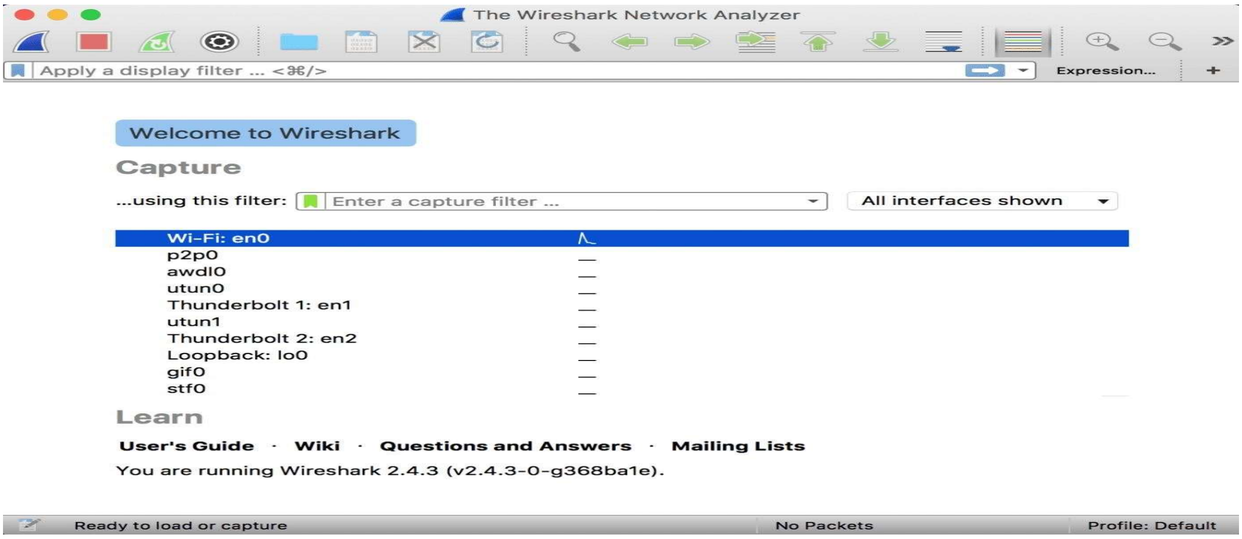
Practical No 5

Aim:Network Traffic Capture and DoS Attack with Wireshark and Nemesy

Network Traffic Capture:

- Use Wireshark to capture network traffic on a specific network interface.
- Analyze the captured packets to extract relevant information and identify potential security issues.
- Denial of Service (DoS) Attack:
- Use Nemesy to launch a DoS attack against a target system or network.
- Observe the impact of the attack on the target's availability and performance.


The Wireshark Network Analyzer
Apply a display filter ... <⌘/>
Expression...
+

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi: en0
p2p0
awdl0
utun0
Thunderbolt 1: en1
utun1
Thunderbolt 2: en2
Loopback: lo0
gif0
stf0

