

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH TN (CO3094)

LAB 8

Wireshark Lab: SSL v8.0

HK: 241 - LỚP: L09

GVHD: Bùi Xuân Giang

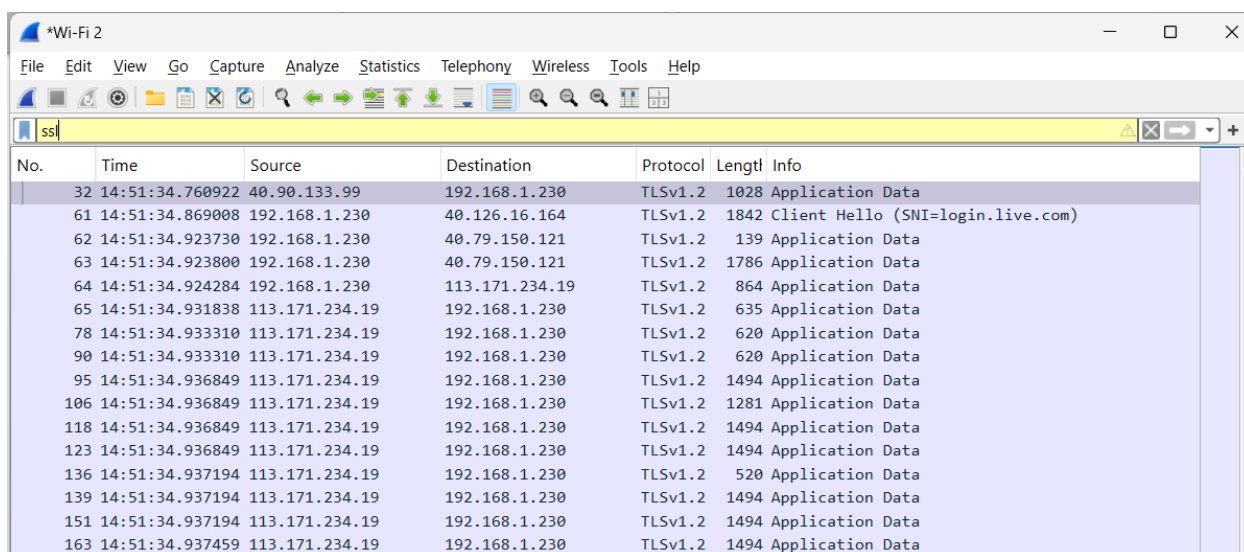
Sinh viên thực hiện

Nguyễn Tấn Tài : 2212990

Thành phố Hồ Chí Minh, tháng 11 năm 2024

Wireshark Lab: SSL v8.0

Trong bài lab này, chúng ta sẽ tìm hiểu về giao thức Lớp Công Bảo mật (SSL - Secure Sockets Layer), tập trung vào các bản ghi SSL được gửi qua kết nối TCP. Chúng ta sẽ thực hiện điều này bằng cách phân tích dấu vết của các bản ghi SSL được gửi giữa máy của bạn và một máy chủ thương mại điện tử. Chúng ta sẽ tìm hiểu các loại bản ghi SSL khác nhau cũng như các trường trong các thông điệp SSL. Bạn có thể muốn xem lại Mục 8.6 trong sách để có thêm thông tin. Chúng tôi hiện đang phát triển một bài lab Wireshark bao gồm TLS, một giao thức thay thế cho SSL trong ấn bản thứ 8 của sách.



No.	Time	Source	Destination	Protocol	Length	Info
32	14:51:34.760922	40.90.133.99	192.168.1.230	TLSv1.2	1028	Application Data
61	14:51:34.869008	192.168.1.230	40.126.16.164	TLSv1.2	1842	Client Hello (SNI=login.live.com)
62	14:51:34.923730	192.168.1.230	40.79.150.121	TLSv1.2	139	Application Data
63	14:51:34.923800	192.168.1.230	40.79.150.121	TLSv1.2	1786	Application Data
64	14:51:34.924284	192.168.1.230	113.171.234.19	TLSv1.2	864	Application Data
65	14:51:34.931838	113.171.234.19	192.168.1.230	TLSv1.2	635	Application Data
78	14:51:34.933310	113.171.234.19	192.168.1.230	TLSv1.2	620	Application Data
90	14:51:34.933310	113.171.234.19	192.168.1.230	TLSv1.2	620	Application Data
95	14:51:34.936849	113.171.234.19	192.168.1.230	TLSv1.2	1494	Application Data
106	14:51:34.936849	113.171.234.19	192.168.1.230	TLSv1.2	1281	Application Data
118	14:51:34.936849	113.171.234.19	192.168.1.230	TLSv1.2	1494	Application Data
123	14:51:34.936849	113.171.234.19	192.168.1.230	TLSv1.2	1494	Application Data
136	14:51:34.937194	113.171.234.19	192.168.1.230	TLSv1.2	520	Application Data
139	14:51:34.937194	113.171.234.19	192.168.1.230	TLSv1.2	1494	Application Data
151	14:51:34.937194	113.171.234.19	192.168.1.230	TLSv1.2	1494	Application Data
163	14:51:34.937459	113.171.234.19	192.168.1.230	TLSv1.2	1494	Application Data

1. Capturing packets in an SSL session

Bước đầu tiên là thu thập các gói tin trong một phiên SSL. Để làm điều này, bạn nên truy cập vào một trang thương mại điện tử yêu thích và bắt đầu quá trình mua một món hàng (nhưng dừng trước khi thực hiện thanh toán thực tế!). Sau khi thu thập các gói tin với Wireshark, bạn cần đặt bộ lọc để chỉ hiển thị các khung Ethernet có chứa các bản ghi SSL được gửi và nhận bởi máy của bạn. (Một bản ghi SSL có cùng ý nghĩa với một thông điệp SSL). Bạn cần có kết quả như hình chụp màn hình ở trang trước.

Nếu gặp khó khăn trong việc tạo dấu vết, bạn có thể tải tệp nén từ liên kết: <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> và giải nén tệp ssl-ethereal-trace-1 để sử dụng.

