AIM: Analyze the packets provided in lab and solve the questions using Wireshark :

- What web server software is used by www.snopes.com?

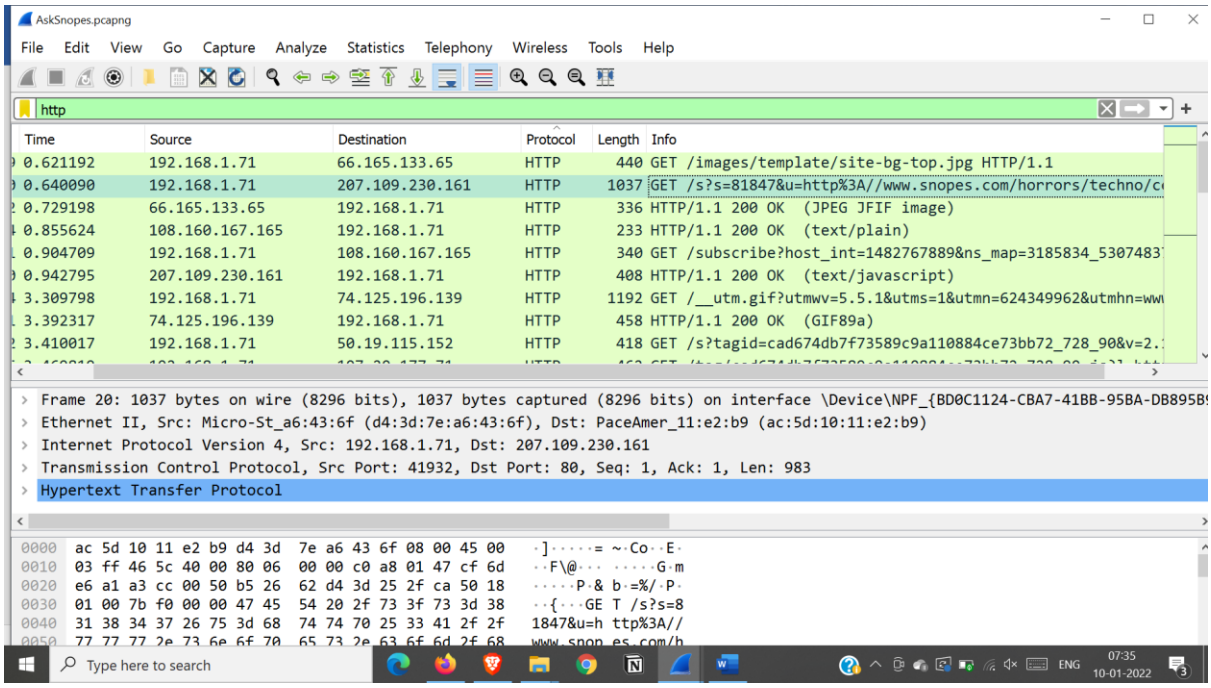
- About what cell phone problem is the client concerned?

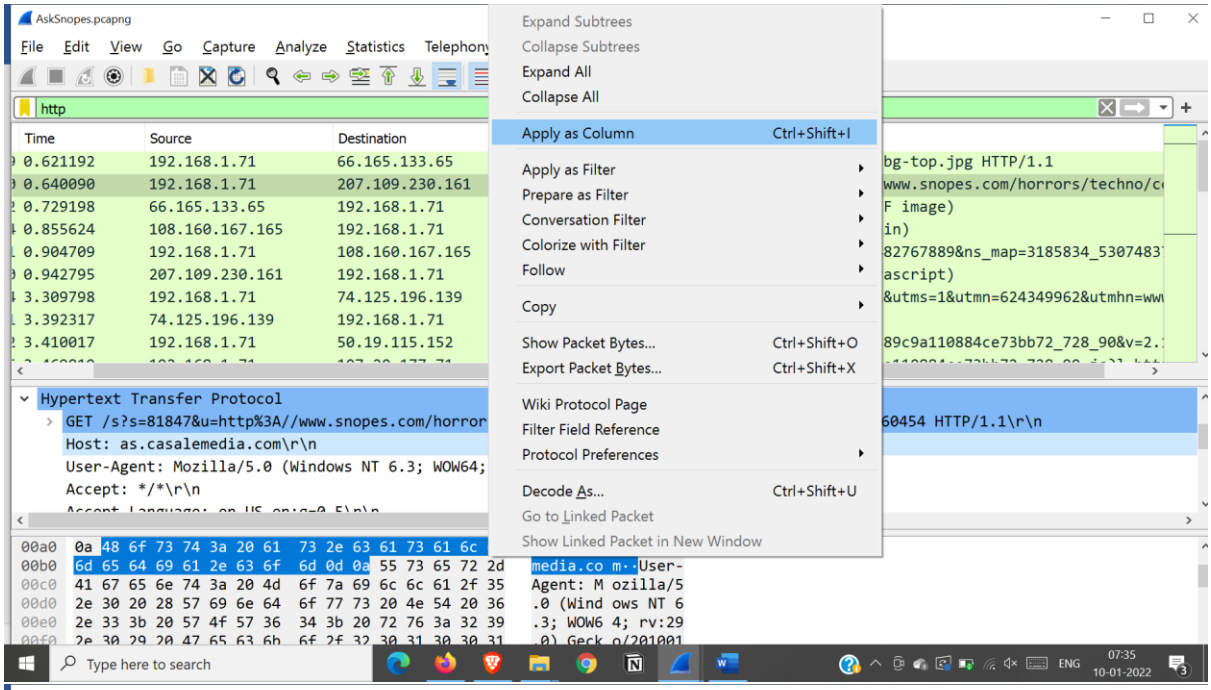
- According to Zillow, what instrument will Ryan learn to play?

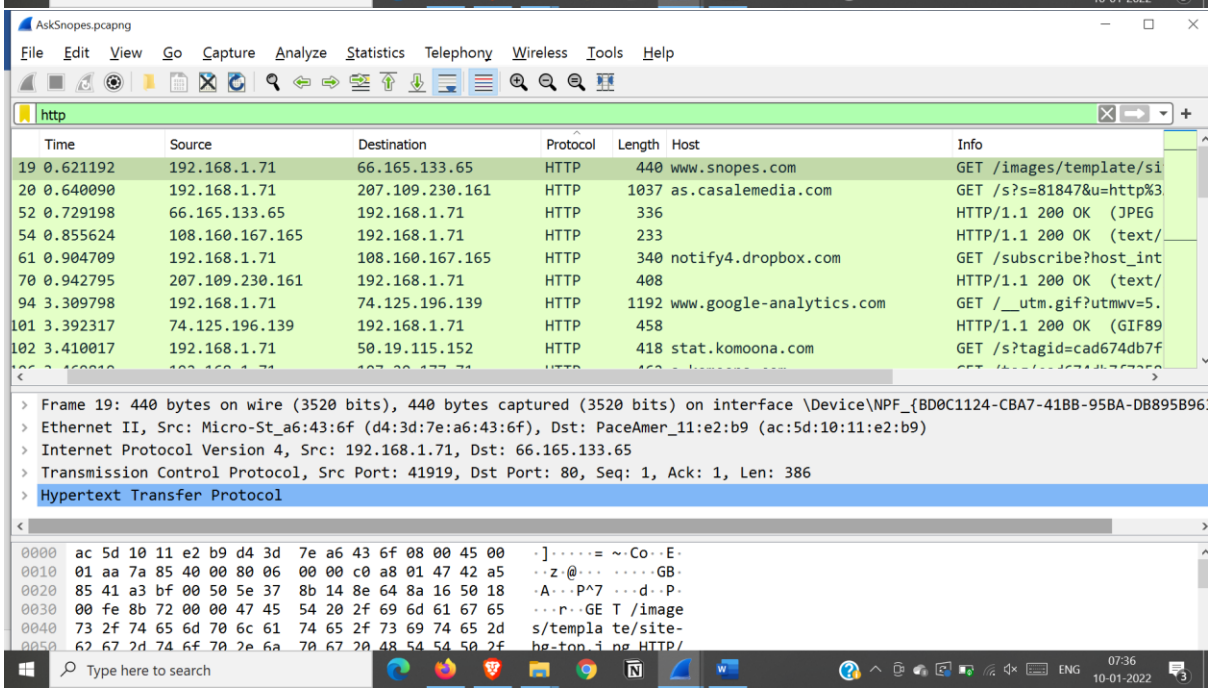
- How many web servers are running Apache?

