Name-Gavade Vishal Ramnath

Roll.No-70

Batch-T3

Class-TY

Scan Report SSL

```
┌──(kali㉿kali)-[~]
└─$ sslscan www.ethicalhackingblog.com
Version: 2.1.3-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 142.250.199.147

Testing SSL server www.ethicalhackingblog.com on port 443 using SNI name
www.ethicalhackingblog.com

  SSL/TLS Protocols:
SSLv2    disabled
SSLv3    disabled
TLSv1.0  enabled
TLSv1.1  enabled
TLSv1.2  enabled
TLSv1.3  enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
```

```
TLSv1.2 not vulnerable to heartbleed

TLSv1.1 not vulnerable to heartbleed

TLSv1.0 not vulnerable to heartbleed


  Supported Server Cipher(s):

Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Preferred TLSv1.2  256 bits  ECDHE-RSA-CHACHA20-POLY1305  Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256  Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384  Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA  Curve 25519 DHE 253
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA  Curve 25519 DHE 253
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Preferred TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA  Curve 25519 DHE 253
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA  Curve 25519 DHE 253
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Preferred TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA  Curve 25519 DHE 253
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA  Curve 25519 DHE 253
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
```

```
  Server Key Exchange Group(s):
TLSv1.3  128 bits  secp256r1 (NIST P-256)
```

```
TLSv1.3  128 bits  x25519

TLSv1.2  128 bits  secp256r1 (NIST P-256)

TLSv1.2  128 bits  x25519


  SSL Certificate:

Signature Algorithm: sha256WithRSAEncryption

RSA Key Strength:  2048


Subject:  www.ethicalhackingblog.com

Altnames: DNS:www.ethicalhackingblog.com

Issuer:  GTS CA 1D4


Not valid before: Mar 17 07:47:03 2024 GMT

Not valid after:  Jun 15 08:35:54 2024 GMT
```

### Analysis Report SSL Protocol ###

```
exam@exam-Veriton-M200-H310:~$ sudo apt-get install ssldump
[sudo] password for exam:
Reading package lists... Done
Building dependency tree
Reading state information... Done
ssldump is already the newest version (1.1-1).
0 upgraded, 0 newly installed, 0 to remove and 121 not upgraded.
exam@exam-Veriton-M200-H310:~$ ssldump -h
Usage: ssldump [-r dumpfile] [-i interface] [-l sslkeylogfile]
               [-k keyfile] [-p password] [-vtaTnsAxVNde]
               [filter]
exam@exam-Veriton-M200-H310:~$ ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.41.212 netmask 255.255.224.0 broadcast 192.168.63.255
        inet6 fe80::cb09:116c:ebd6:aeb6 prefixlen 64  scopeid 0x20<link>
        ether 94:c6:91:3a:4f:30  txqueuelen 1000  (Ethernet)
        RX packets 334727 bytes 109042827 (109.0 MB)
        RX errors 0  dropped 906  overruns 0  frame 0
        TX packets 16308  bytes 1742054 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1821  bytes 186094 (186.0 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1821  bytes 186094 (186.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

exam@exam-Veriton-M200-H310:~$ sudo ssldump -i enp1s0 port 443
New TCP connection #1: exam-Veriton-M200-H310(51800) <-> 104.18.37.251(443)
1 1  0.0189 (0.0189)  C>S  Handshake
      ClientHello
        Version 3.3
        resume [32]=
          fd f8 33 b5 49 5a 81 84 e0 91 d4 1e 17 d5 32 14
          52 2b 7f e2 02 19 3d 41 d9 bf d3 aa 83 79 88 39
        cipher suites
        TLS_AES_256_GCM_SHA384
        TLS_CHACHA20_POLY1305_SHA256