2. A look at the captured trace

Giao diện Wireshark của bạn nên chỉ hiển thị các khung Ethernet chứa các bản ghi SSL. Lưu ý rằng một khung Ethernet có thể chứa một hoặc nhiều bản ghi SSL. (Điều này khác biệt với HTTP, trong đó mỗi khung chứa toàn bộ thông điệp HTTP hoặc một phần của thông điệp HTTP). Ngoài ra, một bản ghi SSL có thể không hoàn toàn vừa với một khung Ethernet, và trong trường hợp đó cần nhiều khung để chứa toàn bộ bản ghi.

Mỗi khi có thể, khi trả lời một câu hỏi bên dưới, bạn nên in ra các gói tin trong dấu vết mà bạn sử dụng để trả lời câu hỏi đó. Chú thích bản in để giải thích câu trả lời của bạn. Để in một gói tin, sử dụng File->Print, chọn Selected packet only, chọn Packet summary line, và chọn mức chi tiết tối thiểu để trả lời câu hỏi.

Câu hỏi 1: Đối với 8 khung Ethernet đầu tiên, xác định nguồn của khung (máy khách hoặc máy chủ), xác định số lượng bản ghi SSL được bao gồm trong khung và liệt kê các loại bản ghi SSL được bao gồm trong khung đó. Vẽ sơ đồ thời gian giữa máy khách và máy chủ, với một mũi tên cho mỗi bản ghi SSL.

```

Frame 3: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}, id 0
  Section number: 1
    Interface id: 0 (\Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5})
      Interface name: \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}
      Interface description: Wi-Fi 2
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 17, 2024 14:53:33.739409000 SE Asia Standard Time
    UTC Arrival Time: Nov 17, 2024 07:53:33.739409000 UTC
    Epoch Arrival Time: 1731830013.739409000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.006378000 seconds]
    Frame Number: 3
    Frame Length: 200 bytes (1600 bits)
    Capture Length: 200 bytes (1600 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]

```

```

Frame 4: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}, id 0
  Section number: 1
    Interface id: 0 (\Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5})
      Interface name: \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}
      Interface description: Wi-Fi 2
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 17, 2024 14:53:33.739409000 SE Asia Standard Time
    UTC Arrival Time: Nov 17, 2024 07:53:33.739409000 UTC
    Epoch Arrival Time: 1731830013.739409000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.006378000 seconds]
    Frame Number: 4
    Frame Length: 116 bytes (928 bits)
    Capture Length: 116 bytes (928 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]

```



```

Frame 43: 2084 bytes on wire (16672 bits), 2084 bytes captured (16672 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585})
    Interface name: \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585}

    Interface description: Wi-Fi 2
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 17, 2024 14:53:34.204701000 SE Asia Standard Time
    UTC Arrival Time: Nov 17, 2024 07:53:34.204701000 UTC
    Epoch Arrival Time: 1731830014.204701000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000351000 seconds]
    [Time delta from previous displayed frame: 0.462197000 seconds]
    [Time since reference or first frame: 0.471670000 seconds]
    Frame Number: 43
    Frame Length: 2084 bytes (16672 bits)
    Capture Length: 2084 bytes (16672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]

```

```

Frame 48: 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585}, id 0
  Section number: 1
  Interface id: 0 (\Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585})
  Interface name: \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585}
  Interface description: Wi-Fi 2
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 17, 2024 14:53:34.255873000 SE Asia Standard Time
  UTC Arrival Time: Nov 17, 2024 07:53:34.255873000 UTC
  Epoch Arrival Time: 1731830014.255873000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.051172000 seconds]
  [Time since reference or first frame: 0.522842000 seconds]

Frame Number: 48
Frame Length: 308 bytes (2464 bits)
Capture Length: 308 bytes (2464 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:tls]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]

50 14:53:34.256504 192.168.1.230 143.92.82.17 TLSv1.3 134 Change Cipher Spec, Application Data
Frame 50: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585}, id 0
  Section number: 1
  Interface id: 0 (\Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585})
  Interface name: \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D70585}
  Interface description: Wi-Fi 2
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 17, 2024 14:53:34.256504000 SE Asia Standard Time
  UTC Arrival Time: Nov 17, 2024 07:53:34.256504000 UTC
  Epoch Arrival Time: 1731830014.256504000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000631000 seconds]
  [Time delta from previous displayed frame: 0.000631000 seconds]
  [Time since reference or first frame: 0.523473000 seconds]
  Frame Number: 50
  Frame Length: 134 bytes (1072 bits)
  Capture Length: 134 bytes (1072 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:tls]

[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: RuijieNetwor_4a:fb:4b (ec:b9:70:4a:fb:4b)

```

<p>Khung 3</p> <ul style="list-style-type: none"> • Nguồn: Máy chủ (13.35.186.15) • Đích: Máy khách (192.168.1.230) • Số lượng bản ghi SSL: 1 • Loại bản ghi SSL: Application Data 	<p>Khung 4</p> <ul style="list-style-type: none"> • Nguồn: Máy chủ (13.35.186.15) • Đích: Máy khách (192.168.1.230) • Số lượng bản ghi SSL: 1 • Loại bản ghi SSL: Application Data
<p>Khung 6</p> <ul style="list-style-type: none"> • Nguồn: Máy khách (192.168.1.230) • Đích: Máy chủ (13.35.186.15) • Số lượng bản ghi SSL: 1 • Loại bản ghi SSL: Application Data 	<p>Khung 7</p> <ul style="list-style-type: none"> • Nguồn: Máy chủ (13.35.186.15) • Đích: Máy khách (192.168.1.230) • Số lượng bản ghi SSL: 1 • Loại bản ghi SSL: Application Data
<p>Khung 9</p> <ul style="list-style-type: none"> • Nguồn: Máy chủ (13.35.186.15) 	<p>Khung 43</p> <ul style="list-style-type: none"> • Nguồn: Máy khách (192.168.1.230)

<ul style="list-style-type: none"> Đích: Máy khách (192.168.1.230) Số lượng bản ghi SSL: 1 Loại bản ghi SSL: Application Data 	<ul style="list-style-type: none"> Đích: Máy chủ (143.92.82.17) Số lượng bản ghi SSL: 1 Loại bản ghi SSL: Client Hello
<p>Khung 48</p> <ul style="list-style-type: none"> Nguồn: Máy chủ (13.35.186.17) Đích: Máy khách (192.168.1.230) Số lượng bản ghi SSL: 4 Loại bản ghi SSL: Server Hello, Change Cipher Spec, Application Data, Application Data 	<p>Khung 50</p> <ul style="list-style-type: none"> Nguồn: Máy khách (192.168.1.230) Đích: Máy chủ (13.35.186.17) Số lượng bản ghi SSL: 2 Loại bản ghi SSL: Change Cipher Spec, Application Data

Câu hỏi 2: Mỗi bản ghi SSL bắt đầu với ba trường giống nhau (có thể có giá trị khác nhau). Một trong các trường này là "content type" (loại nội dung) và có độ dài một byte. Liệt kê cả ba trường và độ dài của chúng.