Learn

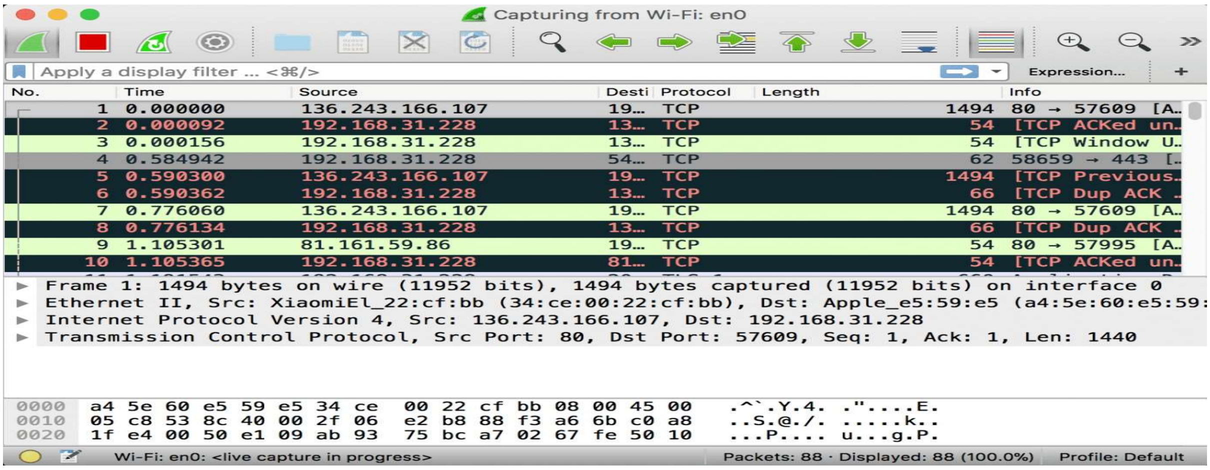
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.3 (v2.4.3-0-g368ba1e).

Ready to load or capture | No Packets | Profile: Default

As soon as you single-click on your network interface‟s name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says “Enable promiscuous mode on all interfaces”.



No.	Time	Source	Desti	Protocol	Length	Info
1	0.000000	136.243.166.107	19...	TCP	1494	80 → 57609 [A...
2	0.000092	192.168.31.228	13...	TCP	54	[TCP ACKed un...
3	0.000156	192.168.31.228	13...	TCP	54	[TCP Window U...
4	0.584942	192.168.31.228	54...	TCP	62	58659 → 443 [...
5	0.590300	136.243.166.107	19...	TCP	1494	[TCP Previous...
6	0.590362	192.168.31.228	13...	TCP	66	[TCP Dup ACK ...
7	0.776060	136.243.166.107	19...	TCP	1494	80 → 57609 [A...
8	0.776134	192.168.31.228	13...	TCP	66	[TCP Dup ACK ...
9	1.105301	81.161.59.86	19...	TCP	54	80 → 57995 [A...
10	1.105365	192.168.31.228	81...	TCP	54	[TCP ACKed un...

```
▶ Frame 1: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
▶ Ethernet II, Src: XiaomiEl_22:cf:bb (34:ce:00:22:cf:bb), Dst: Apple_e5:59:e5 (a4:5e:60:e5:59:
▶ Internet Protocol Version 4, Src: 136.243.166.107, Dst: 192.168.31.228
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 57609, Seq: 1, Ack: 1, Len: 1440
```

```
0000  a4 5e 60 e5 59 e5 34 ce  00 22 cf bb 08 00 45 00   .^`.Y.4. ."....E.
0010  05 c8 53 8c 40 00 2f 06  e2 b8 88 f3 a6 6b c0 a8   ..S.@./. .....k..
0020  1f e4 00 50 e1 09 ab 93  75 bc a7 02 67 fe 50 10   ...P.... u...g.P.
```

Wi-Fi: en0: <live capture in progress> | Packets: 88 · Displayed: 88 (100.0%) | Profile: Default

