



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
20105	62.546830	10.160.37.208	255.255.255.255	UDP	60	61224 → 3289 Len=14
20106	62.546893	10.160.41.150	10.160.47.255	NBNS	92	Name query NB <01><02>_MSBROWSE_<02><01>
20107	62.547696	10.160.41.150	10.160.47.255	NBNS	92	Name query NB <01><02>_MSBROWSE_<02><01>
20108	62.547956	10.160.42.15	10.160.47.255	DTLS	437	Continuation Data
20109	62.547956	::	ff02::1:ff54:54a6	ICMPv6	86	Neighbor Solicitation for fe80::10d5:f636:2054:54a6
20110	62.548994	10.160.34.91	10.160.47.255	NBNS	92	Name query NB BRWE86F385C167D<00>
20111	62.548994	Intel_ac:44:9b	Broadcast	ARP	60	Who has 10.160.34.21? Tell 10.160.35.10
20112	62.549517	Intel_ac:44:9b	Broadcast	ARP	60	Who has 10.160.34.215? Tell 10.160.35.10
20113	62.549555	fe80::10d5:f636:205...	ff02::2	ICMPv6	62	Router Solicitation
20114	62.550649	ba:65:8f:f1:a1:be	Broadcast	ARP	60	Who has 10.160.45.235? Tell 10.160.41.150
20115	62.550649	10.160.41.150	224.0.0.251	MDNS	207	Standard query response 0x0000 PTR _companion-link._tcp.local TXT
20116	62.550649	fe80::1423:7f3b:7b7...	ff02::fb	MDNS	227	Standard query response 0x0000 PTR _companion-link._tcp.local TXT
20117	62.550649	fe:6b:d5:7f:bd:fc	Broadcast	ARP	60	ARP Announcement for 10.160.35.22
20118	62.649139	10.160.41.161	224.0.0.251	MDNS	438	Standard query response 0x0000 TXT, cache flush PTR _rdlink._tcp.local PTR Noraini Ibrahim's iPhone._rdli

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF...
 > Ethernet II, Src: AzureWaveTec_79:f7:52 (c0:bf:be:79:f7:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > 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)

0000 ff ff ff ff ff c0 bf be 79 f7 52 08 00 45 00y.R..E..
 0010 00 38 9d 34 00 00 80 11 72 af 0a a0 20 32 ff ff ..8.4....p...2..
 0020 ff ff e8 ad 56 ce 00 24 d0 12 53 54 52 5f 42 43V...\$...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 00 00 00 00 00 00 00 00 00 00 0...d1

Wi-Fi: <live capture in progress> Packets: 20118 Profile: Default

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.

Mid Panel

- > 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
- > 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)

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

Bottom Panel (to hide this go to view and untick packet bytes)

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 00y.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 43V...\$..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\NPF
- > Ethernet II, Src: AzureWaveTec_79:f7:52 (c0:bf:be:79:f7:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- > 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)

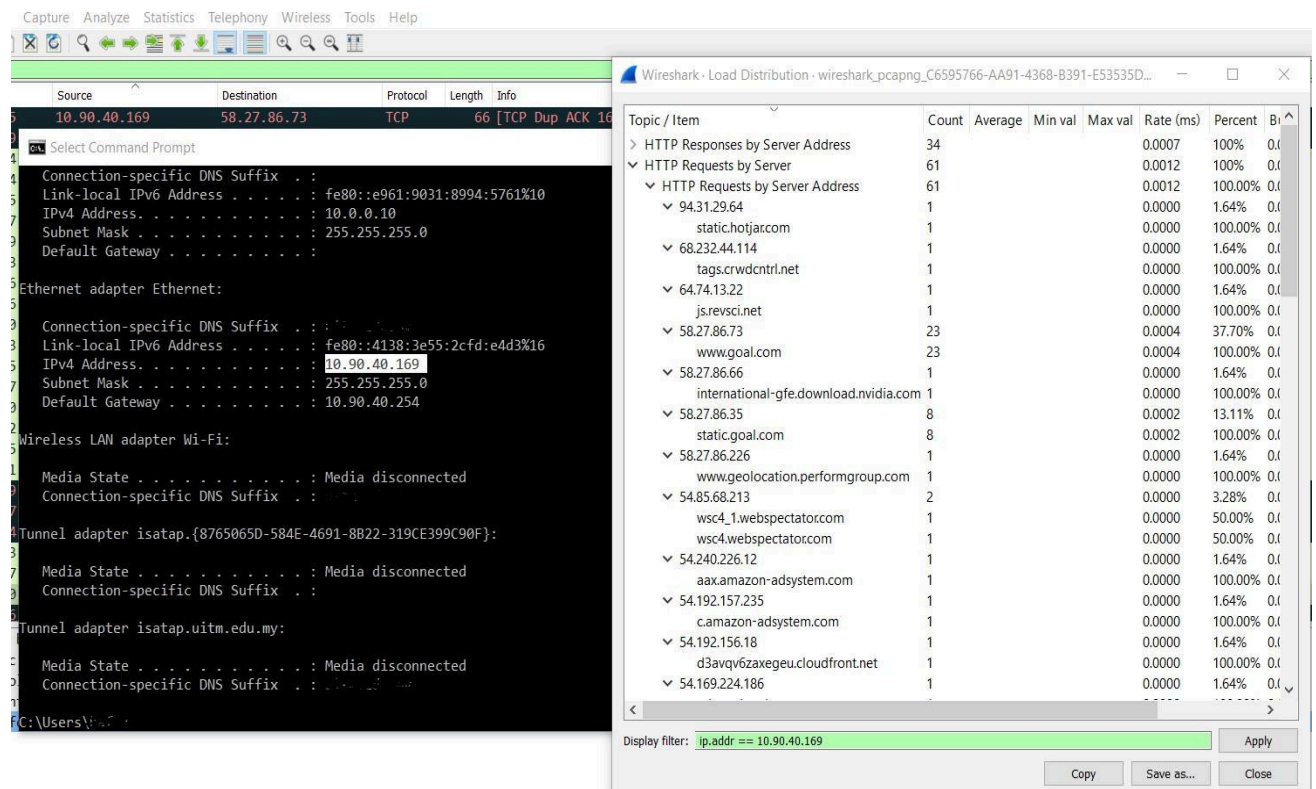
HTTP (Hypertext Transfer Protocol) is a client-server communication protocol used to transfer HTML files.

