Bài thực hành

Sử dụng Wireshark để quan sát gói tin UDP và DNS

Mục tiêu

Sử dụng Wireshark để giám sát lưu lượng

Tạo lưu lượng có UDP

Quan sát gói tin UDP

Quan sát gói tin DNS

Chuẩn bị

Sinh viên có phần mềm wireshark được cài đặt trên máy tính.

Sinh viên có kiến thức về UDP, DNS

Thực hiện

Bước 1: Bật Wireshark và bắt đầu bắt gói tin.

Bước 2: Truy cập vào website https://ntu.edu.vn/

Bước 3: Dừng bắt

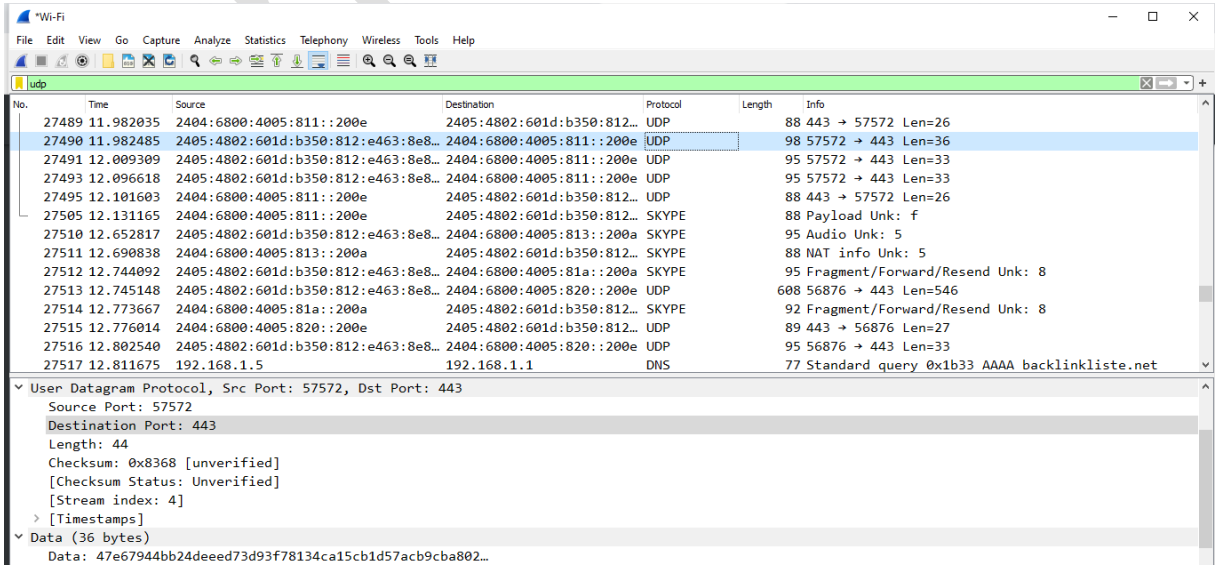
Bước 4: Lọc lưu lượng bắt tay 3 bước sử dụng các cú pháp lọc:

- Lọc giao thức,udp, dns
- Nhiều điều kiện: kết hợp toán tử AND (&&) OR (||)

