

Q1

# Q1

Q.1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
179	2.939721	106.51.145.89	172.16.31.15	HTTP	259	HTTP/1.1 200 OK (application/
184	2.948360	172.16.31.15	146.190.62.39	HTTP	492	GET / HTTP/1.1
193	3.165412	146.190.62.39	172.16.31.15	HTTP	1350	HTTP/1.1 200 OK (text/html)
203	3.217933	172.16.31.15	146.190.62.39	HTTP	378	GET /js/init.min.js HTTP/1.1
298	3.438544	146.190.62.39	172.16.31.15	HTTP	440	HTTP/1.1 200 OK (application/
306	3.788638	172.16.31.15	146.190.62.39	HTTP	396	GET /css/style.min.css HTTP/1.1
307	3.789294	172.16.31.15	146.190.62.39	HTTP	401	GET /css/style-wide.min.css HT
334	4.002772	172.16.31.15	146.190.62.39	HTTP	403	GET /css/style-normal.min.css
345	4.014317	172.16.31.15	146.190.62.39	HTTP	403	GET /css/style-narrow.min.css
346	4.014438	172.16.31.15	146.190.62.39	HTTP	405	GET /css/style-narrower.min.cs
349	4.040579	146.190.62.39	172.16.31.15	HTTP	972	HTTP/1.1 200 OK (text/css)
351	4.041038	172.16.31.15	146.190.62.39	HTTP	403	GET /css/style-mobile.min.css
356	4.226048	146.190.62.39	172.16.31.15	HTTP	1182	HTTP/1.1 200 OK (text/css)
358	4.241597	146.190.62.39	172.16.31.15	HTTP	1232	HTTP/1.1 200 OK (text/css)
360	4.244789	146.190.62.39	172.16.31.15	HTTP	915	HTTP/1.1 200 OK (text/css)
363	4.249995	146.190.62.39	172.16.31.15	HTTP	1252	HTTP/1.1 200 OK (text/css)
373	4.266167	146.190.62.39	172.16.31.15	HTTP	1471	HTTP/1.1 200 OK (text/css)
491	4.970253	172.16.31.15	146.190.62.39	HTTP	463	GET /css/images/banner.svg HT
492	4.971183	172.16.31.15	146.190.62.39	HTTP	478	GET /css/images/header-major-c
493	4.972149	172.16.31.15	146.190.62.39	HTTP	477	GET /css/images/header-major-c
687	5.196189	146.190.62.39	172.16.31.15	HTTP/X...	1337	HTTP/1.1 200 OK
688	5.198311	146.190.62.39	172.16.31.15	HTTP/X...	1331	HTTP/1.1 200 OK
689	5.200553	146.190.62.39	172.16.31.15	HTTP/X...	1381	HTTP/1.1 200 OK
705	5.248888	172.16.31.15	146.190.62.39	HTTP	436	GET /favicon.ico HTTP/1.1
719	5.483363	146.190.62.39	172.16.31.15	HTTP	787	HTTP/1.1 200 OK (image/x-ico

> Frame 687: Packet, 1337 bytes on wire (10696 bits), 1337 bytes  
 > Ethernet II, Src: Sonicwall\_ee:46:3d (18:b1:69:ee:46:3d), Dst:  
 > Internet Protocol Version 4, Src: 146.190.62.39, Dst: 172.16.3  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 55562,  
 > Hypertext Transfer Protocol  
 > HTTP/1.1 200 OK\r\n

0000 e0 d4 e8 b9 6e a0 18 b1 69 ee 46 3d 00  
 0010 05 2b bd 29 40 00 31 06 eb 9e 92 be 30  
 0020 1f 0f 00 50 d9 0a 39 44 9f 12 d9 2d 30  
 0030 01 f5 cb 41 00 00 48 54 54 50 2f 31 20  
 0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 70

Packet (1337 bytes) Decoded UTF-8 text (457 bytes)

Hypertext Transfer Protocol: Protocol Packets: 1484 · Displayed: 28 (1.9%) · Dropped: 0 (0.0%) Profile: Default

Wireshark · HTTP / Requests · Q.1.pcapng

Request Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	18				0.0037	100%	0.0400	4.003
httpforever.com	12				0.0025	66.67%	0.0400	4.003
/js/init.min.js	1				0.0002	8.33%	0.0100	3.218
/favicon.ico	1				0.0002	8.33%	0.0100	5.249
/css/style.min.css	1				0.0002	8.33%	0.0100	3.789
/css/style-wide.min.css	1				0.0002	8.33%	0.0100	3.789
/css/style-normal.min.css	1				0.0002	8.33%	0.0100	4.003
/css/style-narrower.min.css	1				0.0002	8.33%	0.0100	4.014
/css/style-narrow.min.css	1				0.0002	8.33%	0.0100	4.014
/css/style-mobile.min.css	1				0.0002	8.33%	0.0100	4.041
/css/images/header-major-on-light.svg	1				0.0002	8.33%	0.0100	4.971
/css/images/header-major-on-dark.svg	1				0.0002	8.33%	0.0100	4.972
/css/images/banner.svg	1				0.0002	8.33%	0.0100	4.970
/	1				0.0002	8.33%	0.0100	2.948
239.255.255.250:1900	4				0.0008	22.22%	0.0100	4.609
*	4				0.0008	100.00%	0.0100	4.609
x1.i.lencr.org	1				0.0002	5.56%	0.0100	2.836
/	1				0.0002	100.00%	0.0100	2.836

# Q1

Wireshark · HTTP / Packet Counter · Q.1.pcapng

Packet Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
▼ Total HTTP Packets	32				0.0066	100%	0.0500	4.003
▼ HTTP Request Packets	18				0.0037	56.25%	0.0400	4.003
GET	14				0.0029	77.78%	0.0400	4.003
SEARCH	4				0.0008	22.22%	0.0100	4.609
▼ HTTP Response Packets	14				0.0029	43.75%	0.0500	4.226
▼ 2xx: Success	14				0.0029	100.00%	0.0500	4.226
200 OK	14				0.0029	100.00%	0.0500	4.226
??? broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client 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:  Apply

Copy Save as... Close

Wireshark · Conversations · Q.1.pcapng

Conversation Settings

☐ Name resolution

☐ Absolute start time

☐ Display raw data

☒ Limit to display filter

Copy

Follow Stream...

Graph...

I/O Graphs

Protocol

☐ Bluetooth

☐ BPv7

☐ DCCP

☐ DNP 3.0

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☐ ILNP

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ LTP

Filter list for specific type

Ethernet · 1

IPv4 · 2

IPv6

TCP · 8

UDP

Address A	Address B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A
172.16.31.15	106.51.145.89	4	1 kB	10	16	25.00%	
172.16.31.15	146.190.62.39	24	19 kB	6	94	25.53%	

Close Help

Wireshark packet capture showing DNS traffic. The top pane displays a list of packets, with packet 159 selected. The bottom pane shows the details of the selected packet, which is a DNS response from 172.16.31.15 to 192.168.1.100. The response contains a query for 'x1.i.lencr.org' and 'x1.i.lencr.org: type A, class IN'. The response is a standard query response with no error, and it includes the IP address 172.16.31.15 for the query.

# Q1