Trong giao thức SSL/TLS, mỗi bản ghi bắt đầu với ba trường chính, như sau:

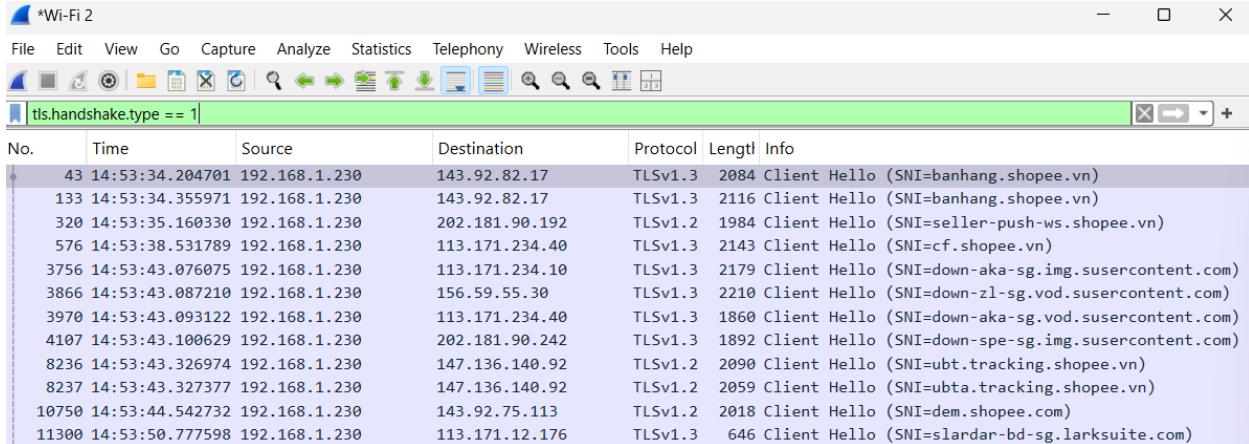
Content Type (Loại Nội Dung)	Version (Phiên Bản)
<ul style="list-style-type: none"> Mô tả: Trường này xác định loại bản ghi SSL/TLS, ví dụ: Handshake, Application Data, Change Cipher Spec. Độ dài: 1 byte. Giá trị ví dụ: 0x16 cho Handshake, 0x17 cho Application Data, 0x14 cho Change Cipher Spec. 	<ul style="list-style-type: none"> Mô tả: Trường này chỉ ra phiên bản SSL/TLS được sử dụng trong bản ghi. Độ dài: 2 byte. Giá trị ví dụ: 0x0301 cho TLS 1.0, 0x0303 cho TLS 1.2, 0x0304 cho TLS 1.3.

Length (Độ Dài)

- Mô tả:** Trường này cho biết độ dài của phần dữ liệu đi kèm trong bản ghi.
- Độ dài:** 2 byte.
- Giá trị ví dụ:** Giá trị này phụ thuộc vào kích thước của dữ liệu bên trong bản ghi.

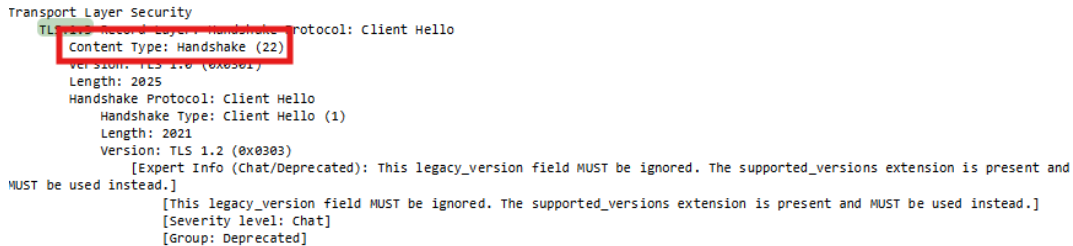
ClientHello Record

Sử dụng bộ lọc `tls.handshake.type == 1` trong Wireshark để chỉ hiển thị các gói tin có bản ghi ClientHello. (Trong giao thức TLS, 1 là mã định danh cho bản ghi ClientHello).



No.	Time	Source	Destination	Protocol	Length	Info
43	14:53:34.204701	192.168.1.230	143.92.82.17	TLSv1.3	2084	Client Hello (SNI=banhang.shopee.vn)
133	14:53:34.355971	192.168.1.230	143.92.82.17	TLSv1.3	2116	Client Hello (SNI=banhang.shopee.vn)
320	14:53:35.160330	192.168.1.230	202.181.90.192	TLSv1.2	1984	Client Hello (SNI=seller-push-ws.shopee.vn)
576	14:53:38.531789	192.168.1.230	113.171.234.40	TLSv1.3	2143	Client Hello (SNI=cf.shopee.vn)
3756	14:53:43.076075	192.168.1.230	113.171.234.10	TLSv1.3	2179	Client Hello (SNI=down-aka-sg.img.susercontent.com)
3866	14:53:43.087210	192.168.1.230	156.59.55.30	TLSv1.3	2210	Client Hello (SNI=down-zl-sg.vod.susercontent.com)
3970	14:53:43.093122	192.168.1.230	113.171.234.40	TLSv1.3	1860	Client Hello (SNI=down-aka-sg.vod.susercontent.com)
4107	14:53:43.100629	192.168.1.230	202.181.90.242	TLSv1.3	1892	Client Hello (SNI=down-spe-sg.img.susercontent.com)
8236	14:53:43.326974	192.168.1.230	147.136.140.92	TLSv1.2	2090	Client Hello (SNI=ubt.tracking.shopee.vn)
8237	14:53:43.327377	192.168.1.230	147.136.140.92	TLSv1.2	2059	Client Hello (SNI=ubta.tracking.shopee.vn)
10750	14:53:44.542732	192.168.1.230	143.92.75.113	TLSv1.2	2018	Client Hello (SNI=dem.shopee.com)
11300	14:53:50.777598	192.168.1.230	113.171.12.176	TLSv1.3	646	Client Hello (SNI=slardar-bd-sg.larksuite.com)