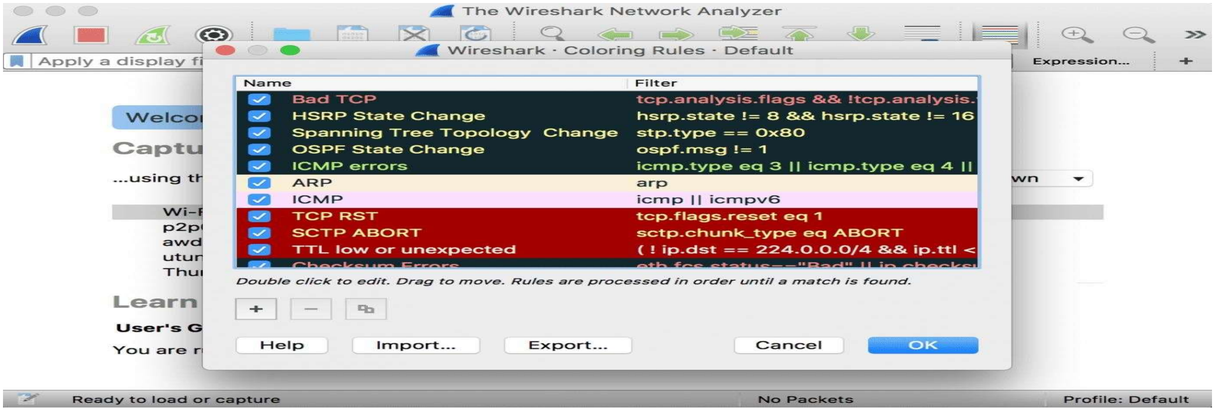
The red box button “STOP” on the top left side of the window can be clicked to stop the capturing of traffic on the network.

Color Coding

Different packets are seen highlighted in various different colors. This is Wireshark‟s way of displaying traffic to help you easily identify the types of it. Default colors are:

- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

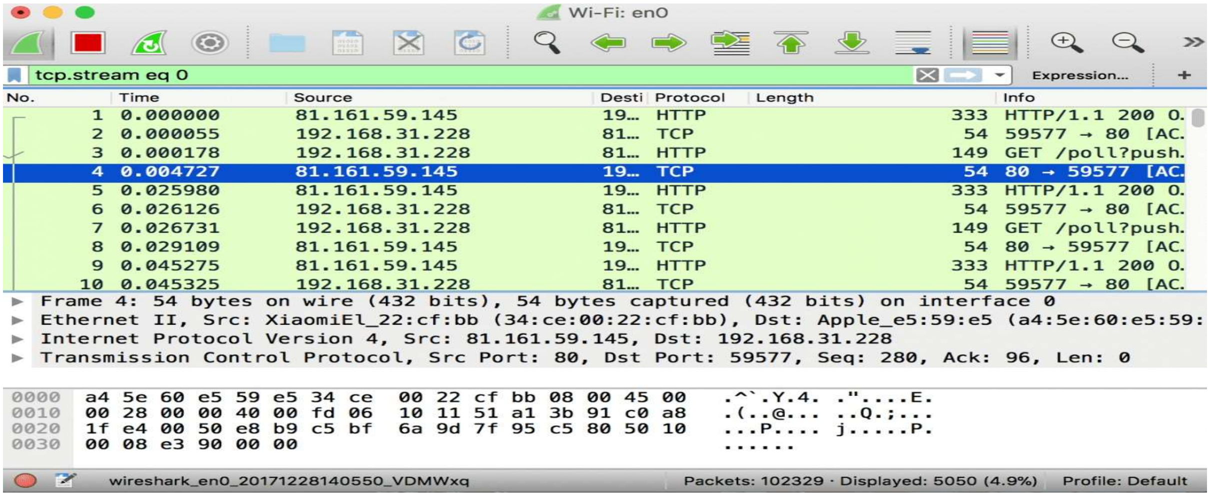


Name	Filter
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type eq 3 || icmp.type eq 4 ||
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl <
☑ Checksum Errors	eth.fcs_status=="Bad" || ip.checks

Double click to edit. Drag to move. Rules are processed in order until a match is found.

