A logo with a person in a hoodie using a computer

AI-generated content may be incorrect.

**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**

1. If not installed, install with :

**sudo apt update**

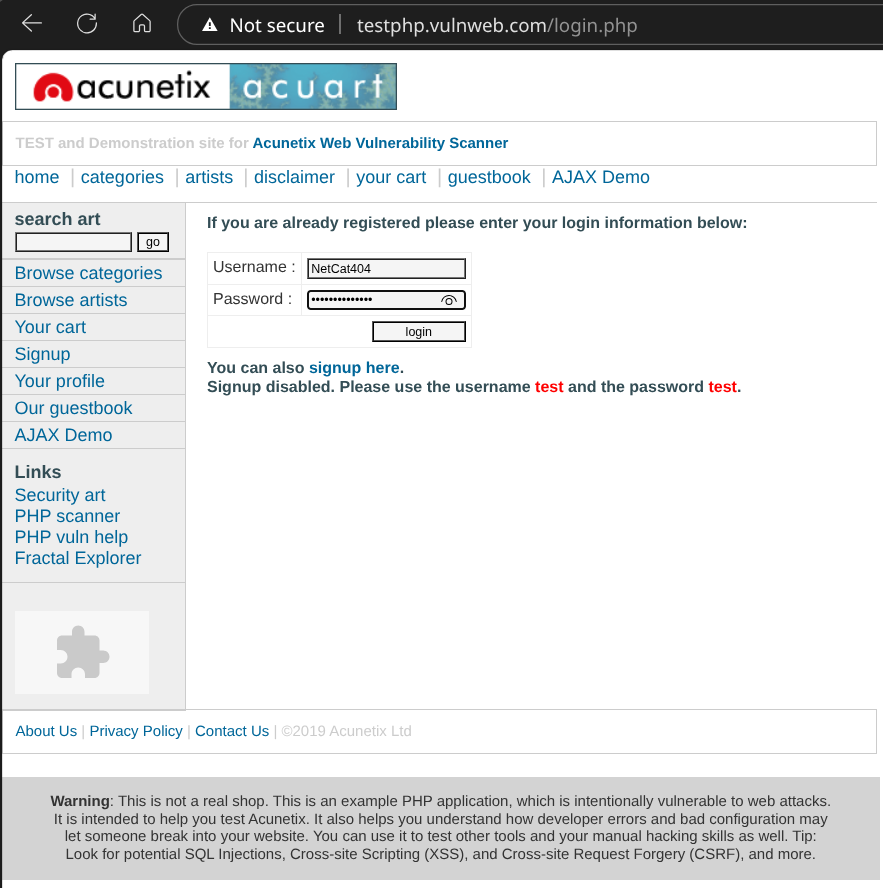
**sudo apt install wireshark -y**

1. 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](http://testphp.vulnweb.com/login.php)

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>
7. After fill up the form entering any dummy credentials like Username : Netcat404

