

BÁO CÁO BÀI THỰC HÀNH SỐ 1 **Làm quen với Wireshark** Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Dương Thuận Trí (22521517)
Thời gian thực hiện	25/10/2023 – 1/11/2023
Tự chấm điểm	10/10

TRẢ LỜI CÁC CÂU HỎI

Câu 1:

IP address	192.168.222.186
MAC address	98-FA-9B-12-13-EC
Default gateway IP address	fe80::1a0f:76ff:fe92:f408%16 192.168.222.1
DNS server IP address	192.168.54.4 192.168.20.4

Câu 2: Tại danh sách các gói tin bắt được, định vị gói tin truy vấn domain google.com. Gợi ý: chứa "standard query" và "A <u>www.google.com</u>"

- Trả lời: Gói tin truy vấn domain google.com là gói tin số 346 có Source là 192.168.222.186 (IP address của máy) và Destination là 192.168.54.4 (IP address của DNS server)

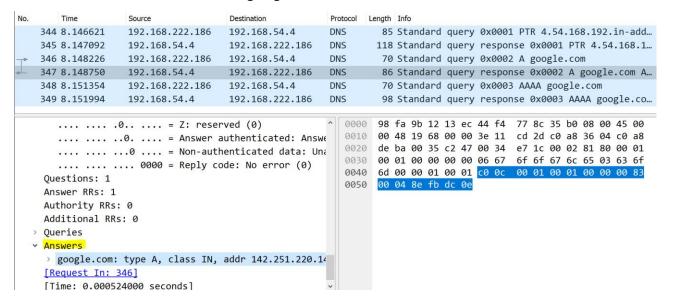
→ 346 8.148226 192.168.222.186 192.168.54.4 DNS 70 Standard query 0x0002 A google.com

Câu 3: Định vị gói tin phản hồi của truy vấn trên? Từ thông điệp trả lời, ghi lại địa chỉ IP của domain google.com

 Gói tin phản hồi của truy vấn trên là gói tin số 347, chứa thông điệp trả lời (Answers).

→ 347 8.148750 192.168.54.4 192.168.222.186 DNS 86 Standard query response 0x0002 A google.com A 142.251...

Địa chỉ IP của domain google.com là 142.251.220.14



Câu 4: Chọn một gói tin DNS, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó?

Lab 1: Làm quen với Wireshark

No.		Time	Source	Destination	Protoc	ol L	.ength	Info													
T►	344	8.146621	192.168.222.186	192.168.54.4	DNS		85	Sta	ndaı	rd o	query	0x	(000	1 PT	TR 4	.54	.16	8.1	92.	in-	ad
上	345	8.147092	192.168.54.4	192.168.222.186	DNS		118	Sta	ndaı	rd o	query	re	spo	nse	0x0	001	. PT	R 4	.54	1.16	8.
	346	8.148226	192.168.222.186	192.168.54.4	DNS		70	Sta	ındaı	rd (query	0x	(000)	2 A	goo	gle	.co	m			
	347	8.148750	192.168.54.4	192.168.222.186	DNS		86	Sta	ındaı	rd (query	re	spo	nse	0x0	002	Α	goo	gle	e.co	m
	348	8.151354	192.168.222.186	192.168.54.4	DNS		70	Sta	ındaı	rd o	query	0x	(000)	3 AA	AAA	goo	gle	.co	m		
	349	8.151994	192.168.54.4	192.168.222.186	DNS		98	Sta	ndaı	rd d	query	re	spo	nse	0x0	003	AA	AA	goo	gle	. c
			: 192.168.222.186			000					5 b0				12						
	Des	stination Add	dress: 192.168.54.4	1		010					0 00				00						
٧ ل	lser	Datagram Pro	tocol, Src Port: 4	9734, Dst Port: 53		020					0 35				54						
	Sou	irce Port: 49	9734			030					0 00				35						
	Des	stination Por	<mark>rt:</mark> 53			040 050		00 (9 6e	Zu	91	64	64	12	04	91	12	70	О.
	Ler	ngth: 51				050	90	00 (00 0	0	1										
	Che	ecksum: 0x965	54 [unverified]																		
	[Ch	necksum Statı	us: Unverified]																		
	[St	ream index:	61]																		
	Tj (imestamps]																			
	UDF	payload (43	B bytes)																		

- Các trường có trong UDP header là Source Port, Destination Port, Length, Checksum:
 - + Sources Port: cổng của người gửi thông tin
 - + Destination Port: cổng nhận thông tin
 - + Length: chiều dài của toàn bộ datagram (header và dữ liệu)
 - + Checksum: dùng để kiểm tra lỗi của header và dữ liệu.

Câu 5: Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?

Sources Port: 2 bytesDestination Port: 2 bytes

Length: 2 bytesChecksum: 2 bytes.

Vuser Datagram Protocol, Src Port: 49734, Dst Port: 53
Source Port: 49734
Destination Port: 53
Length: 51
Checksum: 0x9654 [unverified]
Source Port (udp.srcport), 2 bytes

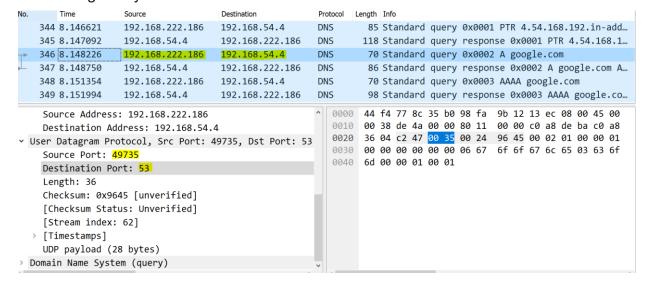
Câu 6: Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này

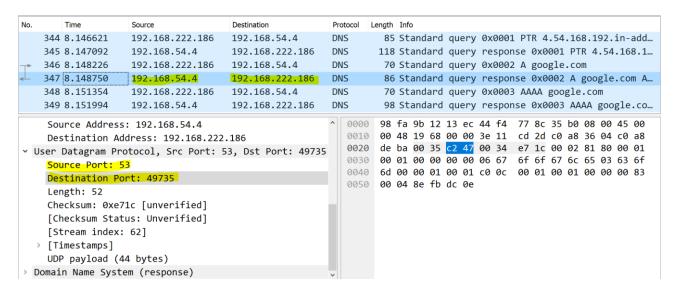
- Giá trị của trường Length trong UDP header là độ dài của toàn bộ datagram, bao gồm: phần header và dữ liêu

```
Vuser Datagram Protocol, Src Port: 49734, Dst Port: 53
    Source Port: 49734
    Destination Port: 53
    Length: 51
    Checksum: 0x9654 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 61]
    [Timestamps]
    UDP payload (43 bytes)
    Domain Name System (query)
    Length in octets including this header and the data (udp.length), 2 bytes
```

Câu 7: Quan sát 2 gói tin tìm được ở Câu 1 và 2, mô tả mối quan hệ giữa các địa chỉ IP và port number của 2 gói tin này.

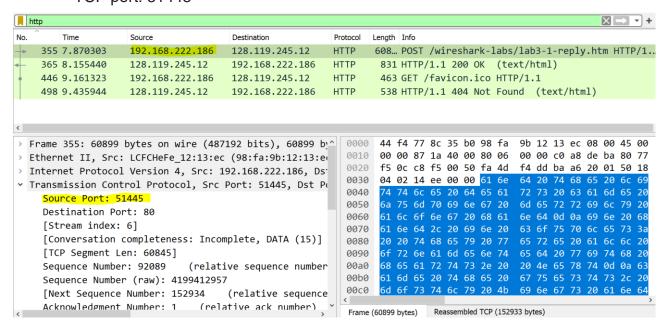
- Gói tin truy vấn domain có địa chỉ IP đích là địa chỉ IP của DNS server, và gói tin phản hồi được gửi từ DNS server có địa chỉ IP đích là máy tính đang sử dụng.
- Port number cũng tương tự: Source port của gói tin truy vấn domain là 49735,
 Destination Port là 53 (53 chính là port number của DNS server), ở gói tin phản hồi, Destination Port mà DNS server gửi tới chính là port number của máy tính đã gửi truy vấn.





Câu 8: Xác định IP và TCP port của client sử dụng để chuyển tệp sang gai.cs.umass.edu là gì?

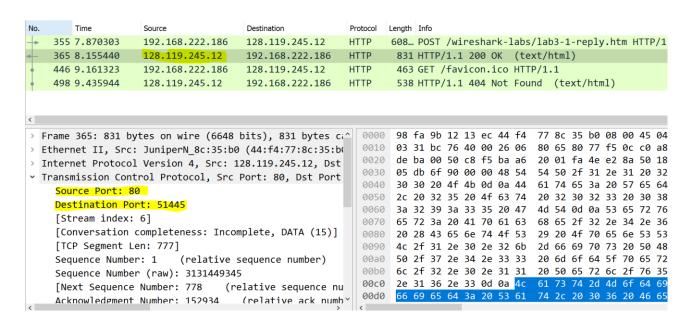
IP: 192.168.222.186TCP port: 51445



Câu 9: Địa chỉ của gaia.cs.umass.edu là gì? Trên số cổng nào nó gửi và nhận các segment TCP cho kết nối này?

