บจก.สยามถนัดแฮก

NCSA CTF Boot Camp #2

Network Security

Responsible: Mr. Peeratach Butto
Version (Date): 1.0 (2024-09-14)
Confidentiality class: Public

whoami

Pichaya (LongCat) Morimoto
Lead Penetration Tester
Siam Thanat Hack Co., Ltd.

Peeratach (Peter) Butto
Penetration Tester
Siam Thanat Hack Co., Ltd.

Yasinthon (Not) Khemprakhon
Penetration Tester
Siam Thanat Hack Co., Ltd.

Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างโค้ด และรูปใน การบรรยาย นี้ เป็นระบบจำลองของทางผู้บรรยาย ไม่ใช่ระบบลูกค้า

Agenda (Day 1)

เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	เสวนาแนะแนวเส้นทางอาชีพ

Content Overview

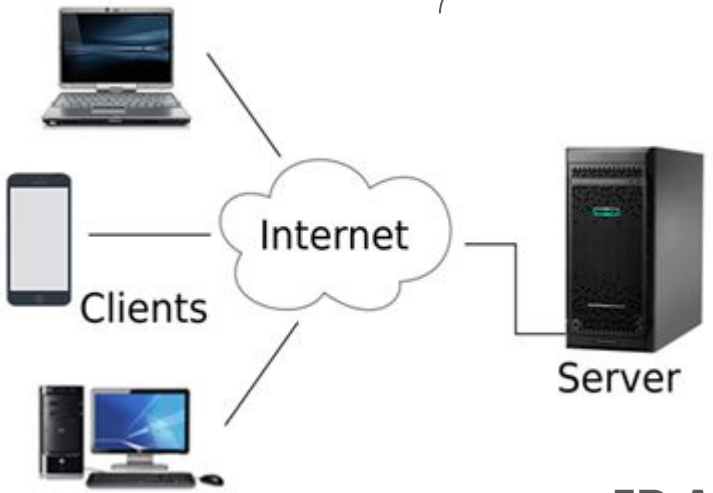
- Network Traffic คืออะไร?
  - Network Packet
  - TCP & UDP
  - Application Protocol
- วิเคราะห์ Network Traffic ด้วย Wireshark
  - netcat
- Plaintext และ Encrypted Packet
- Network Scan ด้วย nmap
- ลองทำแลป !
  - Lab 1: วิเคราะห์ HTTP Protocol ใน PCAP
  - Lab 2: วิเคราะห์ FTP Protocol ใน PCAP

ระบบเครือข่าย (Network) คืออะไร

Client/Server Network = ผู้ใช้งาน และ ผู้ให้บริการ

Client (ผู้ใช้งาน)

Server (ผู้ให้บริการ)

