

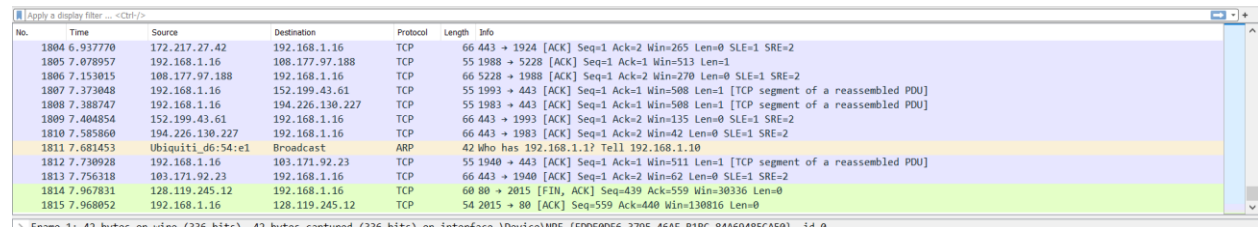
## Bài 1:

1/

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

-Tổng thời gian: 7.968052s.

-Tổng packet: 1815.



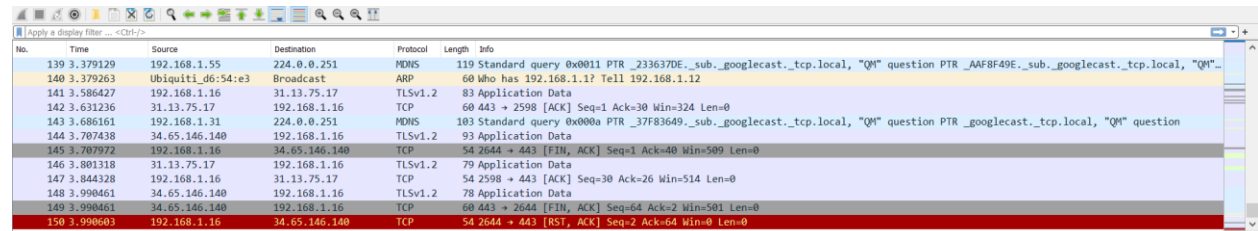
Wireshark packet capture showing ARP and TCP traffic. The display filter is 'Apply a display filter... <Ctrl>'. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
1804	6.937770	172.217.27.42	192.168.1.16	TCP	66	443 → 1924 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
1805	7.078957	192.168.1.16	108.177.97.188	TCP	55	1988 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
1806	7.153015	108.177.97.188	192.168.1.16	TCP	66	5228 → 1988 [ACK] Seq=1 Ack=2 Win=270 Len=0 SLE=1 SRE=2
1807	7.373048	192.168.1.16	152.199.43.61	TCP	55	1993 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
1808	7.388747	192.168.1.16	194.226.130.227	TCP	55	1983 → 443 [ACK] Seq=1 Ack=1 Win=508 Len=1 [TCP segment of a reassembled PDU]
1809	7.484854	152.199.43.61	192.168.1.16	TCP	66	443 → 1993 [ACK] Seq=1 Ack=2 Win=135 Len=0 SLE=1 SRE=2
1810	7.585800	194.226.130.227	192.168.1.16	TCP	66	443 → 1993 [ACK] Seq=1 Ack=2 Win=42 Len=0 SLE=1 SRE=2
1811	7.681453	Ubiquiti_d6:54:e1	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
1812	7.739928	192.168.1.16	103.171.92.23	TCP	55	1940 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
1813	7.756318	103.171.92.23	192.168.1.16	TCP	66	443 → 1940 [ACK] Seq=1 Ack=2 Win=62 Len=0 SLE=1 SRE=2
1814	7.967831	128.119.245.12	192.168.1.16	TCP	60	80 → 2015 [FIN, ACK] Seq=439 Ack=559 Win=30336 Len=0
1815	7.968052	192.168.1.16	128.119.245.12	TCP	54	2015 → 80 [ACK] Seq=559 Ack=440 Win=130816 Len=0

+ <http://www.iuh.edu.vn/>

-Tổng thời gian: 3.990603s.

-Tổng packet: 150.



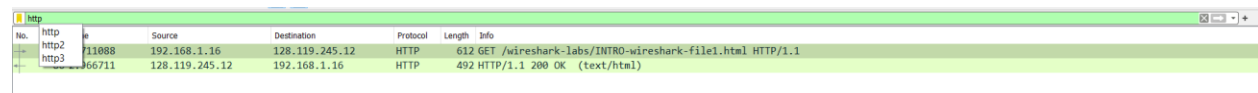
Wireshark packet capture showing DNS and TLS traffic. The display filter is 'Apply a display filter... <Ctrl>'. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
139	3.379129	192.168.1.55	224.0.0.251	MDNS	119	Standard query 0x0011 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _AABF49E._sub._googlecast._tcp.local, "QM"...
140	3.379263	Ubiquiti_d6:54:e3	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.12
141	3.586427	192.168.1.16	31.13.75.17	TLSv1.2	83	Application Data
142	3.631236	31.13.75.17	192.168.1.16	TCP	60	443 → 2598 [ACK] Seq=1 Ack=30 Win=324 Len=0
143	3.686161	192.168.1.31	224.0.0.251	MDNS	103	Standard query 0x000a PTR _37F83649._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" question
144	3.707438	34.65.146.140	192.168.1.16	TLSv1.2	93	Application Data
145	3.707972	192.168.1.16	34.65.146.140	TCP	54	2644 → 443 [FIN, ACK] Seq=1 Ack=40 Win=509 Len=0
146	3.801318	31.13.75.17	192.168.1.16	TLSv1.2	79	Application Data
147	3.844328	192.168.1.16	31.13.75.17	TCP	54	2598 → 443 [ACK] Seq=30 Ack=26 Win=514 Len=0
148	3.990461	34.65.146.140	192.168.1.16	TLSv1.2	78	Application Data
149	3.990461	34.65.146.140	192.168.1.16	TCP	60	443 → 2644 [FIN, ACK] Seq=64 Ack=2 Win=501 Len=0
150	3.990603	192.168.1.16	34.65.146.140	TCP	54	2644 → 443 [RST, ACK] Seq=2 Ack=64 Win=0 Len=0

2/

-HTTP: **Http (HyperText Transfer Protocol)** là giao thức truyền tải siêu văn bản được sử dụng trong www dùng để truyền tải dữ liệu giữa Web server đến các trình duyệt Web và ngược lại. Giao thức này sử dụng cổng 80 (port 80) là chủ yếu.

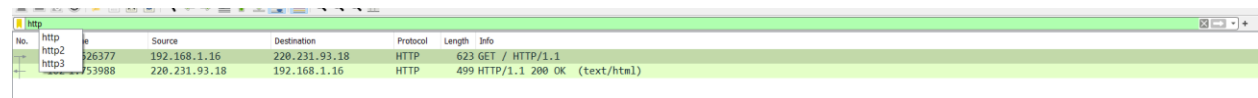
+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>



Wireshark packet capture showing HTTP traffic. The display filter is 'http'. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
http2	11088	192.168.1.16	128.119.245.12	HTTP	612	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
http3	166711	128.119.245.12	192.168.1.16	HTTP	492	HTTP/1.1 200 OK (text/html)

+ <http://www.iuh.edu.vn/>



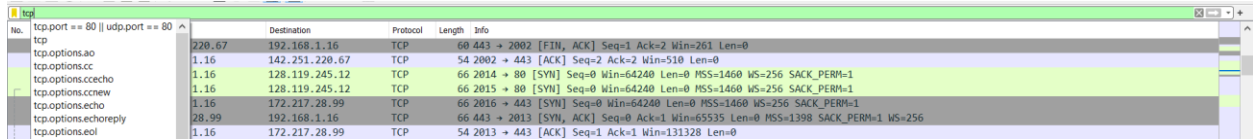
Wireshark packet capture showing HTTP traffic. The display filter is 'http'. The packet list shows:

No.	Time	Source	Destination	Protocol	Length	Info
http2	26377	192.168.1.16	220.231.93.18	HTTP	623	GET / HTTP/1.1
http3	53988	220.231.93.18	192.168.1.16	HTTP	499	HTTP/1.1 200 OK (text/html)

-TCP: **TCP (Transmission Control Protocol)** là một giao thức mạng quan trọng được sử dụng trong việc truyền dữ liệu qua một mạng nào đó. Một giao thức trong phạm vi mạng là một tập hợp các quy tắc và trình tự kiểm soát việc thực hiện truyền dữ liệu sao cho tất cả mọi người trên

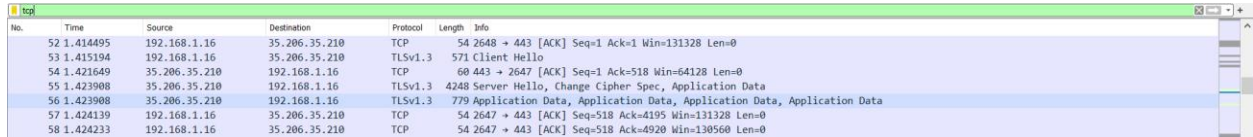
thể giới bất kể vị trí địa lý, bất kể ứng dụng, phần mềm họ đang sử dụng đều có thể thao tác theo cùng một phương thức giống nhau được gọi là TCP.

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>



No.	Time	Source	Destination	Protocol	Length	Info
220.67		192.168.1.16	192.168.1.16	TCP	60	443 → 2002 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
1.16		142.251.220.67	192.168.1.16	TCP	54	2002 → 443 [ACK] Seq=2 Ack=2 Win=510 Len=0
1.16		128.119.245.12	192.168.1.16	TCP	66	2014 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1.16		128.119.245.12	192.168.1.16	TCP	66	2015 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1.16		172.217.28.99	192.168.1.16	TCP	66	2016 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
28.99		192.168.1.16	192.168.1.16	TCP	66	443 → 2013 [SYN, ACK] Seq=0 Ack=1 Win=6535 Len=0 MSS=1398 SACK_PERM=1 WS=256
1.16		172.217.28.99	192.168.1.16	TCP	54	2013 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0

