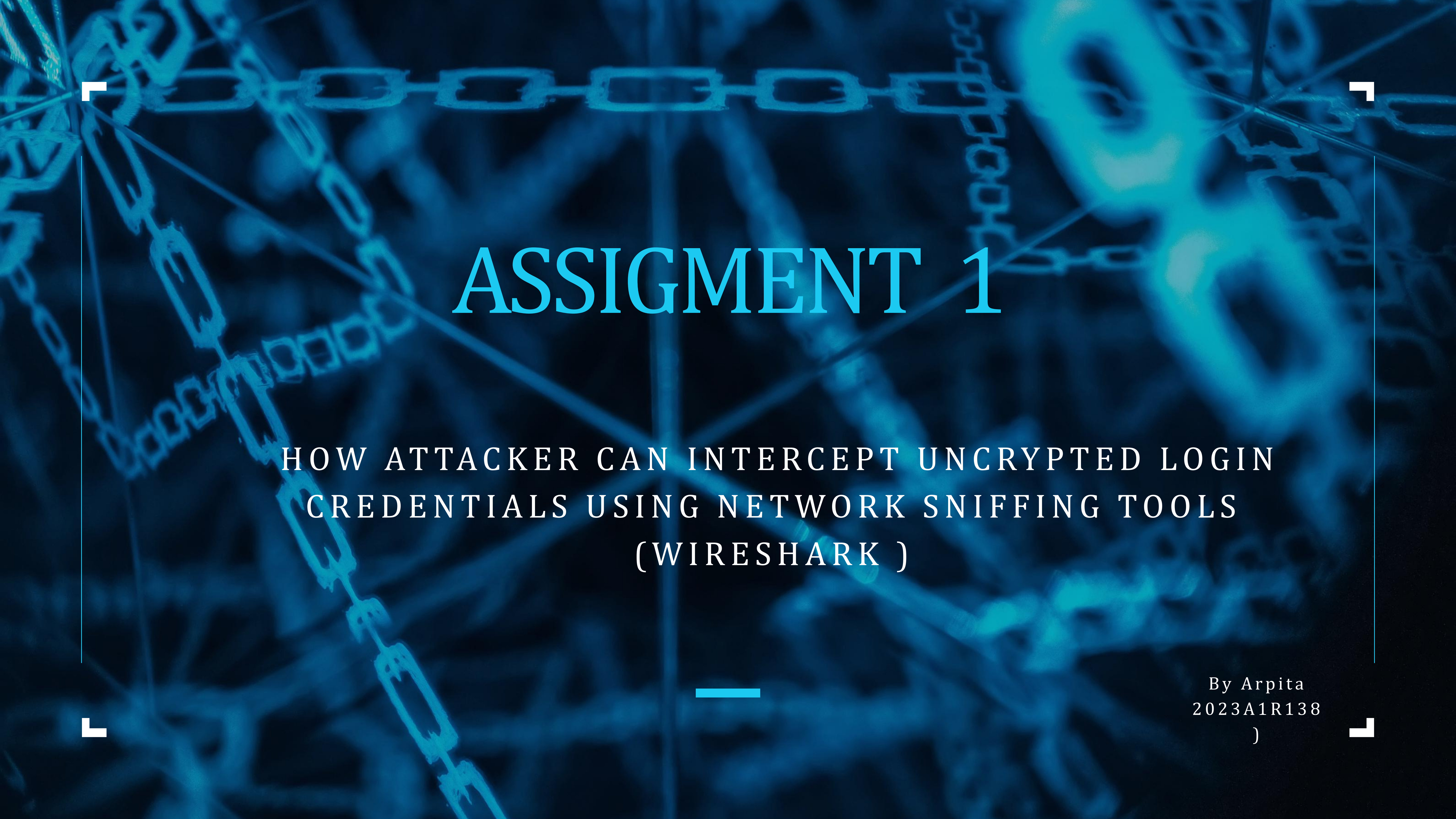
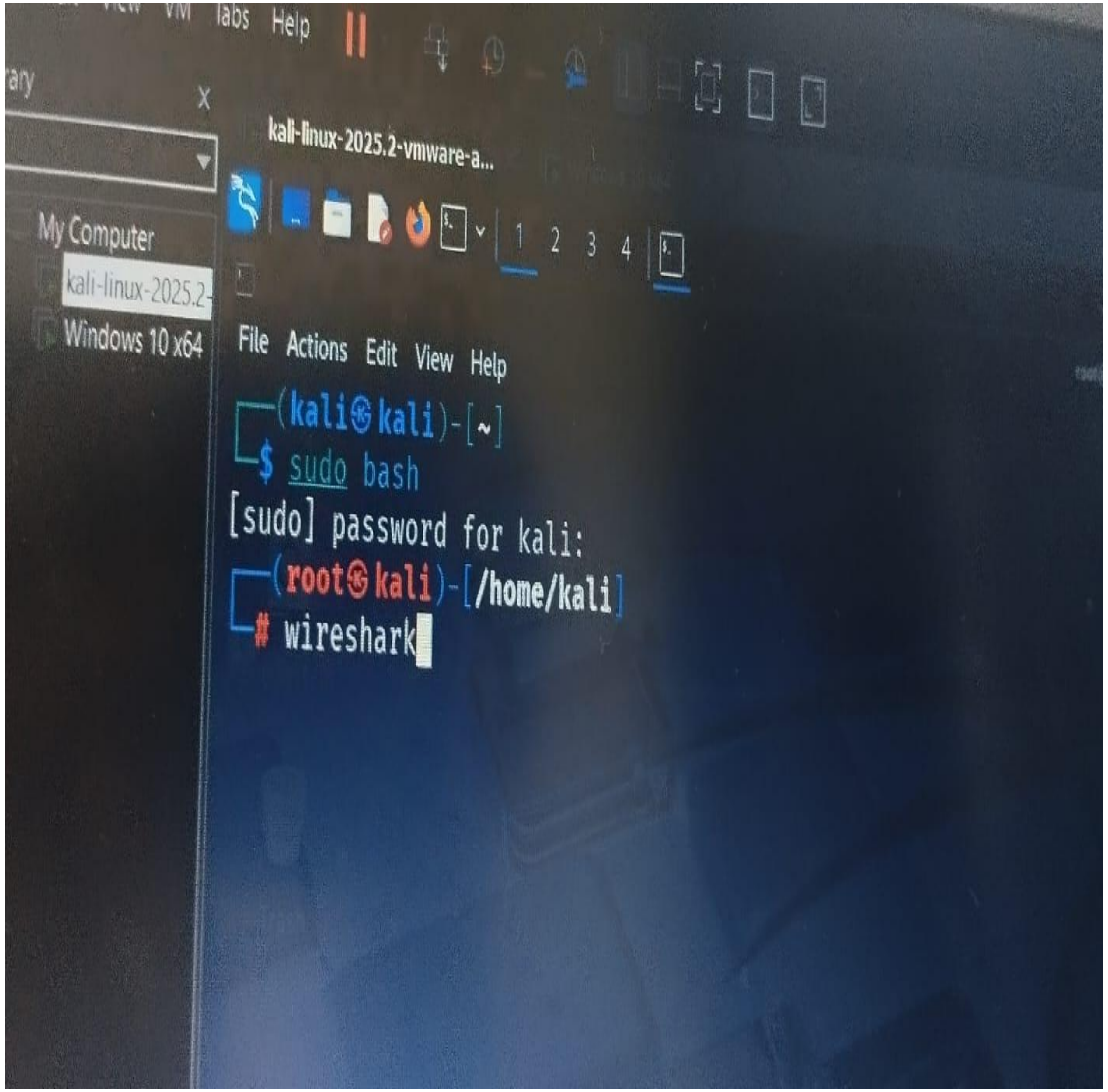


ASSIGMENT 1

HOW ATTACKER CAN INTERCEPT UNCRYPTED LOGIN CREDENTIALS USING NETWORK SNIFFING TOOLS (WIRESHARK)

By Arpita
2023A1R138
)

SNIFFING AND WIRESHARKS



```
┌──(kali㉿kali)-[~]
└─$ sudo bash
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# wireshark
```

The Terminal in Linux is a command-line interface (CLI) that allows users to interact directly with the operating system using typed commands.
It is powerful because:

What is Sniffing?

Sniffing is the process of monitoring and capturing network packets (data traffic) as they travel over a network.

TOOLS USED :

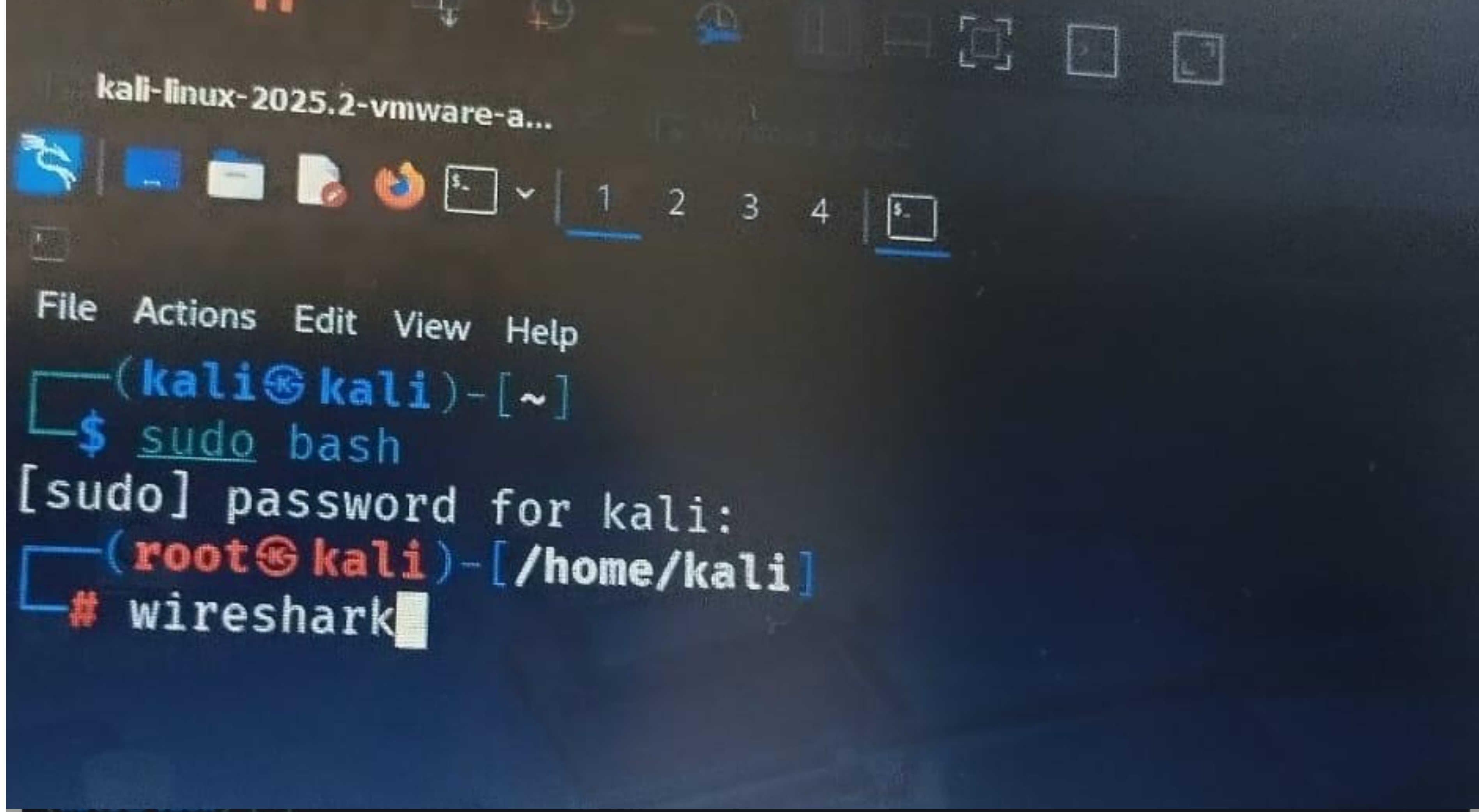
- WIRESHARK: Capture the live traffic networks(GUI)
- TCPDUMP: (CLI)a powerful command-line utility used for capturing and analyzing network traffic.

Wireshark is a free and open-source network protocol analyzer used to capture and analyze data packets in real time. It allows users to see what’s happening on a network at a deep level and is commonly used for network troubleshooting, cybersecurity analysis, and protocol development.

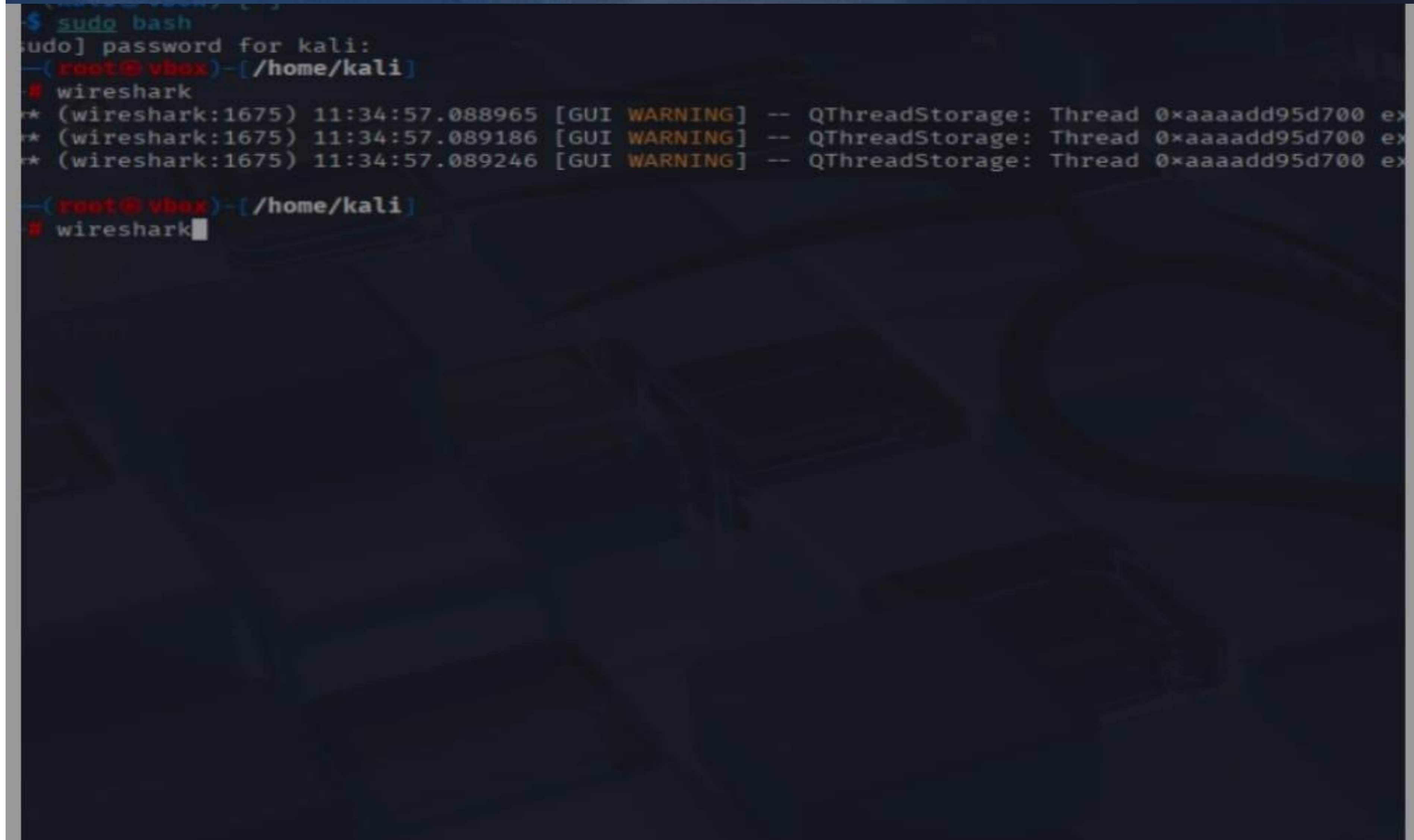
STEP 1:

OPEN TERMINAL AND RUN :

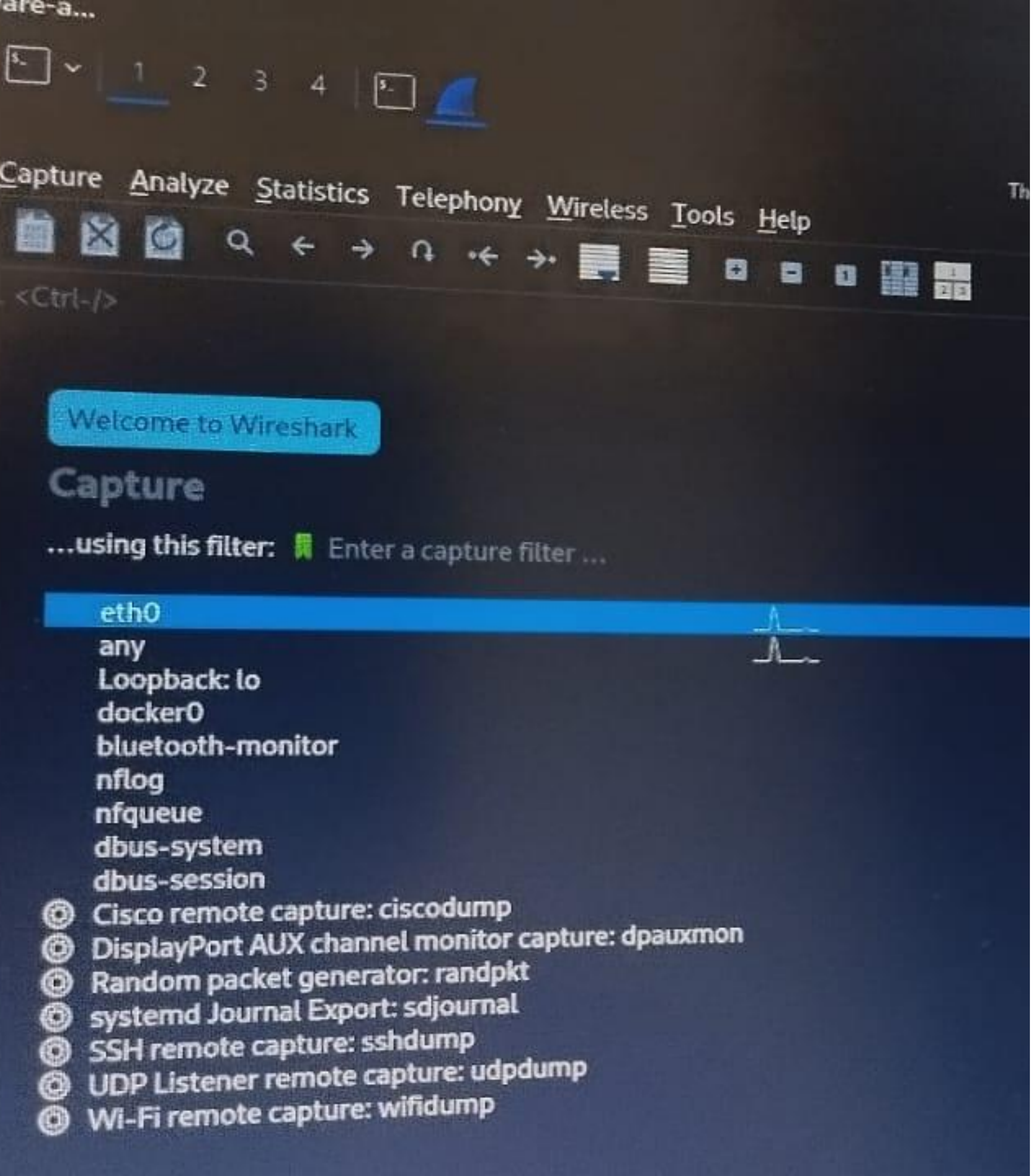
- Sudo bash
- Wireshark



```
┌──(kali㉿kali)-[~]
└─$ sudo bash
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# wireshark
```



```
-$ sudo bash
udo] password for kali:
—(root㉿vbox)-[/home/kali]
-# wireshark
* (wireshark:1675) 11:34:57.088965 [GUI WARNING] -- QThreadStorage: Thread 0×aaaadd95d700 ex
* (wireshark:1675) 11:34:57.089186 [GUI WARNING] -- QThreadStorage: Thread 0×aaaadd95d700 ex
* (wireshark:1675) 11:34:57.089246 [GUI WARNING] -- QThreadStorage: Thread 0×aaaadd95d700 ex

—(root㉿vbox)-[/home/kali]
-# wireshark
```



Capture

...using this filter: Enter a capture filter ...

eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

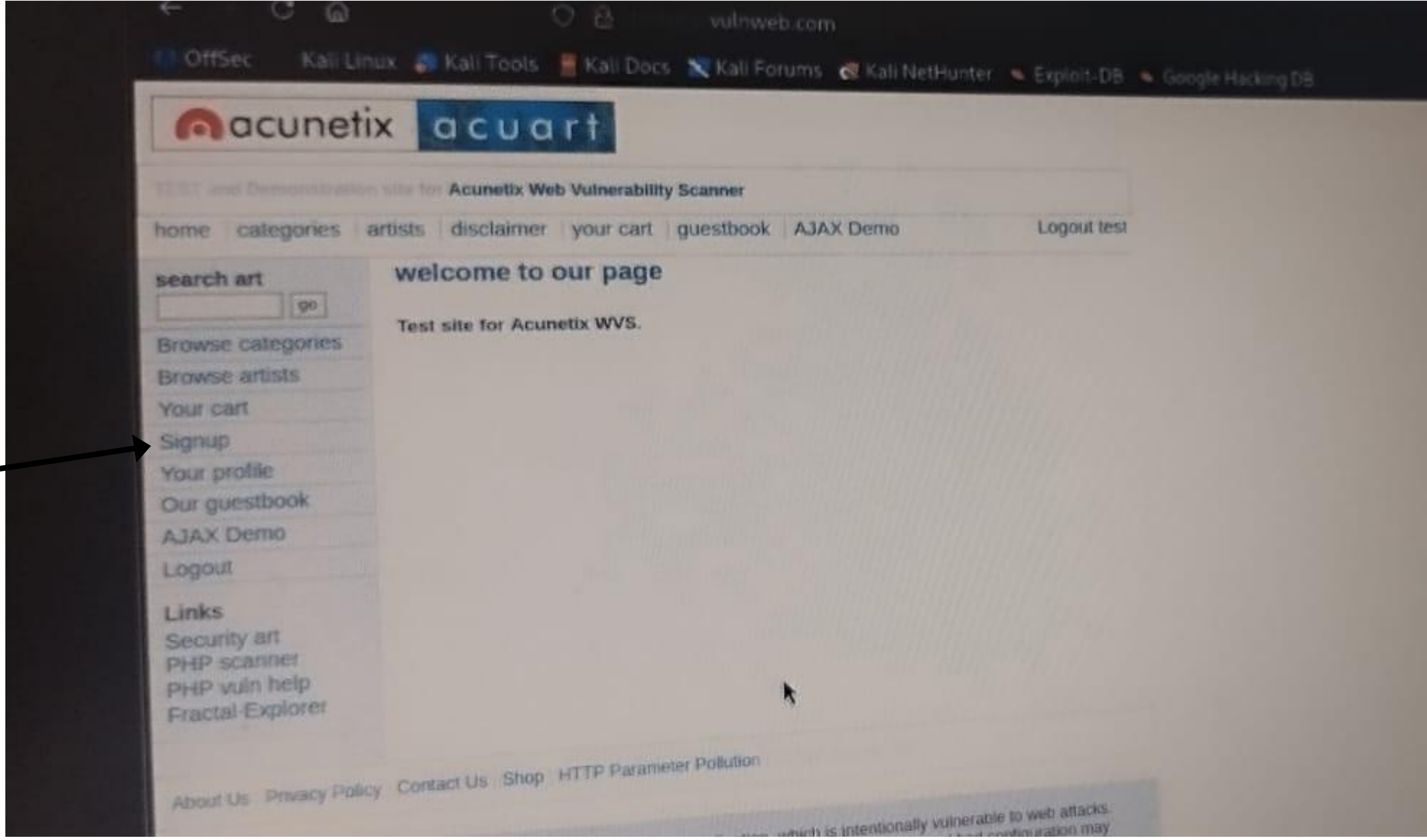
Step 2:

Choose eth0 network interface

It will Begin capturing packets form the networks

Step 3:

Open Browser and go to http://testphpvulnweb.com and click signup



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

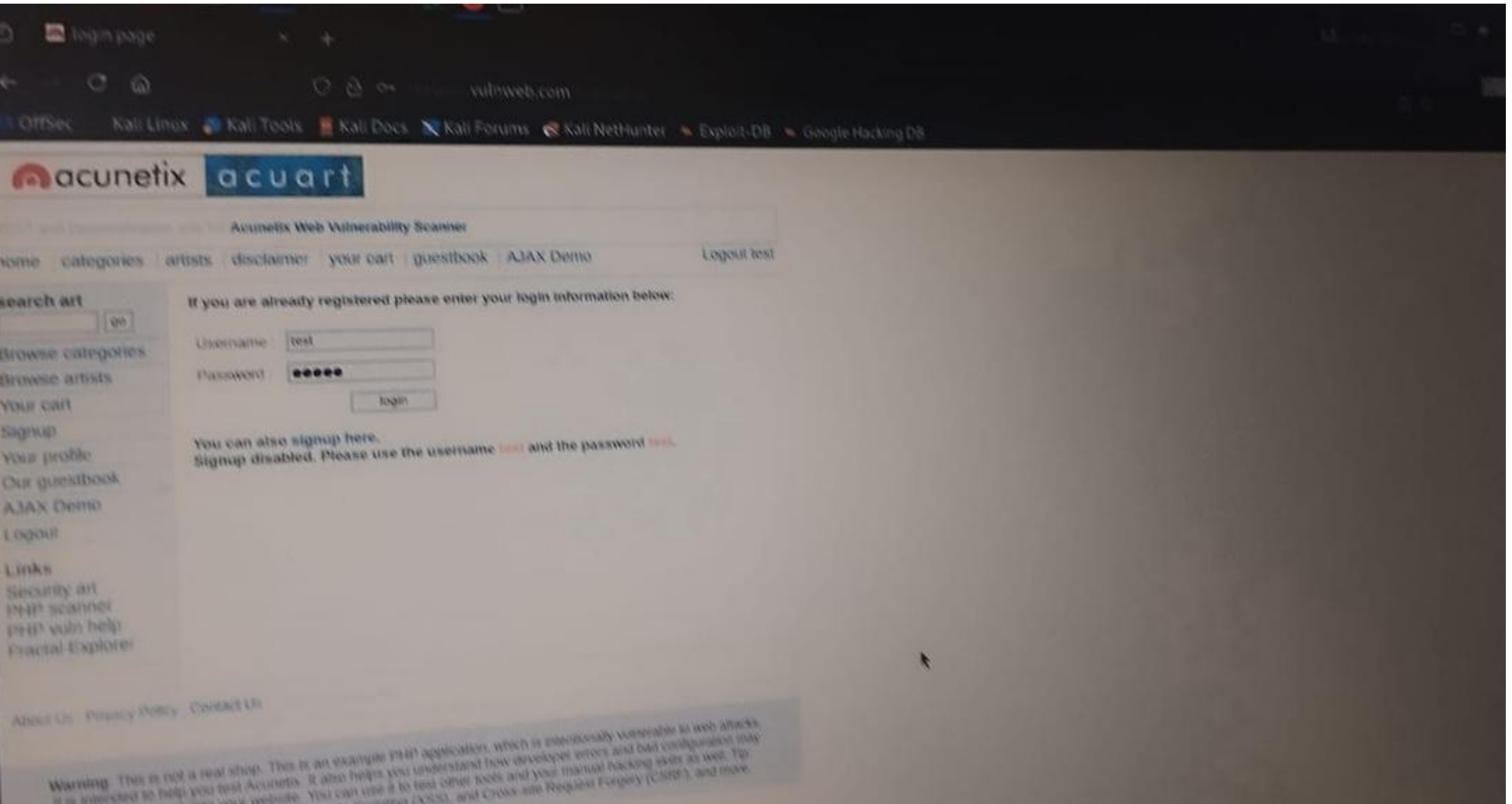
welcome to our page

Test site for Acunetix WVS.

