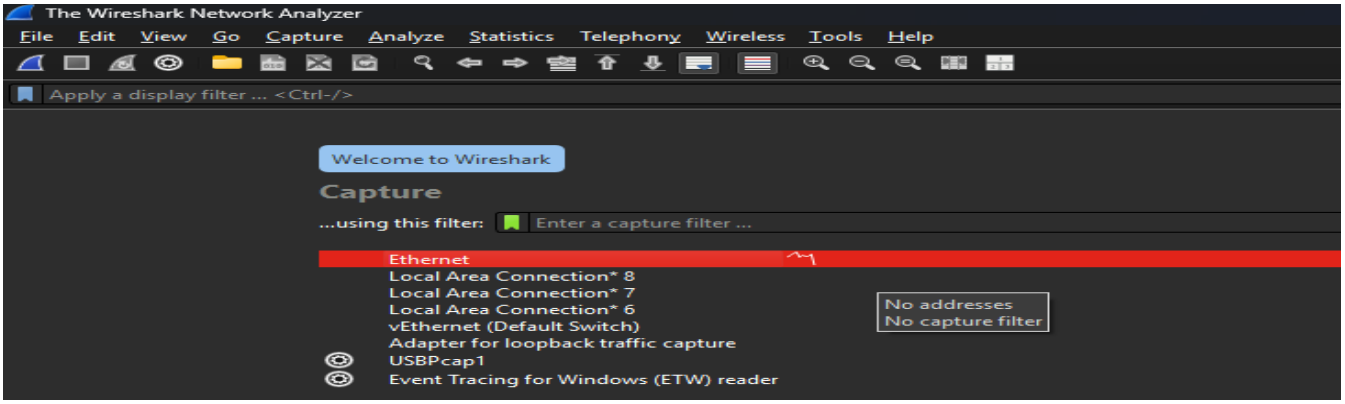
9112 Sudiksha Tawde
TYCS C

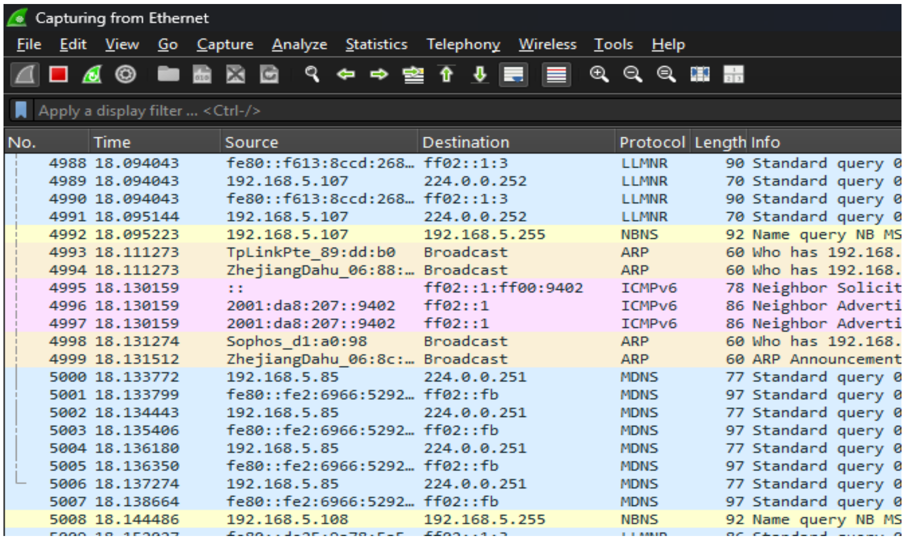
PRACTICAL - 5 (A)

AIM : Use Wireshrap (sniffer)to capture network traffic and analyze

STEP 1: Open Wireshark and click on the Ethernet OR Wifi option then it will open the page .