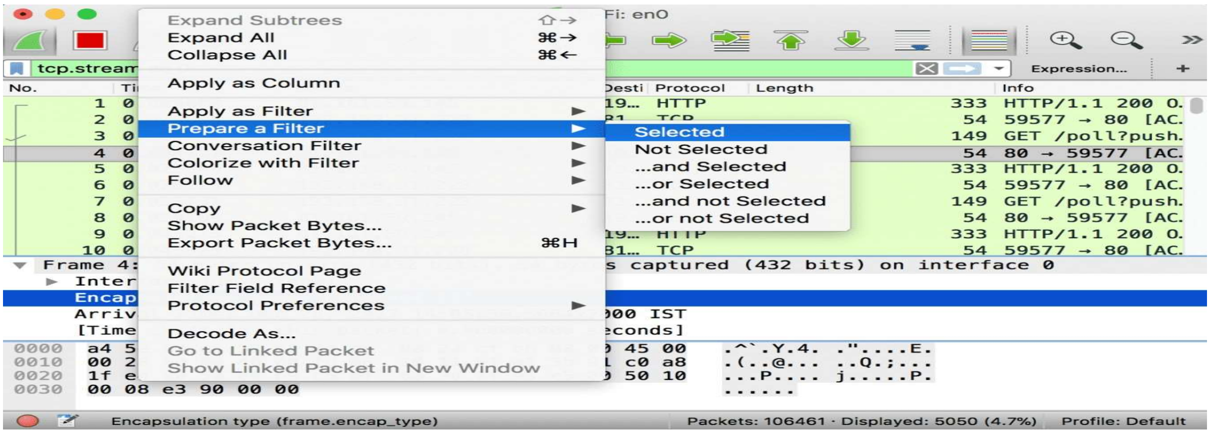
Analyze the captured Packets:

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



```
tcp.stream eq 0
No.    Time       Source           Desti Protocol  Length     Info
   1 0.000000   81.161.59.145     19...  HTTP              333 HTTP/1.1 200 O.
   2 0.000055   192.168.31.228    81...  TCP                54 59577 → 80 [AC.
   3 0.000178   192.168.31.228    81...  HTTP              149 GET /poll?push.
   4 0.004727   81.161.59.145     19...  TCP                54 80 → 59577 [AC.
   5 0.025980   81.161.59.145     19...  HTTP              333 HTTP/1.1 200 O.
   6 0.026126   192.168.31.228    81...  TCP                54 59577 → 80 [AC.
   7 0.026731   192.168.31.228    81...  HTTP              149 GET /poll?push.
   8 0.029109   81.161.59.145     19...  TCP                54 80 → 59577 [AC.
   9 0.045275   81.161.59.145     19...  HTTP              333 HTTP/1.1 200 O.
  10 0.045325   192.168.31.228    81...  TCP                54 59577 → 80 [AC.
▶ Frame 4: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: XiaomiEl_22:cf:bb (34:ce:00:22:cf:bb), Dst: Apple_e5:59:e5 (a4:5e:60:e5:59:
▶ Internet Protocol Version 4, Src: 81.161.59.145, Dst: 192.168.31.228
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 59577, Seq: 280, Ack: 96, Len: 0

0000  a4 5e 60 e5 59 e5 34 ce  00 22 cf bb 08 00 45 00   .^`.Y.4. .".....E.
0010  00 28 00 00 40 00 fd 06  10 11 51 a1 3b 91 c0 a8   .(..@... ..Q.;...
0020  1f e4 00 50 e8 b9 c5 bf  6a 9d 7f 95 c5 80 50 10   ...P.... j.....P.
0030  00 08 e3 90 00 00                                  ......

wireshark_en0_20171228140550_VDMWxq    Packets: 102329 · Displayed: 5050 (4.9%)    Profile: Default
```

Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



(B) Using NEMESIS tool, launch DOS Attack.