        TLS_AES_128_GCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_EMPTY_RENEGOTIATION_INFO_SCSV
        compression methods
                  NULL
        extensions
          server_name
              host_name: plugins.nessus.org
          encrypt_then_mac
          extended_master_secret
          signature_algorithms
1 2  0.0389 (0.0199)  S>C  Handshake
      ServerHello
        Version 3.3
        session_id[32]=
          fd f8 33 b5 49 5a 81 84 e0 91 d4 1e 17 d5 32 14
          52 2b 7f e2 02 19 3d 41 d9 bf d3 aa 83 79 88 39
        cipherSuite         TLS_AES_256_GCM_SHA384
        compressionMethod                   NULL
        extensions
1 3  0.0389 (0.0000)  S>C  ChangeCipherSpec
```

```
1 4  0.0389 (0.0000)  S>C  application_data
1 5  0.0428 (0.0038)  C>S  ChangeCipherSpec
1 6  0.0428 (0.0000)  C>S  application_data
1 7  0.0988 (0.0559)  C>S  application_data
1 8  0.3393 (0.2405)  S>C  application_data
1 9  0.3393 (0.0000)  S>C  application_data
1 10 0.3393 (0.0000)  S>C  application_data
1 11 0.3393 (0.0000)  S>C  application_data
1    0.3393 (0.0000)  S>C  TCP FIN
1    0.3403 (0.0009)  C>S  TCP RST
New TCP connection #2: exam-Veriton-M200-H310(40904) <-> 151.101.194.49(443)
2 1  0.1493 (0.1493)  C>S  Handshake
      ClientHello
        Version 3.3
        cipher suites
        TLS_AES_256_GCM_SHA384
        TLS_CHACHA20_POLY1305_SHA256
        TLS_AES_128_GCM_SHA256
        TLS_AES_128_CCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_CCM
        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_128_CCM
        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_GCM_SHA384
        TLS_RSA_WITH_AES_256_CCM
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_AES_128_GCM_SHA256
        TLS_RSA_WITH_AES_128_CCM
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_DHE_RSA_WITH_AES_256_CCM
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_DHE_RSA_WITH_AES_128_CCM
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        compression methods
                  NULL
        extensions
          status_request
          signature_algorithms
          application_layer_protocol_negotiation
          encrypt_then_mac
          extended_master_secret
          server_name
            host_name: cdn.fwupd.org
2 2  0.1737 (0.0244)  S>C  Handshake
      ServerHello
        Version 3.3
        session_id[32]=
          b0 2f 40 54 39 1d 05 1d 4d ff 5f 23 e0 8a 61 af
          44 e5 56 8f 9a 36 5a 42 d0 48 fd 8a 0a 6d 8a ff
        cipherSuite         TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        compressionMethod                   NULL
        extensions
          server_name
          extended_master_secret
          application_layer_protocol_negotiation
          status_request
2 3  0.1737 (0.0000)  S>C  Handshake
      Certificate
2 4  0.1737 (0.0000)  S>C  Handshake
2 5  0.1737 (0.0000)  S>C  Handshake
      ServerKeyExchange
2 6  0.1737 (0.0000)  S>C  Handshake
      ServerHelloDone
2 7  0.1743 (0.0005)  C>S  Handshake
      ClientKeyExchange
2 8  0.1743 (0.0000)  C>S  ChangeCipherSpec
2 9  0.1743 (0.0000)  C>S  Handshake
2 10 0.1961 (0.0217)  S>C  ChangeCipherSpec
2 11 0.1961 (0.0000)  S>C  Handshake
2 12 0.1973 (0.0011)  C>S  application_data
2 13 0.1973 (0.0000)  C>S  application_data
2 14 0.1973 (0.0000)  C>S  application_data
2 15 0.1973 (0.0000)  C>S  application_data
2 16 0.2196 (0.0222)  S>C  application_data
2 17 0.2197 (0.0001)  C>S  application_data
2 18 0.2201 (0.0004)  S>C  application_data
2 19 0.2202 (0.0000)  S>C  application_data
2 20 0.2214 (0.0012)  C>S  Alert
2    0.2251 (0.0036)  C>S  TCP FIN
New TCP connection #3: exam-Veriton-M200-H310(40918) <-> 151.101.194.49(443)