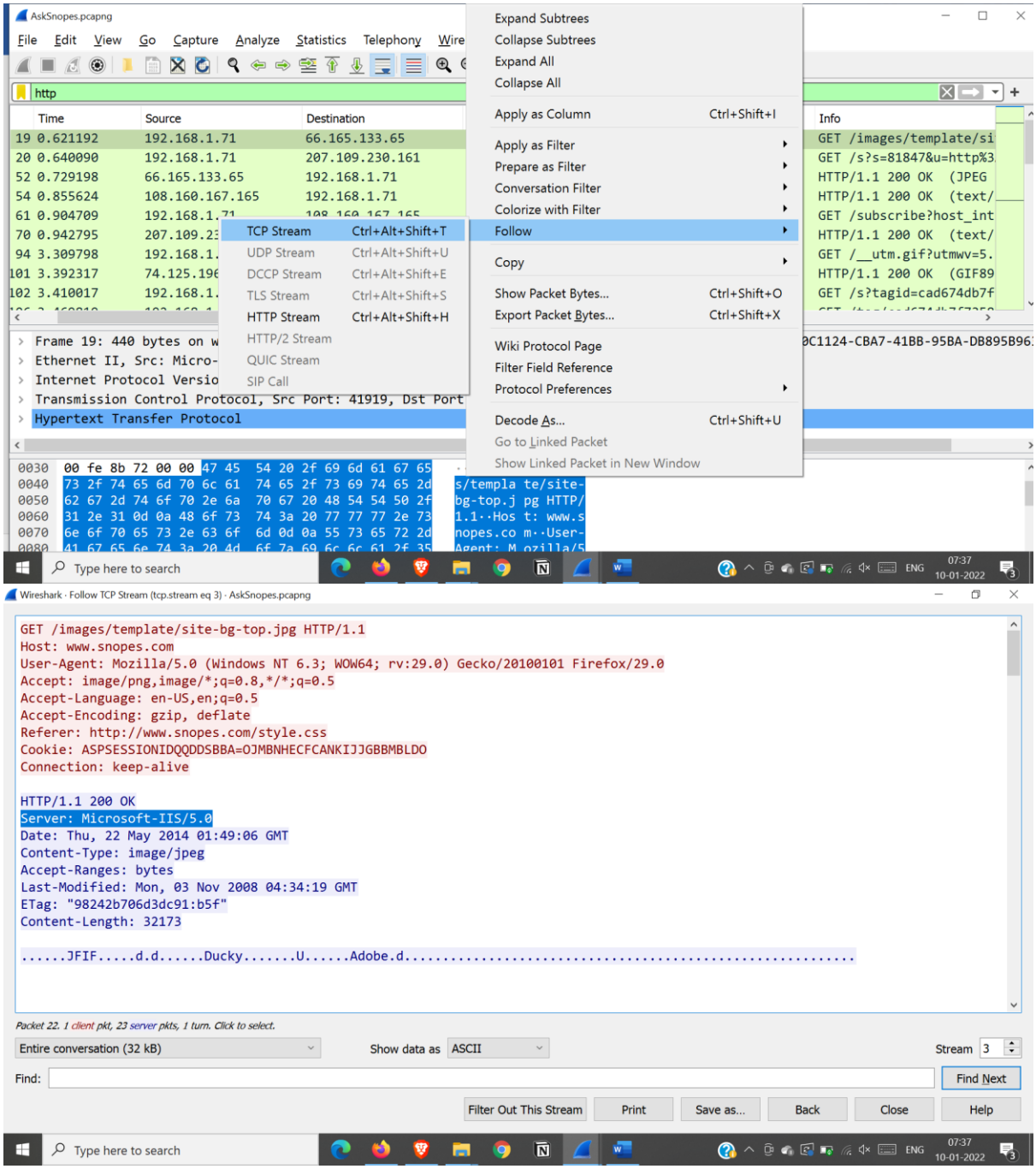
- What hosts (IP addresses) think that jokes are more entertaining when they are explained?

What webserver is this website using?




AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony
http
Time Source Destination
0.621192 192.168.1.71 66.165.133.65
0.640090 192.168.1.71 207.109.230.161
0.729198 66.165.133.65 192.168.1.71
0.855624 108.160.167.165 192.168.1.71
0.904709 192.168.1.71 108.160.167.165
0.942795 207.109.230.161 192.168.1.71
3.309798 192.168.1.71 74.125.196.139
3.392317 74.125.196.139 192.168.1.71
3.410017 192.168.1.71 50.19.115.152
Hypertext Transfer Protocol
GET /s?s=81847&u=http%3A//www.snopes.com/horror
Host: as.casalemedia.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64;
Accept: */*\r\n
00a0 0a 48 6f 73 74 3a 20 61 73 2e 63 61 73 61 6c
00b0 6d 65 64 69 61 2e 63 6f 6d 0d 0a 55 73 65 72 2d
00c0 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35
00d0 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 36
00e0 2e 33 3b 20 57 4f 57 36 34 3b 20 72 76 3a 32 39
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
Type here to search
ENG
07:35
10-01-2022


AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Time Source Destination Protocol Length Host Info
19 0.621192 192.168.1.71 66.165.133.65 HTTP 440 www.snopes.com GET /images/template/si
20 0.640090 192.168.1.71 207.109.230.161 HTTP 1037 as.casalemedia.com GET /s?s=81847&u=http%3
52 0.729198 66.165.133.65 192.168.1.71 HTTP 336 HTTP/1.1 200 OK (JPEG
54 0.855624 108.160.167.165 192.168.1.71 HTTP 233 HTTP/1.1 200 OK (text/
61 0.904709 192.168.1.71 108.160.167.165 HTTP 340 notify4.dropbox.com GET /subscribe?host_int
70 0.942795 207.109.230.161 192.168.1.71 HTTP 408 HTTP/1.1 200 OK (text/
94 3.309798 192.168.1.71 74.125.196.139 HTTP 1192 www.google-analytics.com GET /__utm.gif?utmwv=5.
101 3.392317 74.125.196.139 192.168.1.71 HTTP 458 HTTP/1.1 200 OK (GIF89
102 3.410017 192.168.1.71 50.19.115.152 HTTP 418 stat.komoona.com GET /s?tagid=cad674db7f
Frame 19: 440 bytes on wire (3520 bits), 440 bytes captured (3520 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB895B96
Ethernet II, Src: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f), Dst: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9)
Internet Protocol Version 4, Src: 192.168.1.71, Dst: 66.165.133.65
Transmission Control Protocol, Src Port: 41919, Dst Port: 80, Seq: 1, Ack: 1, Len: 386
Hypertext Transfer Protocol
0000 ac 5d 10 11 e2 b9 d4 3d 7e a6 43 6f 08 00 45 00
0010 01 aa 7a 85 40 00 80 06 00 00 c0 a8 01 47 42 a5
0020 85 41 a3 bf 00 50 5e 37 8b 14 8e 64 8a 16 50 18
0030 00 fe 8b 72 00 00 47 45 54 20 2f 69 6d 61 67 65
0040 73 2f 74 65 6d 70 6c 61 74 65 2f 73 69 74 65 2d
Type here to search
ENG
07:36
10-01-2022

