BÀI BÁO CÁO LAB 1

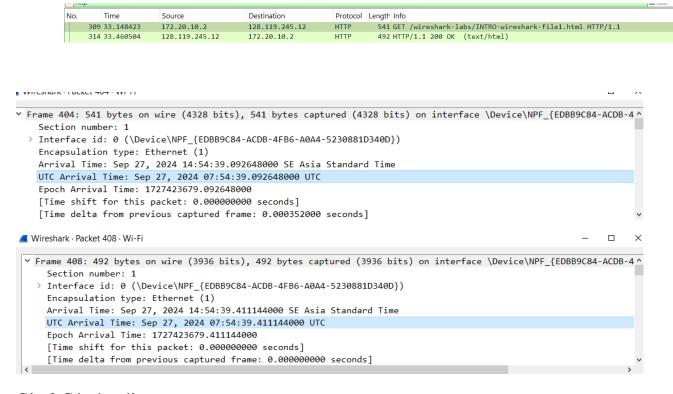
Họ và tên: Bùi Lê Nhật Tri

MSSV: 23521634

Mã môn IT005.P119.2

Câu 1. Tổng thời gian bắt gói tin trong web gaia.cs. umass.edu: 0.318496,

Có tổng cộng 2 gói bắt được



Câu 2.Có các gói:

- TCP: Đảm bảo truyền dữ liệu tin cậy giữa các máy tính trên mạng. TCP chia dữ liệu thành các gói nhỏ, gửi đi và kiểm tra xem tất cả các gói đã đến đích chưa. Nếu có gói bị mất, TCP sẽ yêu cầu gửi lại.
- ICMP: Được sử dụng để gửi các thông báo lỗi và điều khiển giữa các thiết bị trên mạng, giúp chúng có thể giao tiếp và giải quyết các vấn đề phát sinh.
- TLSv1.3: Là giao thức bảo mật được sử dụng rộng rãi để mã hóa các kết nối giữa trình duyệt và máy chủ web, đảm bảo sự riêng tư và toàn vẹn của dữ liệu truyền đi trên Internet.

- DNS: Chuyển đổi tên miền (ví dụ: viettuans.vn) thành địa chỉ IP (ví dụ: 123.45.67.89) để máy tính có thể tìm thấy máy chủ của website đó.
- HTTP: Giao thức dùng để truyền tải các trang web. Khi bạn nhập địa chỉ một website vào trình duyệt, trình duyệt sẽ gửi một yêu cầu HTTP đến máy chủ web, và máy chủ sẽ trả về nội dung của trang web đó.

3 0.156815	203.167.11.211	172.20.10.2	TCP	66 443 → 49980 [ACK] Seg=1 Ack=2 Win=420 Len=0 SLE=1 SRE=2
4 2 . 576642	172.20.10.2	118.69.123.140	ICMP	74 Echo (ping) request id=0x0001, seq=123/31488, ttl=64 (no respon
4 2.370042	172.20.10.2	110.05.125.140	10111	74 ECHO (PING) FEGUESE 10-0x0001; Seq-123/31400; EE1-04 (NO FESPONIII
85 5.907482	172.20.10.2	113.171.10.154	TLSv1.	3 134 Change Cipher Spec, Application Data
86 5.907741	172.20.10.2	113.171.10.154	TLSv1.	3 146 Application Data
101 0.423200	1/4.40.10.4	0.0.0.0	בווט	of Standard Query Oxuoad A logger. Toxittiodd.com
102 6.500874	8.8.8.8	172.20.10.2	DNS 1	L62 Standard query response 0xd0ad No such name A logger.foxitcloud
103 6.615287	172.20.10.2	8.8.8.8	DNS	81 Standard query 0x5b46 A logger.foxitcloud.com
141 /.00/7/2	1/2.20.10.2	200.107.11.211	TUF	אס ב אסממר → סמ [Ack] אפן אסר אברד-וודא סררסד-אסר אר (Ack) אריים אין אספר אר
142 7.868958	203.167.11.211	172.20.10.2	HTTP	326 HTTP/1.1 200 OK (text/html)
143 7.869007	172.20.10.2	203.167.11.211	TCP	54 50002 → 80 [ACK] Seq=465 Ack=16610 Win=131840 Len=0

Câu 3. Tổng thời gian bắt gói tin trong web gaia.cs.umass.edu: 0.318496

```
✓ Frame 404: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF_{EDBB9C84-ACDB-4 ^
    Section number: 1
  > Interface id: 0 (\Device\NPF_{EDBB9C84-ACDB-4FB6-A0A4-5230881D340D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 27, 2024 14:54:39.092648000 SE Asia Standard Time
   UTC Arrival Time: Sep 27, 2024 07:54:39.092648000 UTC
    Epoch Arrival Time: 1727423679.092648000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000352000 seconds]
■ Wireshark · Packet 408 · Wi-Fi
 Y Frame 408: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{EDBB9C84-ACDB-4 ^
     Section number: 1
   > Interface id: 0 (\Device\NPF_{EDBB9C84-ACDB-4FB6-A0A4-5230881D340D})
     Encapsulation type: Ethernet (1)
     Arrival Time: Sep 27, 2024 14:54:39.411144000 SE Asia Standard Time
     UTC Arrival Time: Sep 27, 2024 07:54:39.411144000 UTC
     Epoch Arrival Time: 1727423679.411144000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.000000000 seconds]
```

Tổng thời gian bắt gói tin trong web sv.ktxhcm.edu.vn: 0.095848999

```
Wireshark Packet 44 · Wi-Fi

✓ Frame 44: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface \Device\NPF_{EDBB9C84-ACDB-4F ^ Section number: 1

> Interface id: 0 (\Device\NPF_{EDBB9C84-ACDB-4FB6-A0A4-5230881D340D})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 27, 2024 15:04:56.499810000 SE Asia Standard Time

UTC Arrival Time: Sep 27, 2024 08:04:56.499810000 UTC

Epoch Arrival Time: 1727424296.499810000

[Time shift for this packet: 0.0000000000 seconds]

[Time delta from previous captured frame: 0.000513000 seconds]

✓
```

Câu 4. Nội dung hiển thị trên trang web gaia.cs.umass.edu

"Congratulations! You've downloaded the first Wireshark lab file!"

CÓ nằm trong các gói tin HTTP bắt được

```
✓ Line-based text data: text/html (3 lines)
    Congratulations! You've downloaded the first Wireshark lab file!\n
    </html>\n
0130 67 74 68 3a 20 38 31 0d 0a 4b 65 65 70 2d 41 6c 0140 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20
                                                                gth: 81 - Keep-Al
                                                               ive: tim eout=5,
0150 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74
                                                               max=100 - Connect
0160 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d
                                                                ion: Kee p-Alive
·Content -Type: t
0180 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65
                                                                ext/html; charse
0190 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c
                                                                t=UTF-8· ···<html
                                                                > Congra tulations! You' ve downl
       <mark>3e 0a</mark> 43 6f 6e 67 72 61  74 75 6c 61 74 69 6f 6e
73 21 20 20 59 6f 75 27  76 65 20 64 6f <mark>77</mark> 6e 6c
01a0 3e 0a 43 6f
01h0
                                                                oaded th e first
01c0 6f 61 64 65 64 20 74 68 65 20 66 69 72 73 74 20
91d9
        57 69 72 65 73 68 61 72  6b 20 6c 61 62 20 66 69
       <mark>6c 65 21 0a</mark> 3c 2f 68 74 6d 6c 3e 0a
                                                                 le! </ht ml>.
01e0
```

Câu 5. Đia chỉ của gaia.cs.umass.edu:

```
Header Checksum: 0xb240 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.20.10.2
Destination Address: 128.119.245.12
[Stream index: 15]
```

Địa chỉ của sv.ktxhcm.edu.vn là:

```
Identification: 0x2898 (10392)

> 010. ... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: TCP (6)

Header Checksum: 0x824c [validation disabled]

[Header checksum status: Unverified]

Source Address: 172.20.10.2

Destination Address: 203.167.11.211

[Stream index: 11]
```

Địa chỉ của máy tính đang sử dụng là:

314 33.460504 128.119.245.12 172.20.10.2 HTTP 492 HTTP/1.1 200 OK (text/html)

Câu 6: Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó:

- -Sau khi có địa chỉ IP của trang web từ việc phân giải URL qua máy chủ DNS, trình duyệt thiết lập kết nối TCP đến máy chủ web qua cổng 80 (nếu là HTTP) hoặc cổng 443 (nếu là HTTPS)
- -Trình duyệt gửi yêu cầu GET đến máy chủ để lấy nội dung trang web. Sau khi xử lý yêu cầu, máy chủ sẽ gửi lại dữ liệu của trang web, trình duyệt nhận dữ liệu, tải các tài nguyên cần thiết như hình ảnh,...sau đấy dựng thành trang web và hiển thị ra màn hình để người dùng xem và tương tác.