

Lab 8 – SSL/TLS

```
Command Prompt
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 12:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2600:8806:6202:1d00:b91c:fc89:27b8:2bb
Temporary IPv6 Address. . . . . : 2600:8806:6202:1d00:a001:c226:a8aa:b0d2
IPv4 Address. . . . . : 192.168.0.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::3e37:86ff:fe08:bada%6
192.168.0.1

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\yddi>
```

Questions:

Client Hello Record:

1. What is the SSL/TLS version of the of the Client Hello frame?

TLS 1.2

The image shows a Wireshark network packet capture of a TLS handshake. The packet list on the left shows several frames, with frame 657 (Client Hello) highlighted. The packet details pane on the right shows the structure of the Client Hello frame, with the 'Version: TLS 1.2 (0x0303)' field highlighted. The packet bytes pane at the bottom shows the raw hex and ASCII data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
642	13:53:48.475484	204.79.197.200	192.168.0.15	TLSv1.2	109	Application Data
657	13:53:48.490305	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
658	13:53:48.490365	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
659	13:53:48.492678	204.79.197.200	192.168.0.15	TLSv1.2	175	Application Data
664	13:53:48.507245	13.249.42.221	192.168.0.15	TLSv1.2	1514	Server Hello
669	13:53:48.507720	13.249.42.221	192.168.0.15	TLSv1.2	953	Certificate, Certificate Status, Server Key Exchange,

Frame 657: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits) on interface 0

Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

Internet Protocol Version 4, Src: 192.168.0.15, Dst: 13.249.42.221

Transmission Control Protocol, Src Port: 55419, Dst Port: 443, Seq: 1, Ack: 1, Len: 203

Transport Layer Security

- TLShv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 198
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 194
 - Version: TLS 1.2 (0x0303)
 - Random: 5cb7682cc63743b69089005fe6e79af11b4795ef28da0621...
 - Session ID length: 0

0000 3c 37 86 08 ba da f8 34 41 ac dc da 08 00 45 00 <7.....4 A.....E>

Wireshark Lab 8_Yakubu Iddrisu.pcapng

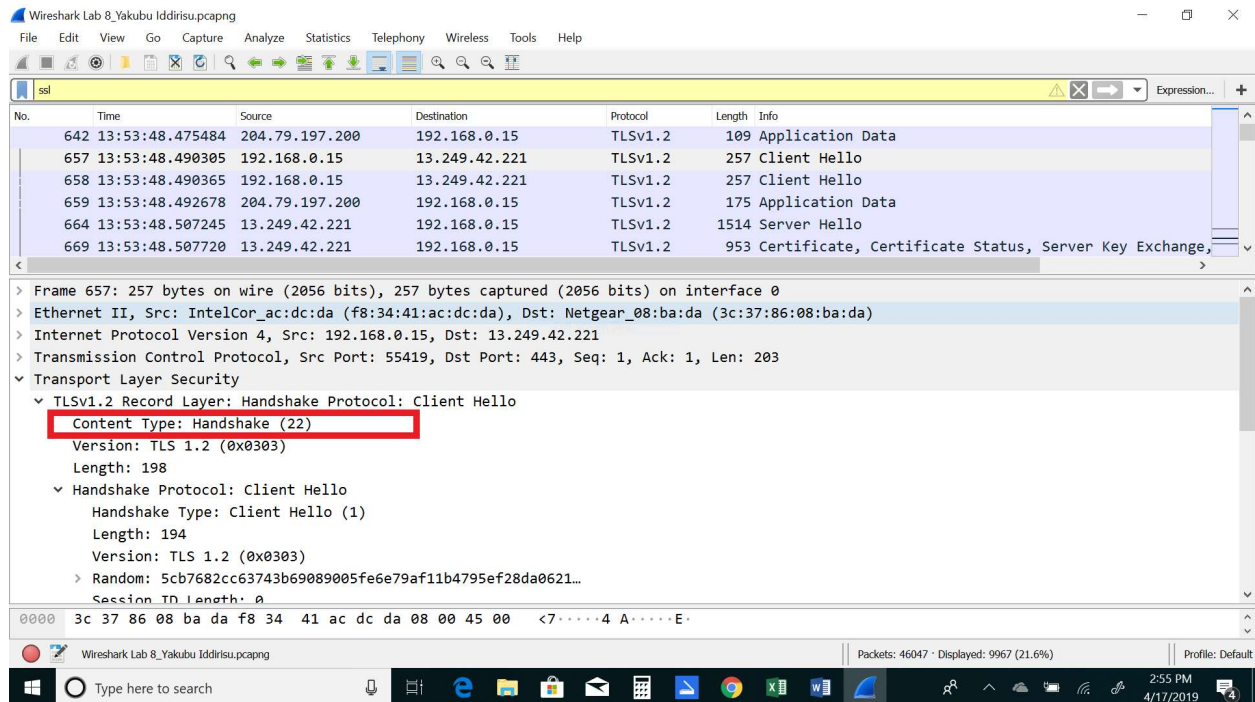
Packets: 46047 · Displayed: 9967 (21.6%)

