


capture.pcapng

http.host = "www.faqs.org"

No.	Time	Source	Destination	Protocol	Length	Info
1362	115.538073	192.168.1.4	199.231.164.68	HTTP	429	GET / HTTP/1.1
1400	115.742105	192.168.1.4	199.231.164.68	HTTP	434	GET /faqs/ HTTP/1.1
1406	115.928833	192.168.1.4	199.231.164.68	HTTP	404	GET /style/faqs.css HTTP/1.1
1436	116.079869	192.168.1.4	199.231.164.68	HTTP	386	GET /style/rs.js HTTP/1.1
1437	116.080276	192.168.1.4	199.231.164.68	HTTP	383	GET /utils.js HTTP/1.1
1483	116.233640	192.168.1.4	199.231.164.68	HTTP	515	GET /images/faqs.org.png HTTP/1.1
1484	116.234196	192.168.1.4	199.231.164.68	HTTP	514	GET /images/library.jpg HTTP/1.1
1554	116.442576	192.168.1.4	199.231.164.68	HTTP	519	GET /style/i/faqs-header.png HTTP/1.1
1738	117.529437	192.168.1.4	199.231.164.68	HTTP	458	GET /favicon.ico HTTP/1.1

Frame Number: 1362
 Frame Length: 429 bytes (3432 bits)
 Capture Length: 429 bytes (3432 bits)

2) Transmission Control Protocol, Src Port: 60291, Dst Port: 80, Seq: 364, Ack: 576, Len: 368

Source Port: 60291
 Destination Port: 80
 [Stream index: 36]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 368]
 Sequence Number: 364 (relative sequence number)

3)

Capture.pcapng

Apply a display filter ... <3%>

No.	Time	Source	Destination	Protocol	Length	Info
2036	138.937879	192.168.1.4	35.186.224.44	TCP	66	59840 → 443 [ACK] Seq=2721 Ack=1055 W
2037	138.938965	35.186.224.44	192.168.1.4	TLSv1...	106	Application Data
2038	138.938966	35.186.224.44	192.168.1.4	TLSv1...	148	Application Data
2039	138.938967	35.186.224.44	192.168.1.4	TLSv1...	94	Application Data
2040	138.938968	35.186.224.44	192.168.1.4	TLSv1...	100	Application Data
2041	138.939052	192.168.1.4	35.186.224.44	TCP	66	59840 → 443 [ACK] Seq=2721 Ack=1095 W
2042	138.939110	192.168.1.4	35.186.224.44	TCP	66	59840 → 443 [ACK] Seq=2721 Ack=1177 W
2043	138.939132	192.168.1.4	35.186.224.44	TCP	66	59840 → 443 [ACK] Seq=2721 Ack=1239 W
2044	139.017312	192.168.1.12	224.0.0.251	MDNS	266	Standard query response 0x0000 TXT, c
2045	139.054754	192.168.1.4	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
2046	139.946197	192.168.1.4	192.168.1.1	DNS	70	Standard query 0x0f0d A github.com
2047	139.966093	192.168.1.1	192.168.1.4	DNS	86	Standard query response 0x0f0d A gith
2048	139.967277	192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=0
2049	140.015860	140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=0

4)

kai ins

```
Type: 0 Echo (ping) reply
Code: 0
Checksum: 0x92a1 [correct]
[Checksum Status: Good]
Identifier (BE): 49703 (0xc227)
Identifier (LE): 10178 (0x27c2)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)
[Request frame: 2048]
```

→ Reply

kai ins

```
▼ Internet Control Message Protocol
  Type: 8 Echo (ping) request
  Code: 0
  Checksum: 0x8aa1 [correct]
  [Checksum Status: Good]
  Identifier (BE): 49703 (0xc227)
  Identifier (LE): 10178 (0x27c2)
  Sequence Number (BE): 0 (0x0000)
  Sequence Number (LE): 0 (0x0000)
```

→ Request

5)