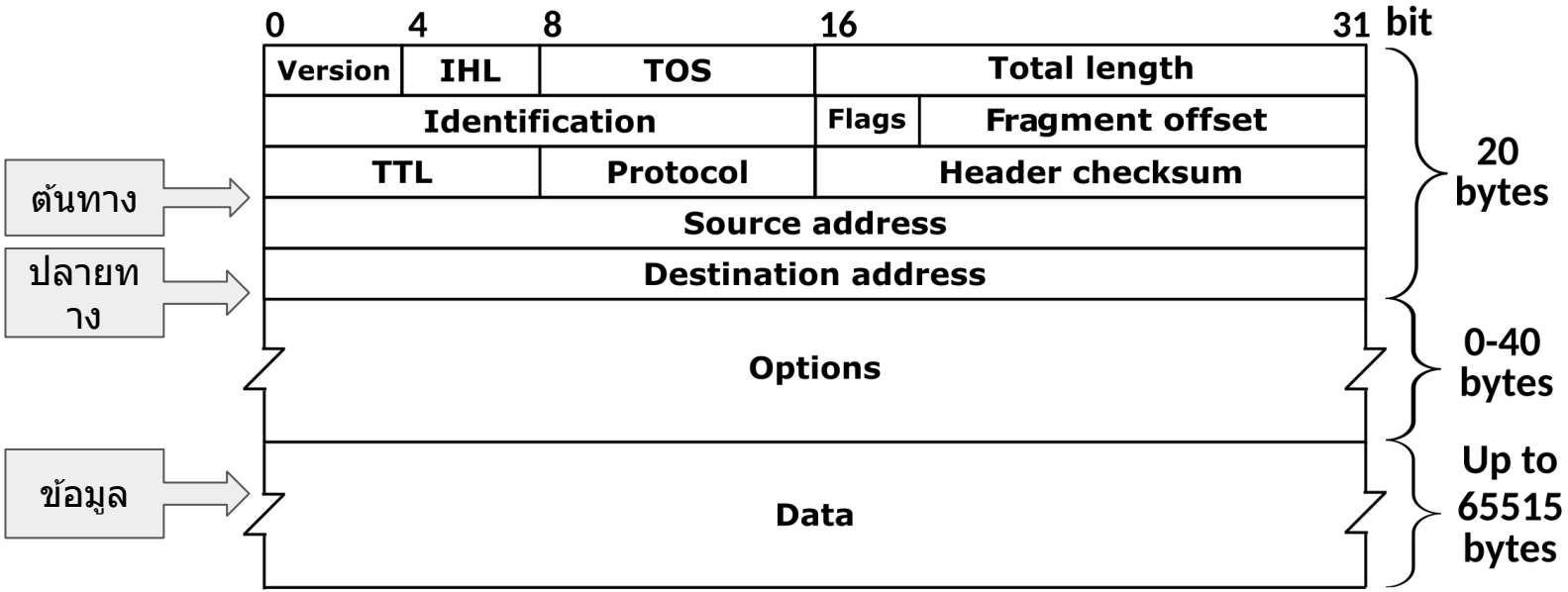


IP Address
(เลขที่บ้านต้นทาง)

Network Packet
(จดหมาย)

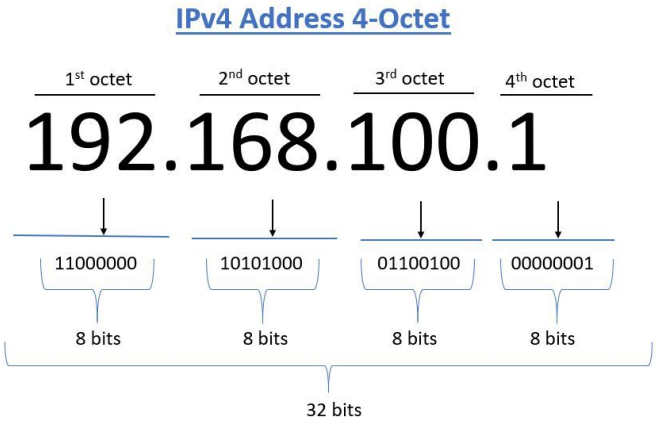
IP Address
(เลขที่บ้านปลายทาง)

Network Packet (จดหมาย)



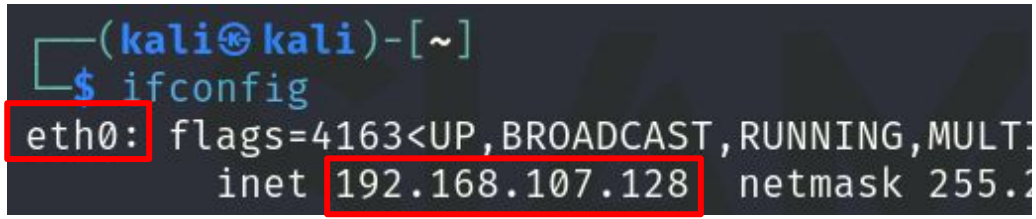
https://en.wikipedia.org/wiki/IPv4

IP Address (เลขที่บ้าน)

