

PHẦN MỀM WIRESHARK

1. Cài đặt

<http://www.wireshark.org>

2. Giới thiệu Wireshark

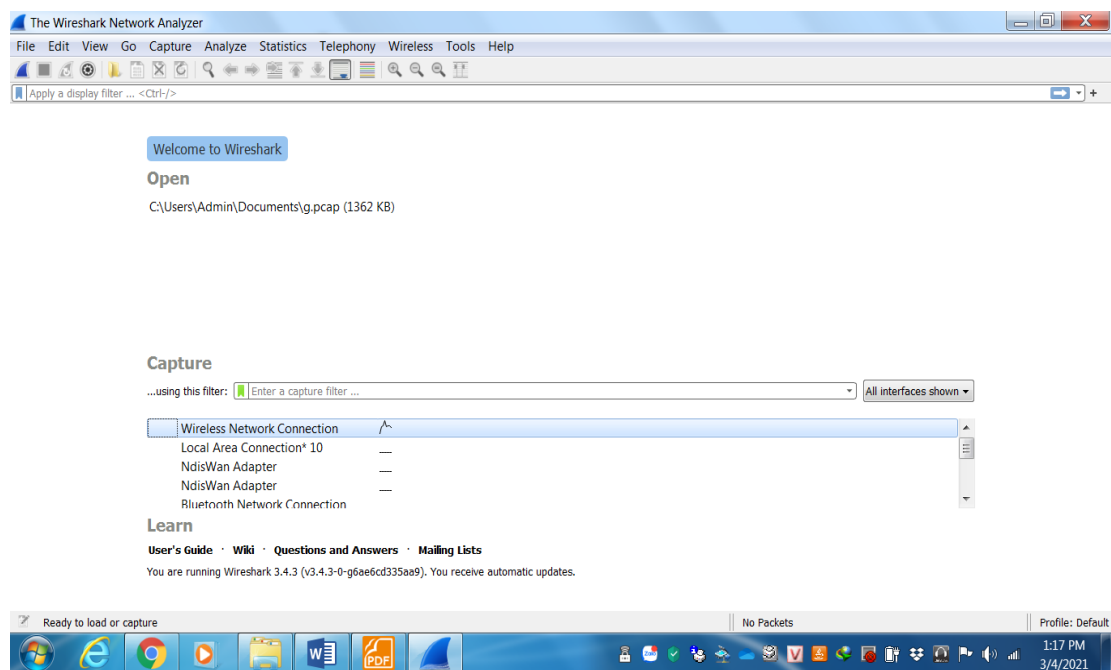
Wireshark là công cụ phân tích giao thức mạng được sử dụng rộng rãi trên thế giới. Nó là phần mềm nguồn mở do Gerald Combs khởi xướng từ năm 1998.

Wireshark cho phép ta xem lưu lượng truy cập và phân tích những gì đang diễn ra trong mạng.

Tính năng chính của Wireshark: Bắt gói tin trực tiếp và lưu trữ dữ liệu bắt được để phân tích ngoại tuyến.

3. Capturing Packets

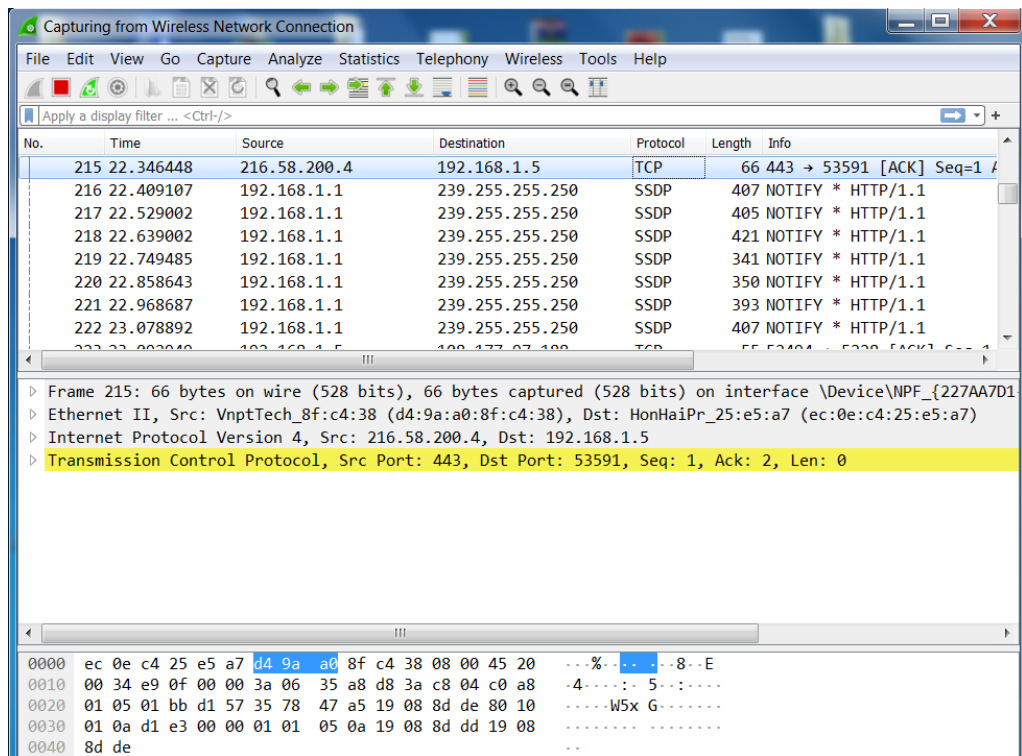
Khởi động Wireshark, xuất hiện giao diện:



Chọn thành phần trong Interface List để bắt đầu hoạt động. Ví dụ, nếu muốn giám sát lưu lượng mạng qua mạng Wireless thì chọn Wireless Network Connection tương ứng. Nhấn nút Start capturing packets để bắt đầu bắt gói tin. Nhấn nút Capture, chọn Options để hiển thị thêm nhiều tùy chọn khác.



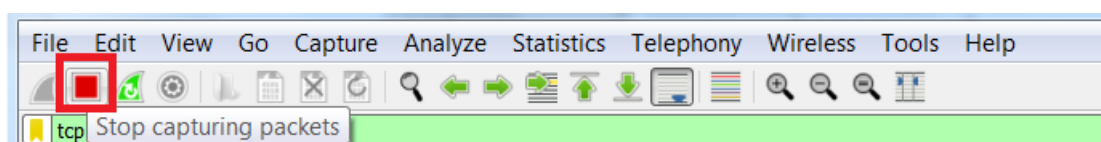
Giao diện các gói tin của toàn bộ hệ thống:



Gồm các thành phần sau:

Command Menu	<div>File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help</div> <div></div>																																																															
Bộ lọc (filter)	<div>Apply a display filter ... <Ctrl-/></div>																																																															
Danh sách gói tin đã bắt	<table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>215</td><td>22.346448</td><td>216.58.200.4</td><td>192.168.1.5</td><td>TCP</td><td>66</td><td>443 → 53591 [ACK] Seq=1</td></tr><tr><td>216</td><td>22.409107</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>407</td><td>NOTIFY * HTTP/1.1</td></tr><tr><td>217</td><td>22.529002</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>405</td><td>NOTIFY * HTTP/1.1</td></tr><tr><td>218</td><td>22.639002</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>421</td><td>NOTIFY * HTTP/1.1</td></tr><tr><td>219</td><td>22.749485</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>341</td><td>NOTIFY * HTTP/1.1</td></tr><tr><td>220</td><td>22.858643</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>350</td><td>NOTIFY * HTTP/1.1</td></tr><tr><td>221</td><td>22.968687</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>393</td><td>NOTIFY * HTTP/1.1</td></tr><tr><td>222</td><td>23.078892</td><td>192.168.1.1</td><td>239.255.255.250</td><td>SSDP</td><td>407</td><td>NOTIFY * HTTP/1.1</td></tr></table>	No.	Time	Source	Destination	Protocol	Length	Info	215	22.346448	216.58.200.4	192.168.1.5	TCP	66	443 → 53591 [ACK] Seq=1	216	22.409107	192.168.1.1	239.255.255.250	SSDP	407	NOTIFY * HTTP/1.1	217	22.529002	192.168.1.1	239.255.255.250	SSDP	405	NOTIFY * HTTP/1.1	218	22.639002	192.168.1.1	239.255.255.250	SSDP	421	NOTIFY * HTTP/1.1	219	22.749485	192.168.1.1	239.255.255.250	SSDP	341	NOTIFY * HTTP/1.1	220	22.858643	192.168.1.1	239.255.255.250	SSDP	350	NOTIFY * HTTP/1.1	221	22.968687	192.168.1.1	239.255.255.250	SSDP	393	NOTIFY * HTTP/1.1	222	23.078892	192.168.1.1	239.255.255.250	SSDP	407	NOTIFY * HTTP/1.1
