

1

BÁO CÁO BÀI THỰC HÀNH SỐ 1 [Tiêu đề bài TH]

Môn học: [Tên môn học]

Sinh viên thực hiện	Trần Hải Đăng (23520237)
Thời gian thực hiện	22/09/2019 – 29/09/2019
Số câu đã hoàn thành	5/5

TRẢ LỜI CÁC CÂU HỎI

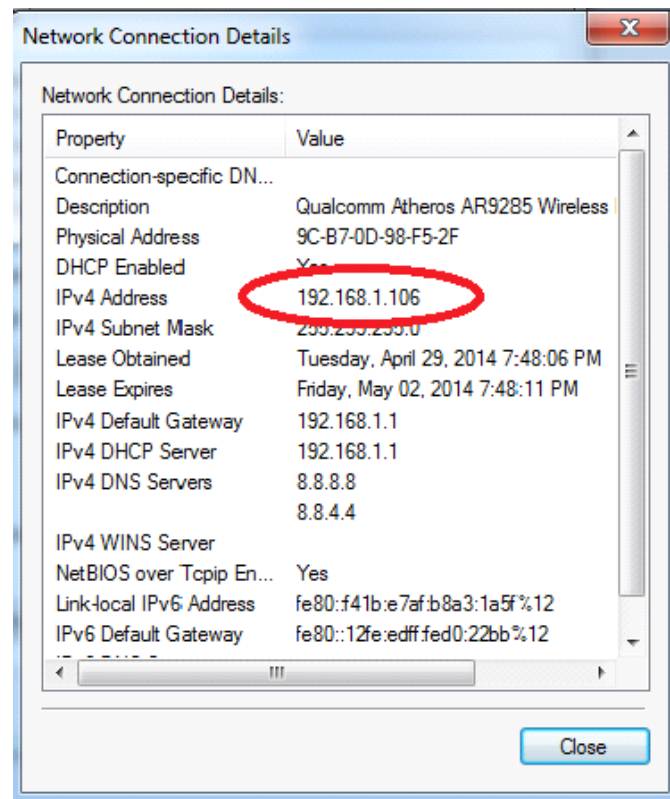
Gợi ý: Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn.

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



Câu 1:

- Tổng thời gian bắt gói tin là 4,6448s và bắt được 1917 gói tin.

1916	4.644696	10.45.212.103	224.0.0.251	MDNS
1917	4.644821	fe80::b1:70b7:16d0::	ff02::fb	MDNS

Câu 2:

- Trong các gói tin bắt dc có 2 gói tin HTTP

No.	Time	Source	Destination	Protocol	Length	Info
796	2.303107	10.45.212.103	128.119.245.12	HTTP	626	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
958	2.570730	128.119.245.12	10.45.212.103	HTTP	492	HTTP/1.1 200 OK (text/html)

Câu 3: Các giao thức xuất hiện trong cột giao thức:

- HTTP là một giao thức dùng để truy xuất tài nguyên như tài liệu HTML. Nó là nền tảng của mọi trao đổi dữ liệu trên Web và là một giao thức client-server, tức là các yêu cầu được khởi tạo bởi người nhận, thường là trình duyệt web
- TCP là một trong những giao thức chính của bộ giao thức Internet. Nó nằm giữa lớp ứng dụng và lớp mạng, được sử dụng để cung cấp dịch

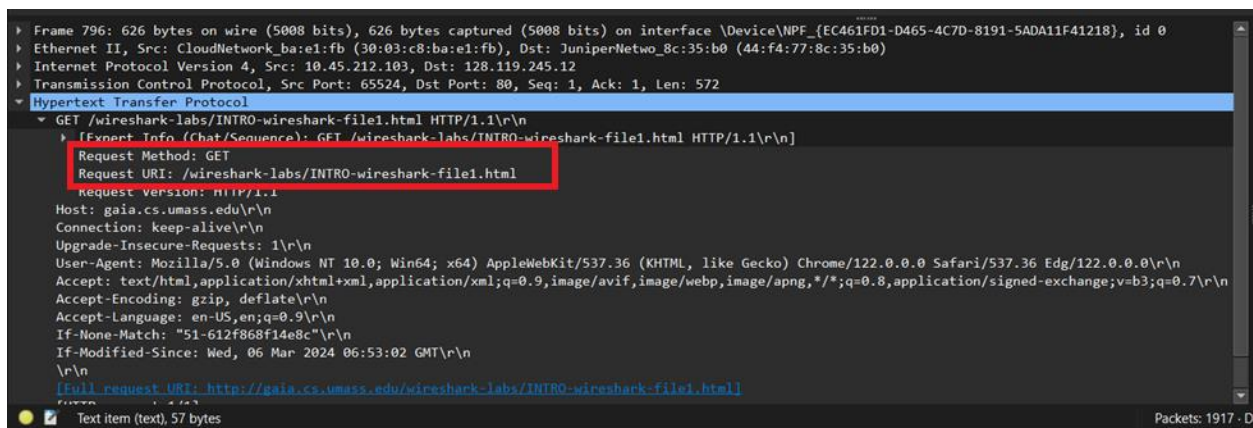
vụ giao hàng đáng tin cậy. TCP theo dõi các phân đoạn được truyền hoặc nhận bằng cách gán số cho từng phân đoạn