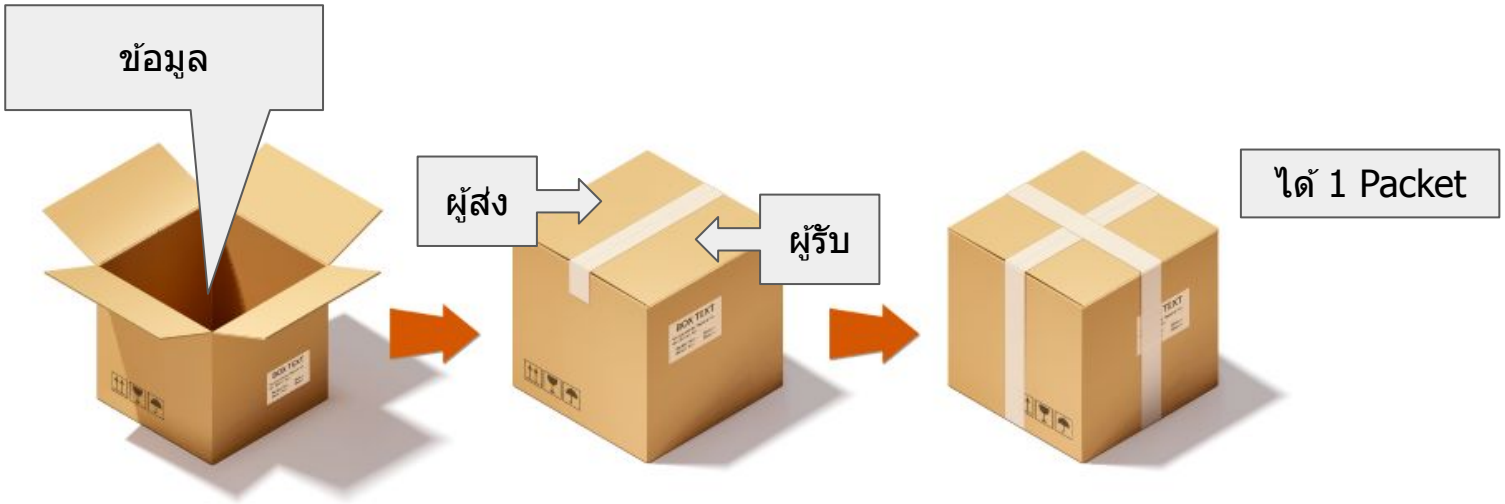


https://medium.com/@shrutiikhatal07

https://checkip.amazonaws.com

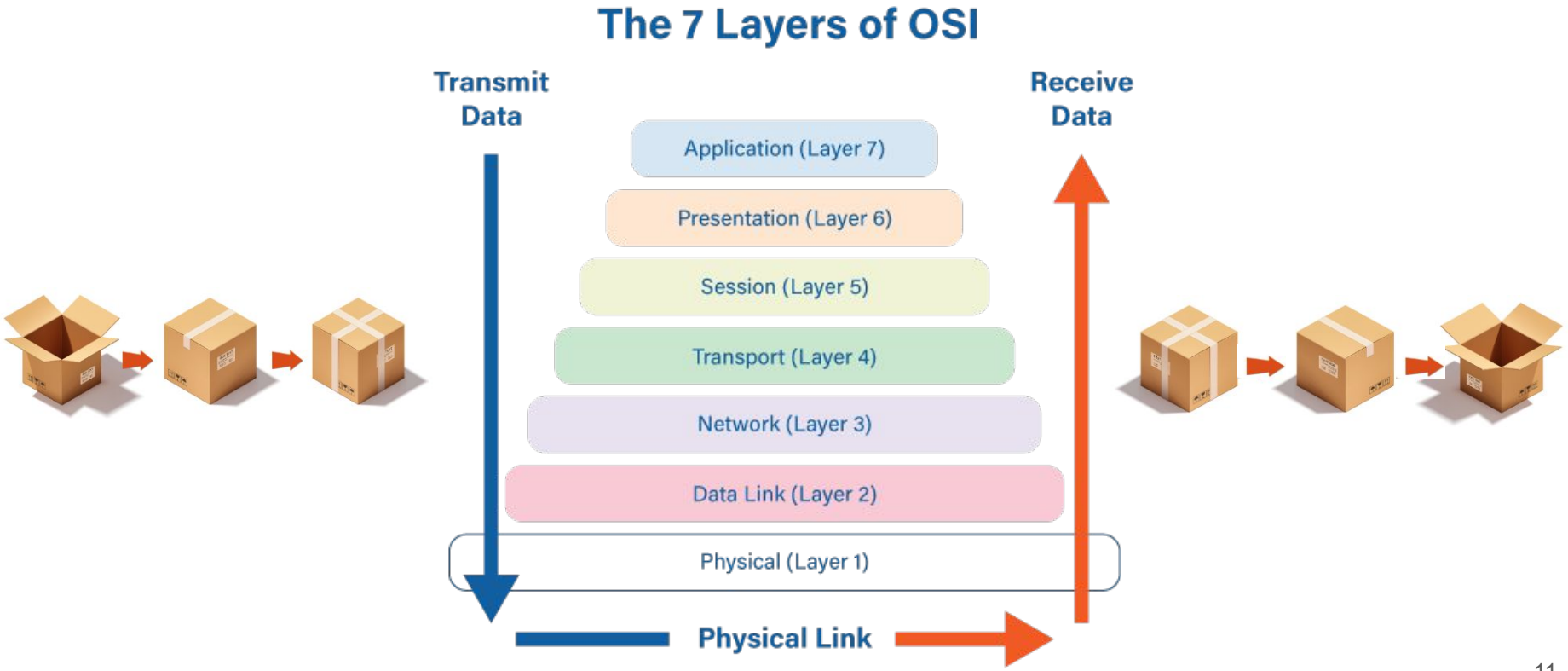


Network Packet คืออะไร



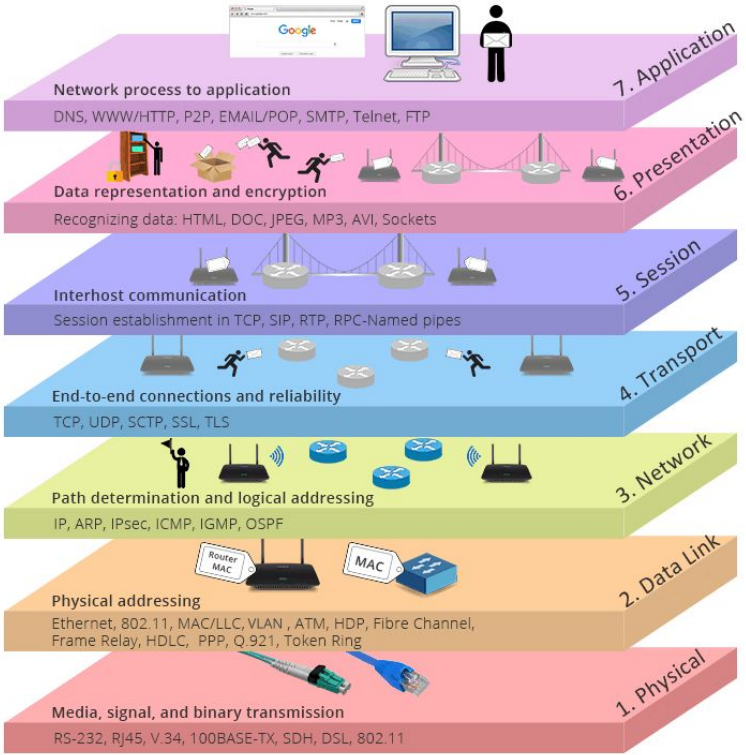
https://www.meowlogis.com

OSI (Open Systems Interconnection) Model



ที่มา: https://insights.profitap.com/osi-7-layers-explained-the-easy-way

