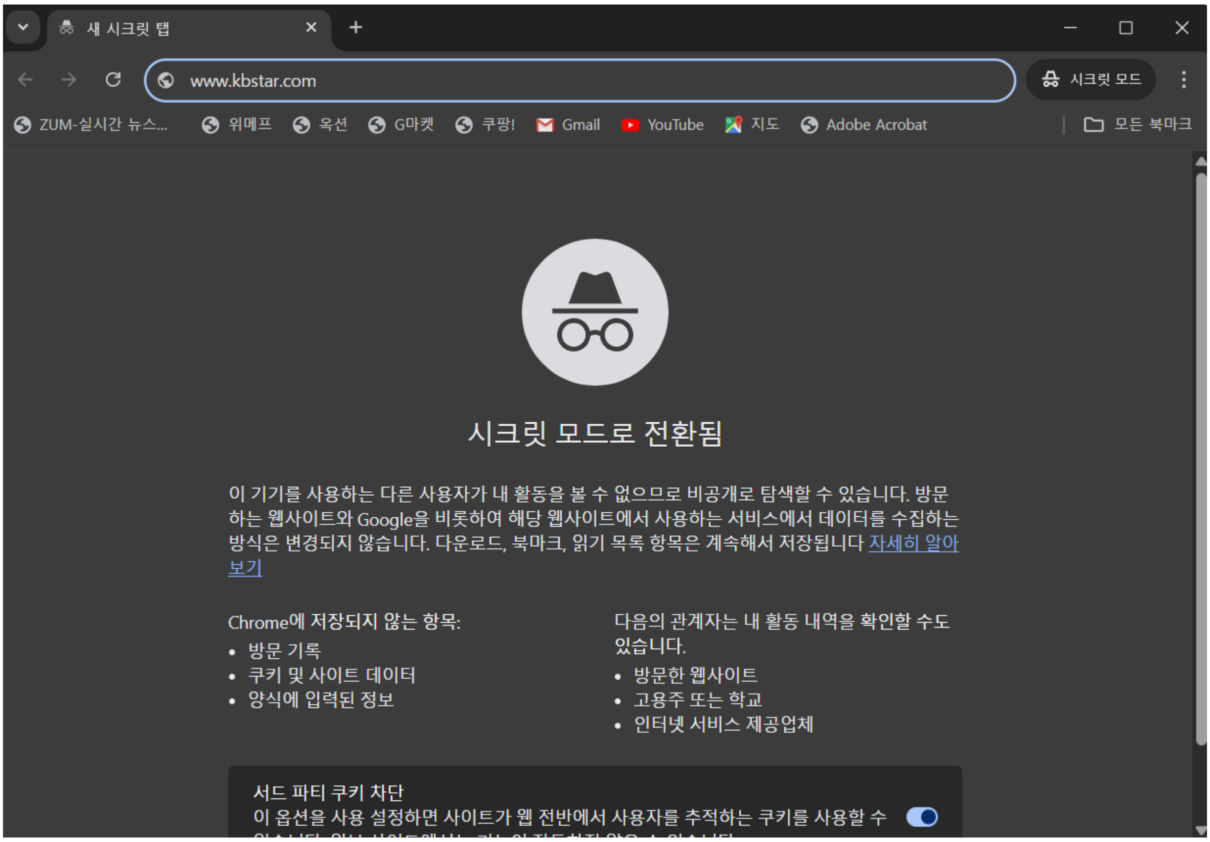
보안프로토콜 12주차 과제

202121556 곽지현

TLS 1.2

크롬 브라우저 창(시크릿 모드)에 www.kbstar.com을 입력



시크릿 모드 전환됨

이 기기를 사용하는 다른 사용자가 내 활동을 볼 수 없으므로 비공개로 탐색할 수 있습니다. 방문하는 웹사이트와 Google을 비롯하여 해당 웹사이트에서 사용하는 서비스에서 데이터를 수집하는 방식은 변경되지 않습니다. 다운로드, 북마크, 읽기 목록 항목은 계속해서 저장됩니다 자세히 알아보기

Chrome에 저장되지 않는 항목:

- 방문 기록
- 쿠키 및 사이트 데이터
- 양식에 입력된 정보

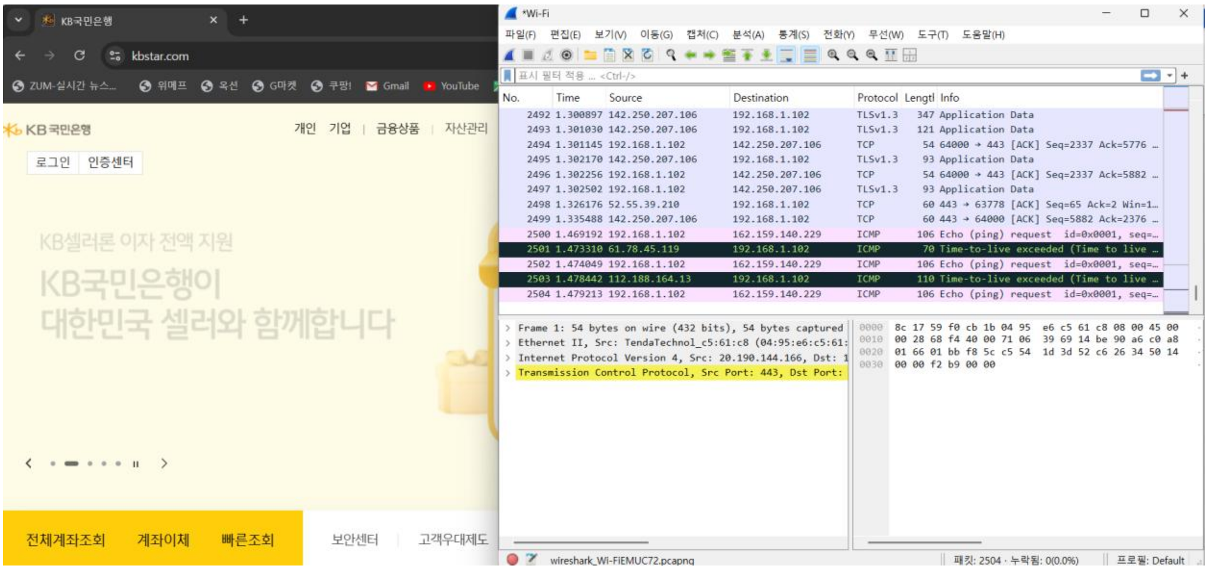
다음의 관계자는 내 활동 내역을 확인할 수도 있습니다.

- 방문한 웹사이트
- 고용주 또는 학교
- 인터넷 서비스 제공업체

서드 파티 쿠키 차단

이 옵션을 사용 설정하면 사이트가 웹 전반에서 사용자를 추적하는 쿠키를 사용할 수

캡쳐 버튼을 클릭 한 뒤 국민은행 페이지에 접속 -> 홈페이지 로딩이 끝나면 캡쳐 중지



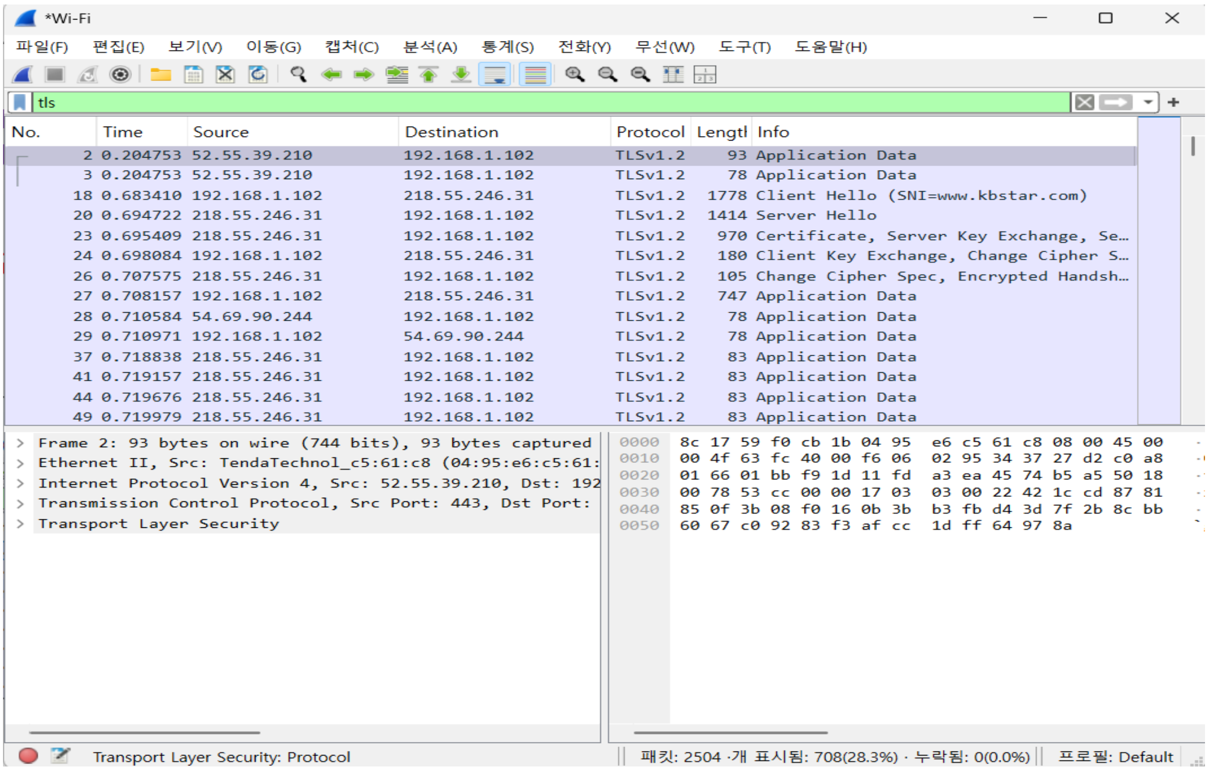
```
No.    Time     Source           Destination      Protocol Lengtl Info
  2492 1.300897 142.250.207.106  192.168.1.102    TLSv1.3    347 Application Data
  2493 1.301030 142.250.207.106  192.168.1.102    TLSv1.3    121 Application Data
  2494 1.301145 192.168.1.102    142.250.207.106  TCP         54 64000 → 443 [ACK] Seq=2337 Ack=5776 …
  2495 1.302170 142.250.207.106  192.168.1.102    TLSv1.3     93 Application Data
  2496 1.302256 192.168.1.102    142.250.207.106  TCP         54 64000 → 443 [ACK] Seq=2337 Ack=5882 …
  2497 1.302502 192.168.1.102    142.250.207.106  TLSv1.3     93 Application Data
  2498 1.326176 52.55.39.210     192.168.1.102    TCP         60 443 → 63778 [ACK] Seq=65 Ack=2 Win=1…
  2499 1.335488 142.250.207.106  192.168.1.102    TCP         60 443 → 64000 [ACK] Seq=5882 Ack=2376 …
  2500 1.469192 192.168.1.102    162.159.140.229  ICMP       106 Echo (ping) request  id=0x0001, seq=…
  2501 1.473310 61.78.45.119     192.168.1.102    ICMP        70 Time-to-live exceeded (Time to live …
  2502 1.474049 192.168.1.102    162.159.140.229  ICMP       106 Echo (ping) request  id=0x0001, seq=…
  2503 1.478442 112.188.164.13   192.168.1.102    ICMP       110 Time-to-live exceeded (Time to live …
  2504 1.479213 192.168.1.102    162.159.140.229  ICMP       106 Echo (ping) request  id=0x0001, seq=…
```

```
> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured
> Ethernet II, Src: TendaTechnol_c5:61:c8 (04:95:e6:c5:61:
> Internet Protocol Version 4, Src: 20.190.144.166, Dst: 1
> Transmission Control Protocol, Src Port: 443, Dst Port:
```

```
0000  8c 17 59 f0 cb 1b 04 95  e6 c5 61 c8 08 00 45 00
0010  00 28 68 f4 40 00 71 06  39 69 14 be 90 a6 c0 a8
0020  01 66 01 bb f8 5c c5 54  1d 3d 52 c6 26 34 50 14
0030  00 00 f2 b9 00 00
```