Câu hỏi 3: Mở rộng bản ghi ClientHello. (Nếu dấu vết của bạn chứa nhiều bản ghi ClientHello, hãy mở rộng khung chứa bản ghi đầu tiên). Giá trị của trường content type là gì?




```

Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 2025
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 2021
      Version: TLS 1.2 (0x0303)
      [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
      [This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
      [Severity level: Chat]
      [Group: Deprecated]
  
```

Trong gói tin ClientHello, trường Content Type có giá trị là 22 (0x16), đại diện cho loại bản ghi Handshake.

Câu hỏi 4: Bản ghi ClientHello có chứa một nonce (còn gọi là "challenge") không? Nếu có, giá trị của thách thức là gì dưới dạng mã thập lục phân?



```

Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 2025
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 2021
      Version: TLS 1.2 (0x0303)
      [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
      [This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
      [Severity level: Chat]
      [Group: Deprecated]
      Random: ae83c4246a15b81b693556669134ecb06ebc35136e4d09372c7d7ee6d2ff30bb
    Session ID Length: 32
  
```


Có, bản ghi ClientHello chứa một nonce (challenge) trong trường Random. Giá trị nonce là: ae83c4246a15b81b693556669134ecb06ebc35136e4d09372c7d7ee6d2ff30bb.

Câu hỏi 5: Bản ghi ClientHello có liệt kê các bộ mật mã mà nó hỗ trợ không? Nếu có, trong bộ đầu tiên được liệt kê, thuật toán mã công khai, thuật toán mã hóa đối xứng và thuật toán băm là gì?

```
Cipher Suites Length: 32
Cipher Suites (16 suites)
Cipher Suite: Reserved (GREASE) (0xdada)
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 (0xc03b)
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)
```

Có, bản ghi ClientHello liệt kê các bộ mật mã mà máy khách hỗ trợ. Bộ mật mã đầu tiên được liệt kê là TLS_AES_128_GCM_SHA256 với các thành phần:

- Thuật toán mã công khai: Không có thuật toán mã công khai riêng lẻ trong bộ mật mã này, vì đây là một mã hóa tổng hợp cho TLS 1.3.
- Thuật toán mã hóa đối xứng: AES_128_GCM
- Thuật toán băm: SHA256

ServerHello Record

Sử dụng bộ lọc `tls.handshake.type == 2` trong Wireshark để chỉ hiển thị các gói tin chứa bản ghi ServerHello. (Trong giao thức TLS, 2 là mã định danh cho bản ghi ServerHello).

No.	Time	Source	Destination	Protocol	Length	Info
48	14:53:34.255873	143.92.82.17	192.168.1.230	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data,
137	14:53:34.401397	143.92.82.17	192.168.1.230	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data,
325	14:53:35.206011	202.181.90.192	192.168.1.230	TLSv1.2	1490	Server Hello
578	14:53:38.538157	113.171.234.40	192.168.1.230	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Data,
3847	14:53:43.086359	113.171.234.10	192.168.1.230	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Data,
4249	14:53:43.105312	156.59.55.30	192.168.1.230	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
4321	14:53:43.107152	113.171.234.40	192.168.1.230	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
5071	14:53:43.158031	202.181.90.242	192.168.1.230	TLSv1.3	1490	Server Hello, Change Cipher Spec, Application Data
8412	14:53:43.373089	147.136.140.92	192.168.1.230	TLSv1.2	204	Server Hello, Change Cipher Spec, Encrypted Handshak
8419	14:53:43.375224	147.136.140.92	192.168.1.230	TLSv1.2	204	Server Hello, Change Cipher Spec, Encrypted Handshak
10753	14:53:44.586618	143.92.75.113	192.168.1.230	TLSv1.2	204	Server Hello, Change Cipher Spec, Encrypted Handshak
11302	14:53:50.782528	113.171.12.176	192.168.1.230	TLSv1.3	309	Server Hello, Change Cipher Spec, Application Data,

Câu hỏi 6: Xác định bản ghi SSL ServerHello. Bản ghi này có chỉ định một bộ mật mã đã chọn không? Các thuật toán trong bộ mật mã đã chọn là gì?

```
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 128
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 124
Version: TLS 1.2 (0x0303)
[Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
[This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
[Severity level: chat]
[Group: Deprecated]
Random: ed9063ddfa6c66c56fc28bca8ebf626cd7e14e996194126a6285806fd827b77f
Session ID Length: 32
Session ID: c2eeb4814f691de5ff13a07f062b4e69a3ff8432b52b1f3a5802948653af714
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Compression Method: null (0)
Extensions Length: 52
Extension: supported_versions (len=2) TLS 1.3
Type: supported_versions (43)
Length: 2
Supported Version: TLS 1.3 (0x0304)
Extension: key_share (len=36) X25519
Type: key_share (51)
Length: 36
Key Share extension
Key Share Entry: Group: X25519, Key Exchange length: 32
Group: X25519 (29)
Key Exchange Length: 32
Key Exchange: 060fb3bfa5a100d9a2ee10b3ab87510e9703abdd68142f4bdc7df35f6977de78
Extension: pre_shared_key (len=2)
Type: pre_shared_key (41)
Length: 2
Pre-Shared Key extension
Selected Identity: 0
[JA3S Fullstring: 771,4866,43-51-41]
[JA3S: 2253c82f09b621c5144709b393fde2c9]
```

