BÀI THỰC HÀNH

BẮT & PHÂN TÍCH GÓI TIN VỚI WIRESHARK

Họ và tên Sinh viên: **Mã Sinh viên:** **Nhóm:**

1.1 Chuẩn bị

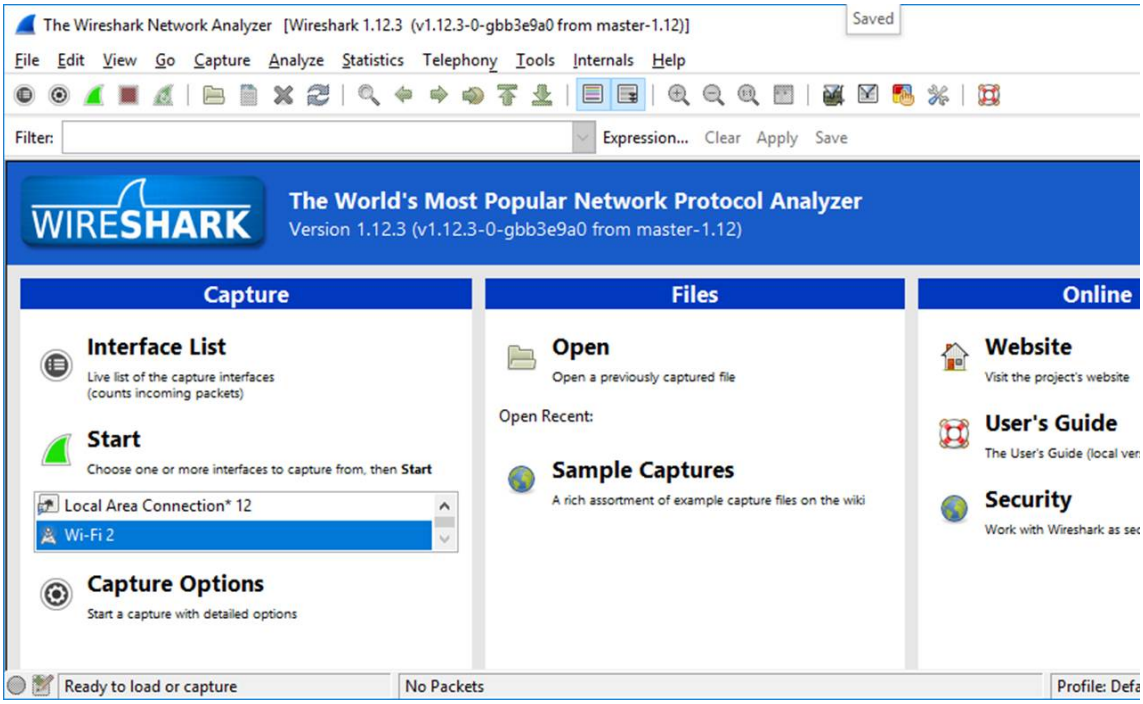
Tải và cài đặt Wireshark:

Cách 1: Tải file từ địa chỉ: *https://www.wireshark.org/download.html*

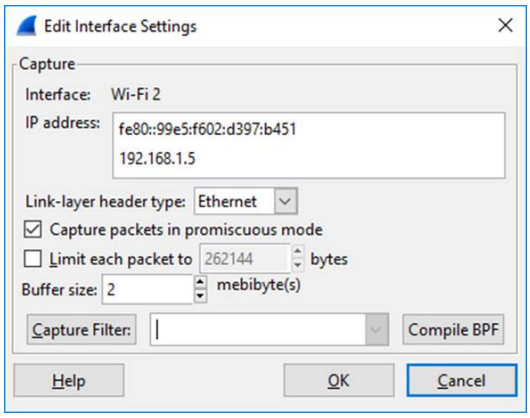
Cách 2: Mở trình duyệt, gõ ftp://192.168.0.10/ToolWireshark/

1. Vào thư mục ToolWireshark tải các file: *WiresharkPortable.rar, WinPcap v4.1.2.exe*
2. Cài đặt *WinPcap v4.1.3.exe*
3. Chạy *WiresharkPortable.rar* để giải nén vào thư mục *C:\WiresharkPortable*
4. Vào thư mục *C:\WiresharkPortable*, chạy file *WiresharkPortable.exe*

- Giao diện chương trình WireShark



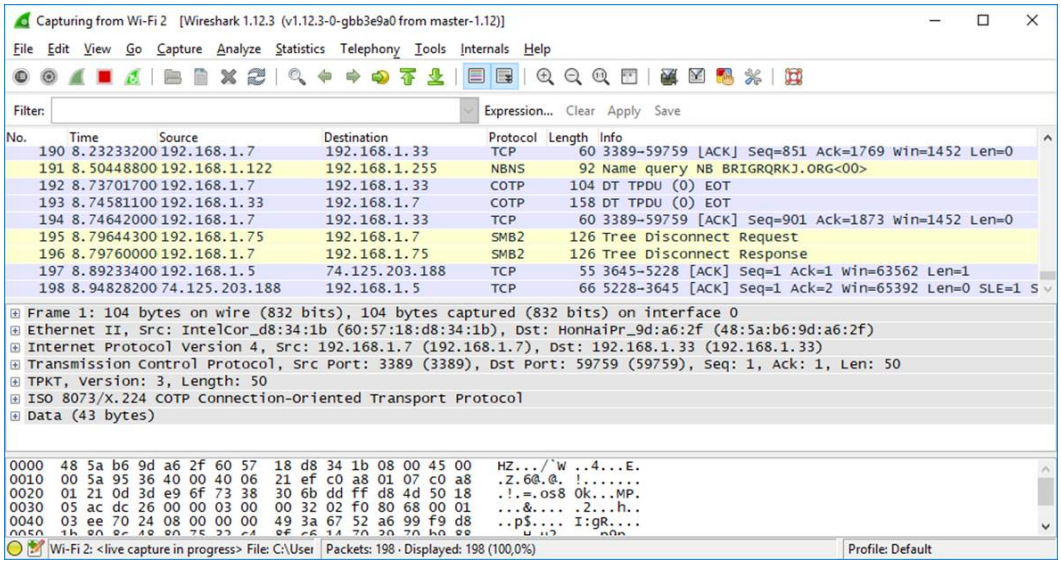
- Chọn Card mạng Wireless để bắt gói tin.



1.2 Bắt và phân tích gói tin

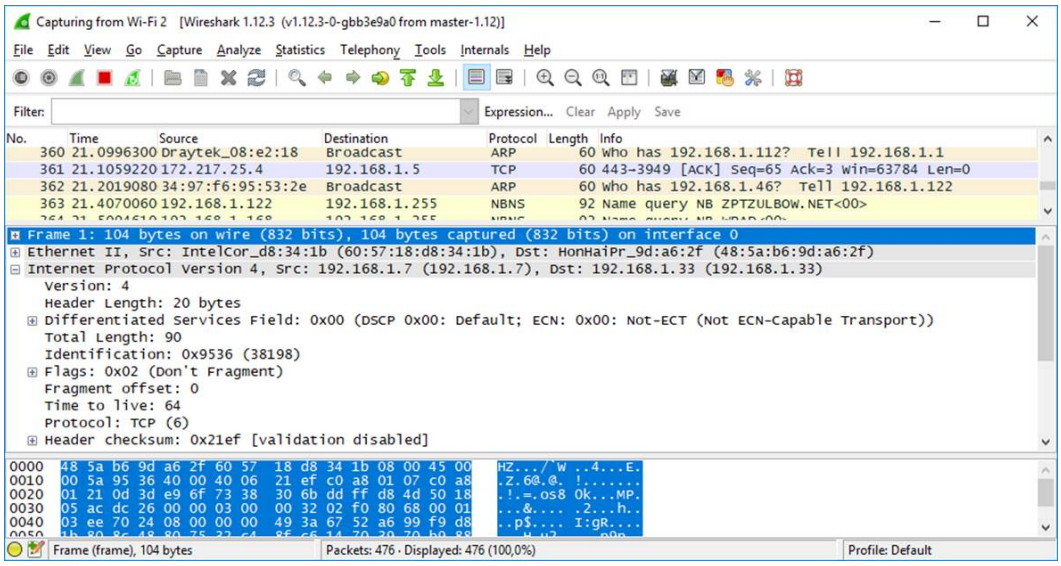
1.2.1 Xem nội dung các gói tin bắt được trên cửa sổ WireShark

1.2.1.1 Tại panel thứ 1: Xem địa chỉ nguồn, đích, giao thức của từng gói tin

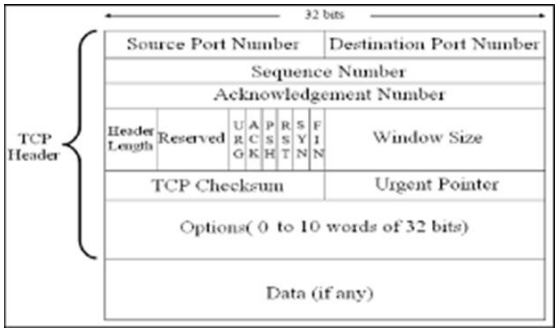


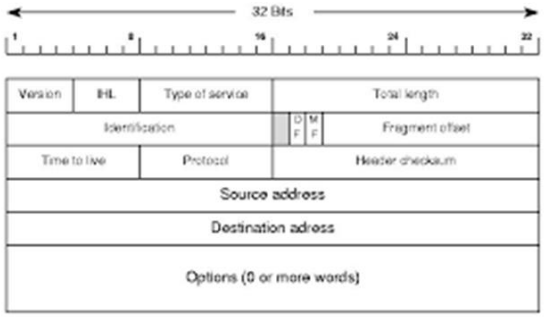
Xem thông tin bắt được: cho biết địa chỉ nguồn, địa chỉ đích, giao thức, chiều dài, nội dung của từng gói tin …

