

MÔN TRIỂN KHAI AN NINH HỆ THỐNG

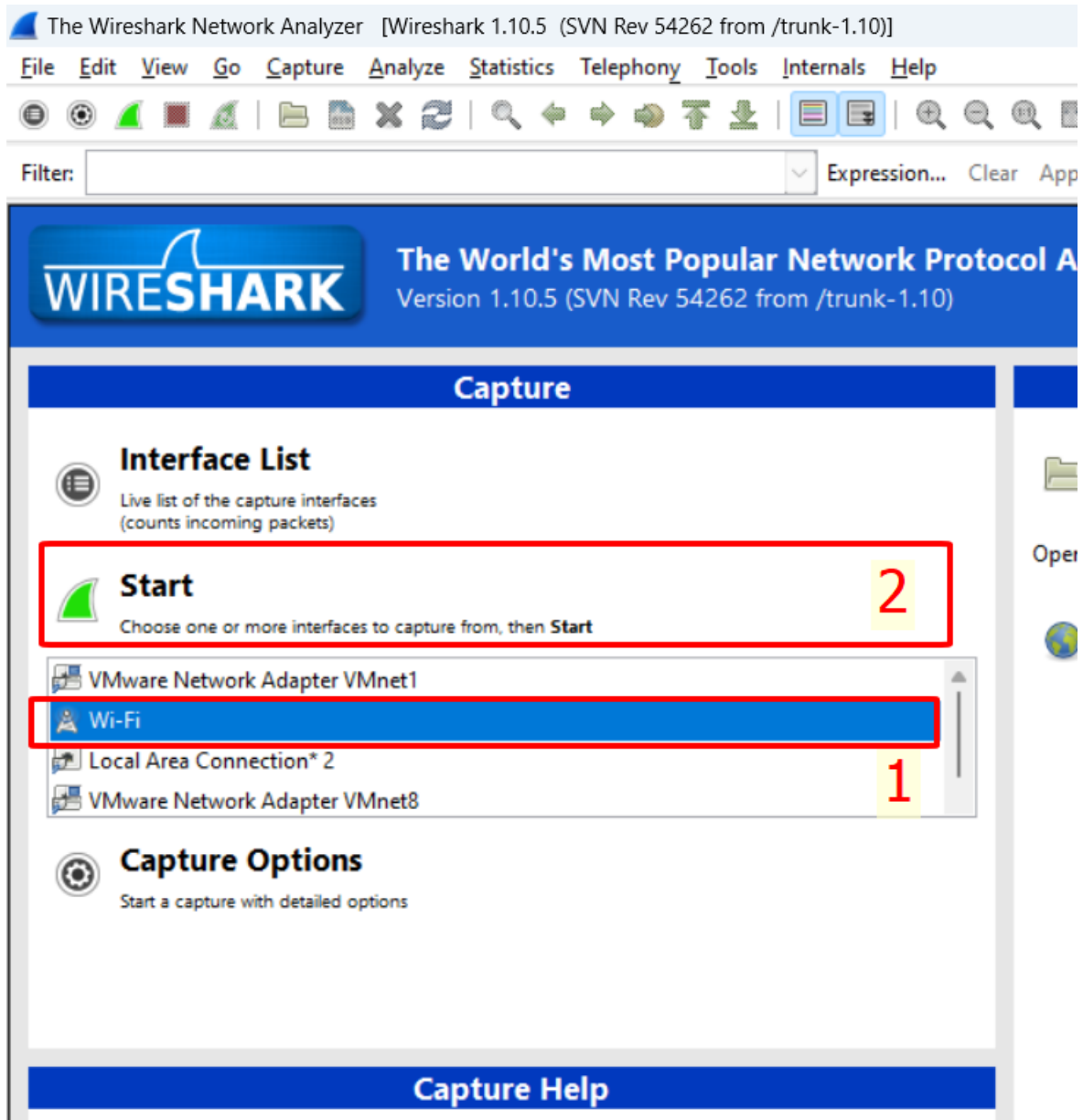
TH02 – Lab03 – WireShark

Phúc Lâm - 08/09/2024

I. TÌM HIỂU QUA BỘ TÀI LIỆU

II. Thực hành phân tích gói tin với Wireshark

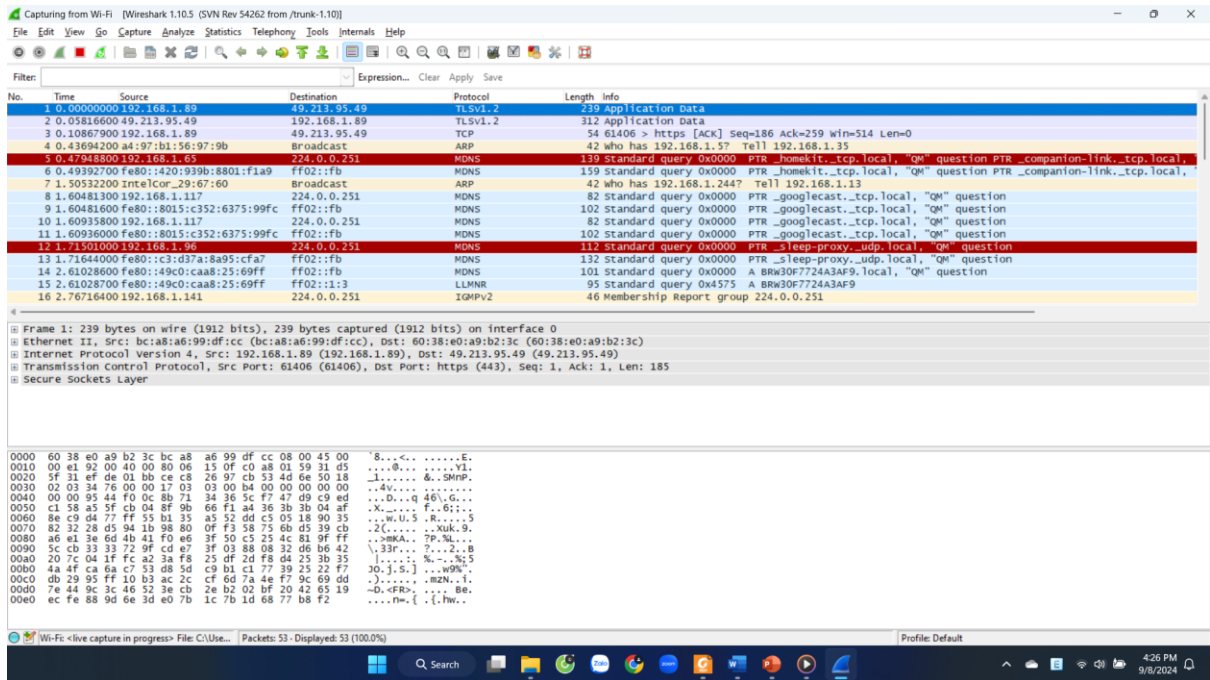
1. Khởi động ứng dụng Wireshark



Bước 1: cài đặt WinPcap_4_1_3.exe và Wireshark-win64-1.10.5.exe

Bước 2: Khởi động Wireshark, chọn loại mạng cần quét. Sau đó nhấn “Start”

Bước 3: Xem kết quả của việc bắt gói tin



2. Thực hành phân tích gói tin với Wireshark

- Mục tiêu:

- Thực nghiệm kiến thức mô hình TCP/IP
- Hiểu cấu trúc các header cơ bản trường ở gói tin thu thập được

- Công cụ: sử dụng công cụ “Wireshark”

- Các mục chính

- Phân tích quá trình ping
- Phân tích quá trình kết nối HTTP

a) Phân tích quá trình ping

- Bước 1: Mở wireshark và capture ở trên card mạng có kết nối internet

- Cài đặt và mở wireshark như trên
- Chọn card mạng “Hợp lý” để capture
- Ở đây tôi chọn “Wi-fi”