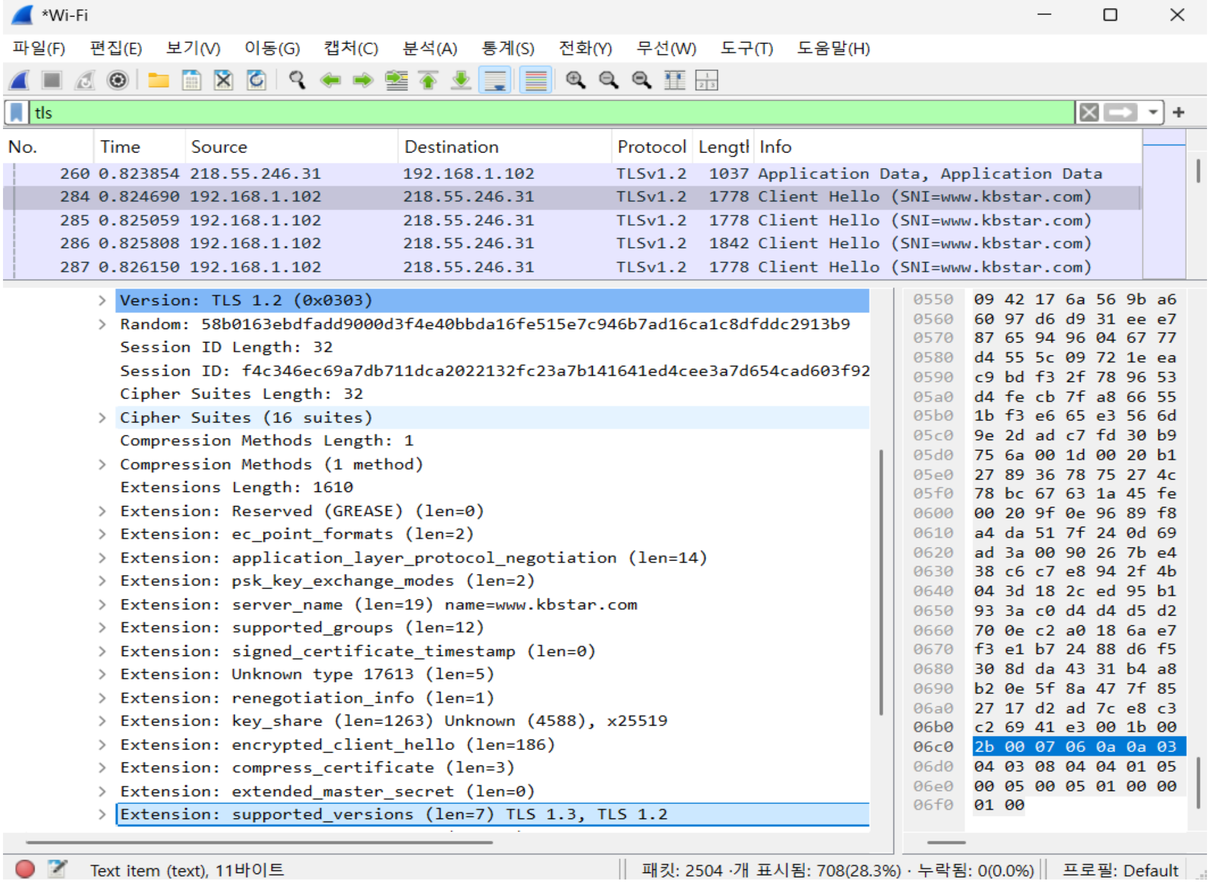
wireshark_Wi-FIEMUC72.pcapng | 패킷: 2504 · 누락됨: 0(0.0%) | 프로필: Default

필터 창에 tls를 검색


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

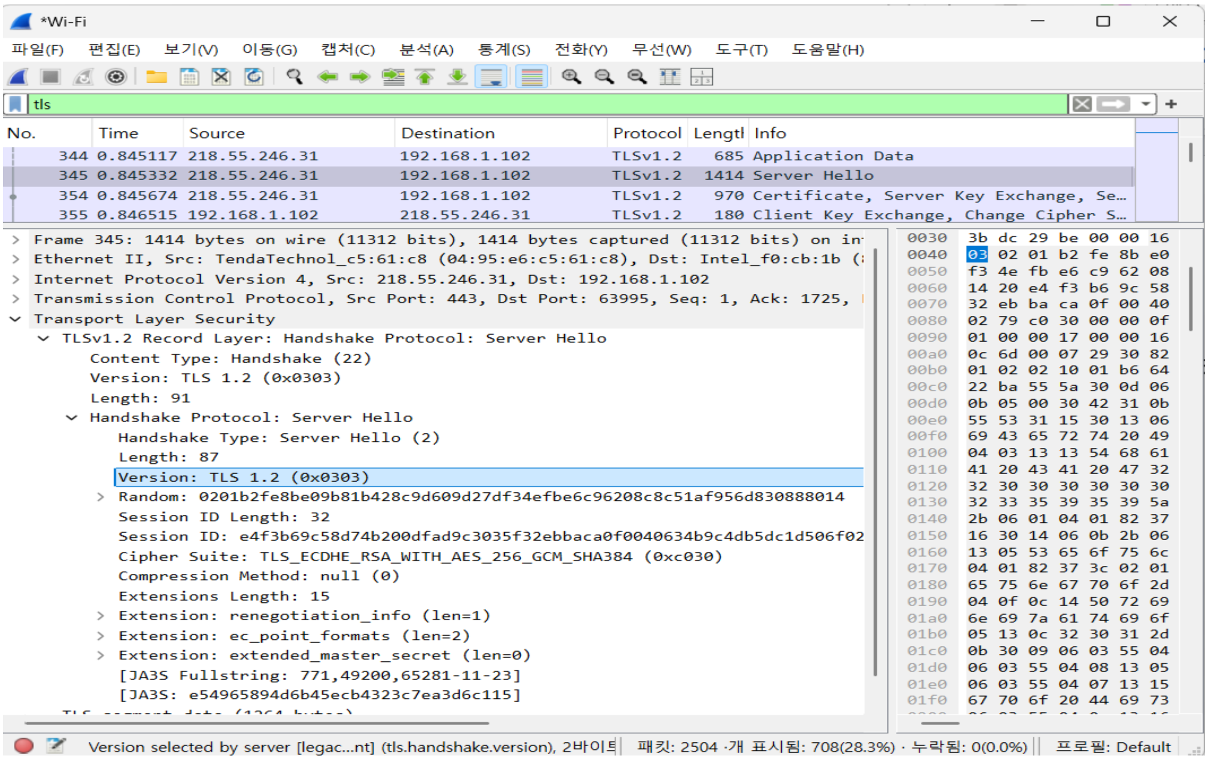
```
tls

No.   Time     Source         Destination    Protocol Lengtl Info
    2 0.204753 52.55.39.210   192.168.1.102  TLSv1.2    93 Application Data
    3 0.204753 52.55.39.210   192.168.1.102  TLSv1.2    78 Application Data
   18 0.683410 192.168.1.102  218.55.246.31  TLSv1.2  1778 Client Hello (SNI=www.kbstar.com)
   20 0.694722 218.55.246.31  192.168.1.102  TLSv1.2  1414 Server Hello
   23 0.695409 218.55.246.31  192.168.1.102  TLSv1.2   970 Certificate, Server Key Exchange, Se…
   24 0.698084 192.168.1.102  218.55.246.31  TLSv1.2   180 Client Key Exchange, Change Cipher S…
   26 0.707575 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
   27 0.708157 192.168.1.102  218.55.246.31  TLSv1.2   747 Application Data
   28 0.710584 54.69.90.244   192.168.1.102  TLSv1.2    78 Application Data
   29 0.710971 192.168.1.102  54.69.90.244   TLSv1.2    78 Application Data
   37 0.718838 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data
   41 0.719157 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data
   44 0.719676 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data
   49 0.719979 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data

> Frame 2: 93 bytes on wire (744 bits), 93 bytes captured
> Ethernet II, Src: TendaTechnol_c5:61:c8 (04:95:e6:c5:61:
> Internet Protocol Version 4, Src: 52.55.39.210, Dst: 192
> Transmission Control Protocol, Src Port: 443, Dst Port:
> Transport Layer Security

0000  8c 17 59 f0 cb 1b 04 95  e6 c5 61 c8 08 00 45 00
0010  00 4f 63 fc 40 00 f6 06  02 95 34 37 27 d2 c0 a8
0020  01 66 01 bb f9 1d 11 fd  a3 ea 45 74 b5 a5 50 18
0030  00 78 53 cc 00 00 17 03  03 00 22 42 1c cd 87 81
0040  85 0f 3b 08 f0 16 0b 3b  b3 fb d4 3d 7f 2b 8c bb
0050  60 67 c0 92 83 f3 af cc  1d ff 64 97 8a

Transport Layer Security: Protocol
패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%)    프로필: Default
```

Client Hello의 버전과 Cipher Suites를 확인 -> Extension 필드에 추가적인 정보 포함


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

```
tls

No.   Time     Source         Destination    Protocol Lengtl Info
  260 0.823854 218.55.246.31  192.168.1.102  TLSv1.2  1037 Application Data, Application Data
  284 0.824690 192.168.1.102  218.55.246.31  TLSv1.2  1778 Client Hello (SNI=www.kbstar.com)
  285 0.825059 192.168.1.102  218.55.246.31  TLSv1.2  1778 Client Hello (SNI=www.kbstar.com)
  286 0.825808 192.168.1.102  218.55.246.31  TLSv1.2  1842 Client Hello (SNI=www.kbstar.com)
  287 0.826150 192.168.1.102  218.55.246.31  TLSv1.2  1778 Client Hello (SNI=www.kbstar.com)

  > Version: TLS 1.2 (0x0303)
  > Random: 58b0163ebdfadd9000d3f4e40bbda16fe515e7c946b7ad16ca1c8dfddc2913b9
    Session ID Length: 32
    Session ID: f4c346ec69a7db711dca2022132fc23a7b141641ed4cee3a7d654cad603f92
    Cipher Suites Length: 32
  > Cipher Suites (16 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 1610
  > Extension: Reserved (GREASE) (len=0)
  > Extension: ec_point_formats (len=2)
  > Extension: application_layer_protocol_negotiation (len=14)
  > Extension: psk_key_exchange_modes (len=2)
  > Extension: server_name (len=19) name=www.kbstar.com
  > Extension: supported_groups (len=12)
  > Extension: signed_certificate_timestamp (len=0)
  > Extension: Unknown type 17613 (len=5)
  > Extension: renegotiation_info (len=1)
  > Extension: key_share (len=1263) Unknown (4588), x25519
  > Extension: encrypted_client_hello (len=186)
  > Extension: compress_certificate (len=3)
  > Extension: extended_master_secret (len=0)
  > Extension: supported_versions (len=7) TLS 1.3, TLS 1.2

0550  09 42 17 6a 56 9b a6
0560  60 97 d6 d9 31 ee e7
0570  87 65 94 96 04 67 77
0580  d4 55 5c 09 72 1e ea
0590  c9 bd f3 2f 78 96 53
05a0  d4 fe cb 7f a8 66 55
05b0  1b f3 e6 65 e3 56 6d
05c0  9e 2d ad c7 fd 30 b9
05d0  75 6a 00 1d 00 20 b1
05e0  27 89 36 78 75 27 4c
05f0  78 bc 67 63 1a 45 fe
0600  00 20 9f 0e 96 89 f8
0610  a4 da 51 7f 24 0d 69
0620  ad 3a 00 90 26 7b e4
0630  38 c6 c7 e8 94 2f 4b
0640  04 3d 18 2c ed 95 b1
0650  93 3a c0 d4 d4 d5 d2
0660  70 0e c2 a0 18 6a e7
0670  f3 e1 b7 24 88 d6 f5
0680  30 8d da 43 31 b4 a8
0690  b2 0e 5f 8a 47 7f 85
06a0  27 17 d2 ad 7c e8 c3
06b0  c2 69 41 e3 00 1b 00
06c0  2b 00 07 06 0a 0a 03
06d0  04 03 08 04 04 01 05
06e0  00 05 00 05 01 00 00
06f0  01 00

Text item (text), 11바이트
패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%)    프로필: Default
```