1.2.1.2 Tại panel thứ 2: Xem nội dung các tiêu đề của mỗi gói tin



Cấu trúc gói tin TCP, IP



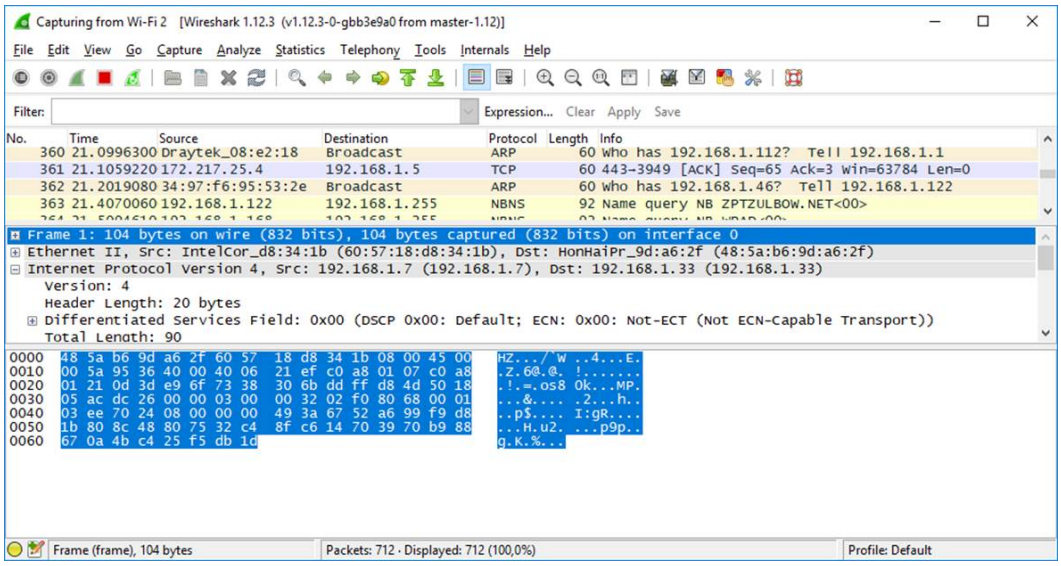


TCP Header *IP Header*

- Chọn một gói tin TCP bắt được, nhập giá trị của các trường TCP Header vào bảng sau:

- Chọn một gói tin TCP bắt được, nhập giá trị của các trường IP Header vào bảng sau:

1.2.1.3 Tại panel thứ 3: Xem nội dung dạng Hexa, ASCII của từng gói tin

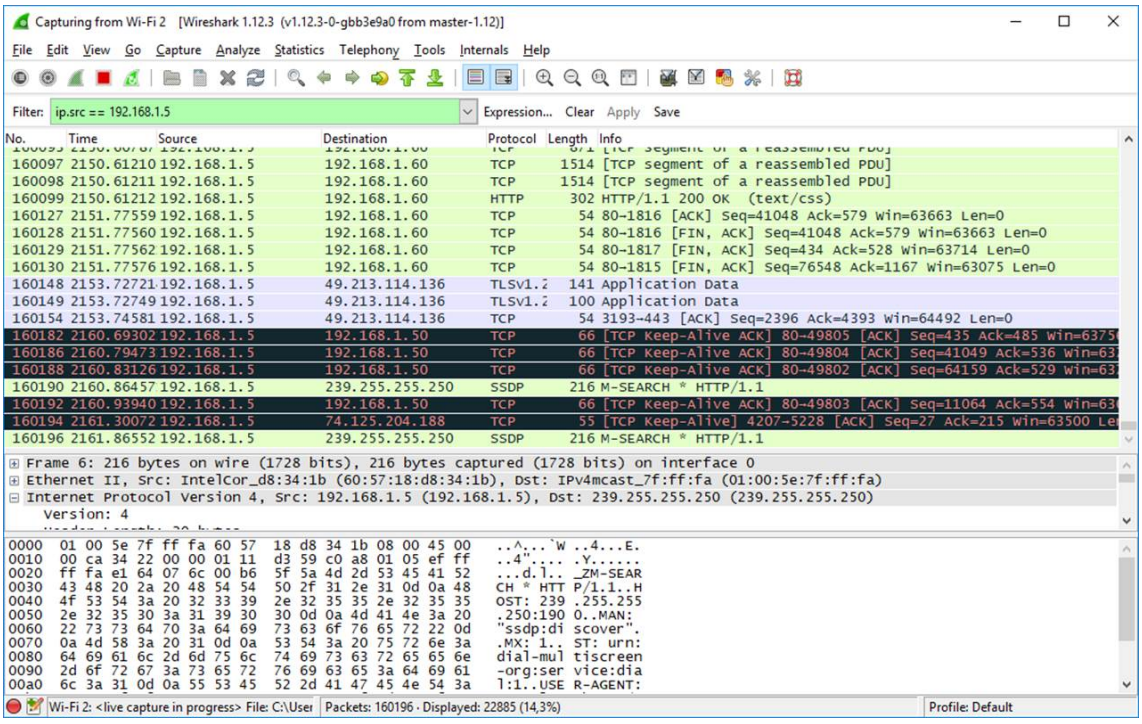


- Để xem chi tiết các nội dung, kích chuột phải vào cửa sổ hiển thị các gói tin bị chặn bắt, chọn menu *Follow TCP Stream*. Các thông tin về quá trình trao đổi gói tin sẽ được hiển thị trong cửa sổ khác.

>> Lưu kết quả vào báo cáo

1.2.2 Lọc các gói tin theo địa chỉ IP nguồn

- Tại cửa sổ WireShark, Kích nút Stop để dừng bắt.
- Tại ô Filter, nhập luật: **ip.**src == 192.168.0.10 Chọn nút Apply.
- Kết quả trên cửa sổ Wireshark sẽ chỉ hiển thị các gói tin có địa chỉ theo luật



1.2.3 Lọc các gói tin theo địa chỉ IP đích

- Tại cửa sổ WireShark, Kích nút Stop để dừng bắt.
- Tại ô Filter, nhập luật: `ip.dst==192.168.0.10` Chọn nút Apply.
- Kết quả trên cửa sổ Wireshark sẽ chỉ hiển thị các gói tin có địa chỉ theo luật

- Lọc, không hiển thị các gói tin có địa chỉ đích:

```
ip.dst != 192.168.0.10
```

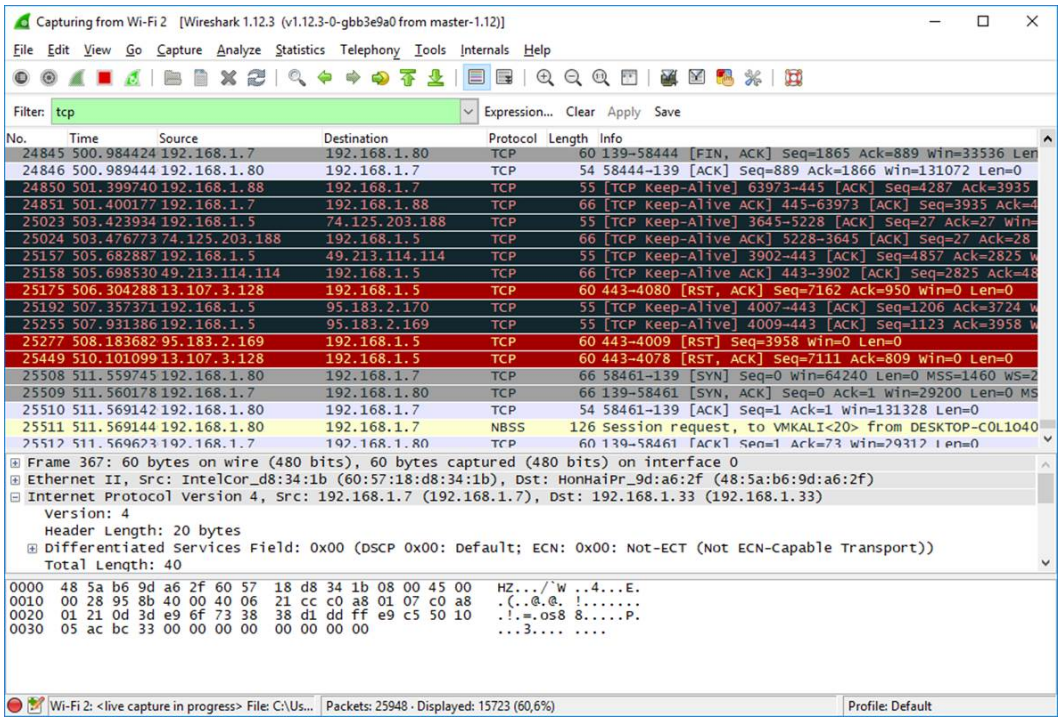
- Lọc các gói tin theo địa chỉ nguồn và đích:

```
ip.src==192.168.0.15 && ip.dst==192.168.0.10
```

