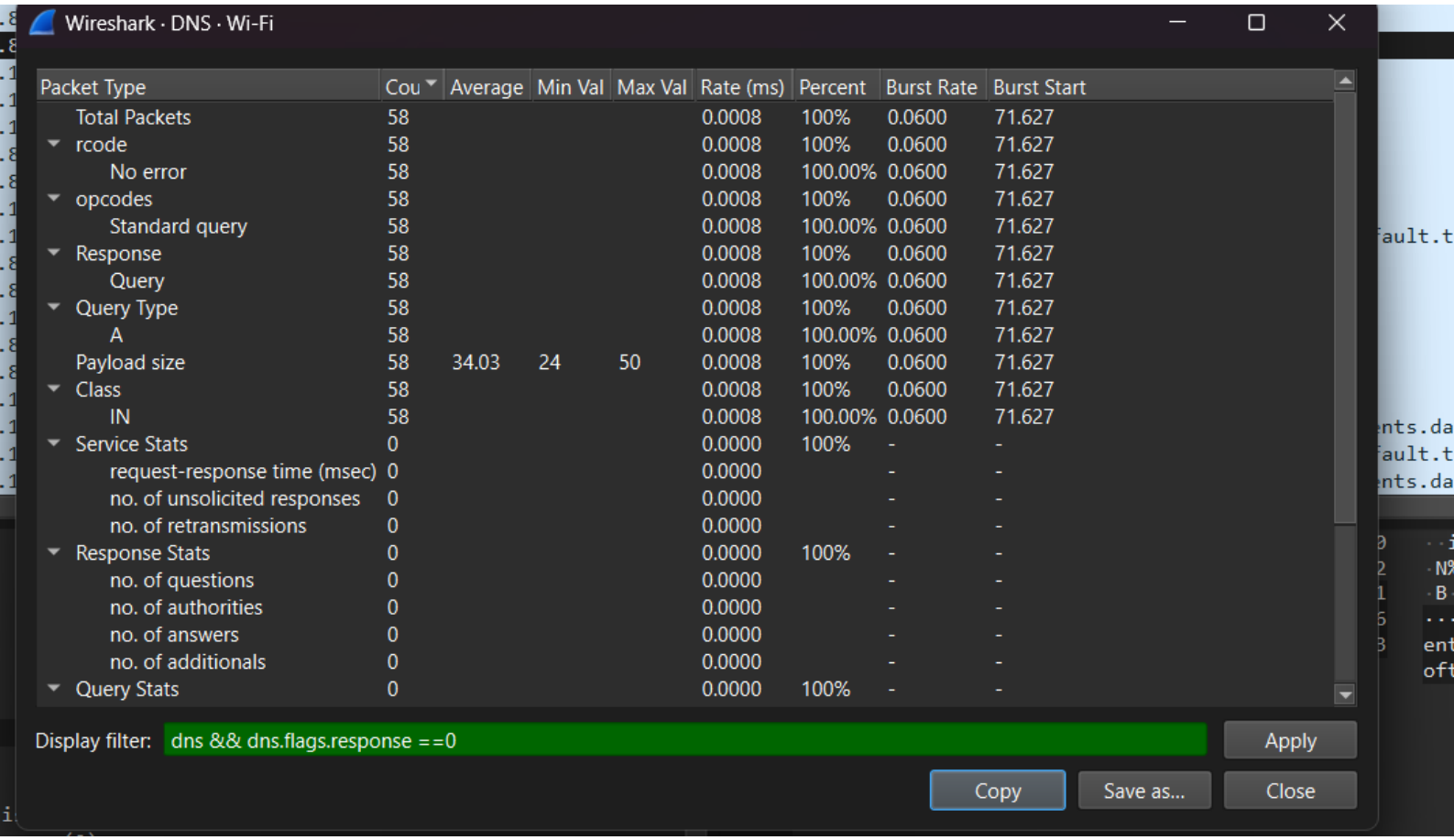
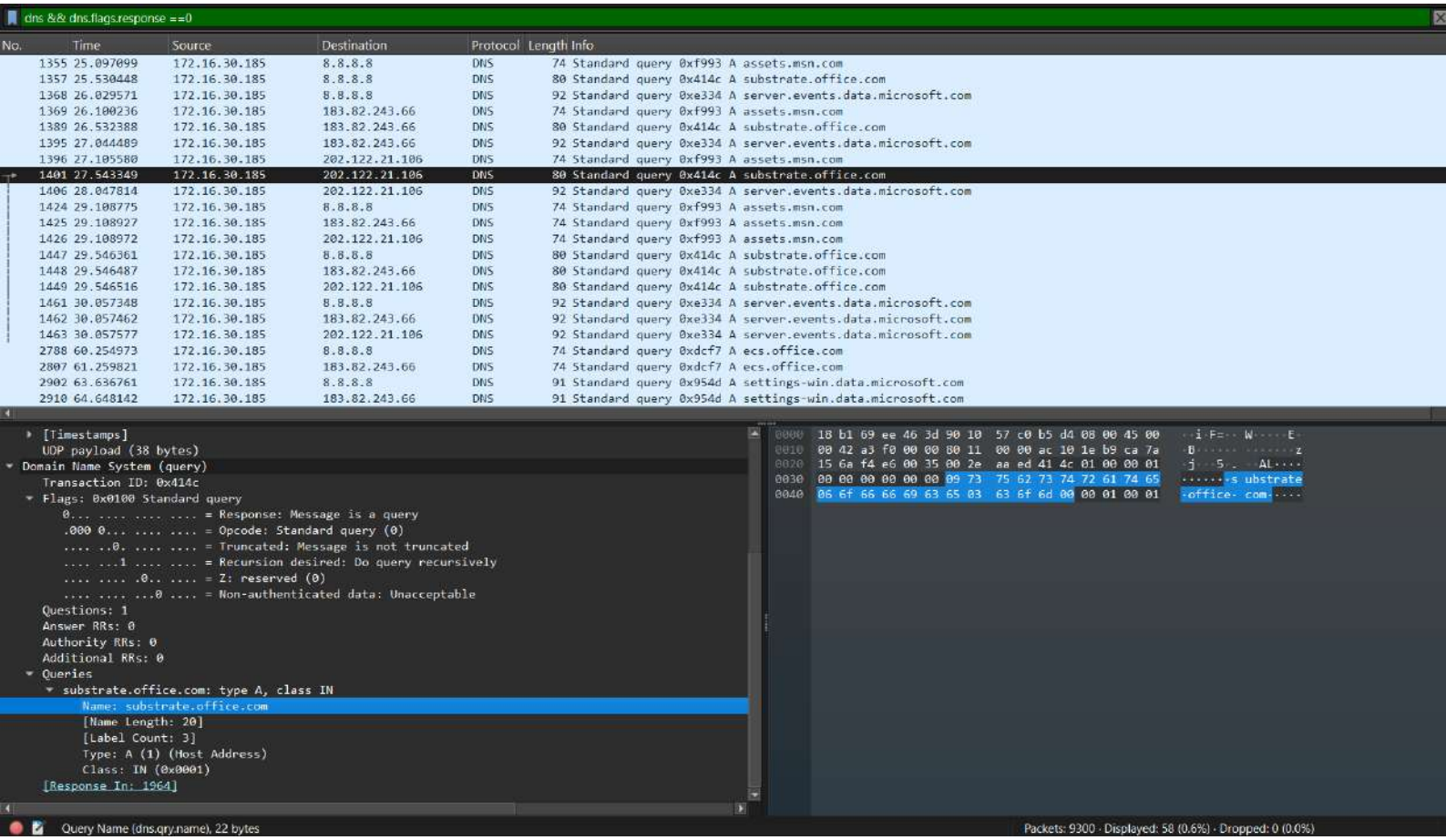
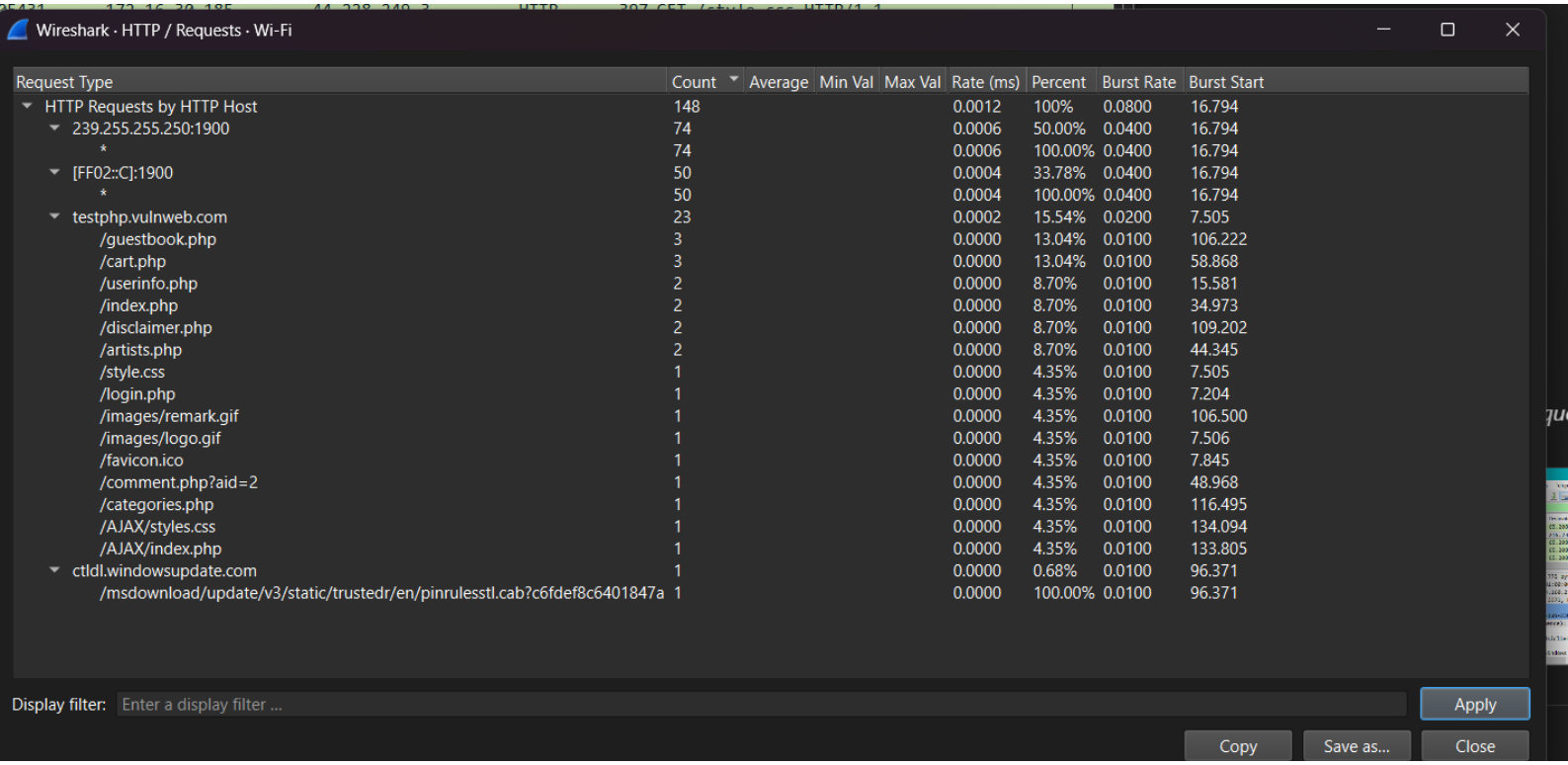
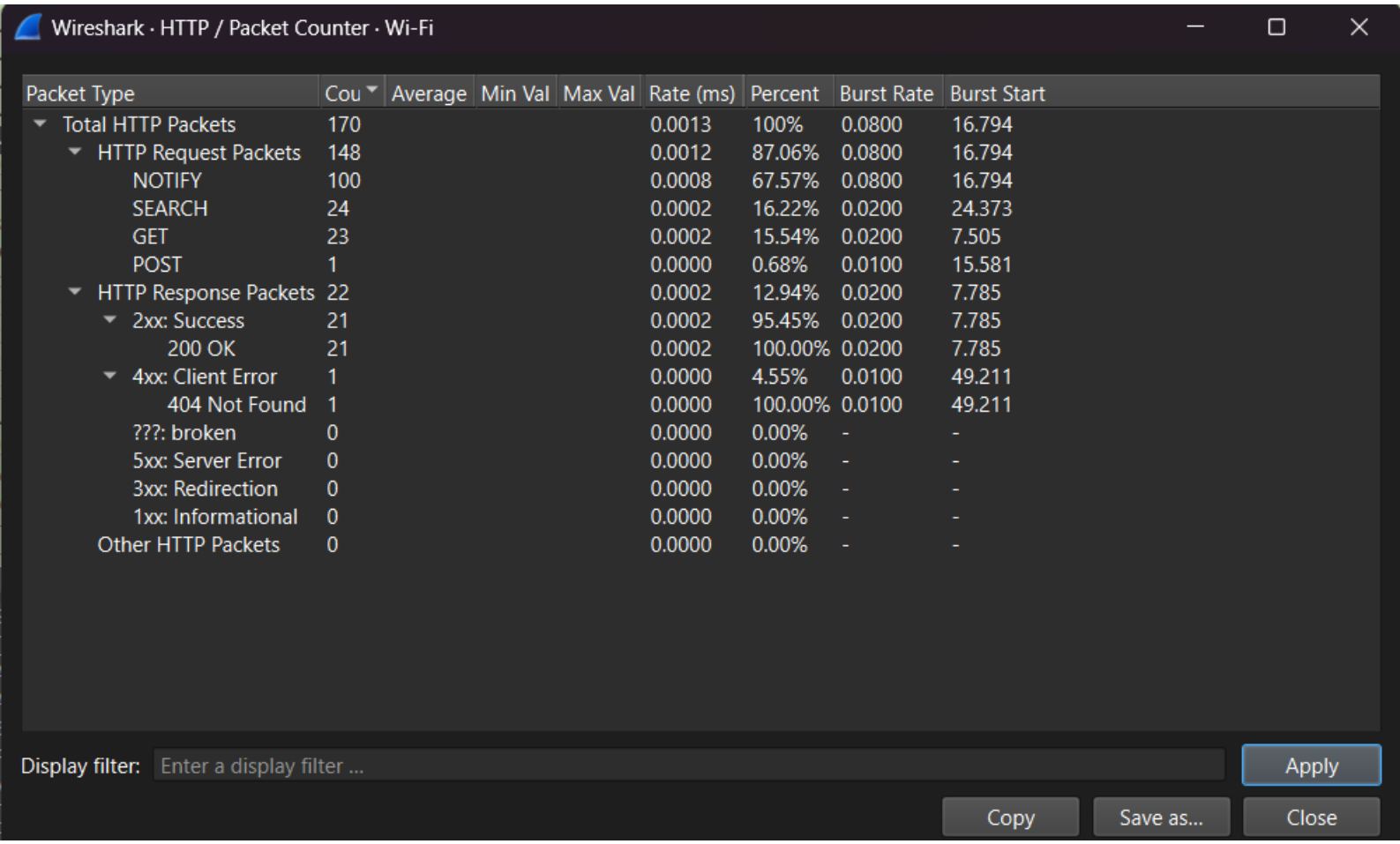