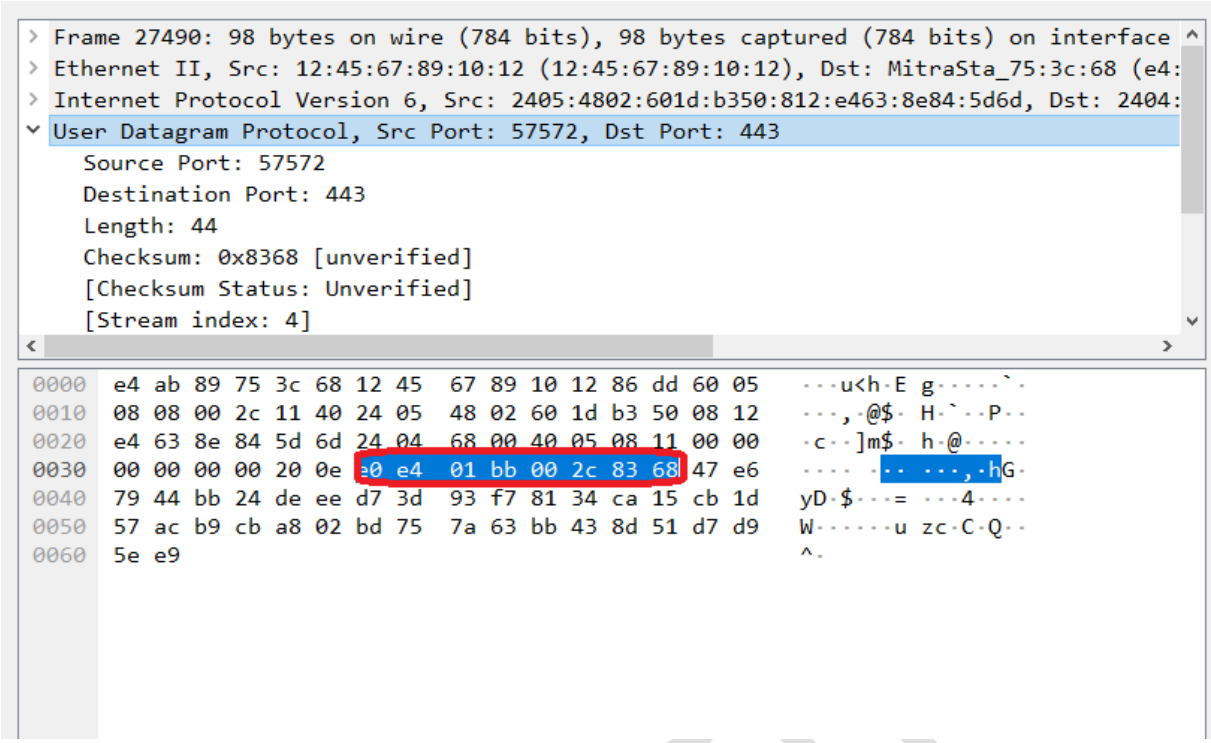
Bước 4: Phân tích lưu lượng bắt được

A- Trường hợp UDP, chỉ lọc giao thức UDP

Câu 1. Chọn một gói UDP. Hãy cho biết có bao nhiêu trường trong UDP header, giá trị của từng trường này?



Câu 2: Phần nào trong nội dung của gói tin là chỉ thông tin về header. Phân này bao nhiêu byte?



Câu 3: Chiều dài của payload (Phần dữ liệu) là bao nhiêu bytes

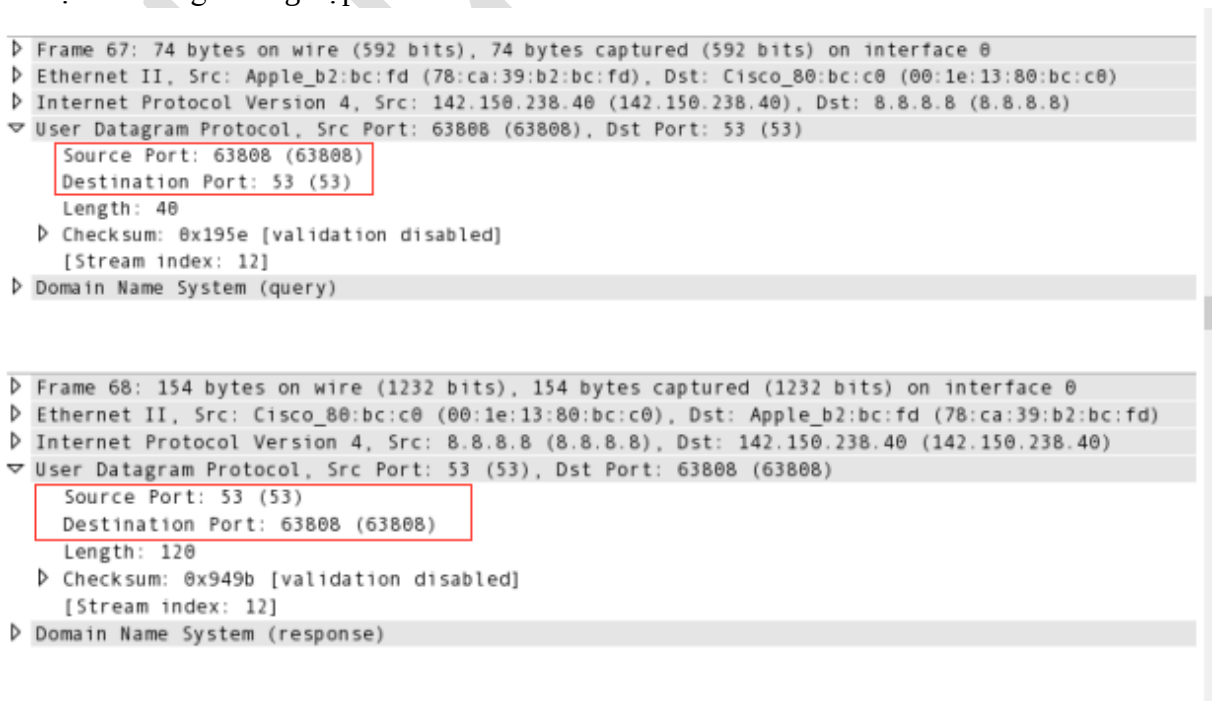
Câu 4: Chiều dài tối đa dữ liệu có thể chứa trong gói UDP là bao nhiêu?