>> Lưu kết quả lọc gói tin vào báo cáo

1.2.4 Lọc các gói tin theo giao thức tcp

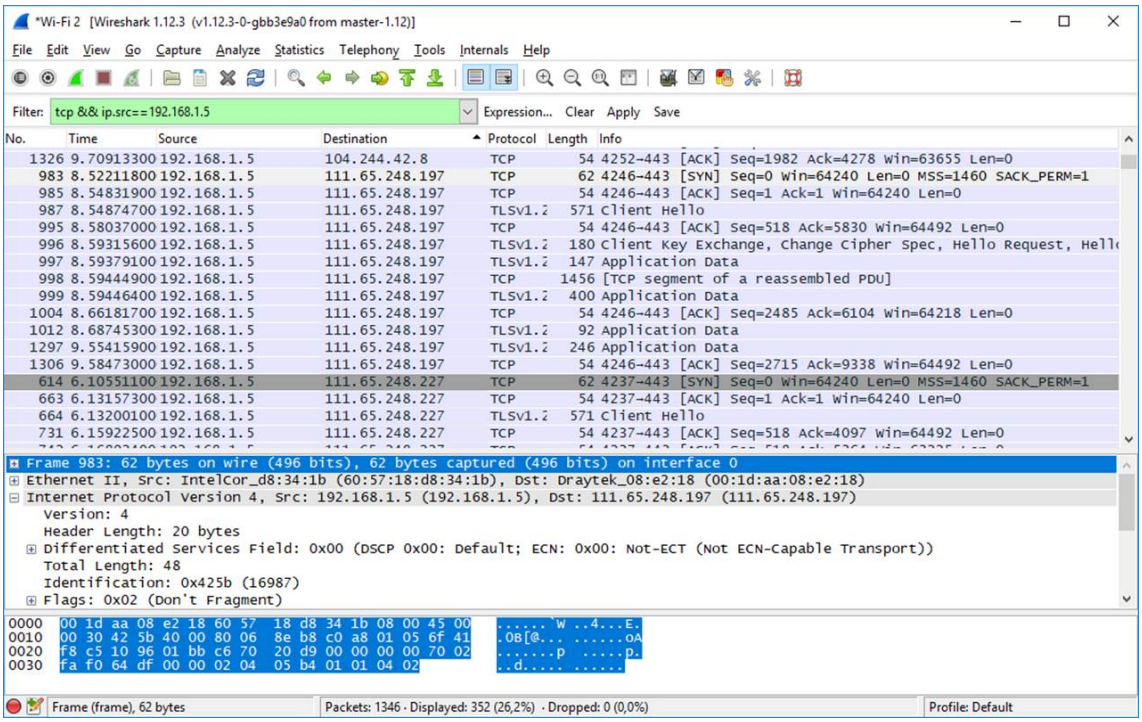
- Kết nối mạng Internet, mở trình duyệt Web, truy xuất vào Website: https://vnexpress.net/
- Tại cửa sổ WireShark, Kích nút Stop để dừng bắt.
- Tại ô Filter, nhập luật: **tcp** Chọn nút Apply.
- Kết quả trên cửa sổ Wireshark sẽ chỉ hiển thị các gói tin theo giao thức tcp.



- Kích chọn cột *Destination* để sắp xếp các gói tin theo địa chỉ đích của gói tin
- Lọc theo giao thức và địa chỉ nguồn: **tcp && ip.src==<Địa chỉ IP máy NSD>**

