

OPEN SOURCES TECHNOLOGIES

CA: 3



L OVELY
P ROFESSIONAL
U NIVERSITY

Transforming Education Transforming India

Name : Banagani Prashanth

Reg No : 11906733

Course Code : INT301

Roll No : 44

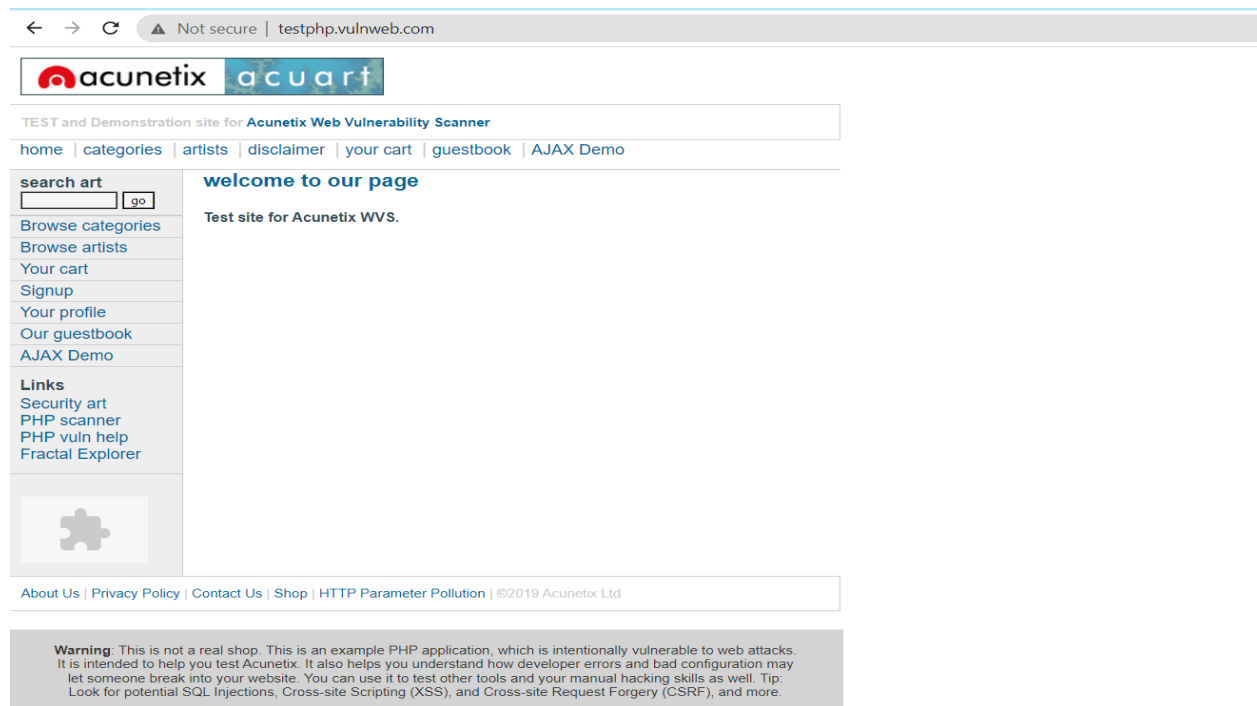
Section : KE011

Q : Suppose you are a network analyst and implemented the sensor inside the firewall, working in the Infotech department of LPU. You have been assigned the responsibility of inspecting HTTP Traffic and retrieving the Username and password from <http://testphp.vulnweb.com/> website. Write the steps involved in scanning the port.

As network analysts, we can use a network protocol analyzer tool like Wireshark to inspect HTTP traffic and retrieve the username and password from the <http://testphp.vulnweb.com/> website.

Wireshark is a free and open-source network protocol analyzer. It is used for network troubleshooting, analysis, software and communications protocol development. It can capture packets from a network connection in real-time and display them at a granular level. Once these packets are broken down, you can use them for real-time or offline analysis.

We need to open the website in our search engine to verify its IP address while performing these tasks



To check the IP address of the website, we are going to use the ping command through the command prompt.