2 21 0.2464 (0.0212)  S>C  Alert
2    0.2466 (0.0001)  S>C  TCP FIN
3 1  0.0380 (0.0380)  C>S  Handshake
      ClientHello
        Version 3.3
        cipher suites
        TLS_AES_256_GCM_SHA384
        TLS_CHACHA20_POLY1305_SHA256
        TLS_AES_128_GCM_SHA256
```

```
        TLS_AES_128_CCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_CCM
        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_128_CCM
        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_GCM_SHA384
        TLS_RSA_WITH_AES_256_CCM
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_AES_128_GCM_SHA256
        TLS_RSA_WITH_AES_128_CCM
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_DHE_RSA_WITH_AES_256_CCM
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_DHE_RSA_WITH_AES_128_CCM
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        compression methods
                  NULL
        extensions
          status_request
          signature_algorithms
          application_layer_protocol_negotiation
          encrypt_then_mac
          extended_master_secret
          server_name
              host_name: cdn.fwupd.org
3 2  0.0545 (0.0164)  S>C  Handshake
      ServerHello
        Version 3.3
        session_id[32]=
          80 8f 26 6a 9d f3 e2 a9 22 90 3a 3c a1 7e f7 68
          18 58 2d e9 45 46 12 e1 17 cd 45 c1 b9 de ee 24
        cipherSuite         TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        compressionMethod                   NULL
        extensions
          server_name
          extended_master_secret
          application_layer_protocol_negotiation
          status_request
3 3  0.0546 (0.0000)  S>C  Handshake
```

```
      Certificate
3 4  0.0546 (0.0000)  S>C  Handshake
3 5  0.0546 (0.0000)  S>C  Handshake
      ServerKeyExchange
3 6  0.0546 (0.0000)  S>C  Handshake
      ServerHelloDone
3 7  0.0564 (0.0017)  C>S  Handshake
      ClientKeyExchange
3 8  0.0564 (0.0000)  C>S  ChangeCipherSpec
3 9  0.0564 (0.0000)  C>S  Handshake
3 10 0.0711 (0.0147)  S>C  ChangeCipherSpec
3 11 0.0711 (0.0000)  S>C  Handshake
3 12 0.0745 (0.0033)  C>S  application_data
3 13 0.0745 (0.0000)  C>S  application_data
3 14 0.0745 (0.0000)  C>S  application_data
3 15 0.0746 (0.0000)  C>S  application_data
3 16 0.0885 (0.0139)  S>C  application_data
3 17 0.0886 (0.0000)  S>C  application_data
3 18 0.0887 (0.0001)  C>S  application_data
3 19 0.0891 (0.0003)  S>C  application_data
3 20 0.0893 (0.0002)  S>C  application_data
3 21 0.0894 (0.0000)  S>C  application_data
3 22 0.0901 (0.0006)  S>C  application_data
3 23 0.0901 (0.0000)  S>C  application_data
3 24 0.0910 (0.0008)  S>C  application_data
3 25 0.0910 (0.0000)  S>C  application_data
3 26 0.0919 (0.0008)  S>C  application_data
3 27 0.0919 (0.0000)  S>C  application_data
3 28 0.0928 (0.0008)  S>C  application_data
3 29 0.0928 (0.0000)  S>C  application_data
3 30 0.0936 (0.0008)  S>C  application_data
3 31 0.0937 (0.0000)  S>C  application_data
3 32 0.0945 (0.0008)  S>C  application_data
3 33 0.0945 (0.0000)  S>C  application_data
3 34 0.0954 (0.0008)  S>C  application_data
3 35 0.0954 (0.0000)  S>C  application_data
3 36 0.0963 (0.0008)  S>C  application_data
3 37 0.0963 (0.0000)  S>C  application_data
3 38 0.0971 (0.0008)  S>C  application_data
3 39 0.0972 (0.0000)  S>C  application_data
3 40 0.0981 (0.0008)  S>C  application_data
3 41 0.0981 (0.0000)  S>C  application_data
3 42 0.0989 (0.0008)  S>C  application_data
3 43 0.0990 (0.0000)  S>C  application_data
3 44 0.0998 (0.0008)  S>C  application_data
3 45 0.0999 (0.0000)  S>C  application_data
