

LAP 8

Name: Mohammad Alhomidan

ID: 2510431

My IP 192.168.0.5

```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 2:

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

Ethernet adapter Bluetooth Network Connection:

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

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::99f1:4a6c:6bfa:4ada%12
    IPv4 Address. . . . . : 192.168.0.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

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

Tunnel adapter isatap.{05DA48C7-5141-437A-BCED-1F29AF2DE6D1}:

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

Tunnel adapter Local Area Connection* 12:

    Connection-specific DNS Suffix . :
    IPv6 Address. . . . . : 2001:0:5cf2:8c02:20f3:1bd6:3f57:fffa
    Link-local IPv6 Address . . . . . : fe80::20f3:1bd6:3f57:fffa%19
    Default Gateway . . . . . : ::

Tunnel adapter isatap.{6384ADFC-9F59-41B6-A461-1FCA8BD0BE49}:

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

Tunnel adapter isatap.{CE98C002-B144-42B7-8B3F-807EE0392342}:

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

EN 11:37 AM 4/17/2019

Client Hello Record:

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

TLSv1.0

The image shows a Wireshark packet capture of a network connection. The top pane displays a list of packets. Packet 12 is highlighted, showing a TLSv1.2 Client Hello frame. The bottom pane shows the details of this frame, including the TLS version (TLS 1.0) and the handshake protocol (Client Hello). The hex dump at the bottom shows the raw data of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
3	11:28:46.268848	172.217.1.131	192.168.0.5	UDP	60	443 → 59286 Len=17
4	11:28:46.281390	192.168.0.5	172.217.1.131	UDP	71	59286 → 443 Len=29