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	

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.

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets, filtered by 'http'. The middle pane shows the packet details for the selected packet (No. 407), highlighting the 'Hypertext Transfer Protocol' section. The bottom pane shows the raw packet data in hexadecimal and ASCII, with the ASCII column displaying the text 'My image'.

No.	Time	Source	Destination	Protocol	Length	Info
232	10.416639	192.168.1.2	1.9.56.66	HTTP	948	GET / HTTP/1.1
253	10.473174	1.9.56.66	192.168.1.2	HTTP	320	HTTP/1.1 301 Moved Permanently
254	10.477852	192.168.1.2	1.9.56.66	HTTP	1005	GET /en-my HTTP/1.1
342	10.747396	1.9.56.66	192.168.1.2	HTTP	699	HTTP/1.1 200 OK (text/html)
344	10.755282	192.168.1.2	1.9.56.25	HTTP	839	GET /3276700/3276742_herol.jpg HTTP/1.1
383	10.924022	192.168.1.2	104.66.23.140	HTTP	540	GET /JS/socialize.js?apikey=2_Y8Ou2zve7e5ZI-lzS_Sx1CPu92065T9xjCUz9vXSC60PxafAuK2Z5FPv0_twf57D HTTP/1.1
386	10.960965	104.66.23.140	192.168.1.2	HTTP	320	HTTP/1.1 304 Not Modified
389	10.968991	192.168.1.2	54.240.226.12	HTTP	489	GET /e/dtb/bid?src=3117&u=http%3A%2F%2Fwww.goal.com%2Fen-my%2F36502 HTTP/1.1
401	11.096674	192.168.1.2	64.74.13.22	HTTP	535	GET /gateway/gw.js?csid=F09828&auto=t&bpid=performgroup HTTP/1.1
403	11.109578	192.168.1.1	192.168.1.2	ICMP	590	Destination unreachable (Fragmentation needed)
405	11.124578	54.240.226.12	192.168.1.2	HTTP	270	HTTP/1.1 200 OK (text/javascript)
408	11.289814	192.168.1.2	1.9.56.25	HTTP	839	GET /3211300/3211362_herol.jpg HTTP/1.1
410	11.291222	192.168.1.2	1.9.56.25	HTTP	839	GET /2070700/2070732_herol.jpg HTTP/1.1
411	11.291354	192.168.1.2	1.9.56.25	HTTP	839	GET /3277600/3277692_herol.jpg HTTP/1.1
442	11.462049	1.9.56.25	192.168.1.2	HTTP	1140	HTTP/1.1 200 OK (JPEG JFIF image)
448	11.477101	192.168.1.2	1.9.56.25	HTTP	840	GET /3275300/3275392_tsasaw.jpg HTTP/1.1
472	11.564168	1.9.56.25	192.168.1.2	HTTP	1301	HTTP/1.1 200 OK (JPEG JFIF image)
475	11.565888	192.168.1.2	1.9.56.25	HTTP	842	GET /3277300/3277372_sq_thumb.jpg HTTP/1.1
509	11.671056	1.9.56.25	192.168.1.2	HTTP	437	HTTP/1.1 200 OK (JPEG JFIF image)
511	11.676468	1.9.56.25	192.168.1.2	HTTP	1171	HTTP/1.1 200 OK (JPEG JFIF image)
516	11.677368	192.168.1.2	54.169.169.78	HTTP	1511	GET /5/c-3376/pey/callback-processaads HTTP/1.1
521	11.680535	192.168.1.2	104.66.28.17	HTTP	556	GET /di/library/Goal_Malaysia/49/63/jdt-vs-selangor-msl-2016_b42ycl7fw7d7112st4iv4udl9.jpg?e=56694906&w=1408&h=130 HTTP/1.1
534	11.732964	192.168.1.2	104.66.28.17	HTTP	545	GET /di/library/GOAL_INTERNAIONAL/5/92/jamie-vardy_1w8hvyxlnfoj1tx33xz3jyhd.jpg?e=852372628&w=408&h=40 HTTP/1.1
537	11.733164	192.168.1.2	104.66.28.17	HTTP	558	GET /di/library/GOAL_uk/90/ba/hd-ilkay-gundogan-borussia-dortmund_h6x9fydwnssxlu0c48679q739.jpg?e=272280588&w=408&h=40 HTTP/1.1
539	11.733314	192.168.1.2	104.66.28.17	HTTP	552	GET /di/library/Goal_France/e9/86/dmitri-sychev-marseille_169vviu372wd1d1rnhw7x73t.jpg?e=773613007&w=408&h=40 HTTP/1.1