Trong bản ghi ServerHello, bộ mật mã đã chọn là TLS_AES_256_GCM_SHA384. Bộ này bao gồm:

- Thuật toán mã hóa đối xứng: AES 256 trong chế độ GCM (Galois/Counter Mode)
- Thuật toán băm: SHA-384

Câu hỏi 7: Bản ghi này có chứa một nonce không? Nếu có, nó dài bao nhiêu? Mục đích của các nonce của máy khách và máy chủ trong SSL là gì?

```
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 128
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 124
Version: TLS 1.2 (0x0303)
[Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
[This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
[Severity level: chat]
[Group: Deprecated]
Random: ed9063ddfa6c66c56fc28bca8ebf626cd7e14e996194126a6285806fd827b77f
Session ID Length: 32
Session ID: c2eeb4814f691de5ff13a07f062b4e69a3ff8432b52b1f3a5802948653af714
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Compression Method: null (0)
Extensions Length: 52
Extension: supported_versions (len=2) TLS 1.3
Type: supported_versions (43)
Length: 2
Supported Version: TLS 1.3 (0x0304)
Extension: key_share (len=36) X25519
Type: key_share (51)
Length: 36
Key Share extension
Key Share Entry: Group: X25519, Key Exchange length: 32
Group: X25519 (29)
Key Exchange Length: 32
Key Exchange: 060fb3bfa5a100d9a2ee10b3ab87510e9703abdd68142f4bdc7df35f6977de78
Extension: pre_shared_key (len=2)
Type: pre_shared_key (41)
Length: 2
Pre-Shared Key extension
Selected Identity: 0
[JA3S Fullstring: 771,4866,43-51-41]
[JA3S: 2253c82f09b621c5144709b393fde2c9]
```

Có, bản ghi ServerHello chứa một nonce trong trường Random. Nonce này có độ dài 32 byte, giá trị:

ed9063ddfafc66c56fc28bca8ebf626cd7e14e996194126a6285806fd827b77f.

Mục đích: Các nonce của máy khách và máy chủ được sử dụng để tạo ra các khóa mã hóa duy nhất cho mỗi phiên, giúp đảm bảo tính bảo mật và độc nhất cho mỗi phiên SSL/TLS.

Câu hỏi 8: Bản ghi này có chứa một ID phiên không? Mục đích của ID phiên là gì?

```
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 128
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 124
Version: TLS 1.2 (0x0303)
[Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
[This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
[Severity level: Chat]
[Group: Suppressed]
Random: ed9063ddfafc66c56fc28bca8ebf626cd7e14e996194126a6285806fd827b77f
Session ID Length: 32
Session ID: c2eeb4814f691de5ff13a07f062b4e69a3f7f8432b52b1f3a5802948653af714
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Compression Method: null (0)
Extensions Length: 52
Extension: supported_versions (len=2) TLS 1.3
Type: supported_versions (43)
Length: 2
Supported Version: TLS 1.3 (0x0304)
Extension: key_share (len=36) x25519
Type: key_share (51)
Length: 36
Key Share extension
Key Share Entry: Group: x25519, Key Exchange length: 32
Group: x25519 (29)
Key Exchange Length: 32
Key Exchange: 060fb3bfa5a100d9a2ee10b3ab87510e9703abdd68142f4bdc7df35f6977de78
Extension: pre_shared_key (len=2)
Type: pre_shared_key (41)
Length: 2
Pre-Shared Key extension
Selected Identity: 0
[JA3S Fullstring: 771,4866,43-51-41]
[JA3S: 2253c82f03b621c5144709b393fde2c9]
```

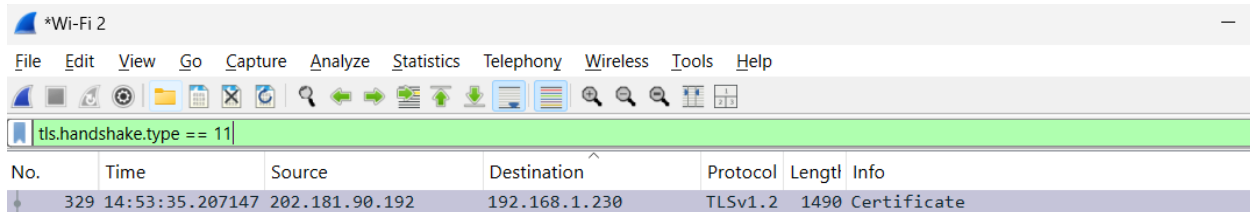
Có, bản ghi ServerHello chứa một Session ID với giá trị: c2eeb4814f691de5ff13a07f062b4e69a3f7f8432b52b1f3a5802948653af714.

Mục đích của Session ID: Session ID giúp duy trì trạng thái phiên giữa máy khách và máy chủ, cho phép các phiên SSL/TLS tái sử dụng khóa mã hóa đã thương lượng trước đó, từ đó giảm thời gian thiết lập kết nối cho các lần kết nối tiếp theo.

Câu hỏi 9: Bản ghi này có chứa một chứng chỉ không, hay chứng chỉ được bao gồm trong một bản ghi riêng biệt? Chứng chỉ có vừa với một khung Ethernet không?

Bản ghi ServerHello không chứa chứng chỉ. Thay vào đó, chứng chỉ của máy chủ thường được gửi trong một bản ghi riêng có loại Certificate.

Kích thước của chứng chỉ: Chứng chỉ thường khá dài và có thể không vừa trong một khung Ethernet duy nhất, do đó, nó có thể cần được chia thành nhiều khung.



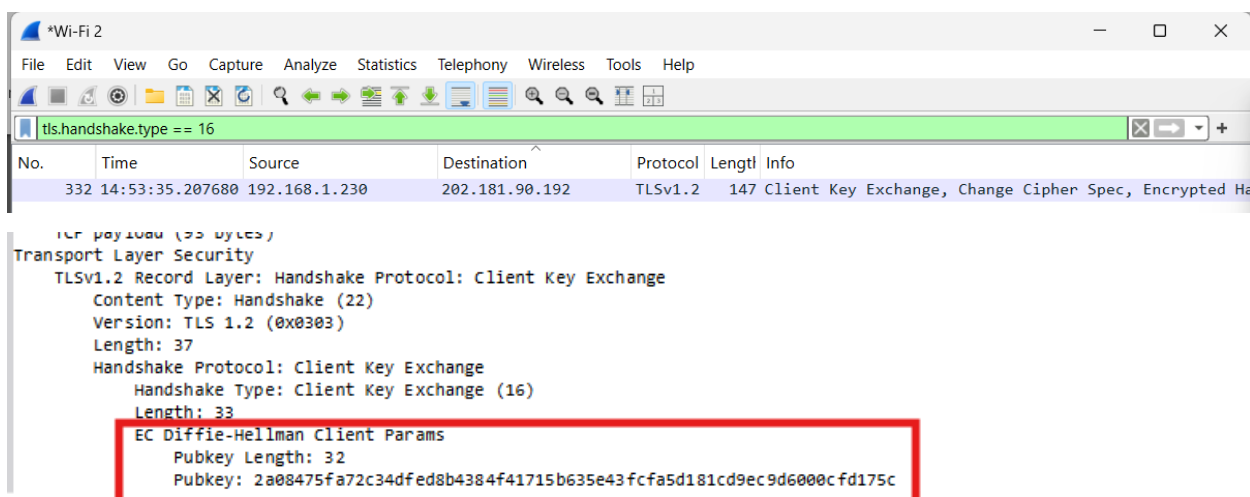
No.	Time	Source	Destination	Protocol	Length	Info
329	14:53:35.207147	202.181.90.192	192.168.1.230	TLSv1.2	1490	Certificate

Để tìm bản ghi Certificate, ta có thể sử dụng bộ lọc `tls.handshake.type == 11` trong Wireshark, vì bản ghi này không nằm trong ServerHello mà được gửi trong một bản ghi riêng biệt.

Client Key Exchange Record

Câu 10: Xác định bản ghi trao đổi khóa của máy khách. Bản ghi này có chứa một bí mật sơ bộ không? Bí mật này được dùng để làm gì? Bí mật này có được mã hóa không? Nếu có, nó dài bao nhiêu?

Trong giao thức TLS, bản ghi trao đổi khóa của máy khách có thể được tìm thấy trong các gói tin thuộc loại Client Key Exchange (TLS 1.2 trở xuống) hoặc Key Share (TLS 1.3). Sử dụng bộ lọc sau để tìm gói tin này: TLS 1.2 trở xuống: `tls.handshake.type == 16`; TLS 1.3: `tls.handshake.type == 1` (ClientHello) và tìm trường **Key Share** trong gói tin này.



No.	Time	Source	Destination	Protocol	Length	Info
332	14:53:35.207680	192.168.1.230	202.181.90.192	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

```

Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 37
    Handshake Protocol: Client Key Exchange
      Handshake Type: Client Key Exchange (16)
      Length: 33
      EC Diffie-Hellman Client Params
        Pubkey Length: 32
        Pubkey: 2a08475fa72c34dfed8b4384f41715b635e43fcfa5d181cd9ec9d600cfd175c
  
```

Bản ghi chứa bí mật sơ bộ: Bản ghi Client Key Exchange có chứa bí mật sơ bộ dưới dạng các tham số khóa công khai của khách hàng trong quá trình trao đổi khóa Diffie-Hellman (EC Diffie-Hellman Client Params).

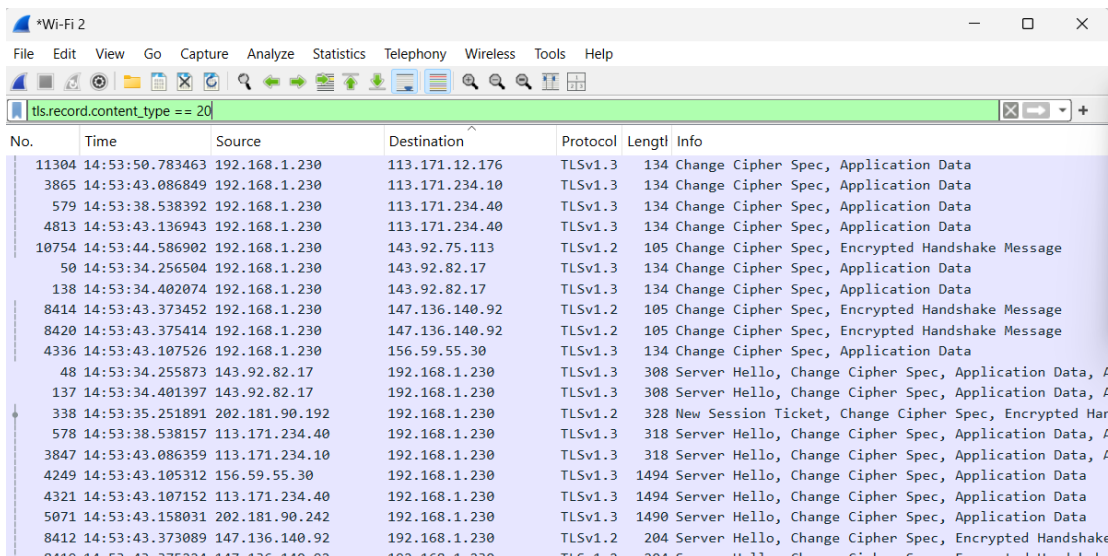
Mục đích của bí mật sơ bộ: Bí mật sơ bộ này được sử dụng để tạo khóa phiên giữa máy khách và máy chủ. Khóa phiên này sẽ được dùng để mã hóa và giải mã dữ liệu trong suốt phiên SSL/TLS nhằm bảo đảm tính bảo mật và toàn vẹn của dữ liệu.

Mã hóa bí mật sơ bộ: Trong phương thức EC Diffie-Hellman, bí mật sơ bộ không được mã hóa trực tiếp bằng khóa công khai của máy chủ. Thay vào đó, nó được trao đổi theo cách mà cả hai bên có thể tạo ra khóa phiên chung mà không cần truyền khóa thực tế.