Câu 5: Giá trị cổng nguồn lớn nhất là bao nhiêu?

Câu 6: Dịch vụ mà UDP đang vận chuyển cho tầng ứng dụng là dịch vụ nào?

Câu 7: Mỗi UDP request sẽ có UDP response, hãy phân tích cổng nguồn đích của hai gói tin này? Thời gian phản hồi là bao lâu?

Ví dụ như trong trường hợp sau:



B- Trường hợp DNS

Câu 1: Sử dụng cú pháp lọc giao thức DNS

Hãy phân tích gói dns request trong trường hợp này là của ntu.edu.vn?

- Transaction id là bao nhiêu? Biểu diễn bằng hệ đếm nào?

- Địa chỉ server của ntu.edu.vn là?

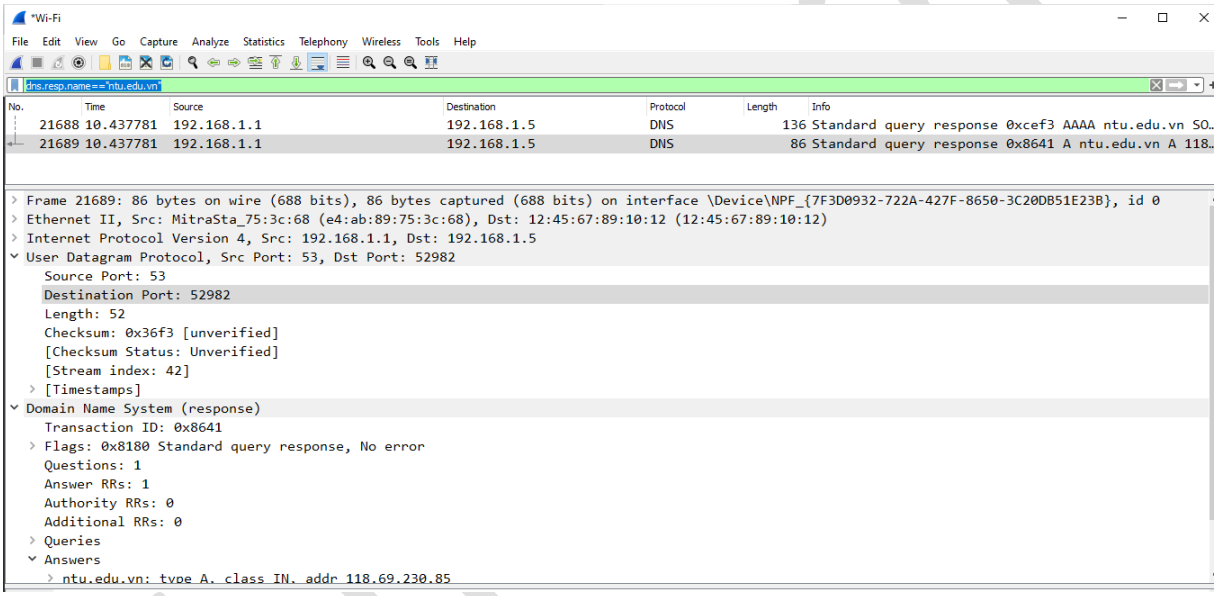
- Địa chỉ MAC nguồn, MAC đích?