5	11:28:47.217381	192.168.0.5	74.125.30.188	TCP	55	65095 → 5228 [ACK] Seq=1 Ack=1 Win=16560 Len=1
6	11:28:47.262570	74.125.30.188	192.168.0.5	TCP	66	5228 → 65095 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
7	11:28:47.389344	192.168.0.5	171.161.207.100	TCP	66	65301 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8	11:28:47.394737	192.168.0.5	171.161.207.100	TCP	66	65302 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
9	11:28:47.409358	192.168.0.5	172.217.6.130	GQUIC	1392	Client Hello, PKN: 1, CID: 6364341275222990608
10	11:28:47.411904	171.161.207.100	192.168.0.5	TCP	62	443 → 65301 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1436 SACK_PERM=1
11	11:28:47.412018	192.168.0.5	171.161.207.100	TCP	54	65301 → 443 [ACK] Seq=1 Ack=1 Win=64620 Len=0
12	11:28:47.412843	192.168.0.5	171.161.207.100	TLSv1.2	571	Client Hello
13	11:28:47.424384	171.161.207.100	192.168.0.5	TCP	62	443 → 65302 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1436 SACK_PERM=1
14	11:28:47.424446	192.168.0.5	171.161.207.100	TCP	54	65302 → 443 [ACK] Seq=1 Ack=1 Win=64620 Len=0
15	11:28:47.425000	192.168.0.5	171.161.207.100	TLSv1.2	571	Client Hello
16	11:28:47.440450	171.161.207.100	192.168.0.5	TLSv1.2	1514	Server Hello

Frame 12: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0

Ethernet II, Src: HonHaiPr_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear_de:1d:73 (3c:37:86:de:1d:73)

Internet Protocol Version 4, Src: 192.168.0.5, Dst: 171.161.207.100

Transmission Control Protocol, Src Port: 65301, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

Secure Sockets Layer

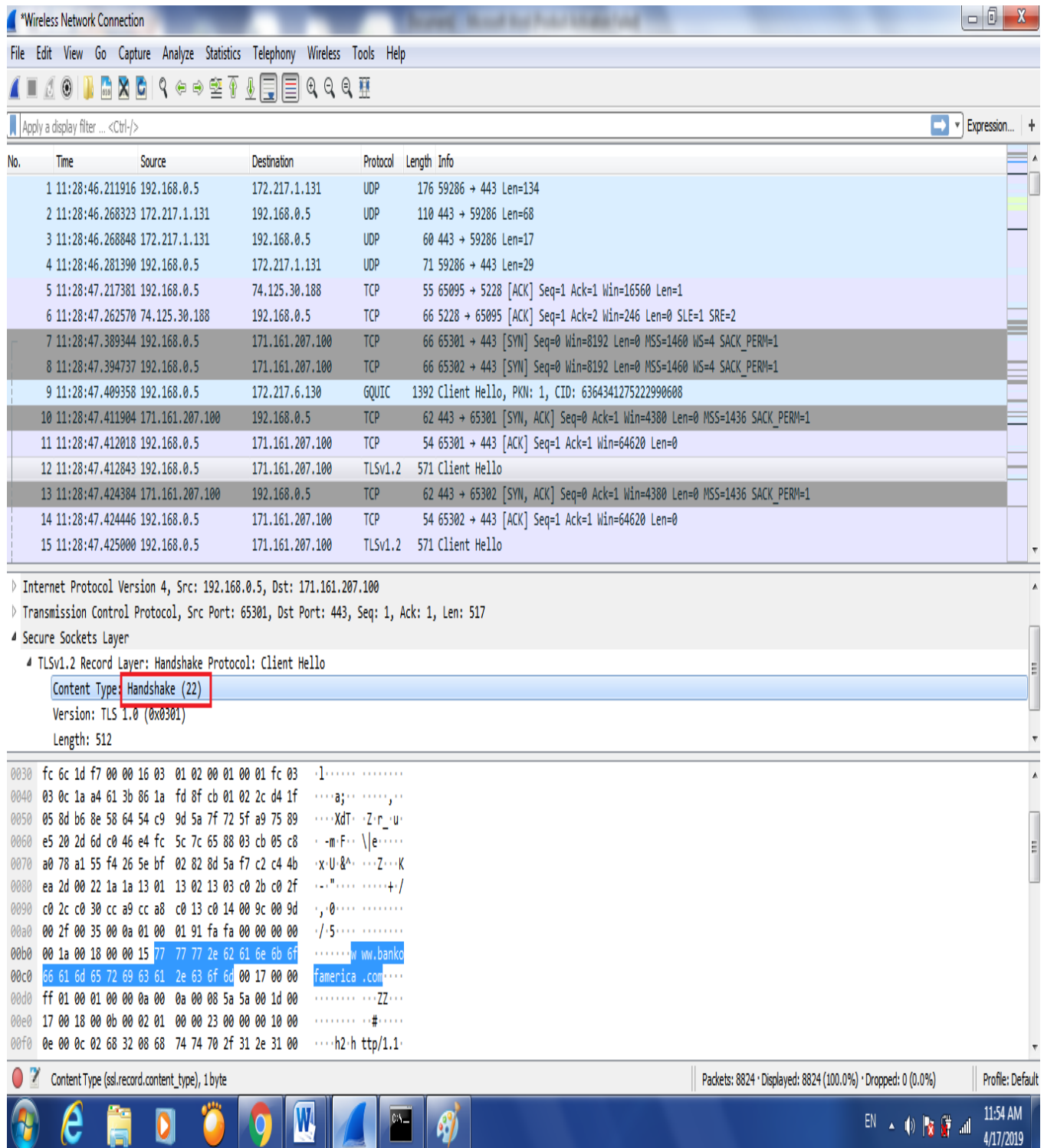
- TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: **TLS 1.0 (0x0301)**
 - Length: 512
 - Handshake Protocol: Client Hello

Hex dump:

```
0030 fc 6c 1d f7 00 00 16 03 01 02 00 01 00 01 fc 03 01.....