Ví dụ: `tcp && ip.src == 192.168.0.10`

`http && ip.src == 192.168.0.10`

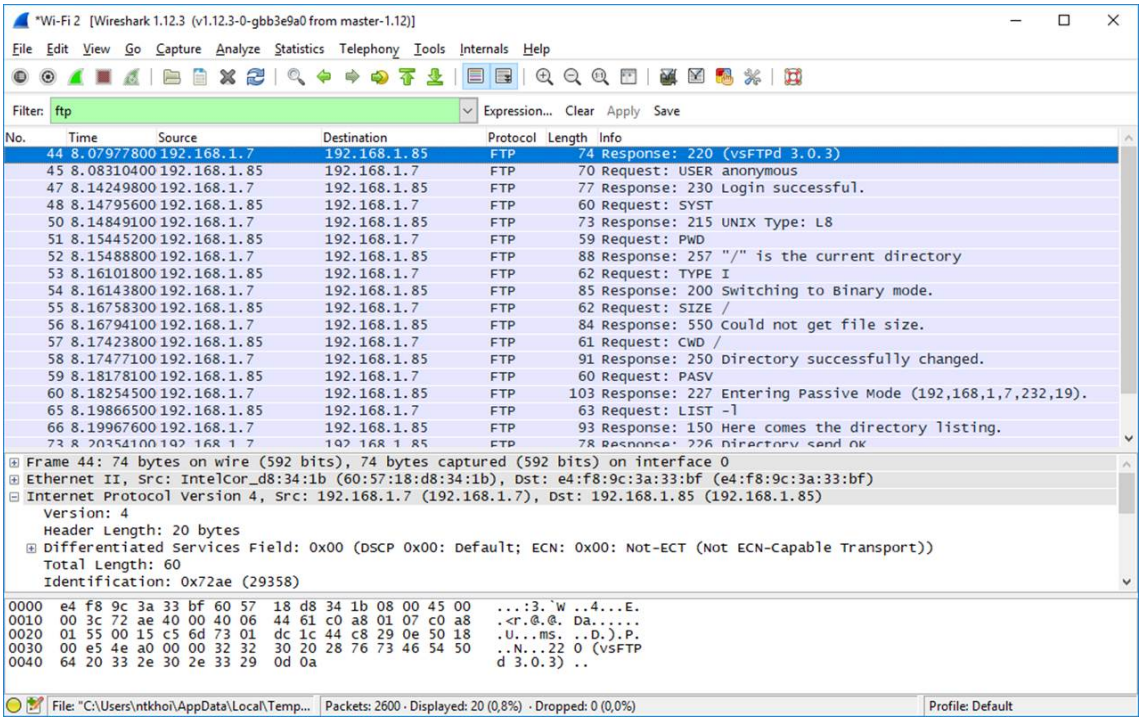


- Lọc theo giao thức và địa chỉ đích: **tcp && ip.dst == <Địa chỉ IP máy NSD>**
- Lọc theo giao thức và cổng: **tcp.port eq 80**

>> Lưu kết quả lọc gói tin vào báo cáo

1.2.5 Lọc các gói tin theo giao thức ftp

- Chạy Wireshark ở chế độ đang bắt gói tin.
- Mở trình duyệt Web, nhập vào địa chỉ: *ftp://192.168.0.10*
- Tại cửa sổ WireShark, tại ô filter, nhập vào giá trị **ftp**. Sau đó chọn nút Apply.
- Kết quả trên cửa sổ bắt gói tin sẽ hiển thị các gói tin theo giao thức ftp.



>> Lưu kết quả lọc gói tin vào báo cáo

1.2.6 Lọc các gói tin theo giao thức http - Bắt gói tin chứa username, password

1.2.6.1 Lọc gói tin theo http

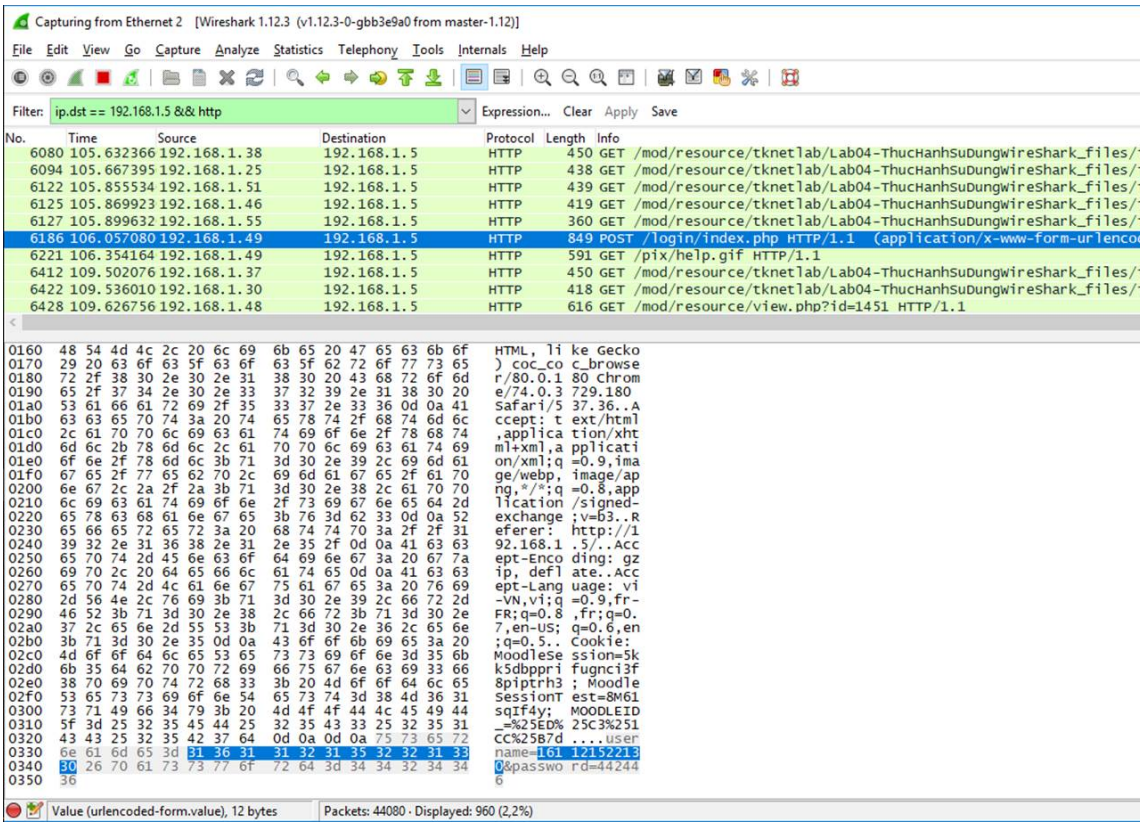
- Chạy Wireshark ở chế độ đang bắt gói tin.
- Mở trình duyệt Web, nhập vào địa chỉ Website: http://192.168.0.5 đây là địa chỉ của máy chạy WebSite E-learning đang dùng.
- Lần lượt sử dụng các luật sau

