    = 0
        options   = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (4211052413,
0)), ('NOP', None), ('WScale', 10)]
-----------------------------------------------------------------------------------
-----------------------------------------------------------------------------------
```