Wireshark · DNS · Wi-Fi
Packet Type
Cou
Average
Min Val
Max Val
Rate (ms)
Percent
Burst Rate
Burst Start
Total Packets 58 0.0008 100% 0.0600 71.627
rcode 58 0.0008 100% 0.0600 71.627
No error 58 0.0008 100.00% 0.0600 71.627
opcodes 58 0.0008 100% 0.0600 71.627
Standard query 58 0.0008 100.00% 0.0600 71.627
Response 58 0.0008 100% 0.0600 71.627
Query 58 0.0008 100.00% 0.0600 71.627
Query Type 58 0.0008 100% 0.0600 71.627
A 58 0.0008 100.00% 0.0600 71.627
Payload size 58 34.03 24 50 0.0008 100% 0.0600 71.627
Class 58 0.0008 100% 0.0600 71.627
IN 58 0.0008 100.00% 0.0600 71.627
Service Stats 0 0.0000 100% - -
request-response time (msec) 0 0.0000 - -
no. of unsolicited responses 0 0.0000 - -
no. of retransmissions 0 0.0000 - -
Response Stats 0 0.0000 100% - -
no. of questions 0 0.0000 - -
no. of authorities 0 0.0000 - -
no. of answers 0 0.0000 - -
no. of additionals 0 0.0000 - -
Query Stats 0 0.0000 100% - -
Display filter:
dns && dns.flags.response ==0
Apply
Copy
Save as...
Close

Ethernet · 2 | IPv4 · 3 | IPv6 | TCP | UDP · 40

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Du
172.16.30.185	49348	8.8.8.8	53	2	1 kB	174	2	100.00%	1	72 bytes	1	1 kB	76.832825	1
172.16.30.185	51064	8.8.8.8	53	3	1 kB	63	3	100.00%	2	184 bytes	1	1 kB	26.029571	6
172.16.30.185	53241	8.8.8.8	53	2	1 kB	183	2	100.00%	1	74 bytes	1	1 kB	89.890205	2
172.16.30.185	55531	8.8.8.8	53	3	1 kB	147	3	100.00%	2	132 bytes	1	1 kB	67.826904	5
172.16.30.185	57362	8.8.8.8	53	4	2 kB	145	4	100.00%	2	148 bytes	2	2 kB	67.672699	7
172.16.30.185	57913	8.8.8.8	53	2	1 kB	197	2	100.00%	1	83 bytes	1	1 kB	94.079491	2
172.16.30.185	58196	8.8.8.8	53	4	2 kB	144	4	100.00%	2	144 bytes	2	2 kB	67.610568	7
172.16.30.185	60427	8.8.8.8	53	2	1 kB	208	2	100.00%	1	72 bytes	1	1 kB	98.859584	0
172.16.30.185	62455	8.8.8.8	53	2	1 kB	207	2	100.00%	1	74 bytes	1	1 kB	98.847093	0
172.16.30.185	62491	8.8.8.8	53	2	1 kB	182	2	100.00%	1	66 bytes	1	1 kB	89.883358	2
172.16.30.185	62651	8.8.8.8	53	2	1 kB	184	2	100.00%	1	72 bytes	1	1 kB	89.890978	3
172.16.30.185	62694	8.8.8.8	53	3	1 kB	60	3	100.00%	2	160 bytes	1	1 kB	25.530448	9
172.16.30.185	62815	8.8.8.8	53	4	2 kB	59	4	100.00%	2	148 bytes	2	2 kB	25.097099	8
172.16.30.185	62948	8.8.8.8	53	2	1 kB	209	2	100.00%	1	66 bytes	1	1 kB	98.866671	0
172.16.30.185	63193	8.8.8.8	53	2	1 kB	131	2	100.00%	1	74 bytes	1	1 kB	60.254973	1
172.16.30.185	63952	8.8.8.8	53	2	1 kB	133	2	100.00%	1	91 bytes	1	1 kB	63.636761	3
172.16.30.185	49348	183.82.243.66	53	2	1 kB	177	2	100.00%	1	72 bytes	1	1 kB	77.834864	1
172.16.30.185	51064	183.82.243.66	53	3	1 kB	72	3	100.00%	2	184 bytes	1	1 kB	27.044489	5
172.16.30.185	53241	183.82.243.66	53	2	1 kB	191	2	100.00%	1	74 bytes	1	1 kB	90.890824	2
172.16.30.185	55531	183.82.243.66	53	3	1 kB	163	3	100.00%	2	132 bytes	1	1 kB	69.826097	5
172.16.30.185	57362	183.82.243.66	53	3	1 kB	162	3	100.00%	2	148 bytes	1	1 kB	69.691712	4
172.16.30.185	57913	183.82.243.66	53	2	1 kB	198	2	100.00%	1	83 bytes	1	1 kB	95.091058	1
172.16.30.185	58196	183.82.243.66	53	4	2 kB	161	4	100.00%	2	144 bytes	2	2 kB	69.624922	5
172.16.30.185	62491	183.82.243.66	53	2	1 kB	190	2	100.00%	1	66 bytes	1	1 kB	90.890821	2
172.16.30.185	62651	183.82.243.66	53	2	1 kB	192	2	100.00%	1	72 bytes	1	1 kB	90.890838	2
172.16.30.185	62694	183.82.243.66	53	2	160 bytes	71	2	100.00%	2	160 bytes	0	0 bytes	26.532388	3
172.16.30.185	62815	183.82.243.66	53	4	2 kB	64	4	100.00%	2	148 bytes	2	2 kB	26.100236	8
172.16.30.185	63193	183.82.243.66	53	2	1 kB	132	2	100.00%	1	74 bytes	1	1 kB	61.259821	1
172.16.30.185	63952	183.82.243.66	53	2	1 kB	134	2	100.00%	1	91 bytes	1	1 kB	64.648142	3
172.16.30.185	51064	202.122.21.106	53	3	1 kB	75	3	100.00%	2	184 bytes	1	1 kB	28.047814	5
172.16.30.185	53241	202.122.21.106	53	2	1 kB	194	2	100.00%	1	74 bytes	1	1 kB	91.896801	2
172.16.30.185	55531	202.122.21.106	53	3	1 kB	159	3	100.00%	2	132 bytes	1	1 kB	68.824599	5
172.16.30.185	57362	202.122.21.106	53	3	1 kB	158	3	100.00%	2	148 bytes	1	1 kB	68.680336	5
172.16.30.185	57913	202.122.21.106	53	2	1 kB	200	2	100.00%	1	83 bytes	1	1 kB	96.094535	0
172.16.30.185	58196	202.122.21.106	53	4	2 kB	156	4	100.00%	2	144 bytes	2	2 kB	68.615221	6
172.16.30.185	62491	202.122.21.106	53	1	66 bytes	196	1	100.00%	1	66 bytes	0	0 bytes	91.897104	0
172.16.30.185	62651	202.122.21.106	53	2	1 kB	195	2	100.00%	1	72 bytes	1	1 kB	91.896983	2
172.16.30.185	62694	202.122.21.106	53	3	1 kB	74	3	100.00%	2	160 bytes	1	1 kB	27.543349	5
172.16.30.185	62815	202.122.21.106	53	3	1 kB	73	3	100.00%	2	148 bytes	1	1 kB	27.105580	7
172.16.30.185	63952	202.122.21.106	53	2	1 kB	141	2	100.00%	1	91 bytes	1	1 kB	65.661684	3