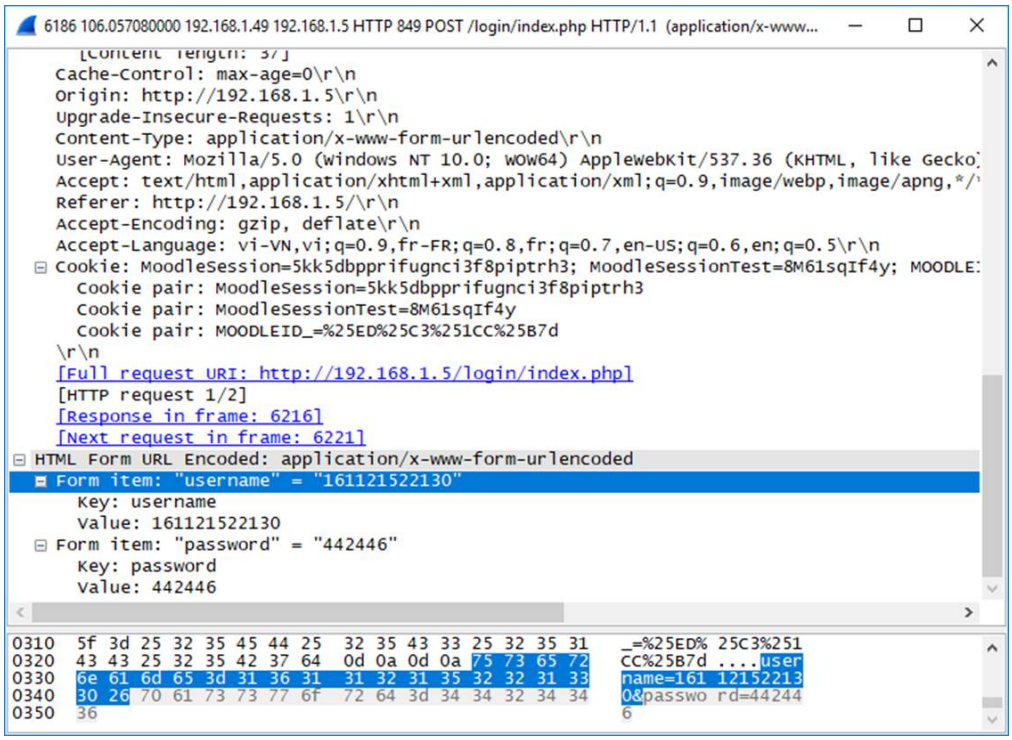
```
http.request && ip.addr == 192.168.0.5
http.request || http.response
dns.qry.name contains microsoft or dns.qry.name contains windows
```

>> Lưu kết quả lọc gói tin vào báo cáo

1.2.6.2 Bắt thông tin đăng nhập Website 192.168.0.5

- Chạy Wireshark ở chế độ đang bắt gói tin.
- Mở trình duyệt Web, nhập vào địa chỉ Website: http://192.168.0.5
- Đăng nhập vào Website theo *username, password.*
- Quay trở lại Wireshark, nhập vào ô filter: *http*
- Tại cửa sổ Wireshark, dò tìm gói tin chứa info: *login.php*
- Tìm trong nội dung gói tin các thông tin: *username, password* bắt được.