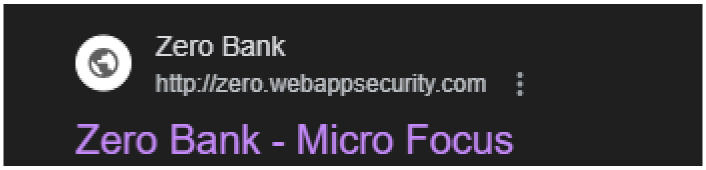

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
No addresses
No capture filter

Ethernet
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
vEthernet (Default Switch)
Adapter for loopback traffic capture
USBPcap1
Event Tracing for Windows (ETW) reader


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

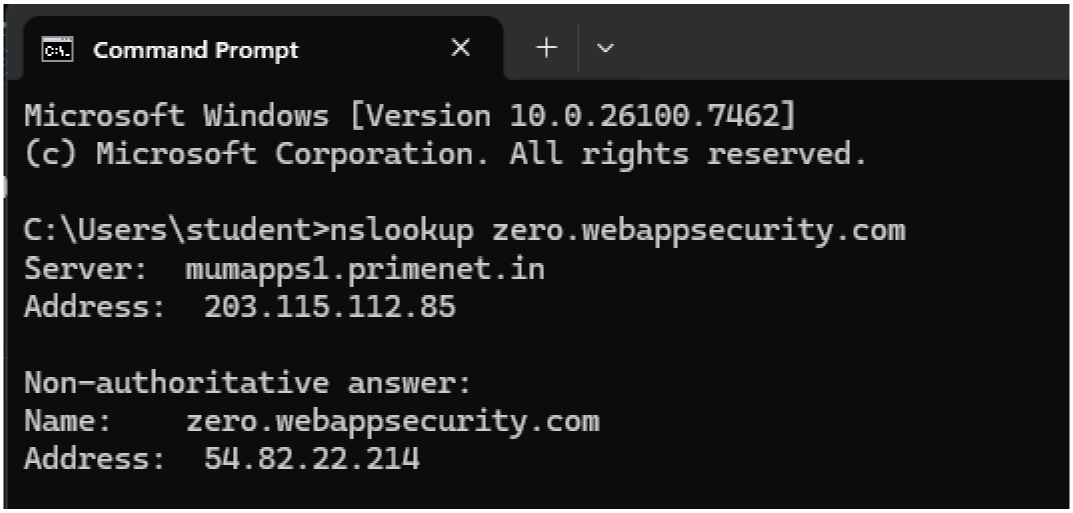
No.	Time	Source	Destination	Protocol	Length	Info
4988	18.094043	fe80::f613:8ccd:268…	ff02::1:3	LLMNR	90	Standard query 0
4989	18.094043	192.168.5.107	224.0.0.252	LLMNR	70	Standard query 0
4990	18.094043	fe80::f613:8ccd:268…	ff02::1:3	LLMNR	90	Standard query 0
4991	18.095144	192.168.5.107	224.0.0.252	LLMNR	70	Standard query 0
4992	18.095223	192.168.5.107	192.168.5.255	NBNS	92	Name query NB MS
4993	18.111273	TpLinkPte_89:dd:b0	Broadcast	ARP	60	Who has 192.168.
4994	18.111273	ZhejiangDahu_06:88:…	Broadcast	ARP	60	Who has 192.168.
4995	18.130159	::	ff02::1:ff00:9402	ICMPv6	78	Neighbor Solicit
4996	18.130159	2001:da8:207::9402	ff02::1	ICMPv6	86	Neighbor Adverti
4997	18.130159	2001:da8:207::9402	ff02::1	ICMPv6	86	Neighbor Adverti
4998	18.131274	Sophos_d1:a0:98	Broadcast	ARP	60	Who has 192.168.
4999	18.131512	ZhejiangDahu_06:8c:…	Broadcast	ARP	60	ARP Announcement
5000	18.133772	192.168.5.85	224.0.0.251	MDNS	77	Standard query 0
5001	18.133799	fe80::fe2:6966:5292…	ff02::fb	MDNS	97	Standard query 0
5002	18.134443	192.168.5.85	224.0.0.251	MDNS	77	Standard query 0
5003	18.135406	fe80::fe2:6966:5292…	ff02::fb	MDNS	97	Standard query 0
5004	18.136180	192.168.5.85	224.0.0.251	MDNS	77	Standard query 0
5005	18.136350	fe80::fe2:6966:5292…	ff02::fb	MDNS	97	Standard query 0
5006	18.137274	192.168.5.85	224.0.0.251	MDNS	77	Standard query 0
5007	18.138664	fe80::fe2:6966:5292…	ff02::fb	MDNS	97	Standard query 0
5008	18.144486	192.168.5.108	192.168.5.255	NBNS	92	Name query NB MS

