

Nội dung và hướng dẫn bài thực hành

Mục đích

Giúp sinh viên nắm vững cách sử dụng Wireshark để thu thập, giám sát và phân tích các gói tin trong mạng

Yêu cầu đối với sinh viên

Có kiến thức cơ bản về hệ điều hành Linux, công cụ wireshark và giao thức UDP

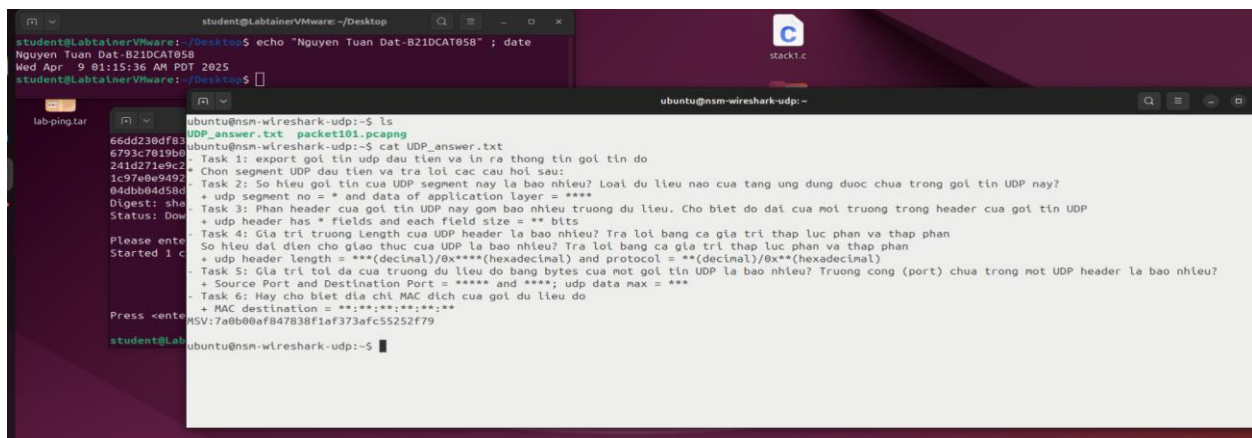
Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

