



BÀI THỰC HÀNH

BẮT & PHÂN TÍCH GÓI TIN VỚI WIRESHARK

Họ và tên Sinh viên:

Mã Sinh viên:

Nhóm:

- [1.1 Chuẩn bị](#)
- [1.2 Bắt và phân tích gói tin](#)
 - [1.2.1 Xem nội dung các gói tin bắt được trên cửa sổ WireShark](#)
 - [1.2.2 Lọc các gói tin theo địa chỉ IP nguồn](#)
 - [1.2.3 Lọc các gói tin theo địa chỉ IP đích](#)
 - [1.2.4 Lọc các gói tin theo giao thức tcp](#)
 - [1.2.5 Lọc các gói tin theo giao thức ftp](#)
 - [1.2.6 Lọc các gói tin theo giao thức http - Bắt gói tin chứa username, password](#)
 - [1.2.7 Lọc các gói tin theo giao thức icmp](#)
 - [1.2.8 Lọc các gói tin bắt được theo địa chỉ nguồn \(ip.src\), địa chỉ đích \(ip.dst\) và giao thức \(http, ftp, ...\)](#)
 - [1.2.9 Phân tích quá trình bắt tay 3 bước TCP bằng WireShark](#)
 - [1.2.10 Xem đồ thị I/O graph thống kê gói tin bắt được](#)
 - [1.2.11 Xem thống kê gói tin bắt được](#)
- [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](#)
 - [1.3.3 Find unencrypted SMTP traffic](#)
- [1.4 BÀI TẬP](#)

1.1 Chuẩn bị

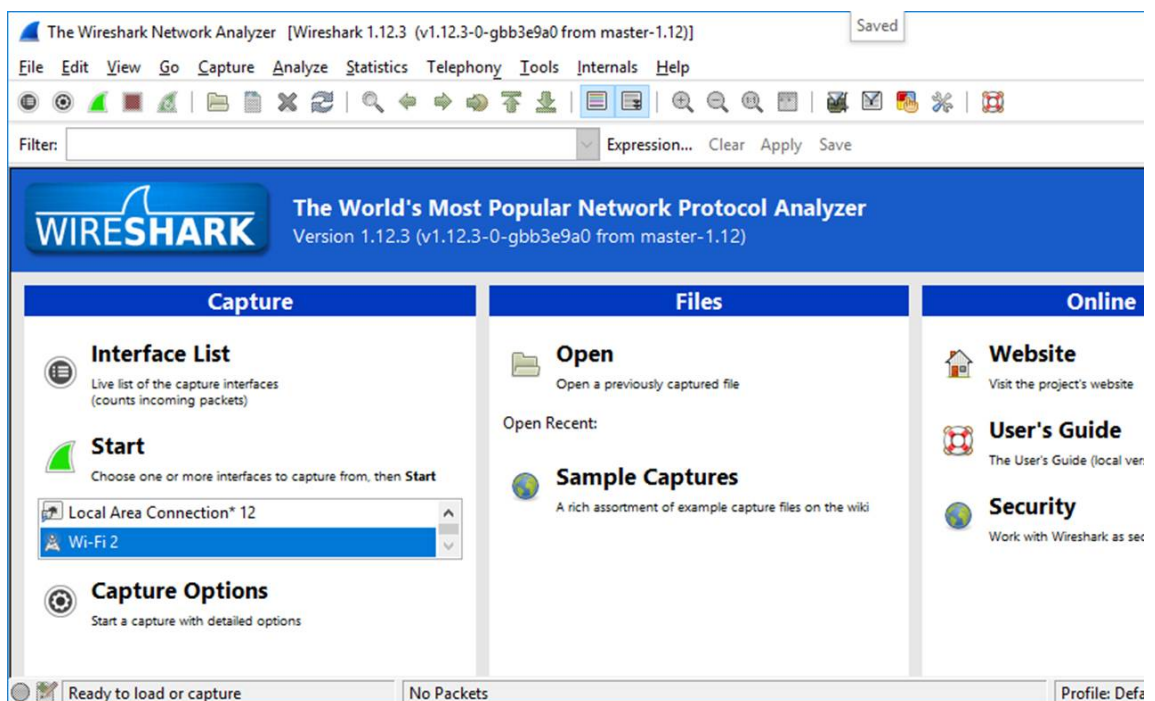
Tải và cài đặt Wireshark:

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

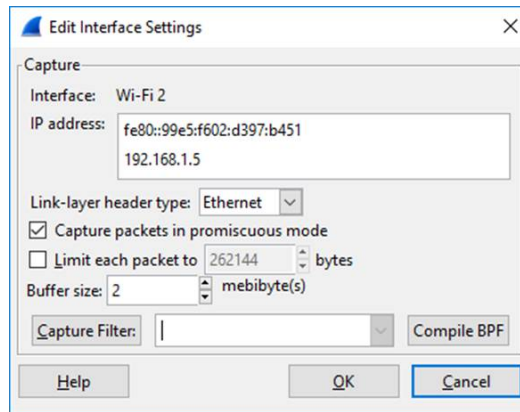
Cách 2: Mở trình duyệt, gõ <ftp://192.168.0.10/ToolWireshark/>

1. Vào thư mục ToolWireshark tải các file: *WiresharkPortable.rar*, *WinPcap v4.1.2.exe*
2. Cài đặt *WinPcap v4.1.2.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



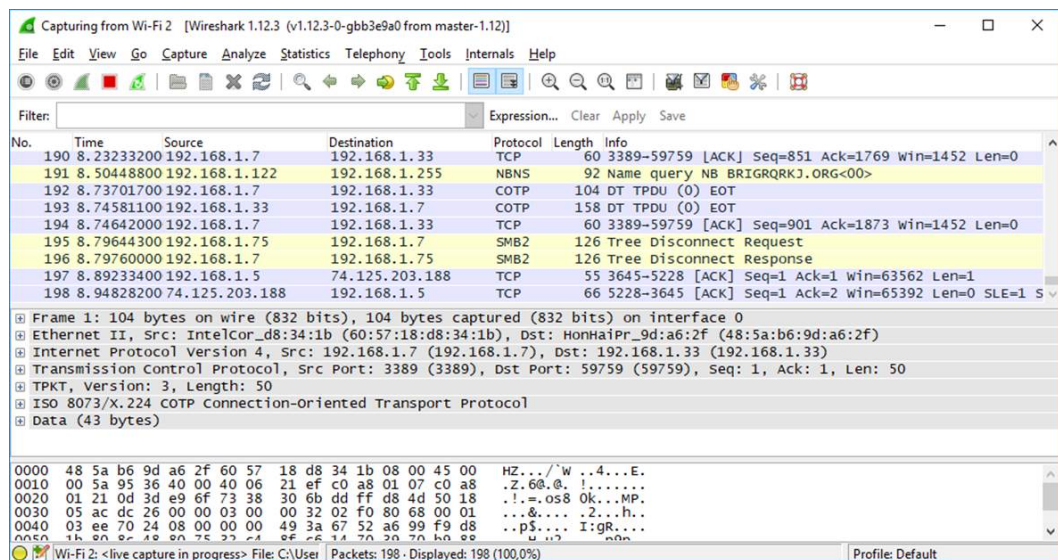
· Chọn Card mạng Wireless để bắt gói tin.



