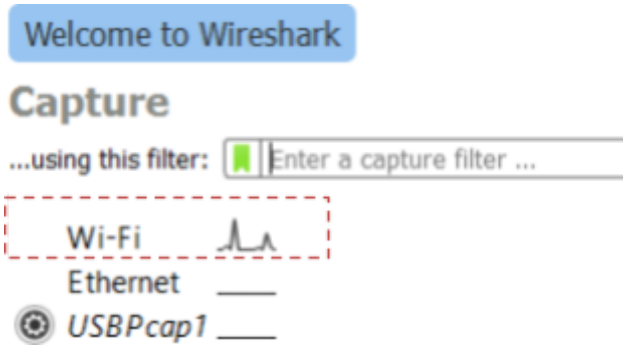
LAB 1: How to capture traffic (Wireshark)

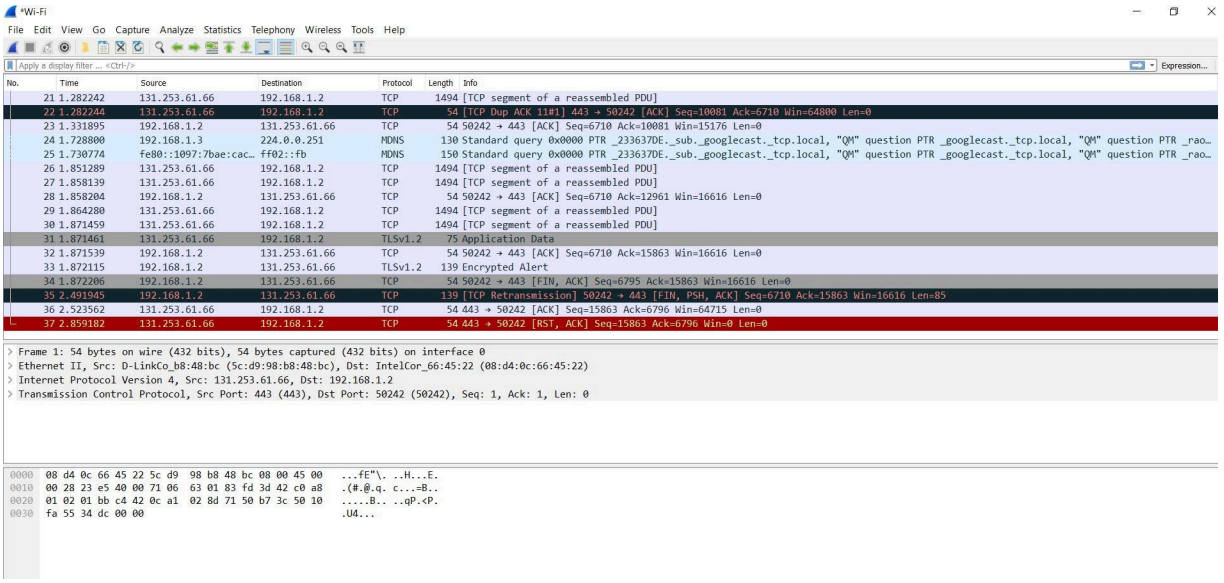
NAME: BEATRICE ANN DAVID
MATRICS NO: A23CS0055

1) Getting use

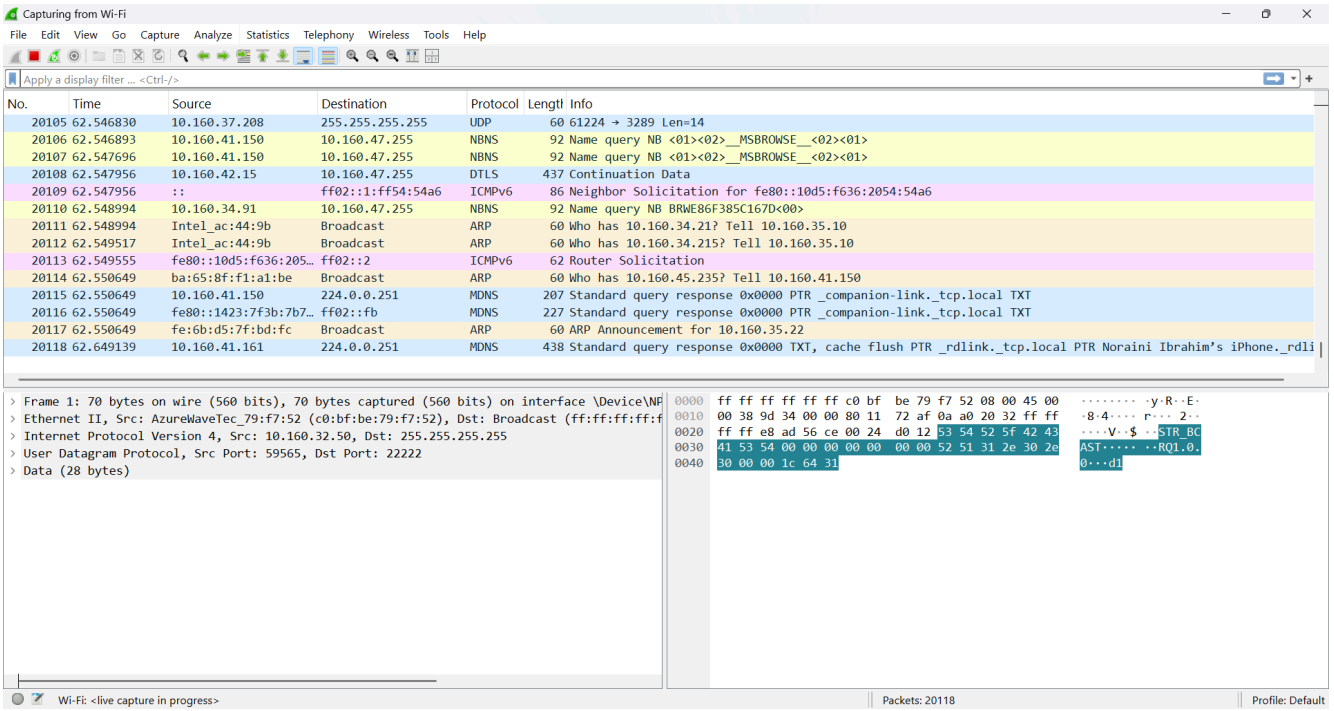
- Double click on Wi-Fi to start capturing wifi packet.



- By default for Wireshark version 2.0.3, upon double click it will auto start capturing the packets.



- If you notice at the top, there are some panel to do control the Wireshark.



My image

Mostly we need to notice the mid panel, since it is in human readable form. Rather than the bottom panel, which is more complicated and machine language form.