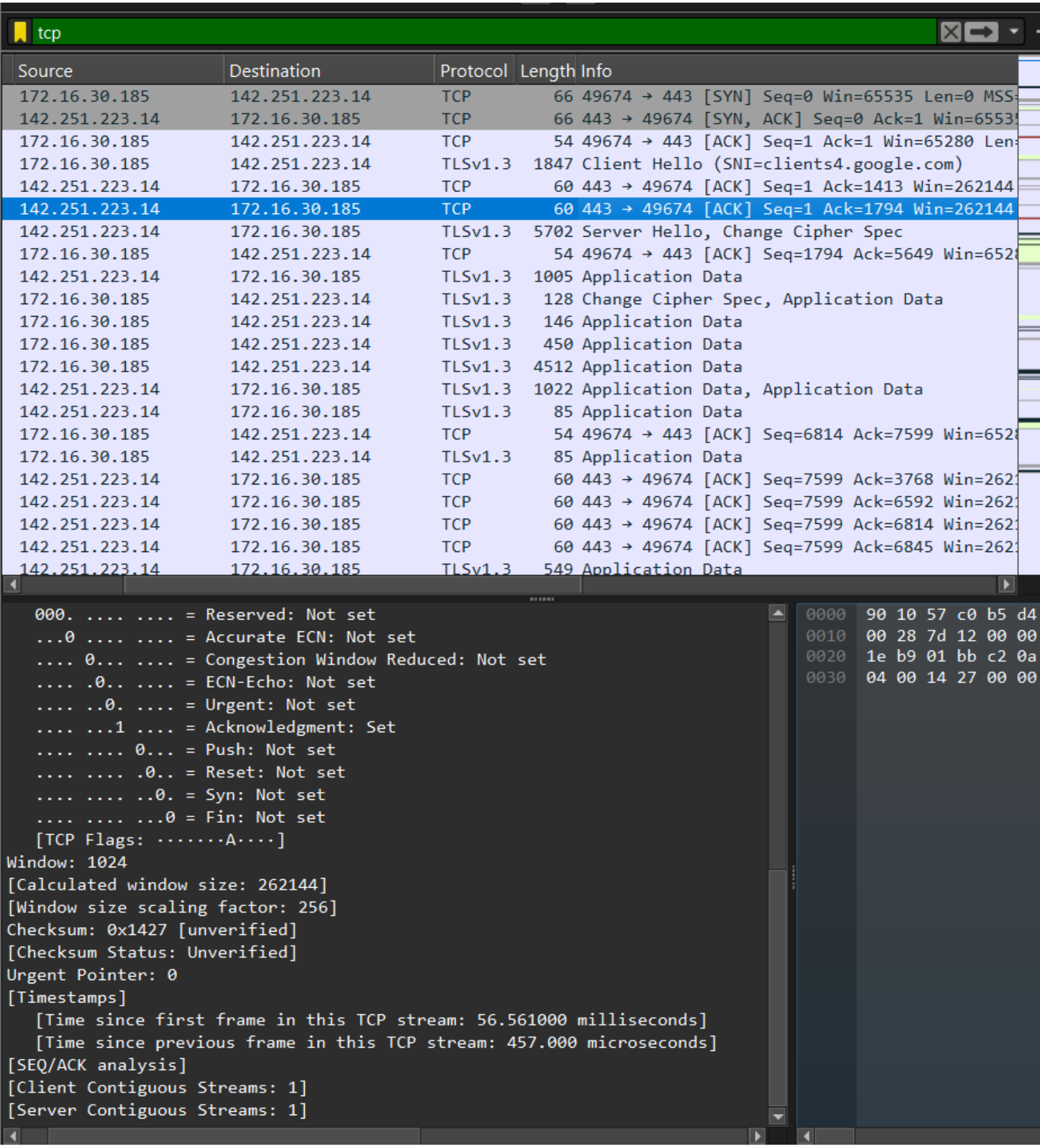

dns && dns.flags.response ==0
No. Time Source Destination Protocol Length Info
1355 25.097099 172.16.30.185 8.8.8.8 DNS 74 Standard query 0xf993 A assets.msn.com
1357 25.530448 172.16.30.185 8.8.8.8 DNS 80 Standard query 0x414c A substrate.office.com
1368 26.029571 172.16.30.185 8.8.8.8 DNS 92 Standard query 0xe334 A server.events.data.microsoft.com
1369 26.100236 172.16.30.185 183.82.243.66 DNS 74 Standard query 0xf993 A assets.msn.com
1389 26.532388 172.16.30.185 183.82.243.66 DNS 80 Standard query 0x414c A substrate.office.com
1395 27.044489 172.16.30.185 183.82.243.66 DNS 92 Standard query 0xe334 A server.events.data.microsoft.com
1396 27.105580 172.16.30.185 202.122.21.106 DNS 74 Standard query 0xf993 A assets.msn.com
1401 27.543349 172.16.30.185 202.122.21.106 DNS 80 Standard query 0x414c A substrate.office.com
1406 28.047814 172.16.30.185 202.122.21.106 DNS 92 Standard query 0xe334 A server.events.data.microsoft.com
1424 29.108775 172.16.30.185 8.8.8.8 DNS 74 Standard query 0xf993 A assets.msn.com
1425 29.108927 172.16.30.185 183.82.243.66 DNS 74 Standard query 0xf993 A assets.msn.com
1426 29.108972 172.16.30.185 202.122.21.106 DNS 74 Standard query 0xf993 A assets.msn.com
1447 29.546361 172.16.30.185 8.8.8.8 DNS 80 Standard query 0x414c A substrate.office.com
1448 29.546487 172.16.30.185 183.82.243.66 DNS 80 Standard query 0x414c A substrate.office.com
1449 29.546516 172.16.30.185 202.122.21.106 DNS 80 Standard query 0x414c A substrate.office.com
1461 30.057348 172.16.30.185 8.8.8.8 DNS 92 Standard query 0xe334 A server.events.data.microsoft.com
1462 30.057462 172.16.30.185 183.82.243.66 DNS 92 Standard query 0xe334 A server.events.data.microsoft.com
1463 30.057577 172.16.30.185 202.122.21.106 DNS 92 Standard query 0xe334 A server.events.data.microsoft.com
2788 60.254973 172.16.30.185 8.8.8.8 DNS 74 Standard query 0xdcf7 A ecs.office.com
2807 61.259821 172.16.30.185 183.82.243.66 DNS 74 Standard query 0xdcf7 A ecs.office.com
2902 63.636761 172.16.30.185 8.8.8.8 DNS 91 Standard query 0x954d A settings-win.data.microsoft.com
2910 64.648142 172.16.30.185 183.82.243.66 DNS 91 Standard query 0x954d A settings-win.data.microsoft.com
[Timestamps]
UDP payload (38 bytes)
Domain Name System (query)
Transaction ID: 0x414c
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
substrate.office.com: type A, class IN
Name: substrate.office.com
[Name Length: 20]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
[Response In: 1964]
0000 18 b1 69 ee 46 3d 90 10 57 c0 b5 d4 08 00 45 00
0010 00 42 a3 f0 00 00 80 11 00 00 ac 10 1e b9 ca 7a
0020 15 6a f4 e6 00 35 00 2e aa ed 41 4c 01 00 00 01
0030 00 00 00 00 00 00 09 73 75 62 73 74 72 61 74 65
0040 06 6f 66 66 69 63 65 03 63 6f 6d 00 00 01 00 01
Query Name (dns.qry.name), 22 bytes
Packets: 9300 · Displayed: 58 (0.6%) · Dropped: 0 (0.0%)

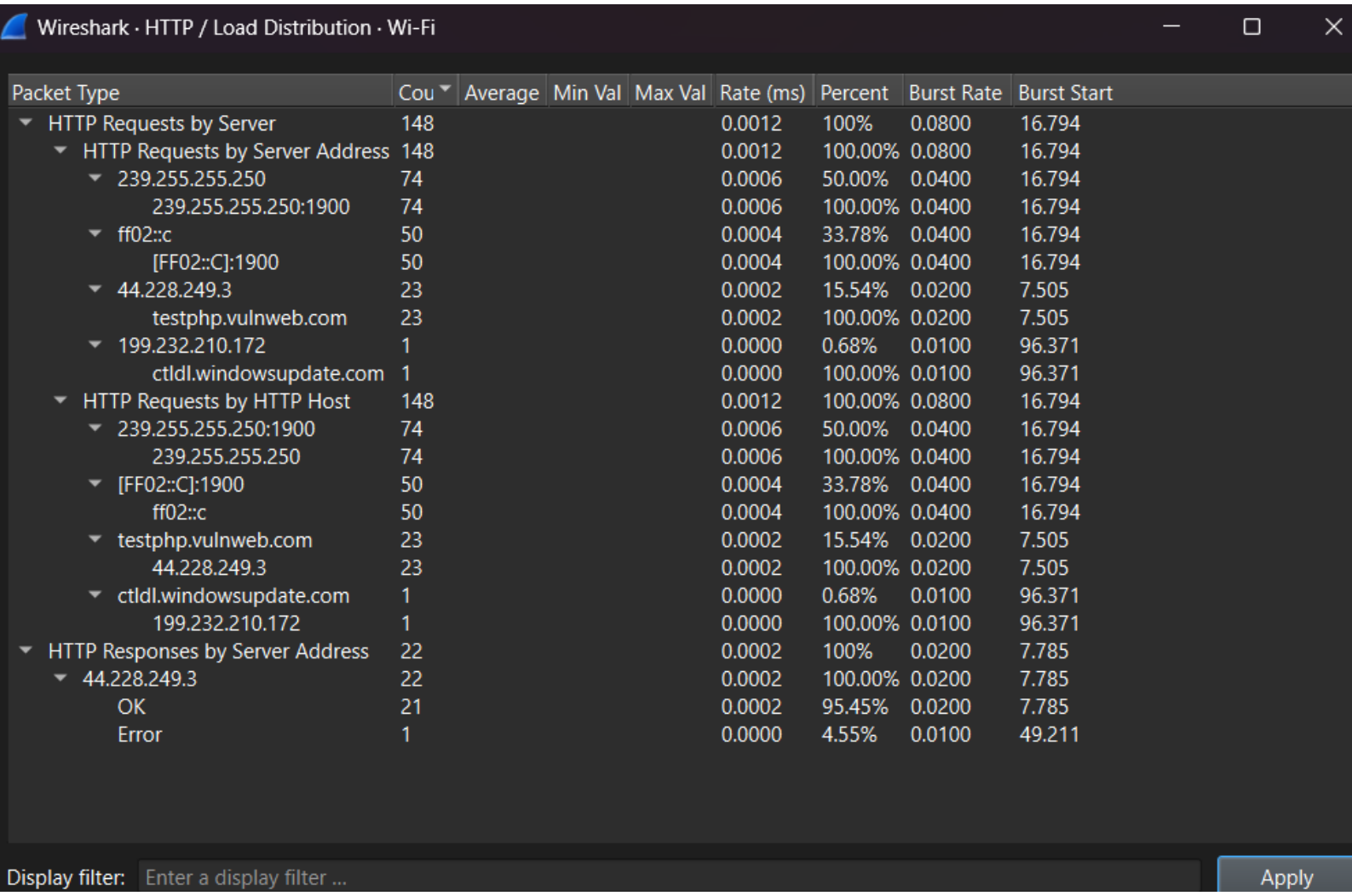

Wireshark · HTTP / Requests · Wi-Fi
Request Type | Count | Average | Min Val | Max Val | Rate (ms) | Percent | Burst Rate | Burst Start
HTTP Requests by HTTP Host | 148 | | | | 0.0012 | 100% | 0.0800 | 16.794
239.255.255.250:1900 | 74 | | | | 0.0006 | 50.00% | 0.0400 | 16.794
* | 74 | | | | 0.0006 | 100.00% | 0.0400 | 16.794
[FF02::C]:1900 | 50 | | | | 0.0004 | 33.78% | 0.0400 | 16.794
* | 50 | | | | 0.0004 | 100.00% | 0.0400 | 16.794
testphp.vulnweb.com | 23 | | | | 0.0002 | 15.54% | 0.0200 | 7.505
/guestbook.php | 3 | | | | 0.0000 | 13.04% | 0.0100 | 106.222
/cart.php | 3 | | | | 0.0000 | 13.04% | 0.0100 | 58.868
/userinfo.php | 2 | | | | 0.0000 | 8.70% | 0.0100 | 15.581
/index.php | 2 | | | | 0.0000 | 8.70% | 0.0100 | 34.973
/disclaimer.php | 2 | | | | 0.0000 | 8.70% | 0.0100 | 109.202
/artists.php | 2 | | | | 0.0000 | 8.70% | 0.0100 | 44.345
/style.css | 1 | | | | 0.0000 | 4.35% | 0.0100 | 7.505
/login.php | 1 | | | | 0.0000 | 4.35% | 0.0100 | 7.204
/images/remark.gif | 1 | | | | 0.0000 | 4.35% | 0.0100 | 106.500
/images/logo.gif | 1 | | | | 0.0000 | 4.35% | 0.0100 | 7.506
/favicon.ico | 1 | | | | 0.0000 | 4.35% | 0.0100 | 7.845
/comment.php?aid=2 | 1 | | | | 0.0000 | 4.35% | 0.0100 | 48.968
/categories.php | 1 | | | | 0.0000 | 4.35% | 0.0100 | 116.495
/AJAX/styles.css | 1 | | | | 0.0000 | 4.35% | 0.0100 | 134.094
/AJAX/index.php | 1 | | | | 0.0000 | 4.35% | 0.0100 | 133.805
ctldl.windowsupdate.com | 1 | | | | 0.0000 | 0.68% | 0.0100 | 96.371
/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c6fdef8c6401847a | 1 | | | | 0.0000 | 100.00% | 0.0100 | 96.371
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

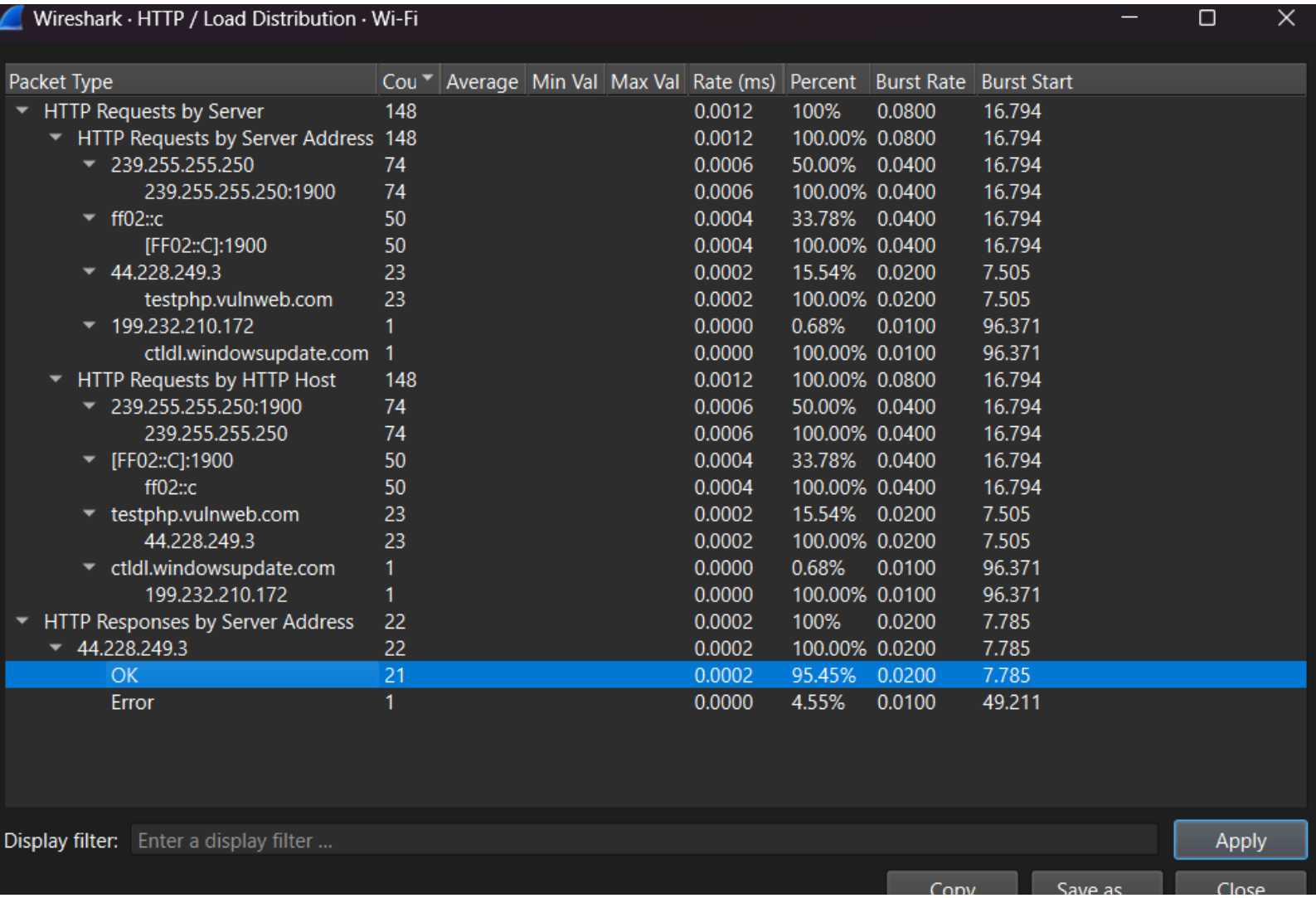

Wireshark · HTTP / Packet Counter · Wi-Fi
Packet Type
Cou
Average
Min Val
Max Val
Rate (ms)
Percent
Burst Rate
Burst Start
Total HTTP Packets 170 0.0013 100% 0.0800 16.794
HTTP Request Packets 148 0.0012 87.06% 0.0800 16.794
NOTIFY 100 0.0008 67.57% 0.0800 16.794
SEARCH 24 0.0002 16.22% 0.0200 24.373
GET 23 0.0002 15.54% 0.0200 7.505
POST 1 0.0000 0.68% 0.0100 15.581
HTTP Response Packets 22 0.0002 12.94% 0.0200 7.785
2xx: Success 21 0.0002 95.45% 0.0200 7.785
200 OK 21 0.0002 100.00% 0.0200 7.785
4xx: Client Error 1 0.0000 4.55% 0.0100 49.211
404 Not Found 1 0.0000 100.00% 0.0100 49.211
???: broken 0 0.0000 0.00% - -
5xx: Server Error 0 0.0000 0.00% - -
3xx: Redirection 0 0.0000 0.00% - -
1xx: Informational 0 0.0000 0.00% - -
Other HTTP Packets 0 0.0000 0.00% - -
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

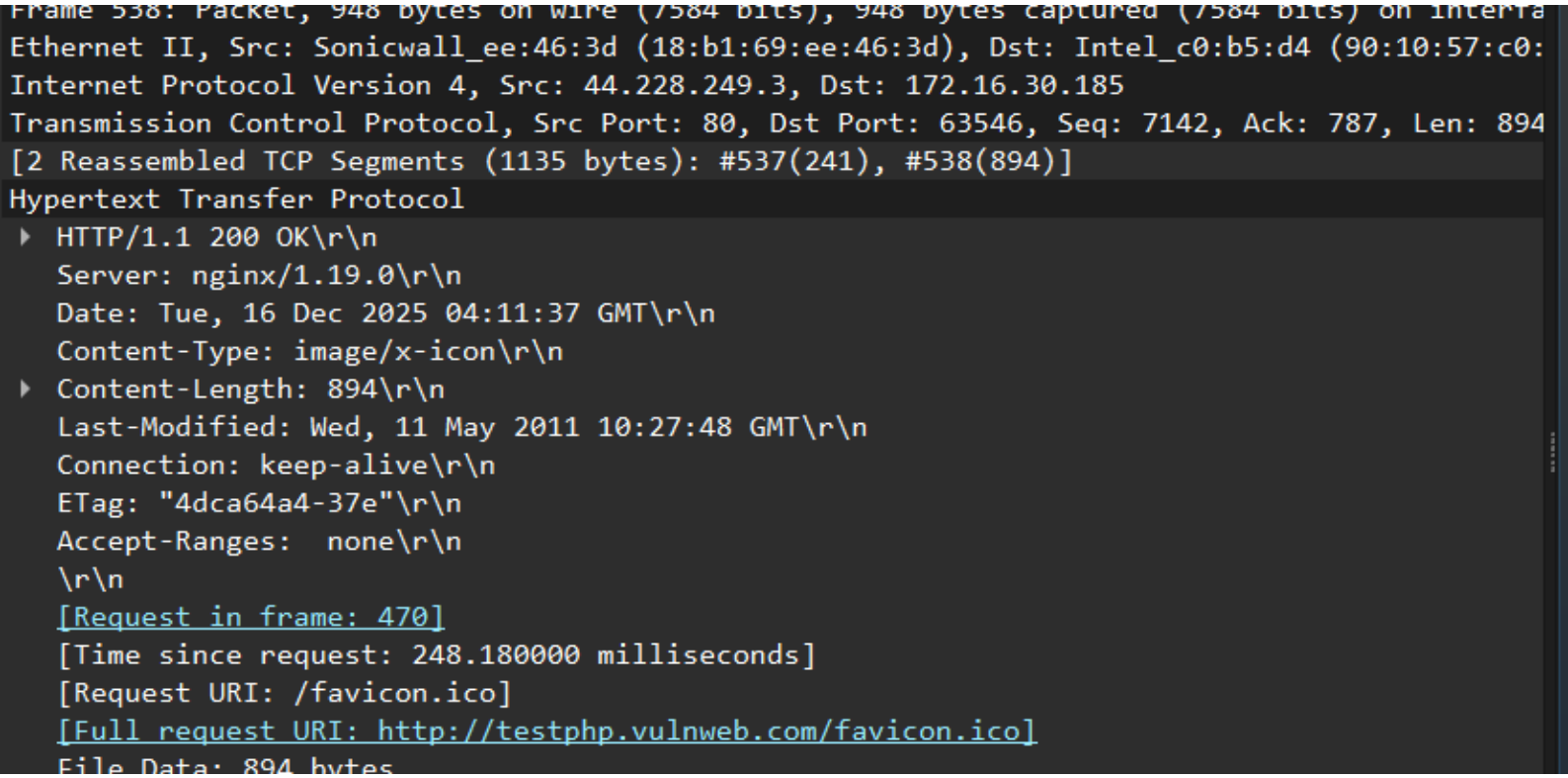
Ethernet · 1 | IPv4 · 57 | IPv6 | TCP · 81 | UDP

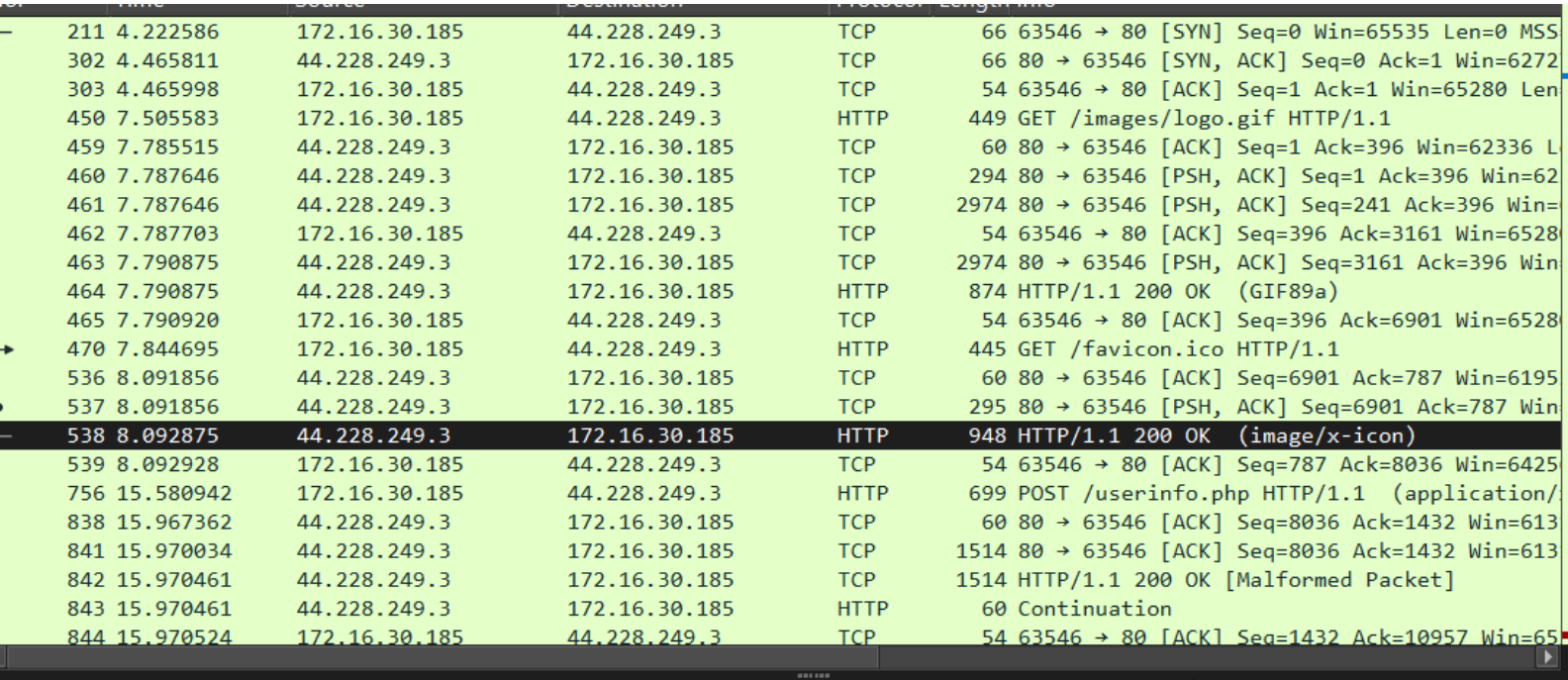
Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	
63298	3.111.241.224	443	77	38 kB	25	77	100.00%	36	23 kB	41	15 kB	15.945281	117.
55851	3.233.9.176	443	26	11 kB	52	26	100.00%	11	3 kB	15	8 kB	67.685468	46.2
49435	4.213.25.241	443	2	121 bytes	79	2	100.00%	1	55 bytes	1	66 bytes	130.043894	0.0
50268	8.8.8.8	443	6	363 bytes	40	6	100.00%	3	165 bytes	3	198 bytes	42.316459	90.1
58154	8.8.8.8	443	8	484 bytes	3	8	100.00%	4	220 bytes	4	264 bytes	2.631415	135.
59328	8.8.8.8	443	26	3 kB	11	26	100.00%	11	1 kB	15	2 kB	4.554607	90.
61102	8.8.8.8	443	6	363 bytes	41	6	100.00%	3	165 bytes	3	198 bytes	42.412784	90.0
63480	8.8.8.8	443	8	484 bytes	2	8	100.00%	4	220 bytes	4	264 bytes	1.693130	135.
58635	18.245.218.109	443	285	319 kB	46	285	100.00%	137	10 kB	148	309 kB	66.801287	34.2
65198	23.11.215.91	443	31	7 kB	33	31	100.00%	14	4 kB	17	3 kB	31.183025	90.3
63685	23.57.38.206	443	24	16 kB	58	24	100.00%	11	4 kB	13	12 kB	68.041963	45.4
61119	23.62.12.33	443	44	29 kB	56	44	100.00%	21	3 kB	23	25 kB	68.028496	45.4
53070	23.62.13.11	443	39	18 kB	32	39	100.00%	16	6 kB	23	12 kB	30.873833	90.5
54872	34.107.218.251	443	36	12 kB	51	36	100.00%	16	4 kB	20	8 kB	67.614567	46.2
52451	34.199.234.25	443	57	36 kB	67	57	100.00%	23	29 kB	34	7 kB	68.599666	32.1
56801	40.99.33.242	443	6	363 bytes	14	6	100.00%	3	165 bytes	3	198 bytes	6.161797	90.1
65200	40.104.134.82	443	51	14 kB	35	51	100.00%	25	4 kB	26	10 kB	33.444349	62.7
54350	40.119.249.228	443	22	7 kB	49	22	100.00%	12	2 kB	10	5 kB	67.556246	0.4
58636	40.119.249.228	443	22	7 kB	47	22	100.00%	12	2 kB	10	5 kB	66.932020	0.4
51948	43.205.77.2	443	33	9 kB	74	33	100.00%	13	3 kB	20	6 kB	89.898347	10.7
54274	43.205.77.2	443	43	10 kB	60	43	100.00%	18	4 kB	25	7 kB	68.049857	19.1
56882	43.205.77.2	443	21	7 kB	75	21	100.00%	7	2 kB	14	5 kB	90.158350	10.4
52126	44.228.249.3	443	6	390 bytes	10	6	100.00%	5	330 bytes	1	60 bytes	4.481866	45.2
52856	44.228.249.3	80	20	10 kB	8	20	100.00%	9	1 kB	11	9 kB	4.222724	71.4
53294	44.228.249.3	443	6	390 bytes	9	6	100.00%	5	330 bytes	1	60 bytes	4.227529	45.2
63275	44.228.249.3	80	3	186 bytes	78	3	100.00%	2	120 bytes	1	66 bytes	101.126786	0.2
63546	44.228.249.3	80	98	66 kB	7	98	100.00%	47	13 kB	51	53 kB	4.222586	130.
65199	51.132.193.104	443	30	12 kB	34	30	100.00%	18	5 kB	12	8 kB	32.674941	63.5
58992	52.84.205.36	443	37	18 kB	61	37	100.00%	18	3 kB	19	15 kB	68.050382	45.4
54315	52.98.123.178	443	6	363 bytes	29	6	100.00%	3	165 bytes	3	198 bytes	27.575117	90.1
60057	52.98.123.178	443	6	363 bytes	28	6	100.00%	3	165 bytes	3	198 bytes	26.814484	90.1
61128	52.98.123.178	443	6	363 bytes	30	6	100.00%	3	165 bytes	3	198 bytes	27.779296	90.1
49169	52.123.129.14	443	57	57 kB	43	57	100.00%	24	3 kB	33	54 kB	61.866320	0.2
63670	57.144.211.32	443	52	6 kB	1	52	100.00%	25	3 kB	27	3 kB	0.953510	136.
49677	99.83.231.3	443	34	11 kB	70	34	100.00%	14	3 kB	20	8 kB	68.723198	60.9
62690	99.83.231.3	443	47	15 kB	72	47	100.00%	20	4 kB	27	11 kB	69.226561	67.2
54538	99.86.182.42	443	69	70 kB	66	69	100.00%	32	4 kB	37	66 kB	68.488392	45.1
51880	99.86.182.101	443	67	57 kB	59	67	100.00%	32	4 kB	35	52 kB	68.046754	45.4
56909	103.43.91.17	443	26	7 kB	68	26	100.00%	13	3 kB	13	4 kB	68.610670	10.1
54349	104.16.80.73	443	27	15 kB	48	27	100.00%	11	3 kB	16	12 kB	67.410256	45.1
60608	104.16.80.73	443	14	7 kB	73	14	100.00%	7	2 kB	7	4 kB	88.439993	45.3
56096	104.18.10.224	443	15	5 kB	45	15	100.00%	8	2 kB	7	2 kB	66.359549	64.3
62169	104.18.10.224	443	797	872 kB	44	797	100.00%	319	49 kB	478	823 kB	66.169560	35.1
56499	106.51.42.26	443	55	13 kB	69	55	100.00%	23	5 kB	32	8 kB	68.612979	31.9
61650	106.51.42.26	443	285	92 kB	62	285	100.00%	115	47 kB	170	46 kB	68.053538	32.7
62646	106.51.45.67	443	22	9 kB	63	22	100.00%	10	3 kB	12	6 kB	68.139953	45.3
53724	106.51.45.80	443	35	35 kB	53	35	100.00%	15	3 kB	20	31 kB	67.953402	45.1