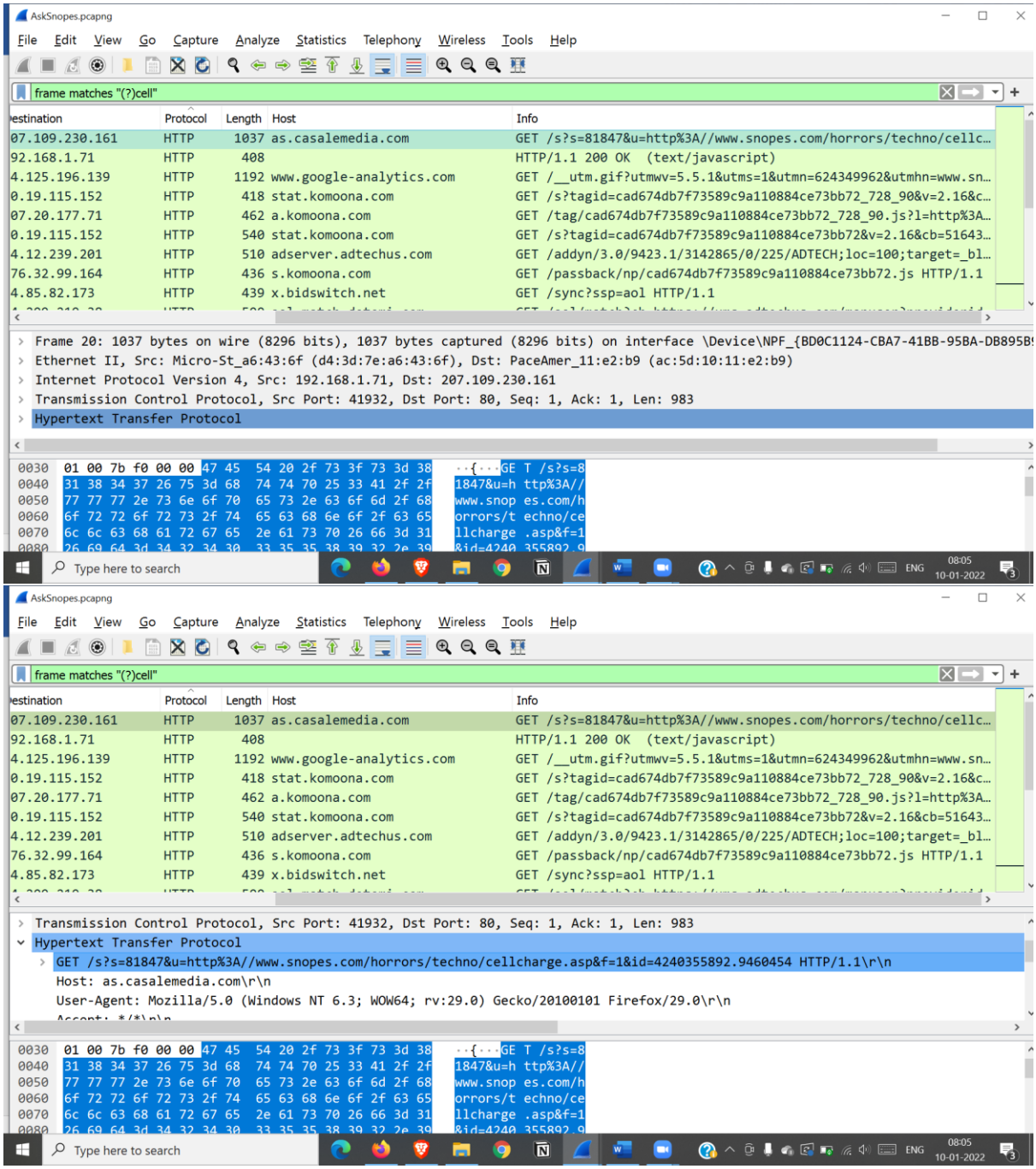


Server is Microsoft iis server

About what cell phone problem is the client concerned with?

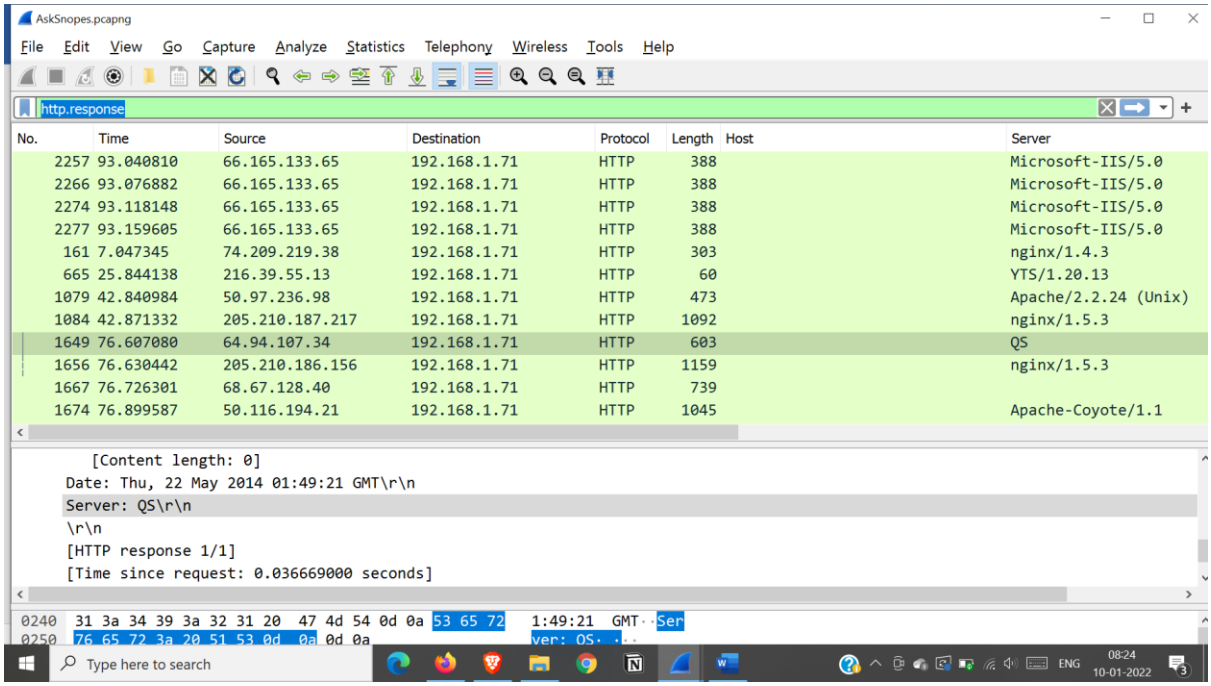
Search for a keyword cell in all cell packets using regex

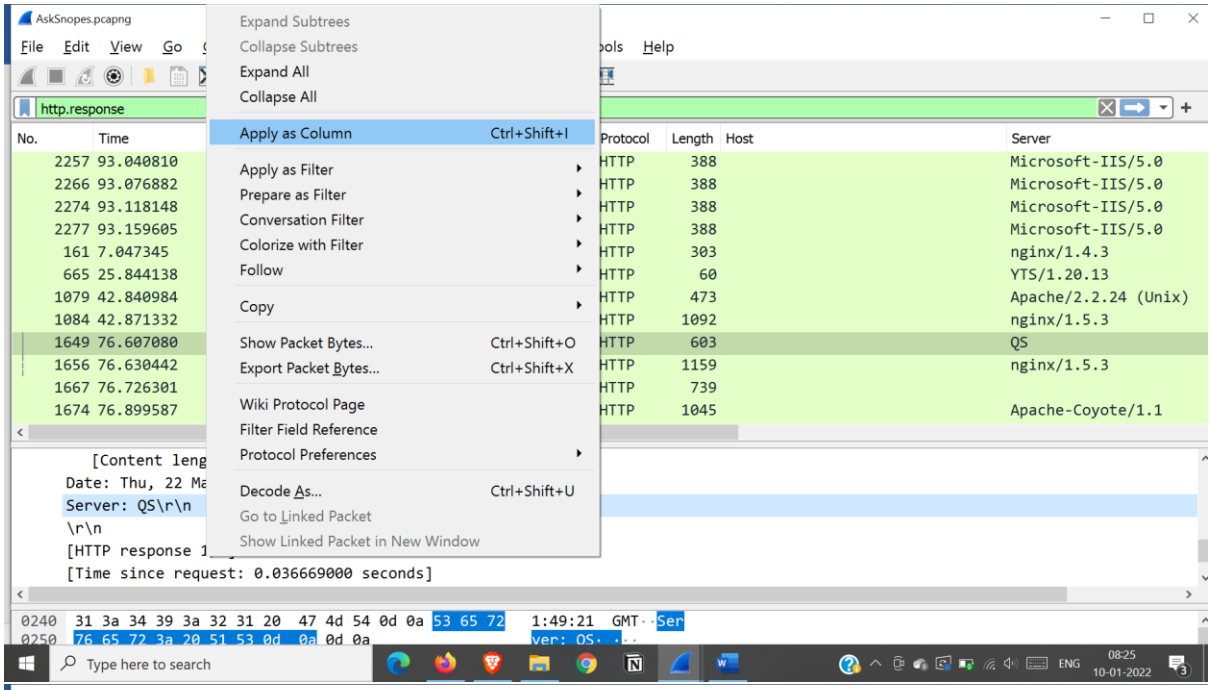
frame matches ”(?)cell”