3 46 0.1007 (0.0008)  S>C  application_data
3 47 0.1008 (0.0000)  S>C  application_data
3 48 0.1016 (0.0008)  S>C  application_data
3 49 0.1017 (0.0000)  S>C  application_data
```

```
3 50 0.1025 (0.0007)  S>C  application_data
3 51 0.1025 (0.0000)  S>C  application_data
3 52 0.1025 (0.0000)  S>C  application_data
3 53 0.1032 (0.0007)  S>C  application_data
3 54 0.1033 (0.0000)  S>C  application_data
3 55 0.1042 (0.0008)  S>C  application_data
3 56 0.1042 (0.0000)  S>C  application_data
3 57 0.1050 (0.0008)  S>C  application_data
3 58 0.1050 (0.0000)  S>C  application_data
3 59 0.1059 (0.0008)  S>C  application_data
3 60 0.1060 (0.0000)  S>C  application_data
3 61 0.1068 (0.0008)  S>C  application_data
3 62 0.1068 (0.0000)  S>C  application_data
3 63 0.1077 (0.0008)  S>C  application_data
3 64 0.1077 (0.0000)  S>C  application_data
3 65 0.1086 (0.0008)  S>C  application_data
3 66 0.1086 (0.0000)  S>C  application_data
3 67 0.1086 (0.0000)  S>C  application_data
3 68 0.1138 (0.0051)  S>C  application_data
3 69 0.1173 (0.0034)  S>C  application_data
3 70 0.1192 (0.0019)  S>C  application_data
3 71 0.1210 (0.0017)  S>C  application_data
3 72 0.1210 (0.0000)  S>C  application_data
3 73 0.1233 (0.0022)  S>C  application_data
3 74 0.1242 (0.0009)  S>C  application_data
3 75 0.1266 (0.0023)  S>C  application_data
3 76 0.1284 (0.0018)  S>C  application_data
3 77 0.1284 (0.0000)  S>C  application_data
3 78 0.1300 (0.0016)  S>C  application_data
3 79 0.1317 (0.0017)  S>C  application_data
3 80 0.1335 (0.0017)  S>C  application_data
3 81 0.1339 (0.0004)  S>C  application_data
3 82 0.1339 (0.0000)  S>C  application_data
3 83 0.1358 (0.0018)  S>C  application_data
3 84 0.1358 (0.0000)  S>C  application_data
3 85 0.1367 (0.0008)  S>C  application_data
3 86 0.1382 (0.0015)  S>C  application_data
3 87 0.1391 (0.0008)  S>C  application_data
3 88 0.1403 (0.0012)  S>C  application_data
3 89 0.1403 (0.0000)  S>C  application_data
3 90 0.1412 (0.0009)  S>C  application_data
3 91 0.1420 (0.0007)  S>C  application_data
3 92 0.1429 (0.0008)  S>C  application_data
3 93 0.1430 (0.0001)  S>C  application_data
3 94 0.1430 (0.0000)  S>C  application_data
3 95 0.1439 (0.0008)  S>C  application_data
3 96 0.1449 (0.0009)  S>C  application_data
3 97 0.1459 (0.0010)  S>C  application_data
3 98 0.1460 (0.0001)  S>C  application_data
3 99 0.1460 (0.0000)  S>C  application_data
```

```
3 100 0.1470 (0.0009)  S>C  application_data
3 101 0.1490 (0.0020)  S>C  application_data
3 102 0.1492 (0.0001)  S>C  application_data
3 103 0.1511 (0.0019)  S>C  application_data
3 104 0.1511 (0.0000)  S>C  application_data
3 105 0.1516 (0.0005)  S>C  application_data
3 106 0.1516 (0.0000)  S>C  application_data
3 107 0.1534 (0.0017)  S>C  application_data
3 108 0.1548 (0.0014)  S>C  application_data
3 109 0.1549 (0.0001)  S>C  application_data
3 110 0.1555 (0.0006)  S>C  application_data
3 111 0.1555 (0.0000)  S>C  application_data
3 112 0.1571 (0.0015)  S>C  application_data
3 113 0.1573 (0.0002)  S>C  application_data
3 114 0.1584 (0.0010)  S>C  application_data
3 115 0.1585 (0.0001)  S>C  application_data
3 116 0.1585 (0.0000)  S>C  application_data
3 117 0.1601 (0.0015)  S>C  application_data
3 118 0.1603 (0.0001)  S>C  application_data
3 119 0.1613 (0.0010)  S>C  application_data
3 120 0.1615 (0.0001)  S>C  application_data
3 121 0.1615 (0.0000)  S>C  application_data
3 122 0.1652 (0.0037)  S>C  application_data
3 123 0.1655 (0.0002)  S>C  application_data
3 124 0.1658 (0.0003)  S>C  application_data
3 125 0.1659 (0.0001)  S>C  application_data
3 126 0.1659 (0.0000)  S>C  application_data
3 127 0.1689 (0.0029)  S>C  application_data