STEP 2: Go to google and search zerobank and open 1st website i.e www.zero.webappsecurity.com copy that website



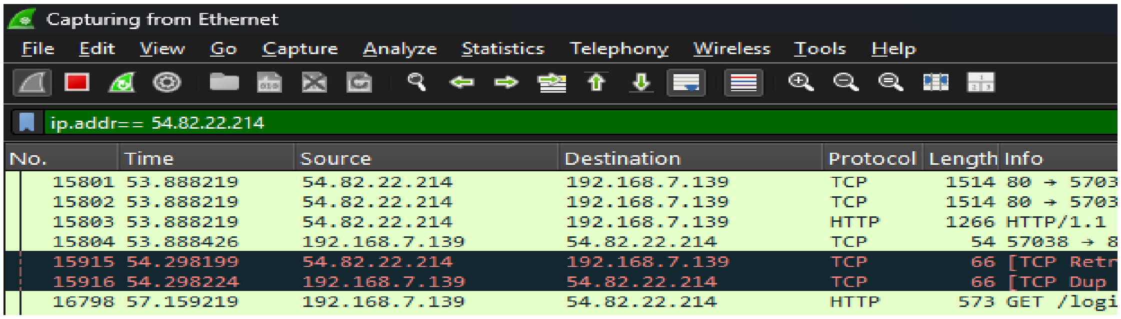
Zero Bank
http://zero.webappsecurity.com
Zero Bank - Micro Focus

STEP 3 : Open cmd and paste www.zero.webappsecurity.com this link then we get the link ip address copy that



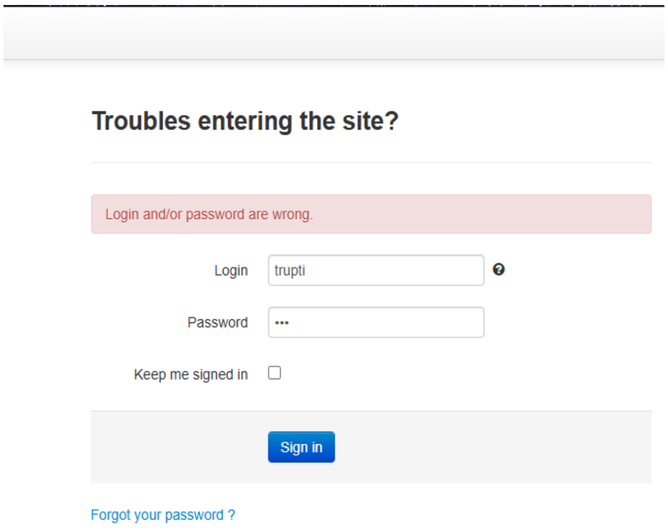
```
Microsoft Windows [Version 10.0.26100.7462]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>nslookup zero.webappsecurity.com
Server:  mumapps1.primenet.in
Address:  203.115.112.85

Non-authoritative answer:
Name:    zero.webappsecurity.com
Address:  54.82.22.214
```