0040 03 0c 1a a4 61 3b 86 1a fd 8f cb 01 02 2c d4 1f .....a;.....
0050 05 8d b6 8e 58 64 54 c9 9d 5a 7f 72 5f a9 75 89 ....XdT..Z.r.u.
0060 e5 20 2d 6d c0 46 e4 fc 5c 7c 65 88 03 cb 05 c8 ..-m.F..\\e....
0070 a0 78 a1 55 f4 26 5e bf 02 82 8d 5a f7 c2 c4 4b ..x.U.&...Z...K
0080 ea 20 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f ..".....+./
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d .,0.....
00a0 00 2f 00 35 00 0a 01 00 01 91 fa fa 00 00 00 00 ./5.....
00b0 00 1a 00 18 00 00 15 77 77 77 2e 62 61 6e 6b 6f .....w ww.banko
```

- 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)



The image shows a Wireshark packet capture of a network trace. The top pane displays a list of 15 packets. Packet 9 is a GQUIC Client Hello, and packet 12 is a TLSv1.2 Client Hello. The bottom pane shows the expanded details of packet 12, which is a TLSv1.2 Record Layer: Handshake Protocol: Client Hello. The 'Content Type' field is highlighted with a red box and contains the value 'Handshake (22)'. The 'Version' field is 'TLS 1.0 (0x0301)' and the 'Length' is 512. The bottom pane also shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	11:28:46.211916	192.168.0.5	172.217.1.131	UDP	176	59286 → 443 Len=134
2	11:28:46.268323	172.217.1.131	192.168.0.5	UDP	110	443 → 59286 Len=68
3	11:28:46.268848	172.217.1.131	192.168.0.5	UDP	60	443 → 59286 Len=17
4	11:28:46.281390	192.168.0.5	172.217.1.131	UDP	71	59286 → 443 Len=29
5	11:28:47.217381	192.168.0.5	74.125.30.188	TCP	55	65095 → 5228 [ACK] Seq=1 Ack=1 Win=16560 Len=1
6	11:28:47.262570	74.125.30.188	192.168.0.5	TCP	66	5228 → 65095 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
7	11:28:47.389344	192.168.0.5	171.161.207.100	TCP	66	65301 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8	11:28:47.394737	192.168.0.5	171.161.207.100	TCP	66	65302 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
9	11:28:47.409358	192.168.0.5	172.217.6.130	GQUIC	1392	Client Hello, PKM: 1, CID: 6364341275222990608
10	11:28:47.411904	171.161.207.100	192.168.0.5	TCP	62	443 → 65301 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1436 SACK_PERM=1
11	11:28:47.412018	192.168.0.5	171.161.207.100	TCP	54	65301 → 443 [ACK] Seq=1 Ack=1 Win=64620 Len=0
12	11:28:47.412843	192.168.0.5	171.161.207.100	TLSv1.2	571	Client Hello
13	11:28:47.424384	171.161.207.100	192.168.0.5	TCP	62	443 → 65302 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1436 SACK_PERM=1
14	11:28:47.424446	192.168.0.5	171.161.207.100	TCP	54	65302 → 443 [ACK] Seq=1 Ack=1 Win=64620 Len=0
15	11:28:47.425000	192.168.0.5	171.161.207.100	TLSv1.2	571	Client Hello

Internet Protocol Version 4, Src: 192.168.0.5, Dst: 171.161.207.100

Transmission Control Protocol, Src Port: 65301, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

Secure Sockets Layer

TLSv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 512

0030 fc 6c 1d f7 00 00 16 03 01 02 00 01 00 01 fc 03 .1.....

0040 03 0c 1a a4 61 3b 86 1a fd 8f cb 01 02 2c d4 1fa;.....

0050 05 8d b6 8e 58 64 54 c9 9d 5a 7f 72 5f a9 75 89XdT..Z.r.u.

0060 e5 20 2d 6d c0 46 e4 fc 5c 7c 65 88 03 cb 05 c8 .-m-F..|e....