Command : ping testphp.vulnweb.com

```
Command Prompt
Microsoft Windows [Version 10.0.22621.1413]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Asus>ping testphp.vulnweb.com

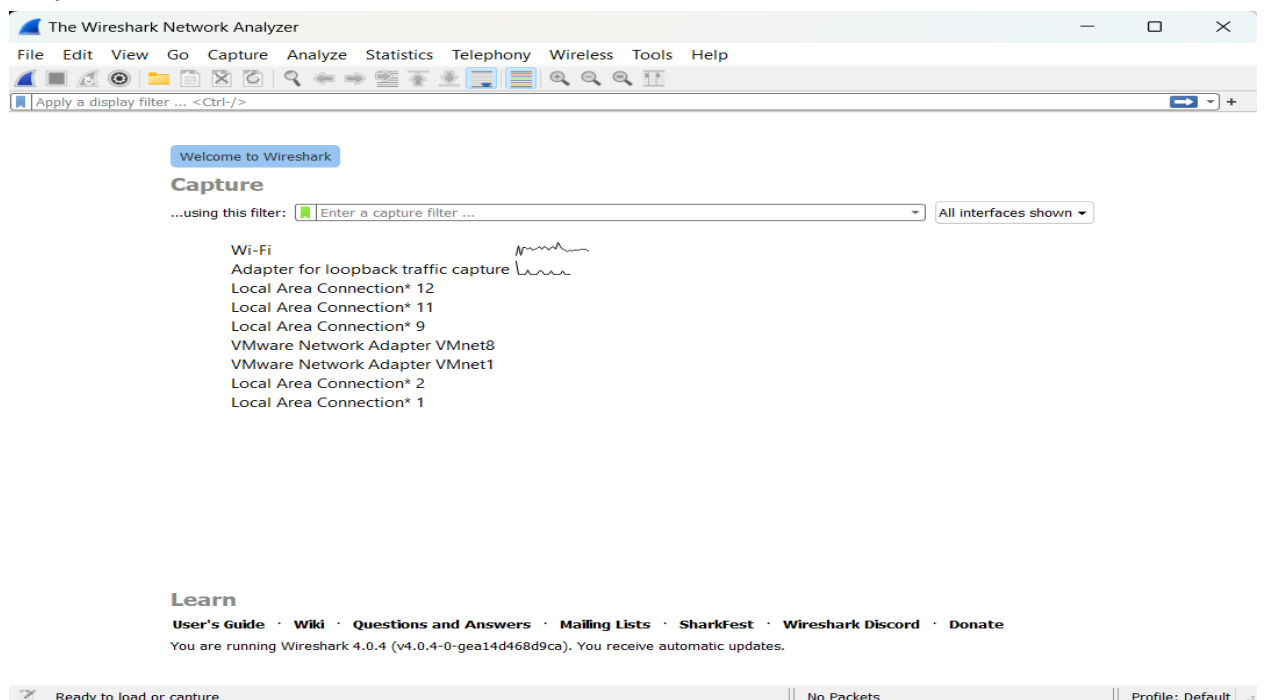
Pinging testphp.vulnweb.com [44.228.249.3] with 32 bytes of data:
Reply from 44.228.249.3: bytes=32 time=367ms TTL=34
Reply from 44.228.249.3: bytes=32 time=339ms TTL=34
Reply from 44.228.249.3: bytes=32 time=331ms TTL=34
Reply from 44.228.249.3: bytes=32 time=299ms TTL=34

Ping statistics for 44.228.249.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 299ms, Maximum = 367ms, Average = 334ms

C:\Users\Asus>
```