1.2 Bắt và phân tích gói tin

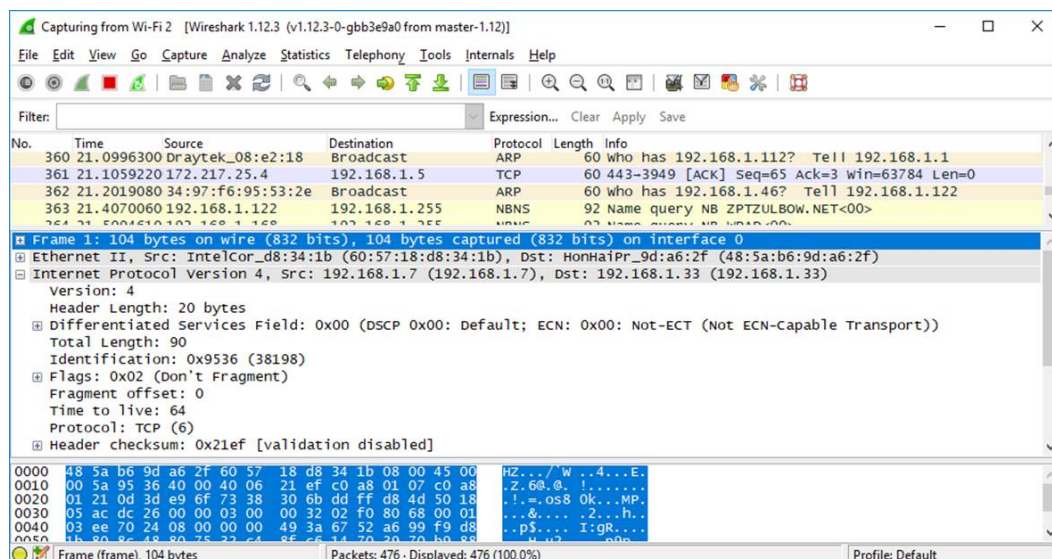
1.2.1 Xem nội dung các gói tin bắt được trên cửa sổ WireShark

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

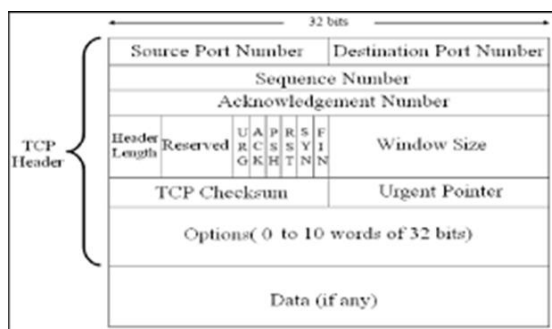


Xem thông tin bắt được: cho biết địa chỉ nguồn, địa chỉ đích, giao thức, chiều dài, nội dung của từng gói tin ...

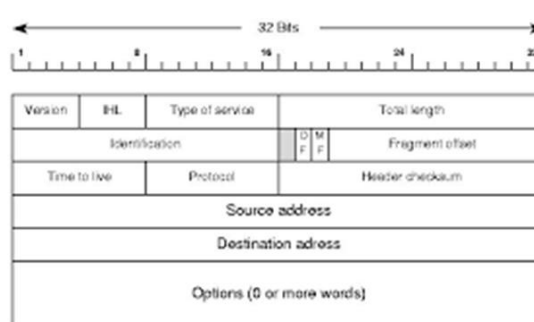
1.2.1.2 Tại panel thứ 2: Xem nội dung các tiêu đề của mỗi gói tin