capture.pcapng

icmp

Source	Destination	Protocol	Length	Info
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=6/153, ttl=43 (request id=0xc227, seq=5/153, ttl=43)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=7/1792, ttl=64 (reply id=0xc227, seq=6/153, ttl=43)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=8/2048, ttl=64 (reply id=0xc227, seq=7/1792, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=9/2304, ttl=64 (reply id=0xc227, seq=8/2048, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=10/2560, ttl=64 (reply id=0xc227, seq=9/2304, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=11/2816, ttl=64 (reply id=0xc227, seq=10/2560, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=11/2816, ttl=64 (reply id=0xc227, seq=10/2560, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=12/3072, ttl=64 (reply id=0xc227, seq=11/2816, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=12/3072, ttl=64 (reply id=0xc227, seq=11/2816, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=13/3328, ttl=64 (reply id=0xc227, seq=12/3072, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=13/3328, ttl=64 (reply id=0xc227, seq=12/3072, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=14/3584, ttl=64 (reply id=0xc227, seq=13/3328, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=14/3584, ttl=64 (reply id=0xc227, seq=13/3328, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=15/3840, ttl=64 (reply id=0xc227, seq=14/3584, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=15/3840, ttl=64 (reply id=0xc227, seq=14/3584, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=16/4096, ttl=64 (reply id=0xc227, seq=15/3840, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=16/4096, ttl=64 (reply id=0xc227, seq=15/3840, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=17/4352, ttl=64 (reply id=0xc227, seq=16/4096, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=17/4352, ttl=64 (reply id=0xc227, seq=16/4096, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=18/4608, ttl=64 (reply id=0xc227, seq=17/4352, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=18/4608, ttl=64 (reply id=0xc227, seq=17/4352, ttl=64)
192.168.1.4	140.82.121.4	ICMP	98	Echo (ping) request id=0xc227, seq=19/4864, ttl=64 (reply id=0xc227, seq=18/4608, ttl=64)
140.82.121.4	192.168.1.4	ICMP	98	Echo (ping) reply id=0xc227, seq=19/4864, ttl=64 (reply id=0xc227, seq=18/4608, ttl=64)

Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:etherhertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Apple_72:bb:82 (1c:57:dc:72:bb:82), Dst: 74:fe:c0:df:38:71 (74:fe:c0:df:38:71)
Destination: 74:fe:c0:df:38:71 (74:fe:c0:df:38:71)

4864

capture.pcapng

http_user_agent

No.	Time	Source	Destination	Protocol	Length	Info
958	00:00:00.000000	192.168.1.4	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
964	68.499647	192.168.1.4	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
973	69.500080	192.168.1.4	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
1067	70.501214	192.168.1.4	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
1106	73.685697	192.168.1.12	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
1117	74.638076	192.168.1.12	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
1125	76.654825	192.168.1.12	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
1362	115.538073	192.168.1.4	199.231.164.68	HTTP	429	GET / HTTP/1.1
1406	115.742105	192.168.1.4	199.231.164.68	HTTP	434	GET /faq/ HTTP/1.1
1406	115.928033	192.168.1.4	199.231.164.68	HTTP	494	GET /style/faqs.css HTTP/1.1
1436	116.079869	192.168.1.4	199.231.164.68	HTTP	386	GET /style/rs.js HTTP/1.1
1443	116.112080	192.168.1.4	199.231.164.68	HTTP	507	GET /style/rs.css HTTP/1.1
1483	116.233640	192.168.1.4	199.231.164.68	HTTP	515	GET /images/faqs.org.png HTTP/1.1
1484	116.234196	192.168.1.4	199.231.164.68	HTTP	514	GET /images/library.jpg HTTP/1.1
1554	116.442576	192.168.1.4	199.231.164.68	HTTP	519	GET /style/l/faqs-header.png HTTP/1.1
1738	117.529437	192.168.1.4	199.231.164.68	HTTP	458	GET /favicon.ico HTTP/1.1

HOST: 239.255.255.250:1900\r\nMAN: ssdp:discover\r\nST: urn:dial-multiscreen-org:service:dial:1\r\nUSER-AGENT: Chromium/128.0.6613.138 Mac OS X\r\n\r\n

```
ST: urn:dial-multiscreen-org:service:dial:1\r\nUSER-AGENT: Chromium/128.0.6613.138 Mac OS X\r\n\r\n
```

FULL request ORA: http://239.255.255.250:1900/\r\n[HTTP request 1/4]\r\n[Next request in Frame: 958]

6)

7)

capture.pcapng

http.host == "www.faqs.org" && http.request.uri contains ".js"

No.	Time	Source	Destination	Protocol	Length	Info
1436	116.079869	192.168.1.4	199.231.164.68	HTTP	386	GET /style/rs.js HTTP/1.1
1437	116.080276	192.168.1.4	199.231.164.68	HTTP	383	GET /utils.js HTTP/1.1

total 2

8)

capture.pcapng

http.response.code

No.	Time	Source	Destination	Protocol	Length	Info
686	53.616500	192.168.1.7	192.168.1.4	SSDP	378	HTTP/1.1 200 OK
1395	115.728337	199.231.164.68	192.168.1.4	HTTP	641	HTTP/1.1 301 Moved Permanently (text/html)
1403	115.912460	199.231.164.68	192.168.1.4	HTTP	1503	HTTP/1.1 200 OK (text/html)
1439	116.080578	199.231.164.68	192.168.1.4	HTTP	648	HTTP/1.1 200 OK (text/css)
1479	116.230873	199.231.164.68	192.168.1.4	HTTP	727	HTTP/1.1 200 OK (application/javascript)
1481	116.232517	199.231.164.68	192.168.1.4	HTTP	910	HTTP/1.1 200 OK (application/javascript)
1532	116.438129	199.231.164.68	192.168.1.4	HTTP	674	HTTP/1.1 200 OK (PNG)
1536	116.438137	199.231.164.68	192.168.1.4	HTTP	1157	HTTP/1.1 200 OK (JPEG JFIF image)
1590	116.593143	199.231.164.68	192.168.1.4	HTTP	729	HTTP/1.1 200 OK (PNG)
1744	117.719138	199.231.164.68	192.168.1.4	HTTP	1109	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