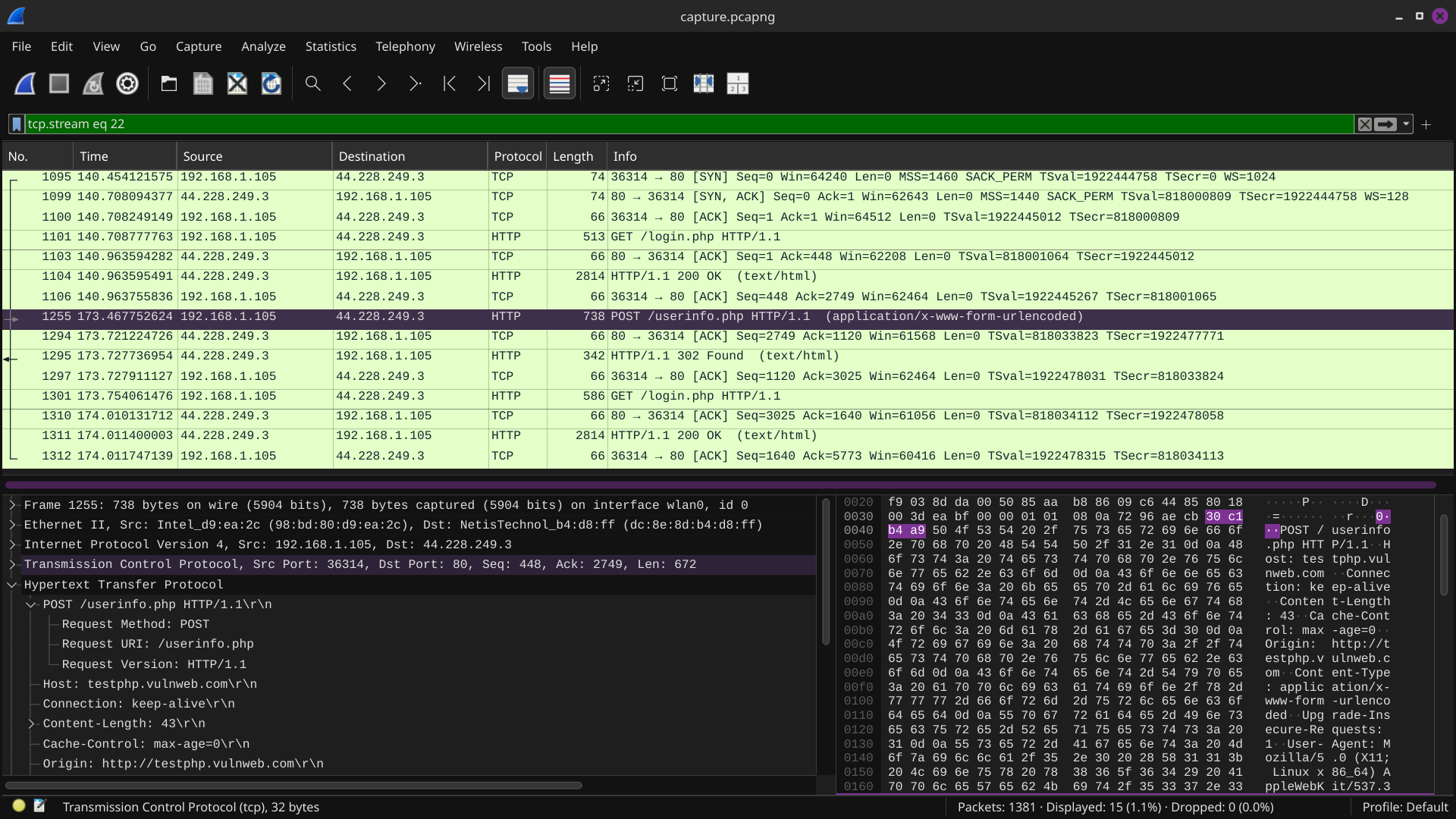
Figure 1: Acunetix Vulnerability Scanner