STEP 4 : Then open wireshark and top type ip.addre==54.82.22.214 that is the ip address and then open zero bank website login with id and password it will show that login/password are wrong but it will fetch the credentials.



ip.addr== 54.82.22.214

No.	Time	Source	Destination	Protocol	Length	Info
15801	53.888219	54.82.22.214	192.168.7.139	TCP	1514	80 → 5703
15802	53.888219	54.82.22.214	192.168.7.139	TCP	1514	80 → 5703
15803	53.888219	54.82.22.214	192.168.7.139	HTTP	1266	HTTP/1.1
15804	53.888426	192.168.7.139	54.82.22.214	TCP	54	57038 → 8
15915	54.298199	54.82.22.214	192.168.7.139	TCP	66	[TCP Retr
15916	54.298224	192.168.7.139	54.82.22.214	TCP	66	[TCP Dup
16798	57.159219	192.168.7.139	54.82.22.214	HTTP	573	GET /logi



Troubles entering the site?

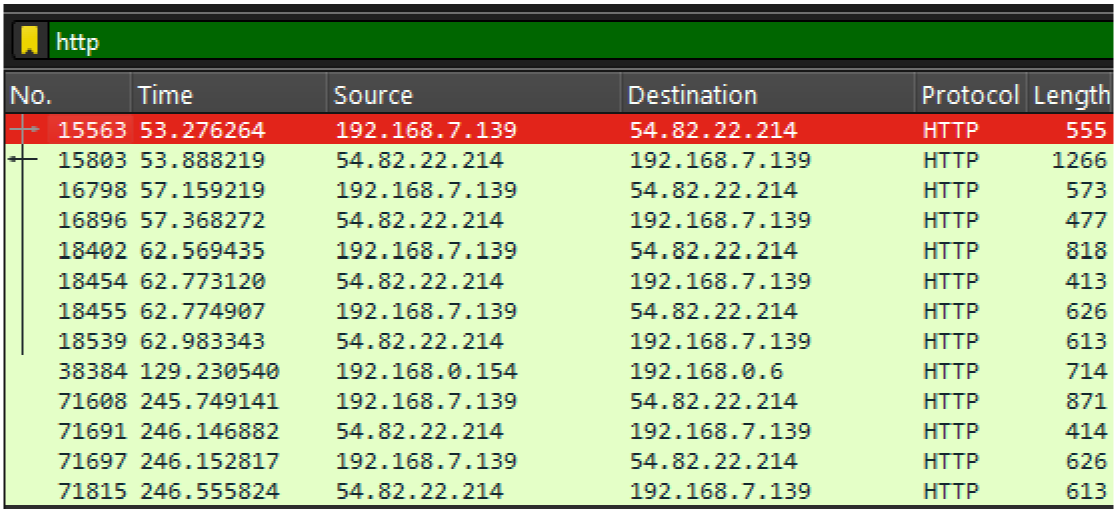
Login and/or password are wrong.