Server Hello 패킷 확인 -> TLS 1.2 선택, Cipher Suite 선택


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

tls

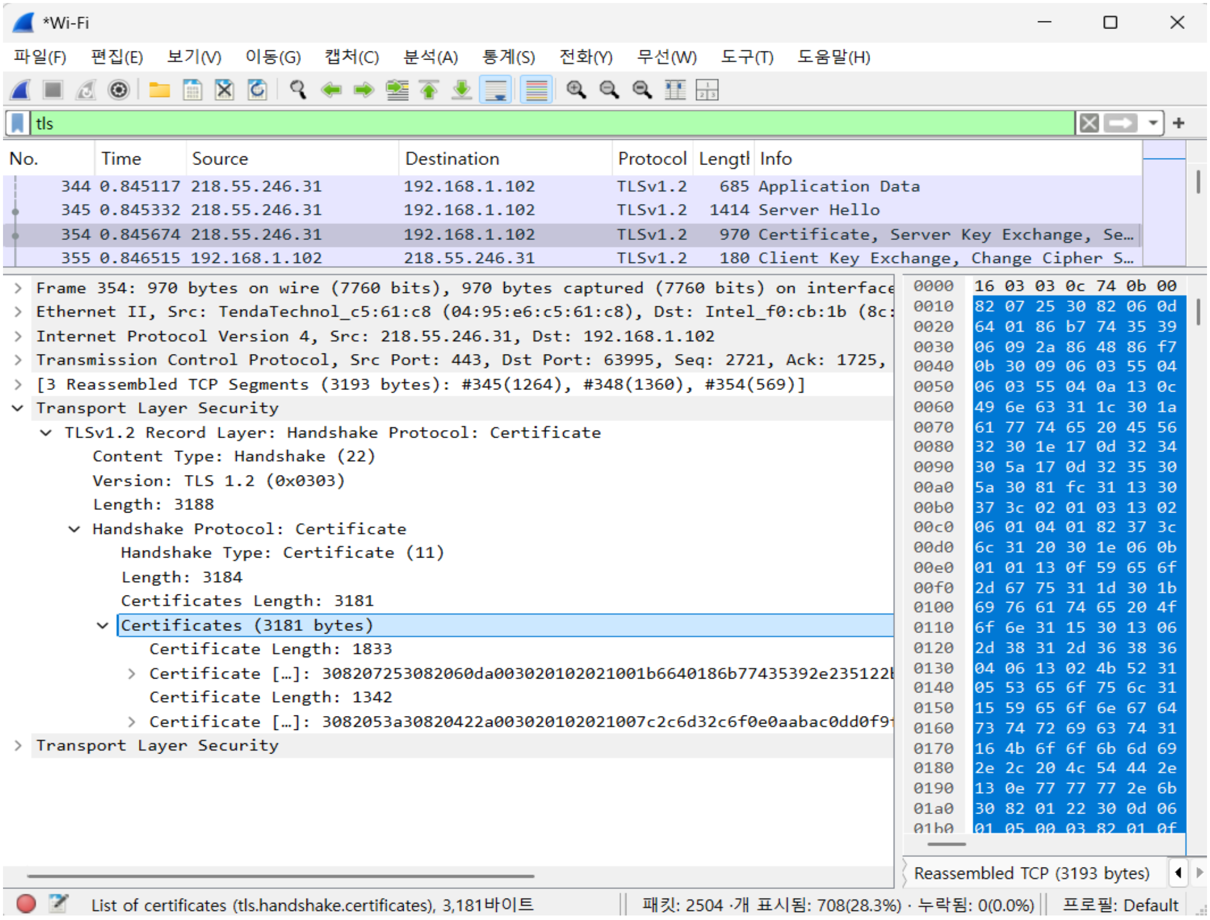
```
No.   Time     Source         Destination    Protocol Lengtl Info
  344 0.845117 218.55.246.31  192.168.1.102  TLSv1.2    685 Application Data
  345 0.845332 218.55.246.31  192.168.1.102  TLSv1.2   1414 Server Hello
  354 0.845674 218.55.246.31  192.168.1.102  TLSv1.2    970 Certificate, Server Key Exchange, Se…
  355 0.846515 192.168.1.102  218.55.246.31  TLSv1.2    180 Client Key Exchange, Change Cipher S…
```

```
> Frame 345: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on in
> Ethernet II, Src: TendaTechnol_c5:61:c8 (04:95:e6:c5:61:c8), Dst: Intel_f0:cb:1b (
> Internet Protocol Version 4, Src: 218.55.246.31, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 63995, Seq: 1, Ack: 1725,
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 91
    v Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 87
        Version: TLS 1.2 (0x0303)
      > Random: 0201b2fe8be09b81b428c9d609d27df34efbe6c96208c8c51af956d830888014
        Session ID Length: 32
        Session ID: e4f3b69c58d74b200dfad9c3035f32ebbaca0f0040634b9c4db5dc1d506f02
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
        Compression Method: null (0)
        Extensions Length: 15
      > Extension: renegotiation_info (len=1)
      > Extension: ec_point_formats (len=2)
      > Extension: extended_master_secret (len=0)
        [JA3S Fullstring: 771,49200,65281-11-23]
        [JA3S: e54965894d6b45ecb4323c7ea3d6c115]
```

```
0030  3b dc 29 be 00 00 16
0040  03 02 01 b2 fe 8b e0
0050  f3 4e fb e6 c9 62 08
0060  14 20 e4 f3 b6 9c 58
0070  32 eb ba ca 0f 00 40
0080  02 79 c0 30 00 00 0f
0090  01 00 00 17 00 00 16
00a0  0c 6d 00 07 29 30 82
00b0  01 02 02 10 01 b6 64
00c0  22 ba 55 5a 30 0d 06
00d0  0b 05 00 30 42 31 0b
00e0  55 53 31 15 30 13 06
00f0  69 43 65 72 74 20 49
0100  04 03 13 13 54 68 61
0110  41 20 43 41 20 47 32
0120  32 30 30 30 30 30 30
0130  32 33 35 39 35 39 5a
0140  2b 06 01 04 01 82 37
0150  16 30 14 06 0b 2b 06
0160  13 05 53 65 6f 75 6c
0170  04 01 82 37 3c 02 01
0180  65 75 6e 67 70 6f 2d
0190  04 0f 0c 14 50 72 69
01a0  6e 69 7a 61 74 69 6f
01b0  05 13 0c 32 30 31 2d
01c0  0b 30 09 06 03 55 04
01d0  06 03 55 04 08 13 05
01e0  06 03 55 04 07 13 15
01f0  67 70 6f 20 44 69 73
```

Version selected by server [legac…nt] (tls.handshake.version), 2바이트 | 패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%) | 프로필: Default

Certificate 패킷 확인 -> 3181byte 길이의 -> 인증서 필드 확장 (인증서 2개)


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

tls

```
No.   Time     Source         Destination    Protocol Lengtl Info
  344 0.845117 218.55.246.31  192.168.1.102  TLSv1.2    685 Application Data
  345 0.845332 218.55.246.31  192.168.1.102  TLSv1.2   1414 Server Hello
  354 0.845674 218.55.246.31  192.168.1.102  TLSv1.2    970 Certificate, Server Key Exchange, Se…
  355 0.846515 192.168.1.102  218.55.246.31  TLSv1.2    180 Client Key Exchange, Change Cipher S…
```

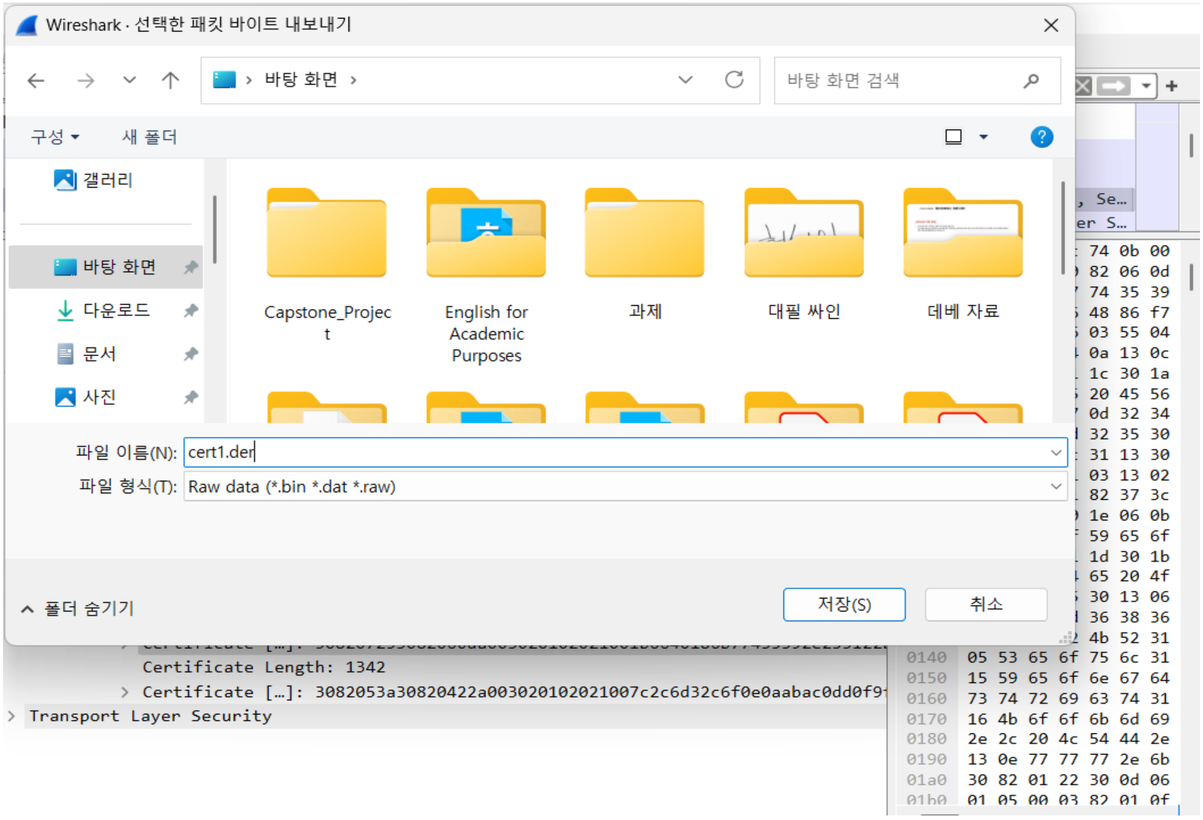
```
> Frame 354: 970 bytes on wire (7760 bits), 970 bytes captured (7760 bits) on interface
> Ethernet II, Src: TendaTechnol_c5:61:c8 (04:95:e6:c5:61:c8), Dst: Intel_f0:cb:1b (8c:
> Internet Protocol Version 4, Src: 218.55.246.31, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 63995, Seq: 2721, Ack: 1725,
> [3 Reassembled TCP Segments (3193 bytes): #345(1264), #348(1360), #354(569)]
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 3188
    v Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 3184
        Certificates Length: 3181
      v Certificates (3181 bytes)
          Certificate Length: 1833
        > Certificate […]: 308207253082060da003020102021001b6640186b77435392e235122b
          Certificate Length: 1342
        > Certificate […]: 3082053a30820422a003020102021007c2c6d32c6f0e0aabac0dd0f9
> Transport Layer Security
```

```
0000  16 03 03 0c 74 0b 00
0010  82 07 25 30 82 06 0d
0020  64 01 86 b7 74 35 39
0030  06 09 2a 86 48 86 f7
0040  0b 30 09 06 03 55 04
0050  06 03 55 04 0a 13 0c
0060  49 6e 63 31 1c 30 1a
0070  61 77 74 65 20 45 56
0080  32 30 1e 17 0d 32 34
0090  30 5a 17 0d 32 35 30
00a0  5a 30 81 fc 31 13 30
00b0  37 3c 02 01 03 13 02
00c0  06 01 04 01 82 37 3c
00d0  6c 31 20 30 1e 06 0b
00e0  01 01 13 0f 59 65 6f
00f0  2d 67 75 31 1d 30 1b
0100  69 76 61 74 65 20 4f
0110  6f 6e 31 15 30 13 06
0120  2d 38 31 2d 36 38 36
0130  04 06 13 02 4b 52 31
0140  05 53 65 6f 75 6c 31
0150  15 59 65 6f 6e 67 64
0160  73 74 72 69 63 74 31
0170  16 4b 6f 6f 6b 6d 69
0180  2e 2c 20 4c 54 44 2e
0190  13 0e 77 77 77 2e 6b
01a0  30 82 01 22 30 0d 06
01b0  01 05 00 03 82 01 0f
```