labtainer nsm-wireshark-udp

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

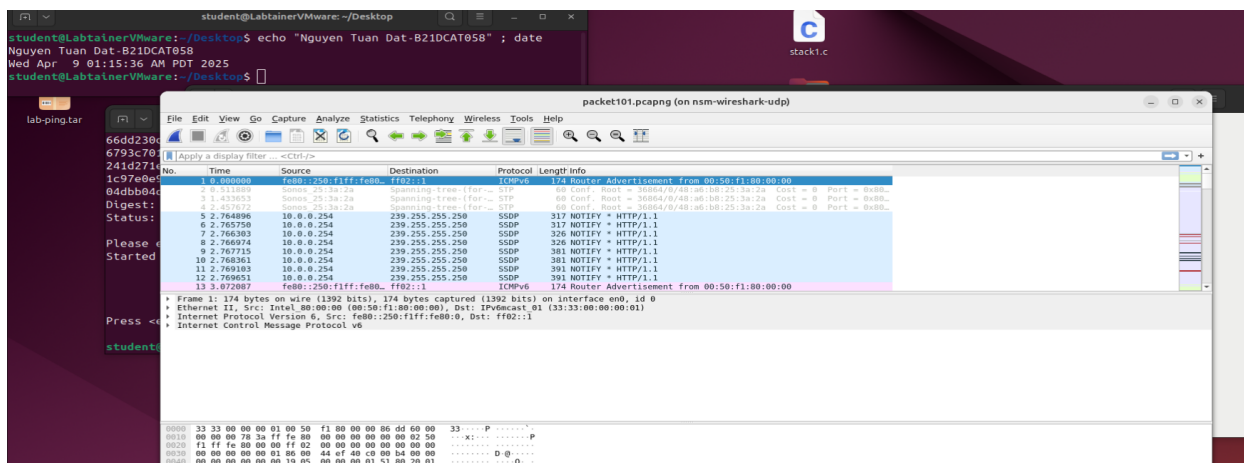


```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCA7058" ; date
Nguyen Tuan Dat-B21DCA7058
Wed Apr  9 01:15:36 AM PDT 2025
student@LabtainerVMware:~/Desktop$

lab-ping.tar
ubuntu@nsm-wireshark-udp:~$ ls
UDP_answer.txt  packet101.pcapng
ubuntu@nsm-wireshark-udp:~$ cat UDP_answer.txt
Task 1: export gói tin udp đầu tiên và in ra thông tin gói tin đó
        * Chon segment UDP đầu tiên và trả lời các câu hỏi sau:
Task 2: So hieu gói tin của UDP segment này là bao nhiêu? Loại dữ liệu nào của tầng ứng dụng được chứa trong gói tin UDP này?
        + udp segment no = * and data of application layer = ****
Task 3: Phan header của gói tin UDP này gồm bao nhiêu trường dữ liệu. Cho biết do đại của mỗi trường trong header của gói tin UDP
        + udp header has * fields and each field size = ** bits
Task 4: Giá trị trường Length của UDP header là bao nhiêu? Trả lời bằng cả giá trị thập lục phân và thập phân
        So hieu đại diện cho giao thức của UDP là bao nhiêu? Trả lời bằng cả giá trị thập lục phân và thập phân
        + udp header length = ***(decimal)/0x*** (hexadecimal) and protocol = ** (decimal)/0x*** (hexadecimal)
Task 5: Giá trị tổng của trường dữ liệu do bao nhiêu trường dữ liệu. Cho biết tổng (port) chứa trong một UDP header là bao nhiêu?
        + Source Port and Destination Port = ***** and ****; udp data max = ***
Task 6: Hay cho biết địa chỉ MAC đích của gói dữ liệu đó
        + MAC destination = **:**:**:**:**:**
Press <enter>
MSV:7a0b00af847838f1af373afc55252f79
student@LabtainerVMware:~/Desktop$
```

Sau khi khởi động xong một terminal ảo sẽ xuất hiện đại diện cho máy khởi chạy wireshark: nsm-wireshark-udp và điền kết quả sau khi phân tích các gói tin .Trên terminal khởi chạy wireshark bằng câu lệnh:

Wireshark



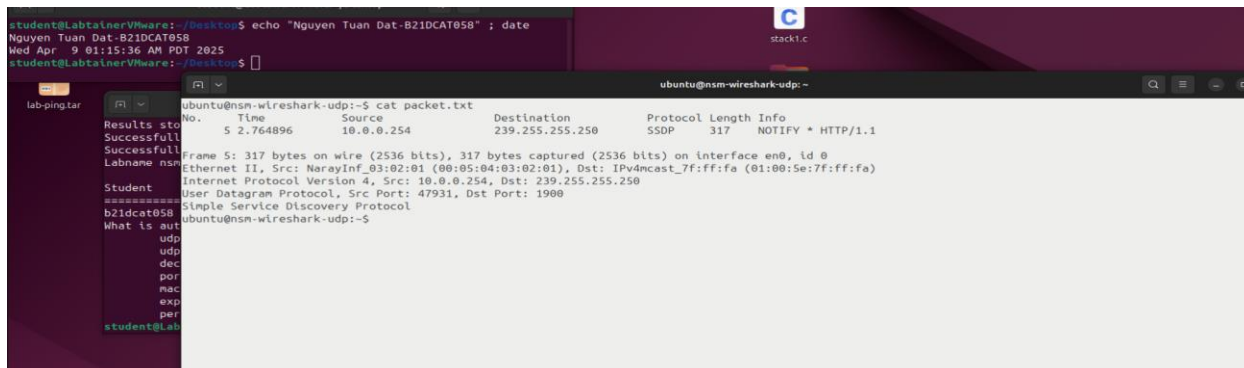
Trên máy nsm-wireshark-udp mở file UDP_answer chứa câu hỏi và form điền kết quả