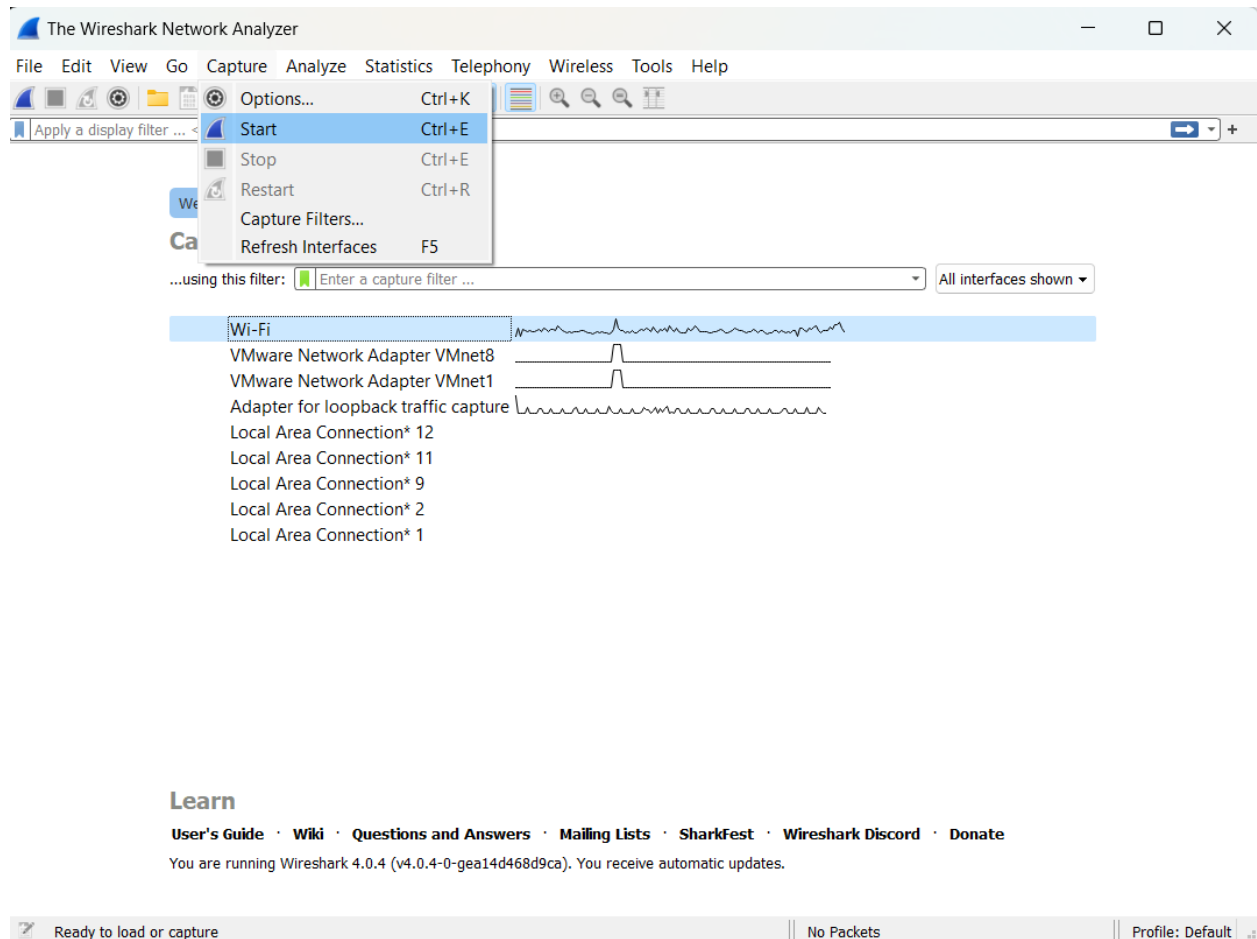
Follow these steps to inspect HTTP traffic and retrieve the username and password from the website:

1.Open Wireshark.



1. In the main window, you will see a list of available network interfaces under the “Capture” section.
2. Identify the network interface that is connected to the internet. It could be a wired or wireless connection and is usually labeled as “Ethernet” or “Wi-Fi”.
3. Click on the interface to select it.

Once you have selected the network interface, you can start capturing packets by clicking on the “Start Capture” button.



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [Sharkfest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.0.4 (v4.0.4-0-gea14d468d9ca). You receive automatic updates.

After Clicking on start capture button:

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
1587	14.703273	172.22.50.135	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1588	14.704799	172.22.50.189	224.0.0.251	MDNS	103	Standard query 0x0024 PTR _233637DE._s
1589	14.712626	fe80::84a6:115:a6ba...	ff02::1:ff45:b780	ICMPv6	86	Neighbor Solicitation for fe80::fac1::
1590	14.767334	172.22.49.104	224.0.0.251	MDNS	154	Standard query 0x0000 PTR _homekit._t
1591	14.768820	fe80::1445:468b:6e1...	ff02::fb	MDNS	174	Standard query 0x0000 PTR _homekit._t
1592	14.860781	172.22.51.203	224.0.0.251	MDNS	484	Standard query response 0x0000 TXT, ca
1593	14.901433	172.22.49.122	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1594	14.924184	172.22.48.127	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
1595	14.954988	CloudNet_89:ae:e9	LiteonTe_40:ba:72	ARP	60	Who has 172.22.48.1? Tell 172.22.50.1
1596	15.004886	JuniperN_45:b7:80	LiteonTe_40:ba:72	ARP	60	Who has 172.22.48.197? Tell 172.22.48.
1597	15.061463	fe80::37b7:dd1b:a31...	ff02::1:ff45:b780	ICMPv6	86	Neighbor Solicitation for fe80::fac1::
1598	15.069836	HonHaiPr_c2:36:e1	LiteonTe_40:ba:72	ARP	60	Who has 172.22.52.46? Tell 172.22.52.