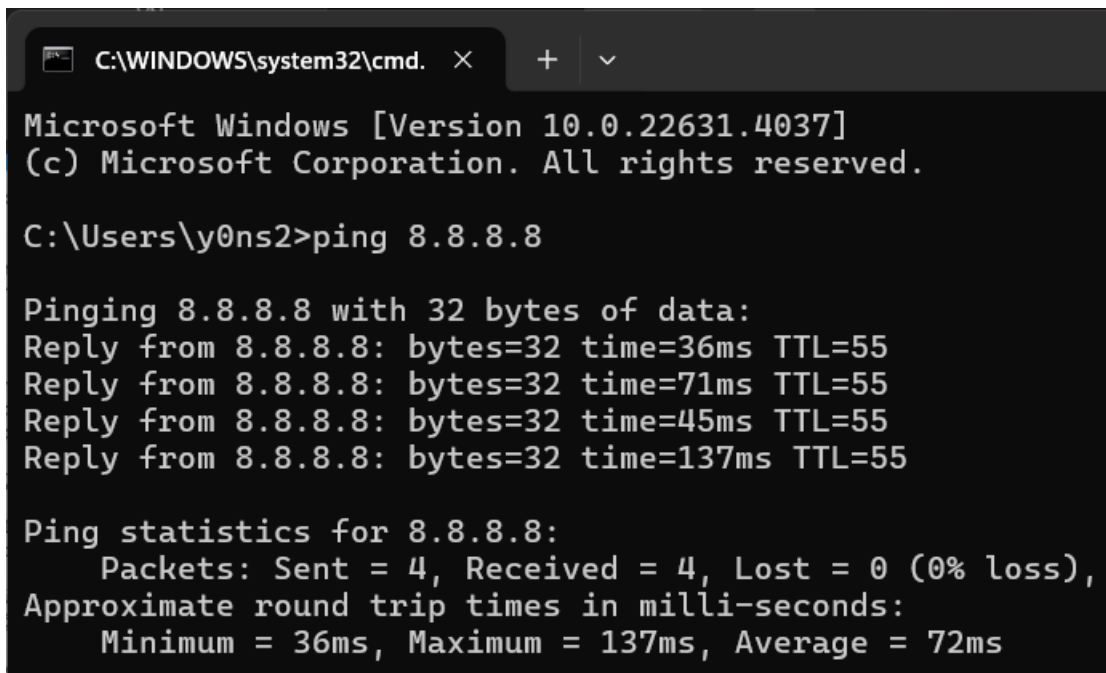
- Bước 2: vào cmd của máy tính ping 8.8.8.8

- Ipconfig

Wireless LAN adapter Wi-Fi:

```
Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::a5dd:e1b3:5530:cfbf%15
IPv4 Address. . . . . : 192.168.1.89
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
```