No.	Time	Source	Destination	Protocol	Length	Info																																																										
215	22.346448	216.58.200.4	192.168.1.5	TCP	66	443 → 53591 [ACK] Seq=1																																																										
216	22.409107	192.168.1.1	239.255.255.250	SSDP	407	NOTIFY * HTTP/1.1																																																										
217	22.529002	192.168.1.1	239.255.255.250	SSDP	405	NOTIFY * HTTP/1.1																																																										
218	22.639002	192.168.1.1	239.255.255.250	SSDP	421	NOTIFY * HTTP/1.1																																																										
219	22.749485	192.168.1.1	239.255.255.250	SSDP	341	NOTIFY * HTTP/1.1																																																										
220	22.858643	192.168.1.1	239.255.255.250	SSDP	350	NOTIFY * HTTP/1.1																																																										
221	22.968687	192.168.1.1	239.255.255.250	SSDP	393	NOTIFY * HTTP/1.1																																																										
222	23.078892	192.168.1.1	239.255.255.250	SSDP	407	NOTIFY * HTTP/1.1																																																										
Thông tin Header của một packets	<div>▶ Frame 215: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{227AA7D1}</div> <div>▶ Ethernet II, Src: VnptTech_8f:c4:38 (d4:9a:a0:8f:c4:38), Dst: HonHaiPr_25:e5:a7 (ec:0e:c4:25:e5:a7)</div> <div>▶ Internet Protocol Version 4, Src: 216.58.200.4, Dst: 192.168.1.5</div> <div>▶ Transmission Control Protocol, Src Port: 443, Dst Port: 53591, Seq: 1, Ack: 2, Len: 0</div>																																																															
Phần mã số dưới dạng Hexadecimal	<div>0000 ec 0e c4 25 e5 a7 d4 9a a0 8f c4 38 08 00 45 20 ...%...-8..E</div> <div>0010 00 34 e9 0f 00 00 3a 06 35 a8 d8 3a c8 04 c0 a8 -4-----5:....</div> <div>0020 01 05 01 bb d1 57 35 78 47 a5 19 08 8d de 80 10W5x G.....</div> <div>0030 01 0a d1 e3 00 00 01 01 05 0a 19 08 8d dd 19 08G.....</div> <div>0040 8d de ..</div>																																																															

Để dừng quá trình bắt gói tin hãy nhấn vào nút Stop capturing packets trên thanh công cụ.

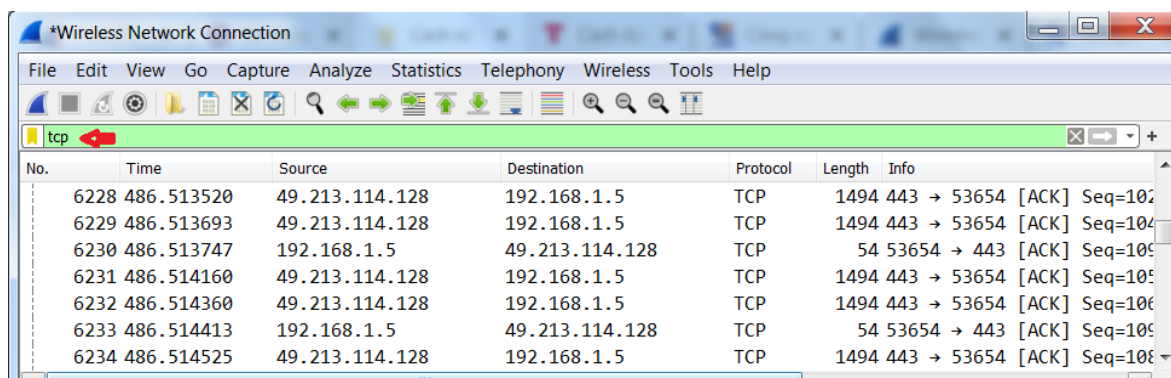


Chúng ta có thể lưu các gói vừa bắt và mở chúng sau này. Nhấn vào File, chọn Save để lưu các gói tin đã bắt vào file .pcap.