Độ dài của bí mật sơ bộ: Bí mật sơ bộ có độ dài 32 byte.

Change Cipher Spec Record (sent by client) and Encrypted Handshake Record

Sử dụng bộ lọc `tls.record.content_type == 20` trong Wireshark để tìm các gói tin có chứa bản ghi Change Cipher Spec (Loại bản ghi này có giá trị 20).



No.	Time	Source	Destination	Protocol	Length	Info
11304	14:53:50.783463	192.168.1.230	113.171.12.176	TLSv1.3	134	Change Cipher Spec, Application Data
3865	14:53:43.086849	192.168.1.230	113.171.234.10	TLSv1.3	134	Change Cipher Spec, Application Data
579	14:53:38.538392	192.168.1.230	113.171.234.40	TLSv1.3	134	Change Cipher Spec, Application Data
4813	14:53:43.136943	192.168.1.230	113.171.234.40	TLSv1.3	134	Change Cipher Spec, Application Data
10754	14:53:44.586902	192.168.1.230	143.92.75.113	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
50	14:53:34.256504	192.168.1.230	143.92.82.17	TLSv1.3	134	Change Cipher Spec, Application Data
138	14:53:34.402074	192.168.1.230	143.92.82.17	TLSv1.3	134	Change Cipher Spec, Application Data
8414	14:53:43.373452	192.168.1.230	147.136.140.92	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
8420	14:53:43.375414	192.168.1.230	147.136.140.92	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
4336	14:53:43.107526	192.168.1.230	156.59.55.30	TLSv1.3	134	Change Cipher Spec, Application Data
48	14:53:34.255873	143.92.82.17	192.168.1.230	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data, A
137	14:53:34.401397	143.92.82.17	192.168.1.230	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data, A
338	14:53:35.251891	202.181.90.192	192.168.1.230	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake
578	14:53:38.538157	113.171.234.40	192.168.1.230	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Data, A
3847	14:53:43.086359	113.171.234.10	192.168.1.230	TLSv1.3	318	Server Hello, Change Cipher Spec, Application Data, A
4249	14:53:43.105312	156.59.55.30	192.168.1.230	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
4321	14:53:43.107152	113.171.234.40	192.168.1.230	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
5071	14:53:43.158031	202.181.90.242	192.168.1.230	TLSv1.3	1490	Server Hello, Change Cipher Spec, Application Data
8412	14:53:43.373089	147.136.140.92	192.168.1.230	TLSv1.2	204	Server Hello, Change Cipher Spec, Encrypted Handshake
8418	14:53:43.375224	147.136.140.92	192.168.1.230	TLSv1.2	204	Server Hello, Change Cipher Spec, Encrypted Handshake

Câu 11: Mục đích của bản ghi Đổi Bộ Mã là gì? Số byte của bản ghi này trong dấu vết của bạn là bao nhiêu?

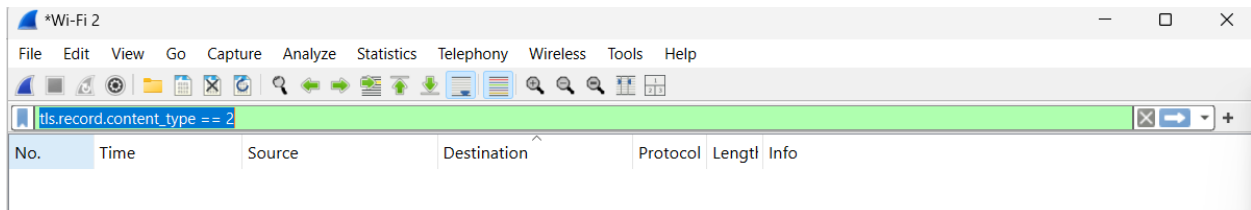
Mục đích của bản ghi Change Cipher Spec là báo hiệu cho phía đối tác (máy chủ hoặc máy khách) rằng từ thời điểm này trở đi, tất cả dữ liệu sẽ được mã hóa và giải mã bằng khóa phiên vừa thiết lập trong quá trình trao đổi khóa.

Trong gói tin chứa bản ghi Change Cipher Spec, xem trường Length để xác định số byte của bản ghi này. Bản ghi Change Cipher Spec chỉ có 1 byte.

```
TCP payload (80 bytes)
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: 69
    Encrypted Application Data:
    ed648c1c7a5c801d238c62855ff10e3dc71ee15970b97d8c02422313cad4bea9b2da816f2b509ae659a1a00c77eae1ad313267
    [Application Data Protocol: Hypertext Transfer Protocol]
  [community ID: 1:TIh8EPFChi75M01GP5ZU7hFKpE=]
```

Câu 12: Trong bản ghi bắt tay đã mã hóa, cái gì được mã hóa? Bằng cách nào?

Sử dụng bộ lọc `tls.handshake.type == 22` trong Wireshark để tìm các gói tin chứa bản ghi Encrypted Handshake Message. Loại bản ghi này thường là bản ghi Finished và có thể xuất hiện sau bản ghi Change Cipher Spec.



Bản ghi Encrypted Handshake Message chứa bản ghi Finished, là thông điệp cuối cùng của quy trình bắt tay SSL/TLS và được mã hóa để đảm bảo rằng cả hai bên đều có cùng khóa phiên. Nội dung của bản ghi Finished bao gồm một giá trị xác thực được tạo dựa trên tất cả các bản ghi bắt tay trước đó.

Bản ghi này được mã hóa bằng khóa phiên (session key) được tạo ra sau khi trao đổi khóa giữa máy khách và máy chủ. Phương thức mã hóa phụ thuộc vào bộ mật mã đã chọn, ví dụ như AES-GCM trong trường hợp của TLS_AES_256_GCM_SHA384.