Cấu trúc gói tin TCP, IP



TCP Header

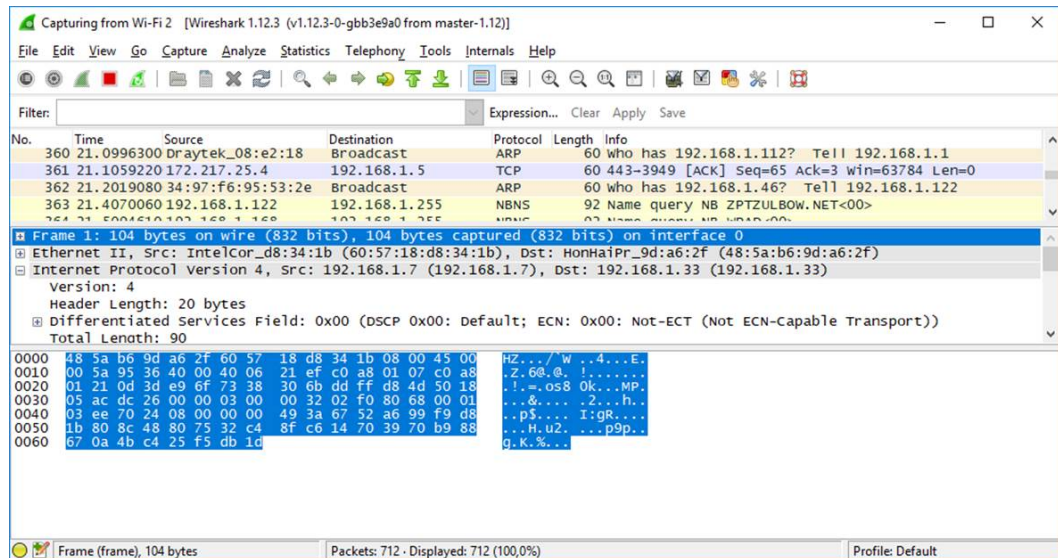


IP Header

- 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

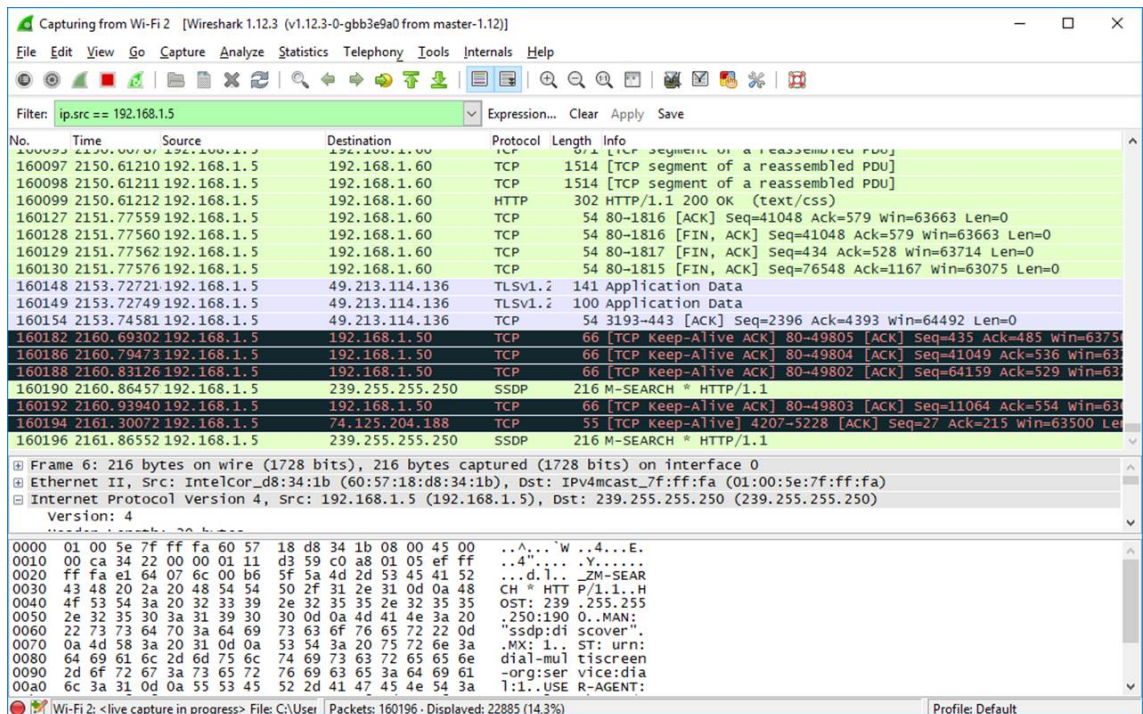


- Để xem chi tiết các nội dung, kích chuột phải vào cửa sổ hiển thị các gói tin bị chặn bắt, chọn menu *Follow TCP Stream*. Các thông tin về quá trình trao đổi gói tin sẽ được hiển thị trong cửa sổ khác.