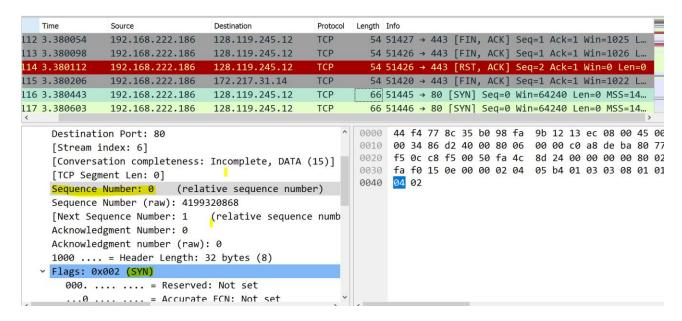
- Dia chỉ của gais.cs.umass.edu là 128.119.245.12

- gais.cs.umass.edu có số cổng gửi là 51445, số cổng nhận là 80.



Câu 10: TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment? Gợi ý: quan sát trường Flags

- TCP SYN segment sử dụng sequence number 0 để khởi tạo kết nối TCP giữa client và server.
- Kế bên trường Flags, tên segment được để cập là SYN. (và trường SYN được bật trong Flags)

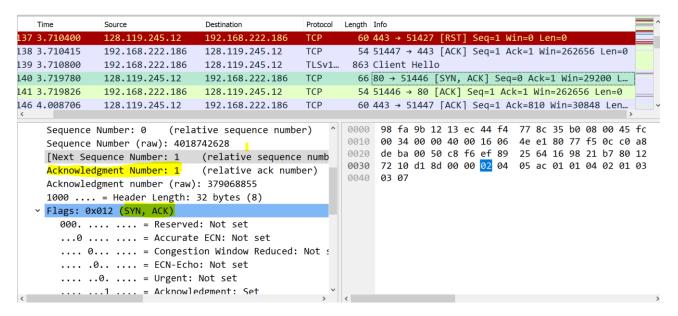


Câu 11: Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment?

 Sequence number của gói tin SYN/ACK segment là 0 (cùng sequence number với SYN segment)

Câu 12: Tìm giá trị của Acknowledgement trong SYN/ACK segment? Làm sao server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYN/ACK segment?

- Giá trị của của Acknowledgement trong SYN/ACK segment là 1.
- Server lấy Sequence number cộng thêm 1 để xác định giá trị ACK.
- Kế bên trường Flags, tên segment được đề cập là SYN/ACK segment.



Câu 13: Tìm độ dài của từng segment trong bộ 6 segments đầu tiên trên? Tìm lượng buffer còn trống nhỏ nhất mà bên nhận thông báo cho bên gửi

- 6 segments đầu tiên đều có đô dài là 54

No.	Time	Source	Destination	Protocol	Length Info
	109 3.379914	192.168.222.186	128.119.245.12	TCP	54 51425 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026
4	110 3.379966	192.168.222.186	128.119.245.12	TCP	54 51424 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1026
	111 3.380009	192.168.222.186	172.217.24.227	TCP	54 51428 → 443 [FIN, ACK] Seq=1 Ack=1 Win=102
	112 3.380054	192.168.222.186	128.119.245.12	TCP	54 51427 → 443 [FIN, ACK] Seq=1 Ack=1 Win=102
	113 3.380098	192.168.222.186	128.119.245.12	TCP	54 51426 → 443 [FIN, ACK] Seq=1 Ack=1 Win=102
	114 3.380112	192.168.222.186	128.119.245.12	TCP	54 51426 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 L
<					-

- Lượng buffer trống nhỏ nhất bên nhận thông báo cho bên gửi là 229

No.	Time	Source	Destination	Protocol	Length Info
	131 3.657141	128.119.245.12	192.168.222.186	TCP	66 80 → 51445 [SYN, ACK] Seq=0 Ack=1 Win=2920
L	132 3.657175	128.119.245.12	192.168.222.186	TCP	60 80 → 51425 [ACK] Seq=1 Ack=2 Win=229 Len=0
	134 3.668773	128.119.245.12	192.168.222.186	TCP	60 80 → 51424 [ACK] Seq=1 Ack=2 Win=229 Len=0
	135 3.708750	128.119.245.12	192.168.222.186	TCP	60 443 → 51426 [RST] Seq=1 Win=0 Len=0
	136 3.710366	128.119.245.12	192.168.222.186	TCP	66 443 → 51447 [SYN, ACK] Seq=0 Ack=1 Win=292
	137 3.710400	128.119.245.12	192.168.222.186	TCP	60 443 → 51427 [RST] Seq=1 Win=0 Len=0

Câu 14: Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó?

- Có, khi kiểm tra trong Time-Sequence-Graph(Steven), biểu đồ cho thấy có nhiều gói tin cùng một Sequence Number nhưng được gửi nhiều lần.

Lab 1: Làm quen với Wireshark