1.2.7 Lọc các gói tin theo giao thức icmp

- Chạy Wireshark ở chế độ đang bắt gói tin.
- Mở cửa sổ lệnh, gõ lệnh: *ping 192.168.0.10 -t* hoặc từ máy khác ping đến máy NSD.
- Tại cửa sổ Wireshark, nhập vào ô filter: icmp
- Xem kết quả lọc theo giao thức này.

>> Lưu kết quả lọc gói tin vào báo cáo

>> Thử đăng nhập vào một WebSite trên mạng và bắt gói tin chứa username, password đăng nhập vào Website này.

1.2.8 Lọc các gói tin bắt được theo địa chỉ nguồn (ip.src), địa chỉ đích (ip.dst) và giao thức (http, ftp, ….)

Tại ô filter, lần lượt nhập các luật sau để lọc các gói tin:

```
tcp
udp
icmp
http
ftp-data
ip.addr==192.168.0.10
ip.src=192.168.0.10
ip.dst=192.168.0.25          // Địa chỉ IP của NSD
ip.src=192.168.0.10 && ip.dst=192.168.0.25
```

>> Lưu kết quả lọc gói tin vào báo cáo

1.2.9 Phân tích quá trình bắt tay 3 bước TCP bằng WireShark

- Mở trình duyệt Web, nhập vào địa chỉ Website: *http://192.168.0.10*
- Mở cửa sổ lệnh, gõ lệnh *ipconfig /all* để xem địa chỉ IP và địa chỉ MAC của máy hiện hành.
- Kiểm tra thông tin trong các gói tin bao gồm địa chỉ IP, cổng TCP (*TCP port numbers*) và cờ TCP (*TCP control flags*).
- Để dễ quan sát, chọn menu *Statistics ® Flow Graph*. Chọn nút OK. Xem quá trình bắt tay 3 bước TCP diễn ra như trên hình.
- Giải thích:

a) A gởi gói tin có cờ SYN = 1 (yêu cầu kết nối), giá trị segment khởi đầu có thứ tự là seq(A) = 0.

b) B đồng ý kết nối trả lời gói tin có cờ SYN = 1, ACK = 1 và giá trị seq(B) = 0, ack = seq(A) + 1 = 0 + 1 = 1 (đã nhận gói tin 0 của A và chờ gói tin 1).

c) A xác nhận thiết lập kết nối trả lời gói tin có cờ ACK = 1; giá trị ack = seq(B) + 1 = 0 = 1 (nghĩa là đã nhận gói tin 0 của B và chờ gói tin 1).

Yêu cầu: Chụp các gói tin thực hiện quá trình bắt tay 3 bước TCP bằng WireShark và giải thích

1.2.10 Xem đồ thị I/O graph thống kê gói tin bắt được

Chọn menu *Statistics ® I/O Graph*

Xem đồ thị biểu diễn lưu lượng dữ liệu trên mạng.

1.2.11 Xem thống kê gói tin bắt được

Chọn menu *Statistics ® Conversation List ® IPv4*

Xem bảng thống kê lưu lượng dữ liệu trên mạng.

Có thể phát hiện các đột biến hoặc những thời điểm không có dữ liệu truyền của các giao thức cụ thể.

1.3 Thực hành Wireshark nâng cao

1.3.1 Lọc các gói tin theo giao thức http

1.3.2 Filters for Web-Based Infection Traffic

http.request or ssl.handshake.type == 1.

The value http.request reveals URLs for HTTP requests, and ssl.handshake.type == 1 reveals domains names used in HTTPS or SSL/TLS traff

1.3.3 Find unencrypted SMTP traffic

1.4 BÀI TẬP

1) Chụp các gói tin thực hiện quá trình bắt tay 3 bước TCP bằng WireShark và giải thích
2) Đăng nhập các trang Web sau để bắt thông tin tài khoản:
   http://testphp.vulnweb.com/
   http://testing-ground.scraping.pro
3) Mở file: "2017-03-25-traffic-analysis-exercise.pcap", phân tích gói tin và hãy cho biết:
   - Ngày và tháng của hoạt động mạng
   - Địa chỉ MAC của máy bị nhiễm mã độc
   - Địa chỉ IP của máy bị nhiễm mã độc (dùng GeoIP)
   - Điều gì đã xảy ra với máy nạn nhân?
   - Nạn nhân tải mã độc về từ đâu? (từ IP và domain nào)
   - Trích xuất các mã độc từ file pcap
   - Tìm thêm 1 số thông tin về mã độc này trên mạng?
4) Làm các bài tập tại https://www.malware-traffic-analysis.net/training-exercises.html PASS: infected

---