Lab 1

BÁO CÁO BÀI THỰC HÀNH SỐ 1

[Tiêu đề bài TH]

Môn học: [Tên môn học]

Sinh viên thực hiện	Trần Thanh Hùng (23520580)
Thời gian thực hiện	13/03/2024 – 19/03/2024
Số câu đã hoàn thành	5/5

TRẢ LỜI CÁC CÂU HỎI

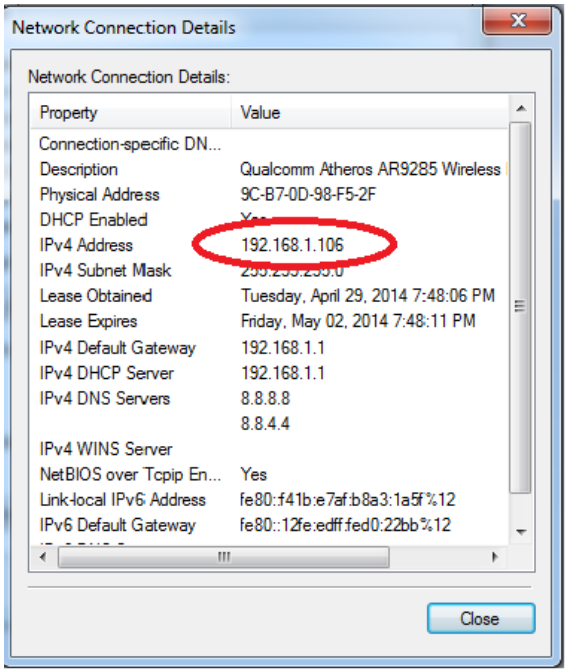
Gợi ý: *Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn*.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

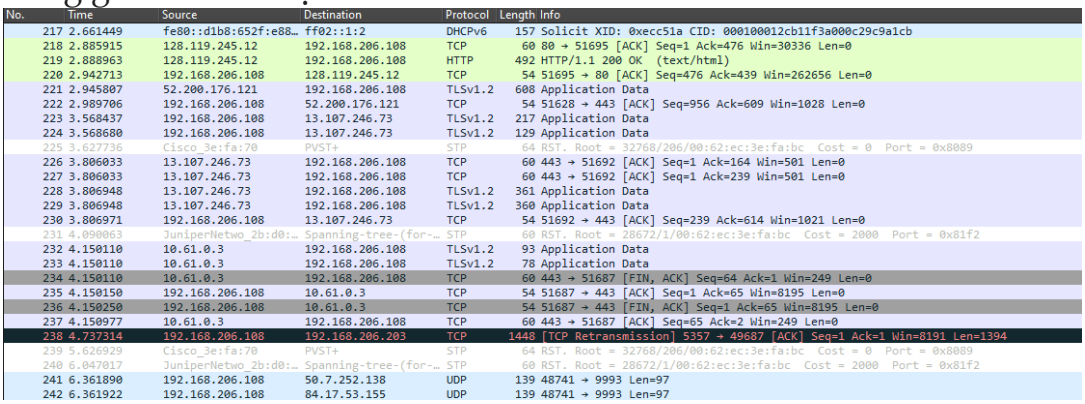
Trả lời: *192.168.1.106*

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



1. Tổng thời gian bắt gói tin đối với website đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

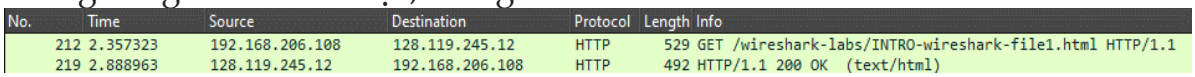
- Tổng thời gian bắt gói tin đối với website đã thử nghiệm là 6.361922(s)
- Tổng gói tin bắt được là 242



