

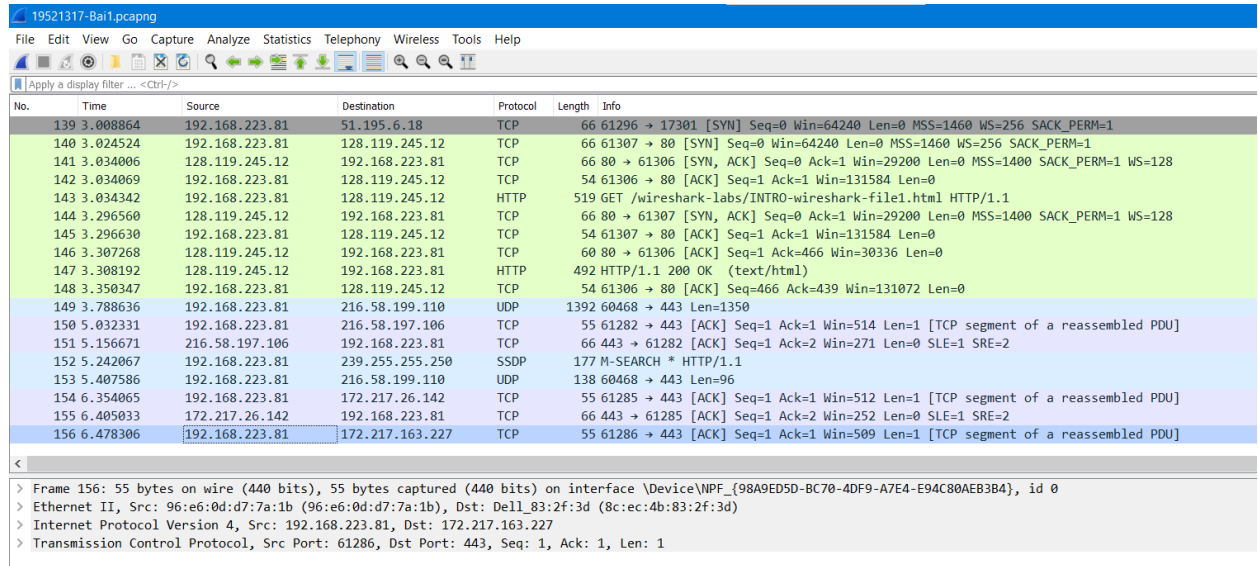
Lab1: Làm quen với Wireshark

Tên: Nguyễn Khải Đăng

MSSV: 19521317

Bài 1:

- Trang web: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> : Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm là **6.478306** và tổng số gói tin bắt được là **156**