Profile: Default

2:46 PM 4/17/2019

2. Expand the ClientHello record. (If your trace contains multiple ClientHello records, expand the frame that contains the first one.) What is the value of the content type?

Handshake (22)



Wireshark Lab 8_Yakubu Iddirisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
642	13:53:48.475484	204.79.197.200	192.168.0.15	TLSv1.2	109	Application Data
657	13:53:48.490305	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
658	13:53:48.490365	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
659	13:53:48.492678	204.79.197.200	192.168.0.15	TLSv1.2	175	Application Data
664	13:53:48.507245	13.249.42.221	192.168.0.15	TLSv1.2	1514	Server Hello
669	13:53:48.507720	13.249.42.221	192.168.0.15	TLSv1.2	953	Certificate, Certificate Status, Server Key Exchange,

> Frame 657: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits) on interface 0

> Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

> Internet Protocol Version 4, Src: 192.168.0.15, Dst: 13.249.42.221

> Transmission Control Protocol, Src Port: 55419, Dst Port: 443, Seq: 1, Ack: 1, Len: 203

▼ Transport Layer Security

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 198

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 194

Version: TLS 1.2 (0x0303)

> Random: 5cb7682cc63743b69089005fe6e79af11b4795ef28da0621...

Session ID Length: 0

0000 3c 37 86 08 ba da f8 34 41 ac dc da 08 00 45 00 <7.....4 A.....E>

Wireshark Lab 8_Yakubu Iddirisu.pcapng

Packets: 46047 · Displayed: 9967 (21.6%)

Profile: Default

Type here to search

2:55 PM 4/17/2019

3. Does the ClientHello record contain a nonce (also known as a “challenge”)? If so, what is the value of the challenge in hexadecimal notation?

c63743b69089005fe6e79af11b4795ef28da0621ce47878d...

The image shows a Wireshark capture of a TLS handshake. The packet list on the left shows several packets, with packet 657 (13:53:48.490305) highlighted in red, indicating it is the selected packet. The packet details pane on the right shows the structure of the ClientHello message. The 'Random Bytes' field is highlighted in red, showing the hexadecimal value c63743b69089005fe6e79af11b4795ef28da0621ce47878d... The packet bytes pane at the bottom shows the raw data of the selected packet, with the first few bytes highlighted in red: 0040 03 5c b7 68 2c c6 37 43 b6 90 89 00 5f e6 e7 9a.

Wireshark Lab 8_Yakubu Iddrisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
642	13:53:48.475484	204.79.197.200	192.168.0.15	TLSv1.2	109	Application Data
657	13:53:48.490305	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
658	13:53:48.490365	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
659	13:53:48.492678	204.79.197.200	192.168.0.15	TLSv1.2	175	Application Data
664	13:53:48.507245	13.249.42.221	192.168.0.15	TLSv1.2	1514	Server Hello
669	13:53:48.507720	13.249.42.221	192.168.0.15	TLSv1.2	953	Certificate, Certificate Status, Server Key Exchange,

▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 198
- ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 194
 - Version: TLS 1.2 (0x0303)
 - ▼ Random: 5cb7682cc63743b69089005fe6e79af11b4795ef28da0621...
 - GMT Unix Time: Apr 17, 2019 13:53:48.00000000 Eastern Daylight Time
 - Random Bytes: c63743b69089005fe6e79af11b4795ef28da0621ce47878d...
 - Session ID Length: 0
 - Cipher Suites Length: 38
 - ▼ Cipher Suites (19 suites)
 - Compression Methods Length: 1

0040 03 5c b7 68 2c c6 37 43 b6 90 89 00 5f e6 e7 9a -\h,7C

Random values used for deriving keys (tls.handshake.random_bytes), 28 bytes

Packets: 46047 · Displayed: 9967 (21.6%)

Profile: Default

4:01 PM 4/17/2019

4. Does the ClientHello record advertise the cyber suites it supports? If so, in the first listed suite, what are the public-key algorithm, the symmetric-key algorithm, and the hash algorithm?