- Địa chỉ IP nguồn, đích

- Địa chỉ cổng nguồn đích?

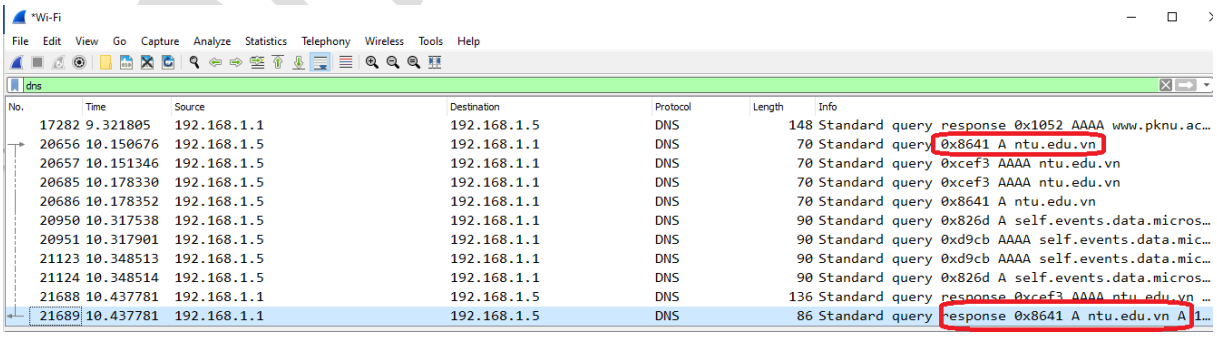
- DNS sử dụng giao thức nào tầng dưới, hãy chỉ ra vị trí?

Câu 2: Sử dụng cú pháp lọc dns.resp.name=="ntu.edu.vn", hãy miêu tả DNS response?



- Kiểu resource record là kiểu gì? Xác định (name, value, type, ttl, class)

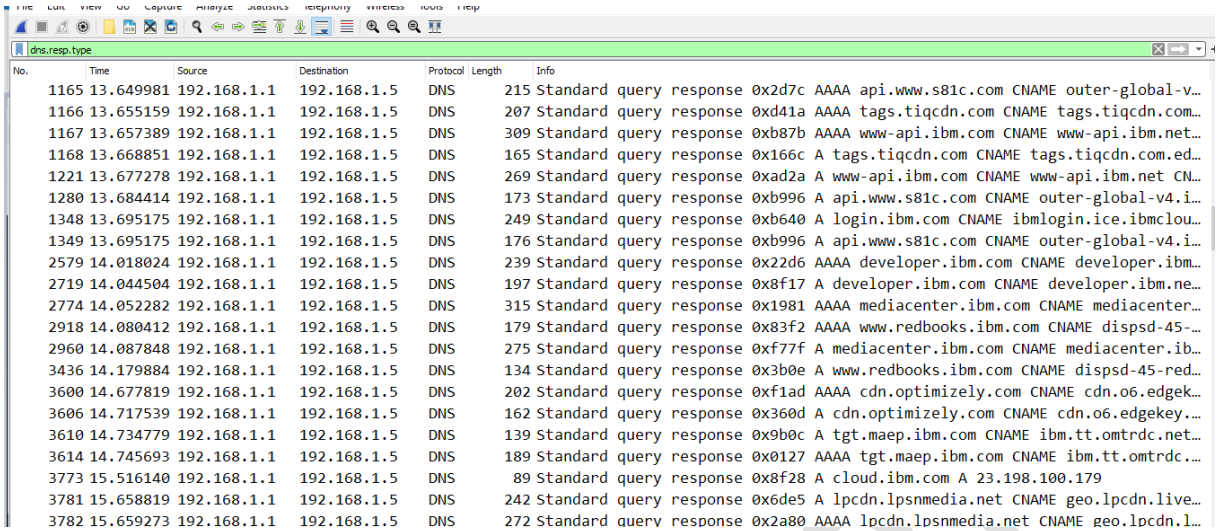
- Transaction id là bao nhiêu? Giá trị này có khớp với transaction id của DNS request



Câu 3: Hãy sử dụng cú pháp dns.resp.type để lọc các resource record đã bắt.