Frame 407: 407 bytes on wire (3256 bits), 407 bytes captured (3256 bits) on interface 0
Ethernet II, Src: CyberTANTech.ba:bf:c9 (00:45:e2:ba:bf:c9), Dst: Cisco_f5:13:9f (88:c5:fd:13:9f:00)
Internet Protocol Version 4, Src: 10.160.43.14, Dst: 203.121.59.248
Transmission Control Protocol, Src Port: 57668, Dst Port: 80, Seq: 1, Ack: 1, Len: 353
Hypertext Transfer Protocol

0000 88 fc 5d f5 13 9f 00 45 e2 ba bf c9 08 00 45 00 ...]...E.....E
0010 01 89 29 6d 40 00 80 06 92 e2 0a a0 2b 0e cb 79 ...m...+...y
0020 3b f8 e1 44 00 50 1e 81 4b e2 dc b6 1e 9a 50 18 ...D.P...K...P
0030 0f ff 1d ab 00 00 48 45 41 44 20 2f 66 69 6c 65 ...HE AD /file
0040 73 74 72 65 61 6d 69 6e 67 73 65 72 76 69 63 65 streamin gservice
0050 2f 66 69 6c 65 73 2f 35 64 33 32 36 30 37 64 2d /files/5 d32607d
0060 65 65 61 39 2d 34 34 66 63 2d 61 63 35 35 2d 37 eea9-44f c-ac55-7
0070 37 38 30 30 62 39 38 36 32 61 35 3f 50 31 3d 31 7800b986 2a5P7P1=1
0080 37 34 35 33 35 36 32 38 34 26 50 32 3d 34 30 34 74535628 4&P2=404
0090 26 50 33 3d 32 26 50 34 3d 4d 68 4b 76 4b 78 44 8P3=2&P4 =MhKvKx0
00a0 63 36 7a 49 61 65 25 32 66 4d 76 38 45 52 49 75 c6Ziae%2 fMv8ERiu
00b0 33 52 43 69 67 44 67 44 55 4d 4f 41 25 32 62 64 3RCigDgD UMOA%2bd
00c0 64 45 68 5a 55 6c 66 73 38 31 6e 6a 67 65 61 69 dEhZulfs 81njgeai
00d0 69 76 6c 49 56 6f 70 4d 61 4e 30 6f 42 72 65 79 ivlIVopM aN00brey
00e0 46 6d 41 43 4d 68 6b 73 4d 5a 50 57 46 35 30 65 fMaCMhks MZPWf50e
00f0 6b 4f 67 25 33 64 25 33 64 20 48 54 54 50 2f 31 kOg%3d%3 d HTTP/1
0100 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 6a 20 .1.-Conn ection:
0110 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 65 Keep-Alli ve-Accep
0120 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d pt: */* -Accept-