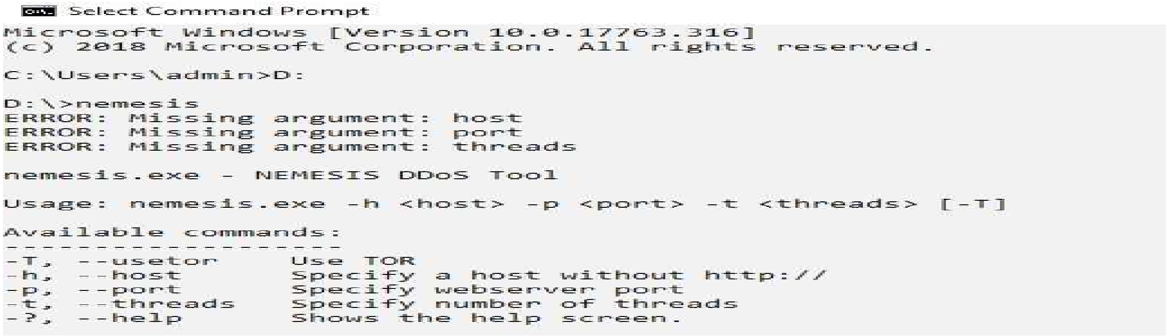
Theory: A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Nemesis is a command-line network packet crafting and injection utility for UNIX-like and Windows systems. Nemesis, is well suited for testing Network Intrusion Detection Systems, firewalls, IP stacks and a variety of other tasks. As a command-line driven utility, Nemesis is perfect for automation and scripting.

Procedure:

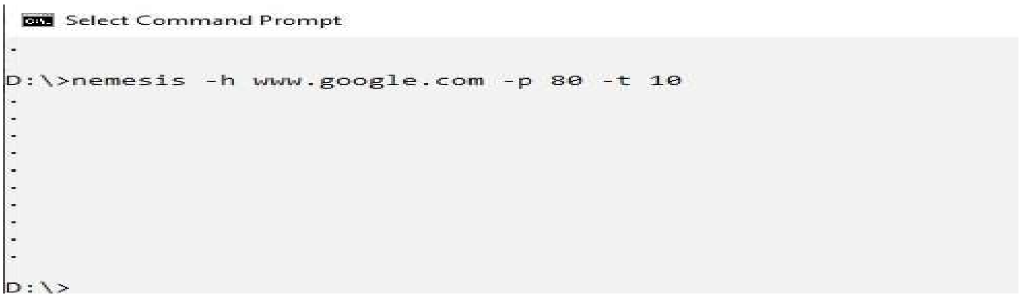
Download NEMESIS tool from “nemesis.sourceforge.net” and unzip the contents in a drive.

Launch the NEMESIS.exe application from command prompt as shown below.

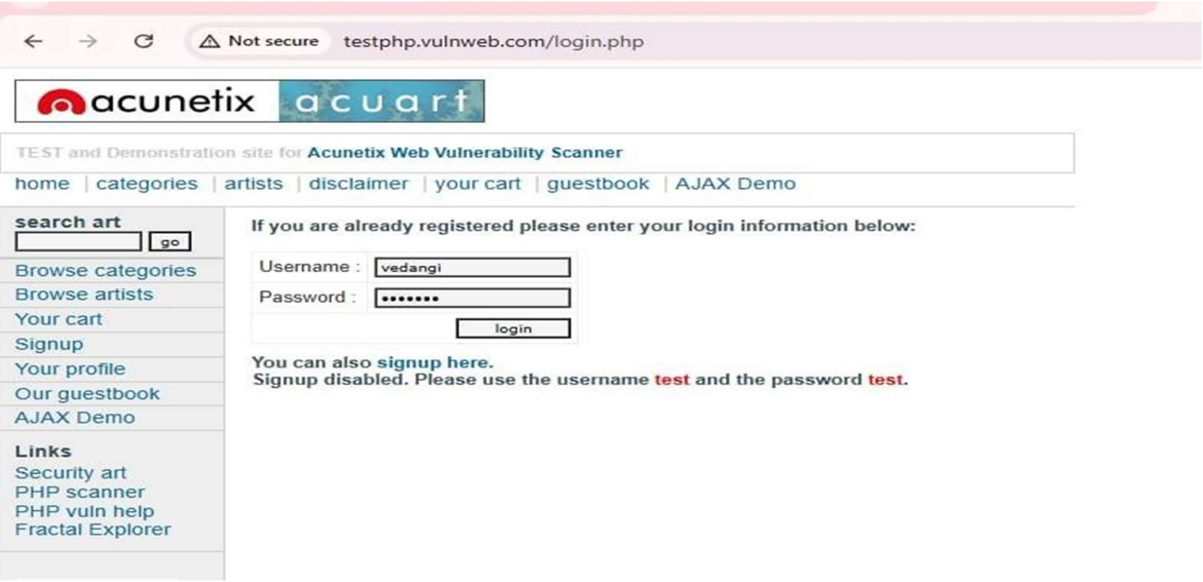


```
Microsoft Windows [Version 10.0.17763.316]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\admin>D:

D:\>nemesis
ERROR: Missing argument: host
ERROR: Missing argument: port
ERROR: Missing argument: threads

nemesis.exe - NEMESIS DDoS Tool

Usage: nemesis.exe -h <host> -p <port> -t <threads> [-T]

Available commands:
-------------------
-T, --usetor      Use TOR
-h, --host        Specify a host without http://
-p, --port        Specify webserver port
-t, --threads     Specify number of threads
-?, --help        Shows the help screen.
```

After launching NEMESIS, provide host and port of webserver on which attack is to be done.



```
.

D:\>nemesis -h www.google.com -p 80 -t 10
.
.
.
.
.
.
.
.

D:\>
```



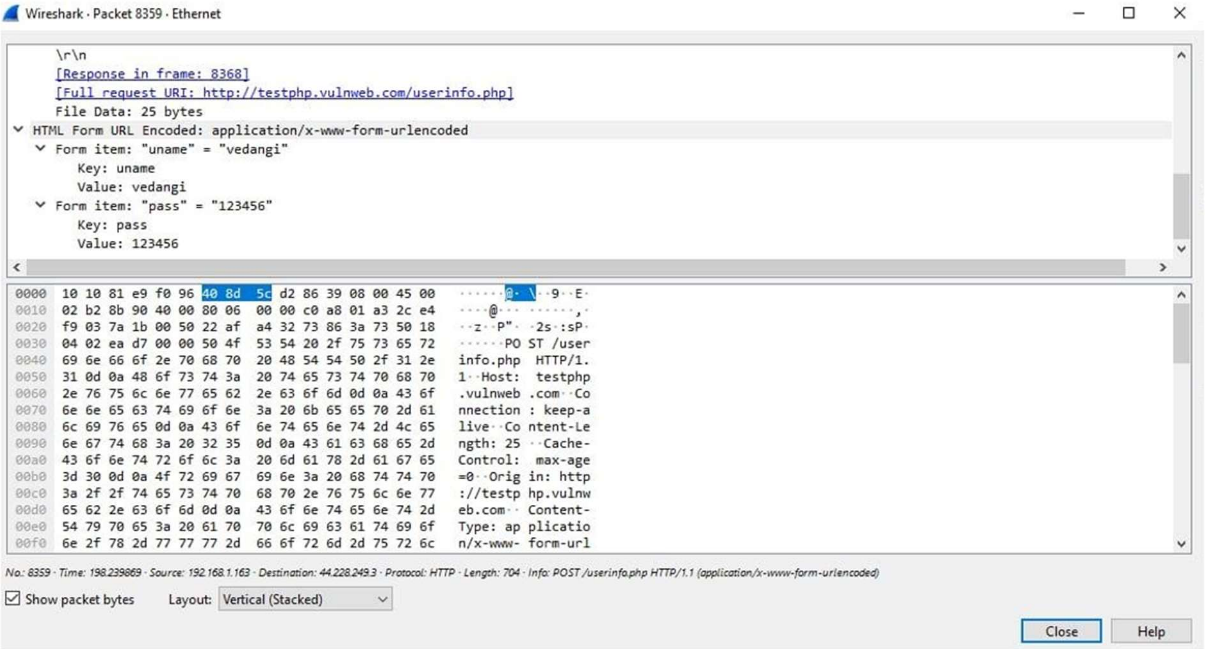
If you are already registered please enter your login information below:

Username : vedangi

Password : •••••••

login

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

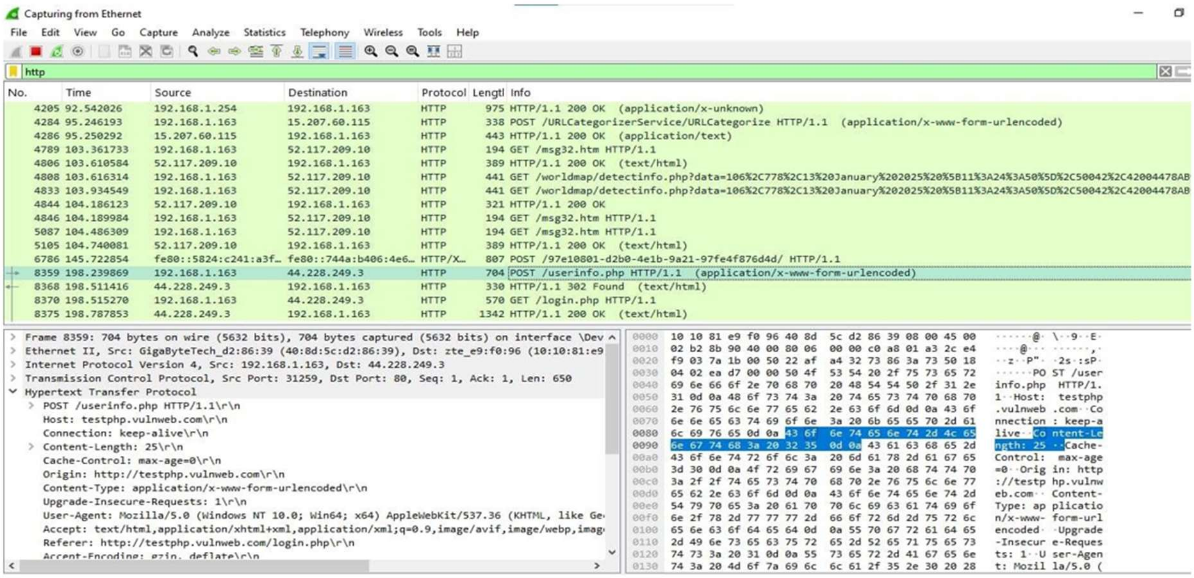


```
    \r\n
    [Response in frame: 8368]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 25 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  ⌄ Form item: "uname" = "vedangi"
      Key: uname
      Value: vedangi
  ⌄ Form item: "pass" = "123456"
      Key: pass
      Value: 123456
```

```
0000  10 10 81 e9 f0 96 40 8d  5c d2 86 39 08 00 45 00   ······@· \··9··E·
0010  02 b2 8b 90 40 00 80 06  00 00 c0 a8 01 a3 2c e4   ····@··· ······,·
0020  f9 03 7a 1b 00 50 22 af  a4 32 73 86 3a 73 50 18   ··z··P"· ·2s·:sP·
0030  04 02 ea d7 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 35  0d 0a 43 61 63 68 65 2d   ngth: 25 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
00e0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
00f0  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
```

No.: 8359 · Time: 198.239869 · Source: 192.168.1.163 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 704 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

☑ Show packet bytes   Layout: Vertical (Stacked)


Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.   Time        Source                Destination           Protocol Lengtl Info
 4205 92.542026   192.168.1.254         192.168.1.163         HTTP      975 HTTP/1.1 200 OK  (application/x-unknown)
 4284 95.246193   192.168.1.163         15.207.60.115         HTTP      338 POST /URLCategorizerService/URLCategorize HTTP/1.1  (application/x-www-form-urlencoded)
 4286 95.250292   15.207.60.115         192.168.1.163         HTTP      443 HTTP/1.1 200 OK  (application/text)
 4789 103.361733  192.168.1.163         52.117.209.10         HTTP      194 GET /msg32.htm HTTP/1.1
 4806 103.610584  52.117.209.10         192.168.1.163         HTTP      389 HTTP/1.1 200 OK  (text/html)
 4808 103.616314  192.168.1.163         52.117.209.10         HTTP      441 GET /worldmap/detectinfo.php?data=106%2C778%2C13%20January%202025%20%5B11%3A24%3A50%5D%2C50042%2C42004478AB
 4833 103.934549  192.168.1.163         52.117.209.10         HTTP      441 GET /worldmap/detectinfo.php?data=106%2C778%2C13%20January%202025%20%5B11%3A24%3A50%5D%2C50042%2C42004478AB
 4844 104.186123  52.117.209.10         192.168.1.163         HTTP      321 HTTP/1.1 200 OK
 4846 104.189984  192.168.1.163         52.117.209.10         HTTP      194 GET /msg32.htm HTTP/1.1
 5087 104.486309  192.168.1.163         52.117.209.10         HTTP      194 GET /msg32.htm HTTP/1.1
 5105 104.740081  52.117.209.10         192.168.1.163         HTTP      389 HTTP/1.1 200 OK  (text/html)
 6786 145.722854  fe80::5824:c241:a3f…  fe80::744a:b406:4e6…  HTTP/X…   807 POST /97e10801-d2b0-4e1b-9a21-97fe4f876d4d/ HTTP/1.1
 8359 198.239869  192.168.1.163         44.228.249.3          HTTP      704 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 8368 198.511416  44.228.249.3          192.168.1.163         HTTP      330 HTTP/1.1 302 Found  (text/html)
 8370 198.515270  192.168.1.163         44.228.249.3          HTTP      570 GET /login.php HTTP/1.1
 8375 198.787853  44.228.249.3          192.168.1.163         HTTP     1342 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 8359: 704 bytes on wire (5632 bits), 704 bytes captured (5632 bits) on interface \Dev
> Ethernet II, Src: GigaByteTech_d2:86:39 (40:8d:5c:d2:86:39), Dst: zte_e9:f0:96 (10:10:81:e9
> Internet Protocol Version 4, Src: 192.168.1.163, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 31259, Dst Port: 80, Seq: 1, Ack: 1, Len: 650
⌄ Hypertext Transfer Protocol
  > POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
  > Content-Length: 25\r\n
    Cache-Control: max-age=0\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0000  10 10 81 e9 f0 96 40 8d  5c d2 86 39 08 00 45 00   ······@· \··9··E·
0010  02 b2 8b 90 40 00 80 06  00 00 c0 a8 01 a3 2c e4   ····@··· ······,·
0020  f9 03 7a 1b 00 50 22 af  a4 32 73 86 3a 73 50 18   ··z··P"· ·2s·:sP·
0030  04 02 ea d7 00 00 50 4f  53 54 20 2f 75 73 65 72   ······PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 35  0d 0a 43 61 63 68 65 2d   ngth: 25 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65   Control:  max-age
00b0  3d 30 0d 0a 4f 72 69 67  69 6e 3a 20 68 74 74 70   =0··Orig in: http
00c0  3a 2f 2f 74 65 73 74 70  68 70 2e 76 75 6c 6e 77   ://testp hp.vulnw
00d0  65 62 2e 63 6f 6d 0d 0a  43 6f 6e 74 65 6e 74 2d   eb.com·· Content-
00e0  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
00f0  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
0100  65 6e 63 6f 64 65 64 0d  0a 55 70 67 72 61 64 65   encoded· ·Upgrade
0110  2d 49 6e 73 65 63 75 72  65 2d 52 65 71 75 65 73   -Insecur e-Reques
0120  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
```