0070 a0 78 a1 55 f4 26 5e bf 02 82 8d 5a f7 c2 c4 4b .x.U.&^...Z...K

0080 ea 2d 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f ..".....+./

0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d .,0.....

00a0 00 2f 00 35 00 0a 01 00 01 91 fa 00 00 00 00 ./S.....

00b0 00 1a 00 18 00 00 15 77 77 77 2e 62 61 6e 6b 6fw ww.banko

00c0 66 61 6d 65 72 69 63 61 2e 63 6f 6d 00 17 00 00 famerica .com....

00d0 ff 01 00 01 00 00 0a 00 0a 00 08 5a 5a 00 1d 00:ZZ...

00e0 17 00 18 00 0b 00 02 01 00 00 23 00 00 10 00:##....

00f0 0e 00 0c 02 68 32 08 68 74 74 70 2f 31 2e 31 00h2-h ttp/1.1.

Content Type (ssl.record.content_type), 1 byte

Packets: 8824 • Displayed: 8824 (100.0%) • Dropped: 0 (0.0%)

Profile: Default

11:54 AM 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?

Yes it does 0c1aa4613b861afd8fcb01022cd41f.....

The image shows a Wireshark network packet capture of a TLS handshake. The packet list on the left shows 16 packets. Packet 9 is the ClientHello message from 192.168.0.5 to 171.161.207.100. The packet details pane on the right shows the structure of the ClientHello message:

- Version: TLS 1.0 (0x0301)
- Length: 512
- Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 508
 - Version: TLS 1.2 (0x0303)
 - Random: 0c1aa4613b861afd8fcb01022cd41f058db68e586454c99d...
 - Session ID Length: 32
 - Session ID: 2d6dc046e4fc5c7c658803cb05c8a078a155f4265ebf0282...
 - Cipher Suites Length: 34
 - Cipher Suites (17 suites)
 - Compression Methods Length: 1

The packet bytes pane at the bottom shows the raw data of the ClientHello message, with the random value highlighted in blue:

```
0040 03 0c 1a a4 61 3b 86 1a fd 8f cb 01 02 2c d4 1f .....a;.....
0050 05 0d b6 8e 58 64 54 c9 9d 5a 7f 72 5f a9 75 89 .....XdT..z.r.u.
0060 e5 20 2d 6d c0 46 e4 fc 5c 7c 65 88 03 cb 05 c8 -m.F..|e....
0070 a0 78 a1 55 f4 26 5e bf 02 82 8d 5a f7 c2 c4 4b .x.U&^...Z...K
0080 ea 2d 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f -. ".....+ /
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d .,0.....
00a0 00 2f 00 35 00 0a 01 00 01 91 fa 00 00 00 00 ./5.....
00b0 00 1a 00 18 00 00 15 77 77 77 2e 62 61 6e 6b 6f .....w ww.banko
00c0 66 61 6d 65 72 69 63 61 2e 63 6f 6d 00 17 00 00 famerica .com....
```

The status bar at the bottom indicates that the random values used for deriving keys are from the handshake.random field, 32 bytes long. The interface also shows the number of packets displayed (8824) and the current time (2:33 PM on 4/17/2019).