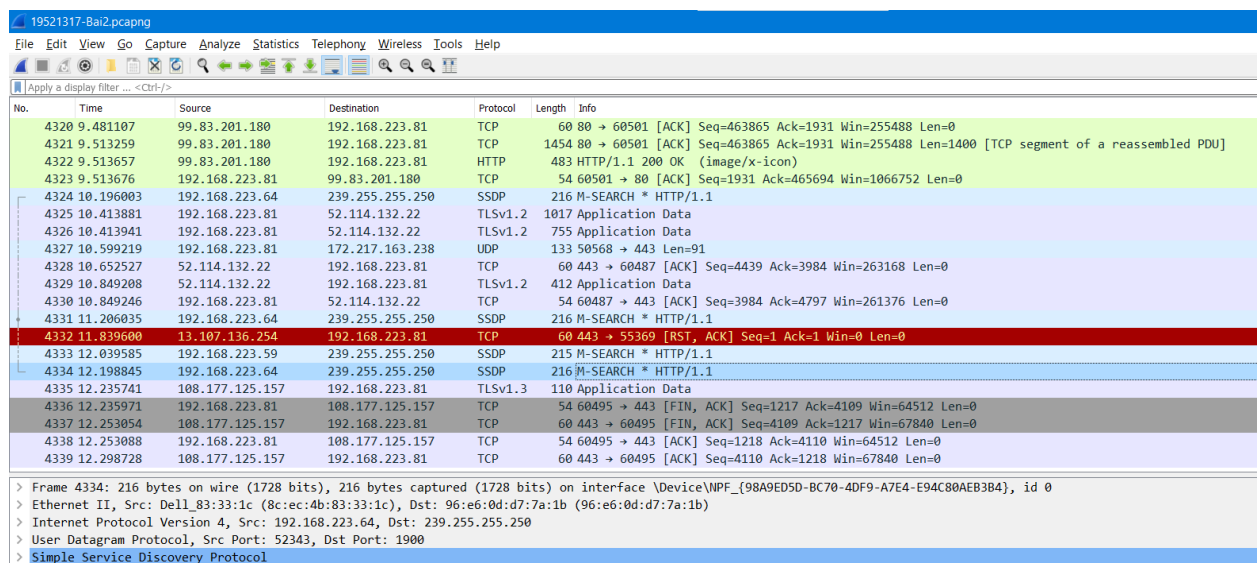


Wireshark capture showing traffic to <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>. The capture shows a series of TCP and HTTP packets. The total time for the capture is 6.478306 seconds, and the total number of packets captured is 156.

No.	Time	Source	Destination	Protocol	Length	Info
139	3.008864	192.168.223.81	51.195.6.18	TCP	66	61296 → 17301 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
140	3.024524	192.168.223.81	128.119.245.12	TCP	66	61307 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
141	3.034006	128.119.245.12	192.168.223.81	TCP	66	80 → 61306 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
142	3.034069	192.168.223.81	128.119.245.12	TCP	54	61306 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
143	3.034342	192.168.223.81	128.119.245.12	HTTP	519	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
144	3.296560	128.119.245.12	192.168.223.81	TCP	66	80 → 61307 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=128
145	3.296630	192.168.223.81	128.119.245.12	TCP	54	61307 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
146	3.307268	128.119.245.12	192.168.223.81	TCP	60	80 → 61306 [ACK] Seq=1 Ack=466 Win=30336 Len=0
147	3.308192	128.119.245.12	192.168.223.81	HTTP	492	HTTP/1.1 200 OK (text/html)
148	3.350347	192.168.223.81	128.119.245.12	TCP	54	61306 → 80 [ACK] Seq=466 Ack=439 Win=131072 Len=0
149	3.788636	192.168.223.81	216.58.199.110	UDP	1392	60468 → 443 Len=1350
150	5.032331	192.168.223.81	216.58.197.106	TCP	55	61282 → 443 [ACK] Seq=1 Ack=1 Win=514 Len=1 [TCP segment of a reassembled PDU]
151	5.156671	216.58.197.106	192.168.223.81	TCP	66	443 → 61282 [ACK] Seq=1 Ack=2 Win=271 Len=0 SLE=1 SRE=2
152	5.242067	192.168.223.81	239.255.255.250	SSDP	177	M-SEARCH * HTTP/1.1
153	5.407586	192.168.223.81	216.58.199.110	UDP	138	60468 → 443 Len=96
154	6.354865	192.168.223.81	172.217.26.142	TCP	55	61285 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
155	6.405033	172.217.26.142	192.168.223.81	TCP	66	443 → 61285 [ACK] Seq=1 Ack=2 Win=252 Len=0 SLE=1 SRE=2
156	6.478306	192.168.223.81	172.217.163.227	TCP	55	61286 → 443 [ACK] Seq=1 Ack=1 Win=509 Len=1 [TCP segment of a reassembled PDU]

> Frame 156: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{98A9ED5D-BC70-4DF9-A7E4-E94C80AEB3B4}, id 0
> Ethernet II, Src: 96:e6:0d:d7:7a:1b (96:e6:0d:d7:7a:1b), Dst: Dell_83:2f:3d (8c:ec:4b:83:2f:3d)
> Internet Protocol Version 4, Src: 192.168.223.81, Dst: 172.217.163.227
> Transmission Control Protocol, Src Port: 61286, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

- Trang web: <http://www.lottecinemavn.com/LCHS/Contents/Movie/Movie-List.aspx> : Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm là **12.298728** và tổng số gói tin bắt được là **4339**



Wireshark capture showing traffic to <http://www.lottecinemavn.com/LCHS/Contents/Movie/Movie-List.aspx>. The capture shows a series of TCP and HTTP packets. The total time for the capture is 12.298728 seconds, and the total number of packets captured is 4339.