No.	Time	Source	Destination	Protocol	Length	Info
217	2.661449	fe80::d1b8:652f:e88…	ff02::1:2	DHCPv6	157	Solicit XID: 0xecc51a CID: 000100012cb11f3a000c29c9a1cb
218	2.885915	128.119.245.12	192.168.206.108	TCP	60	80 → 51695 [ACK] Seq=1 Ack=476 Win=30336 Len=0
219	2.888963	128.119.245.12	192.168.206.108	HTTP	492	HTTP/1.1 200 OK (text/html)
220	2.942713	192.168.206.108	128.119.245.12	TCP	54	51695 → 80 [ACK] Seq=476 Ack=439 Win=262656 Len=0
221	2.945807	52.200.176.121	192.168.206.108	TLSv1.2	608	Application Data
222	2.989706	192.168.206.108	52.200.176.121	TCP	54	51628 → 443 [ACK] Seq=956 Ack=609 Win=1028 Len=0
223	3.568437	192.168.206.108	13.107.246.73	TLSv1.2	217	Application Data
224	3.568680	192.168.206.108	13.107.246.73	TLSv1.2	129	Application Data
225	3.627736	Cisco_3e:fa:70	PVST+	STP	64	RST. Root = 32768/206/00:62:ec:3e:fa:bc Cost = 0 Port = 0x8089
226	3.806033	13.107.246.73	192.168.206.108	TCP	60	443 → 51692 [ACK] Seq=1 Ack=164 Win=501 Len=0
227	3.806033	13.107.246.73	192.168.206.108	TCP	60	443 → 51692 [ACK] Seq=1 Ack=239 Win=501 Len=0
228	3.806948	13.107.246.73	192.168.206.108	TLSv1.2	361	Application Data
229	3.806948	13.107.246.73	192.168.206.108	TLSv1.2	360	Application Data
230	3.806971	192.168.206.108	13.107.246.73	TCP	54	51692 → 443 [ACK] Seq=239 Ack=614 Win=1021 Len=0
231	4.090063	JuniperNetwo_2b:d0:…	Spanning-tree-(for-…	STP	60	RST. Root = 28672/1/00:62:ec:3e:fa:bc Cost = 2000 Port = 0x81f2
232	4.150110	10.61.0.3	192.168.206.108	TLSv1.2	93	Application Data
233	4.150110	10.61.0.3	192.168.206.108	TLSv1.2	78	Application Data
234	4.150110	10.61.0.3	192.168.206.108	TCP	60	443 → 51687 [FIN, ACK] Seq=64 Ack=1 Win=249 Len=0
235	4.150150	192.168.206.108	10.61.0.3	TCP	54	51687 → 443 [ACK] Seq=1 Ack=65 Win=8195 Len=0
236	4.150250	192.168.206.108	10.61.0.3	TCP	54	51687 → 443 [FIN, ACK] Seq=1 Ack=65 Win=8195 Len=0
237	4.150977	10.61.0.3	192.168.206.108	TCP	60	443 → 51687 [ACK] Seq=65 Ack=2 Win=249 Len=0
238	4.737314	192.168.206.108	192.168.206.203	TCP	1448	[TCP Retransmission] 5357 → 49687 [ACK] Seq=1 Ack=1 Win=8191 Len=1394
239	5.626925	Cisco_3e:fa:70	PVST+	STP	64	RST. Root = 32768/206/00:62:ec:3e:fa:bc Cost = 0 Port = 0x8089
240	6.047017	JuniperNetwo_2b:d0:…	Spanning-tree-(for-…	STP	60	RST. Root = 28672/1/00:62:ec:3e:fa:bc Cost = 2000 Port = 0x81f2
241	6.361890	192.168.206.108	50.7.252.138	UDP	139	48741 → 9993 Len=97
242	6.361922	192.168.206.108	84.17.53.155	UDP	139	48741 → 9993 Len=97

2. Trong các gói tin bắt được, có tổng cộng bao nhiêu gói tin HTTP?

Trong các gói tim bắt được, có 2 gói tin HTTP.

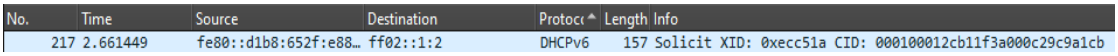


No.	Time	Source	Destination	Protocol	Length	Info
212	2.357323	192.168.206.108	128.119.245.12	HTTP	529	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
219	2.888963	128.119.245.12	192.168.206.108	HTTP	492	HTTP/1.1 200 OK (text/html)

3. Liệt kê ít nhất **5 giao thức khác nhau** xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc "http" khi truy cập website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

- 5 giao thức khác nhau xuất hiện trong cột giao thức:

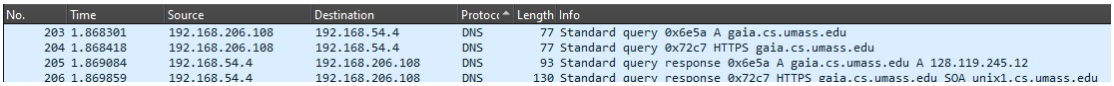
  + DHCPv6



No.	Time	Source	Destination	Protocol	Length	Info
217	2.661449	fe80::d1b8:652f:e88…	ff02::1:2	DHCPv6	157	Solicit XID: 0xecc51a CID: 000100012cb11f3a000c29c9a1cb

  Dynamic Host Configuration Protocol version 6 (DHCPv6) là một Giao thức truyền thông để cấu hình các host IPv6 với địa chỉ IPv6, tiền tố IP và các dữ liệu cấu hình khác cần thiết để hoạt động trong mạng IPv6.

  + DNS



No.	Time	Source	Destination	Protocol	Length	Info
203	1.868301	192.168.206.108	192.168.54.4	DNS	77	Standard query 0x6e5a A gaia.cs.umass.edu
204	1.868418	192.168.206.108	192.168.54.4	DNS	77	Standard query 0x72c7 HTTPS gaia.cs.umass.edu
205	1.869084	192.168.54.4	192.168.206.108	DNS	93	Standard query response 0x6e5a A gaia.cs.umass.edu A 128.119.245.12
206	1.869859	192.168.54.4	192.168.206.108	DNS	130	Standard query response 0x72c7 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu

  DNS (Domain Name System) là hệ thống phân giải tên miền. DNS cơ bản là một hệ thống chuyển đổi các tên miền website mà chúng ta đang sử dụng, ở dạng www.tenmien.com sang một địa chỉ IP dạng số tương ứng với tên miền đó và ngược lại.

+ SSDP

No.	Time	Source	Destination	Protocol	Length	Info
64	0.645373	192.168.123.1	239.255.255.250	SSDP	309	NOTIFY * HTTP/1.1
65	0.646012	192.168.123.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
66	0.646681	192.168.123.1	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
67	0.647315	192.168.123.1	239.255.255.250	SSDP	373	NOTIFY * HTTP/1.1
68	0.647842	192.168.123.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
69	0.648560	192.168.123.1	239.255.255.250	SSDP	357	NOTIFY * HTTP/1.1
70	0.649225	192.168.123.1	239.255.255.250	SSDP	389	NOTIFY * HTTP/1.1
71	0.649702	192.168.123.1	239.255.255.250	SSDP	318	NOTIFY * HTTP/1.1
72	0.650388	192.168.123.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
73	0.651582	192.168.123.1	239.255.255.250	SSDP	383	NOTIFY * HTTP/1.1
74	0.652168	192.168.123.1	239.255.255.250	SSDP	371	NOTIFY * HTTP/1.1
75	0.652684	192.168.123.1	239.255.255.250	SSDP	377	NOTIFY * HTTP/1.1
76	0.653388	192.168.123.1	239.255.255.250	SSDP	305	NOTIFY * HTTP/1.1
77	0.654078	192.168.123.1	239.255.255.250	SSDP	314	NOTIFY * HTTP/1.1
80	0.655398	192.168.123.1	239.255.255.250	SSDP	369	NOTIFY * HTTP/1.1
81	0.655398	192.168.123.1	239.255.255.250	SSDP	379	NOTIFY * HTTP/1.1

SSDP(Simple Service Discovery Protocol) là một phần của phương thức UPnP(Universal Plug and Play) SSDP là tiêu chuẩn cho các dịch vụ quảng cáo trên mạng TCP/IP và phát hiện ra chúng. Giao thức Universal Plug and Play (UPnP) sử dụng SSDP để thông báo và tìm thiết bị theo thứ tự, chẳng hạn như để truyền video từ nguồn đến hệ thống phát lại.