Yes, it does advertise cyber suites.

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA284 (0xc02c)

The image shows a Wireshark capture of a TLS handshake. The packet list on the left shows several packets, with packet 657 (Client Hello) highlighted. The packet details pane on the right shows the structure of the Client Hello message, including the TLS version, random number, session ID length, cipher suites length, and a list of supported cipher suites. The first cipher suite, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c), is highlighted with a red box. The packet bytes pane at the bottom shows the raw data of the cipher suites list.

No.	Time	Source	Destination	Protocol	Length	Info
642	13:53:48.475484	204.79.197.200	192.168.0.15	TLSv1.2	109	Application Data
657	13:53:48.490305	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
658	13:53:48.490365	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
659	13:53:48.492678	204.79.197.200	192.168.0.15	TLSv1.2	175	Application Data
664	13:53:48.507245	13.249.42.221	192.168.0.15	TLSv1.2	1514	Server Hello
669	13:53:48.507720	13.249.42.221	192.168.0.15	TLSv1.2	953	Certificate, Certificate Status, Server Key Exchange,

Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 198
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 194
Version: TLS 1.2 (0x0303)
Random: 5cb7682cc63743b69089005fe6e79af11b4795ef28da0621...
Session ID Length: 0
Cipher Suites Length: 38
Cipher Suites (19 suites)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

0060 b9 00 00 26 c0 2c c0 2b c0 30 c0 2f c0 24 c0 23 ...&.,+ .0./.\$.*#

Server Hello Record:

1. Locate the ServerHello SSL record. Does this record specify a chosen cipher suite? What are the algorithms in the chosen cipher suite?

YTLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

The image shows a Wireshark capture of an SSL/TLS handshake. The packet list on the left shows several packets, with packet 664 (Server Hello) highlighted in red. The packet details pane on the right shows the structure of the Server Hello message, with the 'Cipher Suite' field highlighted in red. The packet bytes pane at the bottom shows the raw data of the packet.

Wireshark Lab 8_Yakubu Iddirisu.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssl

No.	Time	Source	Destination	Protocol	Length	Info
642	13:53:48.475484	204.79.197.200	192.168.0.15	TLSv1.2	109	Application Data
657	13:53:48.490305	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
658	13:53:48.490365	192.168.0.15	13.249.42.221	TLSv1.2	257	Client Hello
659	13:53:48.492678	204.79.197.200	192.168.0.15	TLSv1.2	175	Application Data
664	13:53:48.507245	13.249.42.221	192.168.0.15	TLSv1.2	1514	Server Hello
669	13:53:48.507720	13.249.42.221	192.168.0.15	TLSv1.2	953	Certificate, Certificate Status, Server Key Exchange,

Version: TLS 1.2 (0x0303)
Length: 78
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 74
Version: TLS 1.2 (0x0303)
Random: 2bf3b9664c927fffd11326833cedfb003313104061bfb787...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Compression Method: null (0)
Extensions Length: 34
Extension: server_name (len=0)
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=4)
Extension: session_ticket (len=0)

0000 f8 34 41 ac dc da 3c 37 86 08 ba da 08 00 45 00 ..4A...<7E.

Wireshark Lab 8_Yakubu Iddirisu.pcapng

Packets: 46047 - Displayed: 9967 (21.6%)

Profile: Default

Type here to search

5:54 PM 4/17/2019

HTTP OK PRINT.pdf - Adobe Acrobat Reader DC

File Edit View Window Help

Home Tools HTTP OK PRINT.pdf x

1 / 2 75%

Share

No. Time Source Destination Protocol Length Info

8 13:53:41.961211 2600:8806:6202:1000::b1c:fc89:2708:20b 2607:f80b:4000:802::2003 HTTP 288 GET /G/SGIAG3.cr1 HTTP/1.1

Frame 85: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0

Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

Internet Protocol Version 6, Src: 2600:8806:6202:1000::b1c:fc89:2708:20b, Dst: 2607:f80b:4000:802::2003

Transmission Control Protocol, Src Port: 55415, Dst Port: 80, Seq: 1, Ack: 1, Len: 206

Hypertext Transfer Protocol

No. Time Source Destination Protocol Length Info

271 13:53:42.229125 2607:f80b:4000:802::2003 2600:8806:6202:1000::b1c:fc89:2708:20b PKIX-CRL 635 Certificate Revocation List

Frame 272: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits) on interface 0

Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)

Internet Protocol Version 6, Src: 2607:f80b:4000:802::2003, Dst: 2600:8806:6202:1000::b1c:fc89:2708:20b

Transmission Control Protocol, Src Port: 80, Dst Port: 55415, Seq: 213501, Ack: 207, Len: 561

176 Reassembled TCP Segments (224061 bytes): #10(1220), #11(1220), #13(1220), #14(1220), #16(1220), #17(1220), #19(1220), #20(1220), #21(1220), #23(1220), #25(1220), #26(1220), #28(1220), #29(1220), #31(1220), #32(1220), #34(1220), #35(122)

Hypertext Transfer Protocol

Certificate Revocation List

No. Time Source Destination Protocol Length Info

7316 13:53:58.765262 192.168.0.15 72.21.91.29 HTTP 286 GET /

MFwIz9M9Sw5tA3BgldgMcGuaB8Q0G2galdtSeFnc6C000TnPrQ0Q0d4BhITiYdA4W0N8j10L0G2e1CEASfP0K3mPZeksvd5w5eYK3D HTTP/1.1

Frame 7316: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0

Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29

Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 1, Ack: 1, Len: 232

Hypertext Transfer Protocol

No. Time Source Destination Protocol Length Info

7866 13:53:58.843539 72.21.91.29 192.168.0.15 OCSP 842 Response

Frame 7866: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0

Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)

Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15

Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 1, Ack: 233, Len: 788

Hypertext Transfer Protocol

Online Certificate Status Protocol

No. Time Source Destination Protocol Length Info

5809 13:53:51.327670 192.168.0.15 72.21.91.29 HTTP 288 GET /

MFwIz9M9Sw5tA3BgldgMcGuaB8Q0G2galdtSeFnc6C000TnPrQ0Q0d4BhITiYdA4W0N8j10L0G2e1CEASfP0K3mPZeksvd5w5eYK3D HTTP/1.1

Frame 5809: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0

Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)

Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29

Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 233, Ack: 789, Len: 234

Hypertext Transfer Protocol

No. Time Source Destination Protocol Length Info

9992 13:53:51.348469 72.21.91.29 192.168.0.15 OCSP 842 Response

Frame 9992: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0

Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)

Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15

Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 789, Ack: 467, Len: 788

Hypertext Transfer Protocol

Online Certificate Status Protocol

No. Time Source Destination Protocol Length Info

Export PDF

Create PDF

Edit PDF

Comment

Combine Files

Organize Pages

Redact

Protect

Optimize PDF

Fill & Sign

Convert and edit PDFs with Acrobat Pro DC

Start Free Trial

Type here to search

6:04 PM 4/17/2019

No.	Time	Source	Destination	Protocol	Length	Info
8	13:53:41.961211	2600:8806:6202:1d00:b91c:fc89:27b8:2bb	2607:f8b0:4000:802::2003	HTTP	280	GET /GTSGIAG3.cr1 HTTP/1.1
Frame 8: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0						
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)						
Internet Protocol Version 6, Src: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb, Dst: 2607:f8b0:4000:802::2003						
Transmission Control Protocol, Src Port: 55415, Dst Port: 80, Seq: 1, Ack: 1, Len: 206						
Hypertext Transfer Protocol						
271	13:53:42.229125	2607:f8b0:4000:802::2003	2600:8806:6202:1d00:b91c:fc89:27b8:2bb	PKIX-CRL	635	Certificate Revocation List
Frame 271: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits) on interface 0						
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)						
Internet Protocol Version 6, Src: 2607:f8b0:4000:802::2003, Dst: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb						
Transmission Control Protocol, Src Port: 80, Dst Port: 55415, Seq: 213501, Ack: 207, Len: 561						
[176 Reassembled TCP Segments (214061 bytes): #10(1220), #11(1220), #13(1220), #14(1220), #16(1220), #17(1220), #19(1220), #20(1220), #22(1220), #23(1220), #25(1220), #26(1220), #28(1220), #29(1220), #31(1220), #32(1220), #34(1220), #35(1220)]						
Hypertext Transfer Protocol						
Certificate Revocation List						
7316	13:53:50.765262	192.168.0.15	72.21.91.29	HTTP	286	GET /
MFewTzBNMEsWSTAJBgUrDgMCGGUABBBQX626gAldtSefNc6DC00InqPHDQQU48hHIXYdUvK0eNRji0LOHG2eICEASfM0R3mPZeksxdD5wos4YX3D HTTP/1.1						
Frame 7316: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface 0						
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)						
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29						
Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 1, Ack: 1, Len: 232						
Hypertext Transfer Protocol						
7866	13:53:50.843539	72.21.91.29	192.168.0.15	OCSP	842	Response
Frame 7866: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0						
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)						
Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15						
Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 1, Ack: 233, Len: 788						
Hypertext Transfer Protocol						
Online Certificate Status Protocol						
9889	13:53:51.327670	192.168.0.15	72.21.91.29	HTTP	288	GET /
MFewTzBNMEsWSTAJBgUrDgMCGGUABBBQX626gAldtSefNc6DC00InqPHDQQU48hHIXYdUvK0eNRji0LOHG2eICEAKLqLtGqwfZAM8umB5oX2B9oX3D HTTP/1.1						
Frame 9889: 288 bytes on wire (2304 bits), 288 bytes captured (2304 bits) on interface 0						
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)						
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 72.21.91.29						
Transmission Control Protocol, Src Port: 55504, Dst Port: 80, Seq: 233, Ack: 789, Len: 234						
Hypertext Transfer Protocol						
9992	13:53:51.348469	72.21.91.29	192.168.0.15	OCSP	842	Response
Frame 9992: 842 bytes on wire (6736 bits), 842 bytes captured (6736 bits) on interface 0						
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)						
Internet Protocol Version 4, Src: 72.21.91.29, Dst: 192.168.0.15						
Transmission Control Protocol, Src Port: 80, Dst Port: 55504, Seq: 789, Ack: 467, Len: 788						
Hypertext Transfer Protocol						
Online Certificate Status Protocol						
13266	13:53:54.573386	192.168.0.15	151.101.194.167	HTTP	357	GET / HTTP/1.1
Frame 13266: 357 bytes on wire (2856 bits), 357 bytes captured (2856 bits) on interface 0						
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)						
Internet Protocol Version 4, Src: 192.168.0.15, Dst: 151.101.194.167						
Transmission Control Protocol, Src Port: 55550, Dst Port: 80, Seq: 1, Ack: 1, Len: 303						
Hypertext Transfer Protocol						
13268	13:53:54.587675	151.101.194.167	192.168.0.15	HTTP	333	HTTP/1.1 301 Moved Permanently
Frame 13268: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface 0						
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)						
Internet Protocol Version 4, Src: 151.101.194.167, Dst: 192.168.0.15						
Transmission Control Protocol, Src Port: 80, Dst Port: 55550, Seq: 1, Ack: 304, Len: 279						
Hypertext Transfer Protocol						
13298	13:53:54.685263	2600:8806:6202:1d00:b91c:fc89:27b8:2bb	2606:4700::6812:15e2	HTTP	315	GET /rootr1/
ME8wTTBLMEKwRzAJBgUrDgMCGGUABBS3V7W2nAf4FiMTjpDJKg6%2BMgGqMQUYHtmGkUNl8qJUC99BM00qP%2F8%2FUsCDk0kwjNvPLFRm7zMB3V80 HTTP/1.1						
Frame 13298: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits) on interface 0						
Ethernet II, Src: IntelCor_ac:dc:da (f8:34:41:ac:dc:da), Dst: Netgear_08:ba:da (3c:37:86:08:ba:da)						
Internet Protocol Version 6, Src: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb, Dst: 2606:4700::6812:15e2						
Transmission Control Protocol, Src Port: 55552, Dst Port: 80, Seq: 1, Ack: 1, Len: 241						
Hypertext Transfer Protocol						
13302	13:53:54.711825	2606:4700::6812:15e2	2600:8806:6202:1d00:b91c:fc89:27b8:2bb	OCSP	851	Response
Frame 13302: 851 bytes on wire (6808 bits), 851 bytes captured (6808 bits) on interface 0						
Ethernet II, Src: Netgear_08:ba:da (3c:37:86:08:ba:da), Dst: IntelCor_ac:dc:da (f8:34:41:ac:dc:da)						
Internet Protocol Version 6, Src: 2606:4700::6812:15e2, Dst: 2600:8806:6202:1d00:b91c:fc89:27b8:2bb						
Transmission Control Protocol, Src Port: 80, Dst Port: 55552, Seq: 1361, Ack: 242, Len: 777						
[2 Reassembled TCP Segments (2137 bytes): #13301(1360), #13302(777)]						
Hypertext Transfer Protocol						
Online Certificate Status Protocol						
42184	13:56:05.531537	192.168.0.15	52.218.224.179	HTTP	133	GET /quantcast.html HTTP/1.1