3 128 0.1689 (0.0000)  S>C  application_data
3 129 0.1700 (0.0010)  S>C  application_data
3 130 0.1701 (0.0001)  S>C  application_data
3 131 0.1702 (0.0001)  S>C  application_data
3 132 0.1728 (0.0025)  S>C  application_data
3 133 0.1728 (0.0000)  S>C  application_data
3 134 0.1729 (0.0001)  S>C  application_data
3 135 0.1729 (0.0000)  S>C  application_data
3 136 0.1734 (0.0004)  C>S  Alert
3    0.1747 (0.0012)  C>S  TCP FIN
3 137 0.1889 (0.0141)  S>C  Alert
3    0.1889 (0.0000)  S>C  TCP FIN
New TCP connection #4: exam-Veriton-M200-H310(47592) <-> server-18-239-111-
12.bom54.r.cloudfront.net(443)
4 1  0.0277 (0.0277)  C>S  Handshake
      ClientHello
        Version 3.3
        cipher suites
        TLS_AES_256_GCM_SHA384
        TLS_CHACHA20_POLY1305_SHA256
        TLS_AES_128_GCM_SHA256
        TLS_AES_128_CCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_256_CCM
        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
        TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_ECDSA_WITH_AES_128_CCM
        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
        TLS_RSA_WITH_AES_256_GCM_SHA384
        TLS_RSA_WITH_AES_256_CCM
        TLS_RSA_WITH_AES_256_CBC_SHA
        TLS_RSA_WITH_AES_128_GCM_SHA256
        TLS_RSA_WITH_AES_128_CCM
        TLS_RSA_WITH_AES_128_CBC_SHA
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        TLS_DHE_RSA_WITH_AES_256_CCM
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
        TLS_DHE_RSA_WITH_AES_128_CCM
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA
        compression methods
                  NULL
        extensions
          status_request
          signature_algorithms
          encrypt_then_mac
          extended_master_secret
          server_name
              host_name: repo.mongodb.org
4 2  0.0514 (0.0237)  S>C  Handshake
      ServerHello
        Version 3.3
        session_id[0]=

        cipherSuite         TLS_AES_128_GCM_SHA256
        compressionMethod                   NULL
        extensions
4 3  0.0514 (0.0000)  S>C  ChangeCipherSpec
4 4  0.0514 (0.0000)  S>C  application_data
4 5  0.0516 (0.0001)  C>S  ChangeCipherSpec
4 6  0.0525 (0.0008)  S>C  application_data
4 7  0.0525 (0.0000)  S>C  application_data
4 8  0.0525 (0.0000)  S>C  application_data
New TCP connection #5: exam-Veriton-M200-H310(37956) <-> server-108-158-61-
79.bom78.r.cloudfront.net(443)
```

```
4 9  0.0742 (0.0216)  C>S  application_data
4 10 0.0742 (0.0000)  C>S  application_data
5 1  0.0201 (0.0201)  C>S  Handshake
   ClientHello
    Version 3.3
    cipher suites
    TLS_AES_256_GCM_SHA384
    TLS_CHACHA20_POLY1305_SHA256
    TLS_AES_128_GCM_SHA256
    TLS_AES_128_CCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_CCM
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_128_CCM
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    TLS_RSA_WITH_AES_256_GCM_SHA384
    TLS_RSA_WITH_AES_256_CCM
    TLS_RSA_WITH_AES_256_CBC_SHA
    TLS_RSA_WITH_AES_128_GCM_SHA256
    TLS_RSA_WITH_AES_128_CCM
    TLS_RSA_WITH_AES_128_CBC_SHA
    TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_DHE_RSA_WITH_AES_256_CCM
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_DHE_RSA_WITH_AES_128_CCM
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    compression methods
         NULL
    extensions
     status_request
     signature_algorithms
     encrypt_then_mac
     extended_master_secret
     server_name
       host_name: cloud.r-project.org
New TCP connection #6: exam-Veriton-M200-H310(59598) <-> bom12s20-in-f14.1e100.net(443)
5 2  0.0345 (0.0143)  S>C  Handshake
   ServerHello