+ STP

No.	Time	Source	Destination	Protocol	Length	Info
188	1.627902	Cisco_3e:fa:70	PVST+	STP	64	RST. Root = 32768/206/00:62:ec:3e:fa:bc Cost = 0 Port = 0x8089
209	2.191579	JuniperNetwo_2b:d0:…	Spanning-tree-(for-…	STP	60	RST. Root = 28672/1/00:62:ec:3e:fa:bc Cost = 2000 Port = 0x81f2
225	3.627736	Cisco_3e:fa:70	PVST+	STP	64	RST. Root = 32768/206/00:62:ec:3e:fa:bc Cost = 0 Port = 0x8089
231	4.090063	JuniperNetwo_2b:d0:…	Spanning-tree-(for-…	STP	60	RST. Root = 28672/1/00:62:ec:3e:fa:bc Cost = 2000 Port = 0x81f2
239	5.626929	Cisco_3e:fa:70	PVST+	STP	64	RST. Root = 32768/206/00:62:ec:3e:fa:bc Cost = 0 Port = 0x8089
240	6.047017	JuniperNetwo_2b:d0:…	Spanning-tree-(for-…	STP	60	RST. Root = 28672/1/00:62:ec:3e:fa:bc Cost = 2000 Port = 0x81f2

Spanning Tree Protocol (STP) là một giao thức ngăn chặn sự lặp vòng, cho phép các bridge truyền thông với nhau để phát hiện vòng lặp vật lý trong mạng. Sau đó giao thức này sẽ định rõ một thuật toán mà bridge có thể tạo ra một cấu trúc mạng logic chứa vòng lặp (loop-free). Nói cách khác STP sẽ tạo một cấu trúc cây của free-loop gồm các lá và các nhánh nối toàn bộ mạng lớp 2

+TCP

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000033	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=2785 Win=1025 Len=0
6	0.015855	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=5569 Win=1025 Len=0
9	0.042955	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=8353 Win=1025 Len=0
10	0.068932	192.168.206.108	192.168.206.203	TCP	524	5357 → 49687 [ACK] Seq=1 Ack=1 Win=8191 Len=470 [TCP segment of a reassembled PDU]
13	0.075009	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=11137 Win=1025 Len=0
16	0.104250	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=13921 Win=1025 Len=0
19	0.138842	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=16705 Win=1025 Len=0
22	0.161504	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=19489 Win=1025 Len=0
25	0.190874	192.168.206.108	163.70.158.35	TCP	54	51417 → 443 [ACK] Seq=1 Ack=22273 Win=1025 Len=0

Transmission Control Protocol (TCP) là giao thức tiêu chuẩn trên Internet đảm bảo trao đổi thành công các gói dữ liệu giữa các thiết bị qua mạng. TCP là giao thức truyền tải cơ bản cho nhiều loại ứng dụng, bao gồm máy chủ web và trang web, ứng dụng email, FTP và các ứng dụng ngang hàng.

4. Xác định gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm. Cho biết gói tin này cơ bản dùng để làm gì?

- Gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm là gói tin thứ 212:

No.	Time	Source	Destination	Protocol	Length	Info
212	2.357323	192.168.206.108	128.119.245.12	HTTP	529	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

- Gói tin này dùng để dữ liệu đến máy chủ, phương thức truyền dữ liệu giữa client và sever để truy suất thông tin từ máy chủ

5. Xác định gói tin phản hồi của gói tin HTTP GET ở câu 4, thông tin nào xác định điều đó?

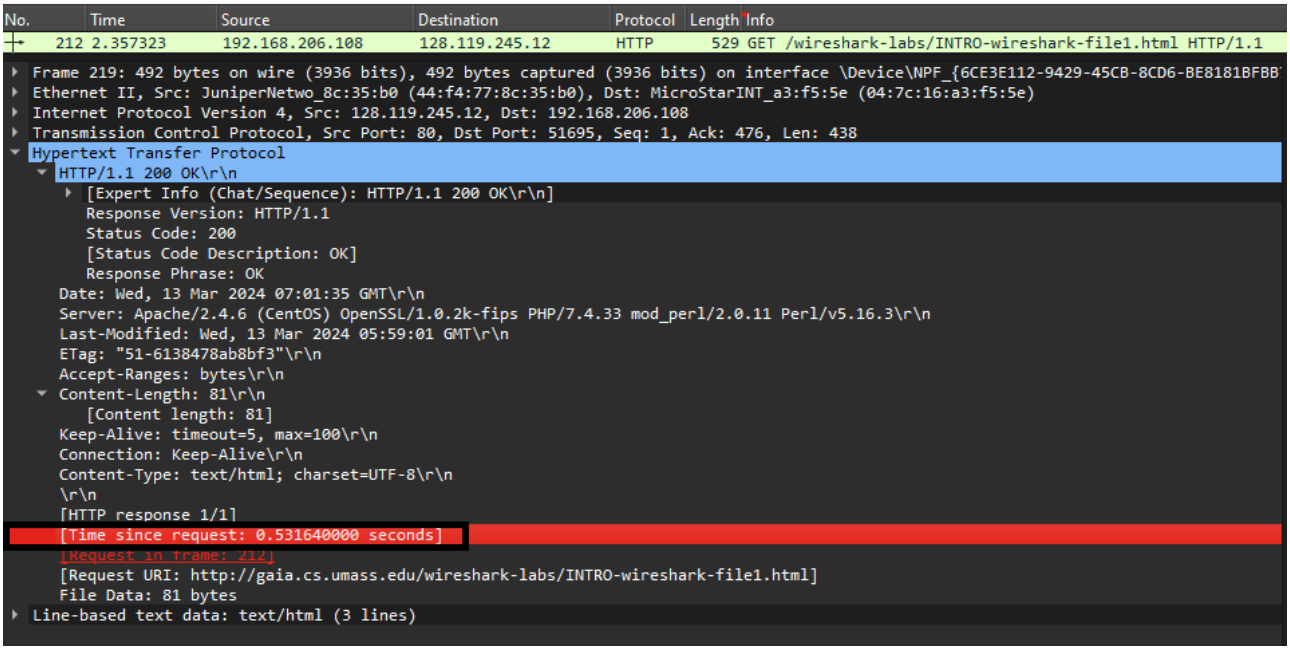
- Gói tin phản hồi HTTP GET ở câu 4 là gói tin 219:

No.	Time	Source	Destination	Protocol	Length	Info
219	2.888963	128.119.245.12	192.168.206.108	HTTP	492	HTTP/1.1 200 OK (text/html)

- Thông tin HTTP/1.1 200 OK xác định được gửi đến sever ở gói tin 212 (câu 4) được trả về từ sever về client với thông tin phản hồi status code 200 OK là dấu hiệu cho thấy yêu cầu đã thành công.

6. Tính thời gian từ khi gói tin **HTTP GET** đầu tiên được gửi cho đến khi có gói tin phản hồi **HTTP 200 OK** đối với website đã thử nghiệm. *(mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).*

- Thời gian từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi có gói tin phản hồi HTTP 200 OK là 0.53164(s)

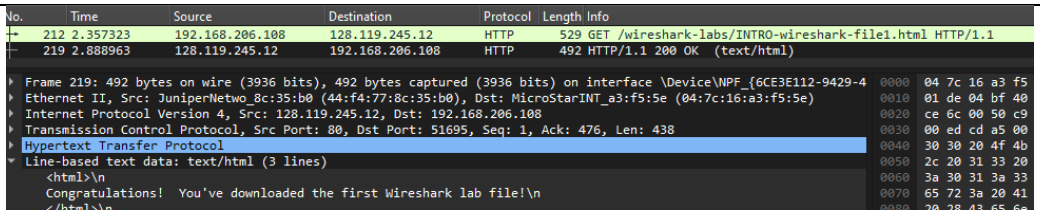


7. Nội dung hiển thị trên trang web gaia.cs.umass.edu

"Congratulations! You've downloaded the first Wireshark lab file!" có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.

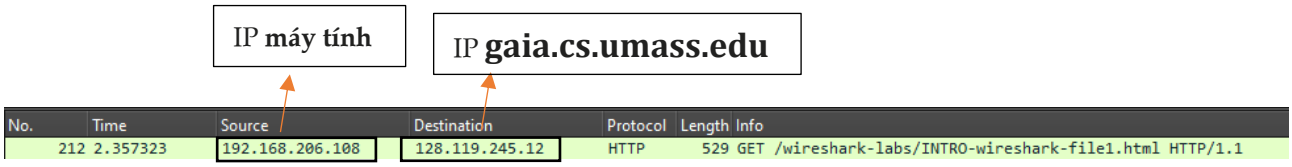
Nội dung hiển thị trên trang web **"Congratulations! You've downloaded the first Wireshark lab file!"** có nằm trong gói tin HTTP bắt được, và nằm ở gói tin thứ 219

```
Line-based text data: text/html (3 lines)
  <html>\n
  Congratulations!  You've downloaded the first Wireshark lab file!\n
  </html>\n
```



8. Hãy tìm hiểu về định dạng của địa chỉ IP và thử phỏng đoán địa chỉ IP của **gaia.cs.umass.edu** là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

- Địa chỉ IP của **gaia.cs.umass.edu** là 128.119.245.12
- Địa chỉ IP của máy tính đang sử dụng là: 192.168.206.108



9. Từ các nội dung trên, hãy mô tả cơ bản khi truy cập một website (ví dụ website đã thử nghiệm ở trên) thì quá trình gửi và nhận gói tin đã hoạt động như thế nào? Trình duyệt mà bạn đang sử dụng đóng vai trò gì?

- Khi nhập tên miền vào trình duyệt (**gaia.cs.umass.edu),** trình duyệt sẽ sử dụng giao thức DNS để gọi tới máy chủ DNS, sau đó máy chủ DNS sẽ gửi về địa chỉ IP của sever để máy client có thể truy cập vào máy chủ

```
203 1.868301    192.168.206.108   192.168.54.4      DNS      77 Standard query 0x6e5a A gaia.cs.umass.edu
204 1.868418    192.168.206.108   192.168.54.4      DNS      77 Standard query 0x72c7 HTTPS gaia.cs.umass.edu
205 1.869084    192.168.54.4      192.168.206.108   DNS      93 Standard query response 0x6e5a A gaia.cs.umass.edu A 128.119.245.12
206 1.869859    192.168.54.4      192.168.206.108   DNS     130 Standard query response 0x72c7 HTTPS gaia.cs.umass.edu SOA unix1.cs.umass.edu
```

- Trình duyệt sẽ sử dụng địa chi IP của sever (128.119.245.12) để yêu cầu HTTP gọi tới Server lưu trữ trang web đó. Nó sẽ kết nối cổng số 80 trên Server bằng giao thức TCP/IP.
- Nếu được sever chấp nhận sẽ gửi về gói tin thông báo 200 OK đồng thời mã HTML và các dữ liệu khác của trang web.
- Trình duyệt sau khi nhận được mã sẽ xuất lên giao diện để người dùng có thể sử dụng.
- Trình duyệt (google chrome, microsoft edge…) đóng vai trò như là một giao diện người dùng với Internet. Tạo ra các yêu cầu và nhận phản hồi từ máy chủ và hiển thị nội dung cho người dùng.

10. Khi sử dụng bộ lọc "http" như ở đối với website ở Task 1 thì kết quả thu được như thế nào, có các gói tin HTTP tương tự không?

- Khi sử dụng bộ lọc "http" như website Task1 thì không có kết quả xuất hiện và không có các gói tin HTTP tương tự.

11. Tìm cách xác định địa chỉ IP của website đã chọn là bao nhiêu? Địa chỉ IP của máy tính bạn lúc này là bao nhiêu?

- Địa chỉ IP website đã chọn là 172.67.136.53:

  + Sử dụng lệnh ping trên CMD

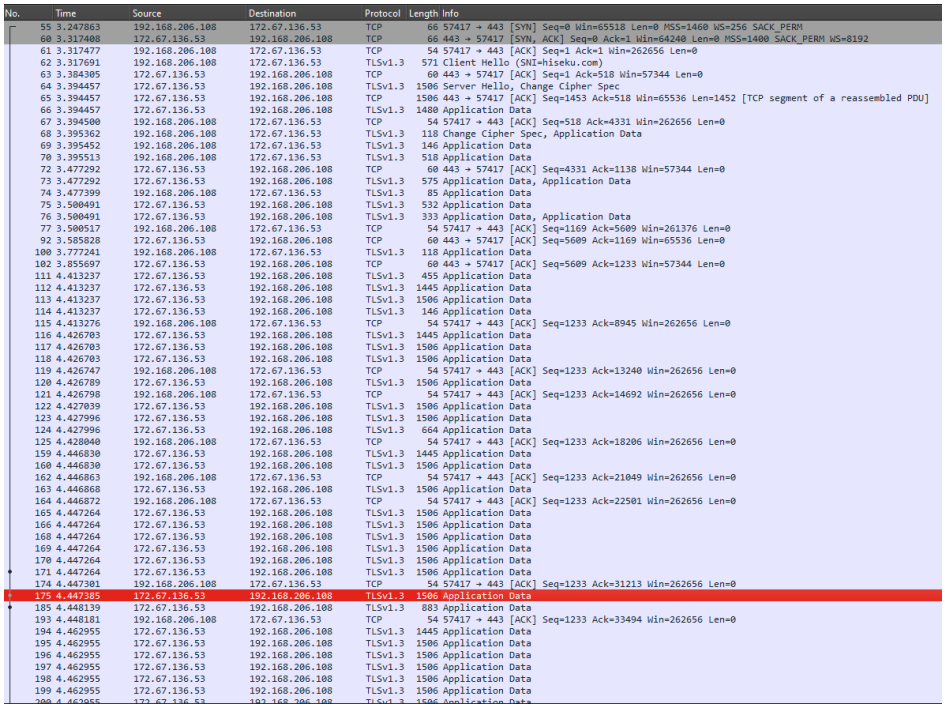
```
C:\Users\Hunn>ping hiseku.com

Pinging hiseku.com [172.67.136.53] with 32 bytes of data:
Reply from 172.67.136.53: bytes=32 time=42ms TTL=55
Reply from 172.67.136.53: bytes=32 time=112ms TTL=55
Reply from 172.67.136.53: bytes=32 time=126ms TTL=55
Reply from 172.67.136.53: bytes=32 time=97ms TTL=55
```

- Địa chỉ IP của máy tính lúc này là: 192.168.206.108
  - Sử dụng lệnh ipconfig trong CMD

```
C:\Users\Hunn>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.206.108
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.206.1
```

12. Sử dụng thành phần packet-display filter để hiển thị đầy đủ quá trình trao đổi gói tin giữa máy tính của bạn và website bằng cú pháp: ip.addr==<địa chỉ IP của máy tính> && ip.addr==<địa chỉ IP của website> . Cho biết rằng bạn có thể thấy được nội dung trả về của website không? Mô tả.

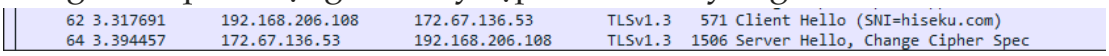
- Không thể tìm thấy nội dung trả về của website vì toàn bộ nội dung của website đã bị mã hóa theo phương thức ssl/tls để đảm bảo an toàn bảo mật của website



No.	Time	Source	Destination	Protocol	Length	Info
55	3.247863	192.168.206.108	172.67.136.53	TCP	66	57417 → 443 [SYN] Seq=0 Win=65518 Len=0 MSS=1460 WS=256 SACK_PERM
60	3.317408	172.67.136.53	192.168.206.108	TCP	66	443 → 57417 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192
61	3.317477	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1 Ack=1 Win=262656 Len=0
62	3.317691	192.168.206.108	172.67.136.53	TLSv1.3	571	Client Hello (SNI=hiseku.com)
63	3.384305	172.67.136.53	192.168.206.108	TCP	60	443 → 57417 [ACK] Seq=1 Ack=518 Win=57344 Len=0
64	3.394457	172.67.136.53	192.168.206.108	TLSv1.3	1506	Server Hello, Change Cipher Spec
65	3.394457	172.67.136.53	192.168.206.108	TCP	1506	443 → 57417 [ACK] Seq=1453 Ack=518 Win=65536 Len=1452 [TCP segment of a reassembled PDU]
66	3.394457	172.67.136.53	192.168.206.108	TLSv1.3	1480	Application Data
67	3.394500	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=518 Ack=4331 Win=262656 Len=0
68	3.395362	192.168.206.108	172.67.136.53	TLSv1.3	118	Change Cipher Spec, Application Data
69	3.395452	192.168.206.108	172.67.136.53	TLSv1.3	146	Application Data
70	3.395513	192.168.206.108	172.67.136.53	TLSv1.3	518	Application Data
72	3.477292	172.67.136.53	192.168.206.108	TCP	60	443 → 57417 [ACK] Seq=4331 Ack=1138 Win=57344 Len=0
73	3.477292	172.67.136.53	192.168.206.108	TLSv1.3	575	Application Data, Application Data
74	3.477399	192.168.206.108	172.67.136.53	TLSv1.3	85	Application Data
75	3.500491	172.67.136.53	192.168.206.108	TLSv1.3	532	Application Data
76	3.500491	172.67.136.53	192.168.206.108	TLSv1.3	333	Application Data, Application Data
77	3.500517	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1169 Ack=5609 Win=261376 Len=0
92	3.585828	172.67.136.53	192.168.206.108	TCP	60	443 → 57417 [ACK] Seq=5609 Ack=1169 Win=65536 Len=0
100	3.777241	192.168.206.108	172.67.136.53	TLSv1.3	118	Application Data
102	3.855697	172.67.136.53	192.168.206.108	TCP	60	443 → 57417 [ACK] Seq=5609 Ack=1233 Win=57344 Len=0
111	4.413237	172.67.136.53	192.168.206.108	TLSv1.3	455	Application Data
112	4.413237	172.67.136.53	192.168.206.108	TLSv1.3	1445	Application Data
113	4.413237	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
114	4.413237	172.67.136.53	192.168.206.108	TLSv1.3	146	Application Data
115	4.413276	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=8945 Win=262656 Len=0
116	4.426703	172.67.136.53	192.168.206.108	TLSv1.3	1445	Application Data
117	4.426703	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
118	4.426703	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
119	4.426747	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=13240 Win=262656 Len=0
120	4.426789	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
121	4.426798	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=14692 Win=262656 Len=0
122	4.427039	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
123	4.427996	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
124	4.427996	172.67.136.53	192.168.206.108	TLSv1.3	664	Application Data
125	4.428040	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=18206 Win=262656 Len=0
159	4.446830	172.67.136.53	192.168.206.108	TLSv1.3	1445	Application Data
160	4.446830	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
162	4.446863	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=21049 Win=262656 Len=0
163	4.446868	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
164	4.446872	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=22501 Win=262656 Len=0
165	4.447264	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
166	4.447264	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
168	4.447264	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
169	4.447264	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
170	4.447264	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
171	4.447264	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
174	4.447301	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=31213 Win=262656 Len=0
175	4.447385	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
185	4.448139	172.67.136.53	192.168.206.108	TLSv1.3	883	Application Data
193	4.448181	192.168.206.108	172.67.136.53	TCP	54	57417 → 443 [ACK] Seq=1233 Ack=33494 Win=262656 Len=0
194	4.462955	172.67.136.53	192.168.206.108	TLSv1.3	1445	Application Data
195	4.462955	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
196	4.462955	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
197	4.462955	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
198	4.462955	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data
199	4.462955	172.67.136.53	192.168.206.108	TLSv1.3	1506	Application Data

13. Hãy chỉ ra **ít nhất 2 gói tin** mà bạn cho rằng là quan trọng khi truy cập website này. Tìm hiểu và mô tả ngắn gọn các giao thức này. Giải thích.

- Hai gói tin quan trọng khi truy cập website này là gói tin 62 và 64:



62	3.317691	192.168.206.108	172.67.136.53	TLSv1.3	571 Client Hello (SNI=hiseku.com)
64	3.394457	172.67.136.53	192.168.206.108	TLSv1.3	1506 Server Hello, Change Cipher Spec

- Sử sụng giao thức TLSv1.3: Là phiên bản giao thức mới nhất của SSL/TLS sử dụng HTTPS và các giao thức khác được mã hóa. Phiên bản mới 1.3 cho khả năng tốc độ truy cập nhanh hơn so với các phiên bản trước đó của SSL/TLS.
- Gói tin 62 và 64 là quan trọng nhất vì:
  + Gói tin 62 là gói tin được gửi đi bởi client đến sever để thực hiện yêu cầu kết nối an toàn SSL/TLS (Client Hello).
  + Gói tin 64 là gói tin được gửi bởi sever đến máy client để xác thực danh tính và cho phép client truy cập trang web (Sever Hello).
  + Hai gói tin này được xem như là giai đoạn "handshake"(bắt tay)
  + Hai gói tin này đóng vai trò quan trọng trong việc thiết lập kết nối an toàn giữa client và server. Gói tin ClientHello cho phép server biết client hỗ trợ những gì, và gói tin ServerHello cho phép client xác minh danh tính của server và thiết lập khóa mã hóa để bảo mật dữ liệu truyền tải.