<u>Mid Panel</u>

```
> Frame 35: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface 0
> Ethernet II, Src: IntelCor_66:45:22 (08:d4:0c:66:45:22), Dst: D-LinkCo_b8:48:bc (5c:d9:98:b8:48:bc)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 131.253.61.66
v Transmission Control Protocol, Src Port: 50242 (50242), Dst Port: 443 (443), Seq: 6710, Ack: 15863, Len: 85
    Source Port: 50242
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 85]
    Sequence number: 6710    (relative sequence number)
    [Next sequence number: 6795    (relative sequence number)]
    Acknowledgment number: 15863    (relative ack number)
    Header Length: 20 bytes
  > Flags: 0x019 (FIN, PSH, ACK)
    Window size value: 16616
    [Calculated window size: 16616]
    [Window size scaling factor: -1 (unknown)]
  > Checksum: 0x3aa5 [validation disabled]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    Retransmitted TCP segment data (85 bytes)
```

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
33905	139.963034	HonHaiPrecis_ba:4e:…	Broadcast	ARP	60	Who has 169.254.46.20? (ARP Probe)
33906	140.064095	10.160.34.91	10.160.47.255	NBNS	92	Name query NB BRWE86F385C167D<00>
33907	140.064095	fe80::b150:17bc:561…	ff02::1:2	DHCPv6	149	Solicit XID: 0xf8ffcc CID: 000100012f1d15823417ebdfec04
33908	140.064246	Intel_6f:18:be	Broadcast	ARP	60	Who has 10.160.33.83? Tell 10.160.42.186
33909	140.064246	10.160.34.91	224.0.0.251	MDNS	81	Standard query 0x0000 A BRWE86F385C167D.local, "QM" question
33910	140.064572	fe80::f912:9918:360…	ff02::fb	MDNS	101	Standard query 0x0000 A BRWE86F385C167D.local, "QM" question
33911	140.064572	56:c3:22:c9:8c:ff	Broadcast	ARP	60	Who has 10.160.40.94? (ARP Probe)
33912	140.166132	HonHaiPrecis_98:92:…	Broadcast	ARP	60	Who has 10.160.42.198? (ARP Probe)
33913	140.166132	::	ff02::1:ff10:5e0f	ICMPv6	78	Neighbor Solicitation for fe80::b150:17bc:5610:5e0f
33914	140.166132	fe80::b150:17bc:561…	ff02::2	ICMPv6	62	Router Solicitation
33915	140.166263	10.160.42.181	224.0.0.251	MDNS	162	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question
33916	140.166263	fe80::c50:cd22:f23:…	ff02::fb	MDNS	182	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _rdlink._tcp.local, "QU" question
33917	140.166735	2a:73:10:e7:3c:ad	Broadcast	ARP	60	Who has 10.160.42.181? Tell 10.160.32.238
33918	140.272419	fa:b6:e0:ad:84:e8	Broadcast	ARP	60	Who has 10.160.42.181? Tell 10.160.43.57

My image

<u>Bottom Panel (to hide this go to view and untick packet bytes)</u>

Hexadecimal view

```
0000  5c d9 98 b8 48 bc 08 d4  0c 66 45 22 08 00 45 00   \...H... .fE"..E.
0010  00 28 45 43 40 00 80 06  32 a3 c0 a8 01 02 83 fd   .(EC@... 2.......
0020  3d 42 c4 42 01 bb 71 50  d1 c6 0c a1 40 83 50 11   =B.B..qP ....@.P.
0030  40 e8 95 c8 00 00                                  @.....
```

```
0000  ff ff ff ff ff ff c0 bf  be 79 f7 52 08 00 45 00   ........ ·y·R··E·
0010  00 38 9d 34 00 00 80 11  72 af 0a a0 20 32 ff ff   ·8·4···· r··· 2··
0020  ff ff e8 ad 56 ce 00 24  d0 12 53 54 52 5f 42 43   ····V··$ ··STR_BC
0030  41 53 54 00 00 00 00 00  00 00 52 51 31 2e 30 2e   AST····· ··RQ1.0.
0040  30 00 00 1c 64 31                                  0···d1
```

My image

Bits view

```
0000  01011100 11011001 10011000 10111000 01001000 10111100 00001000 11010100   \...H...
0008  00001100 01100110 01000101 00100010 00001000 00000000 01000101 00000000   .fE"..E.
0010  00000000 00101000 01000101 01000011 01000000 00000000 10000000 00000110   .(EC@...
0018  00110010 10100011 11000000 10101000 00000001 00000010 10000011 11111101   2.......
0020  00111101 01000010 11000100 01000010 00000001 10111011 01110001 01010000   =B.B..qP
0028  11010001 11000110 00001100 10100001 01000000 10000011 01010000 00010001   ....@.P.
0030  01000000 11101000 10010101 11001000 00000000 00000000                     @.....
```