- MDNS là một giao thức nhằm giúp giải quyết tên trong các mạng nhỏ. Thay vì truy vấn một máy chủ tên, tất cả các thành phần trong mạng được trực tiếp địa chỉ
- UDP là một giao thức tầng vận chuyển. Khác với TCP, nó là một giao thức không đáng tin cậy và không kết nối. Vì vậy, không cần thiết lập kết nối trước khi truyền dữ liệu
- DHCP là một giao thức quản lý mạng được sử dụng trên các mạng Internet Protocol (IP) để tự động gán địa chỉ IP và các thông số giao tiếp khác cho các thiết bị kết nối với mạng sử dụng kiến trúc client-server.

Câu 4:

- Gói tin HTTP GET đầu tiên gửi đến sever thử nghiệm là gói tin số 796.
- Dựa trên packet details của gói tin ta biết được gói tin này dùng để gửi yêu cầu truy cập, lấy thông tin từ sever thử nghiệm về máy thông qua request method: GET.

No.	Time	Source	Destination	Protocol	Length	Info
796	2.303107	10.45.212.103	128.119.245.12	HTTP	626	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
958	2.570730	128.119.245.12	10.45.212.103	HTTP	492	HTTP/1.1 200 OK (text/html)



```
Frame 796: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{EC461FD1-D465-4C7D-8191-5ADA11F41218}, id 0
Ethernet II, Src: CloudNetwork_ba:e1:fb (30:03:c8:ba:e1:fb), Dst: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0)
Internet Protocol Version 4, Src: 10.45.212.103, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 65524, Dst Port: 80, Seq: 1, Ack: 1, Len: 572
Hypertext Transfer Protocol
  GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/INTRO-wireshark-file1.html
    request version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "51-612f868f14e8c"\r\n
    If-Modified-Since: Wed, 06 Mar 2024 06:53:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    \r\n
```

Câu 5:

- Gói tin phản hồi của gói tin HTTP GET là gói tin số 958 dựa vào packet details của gói tin:

No.	Time	Source	Destination	Protocol	Length	Info
796	2.303107	10.45.212.103	128.119.245.12	HTTP	626	GET /wireshark-labs/INTRO-wi
958	2.570730	128.119.245.12	10.45.212.103	HTTP	492	HTTP/1.1 200 OK (text/html)

▶ Frame 796: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface \Device\NPF_{EC461...
 ▶ Ethernet II, Src: CloudNetwork ba:e1:fb (30:03:c8:ba:e1:fb), Dst: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:..
 ▶ Internet Protocol Version 4, Src: 10.45.212.103, Dst: 128.119.245.12
 ▶ Transmission Control Protocol, Src Port: 65524, Dst Port: 80, Seq: 1, Ack: 1, Len: 572
 ▶ Hypertext Transfer Protocol

```

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "51-612f868f14e8c"\r\n
If-Modified-Since: Wed, 06 Mar 2024 06:53:02 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 958]
  
```

Câu 6:

- Thời gian kể từ khi gửi đến khi nhận phản hồi là 0,267623s

```

[Time since request: 0.267623000 seconds]
  
```

Câu 7:

- Nội dung của trang web có hiển thị trong gói tin bắt được :

```

HTTP/1.1 200 OK\r\n
Date: Wed, 06 Mar 2024 07:09:16 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Wed, 06 Mar 2024 06:59:02 GMT\r\n
ETag: "51-612f87e6a068b"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.267623000 seconds]
[Request in frame: 796]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
Line-based text data: text/html (3 lines)
<html>\n
Congratulations! You've downloaded the first Wireshark lab file!\n
</html>\n
  
```

Câu 8:

- Địa chỉ IP của máy tính đang sử dụng là: 10.45.212.103

```
C:\Users\dangn>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::4cd8:830c:384b:5c95%16
    IPv4 Address. . . . . : 10.45.212.103
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.45.0.1

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

- Địa chỉ IP của gaia.cs.umass.edu là: 128.119.245.12

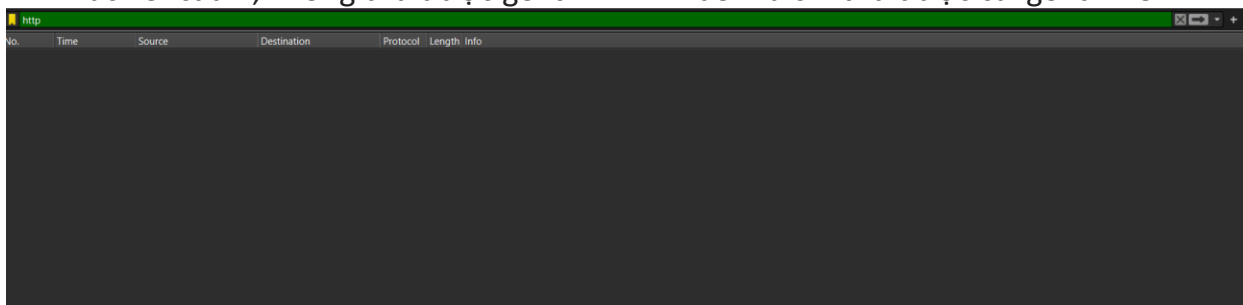
No.	Time	Source	Destination	Protocol	Length	Info
796	2.303107	10.45.212.103	128.119.245.12	HTTP	626	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
958	2.570730	128.119.245.12	10.45.212.103	HTTP	492	HTTP/1.1 200 OK (text/html)

Câu 9:

- Từ các thông tin ở trên, khi truy cập 1 trang web thì chúng ta gửi gói tin yêu cầu quyền truy cập đến sever sau đó sever sẽ gửi các gói tin bao gồm nội dung, thông tin của trang web đến máy tính mình và hiển thị thông qua trình duyệt.
- Trình duyệt có tác dụng như cầu nối giữa người dùng và trang web, nó hiển thị các nội dung được sever cung cấp.

Câu 10:

- Khi sử dụng bộ lọc “http” như ở đối với website ở Task 1 thì kết quả thu được khác với câu 1, không thu được gói tin HTTP nào mà chỉ thu được cái gói tin TLS.



Câu 11:

- Địa chỉ IP của trang web uit.edu.vn là: 192.168.20.23
- IP máy lúc này: 10.45.212.103

```
PS C:\Users\dangn> ping uit.edu.vn

Pinging uit.edu.vn [192.168.20.23] with 32 bytes of data:
Reply from 192.168.20.23: bytes=32 time=5ms TTL=62
Reply from 192.168.20.23: bytes=32 time=5ms TTL=62
Reply from 192.168.20.23: bytes=32 time=9ms TTL=62
Reply from 192.168.20.23: bytes=32 time=9ms TTL=62

Ping statistics for 192.168.20.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 9ms, Average = 7ms

IPv4 Address. . . . . : 10.45.212.103
```

Câu 12:

- Không thể thấy được nội dung trả về của website mà chỉ có thấy được cái gói tin TCP và TLS đã được mã hóa.

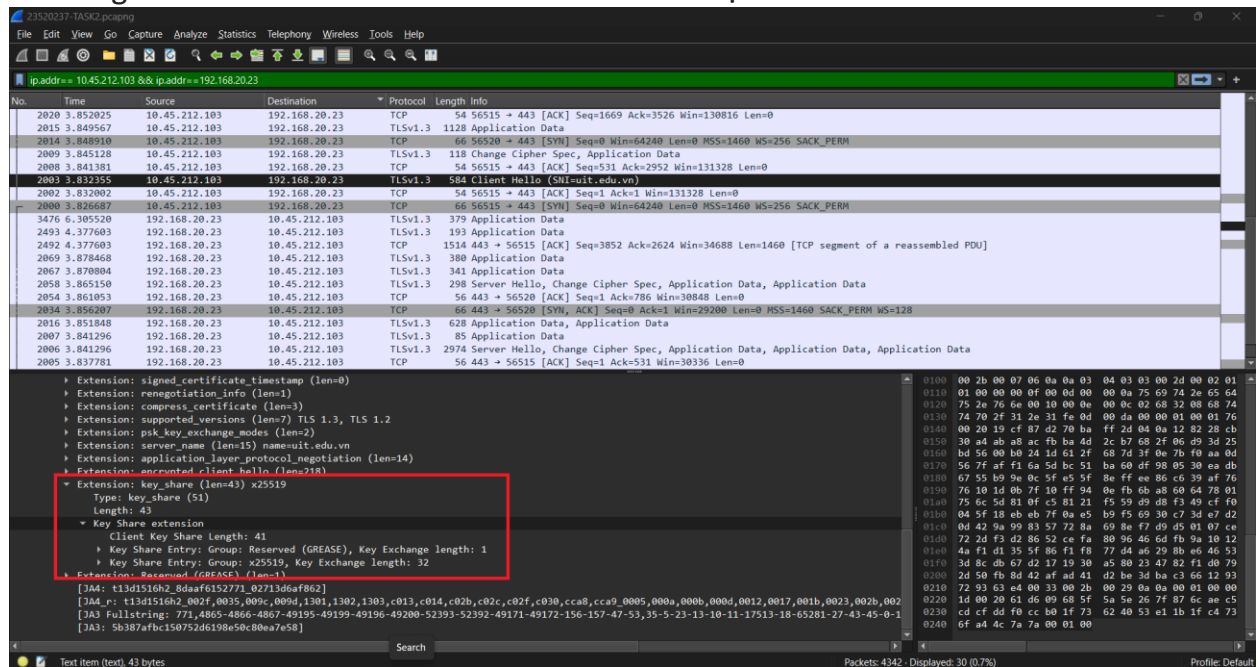
The image shows a Wireshark packet capture of a TLS handshake. The packets are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
2000	3.826687	10.45.212.103	192.168.20.23	TCP	66	56515 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2001	3.831927	192.168.20.23	10.45.212.103	TCP	66	443 → 56515 [ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2002	3.832002	10.45.212.103	192.168.20.23	TCP	54	56515 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
2003	3.832355	10.45.212.103	192.168.20.23	TLSv1.3	584	Client Hello (SHA=uit.edu.vn)
2005	3.837781	192.168.20.23	10.45.212.103	TCP	56	443 → 56515 [ACK] Seq=1 Ack=531 Win=30336 Len=0
2006	3.841296	192.168.20.23	10.45.212.103	TLSv1.3	2974	Server Hello, Change Cipher Spec, Application Data, Application Data
2007	3.841296	192.168.20.23	10.45.212.103	TLSv1.3	85	Application Data
2008	3.841381	10.45.212.103	192.168.20.23	TCP	54	56515 → 443 [ACK] Seq=531 Ack=2952 Win=131328 Len=0
2009	3.845128	10.45.212.103	192.168.20.23	TLSv1.3	118	Change Cipher Spec, Application Data
2014	3.849910	10.45.212.103	192.168.20.23	TCP	66	56520 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2015	3.849967	10.45.212.103	192.168.20.23	TLSv1.3	1128	Application Data
2016	3.851848	192.168.20.23	10.45.212.103	TLSv1.3	628	Application Data, Application Data
2020	3.852025	10.45.212.103	192.168.20.23	TCP	54	56515 → 443 [ACK] Seq=1669 Ack=3526 Win=130816 Len=0
2034	3.856287	192.168.20.23	10.45.212.103	TCP	66	443 → 56520 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
2039	3.856275	10.45.212.103	192.168.20.23	TCP	54	56520 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
2040	3.856552	10.45.212.103	192.168.20.23	TLSv1.3	839	Client Hello (SHA=uit.edu.vn)
2054	3.861053	192.168.20.23	10.45.212.103	TCP	56	443 → 56520 [ACK] Seq=1 Ack=786 Win=30848 Len=0
2058	3.865150	192.168.20.23	10.45.212.103	TLSv1.3	298	Server Hello, Change Cipher Spec, Application Data, Application Data
2065	3.865429	10.45.212.103	192.168.20.23	TLSv1.3	118	Change Cipher Spec, Application Data
2067	3.870804	192.168.20.23	10.45.212.103	TLSv1.3	341	Application Data

Frame 2000: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF... id 0
Ethernet II, Src: CloudNetwork_Base1:fb (30:03:c8:ba:e1:fb), Dst: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0)
Internet Protocol Version 4, Src: 10.45.212.103, Dst: 192.168.20.23
Transmission Control Protocol, Src Port: 56515, Dst Port: 443, Seq: 0, Len: 0

Câu 13:

- 2 gói tin quan trọng khi truy cập website này:
 - + Gói tin TLS Handshake: Có tác dụng trao đổi các chứng chỉ SSL, yêu cầu về bộ mã hóa và dữ liệu được tạo ngẫu nhiên để tạo ra các khóa phiên để mã hóa nội dung của website nhằm đảm bảo về tính bảo mật.



- + Các gói tin TCP: Các gói tin này đóng vai trò cung cấp thông tin của website bằng các gói tin nhỏ đã được mã hóa theo khóa được thống nhất giữa máy tính và sever. Khi máy tính nhận được các gói tin TCP nó sẽ ghép chúng lại thành nội dung của website.

Câu 14:

- Địa chỉ IP là một định danh được gán cho mỗi thiết bị kết nối với internet, nó hoạt động như một địa chỉ giao dịch giúp cho các thiết bị kết nối với nhau qua internet, giúp phân biệt giữa các máy tính, router và website khác nhau/
- Các cách để xem được địa chỉ IP của máy tính:
 - + Setting -> Network and internet -> Wi-Fi -> Hardware properties

Network & internet > Wi-Fi > Wi-Fi

Wi-Fi properties

IP assignment:	Automatic (DHCP)	Edit
DNS server assignment:	Automatic (DHCP)	Edit
SSID:	A22.04 5G	Copy
Protocol:	Wi-Fi 6 (802.11ax)	
Security type:	WPA3-Personal	
Manufacturer:	MediaTek, Inc.	
Description:	MediaTek Wi-Fi 6 MT7921 Wireless LAN Card	
Driver version:	3.3.3.760	
Network band:	5 GHz	
Network channel:	52	
Link speed (Receive/Transmit):	1201/1201 (Mbps)	
IPv6 address:	2405:4802:a612:2cb0:23da:3671:a754:a27e 2405:4802:a612:2cb0:ffff:ffff:ffff:fff5	
Link-local IPv6 address:	fe80::4cd8:830c:384b:5c95%16	
IPv6 DNS servers:	fe80::1%16 (Unencrypted)	
IPv4 address:	192.168.1.248	
IPv4 DNS servers:	192.168.1.1 (Unencrypted)	
Physical address (MAC):	30-03-C8-BA-E1-FB	

+ Dùng lệnh ipconfig trong command prompt:

```
C:\Users\dangn>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2405:4802:a612:2cb0:23da:3671:a754:a27e
    IPv6 Address. . . . . : 2405:4802:a612:2cb0:ffff:ffff:ffff:fff5
    Temporary IPv6 Address. . . . . : 2405:4802:a612:2cb0:e9ce:de54:a9a6:7c38
    Link-local IPv6 Address . . . . . : fe80::4cd8:830c:384b:5c95%16
    IPv4 Address. . . . . : 192.168.1.248
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::1%16
                                192.168.1.1
```

- Cách xem địa chỉ IP của 1 website:

+ Dùng lệnh ping + địa chỉ website trong command prompt:

```
C:\Users\dangn>ping uit.edu.vn
```

```
Pinging uit.edu.vn [118.69.123.140] with 32 bytes of data:
```

+ Dùng lệnh tracert + địa chỉ website trong command prompt:

```
C:\Users\dangn>tracert uit.edu.vn
```

```
Tracing route to uit.edu.vn [118.69.123.140]  
over a maximum of 30 hops:
```

+ Dùng lệnh nslookup + địa chỉ website trong command prompt:

```
PS C:\Users\dangn> nslookup uit.edu.vn
```

```
Server: UnKnown
```

```
Address: fe80::1
```

```
Non-authoritative answer:
```

```
Name: uit.edu.vn
```

```
Address: 118.69.123.140
```

+ Nhập địa chỉ IP của website trên toolbox.googleapps.com:

The screenshot shows the Google Admin Toolbox Dig interface. The browser address bar displays <https://toolbox.googleapps.com/apps/dig/#A/>. The page title is "Google Admin Toolbox Dig". The "Name" field contains "uit.edu.vn". Below the name, there is a row of tabs for different DNS record types: A, AAAA, ANY, CAA, CNAME, DNSKEY, DS, MX, NS, PTR, SOA, and SRV. The "A" tab is selected. Below the tabs, the "TTL" is shown as "6 minutes". Under the "A" label, the "DATA" field displays the IP address "118.69.123.140", which is highlighted with a red box.