My image

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

448	11.477101	192.168.1.2	1.9.56.25	HTTP	840	GET /3275300/3275392_tsasaw.jpg HTTP/1.1
472	11.564168	1.9.56.25	192.168.1.2	HTTP	1301	HTTP/1.1 200 OK (JPEG JFIF image)
475	11.565888	192.168.1.2	1.9.56.25	HTTP	842	GET /3277300/3277372_sq_thumb.jpg HTTP/1.1
509	11.671056	1.9.56.25	192.168.1.2	HTTP	437	HTTP/1.1 200 OK (JPEG JFIF image)
511	11.676468	1.9.56.25	192.168.1.2	HTTP	1171	HTTP/1.1 200 OK (JPEG JFIF image)

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

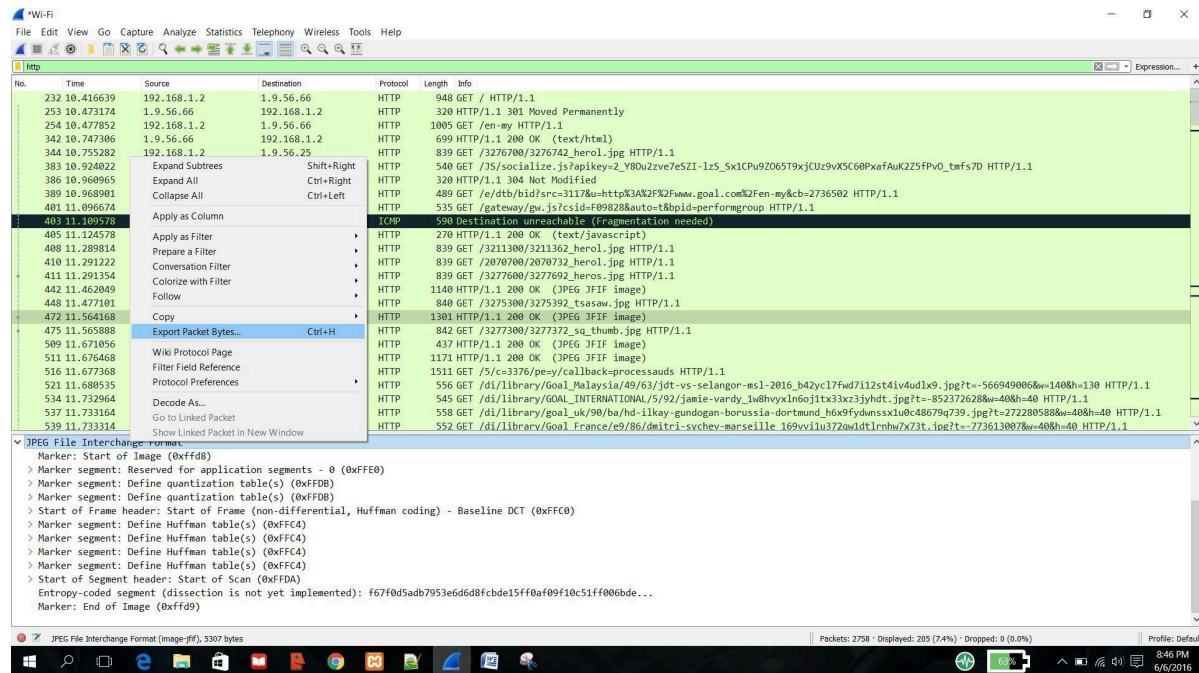
472	11.564168	1.9.56.25	192.168.1.2	HTTP	1301	HTTP/1.1 200 OK (JPEG JFIF image)
-----	-----------	-----------	-------------	------	------	-----------------------------------

Highlight it and go to the JPEG file Interchange format.