No.	Time	Source	Destination	Protocol	Length	Info
4320	9.481107	99.83.201.180	192.168.223.81	TCP	60	80 → 60501 [ACK] Seq=463865 Ack=1931 Win=255488 Len=0
4321	9.513259	99.83.201.180	192.168.223.81	TCP	1454	80 → 60501 [ACK] Seq=463865 Ack=1931 Win=255488 Len=1400 [TCP segment of a reassembled PDU]
4322	9.513657	99.83.201.180	192.168.223.81	HTTP	483	HTTP/1.1 200 OK (image/x-icon)
4323	9.513676	192.168.223.81	99.83.201.180	TCP	54	60501 → 80 [ACK] Seq=1931 Ack=465694 Win=1066752 Len=0
4324	10.196003	192.168.223.64	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4325	10.413881	192.168.223.81	52.114.132.22	TLSv1.2	1017	Application Data
4326	10.413941	192.168.223.81	52.114.132.22	TLSv1.2	755	Application Data
4327	10.599219	192.168.223.81	172.217.163.238	UDP	133	50568 → 443 Len=91
4328	10.652527	52.114.132.22	192.168.223.81	TCP	60	443 → 60487 [ACK] Seq=4439 Ack=3984 Win=263168 Len=0
4329	10.849208	52.114.132.22	192.168.223.81	TLSv1.2	412	Application Data
4330	10.849246	192.168.223.81	52.114.132.22	TCP	54	60487 → 443 [ACK] Seq=3984 Ack=4797 Win=261376 Len=0
4331	11.206035	192.168.223.64	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4332	11.839600	13.107.136.254	192.168.223.81	TCP	60	443 → 55369 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4333	12.039585	192.168.223.59	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4334	12.198845	192.168.223.64	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4335	12.235741	108.177.125.157	192.168.223.81	TLSv1.3	110	Application Data
4336	12.235971	192.168.223.81	108.177.125.157	TCP	54	60495 → 443 [FIN, ACK] Seq=1217 Ack=4109 Win=64512 Len=0
4337	12.253054	108.177.125.157	192.168.223.81	TCP	60	443 → 60495 [FIN, ACK] Seq=4109 Ack=1217 Win=67840 Len=0
4338	12.253088	192.168.223.81	108.177.125.157	TCP	54	60495 → 443 [ACK] Seq=1218 Ack=4110 Win=64512 Len=0
4339	12.298728	108.177.125.157	192.168.223.81	TCP	60	443 → 60495 [ACK] Seq=4110 Ack=1218 Win=67840 Len=0

> Frame 4334: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface \Device\NPF_{98A9ED5D-BC70-4DF9-A7E4-E94C80AEB3B4}, id 0
> Ethernet II, Src: Dell_83:33:1c (8c:ec:4b:83:33:1c), Dst: 96:e6:0d:d7:7a:1b (96:e6:0d:d7:7a:1b)
> Internet Protocol Version 4, Src: 192.168.223.64, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 52343, Dst Port: 1900
> Simple Service Discovery Protocol

Bài 2: 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập 2 website:

- **Domain Name System (DNS)**

Domain Name System (DNS) được sử dụng để chuyển đổi tên miền thành địa chỉ IP. Hệ thống phân cấp DNS bao gồm máy chủ gốc, TLD và máy chủ có thẩm quyền.

- **Simple Service Discovery Protocol**

Giao thức khám phá dịch vụ đơn giản là một giao thức mạng dựa trên bộ giao thức Internet để quảng cáo và khám phá các dịch vụ mạng và thông tin hiện diện.

- **Transmission Control Protocol (TCP)**

Transmission Control Protocol (TCP) là giao thức cốt lõi của Internet Protocol Suite.

Transmission Control Protocol bắt nguồn từ việc thực thi mạng, bổ sung cho Internet Protocol.