> Frame 1: 147 bytes on wire (1176 bits), 147 bytes captured
 > Ethernet II, Src: IntelCor_9d:40:3b (80:38:fb:9d:40:3b),
 > Internet Protocol Version 6, Src: fe80::45af:ace5:2efd:c
 > User Datagram Protocol, Src Port: 546, Dst Port: 547
 > DHCPv6

```

0000 30 d1 6b 40 ba 72 80 38 fb 9d 40 3b 86 dd 60 09 0
0010 c4 c8 00 5d 11 01 fe 80 00 00 00 00 00 00 45 af
0020 ac e5 2e fd cb 40 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 01 00 02 02 22 02 23 00 5d e6 57 01 04
0040 b0 29 00 08 00 02 18 a2 00 01 00 0e 00 01 00 01
0050 2a d2 2c f5 80 38 fb 9d 40 3b 00 03 00 0c 05 80
0060 38 fb 00 00 00 00 00 00 00 00 00 27 00 07 00 05
0070 52 6f 68 69 74 00 10 00 0e 00 00 01 37 00 08 4d
0080 53 46 54 20 35 2e 30 00 06 00 08 00 11 00 17 00
0090 18 00 27
  
```

Wi-Fi: <live capture in progress> | Packets: 1598 · Displayed: 1598 (100.0%) | Profile: Default

After you have started capturing packets and entered “http” in the filter bar to display only HTTP traffic, look for packets in the packet list pane that have the “POST” method in the “Info” column.

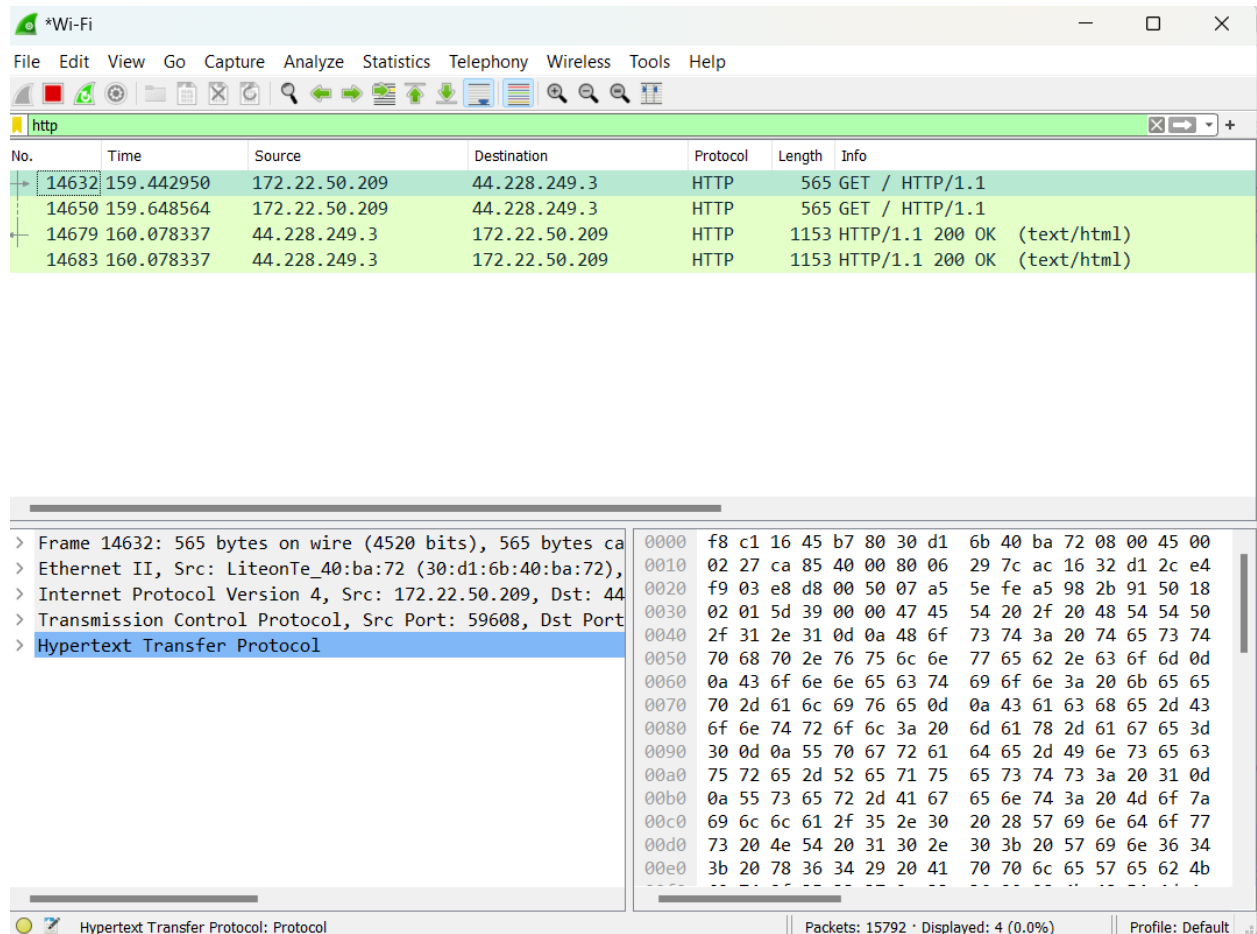
Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
10728	118.043963	172.22.50.209	13.33.88.75	TLSv1.2	180	Client Key Exchange, Change Cipher Spec
10729	118.043858	IntelCor_d1:7d:74	LiteonTe_40:ba:72	ARP	60	ARP Announcement for 172.22.49.134
10728	118.045793	172.22.50.96	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
10729	118.104369	fe80::c419:10d4:365...	ff02::1:2	DHCPv6	157	Solicit XID: 0x0f511f CID: 0001000127
10730	118.159276	fe80::99b7:8f68:5f4...	ff02::1:ff45:b780	ICMPv6	86	Neighbor Solicitation for fe80::fac1::
10731	118.170938	13.33.88.75	172.22.50.209	TCP	60	443 → 59556 [ACK] Seq=5418 Ack=375 Win
10732	118.170938	13.33.88.75	172.22.50.209	TLSv1.2	105	Change Cipher Spec, Encrypted Handshak
10733	118.171577	172.22.50.209	13.33.88.75	TLSv1.2	257	Application Data
10734	118.183135	AzureWav_f4:43:cb	LiteonTe_40:ba:72	ARP	60	ARP Announcement for 172.22.49.219
10735	118.184595	172.22.49.165	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
10736	118.184595	172.22.49.165	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
10737	118.199949	172.22.50.182	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