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NP
> Ethernet II, Src: AzureWaveTec_79:f7:52 (c0:bf:be:79:f7:52), Dst: Broadcast (ff:ff:ff:ff:f
> Internet Protocol Version 4, Src: 10.160.32.50, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 59565, Dst Port: 22222
> Data (28 bytes)
```

My image

2) See visiting website (HTTP)

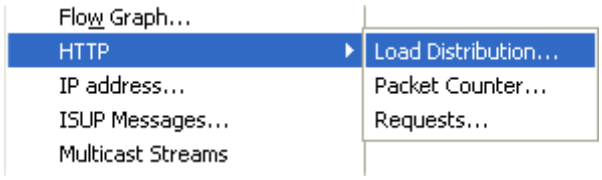
HTTP (Hypertext Transfer Protocol) is a client-server communication protocol used to transfer HTML files.

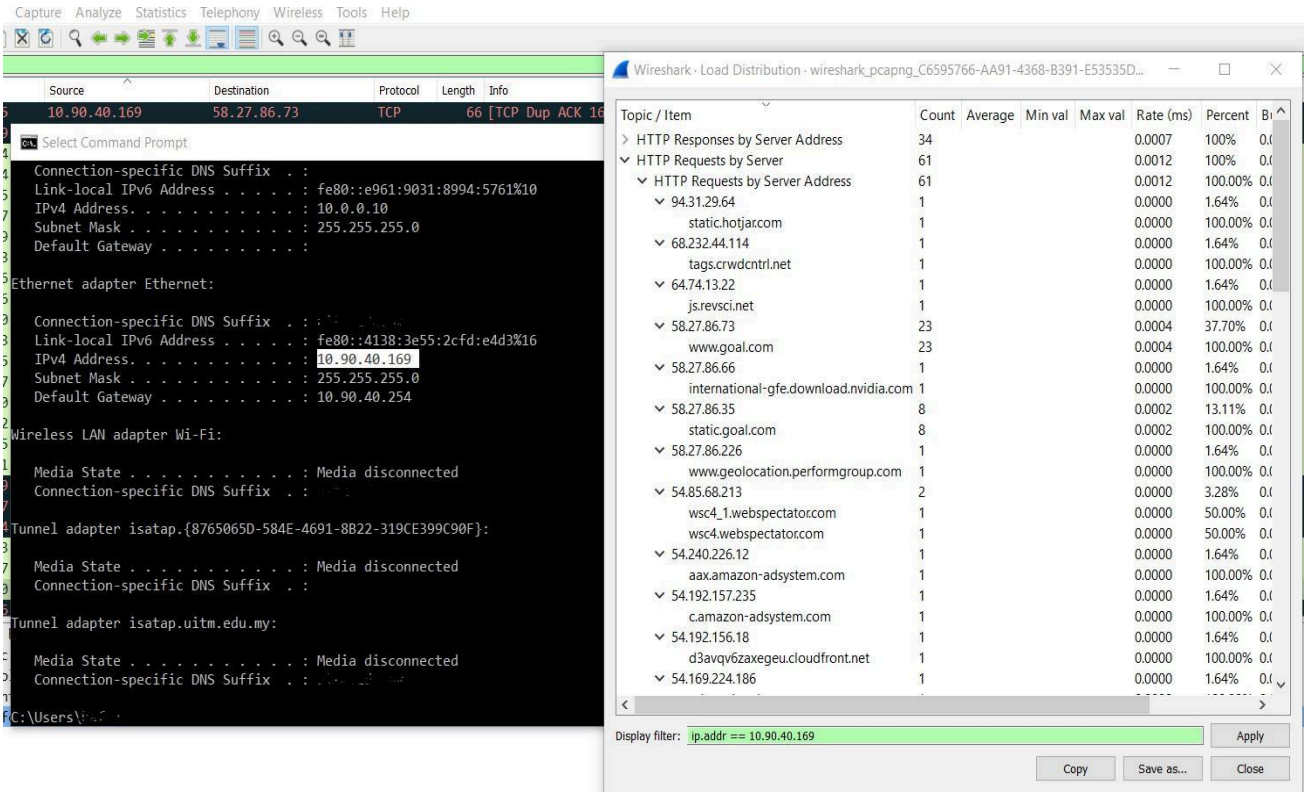
An HTTP client, most of the times a web browser, sends an HTTP request to a web server with the well-known "URL" field to locate the file. The web server will answer with an HTTP response and provides to the client the desired web page.

Three sub-sections are available under "HTTP":

- Load Distribution
- Packet Counter
- Requests

- Go to statistic > load distribution





Wireshark · HTTP / Load Distribution · Wi-Fi

Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Responses by Server Address	8				0.0000	100%	0.0100	5.355
203.121.59.248	3				0.0000	37.50%	0.0100	5.355
OK	3				0.0000	100.00%	0.0100	5.355
203.121.59.219	3				0.0000	37.50%	0.0100	53.066
OK	3				0.0000	100.00%	0.0100	53.066
203.121.59.203	2				0.0000	25.00%	0.0100	15.487
OK	2				0.0000	100.00%	0.0100	15.487
HTTP Requests by Server	1578				0.0048	100%	0.0800	34.093
HTTP Requests by Server Address	1578				0.0048	100.00%	0.0800	34.093
ff02::c	181				0.0005	11.47%	0.0500	174.991
[FF02::C]:1900	181				0.0005	100.00%	0.0500	174.991
239.255.255.250	1376				0.0042	87.20%	0.0500	34.093
239.255.255.250:1900	1376				0.0042	100.00%	0.0500	34.093