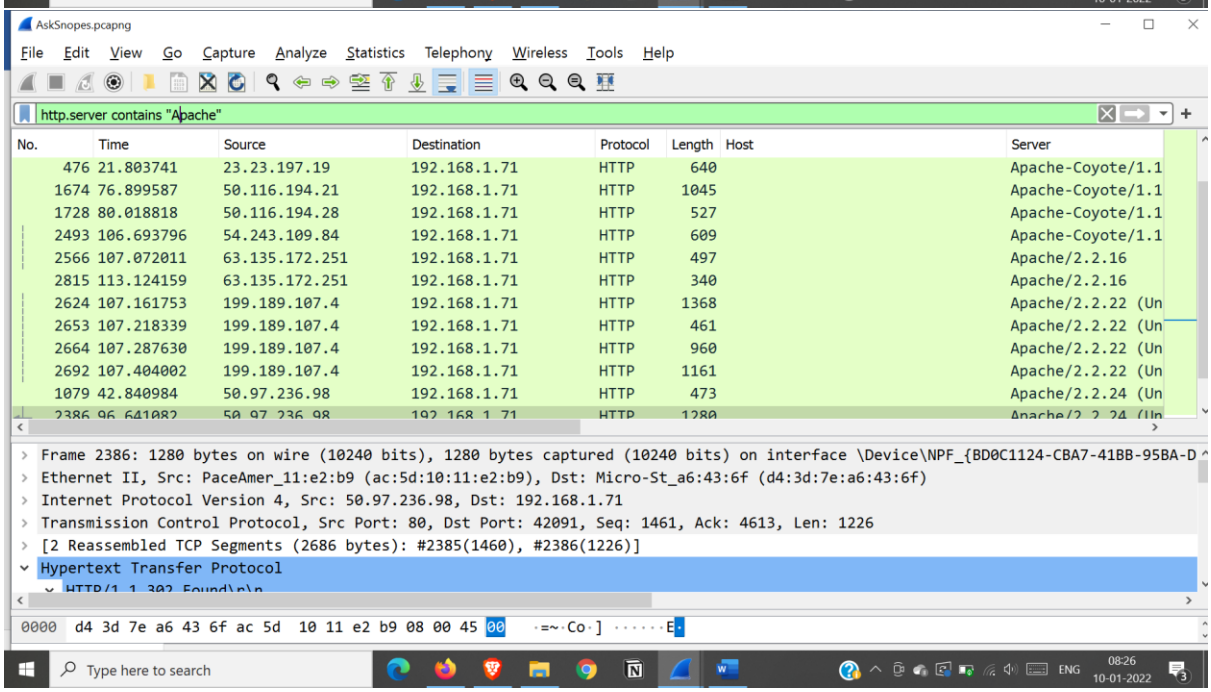


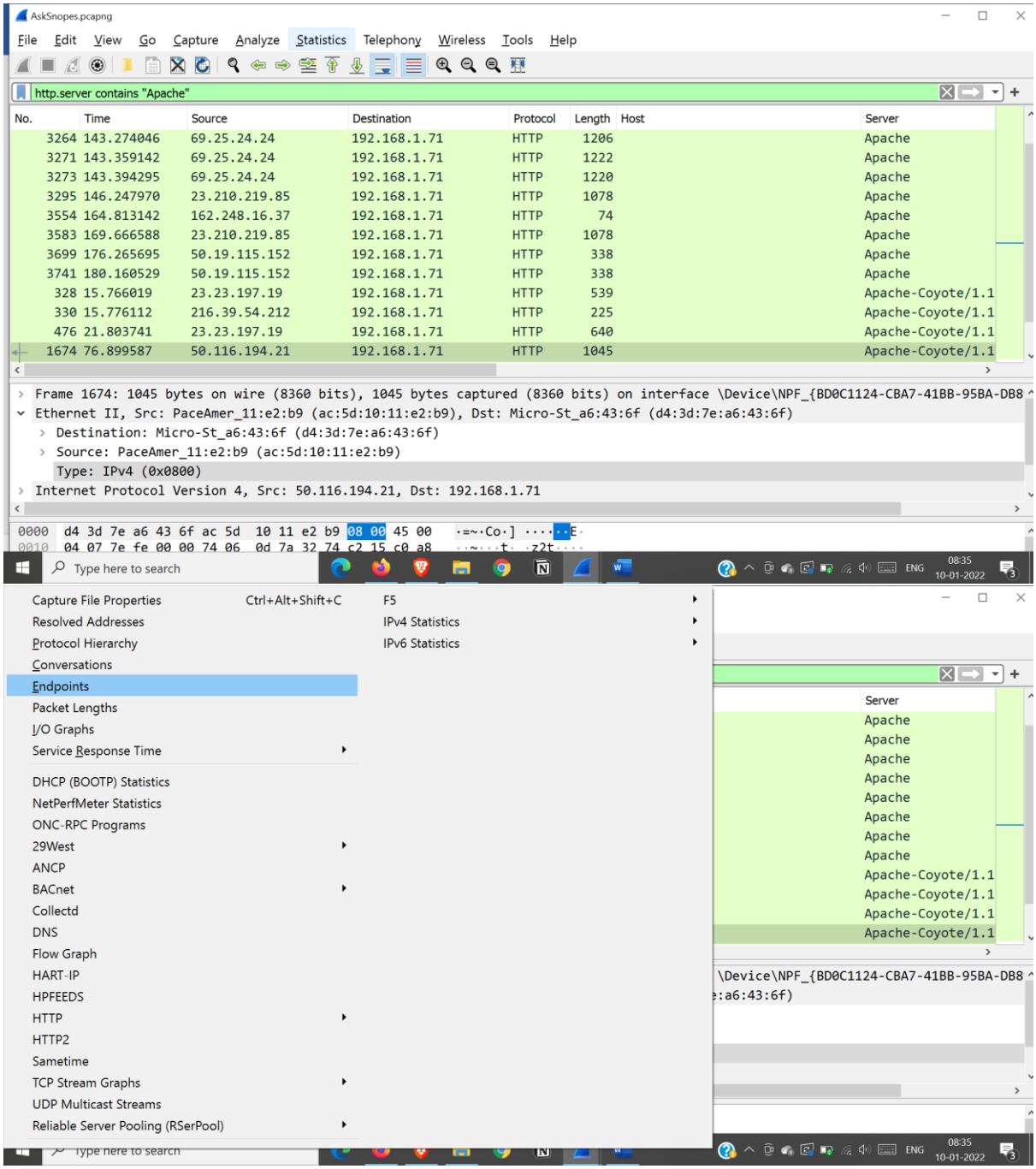
Client had searched for cell charge problem

How many webservers?