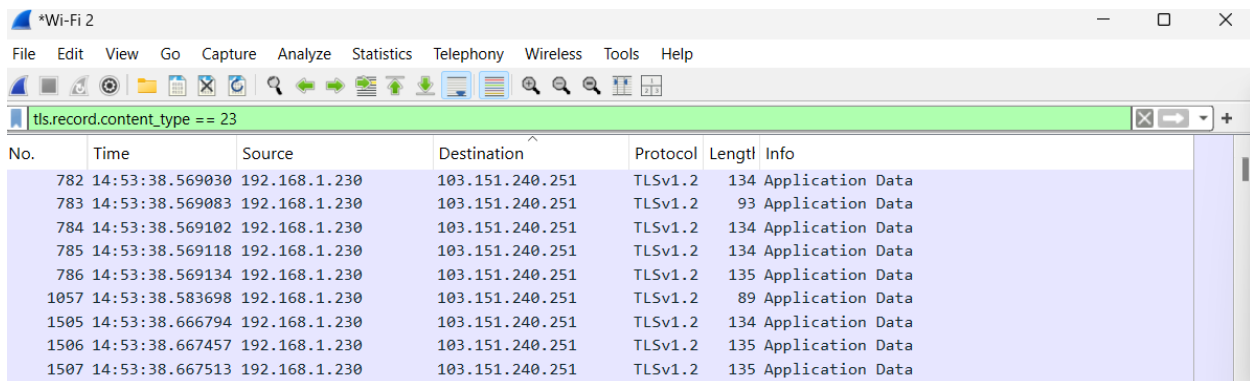
Câu 13: Máy chủ cũng có gửi một bản ghi đổi bộ mã và bản ghi bắt tay đã mã hóa cho máy khách không? Các bản ghi này có khác biệt so với các bản ghi được gửi bởi máy khách không?

Bản ghi Change Cipher Spec từ máy khách và máy chủ có cùng mục đích, nhưng được gửi từ các phía khác nhau để báo hiệu rằng mỗi bên đã sẵn sàng sử dụng mã hóa.

Bản ghi Encrypted Handshake Message từ máy chủ cũng chứa giá trị xác thực cho tất cả các bản ghi trước đó, tương tự như của máy khách, nhưng sẽ có giá trị khác biệt do quá trình mã hóa và các tham số khác nhau.

Application Data

Sử dụng bộ lọc `tls.record.content_type == 23` trong Wireshark để tìm các gói tin chứa bản ghi Application Data. Loại bản ghi này chứa dữ liệu ứng dụng đã được mã hóa.



No.	Time	Source	Destination	Protocol	Length	Info
782	14:53:38.569030	192.168.1.230	103.151.240.251	TLSv1.2	134	Application Data
783	14:53:38.569083	192.168.1.230	103.151.240.251	TLSv1.2	93	Application Data
784	14:53:38.569102	192.168.1.230	103.151.240.251	TLSv1.2	134	Application Data
785	14:53:38.569118	192.168.1.230	103.151.240.251	TLSv1.2	134	Application Data
786	14:53:38.569134	192.168.1.230	103.151.240.251	TLSv1.2	135	Application Data
1057	14:53:38.583698	192.168.1.230	103.151.240.251	TLSv1.2	89	Application Data
1505	14:53:38.666794	192.168.1.230	103.151.240.251	TLSv1.2	134	Application Data
1506	14:53:38.667457	192.168.1.230	103.151.240.251	TLSv1.2	135	Application Data
1507	14:53:38.667513	192.168.1.230	103.151.240.251	TLSv1.2	135	Application Data

Câu 14: Dữ liệu ứng dụng được mã hóa như thế nào? Các bản ghi chứa dữ liệu ứng dụng có bao gồm MAC không? Wireshark có phân biệt được giữa dữ liệu ứng dụng đã mã hóa và MAC không?

```

Transport Layer Security
  TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 141
    Encrypted Application Data [...]:
b9aa177a035c6620ee49c1b394a26757f44a645b0401534bd743ec16636a96345f7114cf309187a14902c910748475d57cd5a393107475b1fbef399c4343209e09d62eeea8edf2
    [Application Data Protocol: Hypertext Transfer Protocol]
[Community ID: 1:Nm/ugrKNwEwfflc/agriHdR7bc=]
Spirent Test Center Signature
  Raw Data: 2dd31bd19f765fa9f5e6844e6320f0e3908613ee
  IV: 0x2d
  StreamID: 2059157496
    ChassisSlotPort: 31420
    0... .. = StreamType: Soft
    Stream Index: 16376
  Sequence Number (SN): 215846011257298
  Timestamp: 104.389659893 seconds
    ... .. = Pseudo-Random Binary Sequence: False
    ... .. = TLSR: StartOfFrame
  Unknown: 908613ee
  
```

Phương thức mã hóa: Dữ liệu ứng dụng trong bản ghi Application Data được mã hóa bằng phương thức AES 256 GCM, dựa trên bộ mật mã đã thương lượng trong quá trình bắt tay SSL/TLS. GCM (Galois/Counter Mode) là chế độ mã hóa tích hợp xác thực, giúp đảm bảo tính toàn vẹn và bảo mật cho dữ liệu truyền tải.

Sự hiện diện của MAC: Trong chế độ GCM, MAC được tích hợp vào quá trình mã hóa, do đó không có MAC riêng biệt cho từng bản ghi dữ liệu.

Khả năng của Wireshark: Wireshark hiển thị dữ liệu ứng dụng đã mã hóa dưới dạng Application Data mà không phân biệt rõ ràng giữa dữ liệu và MAC, vì MAC đã được tích hợp trong mã hóa GCM.

Câu 15: Bình luận và giải thích bất cứ điều gì mà bạn thấy thú vị trong dấu vết.

Trong dấu vết này, quá trình bắt tay SSL/TLS sử dụng bộ mật mã TLS_AES_256_GCM_SHA384, một bộ mật mã mạnh mẽ với mã hóa AES 256-bit và hàm băm SHA-384, đảm bảo mức độ bảo mật cao cho kết nối. Điểm đáng chú ý là cả máy khách và máy chủ đều gửi bản ghi Change Cipher Spec trước khi chuyển sang mã hóa dữ liệu, báo hiệu rằng mỗi bên đã đồng thuận về việc bắt đầu mã hóa phiên. Tất cả dữ liệu ứng dụng sau đó được mã hóa hoàn toàn, đảm bảo tính bí mật và an toàn cho thông tin trao đổi.