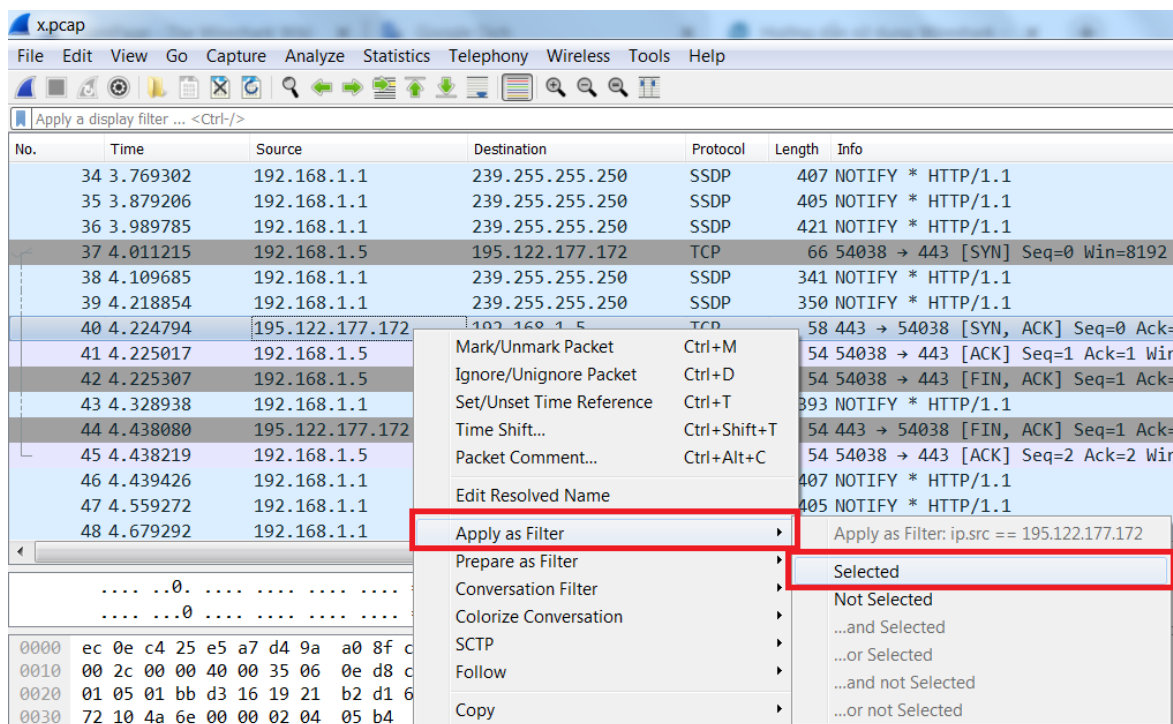
4. Sử dụng Filter

Chúng ta có thể sử dụng filter để loại bỏ các gói mà ta không quan tâm. Filter có thể được sử dụng khi bắt các gói tin realtime hoặc cũng có thể được sử dụng đối với các gói tin được mở từ file .pcap.

Để lọc các gói tin, cách đơn giản nhất là nhập thông tin cần lọc vào ô Filter, sau đó nhấn Enter. Ví dụ, nếu gõ tcp thì chúng ta sẽ chỉ nhìn thấy các gói dữ liệu TCP. Hoặc nhấn menu Analyze, chọn Display Filters để tạo filter mới.



Chỉ xem các gói tin có IP nguồn khớp với IP 192.122.177.172. Nhấn chuột phải lên gói tin có địa chỉ nguồn 192.122.177.172, chọn Apply as Filter, chọn Selected.



Kết quả được:

x.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 195.122.177.172

No.	Time	Source	Destination	Protocol	Length	Info
40	4.224794	195.122.177.172	192.168.1.5	TCP	58	443 → 54038 [SYN, ACK] Seq=
44	4.438080	195.122.177.172	192.168.1.5	TCP	54	443 → 54038 [FIN, ACK] Seq=

Frame 40: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)

Ethernet II, Src: VnptTech_8f:c4:38 (d4:9a:a0:8f:c4:38), Dst: HonHaiPr_25:e5:a7 (ec:0e:c4:25:e5:a7)

Internet Protocol Version 4, Src: 195.122.177.172, Dst: 192.168.1.5

Transmission Control Protocol, Src Port: 443, Dst Port: 54038, Seq: 0, Ack: 1, Len: 0

```

0000  ec 0e c4 25 e5 a7 d4 9a a0 8f c4 38 08 00 45 20  ...%. ...-8-E
0010  00 2c 00 00 40 00 35 06 0e d8 c3 7a b1 ac c0 a8  ,..@.5. ...z....
0020  01 05 01 bb d3 16 19 21 b2 d1 6e ea 95 14 60 12  .....! ..n...`
0030  72 10 4a 6e 00 00 02 04 05 b4                r.Jn.... ..

```