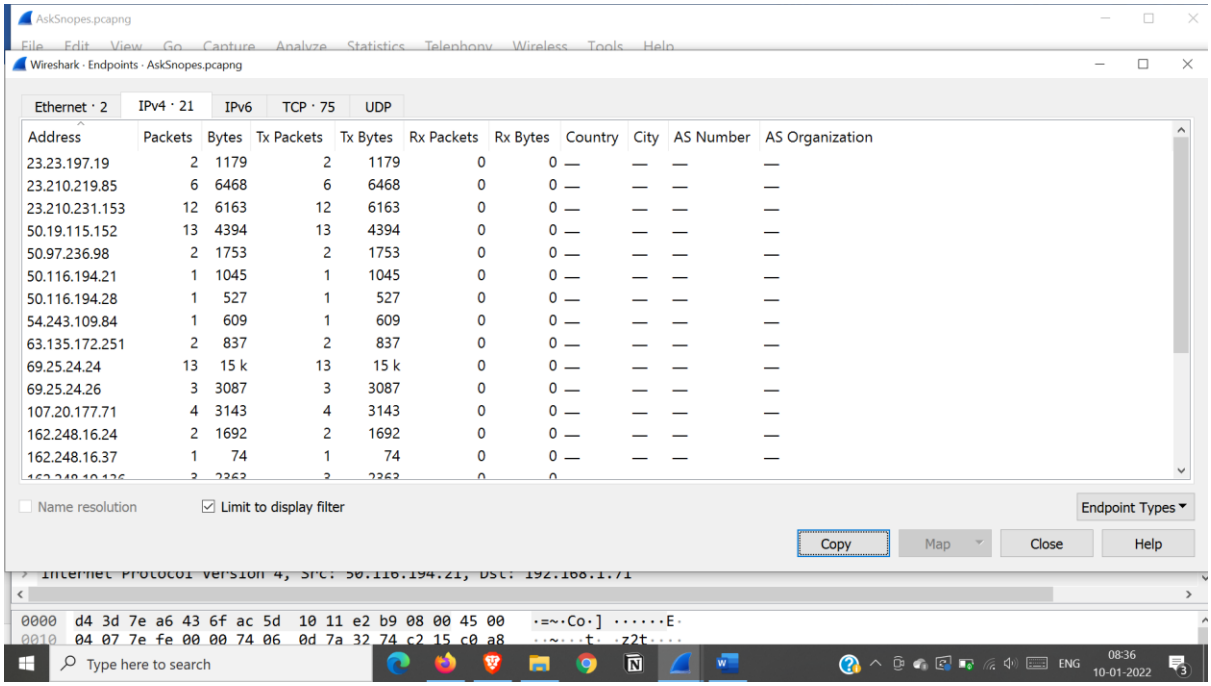



AskSnopes.pcapng
File Edit View Go
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
http.response
No. Time Protocol Length Host Server
2257 93.040810 HTTP 388 Microsoft-IIS/5.0
2266 93.076882 HTTP 388 Microsoft-IIS/5.0
2274 93.118148 HTTP 388 Microsoft-IIS/5.0
2277 93.159605 HTTP 388 Microsoft-IIS/5.0
161 7.047345 HTTP 303 nginx/1.4.3
665 25.844138 HTTP 60 YTS/1.20.13
1079 42.840984 HTTP 473 Apache/2.2.24 (Unix)
1084 42.871332 HTTP 1092 nginx/1.5.3
1649 76.607080 HTTP 603 QS
1656 76.630442 HTTP 1159 nginx/1.5.3
1667 76.726301 HTTP 739
1674 76.899587 HTTP 1045 Apache-Coyote/1.1
[Content leng
Date: Thu, 22 Ma
Server: QS\r\n
\r\n
[HTTP response 1
[Time since request: 0.036669000 seconds]
0240 31 3a 34 39 3a 32 31 20 47 4d 54 0d 0a 53 65 72 1:49:21 GMT··Ser
0250 76 65 72 3a 20 51 53 0d 0a 0d 0a ver: QS· ···
Type here to search
ENG 08:25 10-01-2022

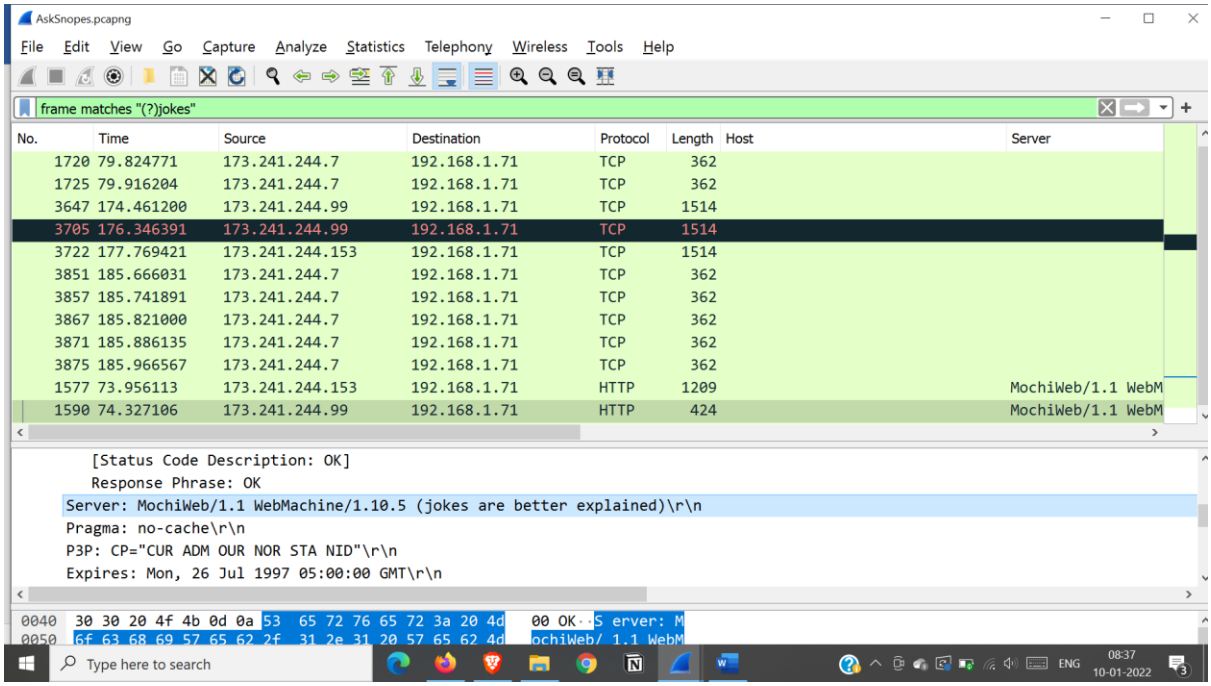

AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.server contains "Apache"
No. Time Source Destination Protocol Length Host Server
476 21.803741 23.23.197.19 192.168.1.71 HTTP 640 Apache-Coyote/1.1
1674 76.899587 50.116.194.21 192.168.1.71 HTTP 1045 Apache-Coyote/1.1
1728 80.018818 50.116.194.28 192.168.1.71 HTTP 527 Apache-Coyote/1.1
2493 106.693796 54.243.109.84 192.168.1.71 HTTP 609 Apache-Coyote/1.1
2566 107.072011 63.135.172.251 192.168.1.71 HTTP 497 Apache/2.2.16
2815 113.124159 63.135.172.251 192.168.1.71 HTTP 340 Apache/2.2.16
2624 107.161753 199.189.107.4 192.168.1.71 HTTP 1368 Apache/2.2.22 (Un
2653 107.218339 199.189.107.4 192.168.1.71 HTTP 461 Apache/2.2.22 (Un
2664 107.287630 199.189.107.4 192.168.1.71 HTTP 960 Apache/2.2.22 (Un
2692 107.404002 199.189.107.4 192.168.1.71 HTTP 1161 Apache/2.2.22 (Un
1079 42.840984 50.97.236.98 192.168.1.71 HTTP 473 Apache/2.2.24 (Un
Frame 2386: 1280 bytes on wire (10240 bits), 1280 bytes captured (10240 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-D
Ethernet II, Src: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f)
Internet Protocol Version 4, Src: 50.97.236.98, Dst: 192.168.1.71
Transmission Control Protocol, Src Port: 80, Dst Port: 42091, Seq: 1461, Ack: 4613, Len: 1226
[2 Reassembled TCP Segments (2686 bytes): #2385(1460), #2386(1226)]
Hypertext Transfer Protocol
0000 d4 3d 7e a6 43 6f ac 5d 10 11 e2 b9 08 00 45 00 ·=~·Co·] ·····E·
Type here to search
ENG 08:26 10-01-2022


AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.server contains "Apache"
No. Time Source Destination Protocol Length Host Server
3264 143.274046 69.25.24.24 192.168.1.71 HTTP 1206 Apache
3271 143.359142 69.25.24.24 192.168.1.71 HTTP 1222 Apache
3273 143.394295 69.25.24.24 192.168.1.71 HTTP 1220 Apache
3295 146.247970 23.210.219.85 192.168.1.71 HTTP 1078 Apache
3554 164.813142 162.248.16.37 192.168.1.71 HTTP 74 Apache
3583 169.666588 23.210.219.85 192.168.1.71 HTTP 1078 Apache
3699 176.265695 50.19.115.152 192.168.1.71 HTTP 338 Apache
3741 180.160529 50.19.115.152 192.168.1.71 HTTP 338 Apache
328 15.766019 23.23.197.19 192.168.1.71 HTTP 539 Apache-Coyote/1.1
330 15.776112 216.39.54.212 192.168.1.71 HTTP 225 Apache-Coyote/1.1
476 21.803741 23.23.197.19 192.168.1.71 HTTP 640 Apache-Coyote/1.1
1674 76.899587 50.116.194.21 192.168.1.71 HTTP 1045 Apache-Coyote/1.1
Frame 1674: 1045 bytes on wire (8360 bits), 1045 bytes captured (8360 bits) on interface \Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB8
Ethernet II, Src: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9), Dst: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f)
Destination: Micro-St_a6:43:6f (d4:3d:7e:a6:43:6f)
Source: PaceAmer_11:e2:b9 (ac:5d:10:11:e2:b9)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 50.116.194.21, Dst: 192.168.1.71
0000 d4 3d 7e a6 43 6f ac 5d 10 11 e2 b9 08 00 45 00
0010 04 07 7e fe 00 00 74 06 0d 7a 32 74 c2 15 c0 a8
Type here to search
ENG 08:35 10-01-2022

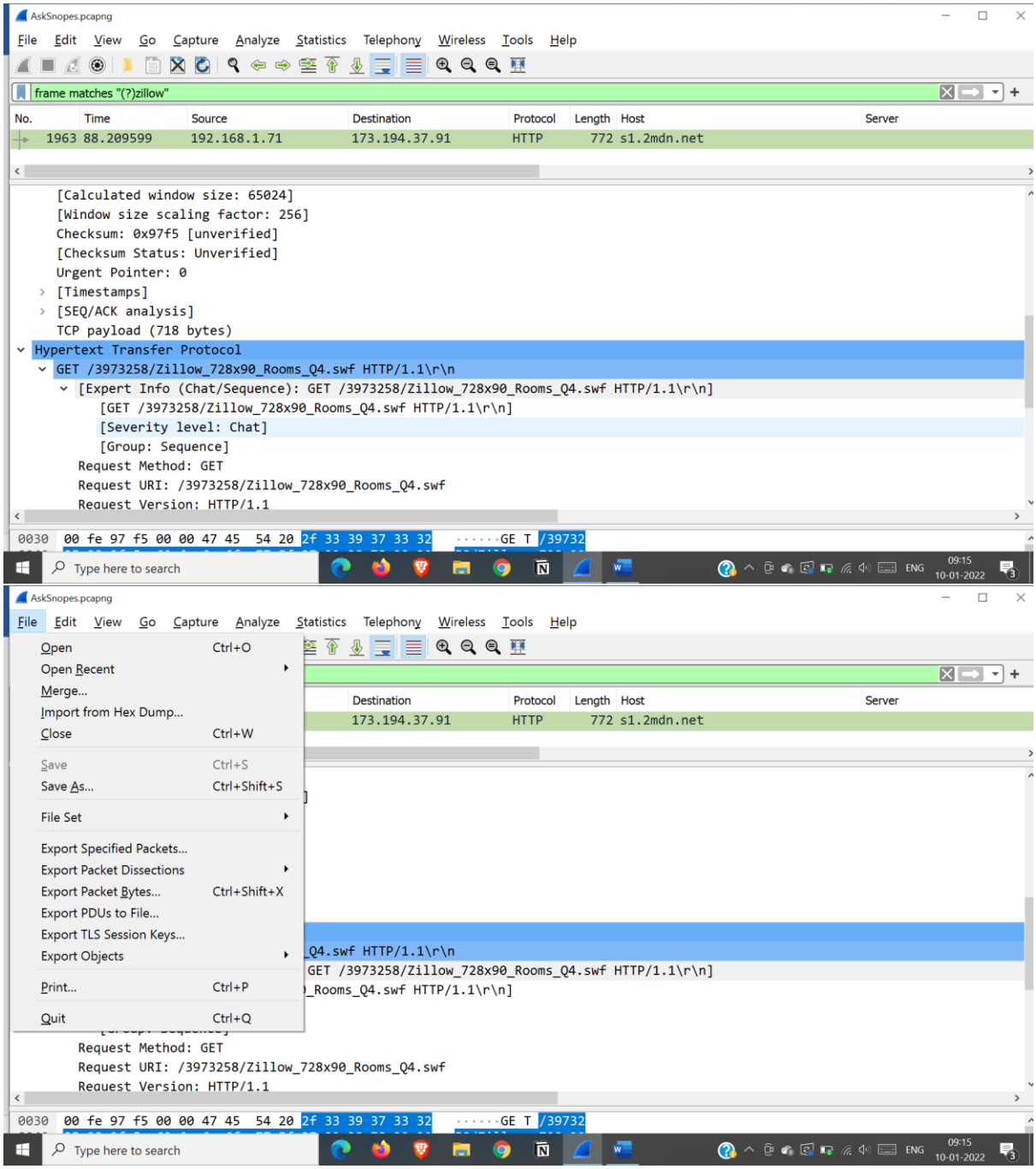
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
Reliable Server Pooling (RSerPool)
F5
IPv4 Statistics
IPv6 Statistics
Server
Apache
Apache-Coyote/1.1
\Device\NPF_{BD0C1124-CBA7-41BB-95BA-DB8
:a6:43:6f)
Type here to search
ENG 08:35 10-01-2022