203.121.59.248	5				0.0000	0.32%	0.0200	47.101
msedge.b.tlu.dl.delivery.mp.microsoft.com	5				0.0000	100.00%	0.0200	47.101
203.121.59.219	7				0.0000	0.44%	0.0100	22.847
www.msftconnecttest.com	7				0.0000	100.00%	0.0100	22.847
203.121.59.203	5				0.0000	0.32%	0.0100	15.468
www.msftconnecttest.com	4				0.0000	80.00%	0.0100	113.182
ctldl.windowsupdate.com	1				0.0000	20.00%	0.0100	15.468
163.70.137.61	4				0.0000	0.25%	0.0100	23.906
c.whatsapp.net	4				0.0000	100.00%	0.0100	23.906
HTTP Requests by HTTP Host	1578				0.0048	100.00%	0.0800	34.093
www.msftconnecttest.com	11				0.0000	0.70%	0.0100	22.847
203.121.59.219	7				0.0000	63.64%	0.0100	22.847
203.121.59.203	4				0.0000	36.36%	0.0100	113.182
msedge.b.tlu.dl.delivery.mp.microsoft.com	5				0.0000	0.32%	0.0200	47.101
203.121.59.248	5				0.0000	100.00%	0.0200	47.101
ctldl.windowsupdate.com	1				0.0000	0.06%	0.0100	15.468
203.121.59.203	1				0.0000	100.00%	0.0100	15.468
c.whatsapp.net	4				0.0000	0.25%	0.0100	23.906
163.70.137.61	4				0.0000	100.00%	0.0100	23.906
[FF02::C]:1900	181				0.0005	11.47%	0.0500	174.991
ff02::c	181				0.0005	100.00%	0.0500	174.991

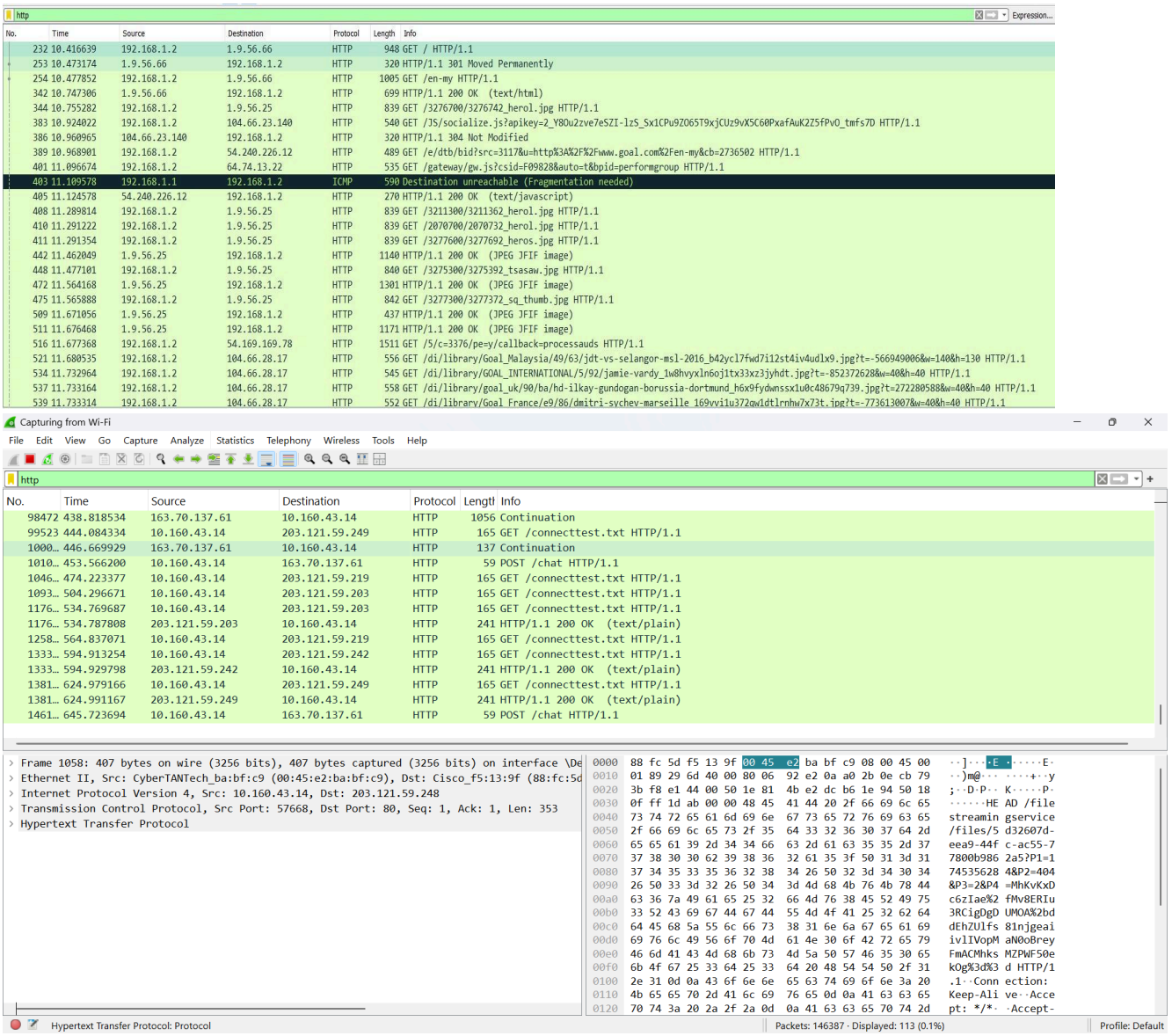
Display filter: Enter a display filter ... Apply

Copy Save as... Close

My image

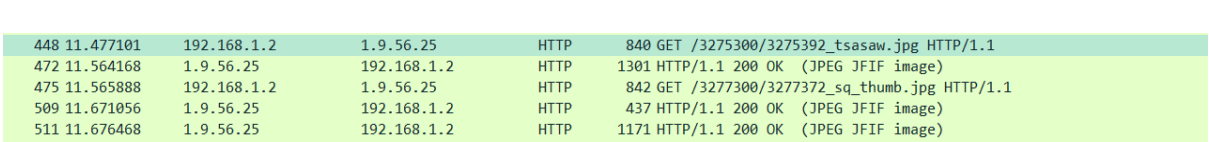
3) See what images that opened within local network

Start the capturing again. And this time just filters only to ‘http’ for website.



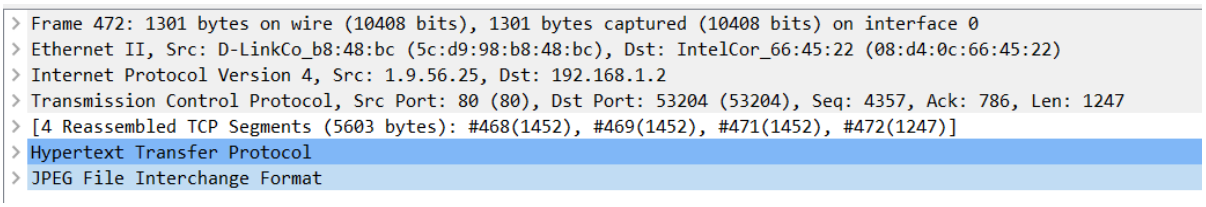
My image

For pictures, see the images format likes png, jpeg and etc.

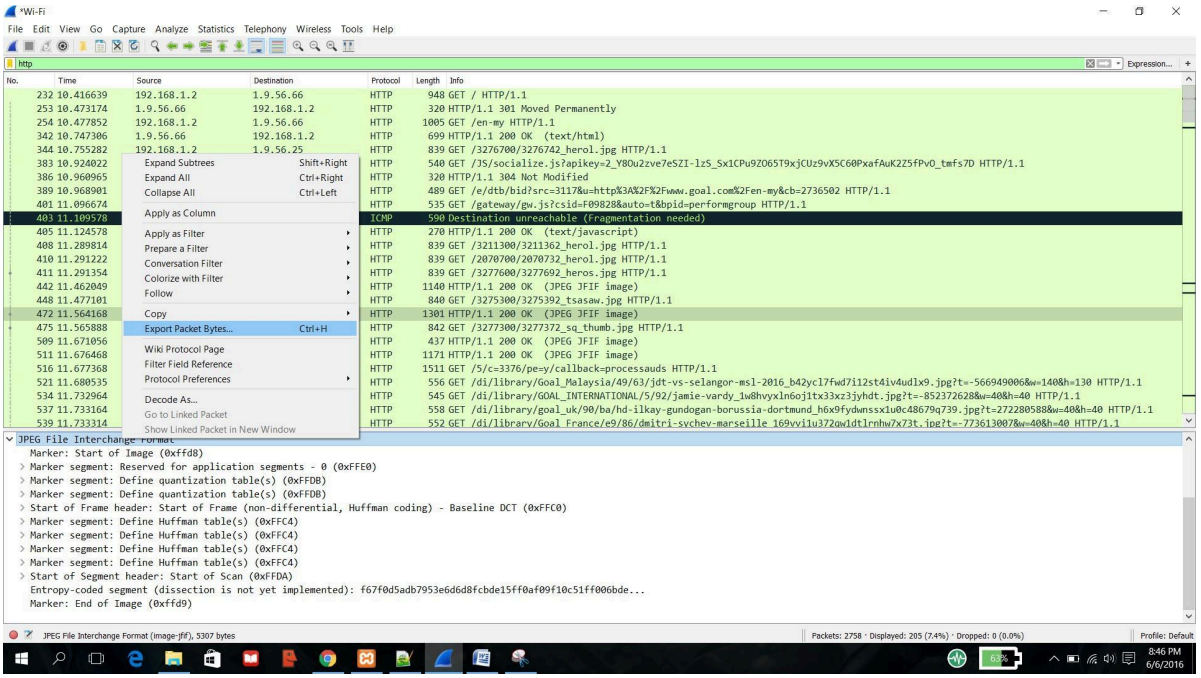


And on the next line you can see JPEG file image there.