200

capture.pcapng

arp

Source	Destination	Protocol	Length	Info
42:83:c1:4d:50:b3	Broadcast	ARP	42	42 Who has 192.168.1.10? Tell 192.168.1.3
Apple_72:bb:82		ARP	42	42 192.168.1.10 is at 1c:57:dc:72:bb:82
Apple_72:bb:82		ARP	42	42 Who has 192.168.1.3? Tell 192.168.1.10
42:83:c1:4d:50:b3	Apple_72:bb:82	ARP	42	42 192.168.1.3 is at 42:83:c1:4d:50:b3
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 192.168.1.1 is at 74:fe:ce:df:38:71
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 Who has 192.168.1.4? Tell 192.168.1.1
Apple_72:bb:82		ARP	42	42 192.168.1.4 is at 1c:57:dc:72:bb:82
Apple_72:bb:82		Broadcast	42	42 Who has 192.168.1.17 Tell 192.168.1.4
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 192.168.1.1 is at 74:fe:ce:df:38:71
Apple_72:bb:82		Broadcast	42	42 Who has 192.168.1.77 Tell 192.168.1.4
04:f9:21:ec:36:4c	Apple_72:bb:82	ARP	42	42 192.168.1.7 is at d4:f9:21:ec:36:4c
Apple_72:bb:82		Broadcast	42	42 Who has 192.168.1.37 Tell 192.168.1.4
42:83:c1:4d:50:b3	Apple_72:bb:82	ARP	42	42 192.168.1.3 is at 42:83:c1:4d:50:b3
Apple_72:bb:82		ARP	42	42 Who has 192.168.1.37 Tell 192.168.1.10
42:83:c1:4d:50:b3	Apple_72:bb:82	ARP	42	42 192.168.1.3 is at 42:83:c1:4d:50:b3
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 Who has 192.168.1.4? Tell 192.168.1.1
Apple_72:bb:82		ARP	42	42 192.168.1.4 is at 1c:57:dc:72:bb:82
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 Who has 192.168.1.4? Tell 192.168.1.1
Apple_72:bb:82		ARP	42	42 192.168.1.4 is at 1c:57:dc:72:bb:82
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 192.168.1.1 is at 74:fe:ce:df:38:71

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4

Sender MAC address: 42:83:c1:4d:50:b3 (42:83:c1:4d:50:b3)
Sender IP address: 192.168.1.3
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.10

capture.pcapng

arp

Source	Destination	Protocol	Length	Info
42:83:c1:4d:50:b3	Broadcast	ARP	42	42 Who has 192.168.1.10? Tell 192.168.1.3
Apple_72:bb:82		ARP	42	42 192.168.1.10 is at 1c:57:dc:72:bb:82
Apple_72:bb:82		ARP	42	42 Who has 192.168.1.3? Tell 192.168.1.10
42:83:c1:4d:50:b3	Apple_72:bb:82	ARP	42	42 192.168.1.3 is at 42:83:c1:4d:50:b3
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 192.168.1.1 is at 74:fe:ce:df:38:71
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 Who has 192.168.1.4? Tell 192.168.1.1
Apple_72:bb:82		ARP	42	42 192.168.1.4 is at 1c:57:dc:72:bb:82
Apple_72:bb:82		Broadcast	42	42 Who has 192.168.1.17 Tell 192.168.1.4
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 192.168.1.1 is at 74:fe:ce:df:38:71
Apple_72:bb:82		Broadcast	42	42 Who has 192.168.1.77 Tell 192.168.1.4
d4:f9:21:ec:36:4c	Apple_72:bb:82	ARP	42	42 192.168.1.7 is at d4:f9:21:ec:36:4c
Apple_72:bb:82		Broadcast	42	42 Who has 192.168.1.37 Tell 192.168.1.4
42:83:c1:4d:50:b3	Apple_72:bb:82	ARP	42	42 192.168.1.3 is at 42:83:c1:4d:50:b3
Apple_72:bb:82		ARP	42	42 Who has 192.168.1.37 Tell 192.168.1.10
42:83:c1:4d:50:b3	Apple_72:bb:82	ARP	42	42 192.168.1.3 is at 42:83:c1:4d:50:b3
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 Who has 192.168.1.4? Tell 192.168.1.1
Apple_72:bb:82		ARP	42	42 192.168.1.4 is at 1c:57:dc:72:bb:82
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
Apple_98:14:8c		Broadcast	42	42 Who has 192.168.1.54? Tell 192.168.1.12
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 Who has 192.168.1.4? Tell 192.168.1.1
Apple_72:bb:82		ARP	42	42 192.168.1.4 is at 1c:57:dc:72:bb:82
74:fe:ce:df:38:71	Apple_72:bb:82	ARP	42	42 192.168.1.1 is at 74:fe:ce:df:38:71