Login: trupti

Password: •••

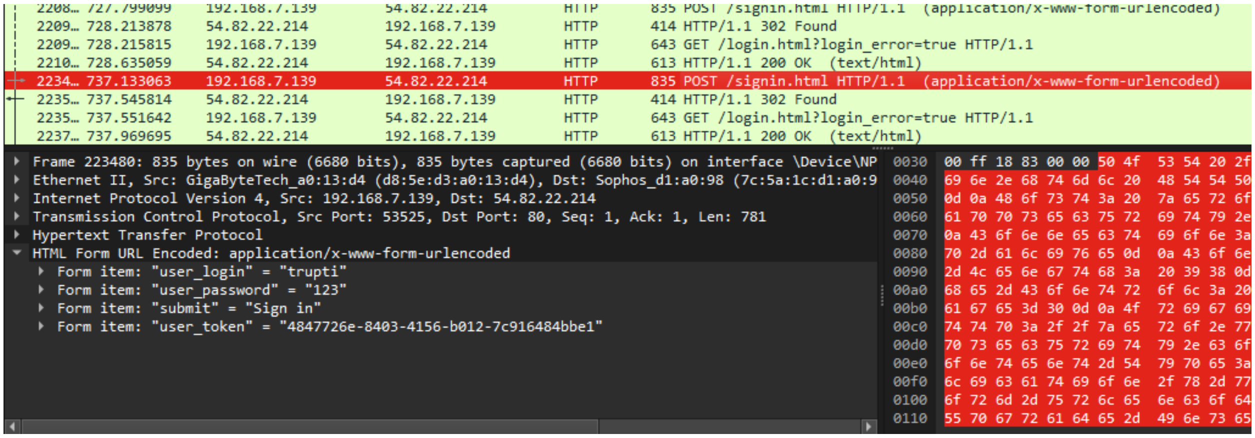
Keep me signed in □

STEP 5 : Go on wireshark and at top search http and in that you will see the POST link i.e 818 POST /signin.html/1/1 (application…) then click on that website and close it



```
http
No.    Time        Source          Destination     Protocol Length
15563  53.276264   192.168.7.139   54.82.22.214    HTTP      555
15803  53.888219   54.82.22.214    192.168.7.139   HTTP     1266
16798  57.159219   192.168.7.139   54.82.22.214    HTTP      573
16896  57.368272   54.82.22.214    192.168.7.139   HTTP      477
18402  62.569435   192.168.7.139   54.82.22.214    HTTP      818
18454  62.773120   54.82.22.214    192.168.7.139   HTTP      413
18455  62.774907   192.168.7.139   54.82.22.214    HTTP      626
18539  62.983343   54.82.22.214    192.168.7.139   HTTP      613
38384  129.230540  192.168.0.154   192.168.0.6     HTTP      714
71608  245.749141  192.168.7.139   54.82.22.214    HTTP      871
71691  246.146882  54.82.22.214    192.168.7.139   HTTP      414
71697  246.152817  192.168.7.139   54.82.22.214    HTTP      626
71815  246.555824  54.82.22.214    192.168.7.139   HTTP      613
```

