

## Nội dung và hướng dẫn bài thực hành

### Mục đích

Giúp sinh viên làm quen với công cụ phân tích mạng Wireshark và giao thức ICMP

### Yêu cầu đối với sinh viên

Có kiến thức cơ bản về công cụ Wireshark.

### Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ:

```
labtainer nsm-wireshark-icmp
```

(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)

Sau khi khởi động xong terminal ảo sẽ xuất hiện. Bài lab tạo sẵn một file icmp-qua chứa câu hỏi và chỉ dẫn của bài lab

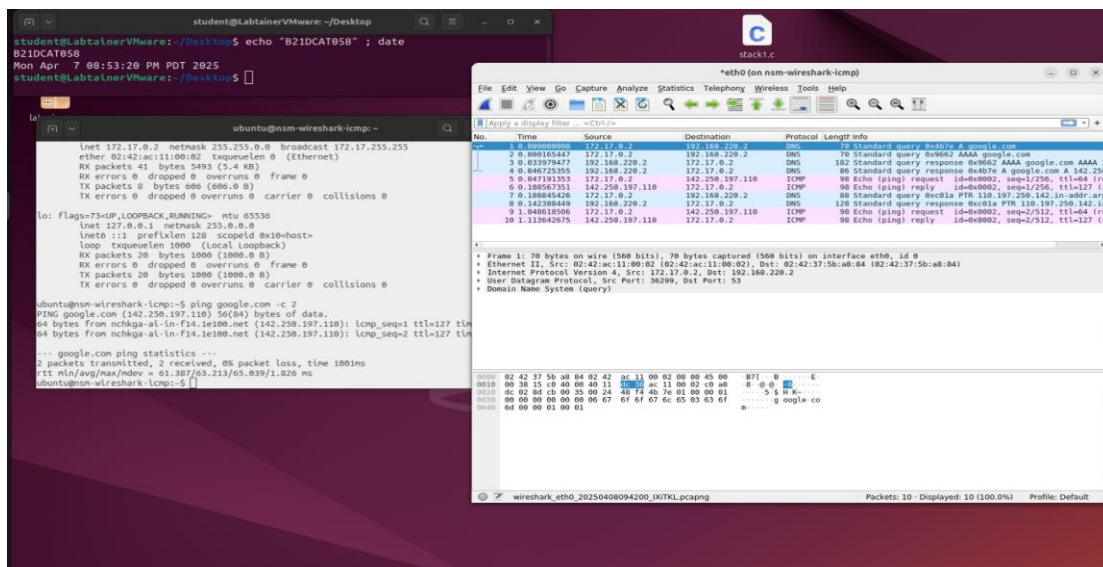
Sinh viên tạo thêm một terminal mới để mở wireshark

```
labtainer nsm-wireshark-icmp
```

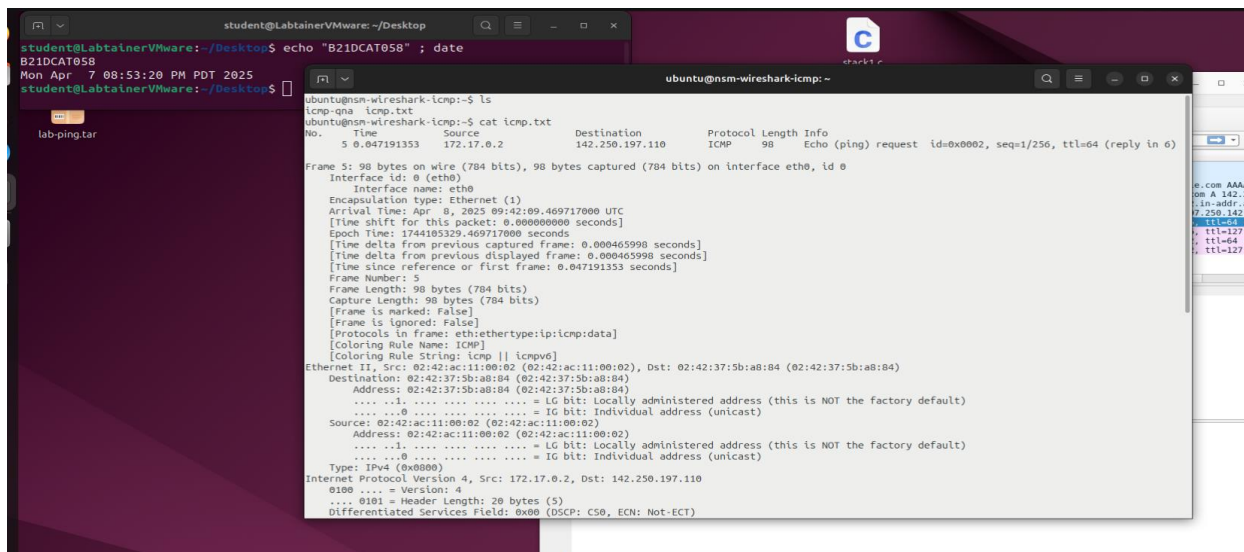
```
wireshark
```

Tại terminal còn lại sinh viên chạy lệnh ping bất kỳ (vd: google.com)

Ping google.com



Tại wireshark sinh viên chọn eth0 để xem các gói tin bắt được. chọn một gói ping request bất kỳ rồi export ra file icmp.txt. Lưu ý phải mở rộng tất cả các trường trước khi export

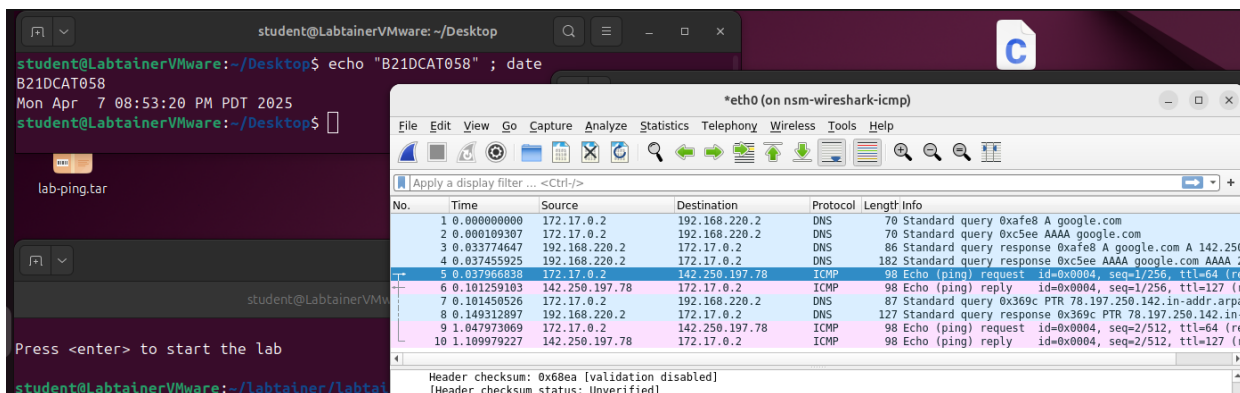


Sau khi export file thành công, sinh viên mở lại file `icmp-qna` để trả lời câu hỏi liên quan đến gói tin vừa bắt được

*nano icmp-qna*

Các câu hỏi trong bài thực hành này bao gồm:

- Gói tin có số cổng nguồn và đích không? Không
- Số thứ tự của gói tin: 5



- Địa chỉ nguồn: 172.17.0.2

The screenshot shows a terminal window on the left and a Wireshark window on the right. In the terminal, the user runs the command `echo "B21DCAT058" ; date`, which outputs `B21DCAT058` and `Mon Apr 7 08:53:20 PM PDT 2025`. The Wireshark window shows a packet capture with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.0.2	142.250.197.78	ICMP	60	Source: 172.17.0.2

- Địa chỉ đích: 142.250.197.78

The screenshot shows a terminal window on the left and a Wireshark window on the right. In the terminal, the user runs the command `echo "B21DCAT058" ; date`, which outputs `B21DCAT058` and `Mon Apr 7 08:53:20 PM PDT 2025`. The Wireshark window shows a packet capture with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.0.2	142.250.197.78	ICMP	60	Destination: 142.250.197.78

- Giá trị trường type number: 8

The screenshot shows a terminal window on the left and a Wireshark window on the right. In the terminal, the user runs the command `echo "B21DCAT058" ; date`, which outputs `B21DCAT058` and `Mon Apr 7 08:53:20 PM PDT 2025`. The Wireshark window shows a packet capture with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.0.2	142.250.197.78	ICMP	60	Type: 8 (Echo (ping) request)

- Giá trị trường code number: 0

The screenshot shows a terminal window on the left and a Wireshark window on the right. In the terminal, the user runs the command `echo "B21DCAT058" ; date`, which outputs `B21DCAT058` and `Mon Apr 7 08:53:20 PM PDT 2025`. The Wireshark window shows a packet capture with the following details:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.17.0.2	142.250.197.78	ICMP	60	Code: 0

- Giá trị trường checksum: 0x9b75

The screenshot shows two windows. The left window is a terminal with the following commands and output:

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

The right window is a Wireshark terminal with the following commands and output:

```
ubuntu@nsm-wireshark-icmp:~$ cat icmp.txt | grep Checksum
Checksum: 0x9b75 [correct]
[Checksum Status: Good]
ubuntu@nsm-wireshark-icmp:~$
```

- Giá trị trường Sequence Number (BE): 1

The screenshot shows two windows. The left window is a terminal with the following commands and output:

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

The right window is a Wireshark terminal with the following commands and output:

```
ubuntu@nsm-wireshark-icmp:~$ cat icmp.txt | grep Sequen
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
ubuntu@nsm-wireshark-icmp:~$
```

- Giá trị trường Identifier(BE)

The screenshot shows two windows. The left window is a terminal with the following commands and output:

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$
```

The right window is a Wireshark terminal with the following commands and output:

```
ubuntu@nsm-wireshark-icmp:~$ cat icmp.txt | grep Ident
Identification: 0xd162 (53602)
Identifier (BE): 4 (0x0004)
Identifier (LE): 1024 (0x0400)
ubuntu@nsm-wireshark-icmp:~$
```

Định dạng lại file icmp.txt để có thể checkwork:

```
sed -i 's/^[[:space:]]*/' icmp.txt
```

Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

```
stoplab
```

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Khởi động lại bài lab:

Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer -r nsm-wireshark-icmp*

```
student@LabtainerVMware: ~/Desktop
student@LabtainerVMware:~/Desktop$ echo "B21DCAT058" ; date
B21DCAT058
Mon Apr 7 08:53:20 PM PDT 2025
student@LabtainerVMware:~/Desktop$

lab-ping.tar

student@LabtainerVMware: ~/labtainer/labtainer
Press <enter> to start the lab

student@LabtainerVMware:~/labtainer/labtainer-student$ check
Results stored in directory: /home/student/labtainer_xfer/ns
Successfully copied 47.6kB to nsm-wireshark-icmp-igrader:/ho
Successfully copied 2.05kB to /home/student/labtainer_xfer/n
Labname nsm-wireshark-icmp

Student | ICMP-file | Answer |
=====|=====|=====|
b21dcat058 | Y |
What is automatically assessed for this lab:
wireshark: Did the student run Wireshark?
ping: Did the student run ping?

student@LabtainerVMware:~/labtainer/labtainer-student$ check
Results stored in directory: /home/student/labtainer_xfer/ns
Successfully copied 47.6kB to nsm-wireshark-icmp-igrader:/ho
Successfully copied 2.05kB to /home/student/labtainer_xfer/n
Labname nsm-wireshark-icmp

Student | ICMP-file | Answer | wireshark | ping |
=====|=====|=====|=====|=====|
b21dcat058 | Y | Y | Y | Y |
What is automatically assessed for this lab:
wireshark: Did the student run Wireshark?
ping: Did the student run ping?

student@LabtainerVMware:~/labtainer/labtainer-student$
```

```
ubuntu@nsm-wireshark-icmp:~$ nano icmp-qna
ubuntu@nsm-wireshark-icmp:~$ cat icmp-qna
1. ping to any address and capture with Wireshark (example: ping google.com)

2. Does ICMP packet have source and destination port?
Answer: No

3. Export a ping request packet to icmp.txt (expand all) and answer
Packet number: 5
Source: 172.17.0.2
Destination: 142.250.197.78
Type number: 8
Code number: 0
Checksum: 0x9b75 [correct]
Sequence Number(BE): 1 (0x0001)
Identifier(BE): 4 (0x0004)
Run: " sed -i 's/^[:space:]*// ' icmp.txt " before checkwork
ubuntu@nsm-wireshark-icmp:~$ sed -i 's/^[:space:]*// ' icmp.txt
ubuntu@nsm-wireshark-icmp:~$
```