>> 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

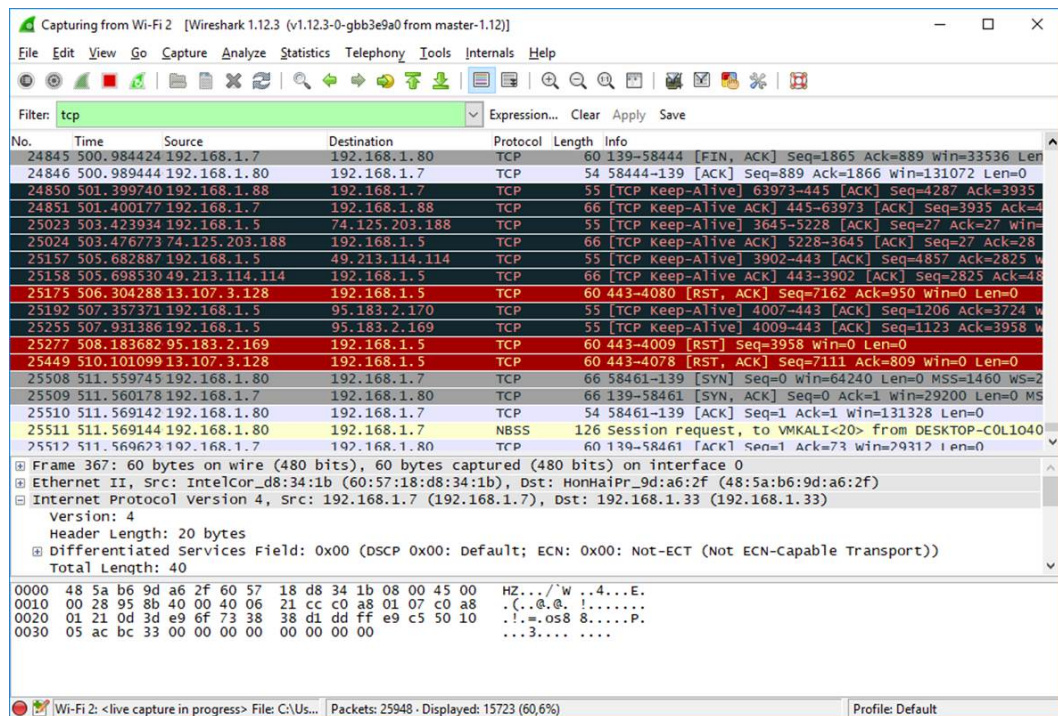
- Lọc các gói tin theo địa chỉ nguồn và đích:

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

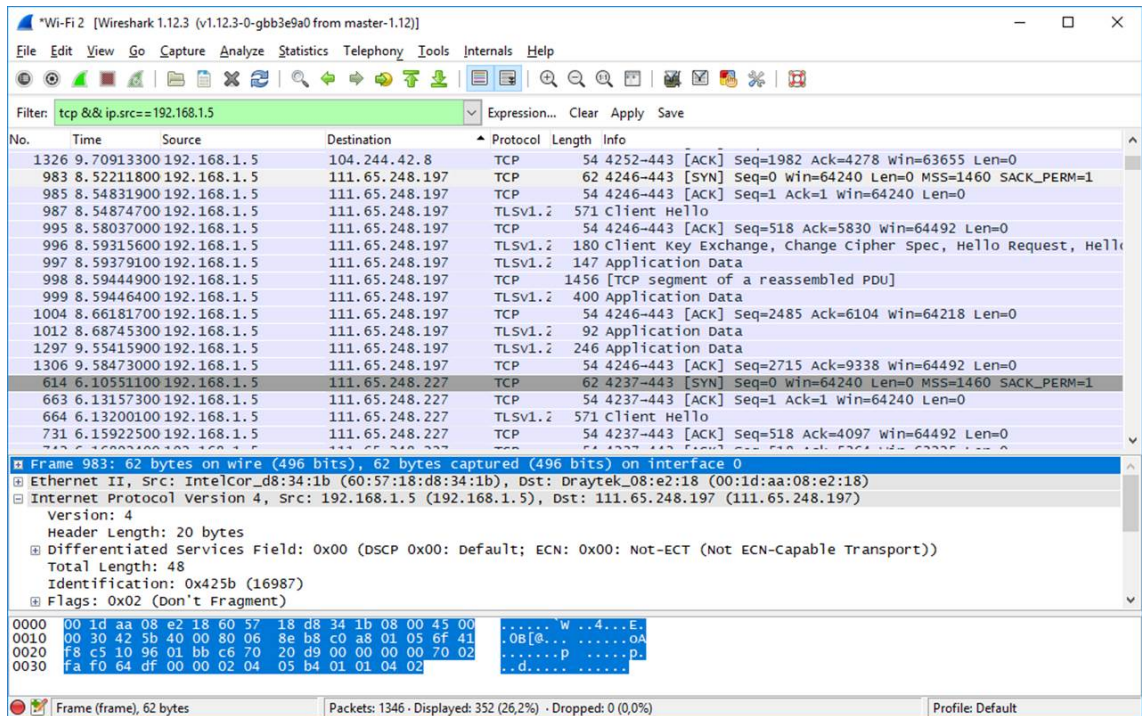
- Kết nối mạng Internet, mở trình duyệt Web, truy xuất vào Website: <https://vnexpress.net/>
- Tại cửa sổ Wireshark, Kích nút Stop để dừng bắt.
- Tại ô Filter, nhập luật: **tcp** Chọn nút Apply.
- Kết quả trên cửa sổ Wireshark sẽ chỉ hiển thị các gói tin theo giao thức tcp.