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

public-key algorithm **AES** symmetric-key algorithm **GCM** hash algorithm **SHA256**

The image shows a Wireshark capture of a network packet, specifically a TLS ClientHello message. The packet list at the top shows the ClientHello at offset 11:28:47.409358. The packet details pane shows the ClientHello structure, including the Random, Session ID, Cipher Suites, and the first cipher suite, TLS_AES_128_GCM_SHA256. The packet bytes pane shows the raw data of the ClientHello message.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
3	11:28:46.268848	172.217.1.131	192.168.0.5	UDP	60	443 → 59286 Len=17
4	11:28:46.281390	192.168.0.5	172.217.1.131	UDP	71	59286 → 443 Len=29
5	11:28:47.217381	192.168.0.5	74.125.30.188	TCP	55	65095 → 5228 [ACK] Seq=1 Ack=1 Win=16560 Len=1
6	11:28:47.262570	74.125.30.188	192.168.0.5	TCP	66	5228 → 65095 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
7	11:28:47.389344	192.168.0.5	171.161.207.100	TCP	66	65301 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8	11:28:47.394737	192.168.0.5	171.161.207.100	TCP	66	65302 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
9	11:28:47.409358	192.168.0.5	172.217.6.130	GQUIC	1392	Client Hello, PKN: 1, CID: 636434127522990608
10	11:28:47.411904	171.161.207.100	192.168.0.5	TCP	62	443 → 65301 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1436 SACK_PERM=1
11	11:28:47.412018	192.168.0.5	171.161.207.100	TCP	54	65301 → 443 [ACK] Seq=1 Ack=1 Win=64620 Len=0
12	11:28:47.412843	192.168.0.5	171.161.207.100	TLSv1.2	571	Client Hello
13	11:28:47.424384	171.161.207.100	192.168.0.5	TCP	62	443 → 65302 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1436 SACK_PERM=1
14	11:28:47.424446	192.168.0.5	171.161.207.100	TCP	54	65302 → 443 [ACK] Seq=1 Ack=1 Win=64620 Len=0
15	11:28:47.425000	192.168.0.5	171.161.207.100	TLSv1.2	571	Client Hello
16	11:28:47.440450	171.161.207.100	192.168.0.5	TLSv1.2	1514	Server Hello

Packet Details:

- Random: 0c1aa4613b861afd8fcb01022cd41f058db68e586454c99d...
- Session ID Length: 32
- Session ID: 2d6dc046e4fc5c7c658803cb05c8a078a155f4265ebf0282...
- Cipher Suites Length: 34
- Cipher Suites (17 suites)
 - Cipher Suite: Reserved (GREASE) (0x1a1a)
 - Cipher Suite: **TLS_AES_128_GCM_SHA256 (0x1301)**
 - Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
 - Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Packet Bytes:

```
0080 ea 2d 00 22 1a 1a 13 01 13 02 13 03 c0 2b c0 2f ...".+/-
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d ,.0.....
00a0 00 2f 00 35 00 0a 01 00 01 91 fa fa 00 00 00 00 ./5.....
00b0 00 1a 00 18 00 00 15 77 77 77 2e 62 61 6e 6b 6f .....w ww.banko
00c0 66 61 6d 65 72 69 63 61 2e 63 6f 6d 00 17 00 00 famerica .com...
00d0 ff 01 00 01 00 00 0a 00 0a 00 08 5a 5a 00 1d 00 .....ZZZ...
00e0 17 00 18 00 0b 00 02 01 00 00 23 00 00 10 00 .....#.....
00f0 0e 00 0c 02 68 32 08 68 74 74 70 2f 31 2e 31 00 ...h2:h ttp/1.1.
0100 05 00 05 01 00 00 00 00 00 0d 00 14 00 12 04 03 .....

```

Packet Info: Cipher Suite (ssl.handshake.ciphersuite), 2 bytes | Packets: 8824 · Displayed: 8824 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

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

Public-key algorithm **RSA with AES** symmetric-key algorithm **GCM** hash algorithm **SHA256**

Version: TLS 1.2 (0x0303)
Length: 85
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 81
Version: TLS 1.2 (0x0303)
Random: 5857fc045b75adbc71b34dd21fbf124202752b32eb29dbc...
Session ID Length: 32
Session ID: 873a517daa0e15710e22f693b1765d1e94d119e5b07ddfe5...
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Compression Method: null (0)
Extensions Length: 9

0000 ed 68 00 9c 00 00 ff 01 00 01 00 00 17 00 00 ·h·····
0001 16 03 03 10 f7 0b 00 10 f3 00 10 f0 00 07 74 30 ······t0
0002 82 07 70 30 82 06 58 a0 03 02 01 02 02 10 13 ea ·p0·X·
0003 6c ee a7 f5 1b 7f 00 00 00 00 54 ce 92 cf 30 0d 1·····T·0
0004 06 09 2a 86 48 06 f7 0d 01 01 0b 05 00 30 81 ba ·*·H·····0
0005 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 16 30 1·0···U· ···US1·0
0006 14 06 03 55 04 0a 13 0d 45 6e 74 72 75 73 74 2c ···U····Entrust,
0007 20 49 6e 63 2e 31 28 30 26 06 03 55 04 0b 13 1f Inc.1(0 &··U··
0008 53 65 65 20 77 77 77 2e 65 6e 74 72 75 73 74 2e See www. entrust.

Cipher Suite (ssl.handshake.ciphersuite), 2 bytes

C:\Users\user\AppData\Local\Temp\wireshark_6D8C6C4E-7F69-4A94-83C7-1D7587D59643_20190417112845_a04704.pcapng 8824 total packets, 30 shown

No. Time Source Destination Protocol Length Info 4397 11:29:33.302104 192.168.0.5 192.168.0.1 HTTP 191 HTTP/1.1 200 OK Frame 4397: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0 Ethernet II, Src: HonHaiPr_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear_de:1d:73 (3c:37:86:de:1d:73) Internet Protocol Version 4, Src: 192.168.0.5, Dst: 192.168.0.1 Transmission Control Protocol, Src Port: 2869, Dst Port: 1082, Seq: 1, Ack: 597, Len: 125 Hypertext Transfer Protocol

C:\Users\user\AppData\Local\Temp\wireshark_6D8C6C4E-7F69-4A94-83C7-1D7587D59643_20190417112845_a04704.pcapng 8824 total packets, 8824 shown

No. Time Source Destination Protocol Length Info 12 11:28:47.412843 192.168.0.5 171.161.207.100 TLSv1.2 571 Client Hello Frame 12: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0 Ethernet II, Src: HonHaiPr_26:b5:f1 (38:59:f9:26:b5:f1), Dst: Netgear_de:1d:73 (3c:37:86:de:1d:73) Internet Protocol Version 4, Src: 192.168.0.5, Dst: 171.161.207.100 Transmission Control Protocol, Src Port: 65301, Dst Port: 443, Seq: 1, Ack: 1, Len: 517 Secure Sockets Layer TLSv1.2 Record Layer: Handshake Protocol: Client Hello Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 512 Handshake Protocol: Client Hello Handshake Type: Client Hello (1) Length: 508 Version: TLS 1.2 (0x0303) Random: 0c1aa4613b861afd8fcb01022cd41f058db68e586454c99d... Session ID Length: 32 Session ID: 2d6dc046e4fc5c7c658803cb05c8a078a155f4265ebf0282... Cipher Suites Length: 34 Cipher Suites (17 suites) Cipher Suite: Reserved (GREASE) (0x1a1a) Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a) Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc038) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a) Compression Methods Length: 1 Compression Methods (1 method) Extensions Length: 401 Extension: Reserved (GREASE) (len=0) Extension: server_name (len=26) Extension: extended_master_secret (len=0) Extension: renegotiation_info (len=1) Extension: supported_groups (len=10) Extension: ec_point_formats (len=2) Extension: SessionTicket TLS (len=0) Extension: application_layer_protocol_negotiation (len=14) Extension: status_request (len=5) Extension: signature_algorithms (len=20) Extension: signed_certificate_timestamp (len=0) Extension: key_share (len=43) Extension: psk_key_exchange_modes (len=2) Extension: supported_versions (len=11) Extension: Unknown type 27 (len=3) Extension: Reserved (GREASE) (len=1) Extension: padding (len=195)