- **Transport layer security (TLS)**

Giao thức bảo mật tầng giao vận là một giao thức bảo mật được áp dụng rộng rãi và thiết kế nhằm tạo điều kiện cho sự riêng tư và bảo mật dữ liệu để liên lạc qua Internet. Giao thức này được phát triển dựa trên tiêu chuẩn ssl v3.0 (Secure Socket Layer)

- **UDP (User Datagram Protocol)**

UDP 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.

Bài 3:

- Trang web: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> : Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm là **0.27385** và tổng số gói tin bắt được là **2**

No.	Time	Source	Destination	Protocol	Length	Info
143	3.034342	192.168.223.81	128.119.245.12	HTTP	519	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
147	3.308192	128.119.245.12	192.168.223.81	HTTP	492	HTTP/1.1 200 OK (text/html)

> Frame 147: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{98A9ED5D-BC70-4DF9-A7E4-E94C80AEB3B4}, id 0
> Ethernet II, Src: Dell_83:2f:3d (8c:ec:4b:83:2f:3d), Dst: 96:e6:0d:d7:7a:1b (96:e6:0d:d7:7a:1b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.223.81
> Transmission Control Protocol, Src Port: 80, Dst Port: 61306, Seq: 1, Ack: 466, Len: 438
> Hypertext Transfer Protocol

- Trang web: <http://www.lottecinemavn.com/LCHS/Contents/Movie/Movie-List.aspx> : Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm là **0.481853** và tổng số gói tin bắt được là **6**

19521317-Bai2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Packet list Narrow & Wide Case sensitive Display filter IP

No.	Time	Source	Destination	Protocol	Length	Info
100	4.724682	192.168.223.81	99.83.201.180	HTTP	543	GET /LCHS/Contents/Movie/Movie-List.aspx HTTP/1.1
125	5.019998	192.168.223.81	99.83.201.180	HTTP	821	GET /LCHS/CSS/reset.css?t=20180508001 HTTP/1.1
127	5.021569	192.168.223.81	99.83.201.180	HTTP	822	GET /LCHS/CSS/common.css?t=20181122001 HTTP/1.1
163	5.127017	192.168.223.81	99.83.201.180	HTTP	824	GET /LCHS/CSS/banner.css?t=2017007050001 HTTP/1.1
164	5.127113	192.168.223.81	99.83.201.180	HTTP	828	GET /LCHS/CSS/swiper.min.css?t=2017007050001 HTTP/1.1
208	5.206535	99.83.201.180	192.168.223.81	HTTP	664	HTTP/1.1 200 OK (text/html)
212	5.206994	192.168.223.81	99.83.201.180	HTTP	813	GET /LCHS/Script/Common/jquery-1.11.3.min.js HTTP/1.1
213	5.207756	192.168.223.81	99.83.201.180	HTTP	809	GET /LCHS/Script/Common/jquery-ui.min.js HTTP/1.1
223	5.298377	99.83.201.180	192.168.223.81	HTTP	1001	HTTP/1.1 200 OK (text/css)
225	5.299123	192.168.223.81	99.83.201.180	HTTP	829	GET /LCHS/Script/Common/jquery.jplayer.min.js?v=201704120011 HTTP/1.1
323	5.386451	99.83.201.180	192.168.223.81	HTTP	127	HTTP/1.1 200 OK (application/javascript)
325	5.387366	192.168.223.81	99.83.201.180	HTTP	809	GET /LCHS/Script/Common/jquery.cookie.js HTTP/1.1
366	5.444056	99.83.201.180	192.168.223.81	HTTP	394	HTTP/1.1 200 OK (application/javascript)
372	5.444837	192.168.223.81	99.83.201.180	HTTP	802	GET /LCHS/Script/Library/json2.js HTTP/1.1
384	5.461148	99.83.201.180	192.168.223.81	HTTP	885	HTTP/1.1 200 OK (application/javascript)
386	5.462356	192.168.223.81	99.83.201.180	HTTP	809	GET /LCHS/Script/Common/StringBuilder.js HTTP/1.1
393	5.483109	99.83.201.180	192.168.223.81	HTTP	987	HTTP/1.1 200 OK (text/css)
395	5.483932	192.168.223.81	99.83.201.180	HTTP	800	GET /LCHS/Script/Common/Util.js HTTP/1.1
398	5.510312	99.83.201.180	192.168.223.81	HTTP	819	HTTP/1.1 200 OK (text/css)
401	5.510312	99.83.201.180	192.168.223.81	HTTP	463	HTTP/1.1 200 OK (text/css)