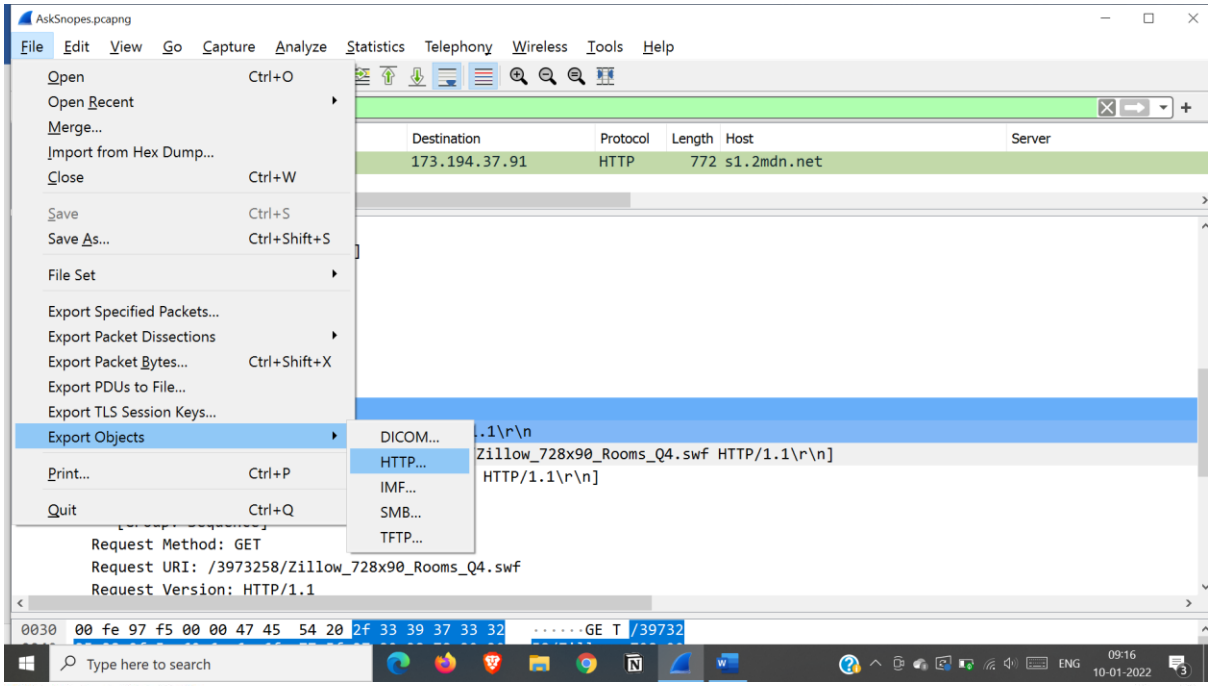

AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Endpoints · AskSnopes.pcapng
Ethernet · 2
IPv4 · 21
IPv6
TCP · 75
UDP
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City AS Number AS Organization
23.23.197.19 2 1179 2 1179 0 0 — — — —
23.210.219.85 6 6468 6 6468 0 0 — — — —
23.210.231.153 12 6163 12 6163 0 0 — — — —
50.19.115.152 13 4394 13 4394 0 0 — — — —
50.97.236.98 2 1753 2 1753 0 0 — — — —
50.116.194.21 1 1045 1 1045 0 0 — — — —
50.116.194.28 1 527 1 527 0 0 — — — —
54.243.109.84 1 609 1 609 0 0 — — — —
63.135.172.251 2 837 2 837 0 0 — — — —
69.25.24.24 13 15 k 13 15 k 0 0 — — — —
69.25.24.26 3 3087 3 3087 0 0 — — — —
107.20.177.71 4 3143 4 3143 0 0 — — — —
162.248.16.24 2 1692 2 1692 0 0 — — — —
162.248.16.37 1 74 1 74 0 0 — — — —
Name resolution
Limit to display filter
Endpoint Types
Copy
Map
Close
Help
Internet Protocol Version 4, Src: 50.116.194.21, Dst: 192.168.1.71
0000 d4 3d 7e a6 43 6f ac 5d 10 11 e2 b9 08 00 45 00
0010 04 07 7e fe 00 00 74 06 0d 7a 32 74 c2 15 c0 a8
Type here to search
ENG
08:36
10-01-2022

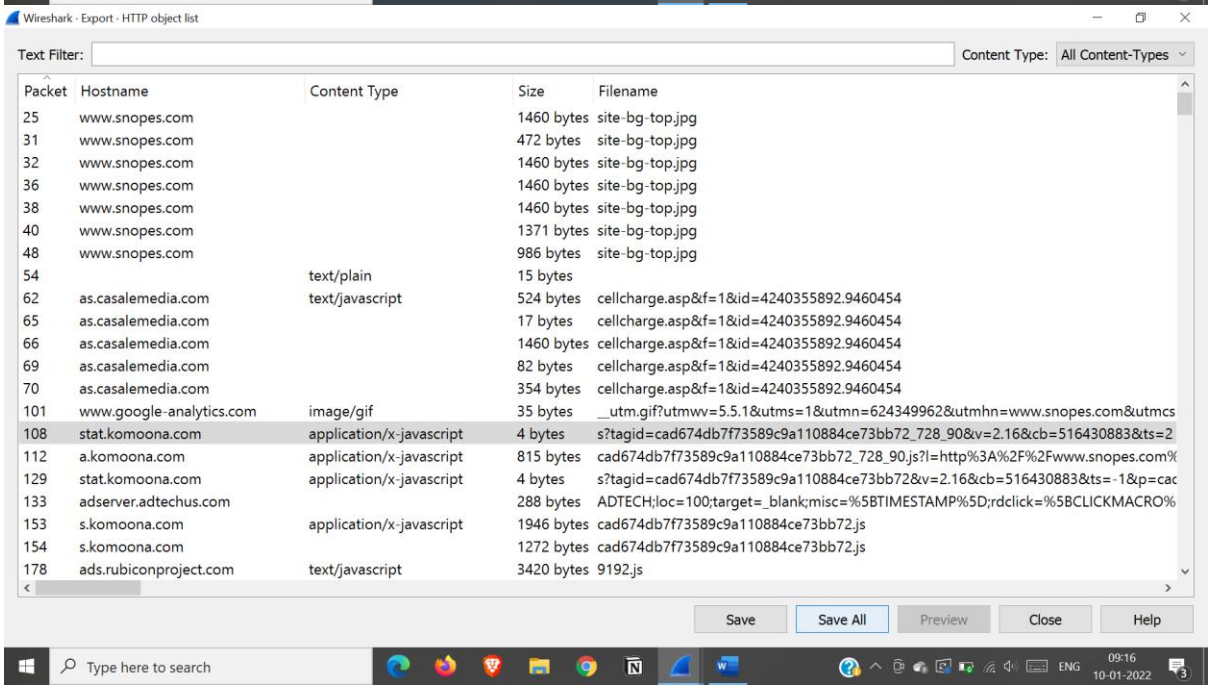
What hosts think Jokes are more entertaining when they are explained?

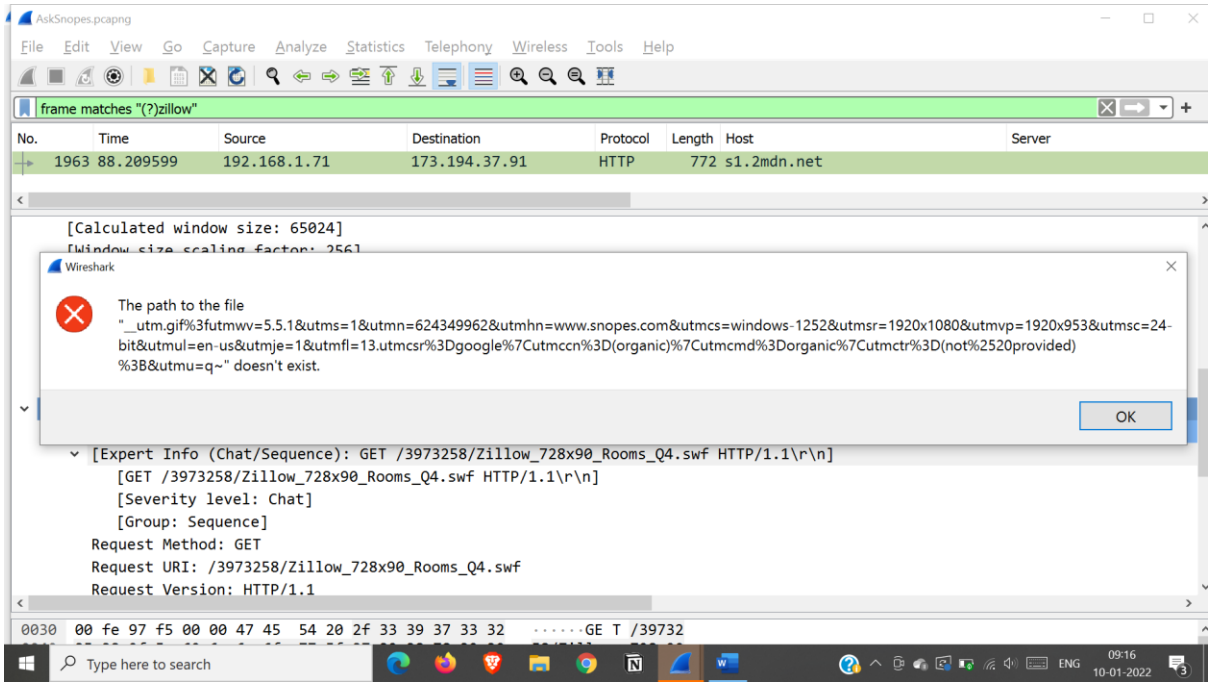


According to Zillow what instrument will reyan learn to play?