Password : Netarious725@3lsm#

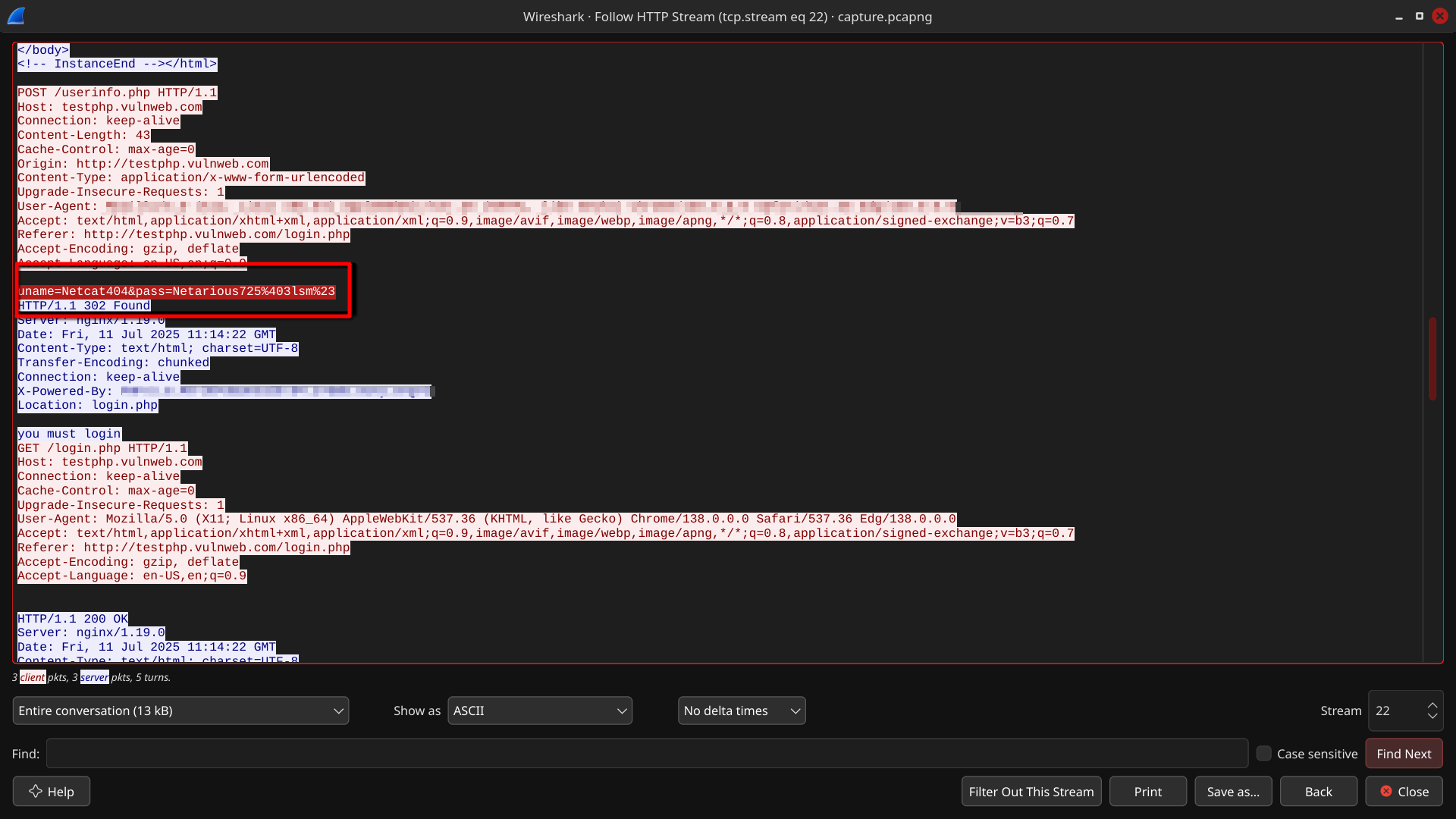
1. Submit the form.
2. Go back to Wireshark and Stop the capturing packet by clicking the red square (Stop) button.

Saving the Capture file as capture.pcapng

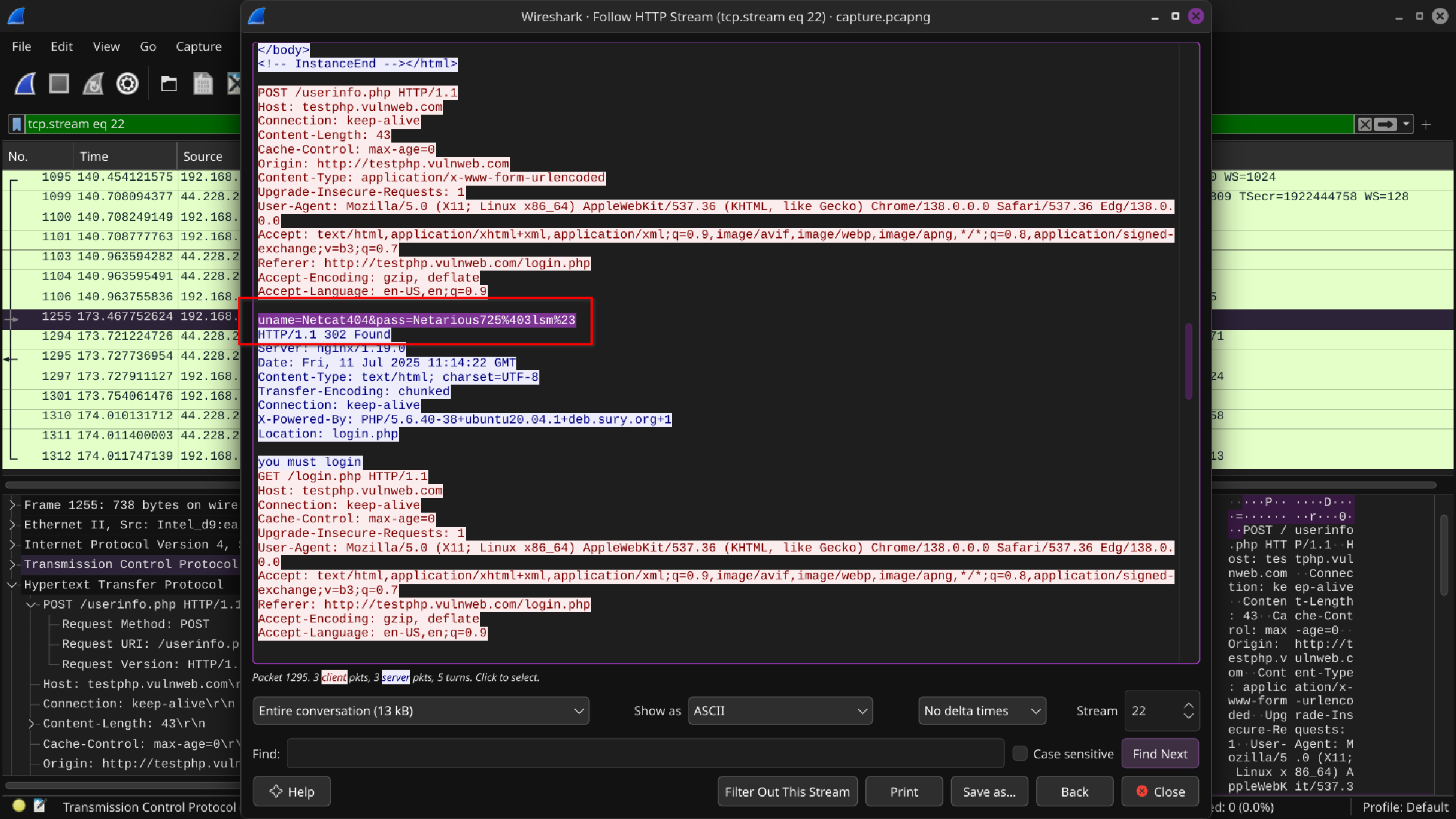
Now, If we search for **post /userinfo.php** we can see there is a packet with the protocol of HTTP :