Bài lab đã tạo sẵn 1 file UDP_answer trong đó chứa nội dung là 1 chuỗi ngẫu nhiên và checkwork bằng mã hash đó để chống học sinh chống sao chép bài làm của nhau

Sinh viên đọc câu hỏi và phân tích các gói tin , kết quả sẽ điền vào file UDP_answer và có những câu hỏi sinh viên phải export bản ghi chứa kết quả để checkwork để chứng minh sinh viên đã làm bài

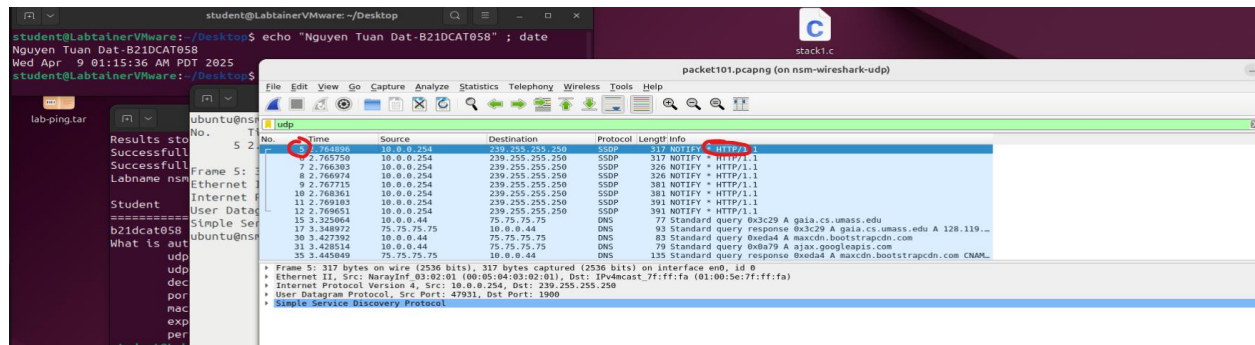
Task 1: export gói tin udp đầu tiên và in ra thông tin gói tin đó

Sử dụng bộ lọc **UDP**



Task 2: So hieu gọi tin của UDP segment này là bao nhiêu? Loại dữ liệu nào của tầng ứng dụng được chứa trong gói tin UDP này?

➔ udp segment no = 5 and data of application layer = http

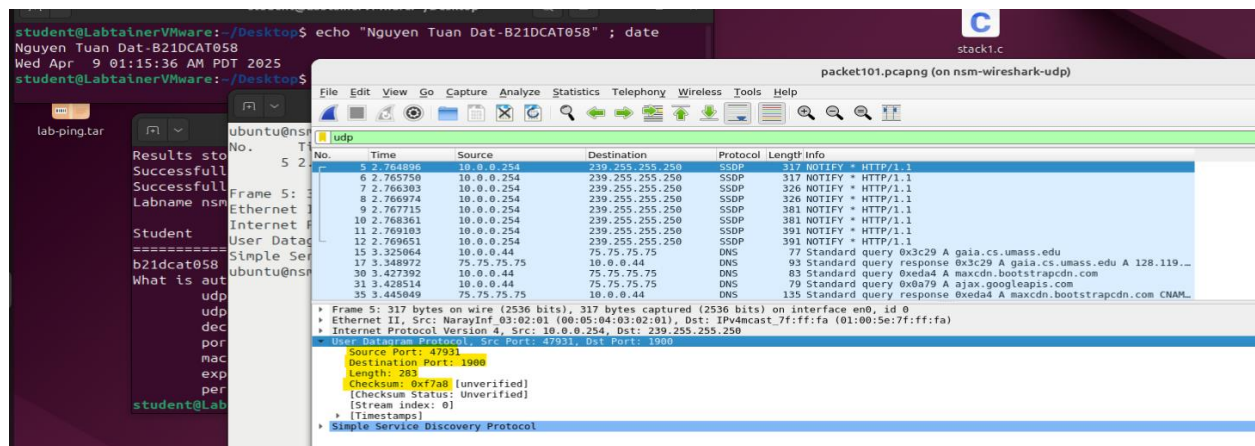


Task 3: Phân header của gói tin UDP này gồm bao nhiêu trường dữ liệu. Cho biết độ dài của mỗi trường trong header của gói tin UDP