If you see a packet with the “POST” method, select it by clicking on it.



The image shows a Wireshark capture window titled "*Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A packet list table is displayed with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
14632	159.442950	172.22.50.209	44.228.249.3	HTTP	565	GET / HTTP/1.1
14650	159.648564	172.22.50.209	44.228.249.3	HTTP	565	GET / HTTP/1.1
14679	160.078337	44.228.249.3	172.22.50.209	HTTP	1153	HTTP/1.1 200 OK (text/html)
14683	160.078337	44.228.249.3	172.22.50.209	HTTP	1153	HTTP/1.1 200 OK (text/html)



Below the packet list, the details pane shows the selected packet (14632) with the following structure:

- > Frame 14632: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on interface 0
- > Ethernet II, Src: LiteonTe_40:ba:72 (30:d1:6b:40:ba:72), Dst: 44:22:82:49:33:37
- > Internet Protocol Version 4, Src: 172.22.50.209, Dst: 44.228.249.3
- > Transmission Control Protocol, Src Port: 59608, Dst Port: 80
- > Hypertext Transfer Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The status bar at the bottom indicates "Packets: 15792 · Displayed: 4 (0.0%)".

If you don't see any packets with the “POST” method while capturing HTTP traffic in Wireshark, it could mean that no data is being sent to the server from the website you are trying to inspect. Try refreshing the website or performing an action on the website that would send data to the server, such as submitting a form or logging in.

← → ↻ Not secure | testphp.vulnweb.com/signup.php



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

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



Signup new user

Please do not enter real information here.
If you press the submit button you will be transferred to a secured connection.

Username:

Password:

Retype password:

Name:

Credit card number:

E-Mail:

Phone number:

Address:

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

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.

After signing up :

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
14632	159.442950	172.22.50.209	44.228.249.3	HTTP	565	GET / HTTP/1.1
14650	159.648564	172.22.50.209	44.228.249.3	HTTP	565	GET / HTTP/1.1
14679	160.078337	44.228.249.3	172.22.50.209	HTTP	1153	HTTP/1.1 200 OK (text/html)
14683	160.078337	44.228.249.3	172.22.50.209	HTTP	1153	HTTP/1.1 200 OK (text/html)
19833	220.204622	172.22.50.209	44.228.249.3	HTTP	586	GET /login.php HTTP/1.1
19866	220.524999	44.228.249.3	172.22.50.209	HTTP	1342	HTTP/1.1 200 OK (text/html)
20162	223.940325	172.22.50.209	44.228.249.3	HTTP	596	GET /signup.php HTTP/1.1
20204	224.268652	44.228.249.3	172.22.50.209	HTTP	1402	HTTP/1.1 200 OK (text/html)
29580	332.608049	172.22.50.209	44.228.249.3	HTTP	872	POST /secured/newuser.php HTTP/1.1 (application/x-www-form-urlencoded)
29626	332.910577	44.228.249.3	172.22.50.209	HTTP	815	HTTP/1.1 200 OK (text/html)

> Frame 14632: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on 0
> Ethernet II, Src: LiteonTe_40:ba:72 (30:d1:6b:40:ba:72), Dst: JuniperN_45:00:00:00:00:00
> Internet Protocol Version 4, Src: 172.22.50.209, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 59608, Dst Port: 80, Seq: 1, Ack: 34875, Win: 65535, Len: 565
> Hypertext Transfer Protocol

0000 f8 c1 16 45 b7 80 30 d1 6b 40 ba 72 08 00 45 00 ...E...k@.r..E
0010 02 27 ca 85 40 00 80 06 29 7c ac 16 32 d1 2c e4 ...@...)]..2.,
0020 f9 03 e8 d8 00 50 07 a5 5e fe a5 98 2b 91 50 18P...^...+P..
0030 02 01 5d 39 00 00 47 45 54 20 2f 20 48 54 54 50 ...]9...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 /1.1..Ho st: test
0050 70 68 70 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d php.vuln web.com.
0060 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 -Connect ion: kee
0070 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 p-alive- .Cache-C
0080 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d ontrol: max-age=
0090 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 0..Upgra de-Insec
00a0 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d ure-Requ ests: 1-
00b0 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a -User-Ag ent: Moz

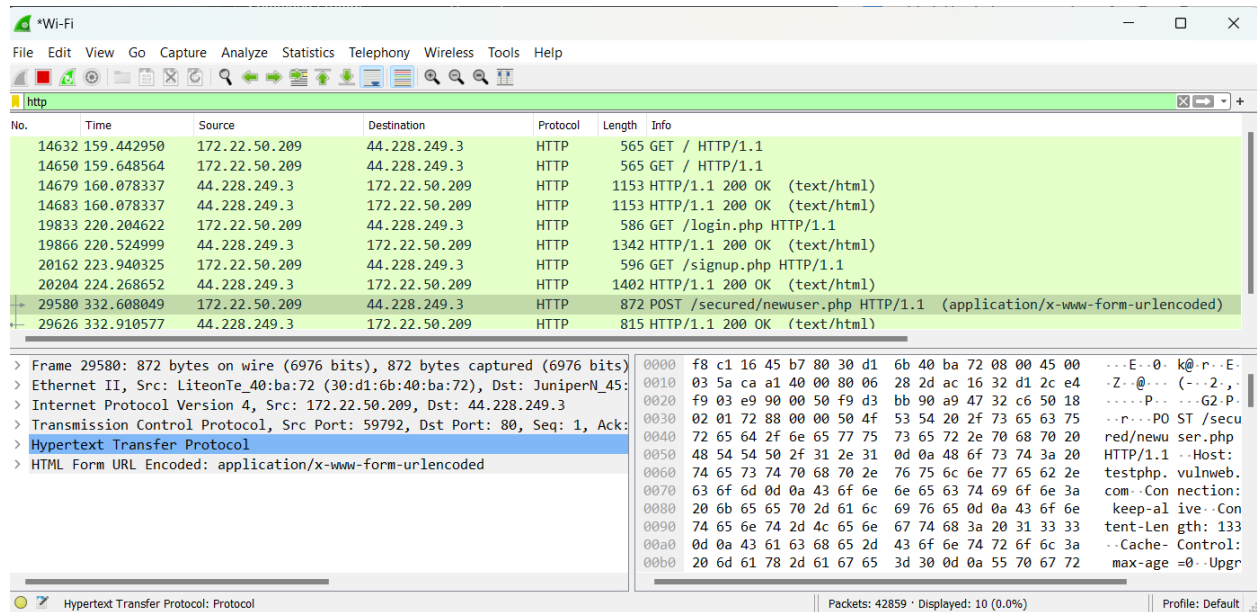
Hypertext Transfer Protocol: Protocol

Packets: 34875 · Displayed: 10 (0.0%)