Hãy trả lời các kiểu resource này xác định (name, value, type, ttl, class)

Ví dụ:



dns.resp.type

No.	Time	Source	Destination	Protocol	Length	Info
1165	13.649981	192.168.1.1	192.168.1.5	DNS	215	Standard query response 0x2d7c AAAA api.www.s81c.com CNAME outer-global-v…
1166	13.655159	192.168.1.1	192.168.1.5	DNS	207	Standard query response 0xd41a AAAA tags.tiqcdn.com CNAME tags.tiqcdn.com…
1167	13.657389	192.168.1.1	192.168.1.5	DNS	309	Standard query response 0xb87b AAAA www-api.ibm.com CNAME www-api.ibm.net…
1168	13.668851	192.168.1.1	192.168.1.5	DNS	165	Standard query response 0x166c A tags.tiqcdn.com CNAME tags.tiqcdn.com.ed…
1221	13.677278	192.168.1.1	192.168.1.5	DNS	269	Standard query response 0xad2a A www-api.ibm.com CNAME www-api.ibm.net CN…
1280	13.684414	192.168.1.1	192.168.1.5	DNS	173	Standard query response 0xb996 A api.www.s81c.com CNAME outer-global-v4.i…
1348	13.695175	192.168.1.1	192.168.1.5	DNS	249	Standard query response 0xb640 A login.ibm.com CNAME ibmlogin.ice.ibmclou…
1349	13.695175	192.168.1.1	192.168.1.5	DNS	176	Standard query response 0xb996 A api.www.s81c.com CNAME outer-global-v4.i…
2579	14.018024	192.168.1.1	192.168.1.5	DNS	239	Standard query response 0x22d6 AAAA developer.ibm.com CNAME developer.ibm…
2719	14.044504	192.168.1.1	192.168.1.5	DNS	197	Standard query response 0x8f17 A developer.ibm.com CNAME developer.ibm.ne…
2774	14.052282	192.168.1.1	192.168.1.5	DNS	315	Standard query response 0x1981 AAAA mediacenter.ibm.com CNAME mediacenter…
2918	14.080412	192.168.1.1	192.168.1.5	DNS	179	Standard query response 0x83f2 AAAA www.redbooks.ibm.com CNAME dispsd-45-…
2960	14.087848	192.168.1.1	192.168.1.5	DNS	275	Standard query response 0xf77f A mediacenter.ibm.com CNAME mediacenter.ib…
3436	14.179884	192.168.1.1	192.168.1.5	DNS	134	Standard query response 0x3b0e A www.redbooks.ibm.com CNAME dispsd-45-red…
3600	14.677819	192.168.1.1	192.168.1.5	DNS	202	Standard query response 0xf1ad AAAA cdn.optimizely.com CNAME cdn.o6.edgek…
3606	14.717539	192.168.1.1	192.168.1.5	DNS	162	Standard query response 0x360d A cdn.optimizely.com CNAME cdn.o6.edgekey.…
3610	14.734779	192.168.1.1	192.168.1.5	DNS	139	Standard query response 0x9b0c A tgt.maep.ibm.com CNAME ibm.tt.omtrdc.net…
3614	14.745693	192.168.1.1	192.168.1.5	DNS	189	Standard query response 0x0127 AAAA tgt.maep.ibm.com CNAME ibm.tt.omtrdc.…
3773	15.516140	192.168.1.1	192.168.1.5	DNS	89	Standard query response 0x8f28 A cloud.ibm.com A 23.198.100.179
3781	15.658819	192.168.1.1	192.168.1.5	DNS	242	Standard query response 0x6de5 A lpcdn.lpsnmedia.net CNAME geo.lpcdn.live…
3782	15.659273	192.168.1.1	192.168.1.5	DNS	272	Standard query response 0x2a80 AAAA lpcdn.lpsnmedia.net CNAME geo.lpcdn.l…

Câu 4: Hãy giải thích một gói chứa CNAME?