- **Ping 8.8.8.8**



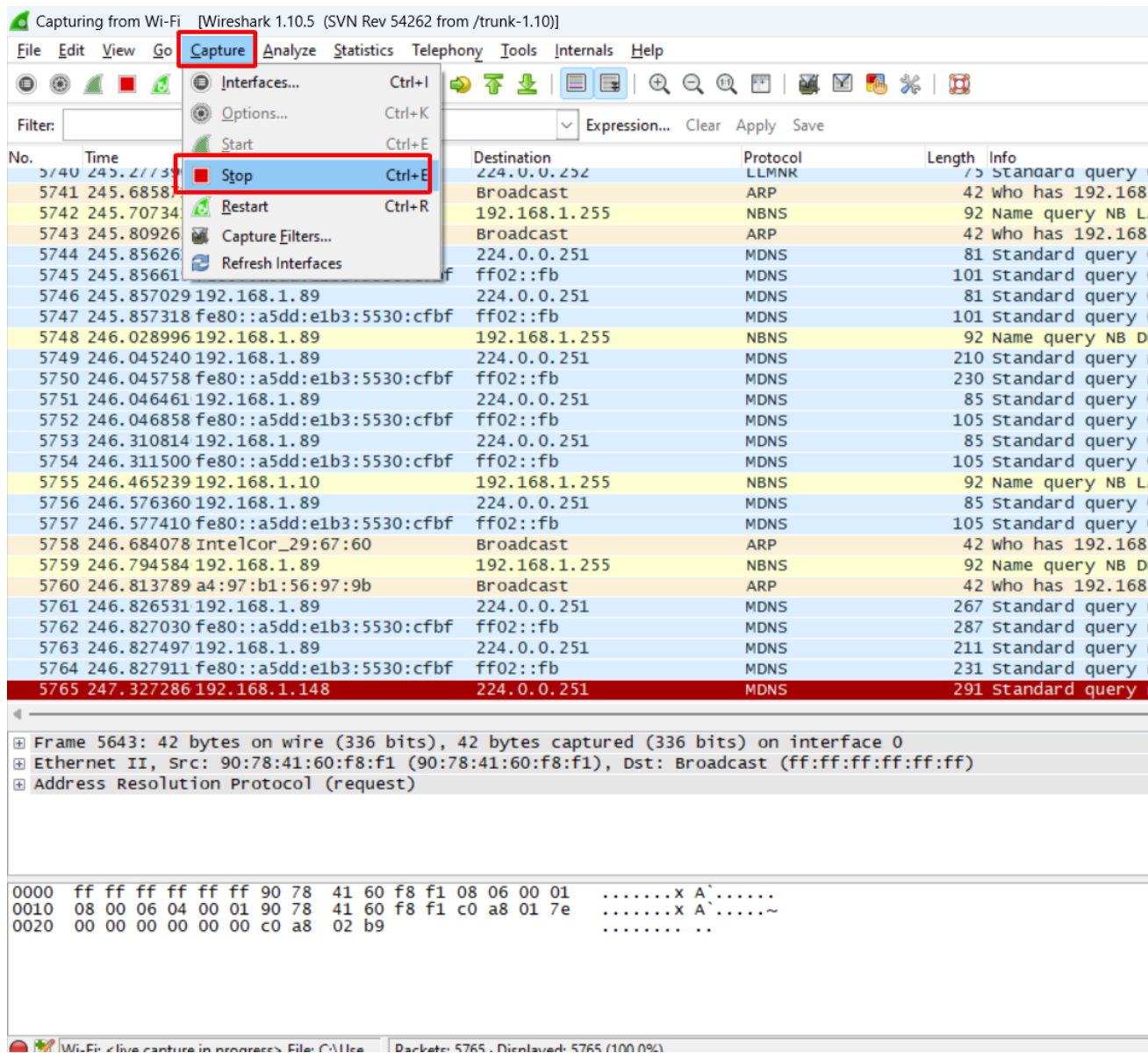
```
C:\WINDOWS\system32\cmd. X + v
Microsoft Windows [Version 10.0.22631.4037]
(c) Microsoft Corporation. All rights reserved.

C:\Users\y0ns2>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=36ms TTL=55
Reply from 8.8.8.8: bytes=32 time=71ms TTL=55
Reply from 8.8.8.8: bytes=32 time=45ms TTL=55
Reply from 8.8.8.8: bytes=32 time=137ms TTL=55

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 137ms, Average = 72ms
```

-
- **Bước 3: Stop quá trình capture của wireshark**



- **Bước 4: Vào thanh filter của wireshark và nhập vào từ khóa “icmp” và ip.addr**

○ Từ khóa “icmp”

Wireshark packet capture showing ICMP ping requests and replies. The filter is set to 'icmp'. The packet list shows several ICMP Echo (ping) requests and replies between 192.168.1.89 and 192.168.1.79.

Terminal output (C:\WINDOWS\system32\cmd.exe):

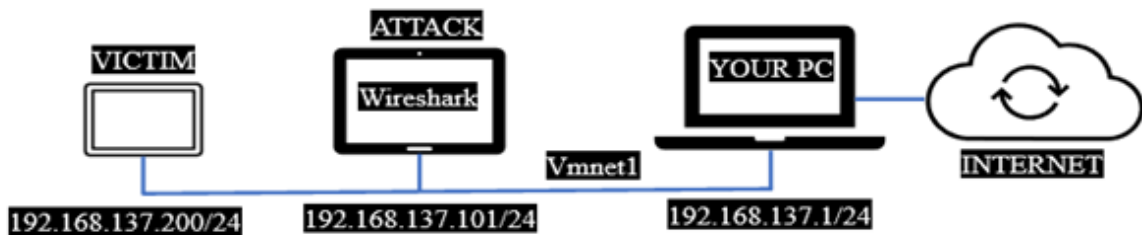
```
C:\Users\y0ns2>ping 192.168.1.79

Pinging 192.168.1.79 with 32 bytes of data:
Reply from 192.168.1.79: bytes=32 time=12ms TTL=128
Reply from 192.168.1.79: bytes=32 time=10ms TTL=128
Reply from 192.168.1.79: bytes=32 time=17ms TTL=128
Reply from 192.168.1.79: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.1.79:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 17ms, Average = 12ms
```

○ Ip.addr

3. Mô phỏng tấn công arp qua victim truy cập server, internet phải thông qua attack.



Chuẩn bị: