

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH TN (CO3094)

BÀI TẬP LAB 4A

WIRESHARK IP

LỚP: L09

GVHD: Bùi Xuân Giang

Sinh viên thực hiện

Nguyễn Tấn Tài : 2212990

Thành phố Hồ Chí Minh, tháng 11 năm 2024

1. Capturing packets from an execution of traceroute

Để tạo một dấu vết của các gói IP cho bài thực hành này, chúng ta sẽ sử dụng chương trình traceroute để gửi các gói dữ liệu với kích thước khác nhau tới một điểm đến Y. Hãy nhớ rằng traceroute hoạt động bằng cách đầu tiên gửi một hoặc nhiều gói dữ liệu có giá trị time-to-live (TTL) trong tiêu đề IP được đặt là 1; sau đó, nó gửi một chuỗi các gói hoặc nhiều gói tới cùng một đích với TTL bằng 2; sau đó, nó gửi một chuỗi các gói tới cùng một đích với TTL bằng 3; và cứ thế tiếp tục. Hãy nhớ rằng mỗi bộ định tuyến phải giảm giá trị TTL trong mỗi gói dữ liệu nhận được đi 1 (thực tế, RFC 791 quy định rằng bộ định tuyến phải giảm TTL ít nhất là 1). Nếu TTL giảm xuống 0, bộ định tuyến trả về một thông điệp ICMP (kiểu 11 – TTL bị vượt quá) tới máy gửi. Do hành vi này, một gói dữ liệu với TTL là 1 (gửi bởi máy chủ thực thi traceroute) sẽ khiến bộ định tuyến ở nút tiếp theo tính từ máy gửi gửi một thông điệp ICMP TTL-vượt quá ngược về cho máy gửi; gói dữ liệu với TTL là 2 sẽ khiến bộ định tuyến hai bước đi gửi một thông điệp ICMP ngược về cho máy gửi; gói dữ liệu với TTL là 3 sẽ khiến bộ định tuyến ba bước đi gửi một thông điệp ICMP ngược về cho máy gửi; và cứ thế tiếp tục. Bằng cách này, máy chủ chạy traceroute có thể tìm ra danh tính của các bộ định tuyến giữa nó và đích Y bằng cách xem địa chỉ IP nguồn trong các gói dữ liệu chứa thông điệp ICMP TTL-vượt quá.

Chúng ta sẽ chạy traceroute và để nó gửi các gói dữ liệu với các độ dài khác nhau.

Windows: Chương trình tracert (dùng cho phòng thí nghiệm ICMP Wireshark của chúng ta) có sẵn trong Windows nhưng không cho phép thay đổi kích thước của gói dữ liệu ICMP echo (yêu cầu ping) mà nó gửi. Một chương trình traceroute trên Windows tốt hơn là pingplotter, có sẵn ở cả phiên bản miễn phí và phiên bản shareware tại <http://www.pingplotter.com>. Hãy tải xuống và cài đặt pingplotter, và kiểm tra nó bằng cách thực hiện một vài traceroutes tới các trang web yêu thích của bạn. Kích thước của yêu cầu ICMP echo có thể được chỉ định rõ ràng trong pingplotter bằng cách chọn mục menu Edit -> Options -> Packet Options và sau đó điền vào trường Packet Size. Kích thước gói mặc định là 56 byte. Một khi pingplotter đã gửi một loạt gói tin với giá trị TTL tăng dần, nó sẽ khởi động lại quá trình gửi với TTL bằng 1, sau khi chờ một khoảng thời gian Trace Interval. Giá trị của Trace Interval và số lượng khoảng thời gian có thể được chỉ định rõ ràng trong pingplotter.

Thực hiện các bước sau:

Nếu bạn sử dụng một nền tảng Windows, khởi động pingplotter và nhập tên hoặc địa chỉ của đích vào trong “Address to Trace”. Nhập số “# of times to Trace” thành 3, để không mất quá nhiều dữ liệu. Chọn mục menu Edit -> Advanced Options -> Packet Options và nhập giá trị là 56 trong trường Packet Size rồi nhấn OK. Sau đó nhấn nút Trace.

Tiếp theo, gửi một loạt các gói dữ liệu có độ dài lớn hơn, bằng cách chọn Edit -> Advanced Options -> Packet Options và nhập giá trị là 2000 trong trường Packet Size, sau đó nhấn OK. Sau đó nhấn nút Resume.

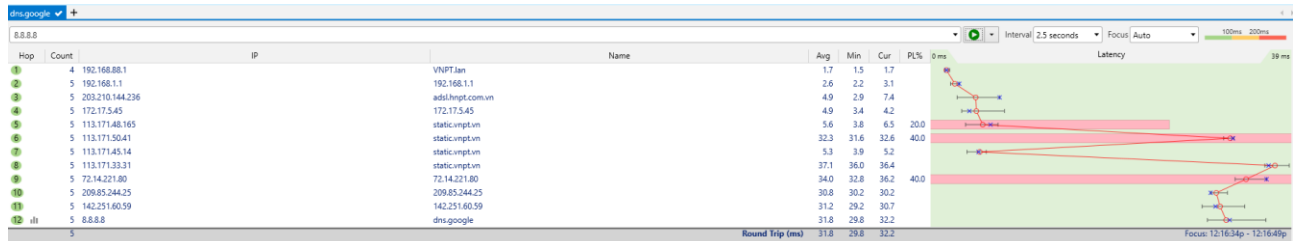
Cuối cùng, gửi một loạt các gói dữ liệu với độ dài lớn hơn nữa, bằng cách chọn Edit -> Advanced Options -> Packet Options và nhập giá trị là 3500 trong trường Packet Size rồi nhấn OK. Sau đó nhấn nút Resume.

Nếu bạn không thể chạy Wireshark trên kết nối mạng thực, bạn có thể tải xuống tệp dấu vết gói đã được thu thập khi theo dõi các bước ở trên trên một máy tính Windows của tác giả.

2. A look at the captured trace

Trong dấu vết của bạn, bạn sẽ có thể thấy chuỗi các yêu cầu ICMP Echo Request (trong trường hợp là máy Windows) hoặc phân đoạn UDP (trong trường hợp là Unix) được gửi bởi máy tính của bạn và các thông điệp ICMP TTL-vượt quá được gửi trả về máy tính của bạn bởi các bộ định tuyến trung gian. Trong các câu hỏi dưới đây, chúng ta sẽ giả định rằng bạn đang sử dụng máy Windows; các câu hỏi tương ứng cho trường hợp của máy Unix sẽ rõ ràng. Bất cứ khi nào có thể, khi trả lời một câu hỏi bên dưới, bạn nên đính kèm bản in của gói tin mà bạn đã sử dụng để trả lời câu hỏi được yêu cầu. Khi bạn nộp bài, chú thích đầu ra để rõ ràng nơi mà trong đầu ra bạn tìm thấy thông tin cho câu trả lời của mình (ví dụ, cho lớp học của chúng tôi, chúng tôi yêu cầu sinh viên đánh dấu các bản sao giấy bằng bút, hoặc chú thích các bản sao điện tử bằng văn bản với phong chữ màu). Để in một gói tin, sử dụng File -> Print, chọn Selected packet only, chọn Packet summary line, và chọn mức chi tiết tối thiểu của gói tin mà bạn cần để trả lời câu hỏi.

1. Chọn gói ICMP Echo Request đầu tiên được gửi bởi máy tính của bạn và mở rộng phần Giao thức Internet của gói trong cửa sổ chi tiết gói. Địa chỉ IP của máy tính của bạn ?



No.	Time	Source	Destination	Protocol	Length	Info
1	12:16:23.194133	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3028/54283, ttl=4 (no response found)
2	12:16:23.194887	192.177.5.45	192.168.88.159	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
3	12:16:23.245881	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3029/54539, ttl=5 (no response found)
4	12:16:23.251137	192.177.5.45	192.168.88.159	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
5	12:16:23.295649	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3030/54795, ttl=6 (no response found)
6	12:16:23.325206	113.171.50.41	192.168.88.159	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
14	12:16:23.346075	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3031/55051, ttl=7 (no response found)
16	12:16:23.351562	113.171.45.14	192.168.88.159	ICMP	182 Time-to-live exceeded	(Time to live exceeded in transit)
28	12:16:23.397376	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3032/55307, ttl=8 (no response found)
33	12:16:23.433268	113.171.33.31	192.168.88.159	ICMP	70 Time-to-live exceeded	(Time to live exceeded in transit)
34	12:16:23.447180	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3033/55563, ttl=9 (no response found)
35	12:16:23.497521	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3034/55819, ttl=10 (no response found)
36	12:16:23.501495	72.14.221.80	192.168.88.159	ICMP	110 Time-to-live exceeded	(Time to live exceeded in transit)
41	12:16:23.522765	209.65.244.95	192.168.88.159	ICMP	110 Time-to-live exceeded	(Time to live exceeded in transit)
42	12:16:23.640300	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3035/56255, ttl=11 (no response found)
45	12:16:23.677480	142.253.60.59	192.168.88.159	ICMP	98 Time-to-live exceeded	(Time to live exceeded in transit)
47	12:16:23.599754	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3036/56331, ttl=12 (reply in 48)
49	12:16:23.649408	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3037/56587, ttl=255 (reply in 51)
53	12:16:23.699811	192.168.88.159	8.8.8.8	ICMP	70 Echo (ping) request	id=0x0001, seq=3038/56843, ttl=1 (no response found)

No.	Time	Source	Destination	Protocol	Length	Info
1	12:16:23.194133	192.168.88.159	8.8.8.8	ICMP	70	Echo (ping) request id=0x0001, seq=3028/54283,
ttl=4 (no response found!)						
Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}, id 0						
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)						
Internet Protocol Version 4, Src: 192.168.88.159, Dst: 8.8.8.8						
Internet Control Message Protocol						
[Community ID: 1]wLdrik/2nN?OmChHqCMV7T>PmOmM=1						

IP address of my computer: 192.168.88.159.

2. Trong tiêu đề gói IP, giá trị trong trường giao thức tầng trên là gì?

The value in the Protocol field indicates the type of upper layer protocol: For **ICMP**, the Protocol field value is **1**; If it's **TCP**, the value is **6**; If it's UDP, the value is 17.

```
Internet Protocol Version 4, Src: 192.168.88.159, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
Identification: 0xa075 (41077)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 4
[Expert Info (Note/Sequence): "Time To Live" only 4]
[Time To Live" only 4]
[Severity level: Note]
[Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.88.159
Destination Address: 8.8.8.8
[Stream index: 0]
```

The value in the upper layer protocol field is **1**, indicating that this is the **ICMP** protocol.

3. Có bao nhiêu byte trong tiêu đề IP? Có bao nhiêu byte trong tải trọng của gói dữ liệu IP? Giải thích cách bạn xác định số byte tải trọng.

```
Internet Protocol Version 4, Src: 192.168.88.159, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
Identification: 0xa075 (41077)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
..0. .... = Don't fragment: Not set
...0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 4
[Expert Info (Note/Sequence): "Time To Live" only 4]
[Time To Live" only 4]
[Severity level: Note]
[Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.88.159
Destination Address: 8.8.8.8
[Stream index: 0]
```

IP Header Size: 20 bytes. This is determined from the **Header Length** field, which has a value of 5 (equivalent to $5 \times 4 \text{ bytes} = 20 \text{ bytes}$).

Payload Size: 36 bytes. The **Total Length** of the IP datagram is 56 bytes. Subtracting the IP header length (20 bytes) gives:

$$56 - 20 = 36 \text{ bytes}$$

4. Gói dữ liệu IP này có bị phân mảnh không? Giải thích cách bạn xác định gói tin có bị phân mảnh hay không.

```
Internet Protocol Version 4, Src: 192.168.88.159, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 56
Identification: 0xa075 (41077)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
..0. .... = Don't fragment: Not set
...0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 4
[Expert Info (Note/Sequence): "Time To Live" only 4]
[Time To Live" only 4]
[Severity level: Note]
[Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.88.159
Destination Address: 8.8.8.8
[Stream index: 0]
```

This IP datagram **has not been fragmented**. This is determined by the **More Fragments** flag, which is set to 0, and the **Fragment Offset** field, which is also 0.

Tiếp theo, sắp xếp các gói tin theo địa chỉ nguồn IP bằng cách nhấp vào tiêu đề cột Source; một mũi tên nhỏ hướng xuống sẽ xuất hiện bên cạnh chữ Source. Nếu mũi tên chỉ lên, nhấp vào tiêu đề cột Source một lần nữa. Chọn gói ICMP Echo Request đầu tiên được gửi bởi máy tính của bạn và mở rộng phần Giao thức Internet trong "các chi tiết của tiêu đề gói tin đã chọn" trong cửa sổ chi tiết gói. Trong "danh sách các gói tin đã thu được", bạn sẽ thấy tất cả các thông điệp ICMP tiếp theo (có thể xen kẽ với các gói tin được gửi bởi các giao thức khác đang chạy trên máy tính của bạn) bên dưới gói ICMP đầu tiên này. Sử dụng mũi tên xuống để di chuyển qua các thông điệp ICMP được gửi bởi máy tính của bạn.

No.	Time	Source	Destination	Protocol	Length	Info
141	12:16:25.647566	203.210.144.236	192.168.88.159	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
59	12:16:23.805115	203.210.144.236	192.168.88.159	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1573	12:16:54.358863	192.168.88.159	8.8.8.8	ICMP	70	Echo (ping) request id=0x0001, seq=3454/32269, ttl=12 (reply in 1574)
1571	12:16:54.307732	192.168.88.159	8.8.8.8	ICMP	70	Echo (ping) request id=0x0001, seq=3453/32013, ttl=11 (no response found!)
1569	12:16:54.257872	192.168.88.159	8.8.8.8	ICMP	70	Echo (ping) request id=0x0001, seq=3452/31757, ttl=10 (no response found!)
1567	12:16:54.206814	192.168.88.159	8.8.8.8	ICMP	70	Echo (ping) request id=0x0001, seq=3451/31501, ttl=9 (no response found!)
1565	12:16:54.156508	192.168.88.159	8.8.8.8	ICMP	70	Echo (ping) request id=0x0001, seq=3450/31245, ttl=8 (no response found!)
1563	12:16:54.126903	192.168.88.159	113.171.12.211	TCP	55	58653 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1

5. Các trường nào trong gói IP luôn thay đổi từ một gói tin này sang gói tin khác trong chuỗi các thông điệp ICMP này được gửi bởi máy tính của bạn?

No. Time
1 12:16:23.194133
ttl=4 (no response found!)

```
Internet Protocol Version 4, Src: 192.168.88.15
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP:
0000 00.. = Differentiated Services Cod
.... ..00 = Explicit Congestion Notific
Total Length: 56
Identification: 0xa075 (41077)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
```

No. Time
1573 12:16:54.358863
ttl=12 (reply in 1574)

```
Internet Protocol Version 4, Src: 192.168.88.1
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP:
0000 00.. = Differentiated Services Co
.... ..00 = Explicit Congestion Notifi
Total Length: 56
Identification: 0xa21f (41503)
000. .... = Flags: 0x0
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
```

So sánh với gói được dùng để mô tả, trả lời 4 câu hỏi ở phía trên (bên trái) và gói thỏa mãn yêu cầu sắp xếp theo source (bên phải)

The Identification and Time to Live (TTL) fields change in each IP datagram. The Identification field changes to give each packet a unique identifier, and the TTL field changes based on the number of hops.

6. Các trường nào luôn giữ nguyên? Trường nào phải giữ nguyên? Trường nào phải thay đổi? Tại sao?

```
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.88.159
Destination Address: 8.8.8.8
[Stream index: 0]
```

Fields that stay constant: The Source Address and Destination Address stay constant, as the packets are sent from your computer to the same destination. The Protocol field also remains constant since all packets are ICMP.

Fields that must change: The Identification field must change to differentiate between packets and avoid confusion with fragmented packets. The TTL field changes as each packet traverses a router to prevent endless looping.

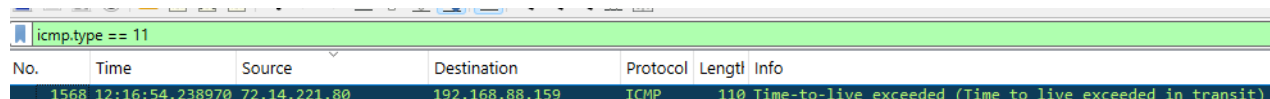
7. Mô tả mẫu mà bạn thấy trong các giá trị trường Identification của gói dữ liệu IP.

The Identification field increments with each new ICMP packet, providing a unique identifier for each packet in the ICMP sequence. This helps distinguish each packet, especially in cases of fragmentation or packet tracking.

Tiếp theo (với các gói tin vẫn được sắp xếp theo địa chỉ nguồn), tìm chuỗi các thông điệp trả lời ICMP TTL-vượt quá được gửi tới máy tính của bạn bởi bộ định tuyến gần nhất (bộ định tuyến ở bước nhảy đầu tiên).

Trong Wireshark, nhấp vào tiêu đề cột **Source** để sắp xếp các gói tin theo địa chỉ nguồn. Đảm bảo rằng các gói tin có địa chỉ nguồn giống nhau sẽ được nhóm lại với nhau, giúp bạn dễ dàng tìm các gói tin đến từ cùng một router.

Trong thanh **Display Filter**, nhập bộ lọc sau để chỉ hiển thị các gói tin ICMP với thông điệp TTL Exceeded: **icmp.type == 11**. Bộ lọc này sẽ giúp chỉ thấy các gói tin ICMP TTL-vượt quá (TTL Exceeded) và loại bỏ các gói ICMP Echo Request hoặc Echo Reply khác.



No.	Time	Source	Destination	Protocol	Length	Info
1568	12:16:54.238970	72.14.221.80	192.168.88.159	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

8. Giá trị trong trường Identification và trường TTL là gì?

```

Internet Protocol Version 4, Src: 72.14.221.80, Dst: 192.168.88.159
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not Set)
    0010 00.. = Differentiated Services Codepoint: Class Selector 1
    .... ..00 = Explicit Congestion Notification: Not Set
  Total Length: 96
  Identification: 0xe422 (58402)
  000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 244
  Protocol: ICMP (1)
  Header Checksum: 0xa3b3 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 72.14.221.80
  Destination Address: 192.168.88.159
  [Stream index: 8]

```

The Identification field value is 0xe422 (hex) or 58402 (decimal).

The TTL field value is 244.

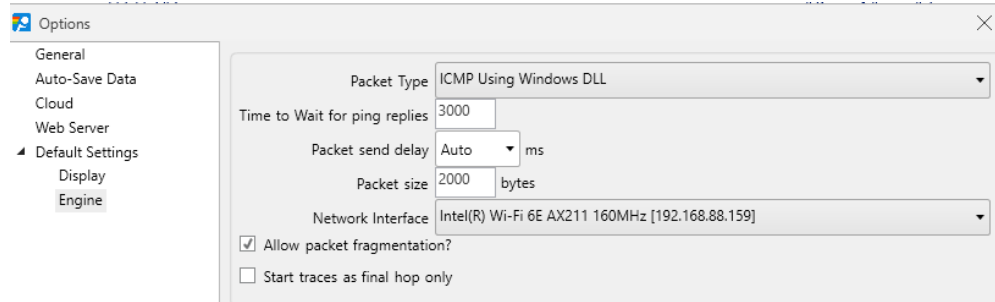
9. Các giá trị này có giữ nguyên không cho tất cả các thông điệp trả lời ICMP TTL-vượt quá được gửi tới máy tính của bạn bởi bộ định tuyến gần nhất (bước nhảy đầu tiên)? Tại sao?

Typically, the TTL value of the ICMP replies will remain the same when sent from the same router, as all packets start from that router to your computer without needing TTL changes.

However, the Identification field may vary for each packet because it is a unique value used to distinguish each individual packet.

Phân mảnh

Sắp xếp danh sách gói tin lại theo thời gian bằng cách nhấp vào cột Time.



10. Tìm gói ICMP Echo Request đầu tiên được gửi bởi máy tính của bạn sau khi bạn đã thay đổi Packet Size trong pingplotter thành 2000. Gói này có bị phân mảnh qua nhiều gói IP không? [Lưu ý: nếu gói của bạn chưa bị phân mảnh, bạn nên tải xuống tệp zip <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> và giải nén dấu vết ip-ethereal-trace-1packet. Nếu máy tính của bạn có giao diện Ethernet, một kích thước gói tin là 2000 nên gây ra phân mảnh.]

```
.... ..00 = Explicit Congestion Notification
Total Length: 1500
Identification: 0x10a0 (4256)
001. .... = Flags: 0x1, More fragments
  0... .... = Reserved bit: Not set
  .0... .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
...0 0000 0000 0000 = Fragment Offset: 0
```

Yes, this packet is fragmented. We can determine this because the More Fragments flag in the Flags field is set, and the Fragment Offset of the first fragment is 0.