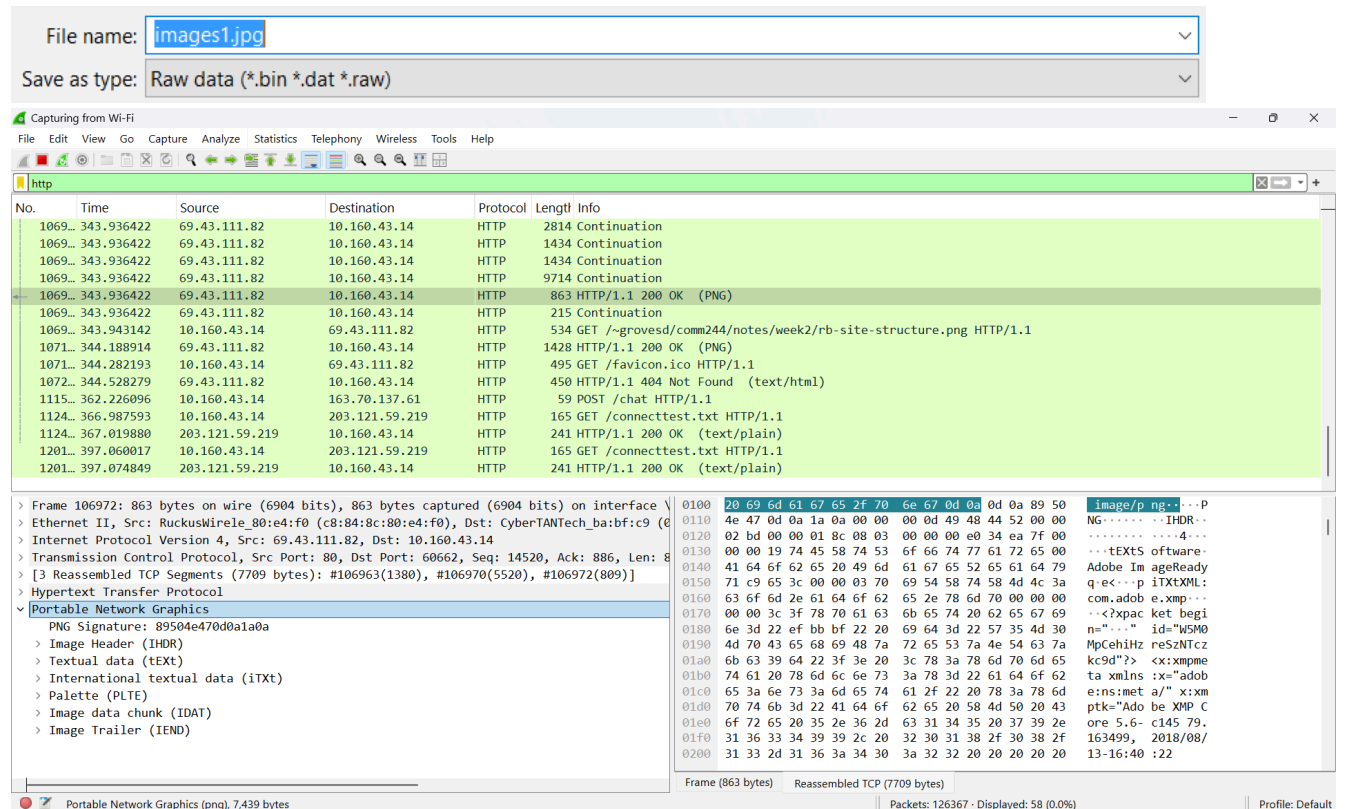
The image shows the packet details view for a selected packet (No. 472). The 'Hypertext Transfer Protocol' section is highlighted, and the 'JPEG File Interchange Format' section is visible below it.

Frame 472: 1301 bytes on wire (10408 bits), 1301 bytes captured (10408 bits) on interface 0
Ethernet II, Src: D-LinkCo_b8:48:bc (5c:d9:98:b8:48:bc), Dst: IntelCor_66:45:22 (08:d4:0c:66:45:22)
Internet Protocol Version 4, Src: 1.9.56.25, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 53204 (53204), Seq: 4357, Ack: 786, Len: 1247
[4 Reassembled TCP Segments (5603 bytes): #468(1452), #469(1452), #471(1452), #472(1247)]
Hypertext Transfer Protocol
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

testphp.vulnweb.com...

Verify it's you

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

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.

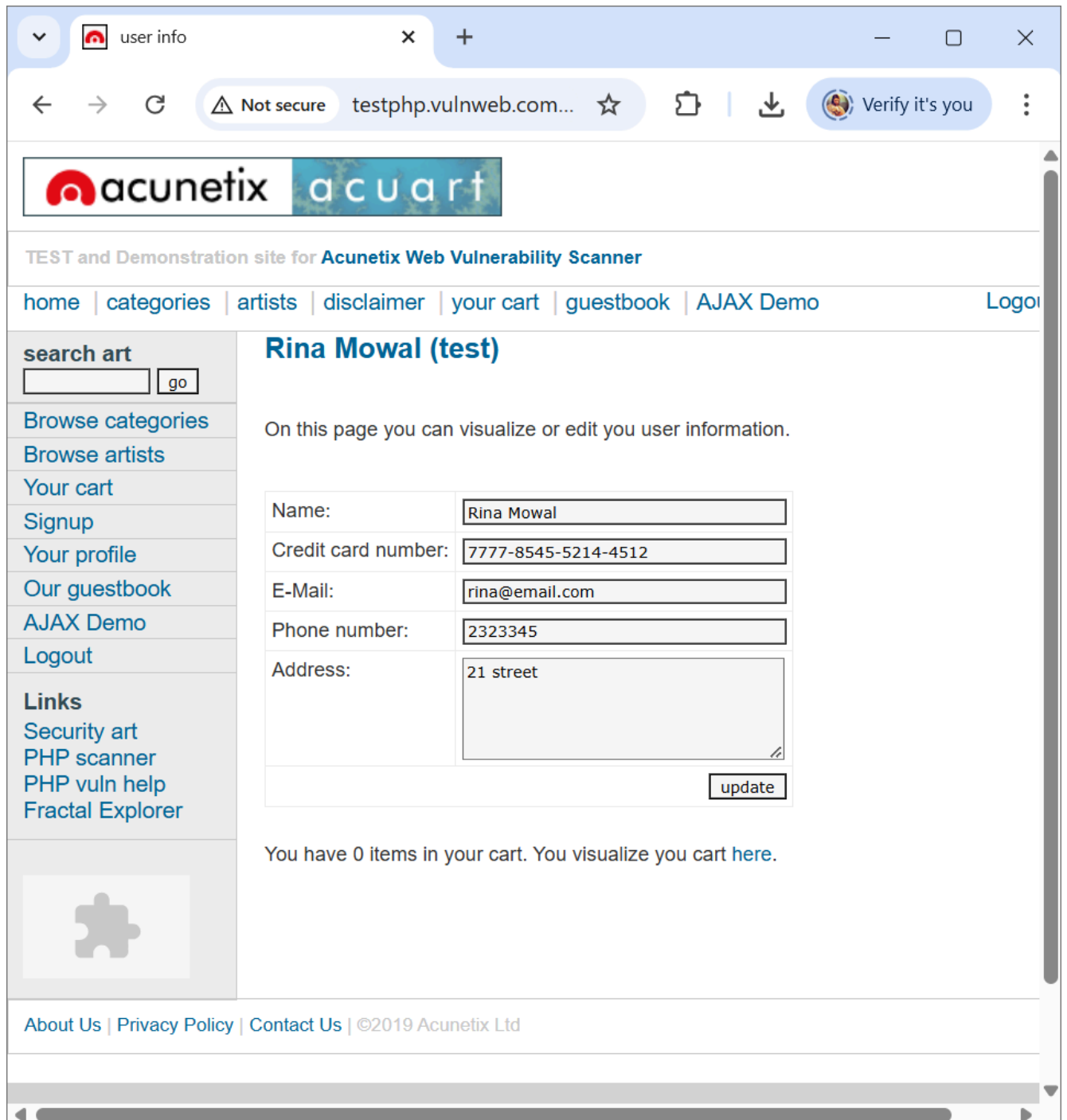
Name:	<input type="text" value="John Smith"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="email@email.com"/>
Phone number:	<input type="text" value="2323345"/>
Address:	<div><input type="text" value="21 street"/></div>
<input type="button" value="update"/>	

You have 0 items in your cart. You visualize you cart [here](#).

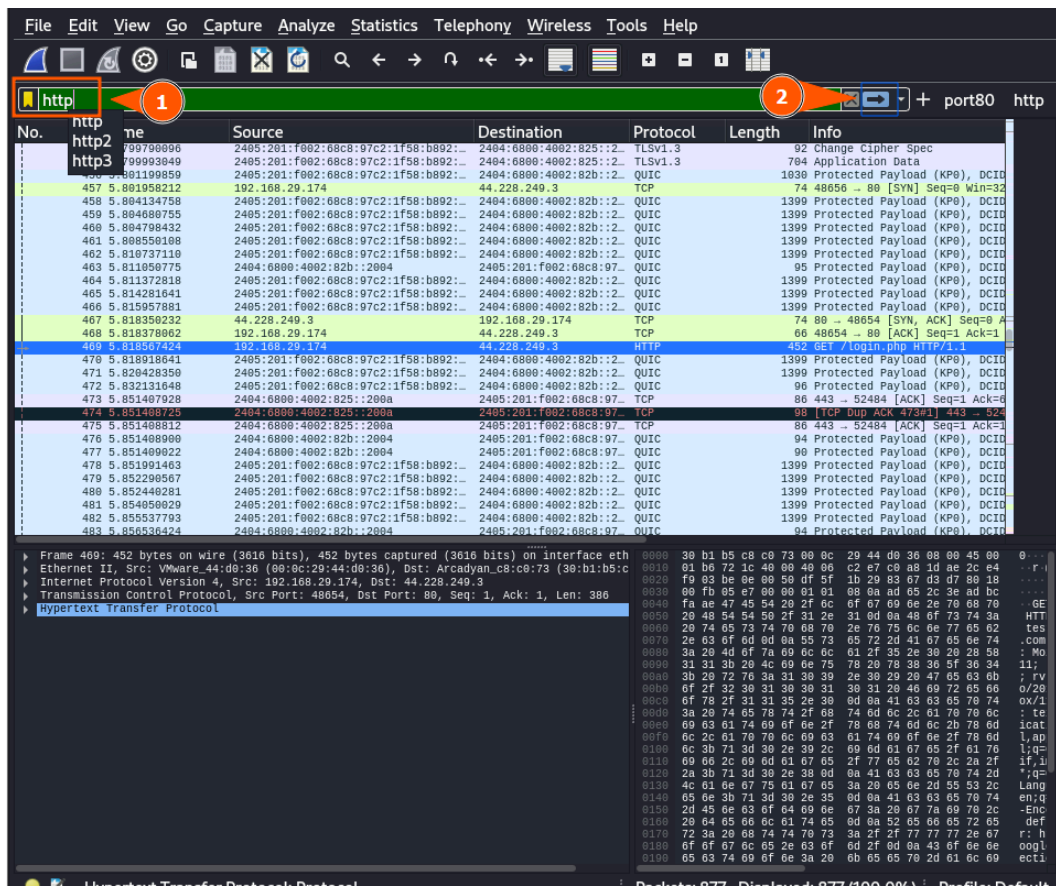
[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may

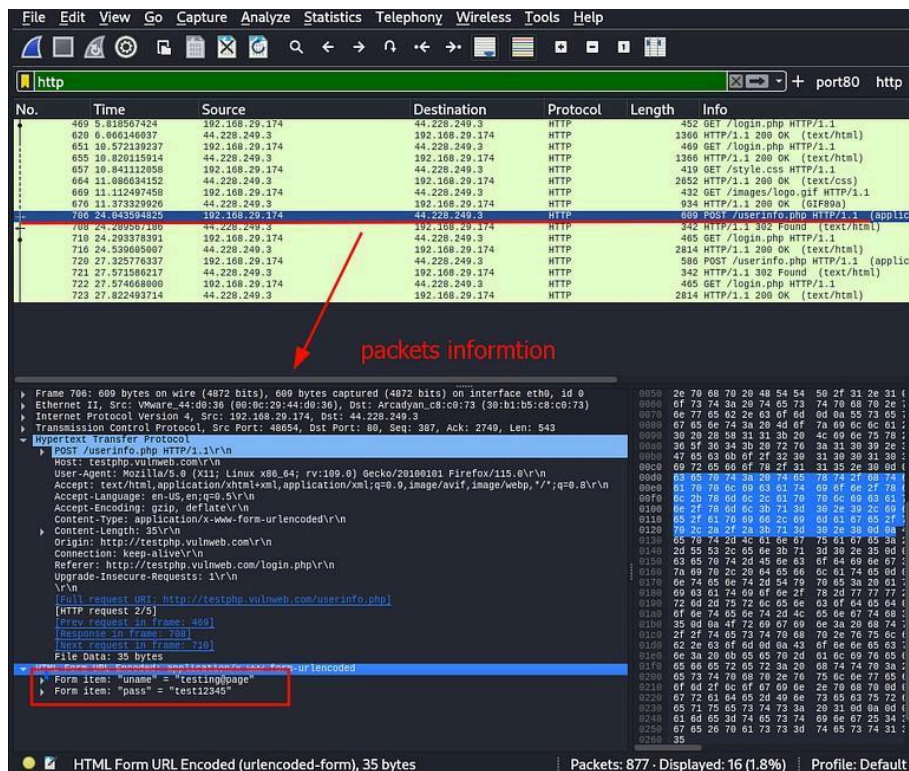
My image



My image



- 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.
- 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]