- 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

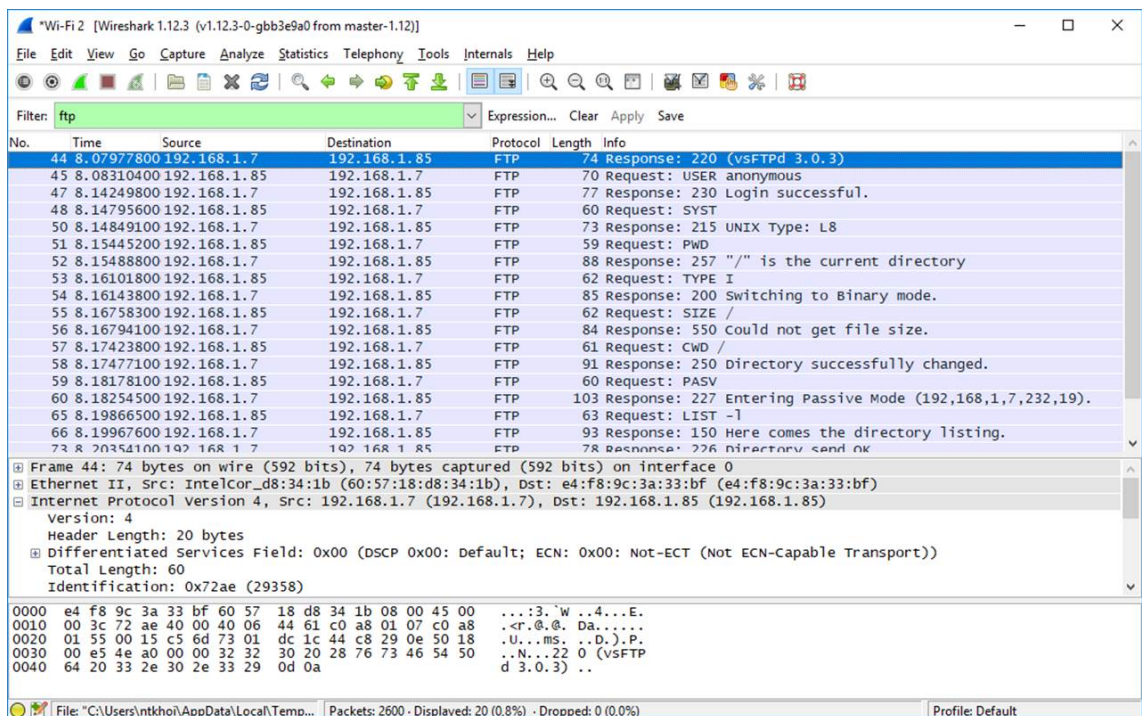


- Loại theo giao thức và địa chỉ đích: **tcp && ip.dst == <Địa chỉ IP máy NSD>**
- Loại theo giao thức và cổng: **tcp.port eq 80**

>> Lưu kết quả lọc gói tin vào báo cáo

1.2.5 Loại 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.

Capturing from Ethernet 2 [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

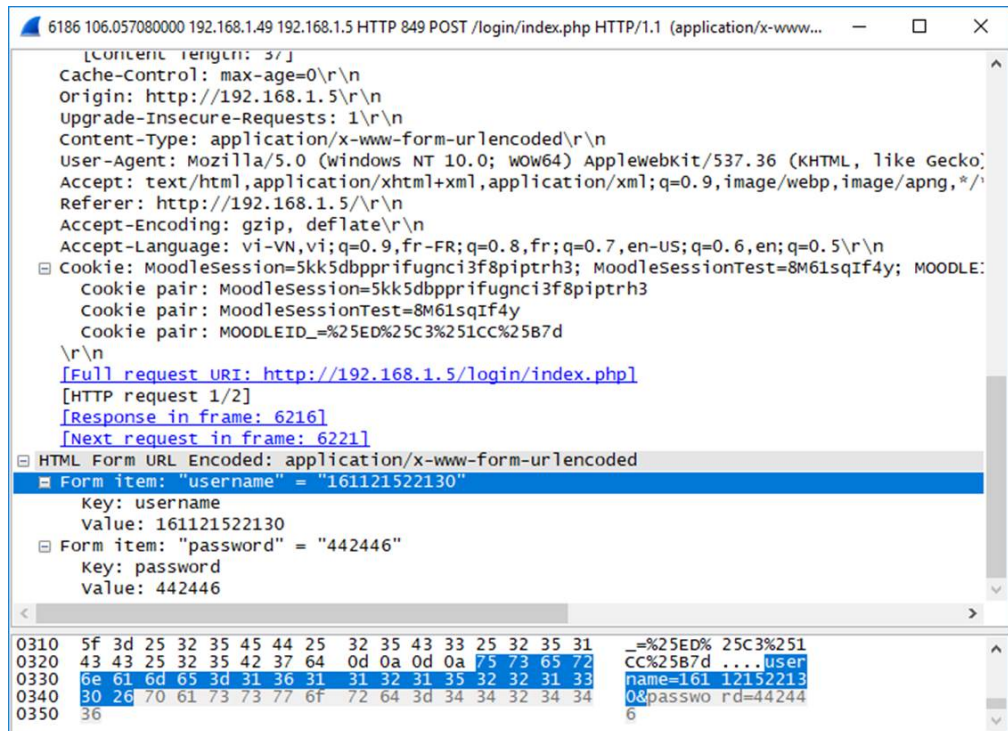
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.dst == 192.168.1.5 && http` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
6080	105.632366	192.168.1.38	192.168.1.5	HTTP	450	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6094	105.667395	192.168.1.25	192.168.1.5	HTTP	438	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6122	105.855534	192.168.1.51	192.168.1.5	HTTP	439	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6125	105.869923	192.168.1.46	192.168.1.5	HTTP	419	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6127	105.899632	192.168.1.55	192.168.1.5	HTTP	360	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6186	106.057080	192.168.1.49	192.168.1.5	HTTP	849	POST /login/index.php HTTP/1.1 (application/x-www-form-urlencoded)
6221	106.354164	192.168.1.49	192.168.1.5	HTTP	591	GET /pix/help.gif HTTP/1.1
6412	109.502076	192.168.1.37	192.168.1.5	HTTP	450	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6422	109.536010	192.168.1.30	192.168.1.5	HTTP	418	GET /mod/resource/tknetlab/Lab04-ThucHanhsudungwireshark_files/
6428	109.626756	192.168.1.48	192.168.1.5	HTTP	616	GET /mod/resource/view.php?id=1451 HTTP/1.1