Step 4:

go to login page .

Enter any dummy user name and password



Acunetix Web Vulnerability Scanner

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

Username: test

Password: ●●●●●

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

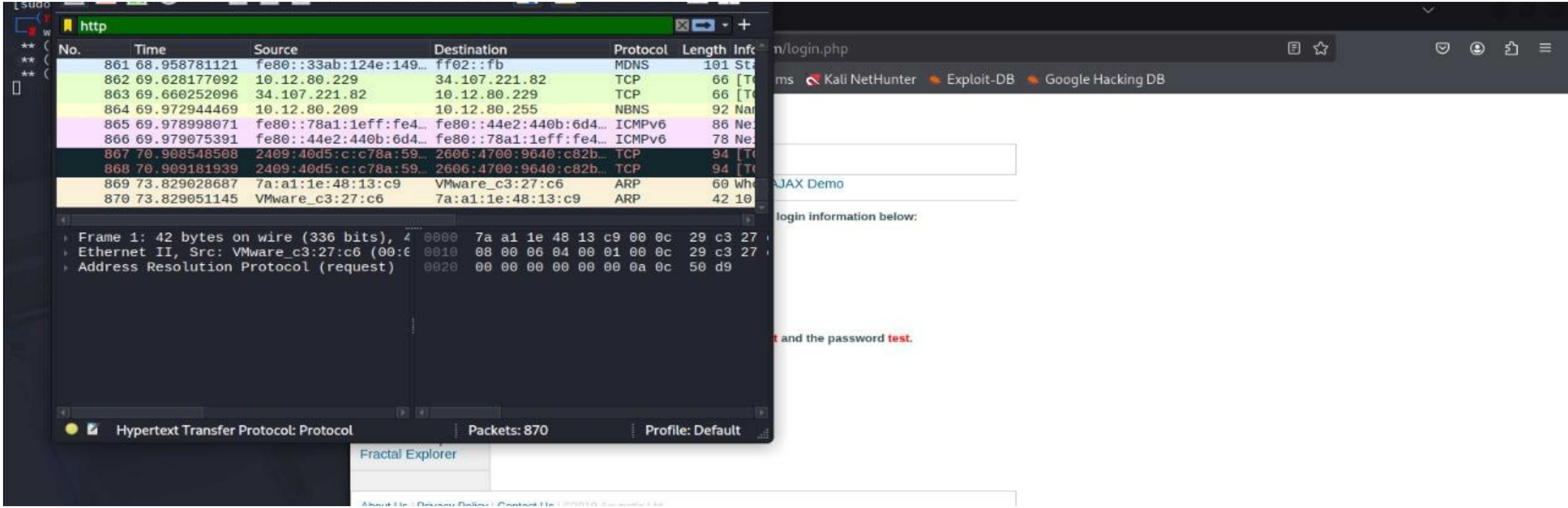
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.

Step 5:

Go back in **Wireshark**

apply filtter (ctrl F)

Select http.request.method ==”POST”
Or
Type http in filtter

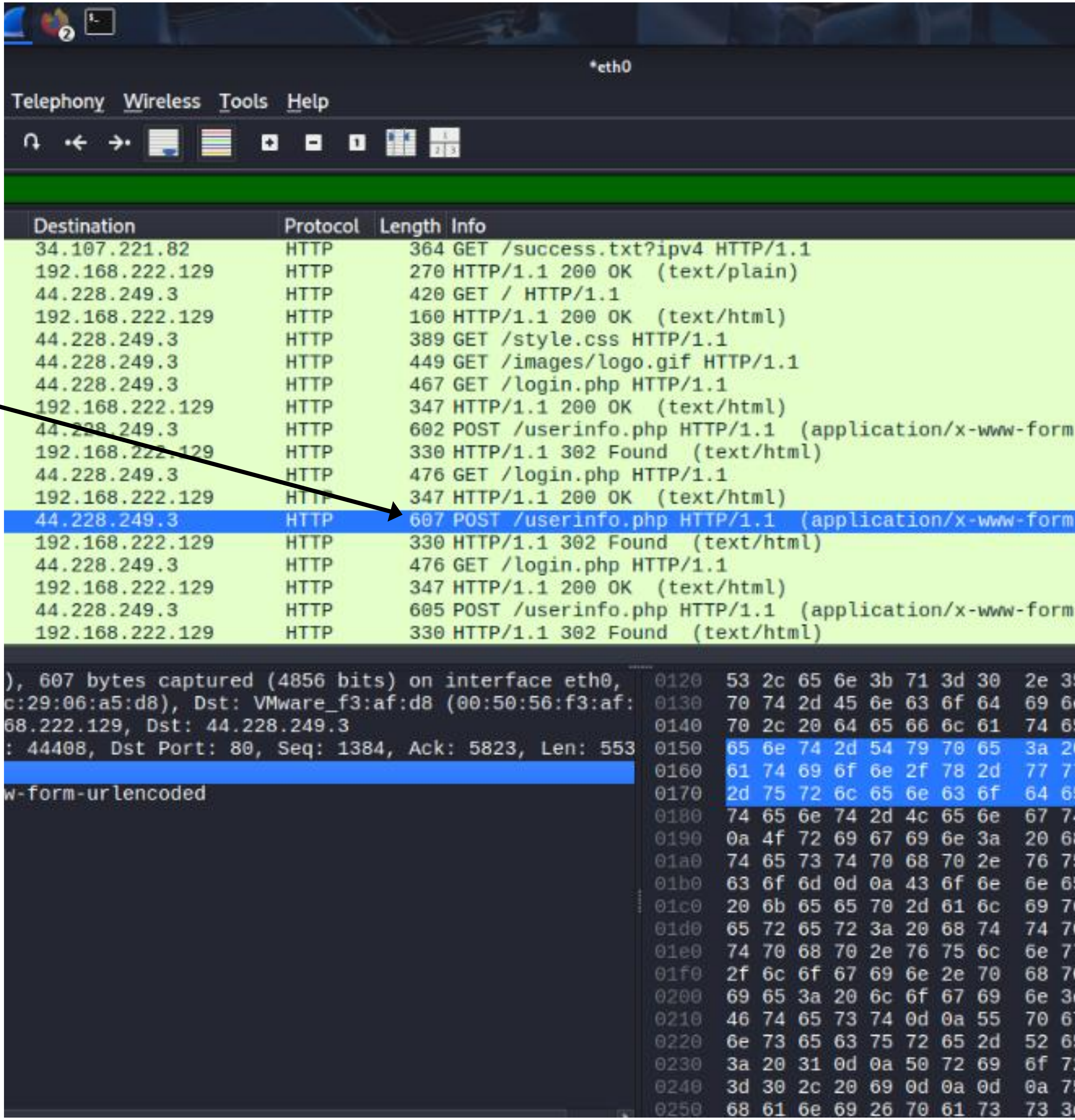


```
http
No.   Time          Source                     Destination                Protocol Length Info
  861 68.958781121  fe80::33ab:124e:149…       ff02::fb                   MDNS        101 Sta
  862 69.628177092  10.12.80.229               34.107.221.82              TCP          66 [T
  863 69.660252096  34.107.221.82              10.12.80.229               TCP          66 [T
  864 69.972944469  10.12.80.209               10.12.80.255               NBNS         92 Nar
  865 69.978998071  fe80::78a1:1eff:fe4…       fe80::44e2:440b:6d4…       ICMPv6       86 Ne
  866 69.979075391  fe80::44e2:440b:6d4…       fe80::78a1:1eff:fe4…       ICMPv6       78 Ne
  867 70.908548508  2409:40d5:c:c78a:59…       2606:4700:9640:c82b…       TCP          94 [T
  868 70.909181939  2409:40d5:c:c78a:59…       2606:4700:9640:c82b…       TCP          94 [T
  869 73.829028687  7a:a1:1e:48:13:c9          VMware_c3:27:c6            ARP          60 Whe
  870 73.829051145  VMware_c3:27:c6            7a:a1:1e:48:13:c9          ARP          42 10

 Frame 1: 42 bytes on wire (336 bits), 4    0000  7a a1 1e 48 13 c9 00 0c  29 c3 27
 Ethernet II, Src: VMware_c3:27:c6 (00:6    0010  08 00 06 04 00 01 00 0c  29 c3 27
 Address Resolution Protocol (request)      0020  00 00 00 00 00 00 0a 0c  50 d9

Hypertext Transfer Protocol: Protocol     Packets: 870     Profile: Default
```

Step 6

Right -click on the POST packets -
>
follow → HTTP Stream.

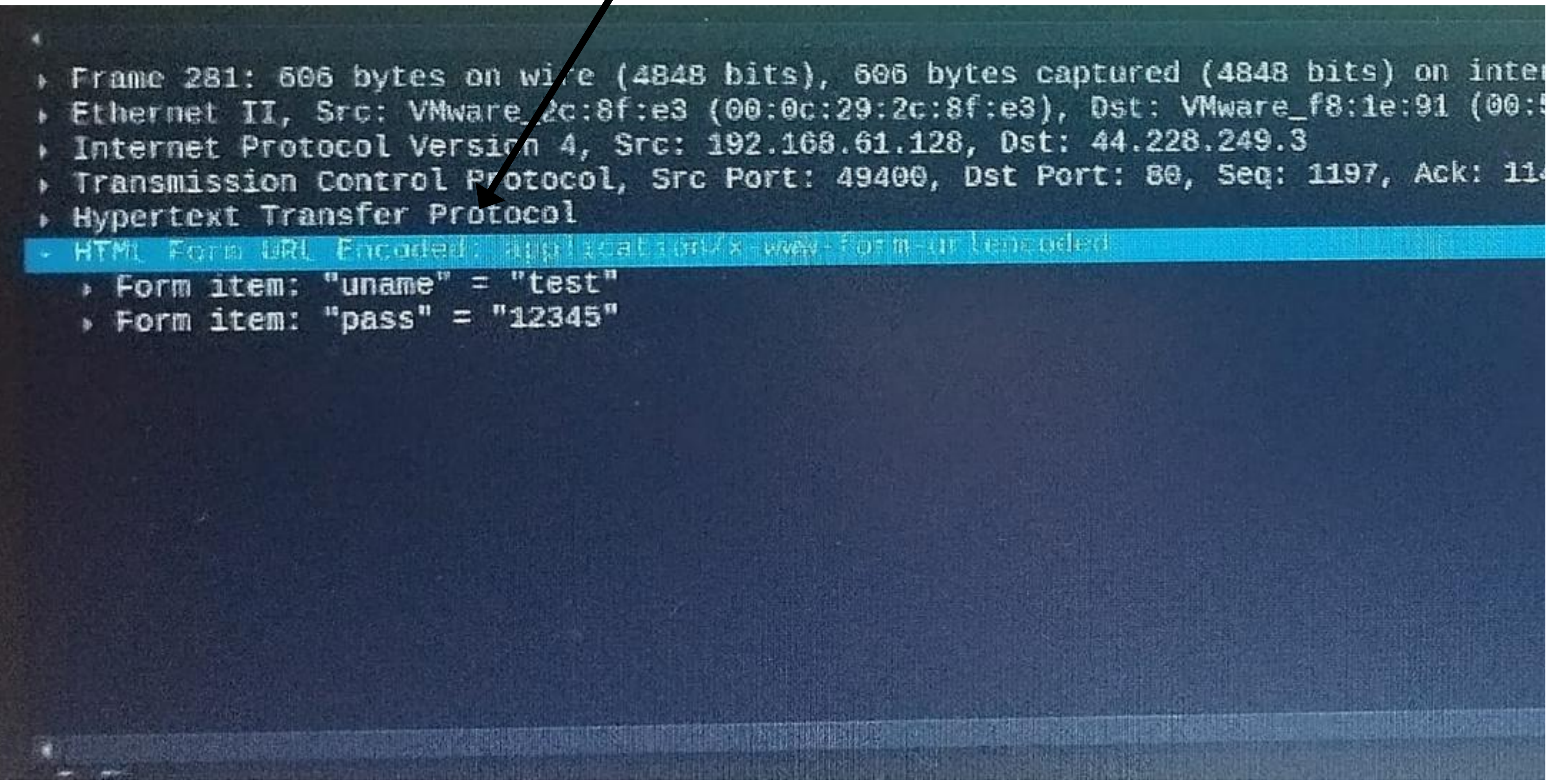
We will get user name and
password in the plain text



```
Destination         Protocol  Length Info
34.107.221.82       HTTP         364 GET /success.txt?ipv4 HTTP/1.1
192.168.222.129     HTTP         270 HTTP/1.1 200 OK  (text/plain)
44.228.249.3        HTTP         420 GET / HTTP/1.1
192.168.222.129     HTTP         160 HTTP/1.1 200 OK  (text/html)
44.228.249.3        HTTP         389 GET /style.css HTTP/1.1
44.228.249.3        HTTP         449 GET /images/logo.gif HTTP/1.1
44.228.249.3        HTTP         467 GET /login.php HTTP/1.1
192.168.222.129     HTTP         347 HTTP/1.1 200 OK  (text/html)
44.228.249.3        HTTP         602 POST /userinfo.php HTTP/1.1  (application/x-www-form
192.168.222.129     HTTP         330 HTTP/1.1 302 Found  (text/html)
44.228.249.3        HTTP         476 GET /login.php HTTP/1.1
192.168.222.129     HTTP         347 HTTP/1.1 200 OK  (text/html)
44.228.249.3        HTTP         607 POST /userinfo.php HTTP/1.1  (application/x-www-form
192.168.222.129     HTTP         330 HTTP/1.1 302 Found  (text/html)
44.228.249.3        HTTP         476 GET /login.php HTTP/1.1
192.168.222.129     HTTP         347 HTTP/1.1 200 OK  (text/html)
44.228.249.3        HTTP         605 POST /userinfo.php HTTP/1.1  (application/x-www-form
192.168.222.129     HTTP         330 HTTP/1.1 302 Found  (text/html)
```

```
), 607 bytes captured (4856 bits) on interface eth0,
c:29:06:a5:d8), Dst: VMware_f3:af:d8 (00:50:56:f3:af:
68.222.129, Dst: 44.228.249.3
: 44408, Dst Port: 80, Seq: 1384, Ack: 5823, Len: 553

w-form-urlencoded
```

```
0120  53 2c 65 6e 3b 71 3d 30  2e 3
0130  70 74 2d 45 6e 63 6f 64  69 6
0140  70 2c 20 64 65 66 6c 61  74 6
0150  65 6e 74 2d 54 79 70 65  3a 2
0160  61 74 69 6f 6e 2f 78 2d  77 7
0170  2d 75 72 6c 65 6e 63 6f  64 6
0180  74 65 6e 74 2d 4c 65 6e  67 7
0190  0a 4f 72 69 67 69 6e 3a  20 6
01a0  74 65 73 74 70 68 70 2e  76 7
01b0  63 6f 6d 0d 0a 43 6f 6e  6e 6
01c0  20 6b 65 65 70 2d 61 6c  69 7
01d0  65 72 65 72 3a 20 68 74  74 7
01e0  74 70 68 70 2e 76 75 6c  6e 7
01f0  2f 6c 6f 67 69 6e 2e 70  68 7
0200  69 65 3a 20 6c 6f 67 69  6e 3
0210  46 74 65 73 74 0d 0a 55  70 6
0220  6e 73 65 63 75 72 65 2d  52 6
0230  3a 20 31 0d 0a 50 72 69  6f 7
0240  3d 30 2c 20 69 0d 0a 0d  0a 7
0250  68 61 6e 69 26 70 61 73  73 3
```



```
› Frame 281: 606 bytes on wire (4848 bits), 606 bytes captured (4848 bits) on inter
› Ethernet II, Src: VMware_2c:8f:e3 (00:0c:29:2c:8f:e3), Dst: VMware_f8:1e:91 (00:5
› Internet Protocol Version 4, Src: 192.168.61.128, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 49400, Dst Port: 80, Seq: 1197, Ack: 11
› Hypertext Transfer Protocol
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
    › Form item: "uname" = "test"
    › Form item: "pass" = "12345"
```

THANK YOU