    Version 3.3
    session_id[0]=
    cipherSuite         TLS_AES_128_GCM_SHA256
    compressionMethod                   NULL
    extensions
5 3  0.0345 (0.0000)  S>C  ChangeCipherSpec
5 4  0.0345 (0.0000)  S>C  application_data
5 5  0.0347 (0.0002)  C>S  ChangeCipherSpec
5 6  0.0355 (0.0008)  S>C  application_data
5 7  0.0355 (0.0000)  S>C  application_data
5 8  0.0355 (0.0000)  S>C  application_data
6 1  0.0231 (0.0231)  C>S  Handshake
   ClientHello
    Version 3.3
    cipher suites
    TLS_AES_256_GCM_SHA384
    TLS_CHACHA20_POLY1305_SHA256
    TLS_AES_128_GCM_SHA256
    TLS_AES_128_CCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_CCM
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_128_CCM
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    TLS_RSA_WITH_AES_256_GCM_SHA384
    TLS_RSA_WITH_AES_256_CCM
    TLS_RSA_WITH_AES_256_CBC_SHA
    TLS_RSA_WITH_AES_128_GCM_SHA256
    TLS_RSA_WITH_AES_128_CCM
    TLS_RSA_WITH_AES_128_CBC_SHA
    TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_DHE_RSA_WITH_AES_256_CCM
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_DHE_RSA_WITH_AES_128_CCM
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    compression methods
          NULL
    extensions
     status_request
     signature_algorithms
     encrypt_then_mac
     extended_master_secret
```

```
            server_name
                host_name: dl.google.com
   4 11 0.0969 (0.0227)  S>C  application_data
   4 12 0.0987 (0.0017)  S>C  application_data
   4 13 0.0994 (0.0006)  C>S  application_data
5    9  0.0485 (0.0129)  C>S  application_data
   5 10 0.0485 (0.0000)  C>S  application_data
   5 11 0.0624 (0.0139)  S>C  application_data
   5 12 0.0633 (0.0009)  S>C  application_data
   New TCP connection #7: exam-Veriton-M200-H310(38000) <-> 13.107.213.72(443)
   7 1  0.0276 (0.0276)  C>S  Handshake
         ClientHello
           Version 3.3
           cipher suites
           TLS_AES_256_GCM_SHA384
           TLS_CHACHA20_POLY1305_SHA256
           TLS_AES_128_GCM_SHA256
           TLS_AES_128_CCM_SHA256
           TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
           TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
           TLS_ECDHE_ECDSA_WITH_AES_256_CCM
           TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
           TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
           TLS_ECDHE_ECDSA_WITH_AES_128_CCM
           TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
           TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
           TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
           TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
           TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
           TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
           TLS_RSA_WITH_AES_256_GCM_SHA384
           TLS_RSA_WITH_AES_256_CCM
           TLS_RSA_WITH_AES_256_CBC_SHA
           TLS_RSA_WITH_AES_128_GCM_SHA256
           TLS_RSA_WITH_AES_128_CCM
           TLS_RSA_WITH_AES_128_CBC_SHA
           TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
           TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
           TLS_DHE_RSA_WITH_AES_256_CCM
           TLS_DHE_RSA_WITH_AES_256_CBC_SHA
           TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
           TLS_DHE_RSA_WITH_AES_128_CCM
           TLS_DHE_RSA_WITH_AES_128_CBC_SHA
           compression methods
                     NULL
           extensions
             status_request
             signature_algorithms
             encrypt_then_mac
             extended_master_secret
```

```