0160 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f HTML, li ke Gecko
0170 29 20 63 6f 63 5f 63 6f 63 5f 62 72 6f 77 73 65) coc_co c_browse
0180 72 2f 38 30 2e 30 2e 31 38 30 20 43 68 72 6f 6d r/80.0.1 80 chrom
0190 65 2f 37 34 2e 30 2e 33 37 32 39 2e 31 38 30 20 e/74.0.3 729.180
01a0 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d 0a 41 Safari/5 37.36. A
01b0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html
01c0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht
01d0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml,a pplicati
01e0 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 on/xml;q =0.9,ima
01f0 67 65 2f 7f 65 62 70 2c 69 6d 61 67 65 2f 61 70 ge/webp, image/ap
0200 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 ng,*/*;q =0.8,app
0210 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d lication /signed-
0220 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 0d 0a 52 exchange ;v=B3..R
0230 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 31 eferer: http://1
0240 39 32 2e 31 36 38 2e 31 2e 35 2f 0d 0a 41 63 63 92.168.1 .5/.Acc
0250 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a ept-Enco ding: gz
0260 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 ip, defl ate..Acc
0270 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 76 69 ept-Lang uage: vi
0280 2d 56 4e 2c 76 69 3b 71 3d 30 2e 39 2c 66 72 2d -VN,vl;q =0.9,fr-
0290 46 52 3b 71 3d 30 2e 38 2c 66 72 3b 71 3d 30 2e FR;q=0.8 ,fr;q=0.
02a0 37 2c 65 6e 2d 55 53 3b 71 3d 30 2e 36 2c 65 6e 7,en-US; q=0.6,en
02b0 3b 71 3d 30 2e 35 0d 0a 43 6f 6f 6b 69 65 3a 20 ;q=0.5.. Cookie:
02c0 4d 6f 6f 64 6c 65 53 65 73 73 69 6f 6e 3d 35 6b MoodlSe ssion=5k
02d0 6b 35 64 62 70 70 72 69 66 75 67 6e 63 69 33 66 k5dbppri fugnci3f
02e0 38 70 69 70 74 72 68 33 3b 20 4d 6f 6f 64 6c 65 8piptrh3 : Moodl
02f0 53 65 73 73 69 6f 6e 34 65 73 74 3d 38 4d 36 31 Session est=8M6L
0300 73 71 49 66 34 79 3b 20 4d 4f 4f 44 4c 45 49 44 sqZF4y: MOODLEID
0310 5f 3d 25 32 35 45 44 25 32 35 43 33 25 32 35 31 _=%25E0% 25C3%251
0320 43 43 25 32 35 42 37 64 0d 0a 0d 0a 75 73 65 72 CC%25B7duser
0330 6e 61 6d 65 3d 31 36 31 31 32 31 35 32 32 31 33 name=161 12152213
0340 26 70 61 73 73 77 6f 72 64 3d 34 34 32 34 34 &passwo rd=44244
0350 36

Value (urlencoded-form.value), 12 bytes Packets: 44080 · Displayed: 960 (2,2%)



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 gửi 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 = 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 traffic

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