> Frame 208: 664 bytes on wire (5312 bits), 664 bytes captured (5312 bits) on interface \Device\NPF_{98A9ED5D-BC70-4DF9-A7E4-E94C80AEB3B4}, id 0

> Ethernet II, Src: Dell_83:2f:3d (8c:ec:4b:83:2f:3d), Dst: 96:e6:0d:d7:7a:1b (96:e6:0d:d7:7a:1b)

> Internet Protocol Version 4, Src: 99.83.201.180, Dst: 192.168.223.81

> Transmission Control Protocol, Src Port: 80, Dst Port: 60481, Seq: 82816, Ack: 490, Len: 610

Bài 4:

- Nội dung hiển thị trên trang web gaia.cs.umass.edu “Congratulations! You’ve downloaded the first Wireshark lab file!” nằm trong các gói tin HTTP bắt được

Wireshark - Packet 147: 19521317-Bai1.pcapng

> Frame 147: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{98A9ED5D-BC70-4DF9-A7E4-E94C80AEB3B4}, id 0

> Ethernet II, Src: Dell_83:2f:3d (8c:ec:4b:83:2f:3d), Dst: 96:e6:0d:d7:7a:1b (96:e6:0d:d7:7a:1b)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.223.81

> Transmission Control Protocol, Src Port: 80, Dst Port: 61306, Seq: 1, Ack: 466, 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
```

by 0000 96 e6 0d d7 7a 1b 8c ec 4b 83 2f 3d 08 00 45 08z...K/-=-E-
c: 0010 01 de c6 ec 40 00 25 06 77 a7 80 77 f5 0c c0 a8 ...@%w-w-...
ol 0020 df 51 00 50 ef 7a 3c b4 29 d8 b6 01 7b d8 50 18 ..Q.P.z<...{.P-
ntv 0030 00 ed 93 aa 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1.2
fer 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 00 OK..D ate: Wed
0050 2c 20 33 30 20 53 65 70 20 32 30 32 30 20 30 38 , 30 Sep 2020 08
7a 0060 3a 35 38 3a 32 37 20 47 4d 54 0d 0a 53 65 72 76 :58:27 GMT..Serv
40 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
ef 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
00 0090 4c 2f 31 2e 30 2e 32 6b 2d 6d 69 70 73 20 50 48 L/1.0.2k -fips PH
4b 00a0 50 2f 37 2e 34 2e 31 30 20 6d 6f 64 5f 70 65 72 P/7.4.10 mod_per
20 00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
32 00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
41 00d0 66 69 65 64 3a 20 57 65 64 2c 20 33 30 20 53 65 fied: We d, 30 Se