Reassembled TCP (3193 bytes)

List of certificates (tls.handshake.certificates), 3,181바이트 | 패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%) | 프로필: Default

첫 번째 인증서 데이터 저장 -> cert1.der



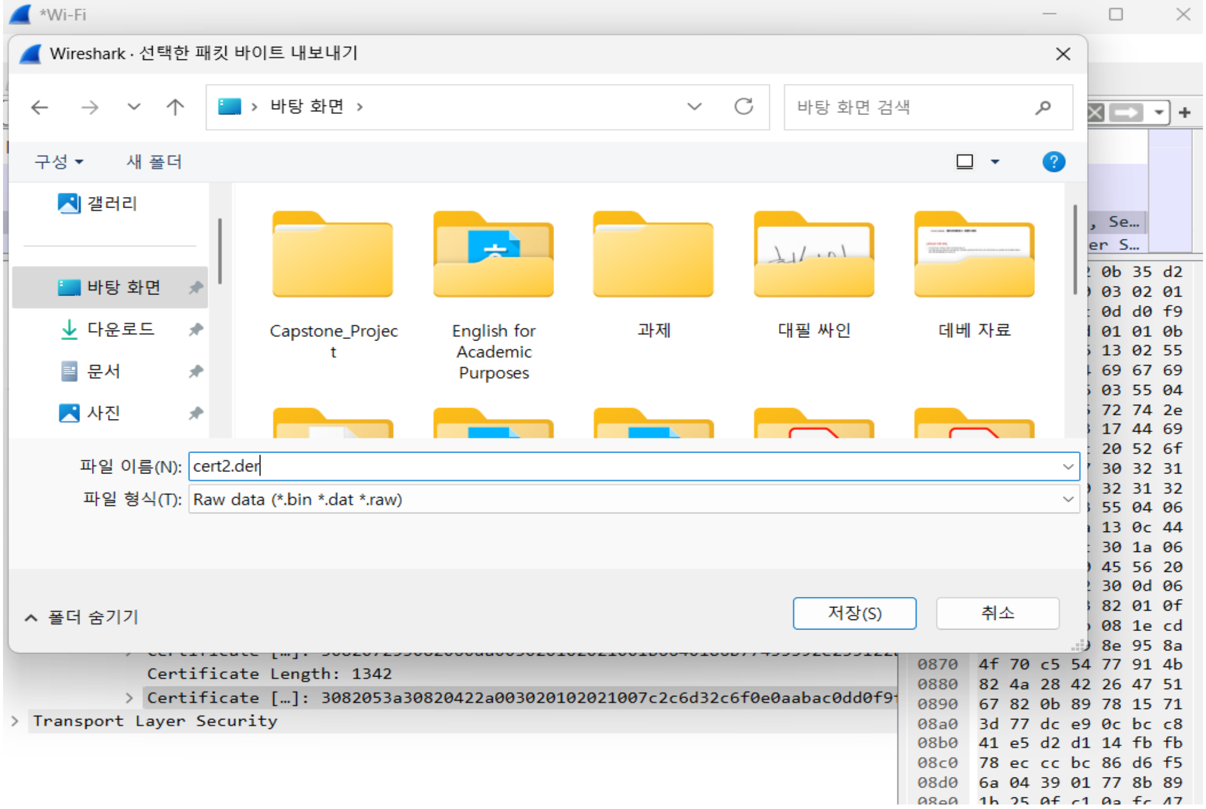
파일 이름(N): cert1.der

파일 형식(T): Raw data (*.bin *.dat *.raw)

```
    Certificate Length: 1342
  > Certificate […]: 3082053a30820422a003020102021007c2c6d32c6f0e0aabac0dd0f9
> Transport Layer Security
```

```
0140  05 53 65 6f 75 6c 31
0150  15 59 65 6f 6e 67 64
0160  73 74 72 69 63 74 31
0170  16 4b 6f 6f 6b 6d 69
0180  2e 2c 20 4c 54 44 2e
0190  13 0e 77 77 77 2e 6b
01a0  30 82 01 22 30 0d 06
01b0  01 05 00 03 82 01 0f
```

두 번째 인증서 데이터 저장 -> cert2.der



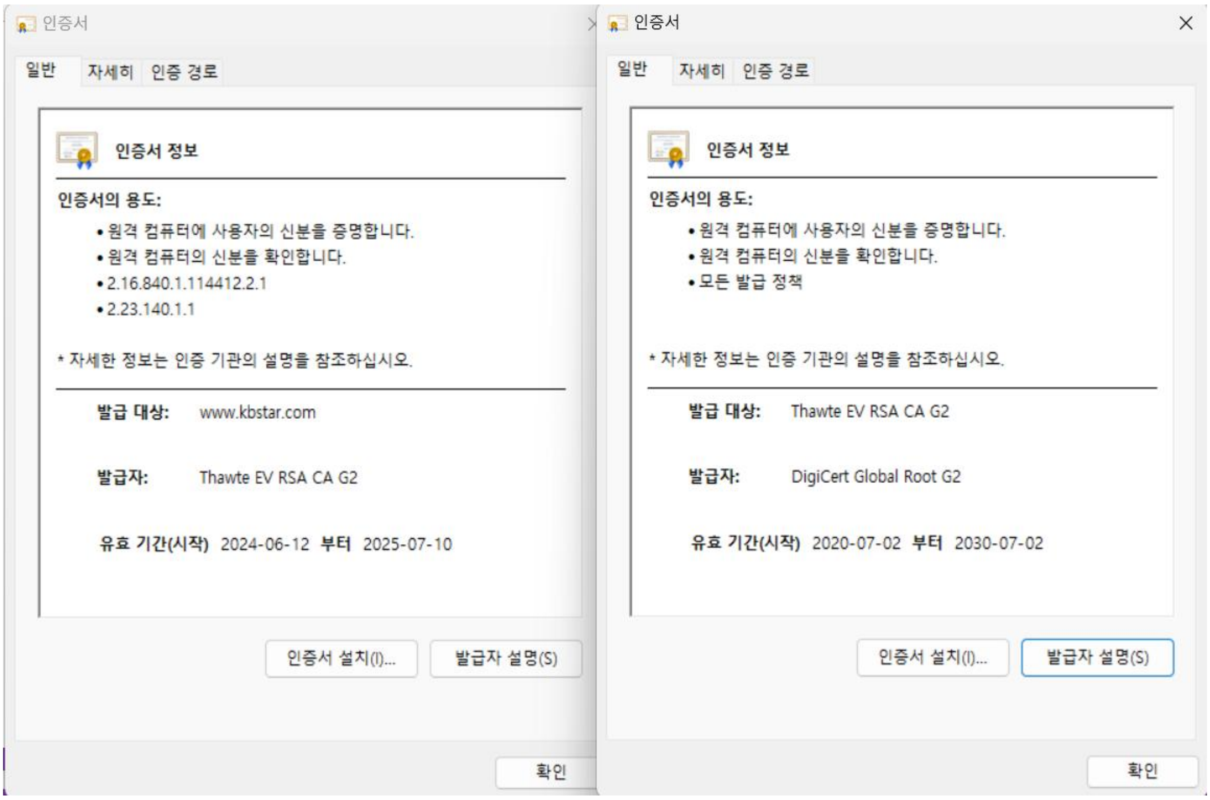
파일 이름(N): cert2.der

파일 형식(T): Raw data (*.bin *.dat *.raw)

```
    Certificate Length: 1342
  > Certificate […]: 3082053a30820422a003020102021007c2c6d32c6f0e0aabac0dd0f9
> Transport Layer Security
```

```
0870  4f 70 c5 54 77 91 4b
0880  82 4a 28 42 26 47 51
0890  67 82 0b 89 78 15 71
08a0  3d 77 dc e9 0c bc c8
08b0  41 e5 d2 d1 14 fb fb
08c0  78 ec cc bc 86 d6 f5
08d0  6a 04 39 01 77 8b 89
```

cert1.der은 국민은행의 인증서이고, cert2.der은 발급자(CA)에 대한 인증서이다.



인증서 정보

인증서의 용도:

- 원격 컴퓨터에 사용자의 신분을 증명합니다.
- 원격 컴퓨터의 신분을 확인합니다.
- 2.16.840.1.114412.2.1
- 2.23.140.1.1

* 자세한 정보는 인증 기관의 설명을 참조하십시오.

발급 대상: www.kbstar.com

발급자: Thawte EV RSA CA G2

유효 기간(시작) 2024-06-12 부터 2025-07-10

인증서 정보

인증서의 용도:

- 원격 컴퓨터에 사용자의 신분을 증명합니다.
- 원격 컴퓨터의 신분을 확인합니다.
- 모든 발급 정책

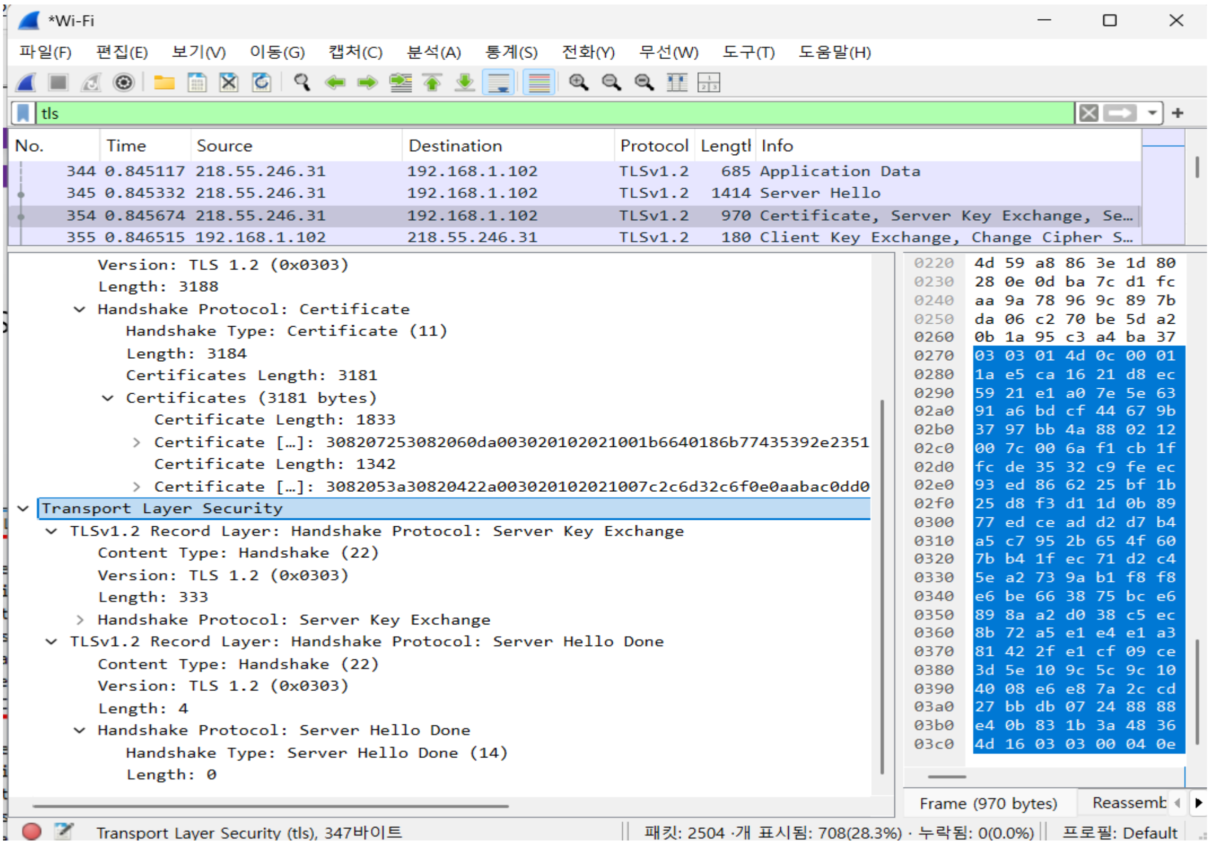
* 자세한 정보는 인증 기관의 설명을 참조하십시오.