Thông tin chuẩn của UDP header:

- Gồm 4 trường:
 1. Source Port (16 bits)
 2. Destination Port (16 bits)
 3. Length (16 bits)
 4. Checksum (16 bits)

➔ udp header has 4 fields and each field size = 16 bits



Task 4: Gia tri truong Length cua UDP header la bao nhieu? (Tra loi bang ca gia tri thap luc phan va thap phan) . So hieu dai dien cho giao thuc cua UDP la bao nhieu? (Tra loi bang ca gia tri thap luc phan va thap phan)

➔ **udp header length = 283(decimal)/0x011b(hexadecimal) and protocol = 17(decimal)/0x11(hexadecimal)**

The screenshot shows a terminal window on the left and a Wireshark packet capture window on the right. The terminal output is as follows:

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 01:15:36 AM PDT 2025
student@LabtainerVMware:~/Desktop$
```

The Wireshark window shows a packet capture of 'packet101.pcapng (on nsm-wireshark-udp)'. The packet list shows several packets, with the selected packet (No. 5) having a source of 10.0.0.254 and a destination of 239.255.255.250. The packet details pane shows the following fields:

- Ethernet II, Src: Narayini (08:00:04:03:02:01), Dst: IPv4mcast_7:ffff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 10.0.0.254, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 47931, Dst Port: 1900
 - Source Port: 47931
 - Destination Port: 1900
 - Length: 283
 - Checksum: 0xf7a8 (unverified)
 - (Checksum Status: Unverified)
 - (Stream index: 0)

Task 5: Gia tri toi da cua truong du lieu do bang bytes cua mot goi tin UDP la bao nhieu? Truong cong (port) chua trong mot UDP header la bao nhieu?

UDP Data size = UDP Length field - 8 (UDP Header)

UDP Data = 283 - 8 = 275 bytes

➔ **Source Port and Destination Port = 47931 and 1900; udp data max = 275**

The screenshot shows a terminal window on the left and a Wireshark packet capture window on the right. The terminal output is as follows:

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "Nguyen Tuan Dat-B21DCAT058" ; date
Nguyen Tuan Dat-B21DCAT058
Wed Apr  9 01:15:36 AM PDT 2025
student@LabtainerVMware:~/Desktop$
```

The Wireshark window shows a packet capture of 'packet101.pcapng (on nsm-wireshark-udp)'. The packet list shows several packets, with the selected packet (No. 5) having a source of 10.0.0.254 and a destination of 239.255.255.250. The packet details pane shows the following fields:

- Ethernet II, Src: Narayini (08:00:04:03:02:01), Dst: IPv4mcast_7:ffff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 10.0.0.254, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 47931, Dst Port: 1900
 - Source Port: 47931
 - Destination Port: 1900
 - Length: 283
 - Checksum: 0xf7a8 (unverified)
 - (Checksum Status: Unverified)
 - (Stream index: 0)

Task 6: Hay cho biet dia chi MAC dich cua goi du lieu do

➔ MAC destination = 01:00:5e:7f:ff:fa

student@LabtainerVMware: ~/Desktop
Nguyen Tuan Dat-B21DCAT058
Wed Apr 9 01:15:36 AM PDT 2025
student@LabtainerVMware:~/Desktop\$ echo "Nguyen Tuan Dat-B21DCAT058" ; date

packet101.pcapng (on nsm-wireshark-udp)

No.	Time	Source	Destination	Protocol	Length	Info
6	2.765750	10.0.0.254	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
7	2.766303	10.0.0.254	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
8	2.766974	10.0.0.254	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
9	2.767715	10.0.0.254	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
10	2.768361	10.0.0.254	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
11	2.769103	10.0.0.254	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
12	2.769651	10.0.0.254	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
15	3.325664	10.0.0.44	75.75.75.75	DNS	77	Standard query 0x3c29 A gaia.cs.umass.edu
17	3.348972	75.75.75.75	10.0.0.44	DNS	93	Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119...
30	3.427392	10.0.0.44	75.75.75.75	DNS	83	Standard query 0xed44 A maxcdn.bootstrapcdn.com
31	3.428514	10.0.0.44	75.75.75.75	DNS	79	Standard query 0xd079 A ajax.googleapis.com
35	3.445849	75.75.75.75	10.0.0.44	DNS	135	Standard query response 0xed44 A maxcdn.bootstrapcdn.com CNAM...