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4

Sender MAC address: Apple_72:bb:82 (1c:57:dc:72:bb:82)
Sender IP address: 192.168.1.10
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.3

10)

capture.pcapng

ip.src == 192.168.1.4 & udp

No.	Time	Source	Destination	Protocol	Length	Info
285	23.901554	192.168.1.4	216.58.212.10	QUIC	1242	Initial, DCID=f22bb64640c02ad2, PKN: 81 Handshake, DCID=fb5289844c12fe5
286	23.903212	192.168.1.4	142.250.187.142	QUIC	81	Handshake, DCID=fb5289844c12fe5
293	23.942237	192.168.1.4	142.250.187.142	QUIC	81	Handshake, DCID=fb5289844c12fe5
294	23.944333	192.168.1.4	216.58.212.10	QUIC	81	Handshake, DCID=f22bb64640c02ad2
295	23.951221	192.168.1.4	142.250.187.142	QUIC	115	Handshake, DCID=fb5289844c12fe5
296	23.952489	192.168.1.4	142.250.187.142	QUIC	73	Protected Payload (KPO), DCID=fb52898
297	23.952866	192.168.1.4	142.250.187.142	QUIC	92	Protected Payload (KPO), DCID=fb52898
298	23.955355	192.168.1.4	142.250.187.142	QUIC	138	Protected Payload (KPO), DCID=fb52898
299	23.955357	192.168.1.4	142.250.187.142	QUIC	139	Protected Payload (KPO), DCID=fb52898
300	23.955375	192.168.1.4	142.250.187.142	QUIC	114	Protected Payload (KPO), DCID=fb52898
301	23.955661	192.168.1.4	142.250.187.142	QUIC	128	Protected Payload (KPO), DCID=fb52898
302	23.955663	192.168.1.4	142.250.187.142	QUIC	129	Protected Payload (KPO), DCID=fb52898
303	23.955675	192.168.1.4	142.250.187.142	QUIC	8	Protected Payload (KPO), DCID=fb52898
304	23.955725	192.168.1.4	142.250.187.142	QUIC	6	Protected Payload (KPO), DCID=fb52898
305	23.956358	192.168.1.4	142.250.187.142	QUIC	54	Protected Payload (KPO), DCID=fb52898
306	23.956299	192.168.1.4	142.250.187.142	QUIC	129	Protected Payload (KPO), DCID=fb52898
307	23.956438	192.168.1.4	142.250.187.142	QUIC	81	Protected Payload (KPO), DCID=fb52898
310	23.976407	192.168.1.4	142.250.187.142	QUIC	3	Protected Payload (KPO), DCID=fb52898
311	23.976431	192.168.1.4	142.250.187.142	QUIC	124	Protected Payload (KPO), DCID=fb52898
318	23.980610	192.168.1.4	216.58.212.10	QUIC	31	Handshake, DCID=f22bb864640c02ad2
322	23.983723	192.168.1.4	216.58.212.10	QUIC	15	Handshake, DCID=f22bb64640c02ad2
323	23.984151	192.168.1.4	216.58.212.10	QUIC	73	Protected Payload (KPO), DCID=f22bb864
324	23.984330	192.168.1.4	216.58.212.10	QUIC	96	Protected Payload (KPO), DCID=f22bb864
325	23.984545	192.168.1.4	216.58.212.10	QUIC	238	Protected Payload (KPO), DCID=f22bb864
326	23.984546	192.168.1.4	216.58.212.10	QUIC	239	Protected Payload (KPO), DCID=f22bb864
327	23.984548	192.168.1.4	216.58.212.10	QUIC	188	Protected Payload (KPO), DCID=f22bb864
328	23.984618	192.168.1.4	216.58.212.10	QUIC	76	Protected Payload (KPO), DCID=f22bb64640c02

Frame Length: 78 bytes (624 bits)
Capture Length: 78 bytes (624 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:quic]
[Coloring Rule Name: UDP]
[Coloring Rule Description:]

QUIC is in majority

the filter