11. In ra phân đoạn đầu tiên của gói IP bị phân mảnh. Thông tin nào trong tiêu đề IP cho biết rằng gói đã bị phân mảnh? Thông tin nào trong tiêu đề IP cho biết đây là phân đoạn đầu tiên so với một phân đoạn sau? Độ dài của gói dữ liệu IP này là bao nhiêu?

```
[Stream Index: 0]
Internet Protocol Version 4, Src: 192.168.88.159, Destination: 192.168.88.1
0100 .... = Version: 4
.... 0101 = Header Length: 10 (bytes)
Differentiated Services Field: 0000 (DSCP: CS0, ECN: Not Set)
0000 00.. = Differentiated Services Field: 0000 (DSCP: CS0, ECN: Not Set)
.... ..00 = Explicit Congestion Notification
Total Length: 1500
```

Information indicating fragmentation: The More Fragments flag is set (value 1), indicating that there are more fragments following this one.

Information indicating this is the first fragment: The **Fragment Offset** is **0**, indicating that this is the first fragment of the IP packet.

Length of this IP packet: The Total Length field shows the length of this fragment is 1514 bytes.

12. In ra phân đoạn thứ hai của gói IP bị phân mảnh. Thông tin nào trong tiêu đề IP cho biết đây không phải là phân đoạn đầu tiên của gói dữ liệu? Có phân đoạn nào khác không? Bạn xác định điều này bằng cách nào?

Information indicating this is not the first fragment: The Fragment Offset in the second fragment has a non-zero value (typically 1480 bytes for each subsequent fragment after the first).

Are there additional fragments? If the More Fragments flag is set, it means there are additional fragments. If the More Fragments flag is cleared (value 0), this is the last fragment.

13. Những trường nào thay đổi trong tiêu đề IP giữa phân đoạn đầu tiên và phân đoạn thứ hai?

Fragment Offset: This value changes between fragments to indicate the position of the fragment in the entire IP packet.

Total Length: The length of each fragment may vary depending on the remaining data size.

Flags: If it's the last fragment, the More Fragments flag will be cleared (value 0), while it remains set (value 1) for preceding fragments.

Bây giờ tìm gói ICMP Echo Request đầu tiên được gửi bởi máy tính của bạn sau khi bạn đã thay đổi Packet Size trong pingplotter thành 3500.

ip.id == 0x26bf						
No.	Time	Source	Destination	Protocol	Length	Info
1	13:11:12.096316	192.168.88.159	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=26bf) [Reassembled in #2]
2	13:11:12.096316	192.168.88.159	8.8.8.8	ICMP	534	Echo (ping) request id=0x0001, seq=37416/10386, ttl=8 (no response found!)

14. Có bao nhiêu phân đoạn được tạo ra từ gói dữ liệu ban đầu?

In the Info column, there is one IP packet with the label "Fragmented IP protocol", having a length of 1514 bytes, and another ICMP packet with a length of 534 bytes.

This image shows only **two fragments** of the original packet: one fragment with a size of 1514 bytes and the remaining fragment with a size of 534 bytes.

15. Những trường nào thay đổi trong tiêu đề IP giữa các phân đoạn?

Fragment Offset: This field changes between fragments to indicate the position of each fragment in the original packet. The first fragment has a Fragment Offset of 0, while the second fragment has a different offset value to indicate its position after the first fragment.

Flags (More Fragments): The More Fragments flag is set to 1 for the first fragment, indicating there are more fragments following it. For the last fragment, the More Fragments flag is set to 0, indicating it is the final fragment.

Total Length: The Total Length field changes between fragments to represent the size of each fragment. The initial fragment usually has the maximum allowed length (typically 1514 bytes including headers), while the last fragment may be smaller depending on the remaining data size.