AskSnopes.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
HTTP...
IMF...
SMB...
TFTP...
Destination Protocol Length Host Server
173.194.37.91 HTTP 772 s1.2mdn.net
Zillow_728x90_Rooms_Q4.swf HTTP/1.1\r\n]
HTTP/1.1\r\n]
Request Method: GET
Request URI: /3973258/Zillow_728x90_Rooms_Q4.swf
Request Version: HTTP/1.1
0030 00 fe 97 f5 00 00 47 45 54 20 2f 33 39 37 33 32 ·····GE T /39732
Type here to search
ENG 09:16 10-01-2022

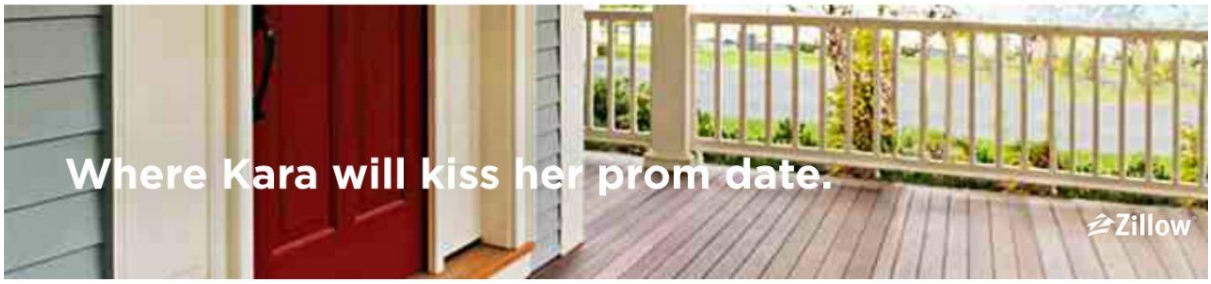

Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
25 www.snopes.com 1460 bytes site-bg-top.jpg
31 www.snopes.com 472 bytes site-bg-top.jpg
32 www.snopes.com 1460 bytes site-bg-top.jpg
36 www.snopes.com 1460 bytes site-bg-top.jpg
38 www.snopes.com 1460 bytes site-bg-top.jpg
40 www.snopes.com 1371 bytes site-bg-top.jpg
48 www.snopes.com 986 bytes site-bg-top.jpg
54 text/plain 15 bytes
62 as.casalemedia.com text/javascript 524 bytes cellcharge.asp&f=1&id=4240355892.9460454
65 as.casalemedia.com 17 bytes cellcharge.asp&f=1&id=4240355892.9460454
66 as.casalemedia.com 1460 bytes cellcharge.asp&f=1&id=4240355892.9460454
69 as.casalemedia.com 82 bytes cellcharge.asp&f=1&id=4240355892.9460454
70 as.casalemedia.com 354 bytes cellcharge.asp&f=1&id=4240355892.9460454
101 www.google-analytics.com image/gif 35 bytes __utm.gif?utmwv=5.5.1&utms=1&utmn=624349962&utmhn=www.snopes.com&utmcs
108 stat.komoona.com application/x-javascript 4 bytes s?tagid=cad674db7f73589c9a110884ce73bb72_728_90&v=2.16&cb=516430883&ts=2
112 a.komoona.com application/x-javascript 815 bytes cad674db7f73589c9a110884ce73bb72_728_90.js?l=http%3A%2F%2Fwww.snopes.com%
129 stat.komoona.com application/x-javascript 4 bytes s?tagid=cad674db7f73589c9a110884ce73bb72&v=2.16&cb=516430883&ts=-1&p=cac
133 adserver.adtechus.com 288 bytes ADTECH;loc=100;target=_blank;misc=%5BTIMESTAMP%5D;rdclick=%5BCLICKMACRO%
153 s.komoona.com application/x-javascript 1946 bytes cad674db7f73589c9a110884ce73bb72.js
154 s.komoona.com 1272 bytes cad674db7f73589c9a110884ce73bb72.js
178 ads.rubiconproject.com text/javascript 3420 bytes 9192.js
Save Save All Preview Close Help
Type here to search
ENG 09:16 10-01-2022



Mark ok to all errors

Open zillow.swf file from extracted paths

Adobe Flash Player 32
File View Control Help

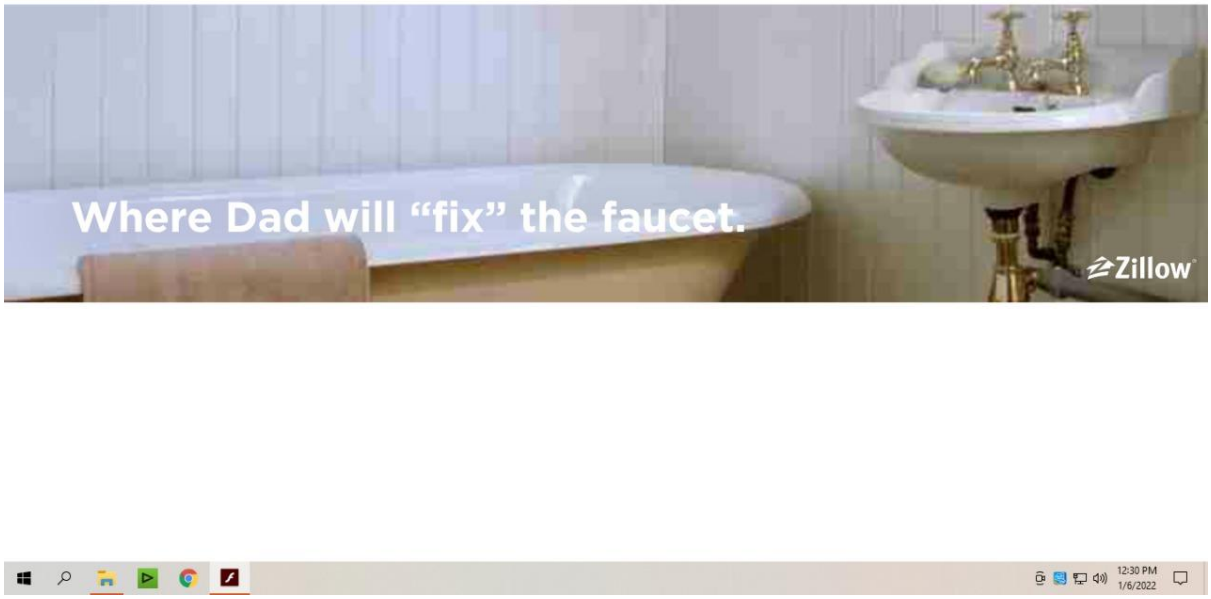


12:30 PM
1/6/2022

Adobe Flash Player 32
File View Control Help

Zillow®
SEARCH
NEARBY HOMES

12:30 PM
1/6/2022


Adobe Flash Player 32
File View Control Help
Where Dad will “fix” the faucet.
Zillow
12:30 PM
1/6/2022