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.

Figure 3: Visible username & password

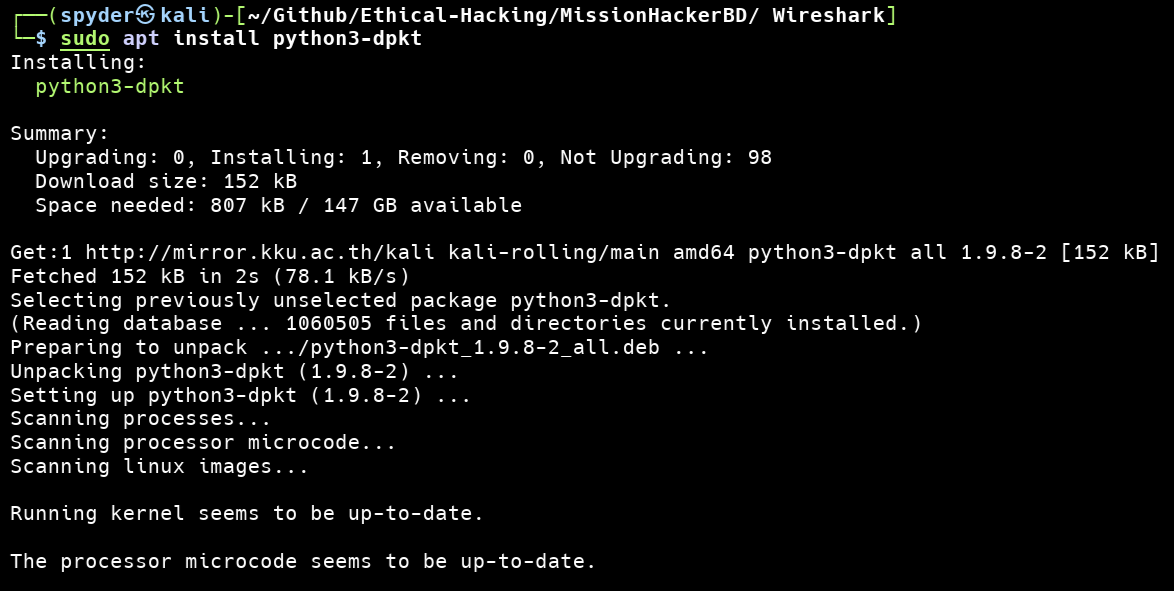
Now this is the process of Capturing Packet and get information from it….

Figure 4: Visible information from captured packet

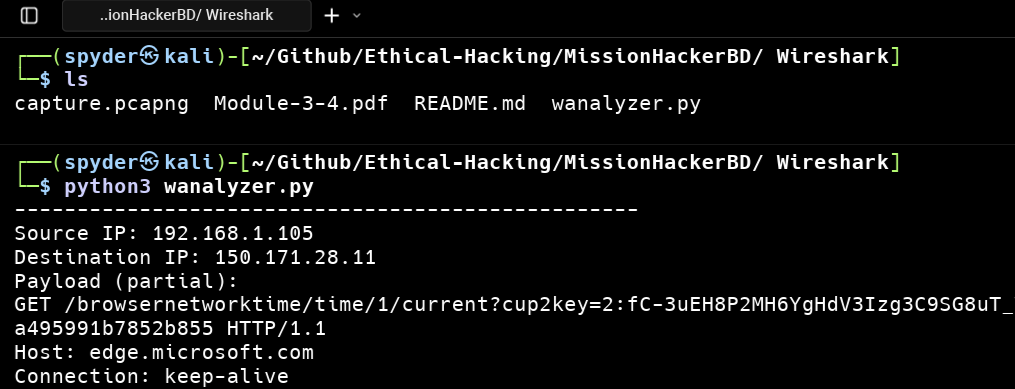
* **Analyses the Captured Packet Using Wanalyzer**

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**

Figure 5: Installing Dependencies

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

Figure 6: Running Wanalyzer

1. 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: 304602210088C3BCDE3A07314D789D55A3160993C6BA46929568D8D28B4B78584482ABFCC0022100F32CDCE3859EC2834AEBA04B2A4B3F41FB0A611C5D102F6A10244A3610229EE4:e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

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;nݦIHę"^Y(3iGX>7?qstn~=:gQ$'݅?8ٝ浑VWIr>ڋJkQ,@YrKRyuTJ1(lMƴ56׹83Y3+MŭH.i9}\ŠXAS6U!~n ̵DFS^8/332[HsU[QnՀ44:OY^rmMQW/^GP`S/

iyV 9!vVJY$qIH݆8;,/b)PiQiDB >'F^e6= F)`3%

r\_'M'\Ʋ׳

я|o斀m/޴s'OU

`KYj䔽c?EhIS[qB[/[(yӼ'\_{aMO7o

9H\o: d3ʺ,lysΟrVSj/b)o xt)\_̽9;`9pps${IxgQD'!G2U&lo\H#Jk:b.ҨQ>G<3j8ax8Rm8#C9!.)=M("<oka W4r>cFi$

2SF^4z~xpU2it1^4z8qfDjiWp\_'pd-U=U`bP5slJVaV.dc[KAd>DA W~oT'c\_zz碪^9;4<wi4<<Fz&%guUbj'O9;)O\_lֻ\[il

zha!M^q93ܬw)s04+jF@җ

c3<z7?=Kk}ҷT

g

wj GR)9AodzN9ĽrK8!\PPj`9Qy+vPU

}#P"BlxDՌ ?޹-\_|A\\*T1~Fh=Cu-u+ѧLUACf7~jllĜwho,릵ANe

MS@%H#a.)C|7m6W-qOZ&<C1?)H' @@A.6%@ȶN;@AI3pQ]u

M~.ƇxЌ,tbEȵL3\*;tݰV޴/ɿvk]F\tO|rg݅?CV'[}=mXo?t'-F4bsٛ-#w]}}8!uͻt;NS<P

cTq\_$ F

&J"t J$

[nV(/EDhx&uk]~ӄy(%P6T]Q)\4a^a]<8;\\a>\_\_xGf5p95pb!ӪiĔї|!3D2)tl

?9Aûx4j!C/||l[\*\)z<q6/tB <;|vQ

;h(x6o7ZaLo;S܋1^3lq44=N\$tue\{|Ah<>3aد?34Z.x/؍B2vI1VV

F2?̴j"vhcUڙӀk6

1&aQ)hxѰyDYыo;:lmf\I6RjeK<r|7

N/2e)nK

ū

1&L\&a-l`ʮ

<x@ڎҡ>:7FCs^J|)P9+`VZ+mL˸OS9k<+V

jˠ &CiI4'X%VF>J<H̼UlF# aoP3v1p+Xlۃg/HǱ\_9W3;>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)]**

-----------------------------------------------------------------------------------

-----------------------------------------------------------------------------------