tcp
Source Destination Protocol Length Info
172.16.30.185 142.251.223.14 TCP 66 49674 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS
142.251.223.14 172.16.30.185 TCP 66 443 → 49674 [SYN, ACK] Seq=0 Ack=1 Win=6553
172.16.30.185 142.251.223.14 TCP 54 49674 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len
172.16.30.185 142.251.223.14 TLSv1.3 1847 Client Hello (SNI=clients4.google.com)
142.251.223.14 172.16.30.185 TCP 60 443 → 49674 [ACK] Seq=1 Ack=1413 Win=262144
142.251.223.14 172.16.30.185 TCP 60 443 → 49674 [ACK] Seq=1 Ack=1794 Win=262144
142.251.223.14 172.16.30.185 TLSv1.3 5702 Server Hello, Change Cipher Spec
172.16.30.185 142.251.223.14 TCP 54 49674 → 443 [ACK] Seq=1794 Ack=5649 Win=652
142.251.223.14 172.16.30.185 TLSv1.3 1005 Application Data
172.16.30.185 142.251.223.14 TLSv1.3 128 Change Cipher Spec, Application Data
172.16.30.185 142.251.223.14 TLSv1.3 146 Application Data
172.16.30.185 142.251.223.14 TLSv1.3 450 Application Data
172.16.30.185 142.251.223.14 TLSv1.3 4512 Application Data
142.251.223.14 172.16.30.185 TLSv1.3 1022 Application Data, Application Data
142.251.223.14 172.16.30.185 TLSv1.3 85 Application Data
172.16.30.185 142.251.223.14 TCP 54 49674 → 443 [ACK] Seq=6814 Ack=7599 Win=652
172.16.30.185 142.251.223.14 TLSv1.3 85 Application Data
142.251.223.14 172.16.30.185 TCP 60 443 → 49674 [ACK] Seq=7599 Ack=3768 Win=262
142.251.223.14 172.16.30.185 TCP 60 443 → 49674 [ACK] Seq=7599 Ack=6592 Win=262
142.251.223.14 172.16.30.185 TCP 60 443 → 49674 [ACK] Seq=7599 Ack=6814 Win=262
142.251.223.14 172.16.30.185 TCP 60 443 → 49674 [ACK] Seq=7599 Ack=6845 Win=262
142.251.223.14 172.16.30.185 TLSv1.3 549 Application Data
000. .... = Reserved: Not set
...0 .... = Accurate ECN: Not set
.... 0... .... = Congestion Window Reduced: Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····A····]
Window: 1024
[Calculated window size: 262144]
[Window size scaling factor: 256]
Checksum: 0x1427 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 56.561000 milliseconds]
[Time since previous frame in this TCP stream: 457.000 microseconds]
[SEQ/ACK analysis]
[Client Contiguous Streams: 1]
[Server Contiguous Streams: 1]
0000 90 10 57 c0 b5 d4
0010 00 28 7d 12 00 00
0020 1e b9 01 bb c2 0a
0030 04 00 14 27 00 00


Wireshark · HTTP / Load Distribution · Wi-Fi
Packet Type Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
HTTP Requests by Server 148 0.0012 100% 0.0800 16.794
HTTP Requests by Server Address 148 0.0012 100.00% 0.0800 16.794
239.255.255.250 74 0.0006 50.00% 0.0400 16.794
239.255.255.250:1900 74 0.0006 100.00% 0.0400 16.794
ff02::c 50 0.0004 33.78% 0.0400 16.794
[FF02::C]:1900 50 0.0004 100.00% 0.0400 16.794
44.228.249.3 23 0.0002 15.54% 0.0200 7.505
testphp.vulnweb.com 23 0.0002 100.00% 0.0200 7.505
199.232.210.172 1 0.0000 0.68% 0.0100 96.371
ctldl.windowsupdate.com 1 0.0000 100.00% 0.0100 96.371
HTTP Requests by HTTP Host 148 0.0012 100.00% 0.0800 16.794
239.255.255.250:1900 74 0.0006 50.00% 0.0400 16.794
239.255.255.250 74 0.0006 100.00% 0.0400 16.794
[FF02::C]:1900 50 0.0004 33.78% 0.0400 16.794
ff02::c 50 0.0004 100.00% 0.0400 16.794
testphp.vulnweb.com 23 0.0002 15.54% 0.0200 7.505
44.228.249.3 23 0.0002 100.00% 0.0200 7.505
ctldl.windowsupdate.com 1 0.0000 0.68% 0.0100 96.371
199.232.210.172 1 0.0000 100.00% 0.0100 96.371
HTTP Responses by Server Address 22 0.0002 100% 0.0200 7.785
44.228.249.3 22 0.0002 100.00% 0.0200 7.785
OK 21 0.0002 95.45% 0.0200 7.785
Error 1 0.0000 4.55% 0.0100 49.211
Display filter: Enter a display filter ...
Apply


Wireshark · HTTP / Load Distribution · Wi-Fi
Packet Type Cou Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start
HTTP Requests by Server 148 0.0012 100% 0.0800 16.794
HTTP Requests by Server Address 148 0.0012 100.00% 0.0800 16.794
239.255.255.250 74 0.0006 50.00% 0.0400 16.794
239.255.255.250:1900 74 0.0006 100.00% 0.0400 16.794
ff02::c 50 0.0004 33.78% 0.0400 16.794
[FF02::C]:1900 50 0.0004 100.00% 0.0400 16.794
44.228.249.3 23 0.0002 15.54% 0.0200 7.505
testphp.vulnweb.com 23 0.0002 100.00% 0.0200 7.505
199.232.210.172 1 0.0000 0.68% 0.0100 96.371
ctldl.windowsupdate.com 1 0.0000 100.00% 0.0100 96.371
HTTP Requests by HTTP Host 148 0.0012 100.00% 0.0800 16.794
239.255.255.250:1900 74 0.0006 50.00% 0.0400 16.794
239.255.255.250 74 0.0006 100.00% 0.0400 16.794
[FF02::C]:1900 50 0.0004 33.78% 0.0400 16.794
ff02::c 50 0.0004 100.00% 0.0400 16.794
testphp.vulnweb.com 23 0.0002 15.54% 0.0200 7.505
44.228.249.3 23 0.0002 100.00% 0.0200 7.505
ctldl.windowsupdate.com 1 0.0000 0.68% 0.0100 96.371
199.232.210.172 1 0.0000 100.00% 0.0100 96.371
HTTP Responses by Server Address 22 0.0002 100% 0.0200 7.785
44.228.249.3 22 0.0002 100.00% 0.0200 7.785
OK 21 0.0002 95.45% 0.0200 7.785
Error 1 0.0000 4.55% 0.0100 49.211
Display filter: Enter a display filter ...
Apply
Copy
Save as
Close

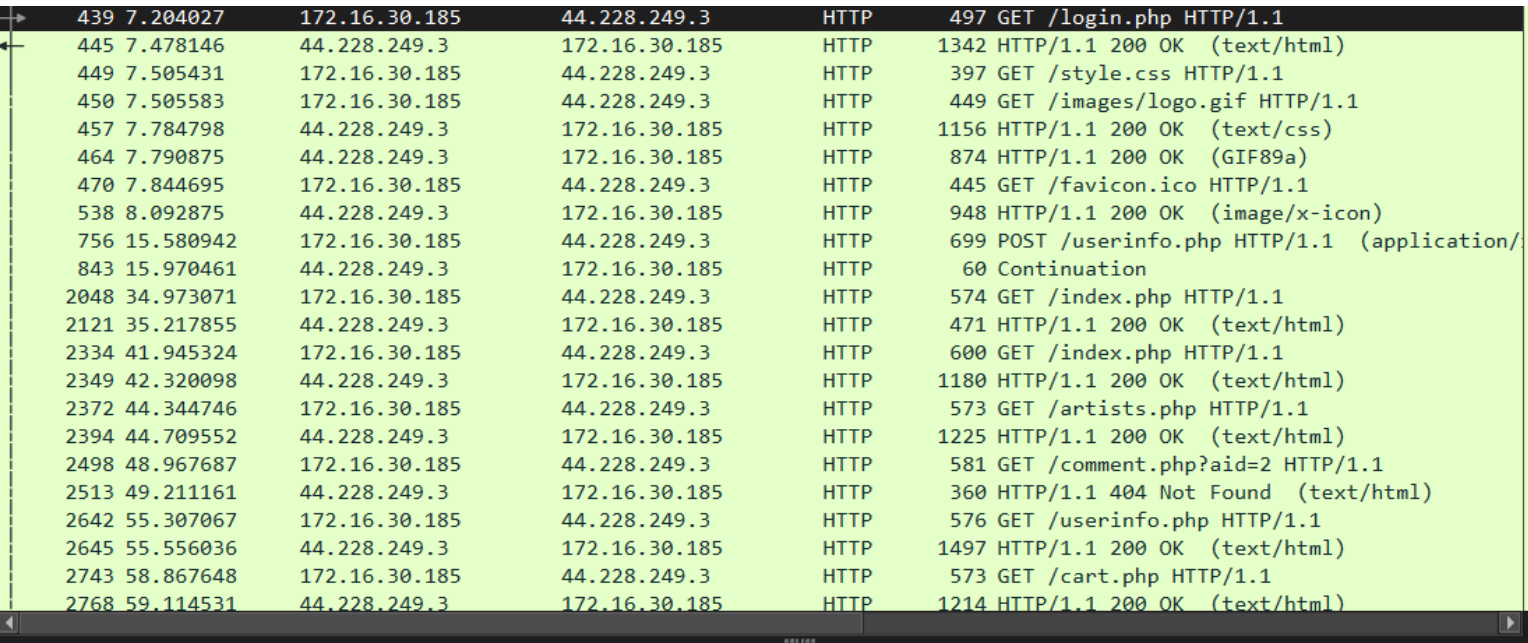

Frame 538: Packet, 948 bytes on wire (7584 bits), 948 bytes captured (7584 bits) on interfa
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: Intel_c0:b5:d4 (90:10:57:c0:
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.30.185
Transmission Control Protocol, Src Port: 80, Dst Port: 63546, Seq: 7142, Ack: 787, Len: 894
[2 Reassembled TCP Segments (1135 bytes): #537(241), #538(894)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Server: nginx/1.19.0\r\n
Date: Tue, 16 Dec 2025 04:11:37 GMT\r\n
Content-Type: image/x-icon\r\n
Content-Length: 894\r\n
Last-Modified: Wed, 11 May 2011 10:27:48 GMT\r\n
Connection: keep-alive\r\n
ETag: "4dca64a4-37e"\r\n
Accept-Ranges: none\r\n
\r\n
[Request in frame: 470]
[Time since request: 248.180000 milliseconds]
[Request URI: /favicon.ico]
[Full request URI: http://testphp.vulnweb.com/favicon.ico]
File Data: 894 bytes



	211	4.222586	172.16.30.185	44.228.249.3	TCP	66 63546 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS
	302	4.465811	44.228.249.3	172.16.30.185	TCP	66 80 → 63546 [SYN, ACK] Seq=0 Ack=1 Win=6272
	303	4.465998	172.16.30.185	44.228.249.3	TCP	54 63546 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len
	450	7.505583	172.16.30.185	44.228.249.3	HTTP	449 GET /images/logo.gif HTTP/1.1
	459	7.785515	44.228.249.3	172.16.30.185	TCP	60 80 → 63546 [ACK] Seq=1 Ack=396 Win=62336 L
	460	7.787646	44.228.249.3	172.16.30.185	TCP	294 80 → 63546 [PSH, ACK] Seq=1 Ack=396 Win=62
	461	7.787646	44.228.249.3	172.16.30.185	TCP	2974 80 → 63546 [PSH, ACK] Seq=241 Ack=396 Win=
	462	7.787703	172.16.30.185	44.228.249.3	TCP	54 63546 → 80 [ACK] Seq=396 Ack=3161 Win=6528
	463	7.790875	44.228.249.3	172.16.30.185	TCP	2974 80 → 63546 [PSH, ACK] Seq=3161 Ack=396 Win
	464	7.790875	44.228.249.3	172.16.30.185	HTTP	874 HTTP/1.1 200 OK (GIF89a)
	465	7.790920	172.16.30.185	44.228.249.3	TCP	54 63546 → 80 [ACK] Seq=396 Ack=6901 Win=6528
→	470	7.844695	172.16.30.185	44.228.249.3	HTTP	445 GET /favicon.ico HTTP/1.1
	536	8.091856	44.228.249.3	172.16.30.185	TCP	60 80 → 63546 [ACK] Seq=6901 Ack=787 Win=6195
	537	8.091856	44.228.249.3	172.16.30.185	TCP	295 80 → 63546 [PSH, ACK] Seq=6901 Ack=787 Win
	538	8.092875	44.228.249.3	172.16.30.185	HTTP	948 HTTP/1.1 200 OK (image/x-icon)
	539	8.092928	172.16.30.185	44.228.249.3	TCP	54 63546 → 80 [ACK] Seq=787 Ack=8036 Win=6425
	756	15.580942	172.16.30.185	44.228.249.3	HTTP	699 POST /userinfo.php HTTP/1.1 (application/
	838	15.967362	44.228.249.3	172.16.30.185	TCP	60 80 → 63546 [ACK] Seq=8036 Ack=1432 Win=613
	841	15.970034	44.228.249.3	172.16.30.185	TCP	1514 80 → 63546 [ACK] Seq=8036 Ack=1432 Win=613
	842	15.970461	44.228.249.3	172.16.30.185	TCP	1514 HTTP/1.1 200 OK [Malformed Packet]
	843	15.970461	44.228.249.3	172.16.30.185	HTTP	60 Continuation
	844	15.970524	172.16.30.185	44.228.249.3	TCP	54 63546 → 80 [ACK] Seq=1432 Ack=10957 Win=65

```
    .... ...1 .... = Acknowledgment: Set
    .... .... 1... = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·······AP···]
  Window: 484
  [Calculated window size: 61952]
  [Window size scaling factor: 128]
  Checksum: 0x74ce [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
▾ [Timestamps]
    [Time since first frame in this TCP stream: 3.870289000 seconds]
    [Time since previous frame in this TCP stream: 1.019000 milliseconds]
▸ [SEQ/ACK analysis]
  [Client Contiguous Streams: 1]
  [Server Contiguous Streams: 1]
  TCP payload (894 bytes)
  TCP segment data (894 bytes)
▸ [2 Reassembled TCP Segments (1135 bytes): #537(241), #538(894)]
▸ Hypertext Transfer Protocol
```

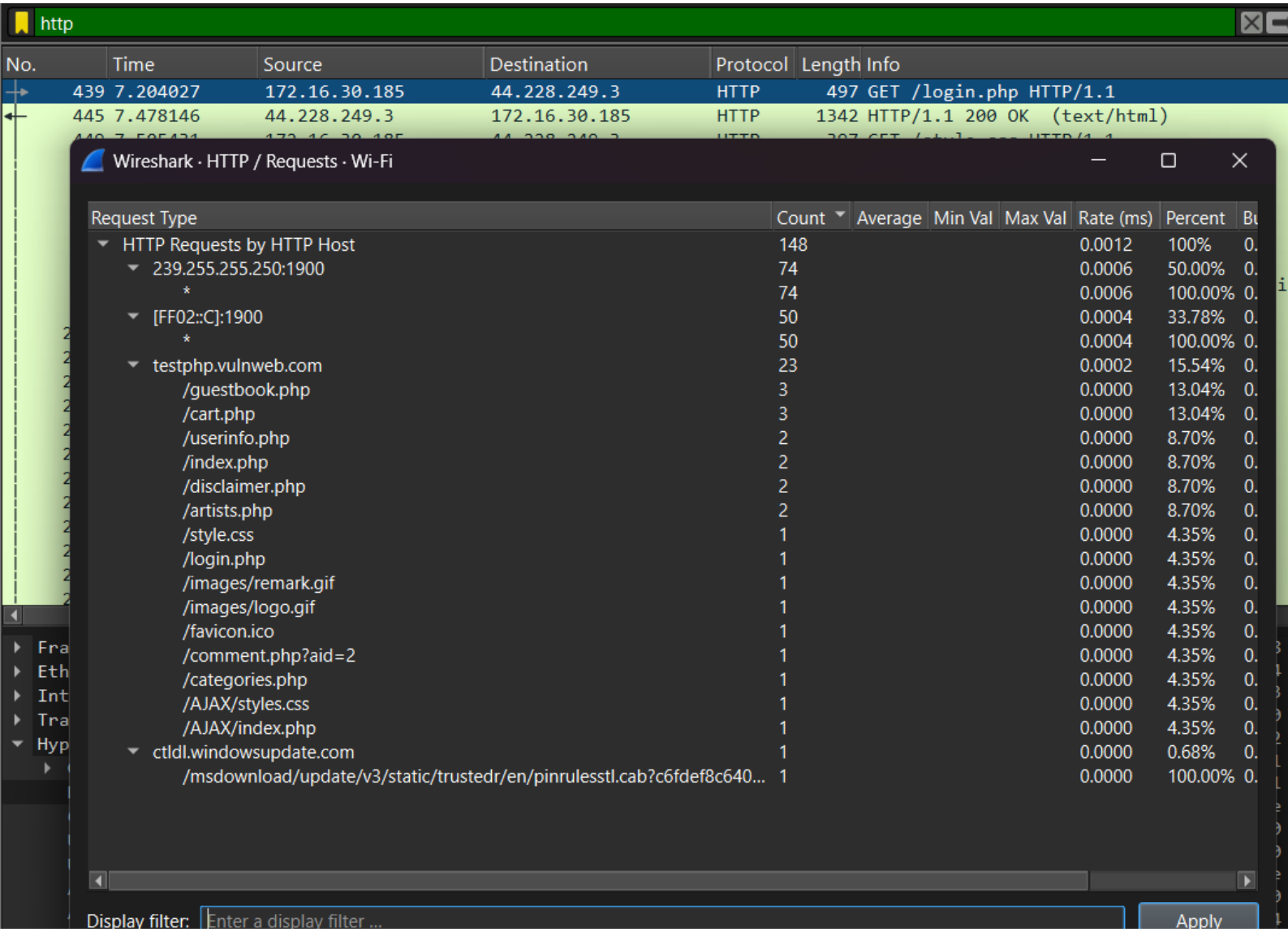
```
0000  90 10 57 c0 b5 d4 18
0010  03 a6 87 0a 40 00 33
0020  1e b9 00 50 f8 3a b5
0030  01 e4 74 ce 00 00 00
0040  01 00 18 00 68 03 00
0050  10 00 00 00 20 00 00
0060  00 00 00 00 48 00 00
0070  00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00
00a0  00 00 00 00 00 00 00
00b0  ff ff ff ff ff ff ff
00c0  ff ff ff ff ff ff ff
00d0  ff 00 00 00 00 00 00
00e0  ff ff ff ff ff ff ff
00f0  ff ff ff ff ff ff ff
0100  ff 00 00 00 00 00 00
0110  ff ff ff ff ff ff ff
0120  ff ff ff ff ff ff ff
0130  ff 00 00 00 00 00 00
0140  26 1b e3 dd db fb f3
0150  f4 fe e4 e3 fc 40 36
0160  fe 00 00 00 00 00 00
```

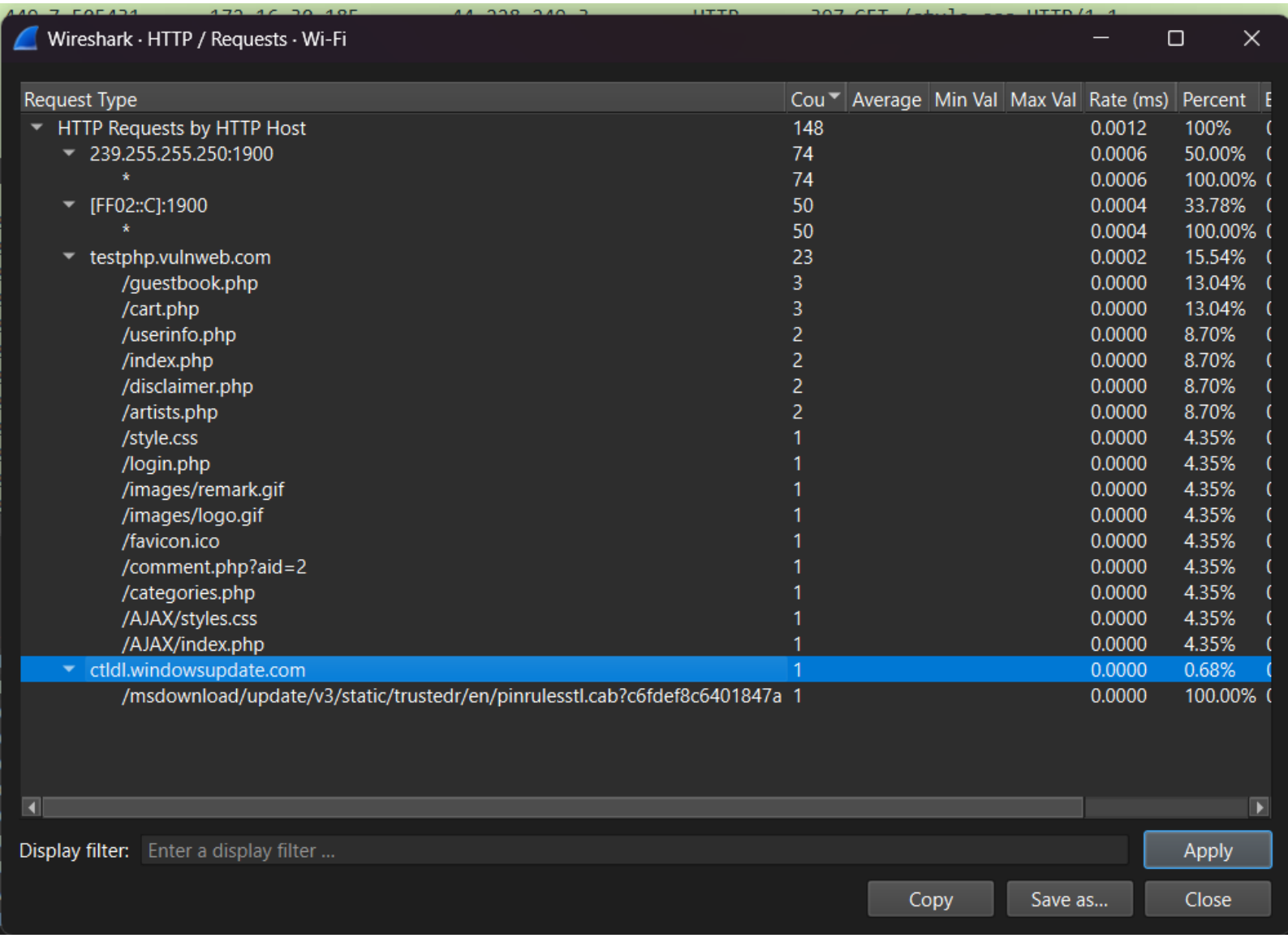


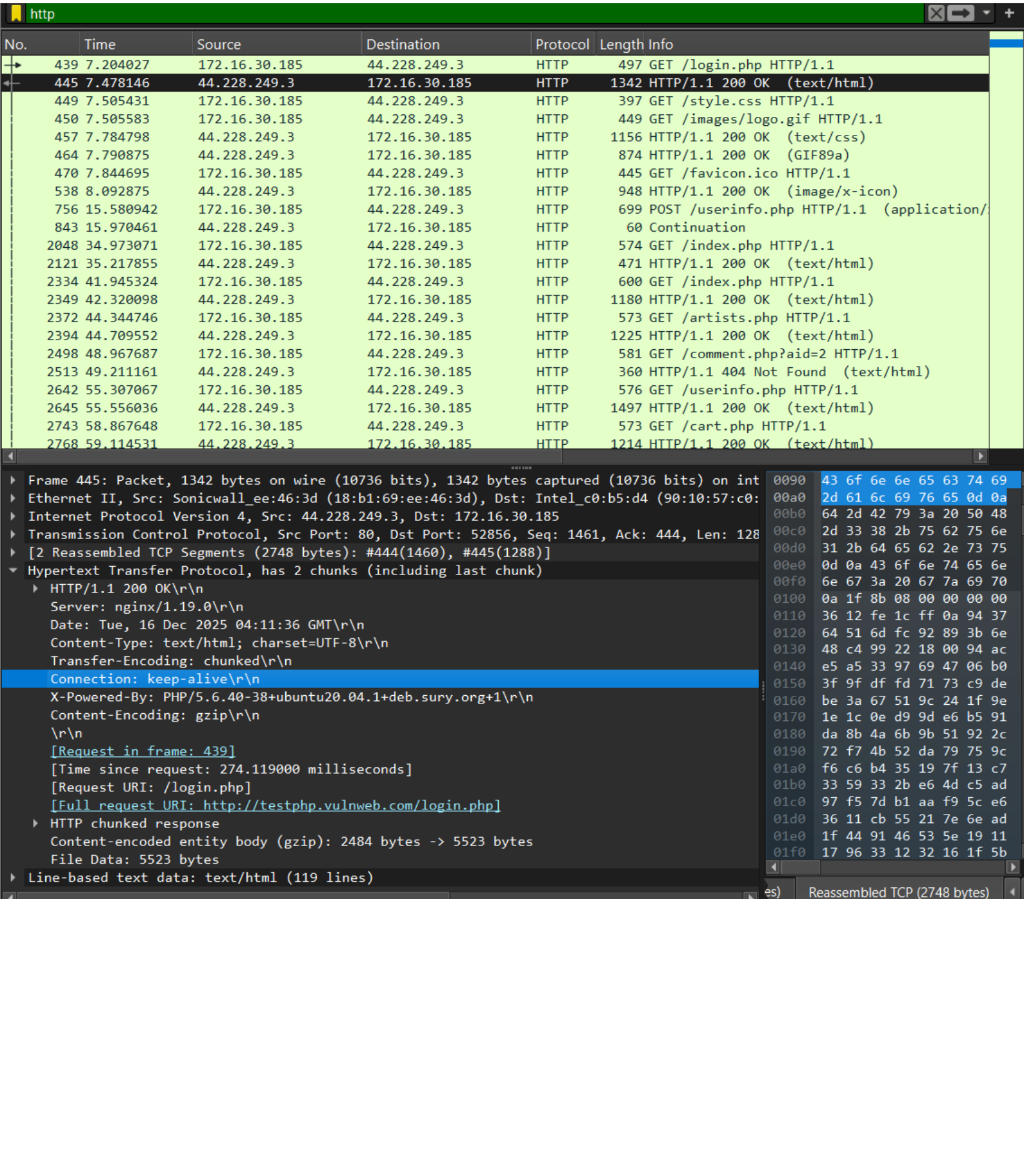
```
   439 7.204027     172.16.30.185     44.228.249.3      HTTP     497 GET /login.php HTTP/1.1
   445 7.478146     44.228.249.3      172.16.30.185     HTTP    1342 HTTP/1.1 200 OK  (text/html)
   449 7.505431     172.16.30.185     44.228.249.3      HTTP     397 GET /style.css HTTP/1.1
   450 7.505583     172.16.30.185     44.228.249.3      HTTP     449 GET /images/logo.gif HTTP/1.1
   457 7.784798     44.228.249.3      172.16.30.185     HTTP    1156 HTTP/1.1 200 OK  (text/css)
   464 7.790875     44.228.249.3      172.16.30.185     HTTP     874 HTTP/1.1 200 OK  (GIF89a)
   470 7.844695     172.16.30.185     44.228.249.3      HTTP     445 GET /favicon.ico HTTP/1.1
   538 8.092875     44.228.249.3      172.16.30.185     HTTP     948 HTTP/1.1 200 OK  (image/x-icon)
   756 15.580942    172.16.30.185     44.228.249.3      HTTP     699 POST /userinfo.php HTTP/1.1  (application/
   843 15.970461    44.228.249.3      172.16.30.185     HTTP      60 Continuation
  2048 34.973071    172.16.30.185     44.228.249.3      HTTP     574 GET /index.php HTTP/1.1
  2121 35.217855    44.228.249.3      172.16.30.185     HTTP     471 HTTP/1.1 200 OK  (text/html)
  2334 41.945324    172.16.30.185     44.228.249.3      HTTP     600 GET /index.php HTTP/1.1
  2349 42.320098    44.228.249.3      172.16.30.185     HTTP    1180 HTTP/1.1 200 OK  (text/html)
  2372 44.344746    172.16.30.185     44.228.249.3      HTTP     573 GET /artists.php HTTP/1.1
  2394 44.709552    44.228.249.3      172.16.30.185     HTTP    1225 HTTP/1.1 200 OK  (text/html)
  2498 48.967687    172.16.30.185     44.228.249.3      HTTP     581 GET /comment.php?aid=2 HTTP/1.1
  2513 49.211161    44.228.249.3      172.16.30.185     HTTP     360 HTTP/1.1 404 Not Found  (text/html)
  2642 55.307067    172.16.30.185     44.228.249.3      HTTP     576 GET /userinfo.php HTTP/1.1
  2645 55.556036    44.228.249.3      172.16.30.185     HTTP    1497 HTTP/1.1 200 OK  (text/html)
  2743 58.867648    172.16.30.185     44.228.249.3      HTTP     573 GET /cart.php HTTP/1.1
  2768 59.114531    44.228.249.3      172.16.30.185     HTTP    1214 HTTP/1.1 200 OK  (text/html)
```

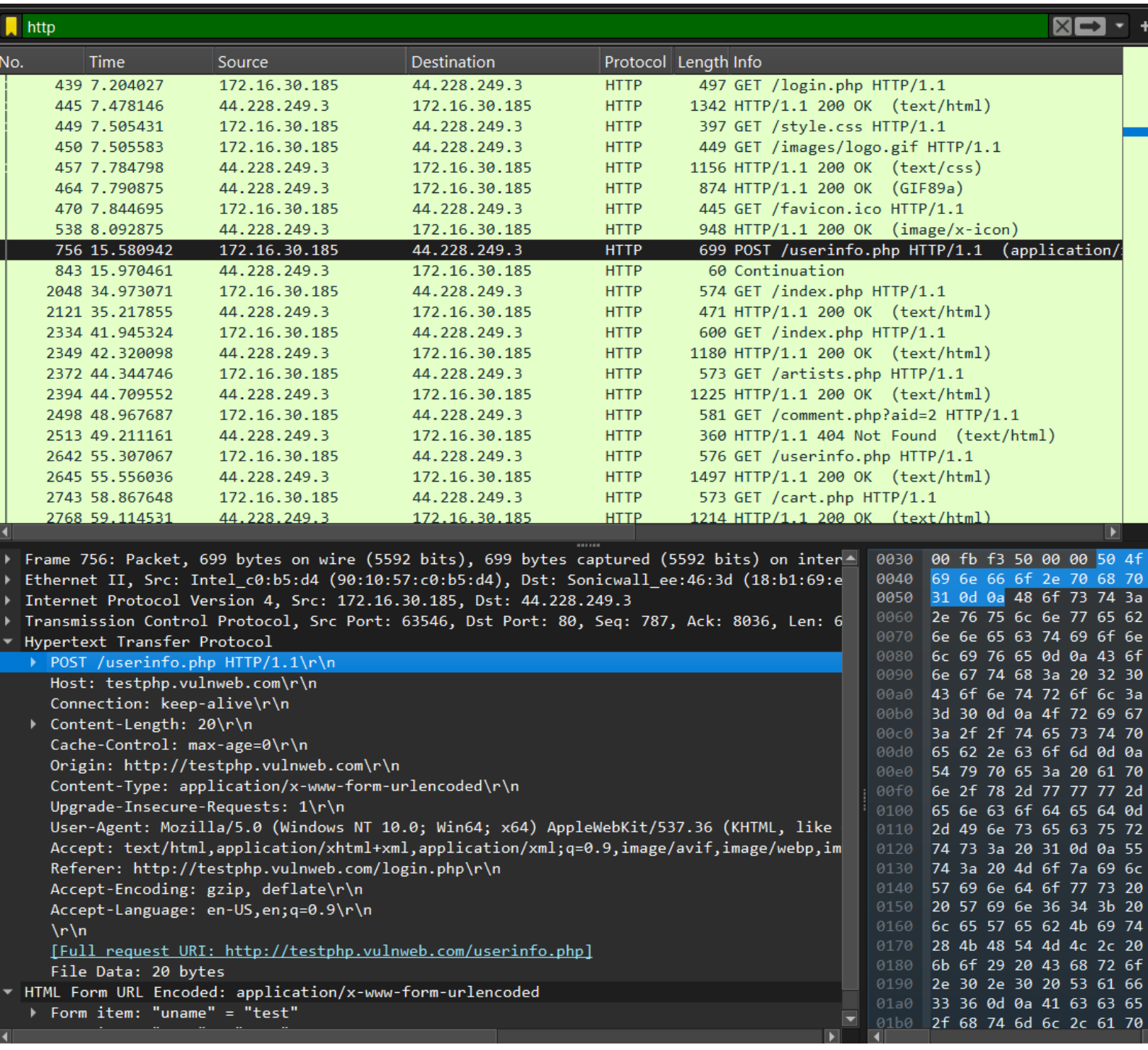
```
▸ Frame 439: Packet, 497 bytes on wire (3976 bits), 497 bytes captured (3976 bits) on interfa
▸ Ethernet II, Src: Intel_c0:b5:d4 (90:10:57:c0:b5:d4), Dst: Sonicwall_ee:46:3d (18:b1:69:ee:
▸ Internet Protocol Version 4, Src: 172.16.30.185, Dst: 44.228.249.3
▸ Transmission Control Protocol, Src Port: 52856, Dst Port: 80, Seq: 1, Ack: 1, Len: 443
▾ Hypertext Transfer Protocol
  ▸ GET /login.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    Connection: keep-alive\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
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Response in frame: 445]
    [Full request URI: http://testphp.vulnweb.com/login.php]
```

```
0040  2e 70 68 70 20 48 54 54
0050  6f 73 74 3a 20 74 65 73
0060  6e 77 65 62 2e 63 6f 6d
0070  74 69 6f 6e 3a 20 6b 65
0080  0d 0a 55 70 67 72 61 64
0090  72 65 2d 52 65 71 75 65
00a0  55 73 65 72 2d 41 67 65
00b0  6c 6c 61 2f 35 2e 30 20
00c0  20 4e 54 20 31 30 2e 30
00d0  20 78 36 34 29 20 41 70
00e0  74 2f 35 33 37 2e 33 36
00f0  20 6c 69 6b 65 20 47 65
0100  6f 6d 65 2f 31 34 33 2e
0110  66 61 72 69 2f 35 33 37
0120  65 70 74 3a 20 74 65 78
0130  70 70 6c 69 63 61 74 69
0140  2b 78 6d 6c 2c 61 70 70
0150  2f 78 6d 6c 3b 71 3d 30
0160  2f 61 76 69 66 2c 69 6d
0170  2c 69 6d 61 67 65 2f 61
0180  71 3d 30 2e 38 2c 61 70
0190  6e 2f 73 69 67 6e 65 64
01a0  65 3b 76 3d 62 33 3b 71
01b0  63 65 70 74 2d 45 6e 63
01c0  7a 69 70 2c 20 64 65 66
```


http
No. Time Source Destination Protocol Length Info
439 7.204027 172.16.30.185 44.228.249.3 HTTP 497 GET /login.php HTTP/1.1
445 7.478146 44.228.249.3 172.16.30.185 HTTP 1342 HTTP/1.1 200 OK (text/html)
Wireshark · HTTP / Requests · Wi-Fi
Request Type Count Average Min Val Max Val Rate (ms) Percent
HTTP Requests by HTTP Host 148 0.0012 100%
239.255.255.250:1900 74 0.0006 50.00%
* 74 0.0006 100.00%
[FF02::C]:1900 50 0.0004 33.78%
* 50 0.0004 100.00%
testphp.vulnweb.com 23 0.0002 15.54%
/guestbook.php 3 0.0000 13.04%
/cart.php 3 0.0000 13.04%
/userinfo.php 2 0.0000 8.70%
/index.php 2 0.0000 8.70%
/disclaimer.php 2 0.0000 8.70%
/artists.php 2 0.0000 8.70%
/style.css 1 0.0000 4.35%
/login.php 1 0.0000 4.35%
/images/remark.gif 1 0.0000 4.35%
/images/logo.gif 1 0.0000 4.35%
/favicon.ico 1 0.0000 4.35%
/comment.php?aid=2 1 0.0000 4.35%
/categories.php 1 0.0000 4.35%
/AJAX/styles.css 1 0.0000 4.35%
/AJAX/index.php 1 0.0000 4.35%
ctldl.windowsupdate.com 1 0.0000 0.68%
/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c6fdef8c640... 1 0.0000 100.00%
Display filter: Enter a display filter ...
Apply