6e 00e0 70 20 32 30 32 30 20 30 35 3a 35 39 3a 30 32 20 p 2020 0 5:59:02
30 00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 35 31 2d 35 GMT..ETa g: "51-5
34 0100 62 30 38 31 39 38 62 30 34 62 38 30 22 0d 0a 41 b08198b0 4b80"-A
30 0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
33 0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes..Con tent-Len

No: 147 • Time: 3.308192 • Source: 128.119.245.12 • Destination: 192.168.223.81 • Protocol: HTTP • Length: 492 • Info: HTTP/1.1 200 OK (text/html)

Close Help

Bài 5:

- Địa chỉ IP của gaia.cs.umass.edu: **128.119.245.12**
- Địa chỉ IP của <http://www.lottecinemavn.com/LCHS/Contents/Movie/Movie-List.aspx> : **99.83.201.180**

- Địa chỉ IP của máy tính đang sử dụng là: **192.168.223.81**

Bài 6:

Khi bạn nhập một địa chỉ web vào trình duyệt:

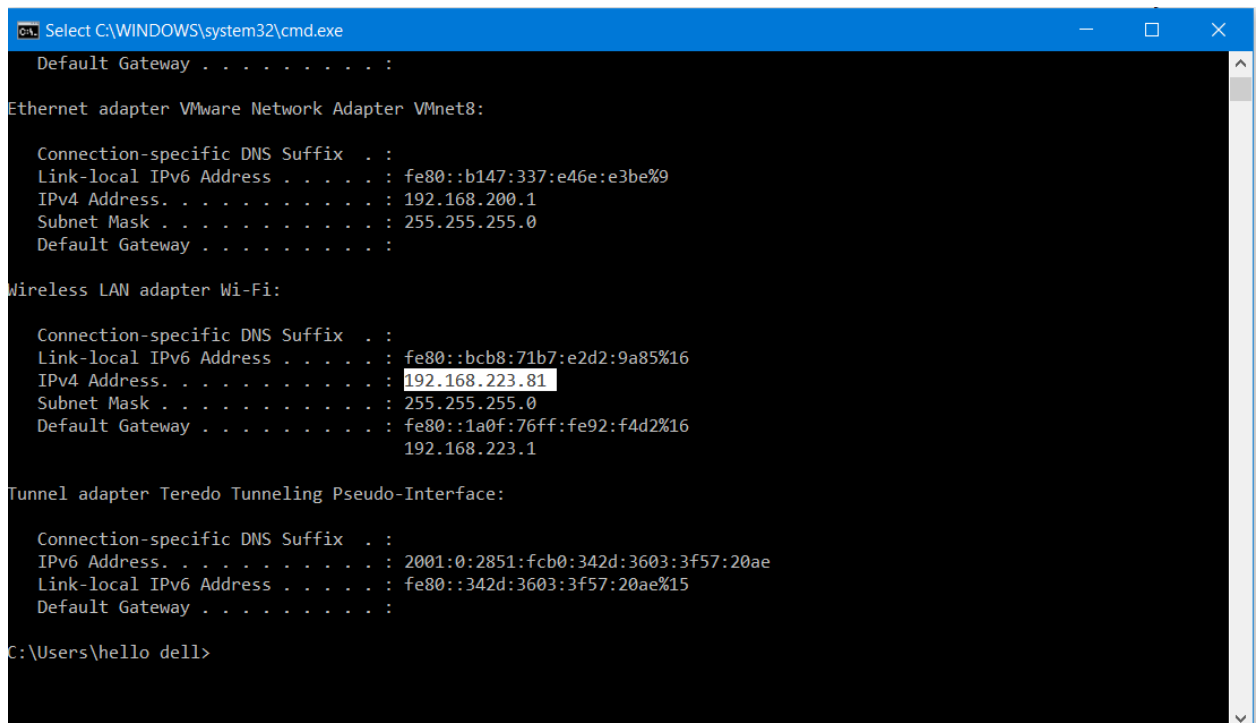
1. Trình duyệt tìm đến máy chủ DNS và tìm địa chỉ thật sự của máy chủ chứa trang web.
2. Trình duyệt gửi một tin yêu cầu HTTP (HTTP request) tới máy chủ đó yêu cầu nó gửi về một bản copy của trang web tới máy của người dùng. Yêu cầu HTTP đó, và tất cả dữ liệu khác gửi qua lại giữa máy chủ và máy khách, được truyền tải qua mạng Internet sử dụng giao thức TCP/IP.
3. Nếu máy chủ chấp nhận yêu cầu của máy khách, máy chủ sẽ gửi một tin nhắn “200 OK”, có nghĩa là “Tất nhiên là bạn có thể xem trang web này rồi! Nhận lấy này!”, và sau đó bắt đầu gửi những file của trang web tới trình duyệt dưới dạng những mảnh nhỏ dữ liệu được gọi là gói dữ liệu (data packets).
4. Trình duyệt sẽ ráp những mảnh nhỏ đó thành một trang web hoàn chỉnh và hiển thị nó lên màn hình.

Nguồn:

https://developer.mozilla.org/vi/docs/Learn/Getting_started_with_the_web/How_the_Web_works

*** Mở rộng:

- Địa chỉ IP dùng để nhận diện và liên lạc với nhau trên mạng máy tính bằng cách sử dụng giao thức Internet.
- Cách xem địa chỉ ip máy tính:
 1. Phím window + R → Mở CMD
 2. Gõ câu lệnh **ipconfig**