발급 대상: Thawte EV RSA CA G2

발급자: DigiCert Global Root G2

유효 기간(시작) 2020-07-02 부터 2030-07-02

Certificate 패킷에 Server Key Exchange와 Server Hello Done 패킷도 함께 포함되어 있다.



tls

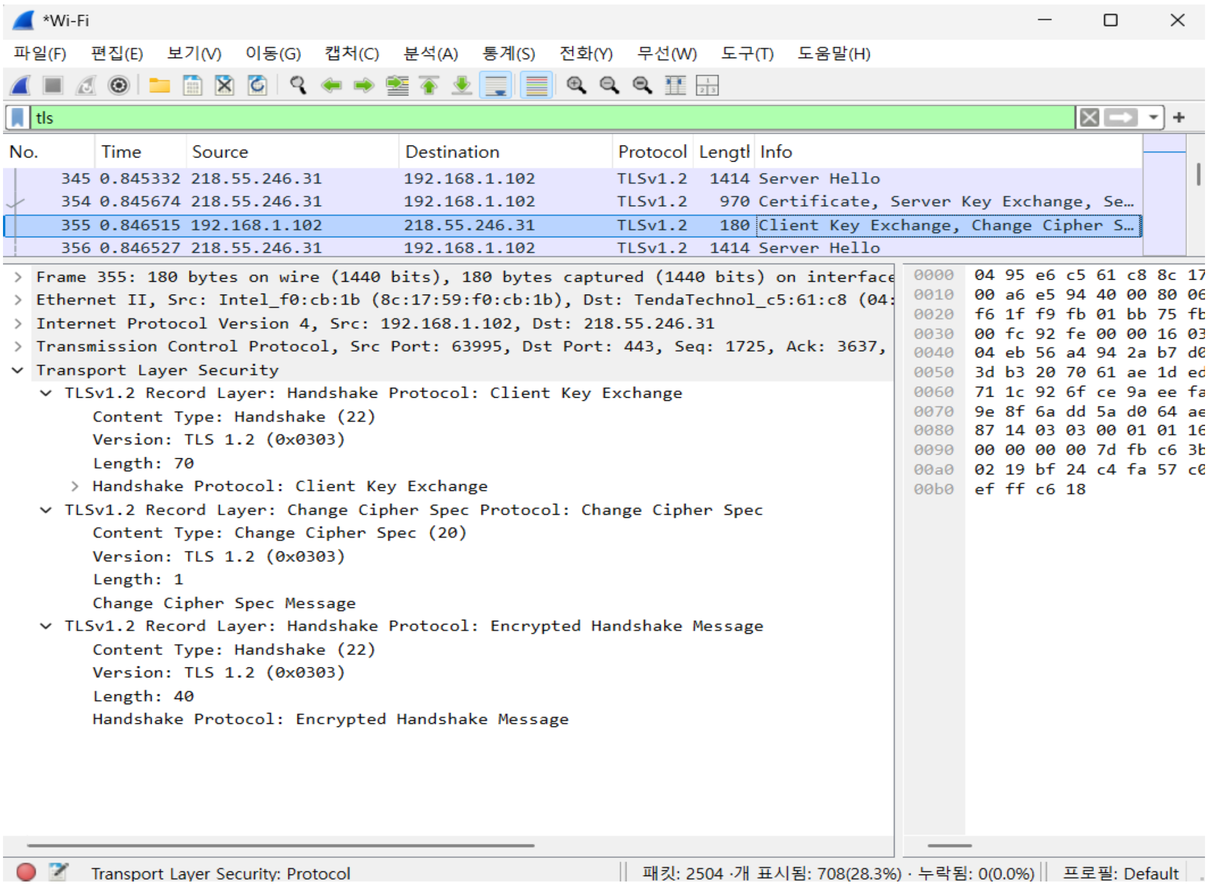
```
No.  Time     Source         Destination    Protocol Lengtl Info
 344 0.845117 218.55.246.31  192.168.1.102  TLSv1.2   685 Application Data
 345 0.845332 218.55.246.31  192.168.1.102  TLSv1.2  1414 Server Hello
 354 0.845674 218.55.246.31  192.168.1.102  TLSv1.2   970 Certificate, Server Key Exchange, Se…
 355 0.846515 192.168.1.102  218.55.246.31  TLSv1.2   180 Client Key Exchange, Change Cipher S…
```

```
        Version: TLS 1.2 (0x0303)
        Length: 3188
      ⌄ Handshake Protocol: Certificate
          Handshake Type: Certificate (11)
          Length: 3184
          Certificates Length: 3181
        ⌄ Certificates (3181 bytes)
            Certificate Length: 1833
          > Certificate […]: 308207253082060da003020102021001b6640186b77435392e2351
            Certificate Length: 1342
          > Certificate […]: 3082053a30820422a003020102021007c2c6d32c6f0e0aabac0dd0
⌄ Transport Layer Security
    ⌄ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 333
      > Handshake Protocol: Server Key Exchange
    ⌄ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 4
      ⌄ Handshake Protocol: Server Hello Done
          Handshake Type: Server Hello Done (14)
          Length: 0
```

```
0220  4d 59 a8 86 3e 1d 80
0230  28 0e 0d ba 7c d1 fc
0240  aa 9a 78 96 9c 89 7b
0250  da 06 c2 70 be 5d a2
0260  0b 1a 95 c3 a4 ba 37
0270  03 03 01 4d 0c 00 01
0280  1a e5 ca 16 21 d8 ec
0290  59 21 e1 a0 7e 5e 63
02a0  91 a6 bd cf 44 67 9b
02b0  37 97 bb 4a 88 02 12
02c0  00 7c 00 6a f1 cb 1f
02d0  fc de 35 32 c9 fe ec
02e0  93 ed 86 62 25 bf 1b
02f0  25 d8 f3 d1 1d 0b 89
0300  77 ed ce ad d2 d7 b4
0310  a5 c7 95 2b 65 4f 60
0320  7b b4 1f ec 71 d2 c4
0330  5e a2 73 9a b1 f8 f8
0340  e6 be 66 38 75 bc e6
0350  89 8a a2 d0 38 c5 ec
0360  8b 72 a5 e1 e4 e1 a3
0370  81 42 2f e1 cf 09 ce
0380  3d 5e 10 9c 5c 9c 10
0390  40 08 e6 e8 7a 2c cd
03a0  27 bb db 07 24 88 88
03b0  e4 0b 83 1b 3a 48 36
03c0  4d 16 03 03 00 04 0e
```

Transport Layer Security (tls), 347바이트 || 패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%) || 프로필: Default

클라이언트가 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message(Finish) 패킷을 보낸다.


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

tls

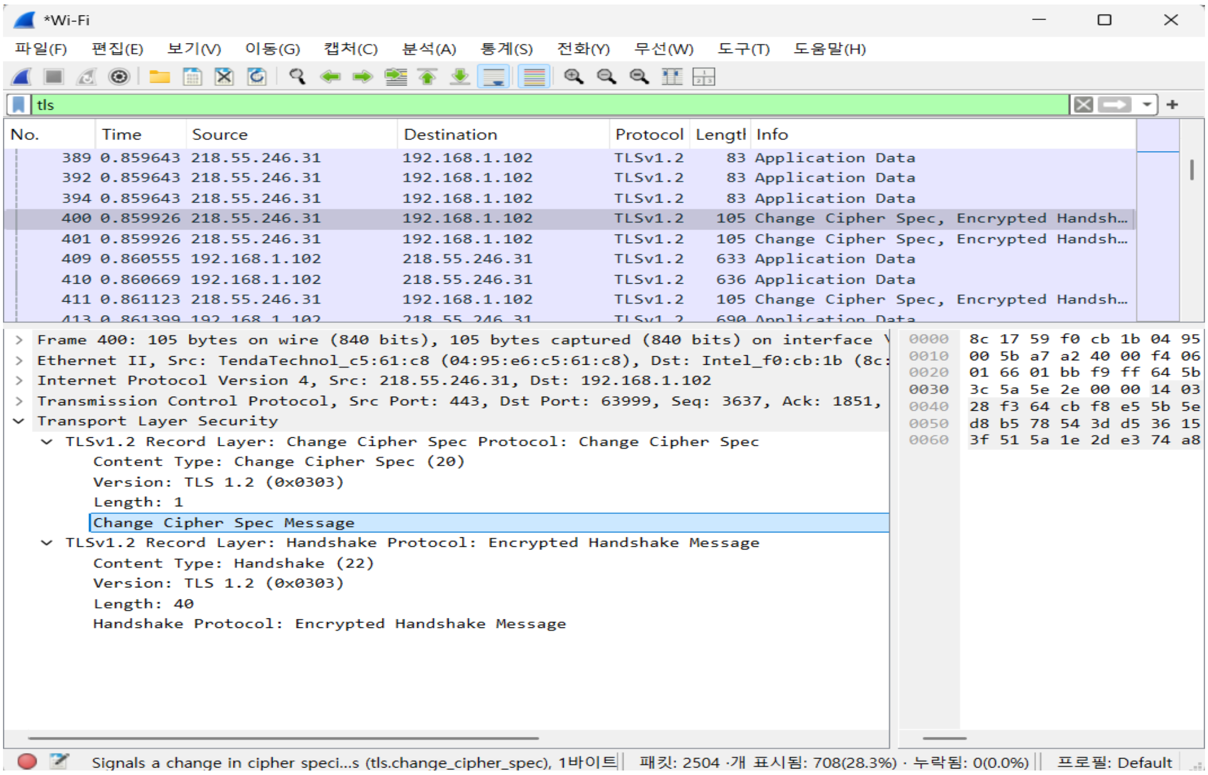
```
No.  Time     Source         Destination    Protocol Lengtl Info
  345 0.845332 218.55.246.31  192.168.1.102  TLSv1.2  1414 Server Hello
  354 0.845674 218.55.246.31  192.168.1.102  TLSv1.2   970 Certificate, Server Key Exchange, Se…
  355 0.846515 192.168.1.102  218.55.246.31  TLSv1.2   180 Client Key Exchange, Change Cipher S…
  356 0.846527 218.55.246.31  192.168.1.102  TLSv1.2  1414 Server Hello
```

```
> Frame 355: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface
> Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: TendaTechnol_c5:61:c8 (04:
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 218.55.246.31
> Transmission Control Protocol, Src Port: 63995, Dst Port: 443, Seq: 1725, Ack: 3637,
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 70
    > Handshake Protocol: Client Key Exchange
  v TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  v TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

```
0000  04 95 e6 c5 61 c8 8c 17
0010  00 a6 e5 94 40 00 80 06
0020  f6 1f f9 fb 01 bb 75 fb
0030  00 fc 92 fe 00 00 16 03
0040  04 eb 56 a4 94 2a b7 d0
0050  3d b3 20 70 61 ae 1d ed
0060  71 1c 92 6f ce 9a ee fa
0070  9e 8f 6a dd 5a d0 64 ae
0080  87 14 03 03 00 01 01 16
0090  00 00 00 00 7d fb c6 3b
00a0  02 19 bf 24 c4 fa 57 c0
00b0  ef ff c6 18
```

Transport Layer Security: Protocol | 패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%) | 프로필: Default

서버에서 Change Cipher Spec, Encrypted Handshake Message(Finish) 패킷을 보낸다.


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

tls

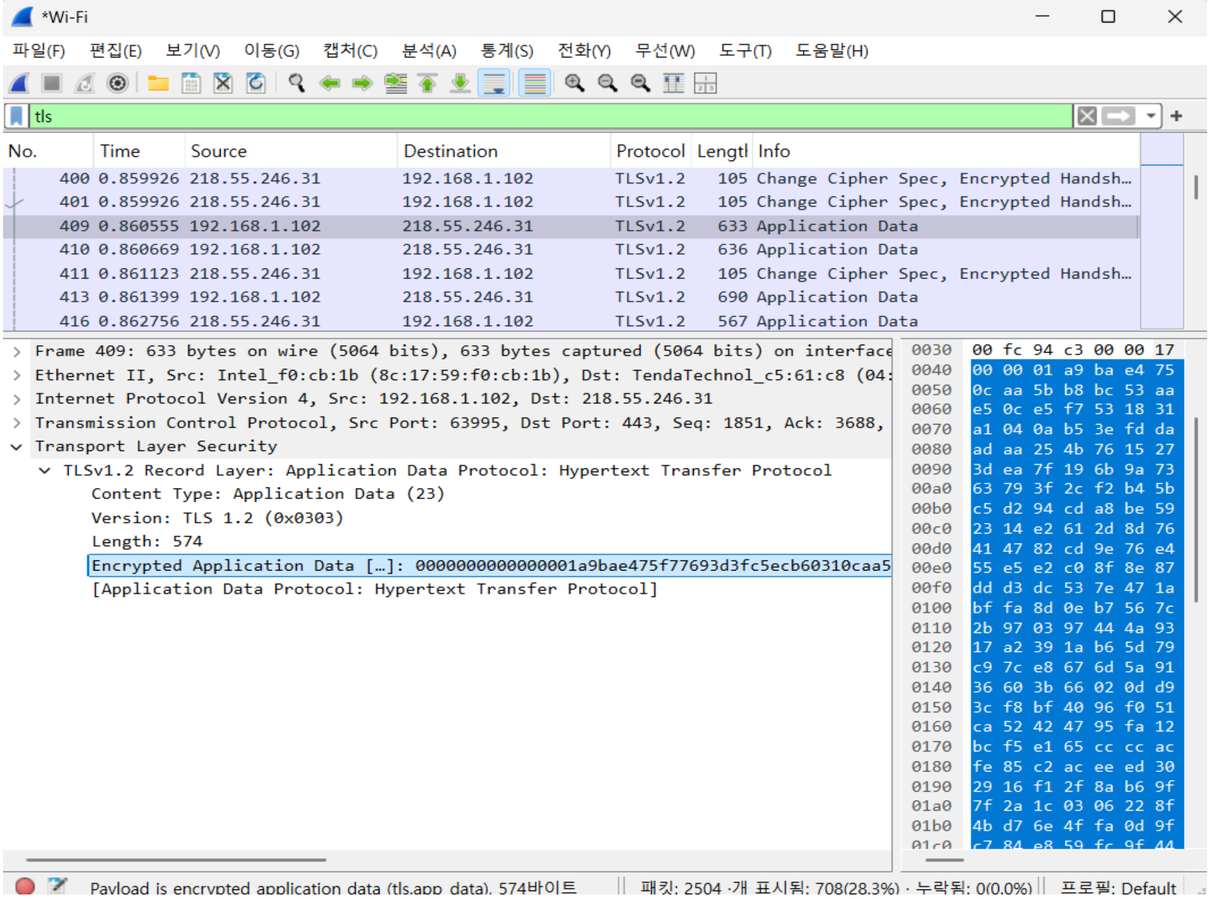
```
No.  Time     Source         Destination    Protocol Lengtl Info
  389 0.859643 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data
  392 0.859643 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data
  394 0.859643 218.55.246.31  192.168.1.102  TLSv1.2    83 Application Data
  400 0.859926 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
  401 0.859926 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
  409 0.860555 192.168.1.102  218.55.246.31  TLSv1.2   633 Application Data
  410 0.860669 192.168.1.102  218.55.246.31  TLSv1.2   636 Application Data
  411 0.861123 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
  413 0.861399 192.168.1.102  218.55.246.31  TLSv1.2   690 Application Data
```

```
> Frame 400: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \
> Ethernet II, Src: TendaTechnol_c5:61:c8 (04:95:e6:c5:61:c8), Dst: Intel_f0:cb:1b (8c:
> Internet Protocol Version 4, Src: 218.55.246.31, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 443, Dst Port: 63999, Seq: 3637, Ack: 1851,
v Transport Layer Security
  v TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  v TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 40
      Handshake Protocol: Encrypted Handshake Message
```

```
0000  8c 17 59 f0 cb 1b 04 95
0010  00 5b a7 a2 40 00 f4 06
0020  01 66 01 bb f9 ff 64 5b
0030  3c 5a 5e 2e 00 00 14 03
0040  28 f3 64 cb f8 e5 5b 5e
0050  d8 b5 78 54 3d d5 36 15
0060  3f 51 5a 1e 2d e3 74 a8
```

Signals a change in cipher speci...s (tls.change_cipher_spec), 1바이트 | 패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%) | 프로필: Default

TLS handshake 이후의 Application Data 패킷들은 모두 암호화 되어 전송


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

tls

```
No.   Time     Source         Destination    Protocol Lengtl Info
  400 0.859926 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
  401 0.859926 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
  409 0.860555 192.168.1.102  218.55.246.31  TLSv1.2   633 Application Data
  410 0.860669 192.168.1.102  218.55.246.31  TLSv1.2   636 Application Data
  411 0.861123 218.55.246.31  192.168.1.102  TLSv1.2   105 Change Cipher Spec, Encrypted Handsh…
  413 0.861399 192.168.1.102  218.55.246.31  TLSv1.2   690 Application Data
  416 0.862756 218.55.246.31  192.168.1.102  TLSv1.2   567 Application Data
```

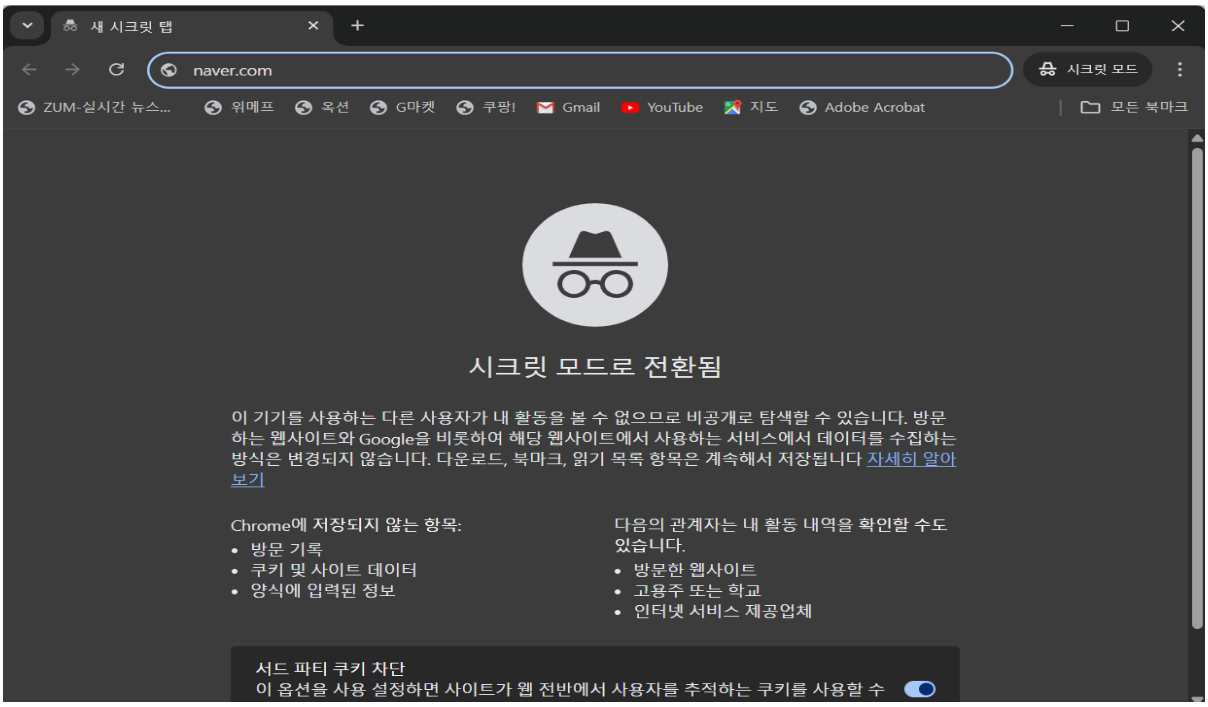
```
> Frame 409: 633 bytes on wire (5064 bits), 633 bytes captured (5064 bits) on interface
> Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: TendaTechnol_c5:61:c8 (04:
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 218.55.246.31
> Transmission Control Protocol, Src Port: 63995, Dst Port: 443, Seq: 1851, Ack: 3688,
v Transport Layer Security
  v TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 574
      Encrypted Application Data […]: 0000000000000001a9bae475f77693d3fc5ecb60310caa5
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0030  00 fc 94 c3 00 00 17
0040  00 00 01 a9 ba e4 75
0050  0c aa 5b b8 bc 53 aa
0060  e5 0c e5 f7 53 18 31
0070  a1 04 0a b5 3e fd da
0080  ad aa 25 4b 76 15 27
0090  3d ea 7f 19 6b 9a 73
00a0  63 79 3f 2c f2 b4 5b
00b0  c5 d2 94 cd a8 be 59
00c0  23 14 e2 61 2d 8d 76
00d0  41 47 82 cd 9e 76 e4
00e0  55 e5 e2 c0 8f 8e 87
00f0  dd d3 dc 53 7e 47 1a
0100  bf fa 8d 0e b7 56 7c
0110  2b 97 03 97 44 4a 93
0120  17 a2 39 1a b6 5d 79
0130  c9 7c e8 67 6d 5a 91
0140  36 60 3b 66 02 0d d9
0150  3c f8 bf 40 96 f0 51
0160  ca 52 42 47 95 fa 12
0170  bc f5 e1 65 cc cc ac
0180  fe 85 c2 ac ee ed 30
0190  29 16 f1 2f 8a b6 9f
01a0  7f 2a 1c 03 06 22 8f
01b0  4b d7 6e 4f fa 0d 9f
01c0  c7 84 e8 59 fc 9f 44
```

Payload is encrypted application data (tls.app_data), 574바이트 | 패킷: 2504 ·개 표시됨: 708(28.3%) · 누락됨: 0(0.0%) | 프로필: Default

TLS 1.3

크롬 브라우저 창(시크릿 모드)에 www.naver.com을 입력



시크릿 모드로 전환됨

이 기기를 사용하는 다른 사용자가 내 활동을 볼 수 없으므로 비공개로 탐색할 수 있습니다. 방문하는 웹사이트와 Google을 비롯하여 해당 웹사이트에서 사용하는 서비스에서 데이터를 수집하는 방식은 변경되지 않습니다. 다운로드, 북마크, 읽기 목록 항목은 계속해서 저장됩니다 자세히 알아보기

Chrome에 저장되지 않는 항목:

- 방문 기록
- 쿠키 및 사이트 데이터
- 양식에 입력된 정보

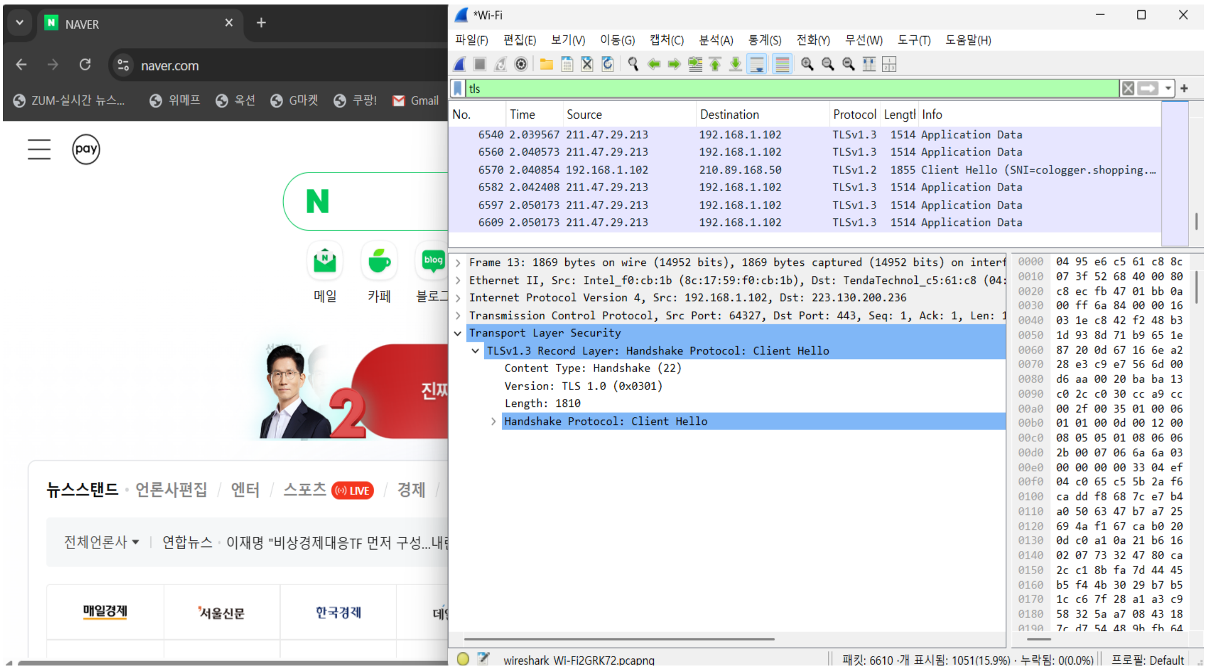
다음의 관계자는 내 활동 내역을 확인할 수도 있습니다.

- 방문한 웹사이트
- 고용주 또는 학교
- 인터넷 서비스 제공업체

서드 파티 쿠키 차단

이 옵션을 사용 설정하면 사이트가 웹 전반에서 사용자를 추적하는 쿠키를 사용할 수

캡쳐 버튼을 클릭 한 뒤 네이버 페이지에 접속 -> 홈페이지 로딩이 끝나면 캡쳐 중지


NAVER
naver.com
ZUM-실시간 뉴스...
위메프
옥션
G마켓
쿠팡!
Gmail
pay
메일
카페
블로그
진짜
뉴스스탠드 · 언론사편집 / 엔터 / 스포츠 LIVE / 경제 /
전체언론사 ▾ | 연합뉴스 · 이재명 "비상경제대응TF 먼저 구성...내
매일경제
서울신문
한국경제
*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

```
tls
```

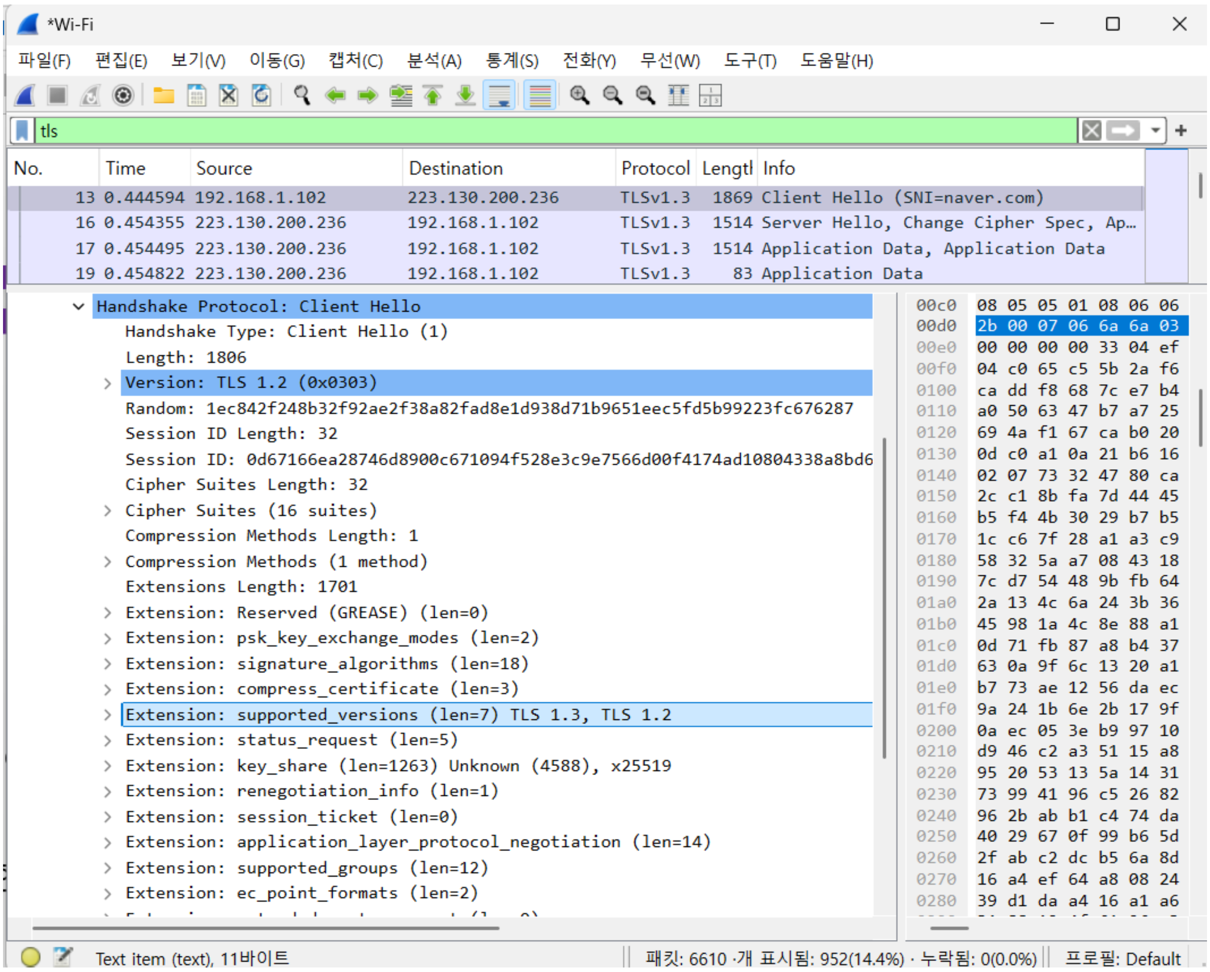
```
No.   Time     Source         Destination    Protocol Length Info
 6540 2.039567 211.47.29.213  192.168.1.102  TLSv1.3  1514 Application Data
 6560 2.040573 211.47.29.213  192.168.1.102  TLSv1.3  1514 Application Data
 6570 2.040854 192.168.1.102  210.89.168.50  TLSv1.2  1855 Client Hello (SNI=cologger.shopping.…
 6582 2.042408 211.47.29.213  192.168.1.102  TLSv1.3  1514 Application Data
 6597 2.050173 211.47.29.213  192.168.1.102  TLSv1.3  1514 Application Data
 6609 2.050173 211.47.29.213  192.168.1.102  TLSv1.3  1514 Application Data
```

```
> Frame 13: 1869 bytes on wire (14952 bits), 1869 bytes captured (14952 bits) on interf
> Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: TendaTechnol_c5:61:c8 (04:
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 223.130.200.236
> Transmission Control Protocol, Src Port: 64327, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1810
    > Handshake Protocol: Client Hello
```

```
0000  04 95 e6 c5 61 c8 8c
0010  07 3f 52 68 40 00 80
0020  c8 ec fb 47 01 bb 0a
0030  00 ff 6a 84 00 00 16
0040  03 1e c8 42 f2 48 b3
0050  1d 93 8d 71 b9 65 1e
0060  87 20 0d 67 16 6e a2
0070  28 e3 c9 e7 56 6d 00
0080  d6 aa 00 20 ba ba 13
0090  c0 2c c0 30 cc a9 cc
00a0  00 2f 00 35 01 00 06
00b0  01 01 00 0d 00 12 00
00c0  08 05 05 01 08 06 06
00d0  2b 00 07 06 6a 6a 03
00e0  00 00 00 00 33 04 ef
00f0  04 c0 65 c5 5b 2a f6
0100  ca dd f8 68 7c e7 b4
0110  a0 50 63 47 b7 a7 25
0120  69 4a f1 67 ca b0 20
0130  0d c0 a1 0a 21 b6 16
0140  02 07 73 32 47 80 ca
0150  2c c1 8b fa 7d 44 45
0160  b5 f4 4b 30 29 b7 b5
0170  1c c6 7f 28 a1 a3 c9
0180  58 32 5a a7 08 43 18
```

wireshark Wi-Fi2GRK72.pcapng | 패킷: 6610 ·개 표시됨: 1051(15.9%) · 누락됨: 0(0.0%) | 프로필: Default

Client Hello 패킷 확인 -> TLS 1.2, TLS 1.3 모두 지원, 그에 따른 데이터들을 전송


*Wi-Fi
파일(F) 편집(E) 보기(V) 이동(G) 캡처(C) 분석(A) 통계(S) 전화(Y) 무선(W) 도구(T) 도움말(H)

```
tls
```

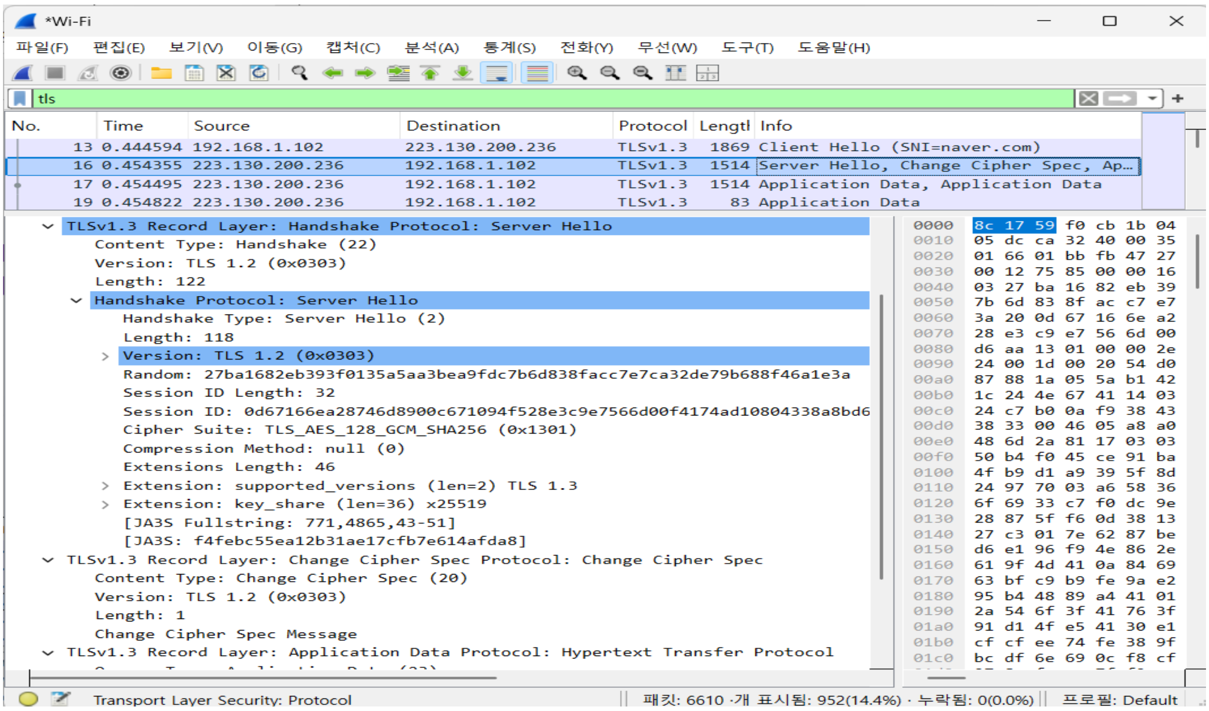
```
No. Time     Source          Destination     Protocol Length Info
 13 0.444594 192.168.1.102   223.130.200.236 TLSv1.3  1869 Client Hello (SNI=naver.com)
 16 0.454355 223.130.200.236 192.168.1.102   TLSv1.3  1514 Server Hello, Change Cipher Spec, Ap…
 17 0.454495 223.130.200.236 192.168.1.102   TLSv1.3  1514 Application Data, Application Data
 19 0.454822 223.130.200.236 192.168.1.102   TLSv1.3    83 Application Data
```

```
v Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 1806
  > Version: TLS 1.2 (0x0303)
    Random: 1ec842f248b32f92ae2f38a82fad8e1d938d71b9651eec5fd5b99223fc676287
    Session ID Length: 32
    Session ID: 0d67166ea28746d8900c671094f528e3c9e7566d00f4174ad10804338a8bd6
    Cipher Suites Length: 32
  > Cipher Suites (16 suites)
    Compression Methods Length: 1
  > Compression Methods (1 method)
    Extensions Length: 1701
  > Extension: Reserved (GREASE) (len=0)
  > Extension: psk_key_exchange_modes (len=2)
  > Extension: signature_algorithms (len=18)
  > Extension: compress_certificate (len=3)
  > Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
  > Extension: status_request (len=5)
  > Extension: key_share (len=1263) Unknown (4588), x25519
  > Extension: renegotiation_info (len=1)
  > Extension: session_ticket (len=0)
  > Extension: application_layer_protocol_negotiation (len=14)
  > Extension: supported_groups (len=12)
  > Extension: ec_point_formats (len=2)
```

```
00c0  08 05 05 01 08 06 06
00d0  2b 00 07 06 6a 6a 03
00e0  00 00 00 00 33 04 ef
00f0  04 c0 65 c5 5b 2a f6
0100  ca dd f8 68 7c e7 b4
0110  a0 50 63 47 b7 a7 25
0120  69 4a f1 67 ca b0 20
0130  0d c0 a1 0a 21 b6 16
0140  02 07 73 32 47 80 ca
0150  2c c1 8b fa 7d 44 45
0160  b5 f4 4b 30 29 b7 b5
0170  1c c6 7f 28 a1 a3 c9
0180  58 32 5a a7 08 43 18
0190  7c d7 54 48 9b fb 64
01a0  2a 13 4c 6a 24 3b 36
01b0  45 98 1a 4c 8e 88 a1
01c0  0d 71 fb 87 a8 b4 37
01d0  63 0a 9f 6c 13 20 a1
01e0  b7 73 ae 12 56 da ec
01f0  9a 24 1b 6e 2b 17 9f
0200  0a ec 05 3e b9 97 10
0210  d9 46 c2 a3 51 15 a8
0220  95 20 53 13 5a 14 31
0230  73 99 41 96 c5 26 82
0240  96 2b ab b1 c4 74 da
0250  40 29 67 0f 99 b6 5d
0260  2f ab c2 dc b5 6a 8d
0270  16 a4 ef 64 a8 08 24
0280  39 d1 da a4 16 a1 a6
```

Text item (text), 11바이트 | 패킷: 6610 ·개 표시됨: 952(14.4%) · 누락됨: 0(0.0%) | 프로필: Default

Server Hello 패킷 확인 -> TLS 1.3 선택, Cipher Suite 선택하여 응답, 세션키 생성을 끝내서 바로 Change Cipher Spec 패킷을 보내고 Application Data 패킷으로 암호화된 데이터를 전송



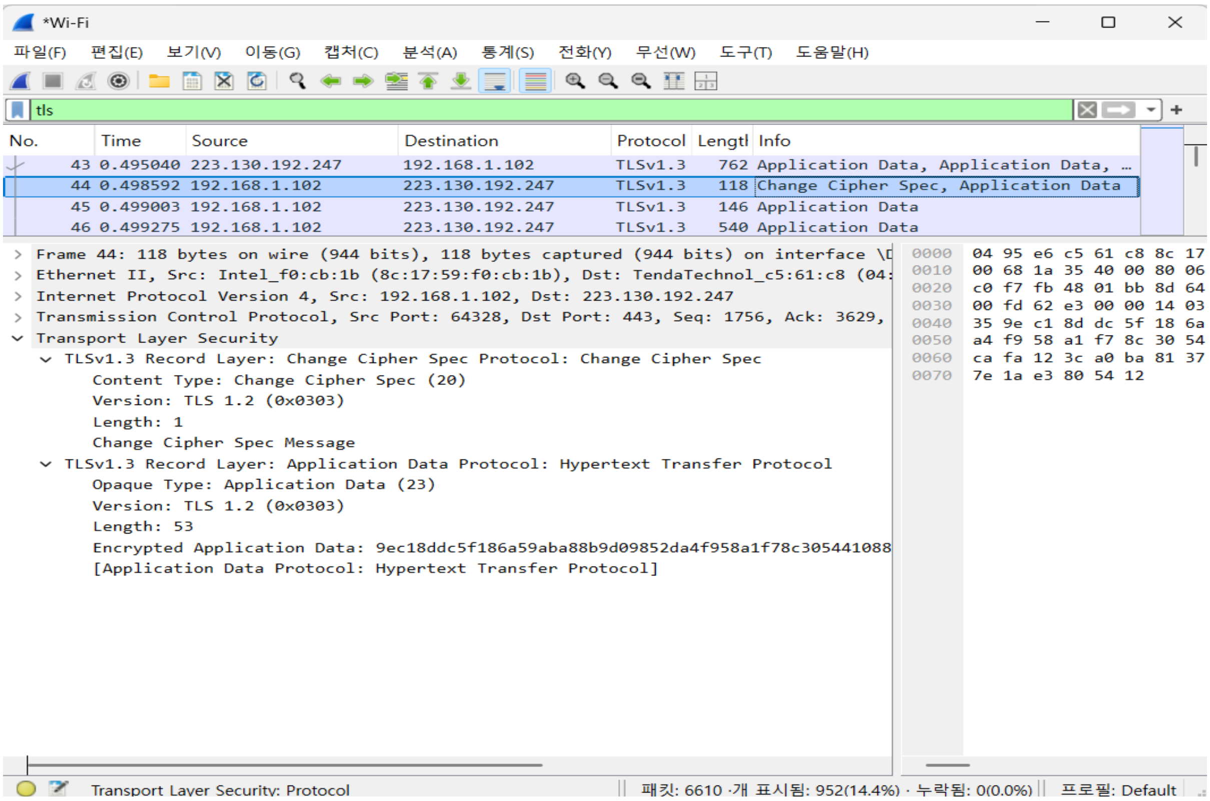
```
No.  Time      Source           Destination      Protocol Lengtl Info
  13 0.444594  192.168.1.102    223.130.200.236  TLSv1.3  1869 Client Hello (SNI=naver.com)
  16 0.454355  223.130.200.236  192.168.1.102    TLSv1.3  1514 Server Hello, Change Cipher Spec, Ap…
  17 0.454495  223.130.200.236  192.168.1.102    TLSv1.3  1514 Application Data, Application Data
  19 0.454822  223.130.200.236  192.168.1.102    TLSv1.3    83 Application Data
```

```
  ⌄ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 122
    ⌄ Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 118
      > Version: TLS 1.2 (0x0303)
        Random: 27ba1682eb393f0135a5aa3bea9fdc7b6d838facc7e7ca32de79b688f46a1e3a
        Session ID Length: 32
        Session ID: 0d67166ea28746d8900c671094f528e3c9e7566d00f4174ad10804338a8bd6
        Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
        Compression Method: null (0)
        Extensions Length: 46
      > Extension: supported_versions (len=2) TLS 1.3
      > Extension: key_share (len=36) x25519
        [JA3S Fullstring: 771,4865,43-51]
        [JA3S: f4febc55ea12b31ae17cfb7e614afda8]
  ⌄ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ⌄ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
```

```
0000  8c 17 59 f0 cb 1b 04
0010  05 dc ca 32 40 00 35
0020  01 66 01 bb fb 47 27
0030  00 12 75 85 00 00 16
0040  03 27 ba 16 82 eb 39
0050  7b 6d 83 8f ac c7 e7
0060  3a 20 0d 67 16 6e a2
0070  28 e3 c9 e7 56 6d 00
0080  d6 aa 13 01 00 00 2e
0090  24 00 1d 00 20 54 d0
00a0  87 88 1a 05 5a b1 42
00b0  1c 24 4e 67 41 14 03
00c0  24 c7 b0 0a f9 38 43
00d0  38 33 00 46 05 a8 a0
00e0  48 6d 2a 81 17 03 03
00f0  50 b4 f0 45 ce 91 ba
0100  4f b9 d1 a9 39 5f 8d
0110  24 97 70 03 a6 58 36
0120  6f 69 33 c7 f0 dc 9e
0130  28 87 5f f6 0d 38 13
0140  27 c3 01 7e 62 87 be
0150  d6 e1 96 f9 4e 86 2e
0160  61 9f 4d 41 0a 84 69
0170  63 bf c9 b9 fe 9a e2
0180  95 b4 48 89 a4 41 01
0190  2a 54 6f 3f 41 76 3f
01a0  91 d1 4f e5 41 30 e1
01b0  cf cf ee 74 fe 38 9f
01c0  bc df 6e 69 0c f8 cf
```

Transport Layer Security: Protocol || 패킷: 6610 ·개 표시됨: 952(14.4%) · 누락됨: 0(0.0%) || 프로필: Default

클라이언트도 Change Cipher Spec 패킷을 보내고, 이후의 Application Data 패킷들은 모두 암호화되어 전송



```
No.  Time      Source           Destination      Protocol Lengtl Info
  43 0.495040  223.130.192.247  192.168.1.102    TLSv1.3   762 Application Data, Application Data, …
  44 0.498592  192.168.1.102    223.130.192.247  TLSv1.3   118 Change Cipher Spec, Application Data
  45 0.499003  192.168.1.102    223.130.192.247  TLSv1.3   146 Application Data
  46 0.499275  192.168.1.102    223.130.192.247  TLSv1.3   540 Application Data
```

```
> Frame 44: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \D
> Ethernet II, Src: Intel_f0:cb:1b (8c:17:59:f0:cb:1b), Dst: TendaTechnol_c5:61:c8 (04:
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 223.130.192.247
> Transmission Control Protocol, Src Port: 64328, Dst Port: 443, Seq: 1756, Ack: 3629,
⌄ Transport Layer Security
  ⌄ TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ⌄ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 53
      Encrypted Application Data: 9ec18ddc5f186a59aba88b9d09852da4f958a1f78c305441088
      [Application Data Protocol: Hypertext Transfer Protocol]
```

```
0000  04 95 e6 c5 61 c8 8c 17
0010  00 68 1a 35 40 00 80 06
0020  c0 f7 fb 48 01 bb 8d 64
0030  00 fd 62 e3 00 00 14 03
0040  35 9e c1 8d dc 5f 18 6a
0050  a4 f9 58 a1 f7 8c 30 54
0060  ca fa 12 3c a0 ba 81 37
0070  7e 1a e3 80 54 12
```

Transport Layer Security: Protocol || 패킷: 6610 ·개 표시됨: 952(14.4%) · 누락됨: 0(0.0%) || 프로필: Default