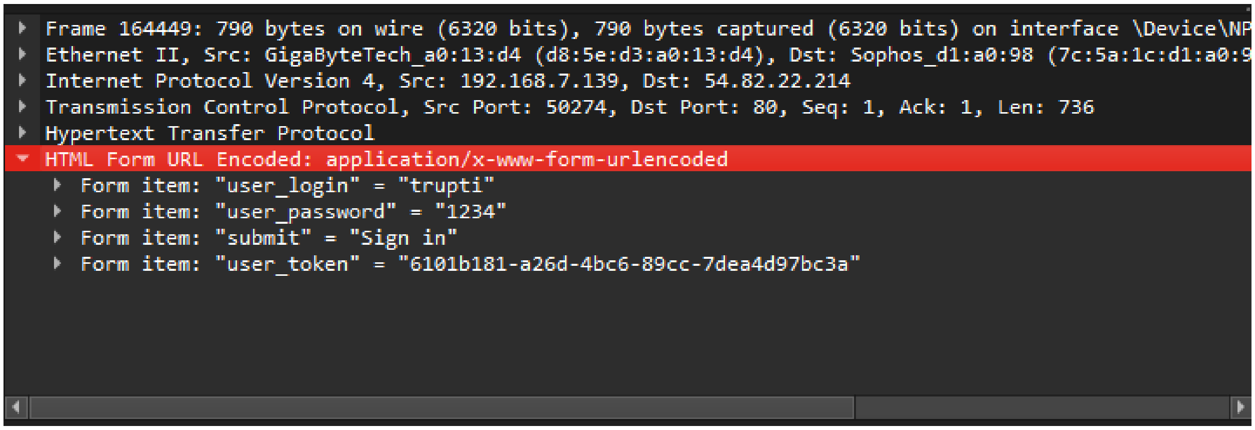
STEP 6 : Then at bottom we will see HTMLform url Encoded…. Then click on it and we can see the credentials



```
2208… 727.799099  192.168.7.139  54.82.22.214   HTTP  835 POST /signin.html HTTP/1.1  (application/x-www-form-urlencoded)
2209… 728.213878  54.82.22.214   192.168.7.139  HTTP  414 HTTP/1.1 302 Found
2209… 728.215815  192.168.7.139  54.82.22.214   HTTP  643 GET /login.html?login_error=true HTTP/1.1
2210… 728.635059  54.82.22.214   192.168.7.139  HTTP  613 HTTP/1.1 200 OK  (text/html)
2234… 737.133063  192.168.7.139  54.82.22.214   HTTP  835 POST /signin.html HTTP/1.1  (application/x-www-form-urlencoded)
2235… 737.545814  54.82.22.214   192.168.7.139  HTTP  414 HTTP/1.1 302 Found
2235… 737.551642  192.168.7.139  54.82.22.214   HTTP  643 GET /login.html?login_error=true HTTP/1.1
2237… 737.969695  54.82.22.214   192.168.7.139  HTTP  613 HTTP/1.1 200 OK  (text/html)
```

```
Frame 223480: 835 bytes on wire (6680 bits), 835 bytes captured (6680 bits) on interface \Device\NP
Ethernet II, Src: GigaByteTech_a0:13:d4 (d8:5e:d3:a0:13:d4), Dst: Sophos_d1:a0:98 (7c:5a:1c:d1:a0:9
Internet Protocol Version 4, Src: 192.168.7.139, Dst: 54.82.22.214
Transmission Control Protocol, Src Port: 53525, Dst Port: 80, Seq: 1, Ack: 1, Len: 781
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "user_login" = "trupti"
  Form item: "user_password" = "123"
  Form item: "submit" = "Sign in"
  Form item: "user_token" = "4847726e-8403-4156-b012-7c916484bbe1"
```

```
0030  00 ff 18 83 00 00 50 4f  53 54 20 2f
0040  69 6e 2e 68 74 6d 6c 20  48 54 54 50
0050  0d 0a 48 6f 73 74 3a 20  7a 65 72 6f
0060  61 70 70 73 65 63 75 72  69 74 79 2e
0070  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a
0080  70 2d 61 6c 69 76 65 0d  0a 43 6f 6e
0090  2d 4c 65 6e 67 74 68 3a  20 39 38 0d
00a0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20
00b0  61 67 65 3d 30 0d 0a 4f  72 69 67 69
00c0  74 74 70 3a 2f 2f 7a 65  72 6f 2e 77
00d0  70 73 65 63 75 72 69 74  79 2e 63 6f
00e0  6f 6e 74 65 6e 74 2d 54  79 70 65 3a
00f0  6c 69 63 61 74 69 6f 6e  2f 78 2d 77
0100  6f 72 6d 2d 75 72 6c 65  6e 63 6f 64
0110  55 70 67 72 61 64 65 2d  49 6e 73 65
```



```
Frame 164449: 790 bytes on wire (6320 bits), 790 bytes captured (6320 bits) on interface \Device\NP
Ethernet II, Src: GigaByteTech_a0:13:d4 (d8:5e:d3:a0:13:d4), Dst: Sophos_d1:a0:98 (7c:5a:1c:d1:a0:9
Internet Protocol Version 4, Src: 192.168.7.139, Dst: 54.82.22.214
Transmission Control Protocol, Src Port: 50274, Dst Port: 80, Seq: 1, Ack: 1, Len: 736
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "user_login" = "trupti"
  Form item: "user_password" = "1234"
  Form item: "submit" = "Sign in"
  Form item: "user_token" = "6101b181-a26d-4bc6-89cc-7dea4d97bc3a"
```