Wireshark · HTTP / Requests · Wi-Fi
Request Type
Cou
Average
Min Val
Max Val
Rate (ms)
Percent
HTTP Requests by HTTP Host 148 0.0012 100%
239.255.255.250:1900 74 0.0006 50.00%
* 74 0.0006 100.00%
[FF02::C]:1900 50 0.0004 33.78%
* 50 0.0004 100.00%
testphp.vulnweb.com 23 0.0002 15.54%
/guestbook.php 3 0.0000 13.04%
/cart.php 3 0.0000 13.04%
/userinfo.php 2 0.0000 8.70%
/index.php 2 0.0000 8.70%
/disclaimer.php 2 0.0000 8.70%
/artists.php 2 0.0000 8.70%
/style.css 1 0.0000 4.35%
/login.php 1 0.0000 4.35%
/images/remark.gif 1 0.0000 4.35%
/images/logo.gif 1 0.0000 4.35%
/favicon.ico 1 0.0000 4.35%
/comment.php?aid=2 1 0.0000 4.35%
/categories.php 1 0.0000 4.35%
/AJAX/styles.css 1 0.0000 4.35%
/AJAX/index.php 1 0.0000 4.35%
ctldl.windowsupdate.com 1 0.0000 0.68%
/msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c6fdef8c6401847a 1 0.0000 100.00%
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close


http
No. Time Source Destination Protocol Length Info
439 7.204027 172.16.30.185 44.228.249.3 HTTP 497 GET /login.php HTTP/1.1
445 7.478146 44.228.249.3 172.16.30.185 HTTP 1342 HTTP/1.1 200 OK (text/html)
449 7.505431 172.16.30.185 44.228.249.3 HTTP 397 GET /style.css HTTP/1.1
450 7.505583 172.16.30.185 44.228.249.3 HTTP 449 GET /images/logo.gif HTTP/1.1
457 7.784798 44.228.249.3 172.16.30.185 HTTP 1156 HTTP/1.1 200 OK (text/css)
464 7.790875 44.228.249.3 172.16.30.185 HTTP 874 HTTP/1.1 200 OK (GIF89a)
470 7.844695 172.16.30.185 44.228.249.3 HTTP 445 GET /favicon.ico HTTP/1.1
538 8.092875 44.228.249.3 172.16.30.185 HTTP 948 HTTP/1.1 200 OK (image/x-icon)
756 15.580942 172.16.30.185 44.228.249.3 HTTP 699 POST /userinfo.php HTTP/1.1 (application/
843 15.970461 44.228.249.3 172.16.30.185 HTTP 60 Continuation
2048 34.973071 172.16.30.185 44.228.249.3 HTTP 574 GET /index.php HTTP/1.1
2121 35.217855 44.228.249.3 172.16.30.185 HTTP 471 HTTP/1.1 200 OK (text/html)
2334 41.945324 172.16.30.185 44.228.249.3 HTTP 600 GET /index.php HTTP/1.1
2349 42.320098 44.228.249.3 172.16.30.185 HTTP 1180 HTTP/1.1 200 OK (text/html)
2372 44.344746 172.16.30.185 44.228.249.3 HTTP 573 GET /artists.php HTTP/1.1
2394 44.709552 44.228.249.3 172.16.30.185 HTTP 1225 HTTP/1.1 200 OK (text/html)
2498 48.967687 172.16.30.185 44.228.249.3 HTTP 581 GET /comment.php?aid=2 HTTP/1.1
2513 49.211161 44.228.249.3 172.16.30.185 HTTP 360 HTTP/1.1 404 Not Found (text/html)
2642 55.307067 172.16.30.185 44.228.249.3 HTTP 576 GET /userinfo.php HTTP/1.1
2645 55.556036 44.228.249.3 172.16.30.185 HTTP 1497 HTTP/1.1 200 OK (text/html)
2743 58.867648 172.16.30.185 44.228.249.3 HTTP 573 GET /cart.php HTTP/1.1
2768 59.114531 44.228.249.3 172.16.30.185 HTTP 1214 HTTP/1.1 200 OK (text/html)
Frame 445: Packet, 1342 bytes on wire (10736 bits), 1342 bytes captured (10736 bits) on int
Ethernet II, Src: Sonicwall_ee:46:3d (18:b1:69:ee:46:3d), Dst: Intel_c0:b5:d4 (90:10:57:c0:
Internet Protocol Version 4, Src: 44.228.249.3, Dst: 172.16.30.185
Transmission Control Protocol, Src Port: 80, Dst Port: 52856, Seq: 1461, Ack: 444, Len: 128
[2 Reassembled TCP Segments (2748 bytes): #444(1460), #445(1288)]
Hypertext Transfer Protocol, has 2 chunks (including last chunk)
HTTP/1.1 200 OK\r\n
Server: nginx/1.19.0\r\n
Date: Tue, 16 Dec 2025 04:11:36 GMT\r\n
Content-Type: text/html; charset=UTF-8\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1\r\n
Content-Encoding: gzip\r\n
\r\n
[Request in frame: 439]
[Time since request: 274.119000 milliseconds]
[Request URI: /login.php]
[Full request URI: http://testphp.vulnweb.com/login.php]
HTTP chunked response
Content-encoded entity body (gzip): 2484 bytes -> 5523 bytes
File Data: 5523 bytes
Line-based text data: text/html (119 lines)
0090 43 6f 6e 6e 65 63 74 69
00a0 2d 61 6c 69 76 65 0d 0a
00b0 64 2d 42 79 3a 20 50 48
00c0 2d 33 38 2b 75 62 75 6e
00d0 31 2b 64 65 62 2e 73 75
00e0 0d 0a 43 6f 6e 74 65 6e
00f0 6e 67 3a 20 67 7a 69 70
0100 0a 1f 8b 08 00 00 00 00
0110 36 12 fe 1c ff 0a 94 37
0120 64 51 6d fc 92 89 3b 6e
0130 48 c4 99 22 18 00 94 ac
0140 e5 a5 33 97 69 47 06 b0
0150 3f 9f df fd 71 73 c9 de
0160 be 3a 67 51 9c 24 1f 9e
0170 1e 1c 0e d9 9d e6 b5 91
0180 da 8b 4a 6b 9b 51 92 2c
0190 72 f7 4b 52 da 79 75 9c
01a0 f6 c6 b4 35 19 7f 13 c7
01b0 33 59 33 2b e6 4d c5 ad
01c0 97 f5 7d b1 aa f9 5c e6
01d0 36 11 cb 55 21 7e 6e ad
01e0 1f 44 91 46 53 5e 19 11
01f0 17 96 33 12 32 16 1f 5b
es)
Reassembled TCP (2748 bytes)


http
No. Time Source Destination Protocol Length Info
439 7.204027 172.16.30.185 44.228.249.3 HTTP 497 GET /login.php HTTP/1.1
445 7.478146 44.228.249.3 172.16.30.185 HTTP 1342 HTTP/1.1 200 OK (text/html)
449 7.505431 172.16.30.185 44.228.249.3 HTTP 397 GET /style.css HTTP/1.1
450 7.505583 172.16.30.185 44.228.249.3 HTTP 449 GET /images/logo.gif HTTP/1.1
457 7.784798 44.228.249.3 172.16.30.185 HTTP 1156 HTTP/1.1 200 OK (text/css)
464 7.790875 44.228.249.3 172.16.30.185 HTTP 874 HTTP/1.1 200 OK (GIF89a)
470 7.844695 172.16.30.185 44.228.249.3 HTTP 445 GET /favicon.ico HTTP/1.1
538 8.092875 44.228.249.3 172.16.30.185 HTTP 948 HTTP/1.1 200 OK (image/x-icon)
756 15.580942 172.16.30.185 44.228.249.3 HTTP 699 POST /userinfo.php HTTP/1.1 (application/
843 15.970461 44.228.249.3 172.16.30.185 HTTP 60 Continuation
2048 34.973071 172.16.30.185 44.228.249.3 HTTP 574 GET /index.php HTTP/1.1
2121 35.217855 44.228.249.3 172.16.30.185 HTTP 471 HTTP/1.1 200 OK (text/html)
2334 41.945324 172.16.30.185 44.228.249.3 HTTP 600 GET /index.php HTTP/1.1
2349 42.320098 44.228.249.3 172.16.30.185 HTTP 1180 HTTP/1.1 200 OK (text/html)
2372 44.344746 172.16.30.185 44.228.249.3 HTTP 573 GET /artists.php HTTP/1.1
2394 44.709552 44.228.249.3 172.16.30.185 HTTP 1225 HTTP/1.1 200 OK (text/html)
2498 48.967687 172.16.30.185 44.228.249.3 HTTP 581 GET /comment.php?aid=2 HTTP/1.1
2513 49.211161 44.228.249.3 172.16.30.185 HTTP 360 HTTP/1.1 404 Not Found (text/html)
2642 55.307067 172.16.30.185 44.228.249.3 HTTP 576 GET /userinfo.php HTTP/1.1
2645 55.556036 44.228.249.3 172.16.30.185 HTTP 1497 HTTP/1.1 200 OK (text/html)
2743 58.867648 172.16.30.185 44.228.249.3 HTTP 573 GET /cart.php HTTP/1.1
2768 59.114531 44.228.249.3 172.16.30.185 HTTP 1214 HTTP/1.1 200 OK (text/html)
Frame 756: Packet, 699 bytes on wire (5592 bits), 699 bytes captured (5592 bits) on inter
Ethernet II, Src: Intel_c0:b5:d4 (90:10:57:c0:b5:d4), Dst: Sonicwall_ee:46:3d (18:b1:69:e
Internet Protocol Version 4, Src: 172.16.30.185, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 63546, Dst Port: 80, Seq: 787, Ack: 8036, Len: 6
Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Content-Length: 20\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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
File Data: 20 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test"
0030 00 fb f3 50 00 00 50 4f
0040 69 6e 66 6f 2e 70 68 70
0050 31 0d 0a 48 6f 73 74 3a
0060 2e 76 75 6c 6e 77 65 62
0070 6e 6e 65 63 74 69 6f 6e
0080 6c 69 76 65 0d 0a 43 6f
0090 6e 67 74 68 3a 20 32 30
00a0 43 6f 6e 74 72 6f 6c 3a
00b0 3d 30 0d 0a 4f 72 69 67
00c0 3a 2f 2f 74 65 73 74 70
00d0 65 62 2e 63 6f 6d 0d 0a
00e0 54 79 70 65 3a 20 61 70
00f0 6e 2f 78 2d 77 77 77 2d
0100 65 6e 63 6f 64 65 64 0d
0110 2d 49 6e 73 65 63 75 72
0120 74 73 3a 20 31 0d 0a 55
0130 74 3a 20 4d 6f 7a 69 6c
0140 57 69 6e 64 6f 77 73 20
0150 20 57 69 6e 36 34 3b 20
0160 6c 65 57 65 62 4b 69 74
0170 28 4b 48 54 4d 4c 2c 20
0180 6b 6f 29 20 43 68 72 6f
0190 2e 30 2e 30 20 53 61 66
01a0 33 36 0d 0a 41 63 63 65
01b0 2f 68 74 6d 6c 2c 61 70