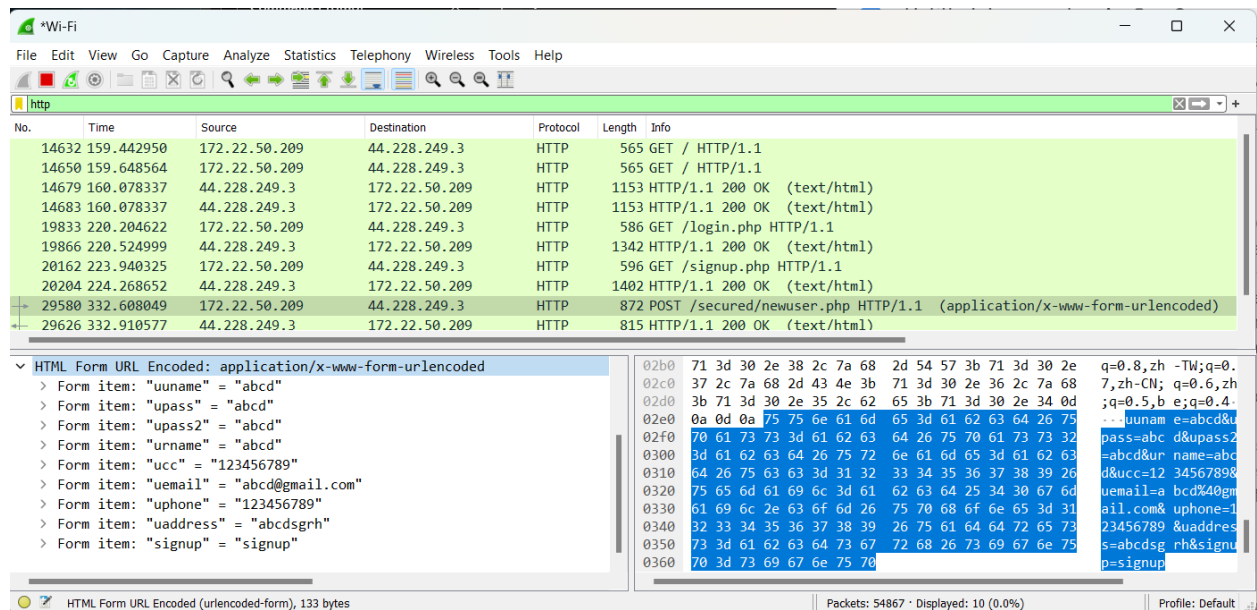
Profile: Default

Now that you can see packets with the “POST” method in Wireshark, you can proceed to the next step which is to select the packet and expand the “Hypertext Transfer Protocol” section in the packet details pane. Here’s how you can do it:

1. Select the packet with the “POST” method by clicking on it in the packet list pane.
2. In the packet details pane, look for the “Hypertext Transfer Protocol” section and click on the “>” icon next to it to expand it.



3. Look for the “Form item” field which contains the username and password



The “Form item” field in the “Hypertext Transfer Protocol” section of a packet in Wireshark displays the data that is being sent to the server from a form on a website.

The field is usually labeled with the name of the form input element, such as “username” or “password”.

To identify which “Form item” field contains the username and password, you can look for fields that are labeled with names that are commonly used for username and password input elements, such as “username”, “user”, “email”, “login”, “password”, “pass”, etc.

Once you have identified the “Form item” fields that contain the username and password, you can view their values to retrieve the information.

Wireshark is a powerful tool that can be used to inspect HTTP traffic and retrieve information such as usernames and passwords from websites. By following the steps outlined in this report, a network analyst can successfully use Wireshark to capture packets, filter HTTP traffic, and identify packets with the “POST” method to retrieve the desired information. This demonstrates the usefulness of Wireshark as a network protocol analyzer for troubleshooting and analysis purposes.