     server_name
       host_name: packages.microsoft.com
6 2  0.0971 (0.0740)  S>C  Handshake
   ServerHello
    Version 3.3
    session_id[0]=

    cipherSuite         TLS_AES_256_GCM_SHA384
    compressionMethod                   NULL
    extensions
6 3  0.0971 (0.0000)  S>C  ChangeCipherSpec
6 4  0.0973 (0.0001)  S>C  application_data
6 5  0.0974 (0.0000)  C>S  ChangeCipherSpec
6 6  0.1119 (0.0145)  C>S  application_data
6 7  0.1119 (0.0000)  C>S  application_data
7 2  0.0718 (0.0442)  S>C  Handshake
   ServerHello
    Version 3.3
    session_id[0]=

    cipherSuite         TLS_AES_256_GCM_SHA384
    compressionMethod                   NULL
    extensions
7 3  0.0718 (0.0000)  S>C  ChangeCipherSpec
7 4  0.0718 (0.0000)  S>C  application_data
7 5  0.0723 (0.0004)  C>S  ChangeCipherSpec
7 6  0.0992 (0.0269)  S>C  application_data
7 7  0.0992 (0.0000)  S>C  application_data
7 8  0.0992 (0.0000)  S>C  application_data
7 9  0.1019 (0.0026)  C>S  application_data
7 10 0.1353 (0.0333)  S>C  application_data
7 11 0.1353 (0.0000)  C>S  application_data
7 12 0.1354 (0.0000)  S>C  application_data
6 8  0.2317 (0.1198)  S>C  application_data
6 9  0.2317 (0.0000)  S>C  application_data
New TCP connection #8: exam-Veriton-M200-H310(42150) <-> esm-content-cache-
2.ps5.canonical.com(443)
7 13 0.2156 (0.0801)  S>C  application_data
8 1  0.1880 (0.1880)  C>S  Handshake
   ClientHello
    Version 3.3
    cipher suites
    TLS_AES_256_GCM_SHA384
    TLS_CHACHA20_POLY1305_SHA256
    TLS_AES_128_GCM_SHA256
    TLS_AES_128_CCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_256_CCM
    TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_ECDSA_WITH_AES_128_CCM
    TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    TLS_RSA_WITH_AES_256_GCM_SHA384
    TLS_RSA_WITH_AES_256_CCM
    TLS_RSA_WITH_AES_256_CBC_SHA
    TLS_RSA_WITH_AES_128_GCM_SHA256
    TLS_RSA_WITH_AES_128_CCM
    TLS_RSA_WITH_AES_128_CBC_SHA
    TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
    TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    TLS_DHE_RSA_WITH_AES_256_CCM
    TLS_DHE_RSA_WITH_AES_256_CBC_SHA
    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
    TLS_DHE_RSA_WITH_AES_128_CCM
    TLS_DHE_RSA_WITH_AES_128_CBC_SHA
    compression methods
         NULL
    extensions
     status_request
     signature_algorithms
     encrypt_then_mac
     extended_master_secret
     server_name
       host_name: esm.ubuntu.com
8 2  0.3513 (0.1633)  S>C  Handshake
   ServerHello
    Version 3.3
    session_id[0]=

    cipherSuite         TLS_AES_256_GCM_SHA384
    compressionMethod                   NULL
    extensions
8 3  0.3513 (0.0000)  S>C  ChangeCipherSpec
8 4  0.3513 (0.0000)  S>C  application_data
8 5  0.3513 (0.0000)  S>C  application_data
8 6  0.3520 (0.0007)  C>S  ChangeCipherSpec
8 7  0.3622 (0.0101)  S>C  application_data
8 8  0.3622 (0.0000)  S>C  application_data
4 14 0.5471 (0.4477)  S>C  application_data
8 9  0.5515 (0.1893)  C>S  application_data
8 10 0.5515 (0.0000)  C>S  application_data
8 11 0.7051 (0.1535)  S>C  application_data
8 12 0.7061 (0.0009)  S>C  application_data
8 13 0.7061 (0.0000)  S>C  application_data
```

```
8 14 0.7065 (0.0004)  C>S  application_data
8 15 0.8588 (0.1522)  S>C  application_data
8    0.9338 (0.0749)  C>S  TCP FIN
8 16 1.0833 (0.1494)  S>C  application_data
7    5.2268 (5.0112)  C>S  TCP FIN
4    5.3657 (4.8186)  C>S  TCP FIN
6    5.2956 (5.0638)  C>S  TCP FIN
5    5.3108 (5.2475)  C>S  TCP FIN
5    5.3247 (0.0138)  S>C  TCP FIN
6    5.3100 (0.0144)  S>C  TCP FIN
7    5.2448 (0.0180)  S>C  TCP FIN
4    5.3886 (0.0228)  S>C  TCP FIN
```