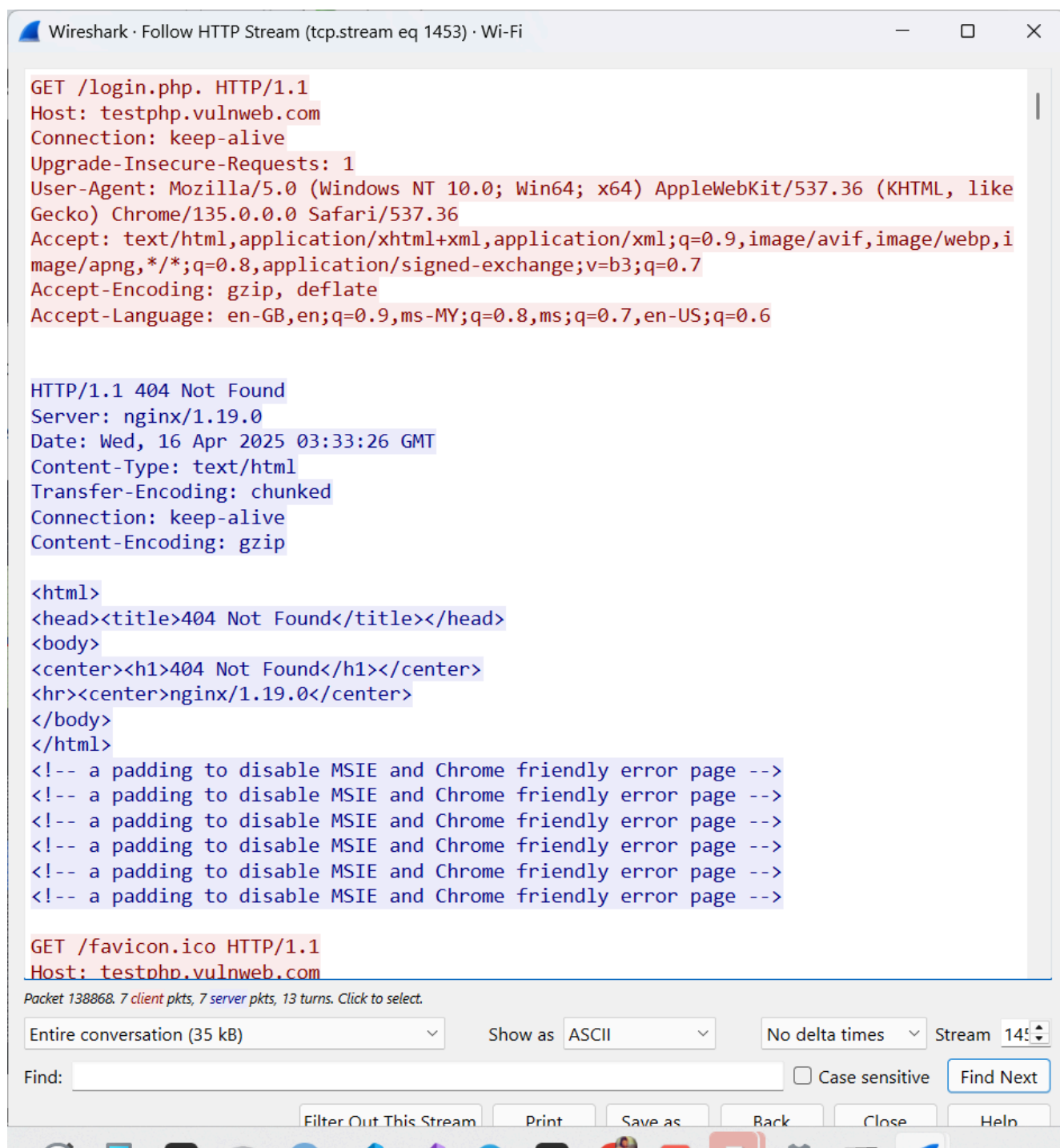
> Frame 138868: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface
> Ethernet II, Src: RuckusWirele_80:e4:f0 (c8:84:8c:80:e4:f0), Dst: CyberTANTech_ba:bf:c9
> Internet Protocol Version 4, Src: 44.228.249.3, Dst: 10.160.43.14
> Transmission Control Protocol, Src Port: 80, Dst Port: 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 00 77 4a 00 00 48 54 54 50 2f 31 2e 31 20 34 04 04 HT TP/1.1 4
0040 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 53 65 04 Not F ound-Se
0050 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e 31 39 rver: ng inx/1.19
0060 2e 30 0d 0a 44 61 74 65 3a 20 57 65 64 2c 20 31 0 Date : Wed, 1
0070 36 20 41 70 72 20 32 30 32 35 20 30 33 3a 33 33 6 Apr 20 25 03:33
0080 3a 32 36 20 47 4d 54 0d 0a 43 6f 6e 74 65 6e 74 :26 GMT Content
0090 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c Type: t ext/html
00a0 0d 0a 54 72 61 6e 73 66 65 72 2d 45 6e 63 6f 64 Transf er-Encod
00b0 69 6e 67 3a 20 63 68 75 6e 6b 65 64 0d 0a 43 6f ing: chu nkedCo
00c0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
00d0 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e liveCo ntent-En
00e0 63 6f 64 69 6e 67 3a 20 67 7a 69 70 0d 0a 0d 0a coding: gzip
00f0 62 31 0d 0a 1f 8b 08 00 00 00 00 00 04 03 ed 90 b1
0100 c1 0a c2 30 10 44 ef 82 ff b0 7e 40 9a 16 7a 11 00 00
0110 96 5c 44 c1 83 5e fc 82 d4 5d 9b 40 9a 48 8c 60 00 00
0120 ff de 44 5b 10 cf 1e 3d ee ec 9b 61 18 34 69 70 00 00
0130 6a b9 40 c3 9a 14 26 9b 1c ab b6 6e e1 18 12 ec j-@...&...n...

Frame (428 bytes) De-chunked entity body (177 bytes) Uncompressed entity body (555 bytes)

Packets: 276224 · Displayed: 46 (0.0%) Profile: Default

My image



My image