```
Select C:\WINDOWS\system32\cmd.exe

Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b147:337:e46e:e3be%9
    IPv4 Address. . . . . : 192.168.200.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

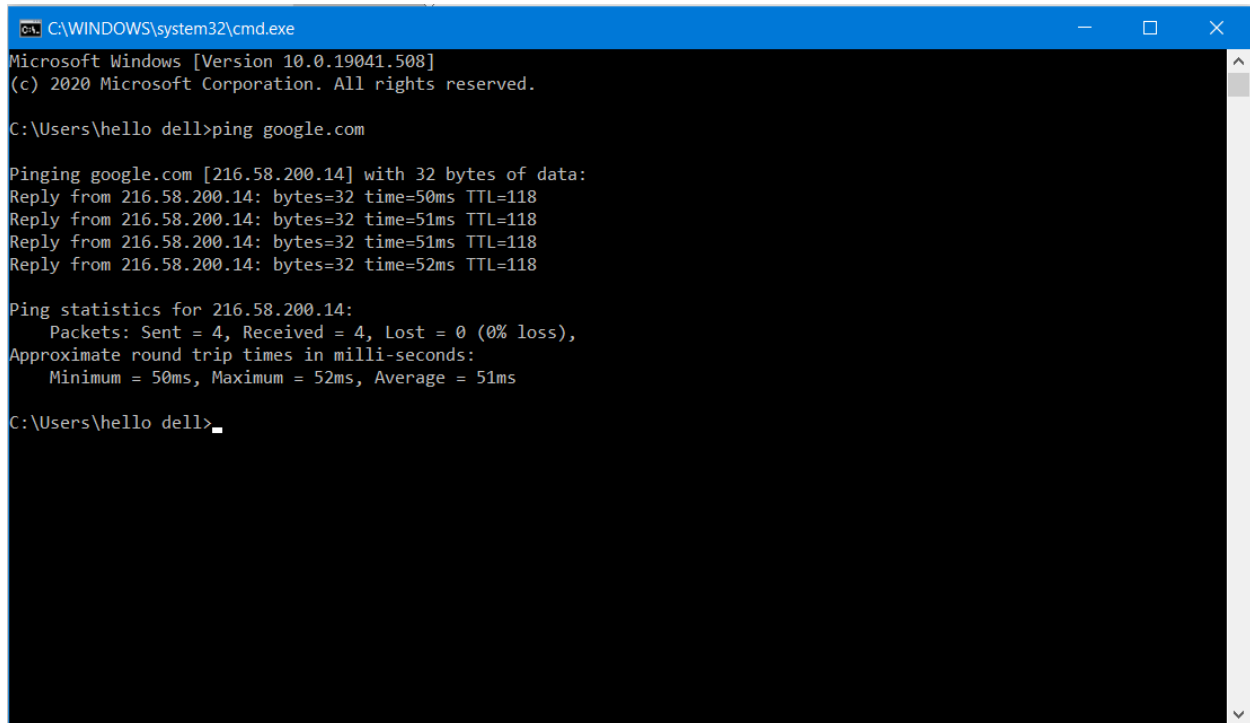
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::bcb8:71b7:e2d2:9a85%16
    IPv4 Address. . . . . : 192.168.223.81
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1a0f:76ff:fe92:f4d2%16
                                192.168.223.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:0:2851:fc0:342d:3603:3f57:20ae
    Link-local IPv6 Address . . . . . : fe80::342d:3603:3f57:20ae%15
    Default Gateway . . . . . :

C:\Users\hello dell>
```

- Cách xem địa chỉ website khác:
 1. Gõ Window + R → Mở CMD
 2. Gõ ping + Tên trang web



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\hello dell>ping google.com

Pinging google.com [216.58.200.14] with 32 bytes of data:
Reply from 216.58.200.14: bytes=32 time=50ms TTL=118
Reply from 216.58.200.14: bytes=32 time=51ms TTL=118
Reply from 216.58.200.14: bytes=32 time=51ms TTL=118
Reply from 216.58.200.14: bytes=32 time=52ms TTL=118

Ping statistics for 216.58.200.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 52ms, Average = 51ms

C:\Users\hello dell>
```