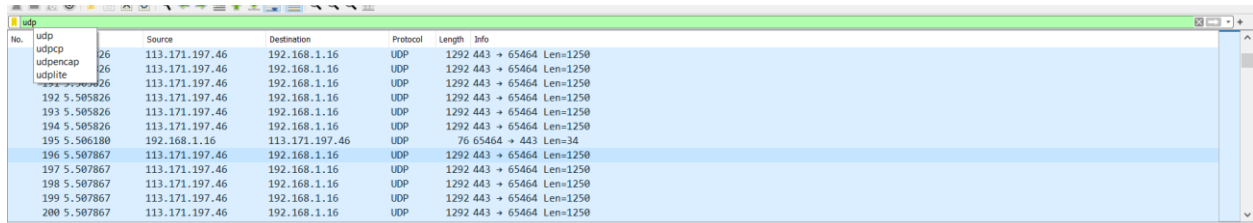
+ <http://www.iuh.edu.vn/>



No.	Time	Source	Destination	Protocol	Length	Info
52	1.414495	192.168.1.16	35.206.35.210	TCP	54	2648 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
53	1.415194	192.168.1.16	35.206.35.210	TLSv1.3	571	Client Hello
54	1.421649	35.206.35.210	192.168.1.16	TCP	60	443 → 2647 [ACK] Seq=1 Ack=518 Win=64128 Len=0
55	1.423908	35.206.35.210	192.168.1.16	TLSv1.3	4248	Server Hello, Change Cipher Spec, Application Data
56	1.423908	35.206.35.210	192.168.1.16	TLSv1.3	779	Application Data, Application Data, Application Data
57	1.424139	192.168.1.16	35.206.35.210	TCP	54	2647 → 443 [ACK] Seq=518 Ack=4195 Win=131328 Len=0
58	1.424233	192.168.1.16	35.206.35.210	TCP	54	2647 → 443 [ACK] Seq=518 Ack=4920 Win=130560 Len=0

-UDP: **UDP (User Datagram Protocol)** là một trong những giao thức cốt lõi của giao thức TCP/IP. Dùng UDP, chương trình trên mạng máy tính có thể gửi những dữ liệu ngắn được gọi là datagram tới máy khác. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP làm; các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái của nó nên nó hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu.

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

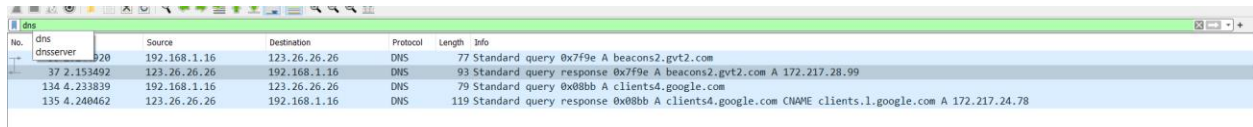


No.	Time	Source	Destination	Protocol	Length	Info
26		113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
26		113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
26		113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
192	5.505826	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
193	5.505826	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
194	5.505826	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
195	5.506180	192.168.1.16	113.171.197.46	UDP	76	65464 → 443 Len=34
196	5.507867	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
197	5.507867	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
198	5.507867	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
199	5.507867	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250
200	5.507867	113.171.197.46	192.168.1.16	UDP	1292	443 → 65464 Len=1250

+ <http://www.iuh.edu.vn/>

-DNS: DNS được phát minh vào năm 1984 và là cụm từ viết tắt của **Domain Name System** với tên tiếng Việt là hệ thống phân giải tên miền. DNS chỉ cho phép một hệ thống thiết lập tương ứng giữa địa chỉ IP và tên miền. Hệ thống này giúp cho máy tính và con người có thể giao tiếp với nhau một cách tiện lợi và dễ dàng hơn, giúp cho biên dịch tên miền trở thành các dãy số để máy tính có thể đọc hiểu được.

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>



No.	Time	Source	Destination	Protocol	Length	Info
37	2.153492	123.26.26.26	192.168.1.16	DNS	77	Standard query 0x7f9e A beacons2.gvt2.com
134	4.233839	192.168.1.16	123.26.26.26	DNS	93	Standard query response 0x7f9e A beacons2.gvt2.com A 172.217.28.99
135	4.240462	123.26.26.26	192.168.1.16	DNS	79	Standard query 0x80bb A clients4.google.com
				DNS	119	Standard query response 0x80bb A clients4.google.com CNAME clients1.google.com A 172.217.24.78

+ <http://www.iuh.edu.vn/>

No.	Time	Source	Destination	Protocol	Length	Info
13	0.688815	192.168.1.16	123.26.26.26	DNS	76	Standard query 0xe376 A beacons.gvt2.com
14	0.697715	123.26.26.26	192.168.1.16	DNS	115	Standard query response 0xe376 A beacons.gvt2.com CNAME beacons6.gvt2.com A 142.250.204.131
34	0.936576	192.168.1.16	123.26.26.26	DNS	78	Standard query 0x4625 A e2c48.gcp.gvt2.com
35	0.959908	123.26.26.26	192.168.1.16	DNS	94	Standard query response 0x4625 A e2c48.gcp.gvt2.com A 35.206.35.210
117	1.977922	192.168.1.16	123.26.26.26	DNS	81	Standard query 0x5092 A icatsd2016.iuh.edu.vn
118	1.978058	192.168.1.16	123.26.26.26	DNS	76	Standard query 0x0d9a A kosen.iuh.edu.vn
119	1.983102	123.26.26.26	192.168.1.16	DNS	137	Standard query response 0x0d9a No such name A kosen.iuh.edu.vn SOA ns2.pavietnam.vn
120	1.983102	123.26.26.26	192.168.1.16	DNS	142	Standard query response 0x5092 No such name A icatsd2016.iuh.edu.vn SOA ns2.pavietnam.vn