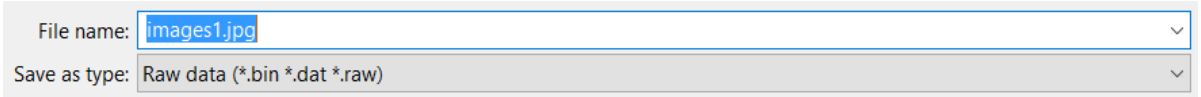
Highlight it and go to the JPEG file Interchange format.

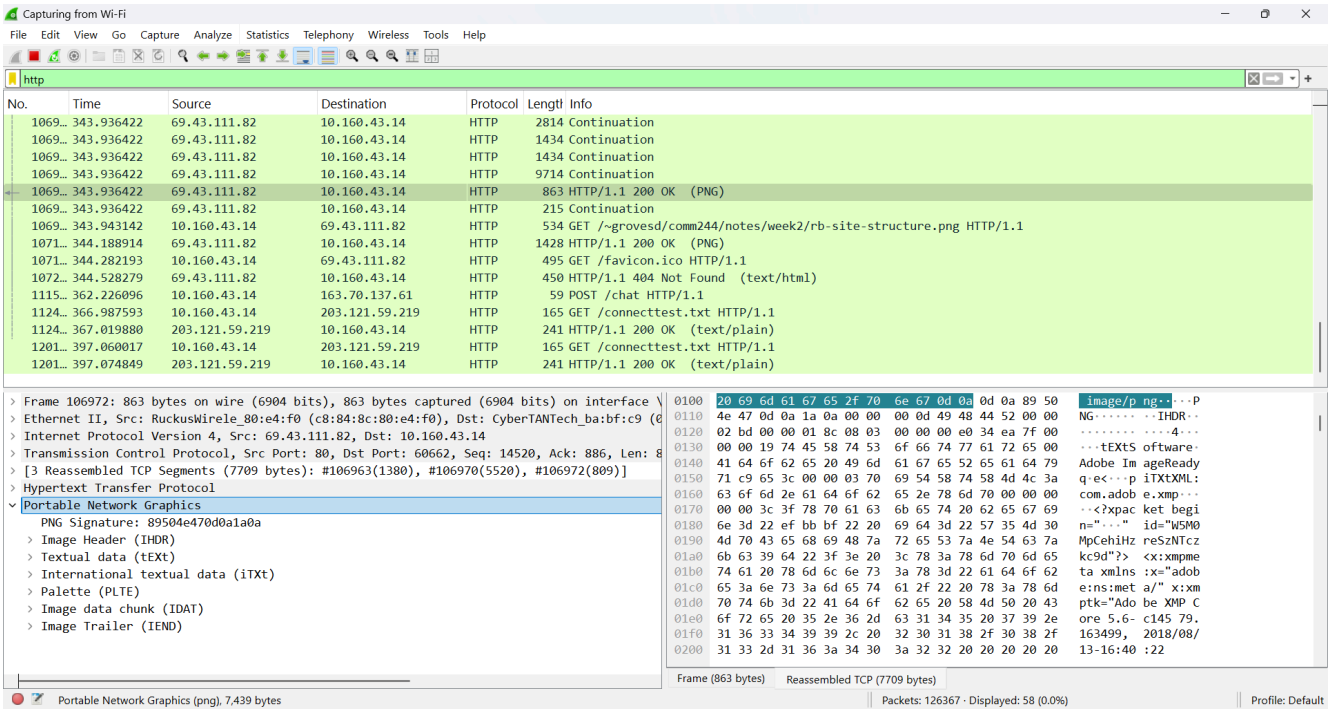


Right click the format and export packets bytes



As the images is JPEG, so go on save it as jpeg. If PNG save it as png.



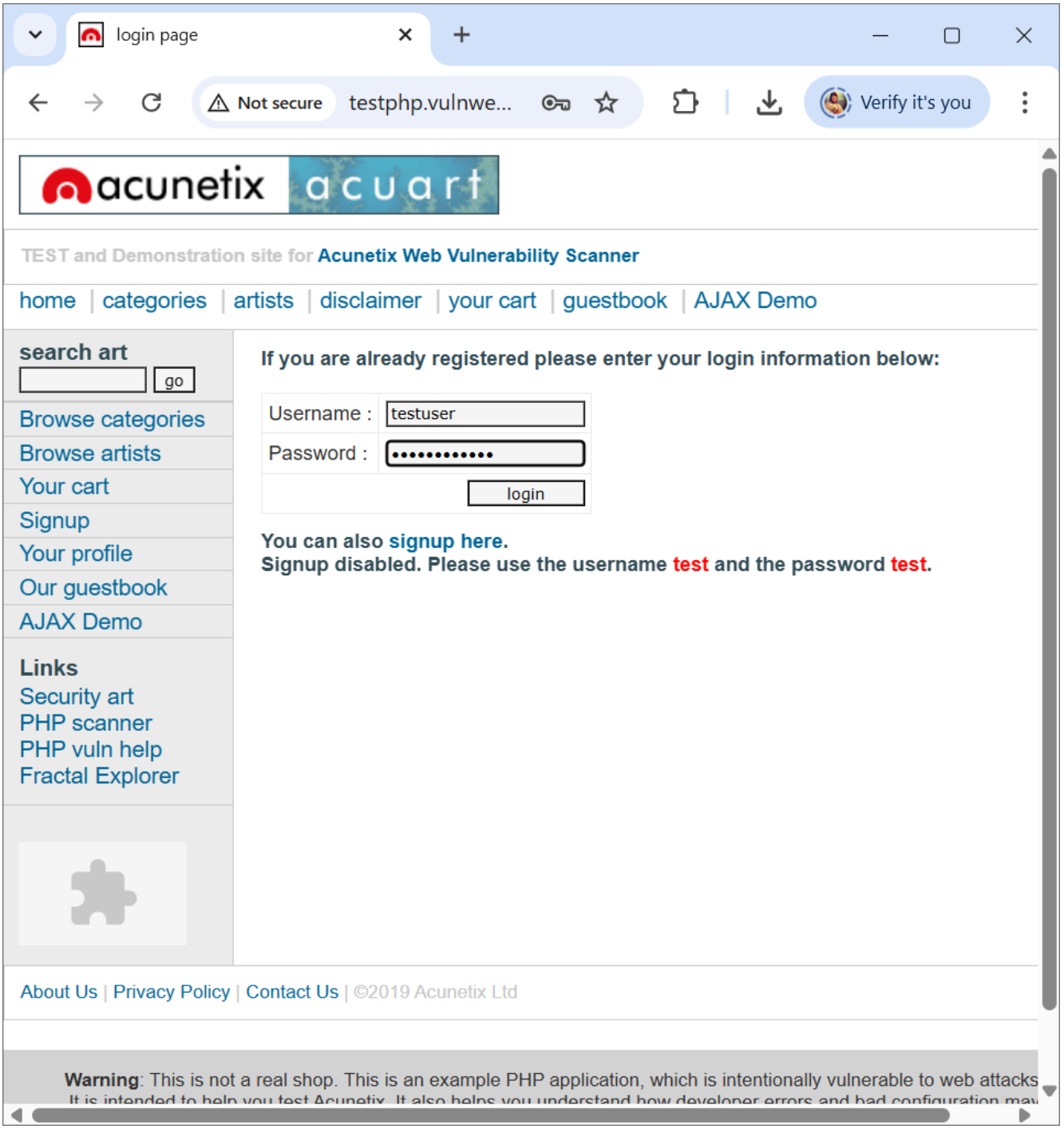


My image

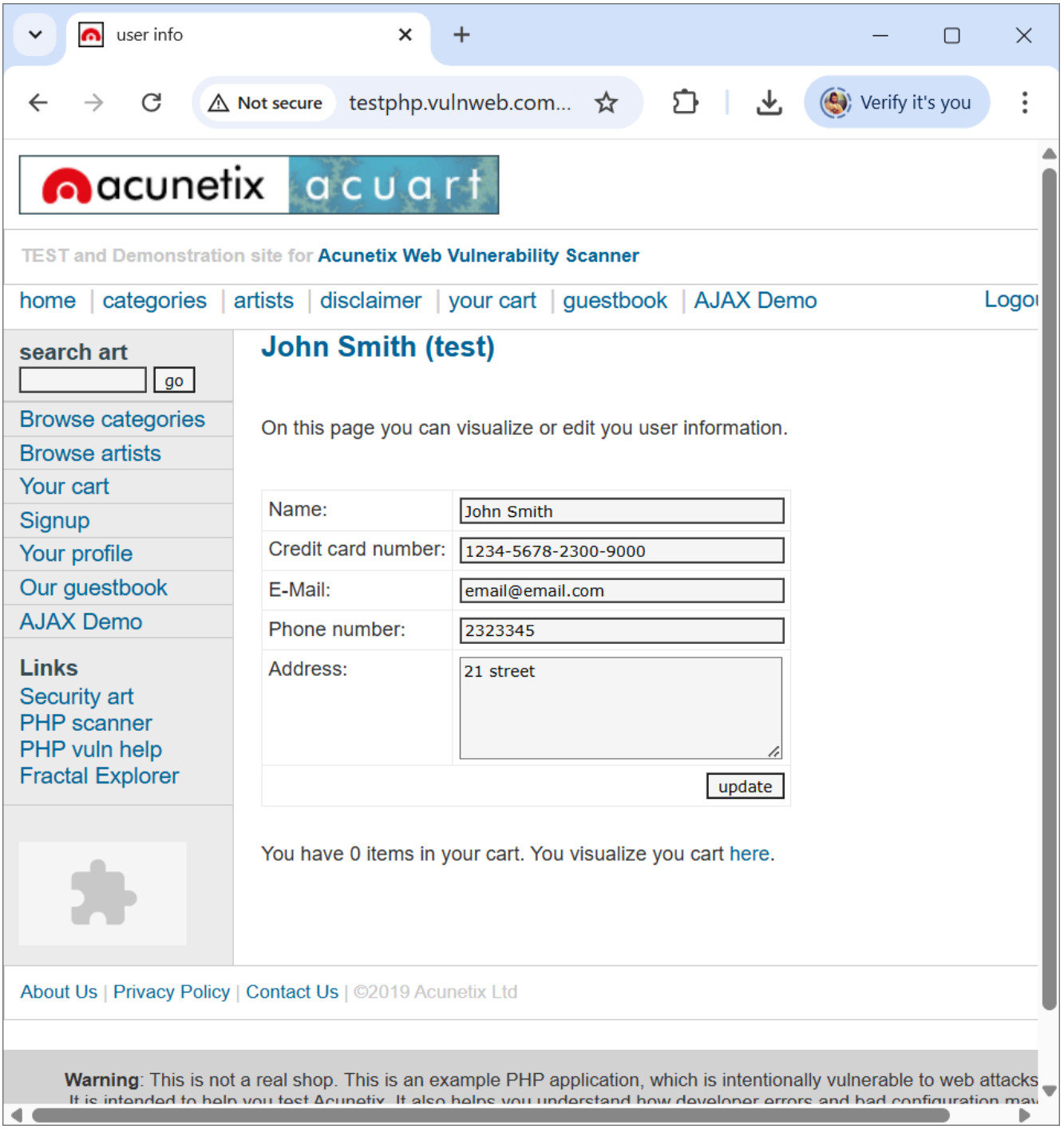
4) Sniff username & password from

HTTP Try running HTTP login page:

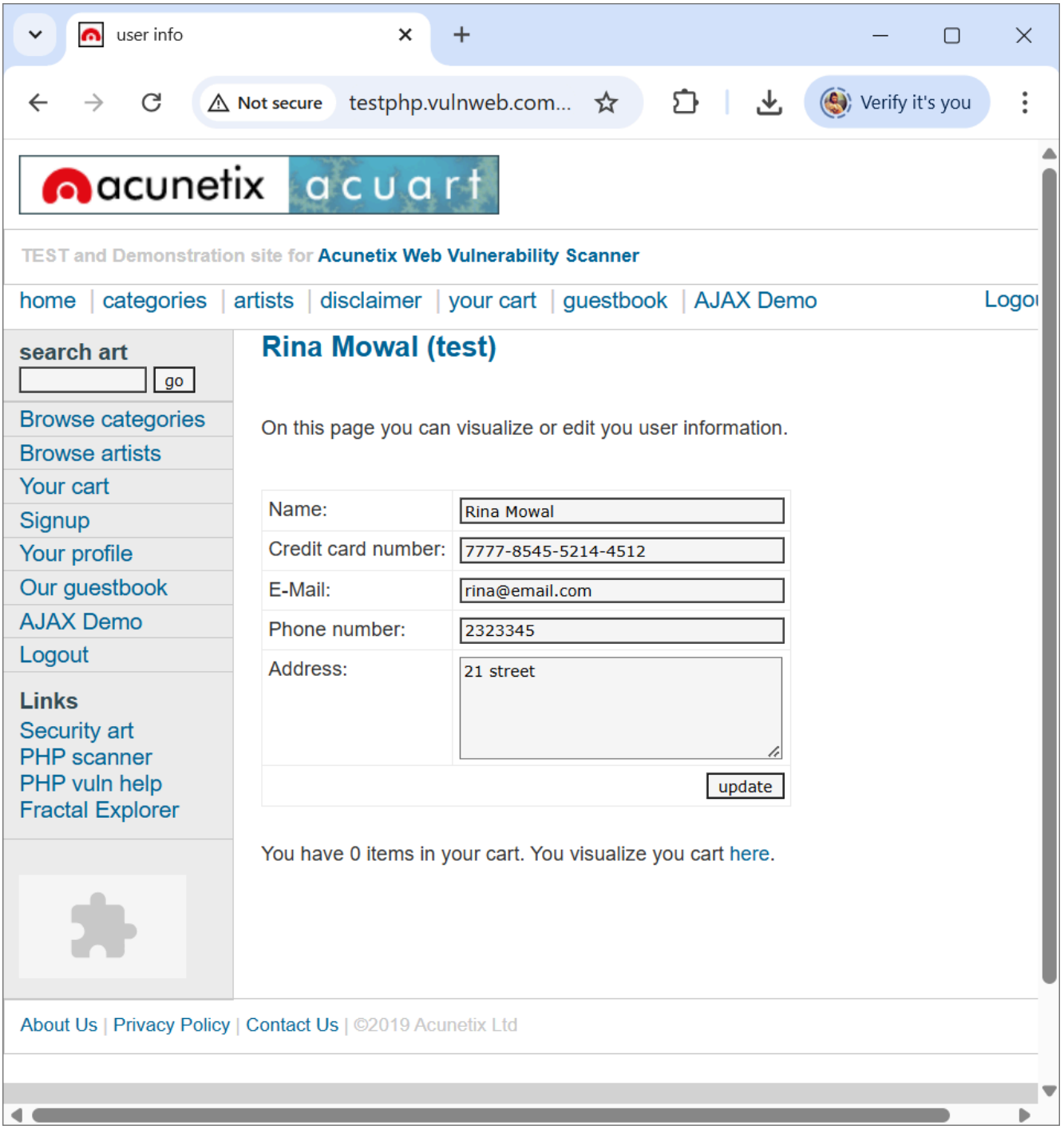
1. Open your web browser.
2. Navigate to an HTTP testing login site such as http://testphp.vulnweb.com/login.php. This site is designed for testing purposes.
3. Enter the login credentials (e.g., username: testuser, password: testpassword) on the HTTP login page.
4. Submit the form.
5. Apply a display filter to isolate HTTP traffic. In the filter bar, type http and press Enter.



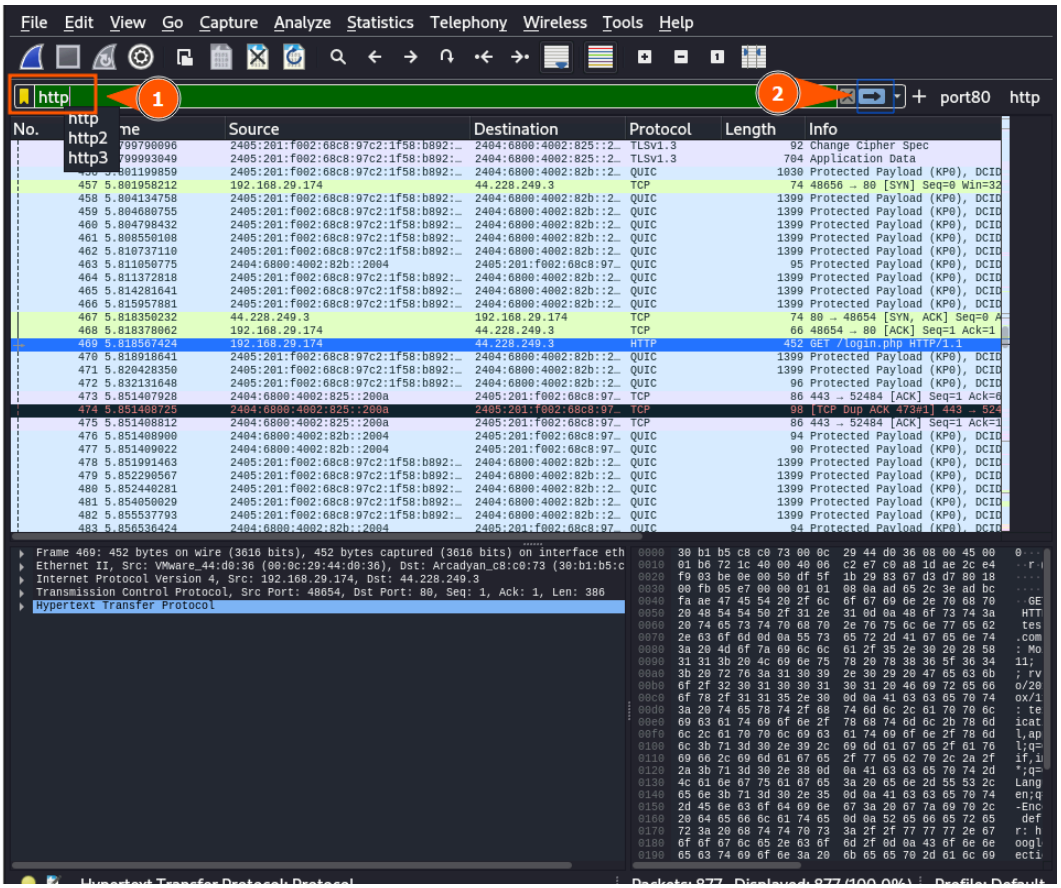
My image


user info
Not secure
testphp.vulnweb.com...
Verify it's you
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
John Smith (test)
On this page you can visualize or edit you user information.
Name:
John Smith
Credit card number:
1234-5678-2300-9000
E-Mail:
email@email.com
Phone number:
2323345
Address:
21 street
update
You have 0 items in your cart. You visualize you cart here.
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

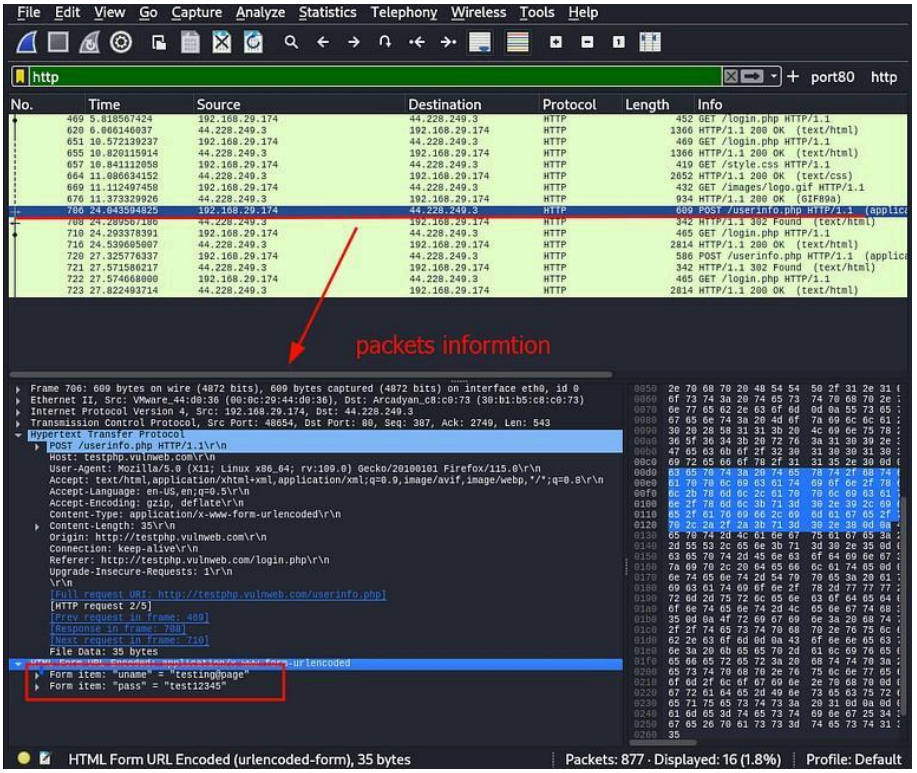
My image

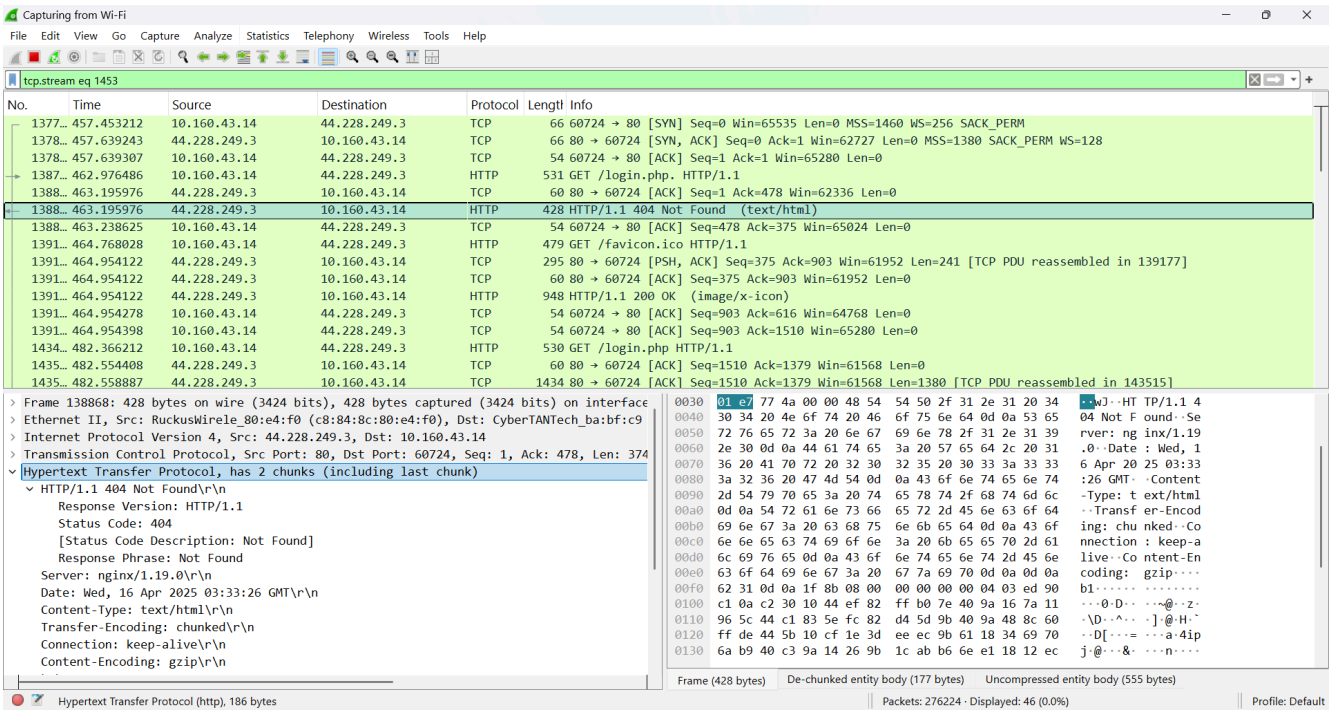

user info
Not secure
testphp.vulnweb.com...
Verify it's you
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Rina Mowal (test)
On this page you can visualize or edit you user information.
Name:
Rina Mowal
Credit card number:
7777-8545-5214-4512
E-Mail:
rina@email.com
Phone number:
2323345
Address:
21 street
update
You have 0 items in your cart. You visualize you cart here.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

My image

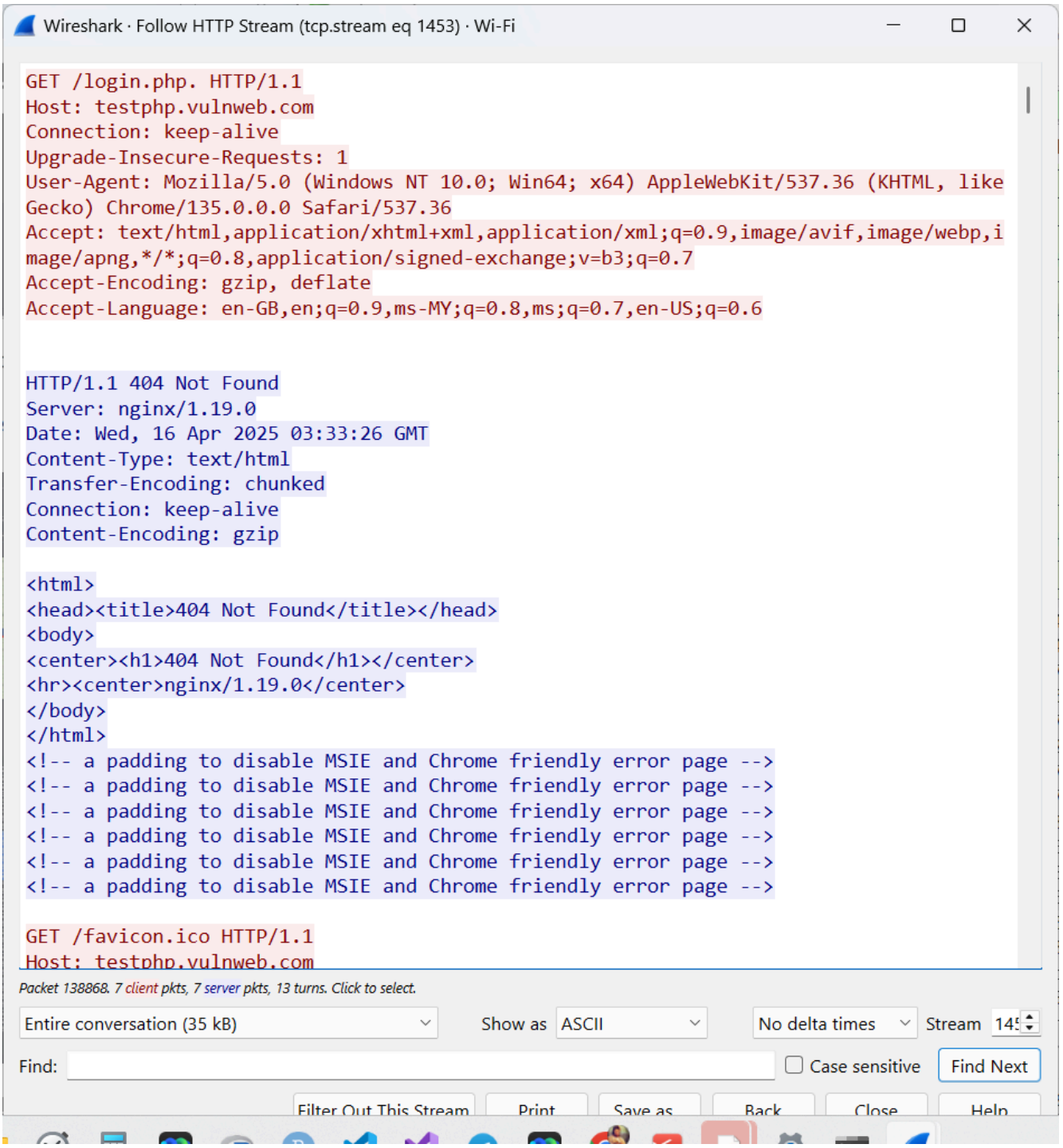


6. Look through the filtered packets for the HTTP POST request that contains the login credentials. This typically includes a packet where the form data is being sent to the server.
7. Right-click on the packet and select “Follow > HTTP Stream” to see the entire HTTP conversation.




Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1453
No. Time Source Destination Protocol Length Info
1377… 457.453212 10.160.43.14 44.228.249.3 TCP 66 60724 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
1378… 457.639243 44.228.249.3 10.160.43.14 TCP 66 80 → 60724 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1380 SACK_PERM WS=128
1378… 457.639307 10.160.43.14 44.228.249.3 TCP 54 60724 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1387… 462.976486 10.160.43.14 44.228.249.3 HTTP 531 GET /login.php. HTTP/1.1
1388… 463.195976 44.228.249.3 10.160.43.14 TCP 60 80 → 60724 [ACK] Seq=1 Ack=478 Win=62336 Len=0
1388… 463.195976 44.228.249.3 10.160.43.14 HTTP 428 HTTP/1.1 404 Not Found (text/html)
1388… 463.238625 10.160.43.14 44.228.249.3 TCP 54 60724 → 80 [ACK] Seq=478 Ack=375 Win=65024 Len=0
1391… 464.768028 10.160.43.14 44.228.249.3 HTTP 479 GET /favicon.ico HTTP/1.1
1391… 464.954122 44.228.249.3 10.160.43.14 TCP 295 80 → 60724 [PSH, ACK] Seq=375 Ack=903 Win=61952 Len=241 [TCP PDU reassembled in 139177]
1391… 464.954122 44.228.249.3 10.160.43.14 TCP 60 80 → 60724 [ACK] Seq=375 Ack=903 Win=61952 Len=0
1391… 464.954122 44.228.249.3 10.160.43.14 HTTP 948 HTTP/1.1 200 OK (image/x-icon)
1391… 464.954278 10.160.43.14 44.228.249.3 TCP 54 60724 → 80 [ACK] Seq=903 Ack=616 Win=64768 Len=0
1391… 464.954398 10.160.43.14 44.228.249.3 TCP 54 60724 → 80 [ACK] Seq=903 Ack=1510 Win=65280 Len=0
1434… 482.366212 10.160.43.14 44.228.249.3 HTTP 530 GET /login.php HTTP/1.1
1435… 482.554408 44.228.249.3 10.160.43.14 TCP 60 80 → 60724 [ACK] Seq=1510 Ack=1379 Win=61568 Len=0
1435… 482.558887 44.228.249.3 10.160.43.14 TCP 1434 80 → 60724 [ACK] Seq=1510 Ack=1379 Win=61568 Len=1380 [TCP PDU reassembled in 143515]
Frame 138868: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface
Ethernet II, Src: RuckusWirele_80:e4:f0 (c8:84:8c:80:e4:f0), Dst: CyberTANTech_ba:bf:c9
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 10.160.43.14
Transmission Control Protocol, Src Port: 80, Dst Port: 60724, Seq: 1, Ack: 478, Len: 374
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
HTTP/1.1 404 Not Found\r\n
Response Version: HTTP/1.1
Status Code: 404
[Status Code Description: Not Found]
Response Phrase: Not Found
Server: nginx/1.19.0\r\n
Date: Wed, 16 Apr 2025 03:33:26 GMT\r\n
Content-Type: text/html\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
Content-Encoding: gzip\r\n
0030 01 e7 77 4a 00 00 48 54 54 50 2f 31 2e 31 20 34
0040 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 53 65
0050 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e 31 39
0060 2e 30 0d 0a 44 61 74 65 3a 20 57 65 64 2c 20 31
0070 36 20 41 70 72 20 32 30 32 35 20 30 33 3a 33 33
0080 3a 32 36 20 47 4d 54 0d 0a 43 6f 6e 74 65 6e 74
0090 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c
00a0 0d 0a 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64
00b0 69 6e 67 3a 20 63 68 75 6e 6b 65 64 0d 0a 43 6f
00c0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61
00d0 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e
00e0 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0d 0a 0d 0a
00f0 62 31 0d 0a 1f 8b 08 00 00 00 00 00 04 03 ed 90
0100 c1 0a c2 30 10 44 ef 82 ff b0 7e 40 9a 16 7a 11
0110 96 5c 44 c1 83 5e fc 82 d4 5d 9b 40 9a 48 8c 60
0120 ff de 44 5b 10 cf 1e 3d ee ec 9b 61 18 34 69 70
0130 6a b9 40 c3 9a 14 26 9b 1c ab b6 6e e1 18 12 ec
Frame (428 bytes) De-chunked entity body (177 bytes) Uncompressed entity body (555 bytes)
Hypertext Transfer Protocol (http), 186 bytes
Packets: 276224 · Displayed: 46 (0.0%)
Profile: Default

My image


Wireshark · Follow HTTP Stream (tcp.stream eq 1453) · Wi-Fi
GET /login.php. HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
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-GB,en;q=0.9,ms-MY;q=0.8,ms;q=0.7,en-US;q=0.6
HTTP/1.1 404 Not Found
Server: nginx/1.19.0
Date: Wed, 16 Apr 2025 03:33:26 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Content-Encoding: gzip
<html>
<head><title>404 Not Found</title></head>
<body>
<h1>404 Not Found</h1>
<hr> nginx/1.19.0
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
GET /favicon.ico HTTP/1.1
Host: testphp.vulnweb.com
Packet 138868. 7 client pkts, 7 server pkts, 13 turns. Click to select.
Entire conversation (35 kB)
Show as
ASCII
No delta times
Stream
Find:
Case sensitive
Find Next
Filter Out This Stream
Print
Save as
Back
Close
Help

My image