Frame 5: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface en0, id 0
Ethernet II, Src: NarayInf 03:02:01:00:05:04:03:02:01, Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Address: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
...0... = LG bit: Globally unique address (factory default)
...1... = IG bit: Group address (multicast/broadcast)
Source: NarayInf 03:02:01:00:05:04:03:02:01
Address: NarayInf 03:02:01:00:05:04:03:02:01
...0... = LG bit: Globally unique address (factory default)
...0... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.254, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 47931, Dst Port: 1900
Simple Service Discovery Protocol

Kết thúc bài lab:

Checkwork

student@LabtainerVMware: ~/Desktop
Nguyen Tuan Dat-B21DCAT058
Wed Apr 9 01:15:36 AM PDT 2025
student@LabtainerVMware:~/Desktop\$ echo "Nguyen Tuan Dat-B21DCAT058" ; date

Results stored in directory: /home/student/labtainer_xfer/nsm-wireshark-udp
Successfully copied 46.4kB to nsm-wireshark-udp-igrader:/home/instructor/b21dc058.nsm-wireshark-udp.lab
Successfully copied 3.07kB to /home/student/labtainer_xfer/nsm-wireshark-udp
Labname nsm-wireshark-udp

Student	export_packet	personalization	udp_segment	udp_header	decimal_hexadec	port_maxdata	mac_des
b21dc058	Y	Y	Y	Y	Y	Y	Y

What is automatically assessed for this lab:
udp_segment: student read the packet details to find the result
udp_header: student understand the theory related to the UDP header to answer the question
decimal_hexadecimal: student read additional details about the User Datagram Protocol to find the result
port_maxdata: student read additional details about the User Datagram Protocol to find the result
mac_des: student read additional details about Ethernet II to find the result
export_packet: student export the first packet and print its content
personalization: A unique hash is generated to identify each student's submission

student@LabtainerVMware:~/Desktop\$

ubuntu@nsm-wireshark-udp:~\$ cat UDP_answer.txt

- Task 1: export gói tin udp đầu tiên và in ra thông tin gói tin đó
- Chon segment UDP đầu tiên và tra lời các câu hỏi sau:
- Task 2: So hieu gói tin của UDP segment này là bao nhiêu? Loại du lieu nao của tang ung dung duoc chua trong gói tin UDP này?
+ udp segment no = 5 and data of application layer = HTTP
- Task 3: Phan header của gói tin UDP này gom bao nhiêu trường du lieu. Cho biet do dai của moi trường trong header của gói tin UDP
+ udp header has 4 fields and each field size = 16 bits
- Task 4: Giá trị trường Length của UDP header là bao nhiêu? Tra loi bang ca giá trị thập lục phân và thập phân
+ So hieu dat dien cho giao thuc của UDP là bao nhiêu? Tra loi bang ca giá trị thập lục phân và thập phân
+ udp header length = 283(decimal)/0x011b(hexadecimal) and protocol = 17(decimal)/0x11(hexadecimal)
- Task 5: Giá trị toi da của trường du lieu do bang bytes của mot gói tin UDP là bao nhiêu? Trường cong (port) chua trong mot UDP header là bao nhiêu?
+ Source Port and Destination Port = 47931 and 1900; udp data max = 275
- Task 6: Hay cho biet dia chi MAC dich của gói du lieu do
+ MAC destination = 01:00:5e:7f:ff:fa
MSV:7a0b0af8478381af373afc5252f79

ubuntu@nsm-wireshark-udp:~\$