-QUIC: QUIC là viết tắt của **Quick Connections UDP Internet (Giao thức kết nối Internet nhanh UDP)**, đây là một giao thức truyền tải do Google phát triển nhằm thay thế cho giao thức TCP (Transmission Control Protocol). QUIC chạy một dòng giao thức ghép kênh trên UDP (a multiplexed stream transport over UDP) thay vì TCP. Google phát triển giao thức QUIC này với mục đích tăng tốc các giao thức mạng của mình nhằm giảm thiểu thời gian phản ứng của trang web, bằng cách giảm thiểu RTT (Round Trip Times) giữa người gửi và người nhận. Điều mà giao thức TCP đang gặp phải.

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

quic							
No.	Quic	Time	Source	Destination	Protocol	Length	Info
38	2.155215	192.168.1.16	172.217.28.99	QUIC	1292	Initial, DCID=dc12036ceb65974a, PKN: 1, PADDING, PING, PING, CRYPTO, PADDING, PING, PADDING, PING, PING, PADDING, CRYPTO, CRYPT...	
45	2.416286	192.168.1.16	172.217.28.99	QUIC	1292	Initial, DCID=dc12036ceb65974a, PKN: 3, CRYPTO, PADDING, CRYPTO, PING, PADDING, PING, PING, CRYPTO, PING, PADDING, CRYPTO, CRYPT...	
46	2.422019	172.217.28.99	192.168.1.16	QUIC	1292	Initial, SCID=dc12036ceb65974a, PKN: 1, ACK, CRYPTO, PADDING	
47	2.423788	192.168.1.16	172.217.28.99	QUIC	1292	Initial, DCID=dc12036ceb65974a, PKN: 4, ACK, PADDING	
50	2.470830	172.217.28.99	192.168.1.16	QUIC	1292	Handshake, SCID=dc12036ceb65974a	
51	2.471204	172.217.28.99	192.168.1.16	QUIC	1292	Handshake, SCID=dc12036ceb65974a	
52	2.471425	192.168.1.16	172.217.28.99	QUIC	83	Handshake, DCID=dc12036ceb65974a	
57	2.681177	172.217.28.99	192.168.1.16	QUIC	1292	Handshake, SCID=dc12036ceb65974a	
58	2.681278	172.217.28.99	192.168.1.16	QUIC	199	Protected Payload (KP0)	
59	2.681935	192.168.1.16	172.217.28.99	QUIC	83	Handshake, DCID=dc12036ceb65974a	
60	2.682234	192.168.1.16	172.217.28.99	QUIC	83	Handshake, DCID=dc12036ceb65974a	
61	2.689938	192.168.1.16	172.217.28.99	QUIC	125	Handshake, DCID=dc12036ceb65974a	

+ <http://www.iuh.edu.vn/>

No.	Time	Source	Destination	Protocol	Length	Info
15	0.699253	192.168.1.16	142.250.204.131	QUIC	1292	Initial, DCID=ba691d0176c486b3, PKN: 1, CRYPTO, PADDING, CRYPTO, PING, PADDING, PING, PING, PING, CRYPTO, PADDING, CRYPTO, PING, P

3/

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

$$2.96711 - 1.711088 = 0.256022s$$

No.	Time	Source	Destination	Protocol	Length	Info
67	2.711088	192.168.1.16	128.119.245.12	HTTP	612	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
86	2.966711	128.119.245.12	192.168.1.16	HTTP	492	HTTP/1.1 200 OK (text/html)

+ <http://www.iuh.edu.vn/>

$$1.753988 - 1.626377 = 0.127611s$$

No.	Time	Source	Destination	Protocol	Length	Info
64	1.626377	192.168.1.16	220.231.93.18	HTTP	623	GET / HTTP/1.1
102	1.753988	220.231.93.18	192.168.1.16	HTTP	499	HTTP/1.1 200 OK (text/html)

4/

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

No.	Time	Source	Destination	Protocol	Length	Info
67	2.711088	192.168.1.16	128.119.245.12	HTTP	612	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
86	2.966711	128.119.245.12	192.168.1.16	HTTP	492	HTTP/1.1 200 OK (text/html)

```

> Frame 86: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{F0DE00F6-3795-46AF-B18C-8AA69485CA50}, id 0
> Ethernet II, Src: DruyTek_52:ee:f8 (00:1d:aa:52:ee:f8), Dst: Chongqin_83:05:d7 (d4:1b:81:83:05:d7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.16
> Transmission Control Protocol, Src Port: 80, Dst Port: 2015, Seq: 1, Ack: 559, Len: 438
> Hypertext Transfer Protocol
  Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations! You've downloaded the first Wireshark lab file!\n
    </html>\n

```

+ <http://www.iuh.edu.vn/>

No.	Time	Source	Destination	Protocol	Length	Info
64	1.626377	192.168.1.16	220.231.93.18	HTTP	623	GET / HTTP/1.1
102	1.753988	220.231.93.18	192.168.1.16	HTTP	499	HTTP/1.1 200 OK (text/html)

```

  Line-based text data: text/html (1415 lines)
    \u0000<!DOCTYPE html>\n
    <html>\n
    <head>\n
    <meta charset="utf-8">\n
    <!--meta content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=0" name="viewport" />-->\n
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />\n
    <meta name="description">\n
    content="Trường Đại học Công nghiệp Thành phố Hồ Chí Minh" />\n
    <meta name="keywords" content="Trường Đại học Công nghiệp TP.HCM, Trường Đại học trọng điểm của Bộ Công Thương, www.iuh.edu.vn, iuh" />\n
    <meta name="viewport" content="width=device-width, initial-scale=1.0">\n
    <meta property="og:image" content="http://iuh.edu.vn/templates/2015/image/logo.png">\n
    \t\t<link href="/templates/images/icon.ico" rel="shortcut icon">\n

```

5/

+ <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

**128.119.245.12**

+ <http://www.iuh.edu.vn/>

**220.231.93.18**

6/

- Từ máy client gửi yêu cầu truy cập trang web đến máy chủ(phương thức GET). Máy chủ sẽ gửi lại file html của trang web đến máy khách và trình chiếu lên browser của máy khách.

(\*) Mở rộng:

- Địa chỉ IP giống như 1 mã định danh của các thiết bị đầu cuối giúp chúng có thể nhận biết, giao tiếp và trao đổi thông tin với nhau.

-Mở cmd, sử dụng lệnh ping [tên host] hoặc tracert [tên host]

```
ga C:\Users\GIAHUY>ping gaia.cs.umass.edu
1 -Pinging gaia.cs.umass.edu [128.119.245.12] with 32 bytes of data:
  Reply from 128.119.245.12: bytes=32 time=256ms TTL=39
  Reply from 128.119.245.12: bytes=32 time=256ms TTL=39
  Reply from 128.119.245.12: bytes=32 time=287ms TTL=39
  Reply from 128.119.245.12: bytes=32 time=301ms TTL=39
8 -
Ping statistics for 128.119.245.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 256ms, Maximum = 301ms, Average = 275ms
```