OSI (Open Systems Interconnection) Model



ที่มา: https://media.fs.com/images/community/upload/kindEditor/202107/29/original-seven-layers-of-osi-model-1627523878-JYjV8oybcC.png

Network Packet Analyzer (การวิเคราะห์ข้อมูล Packet)

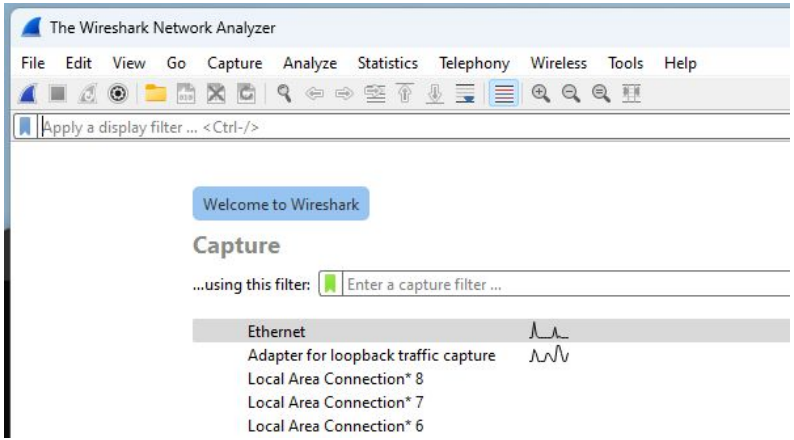
Client

IP Address
(เลขที่บ้าน)

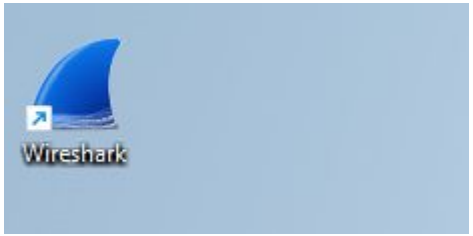
Network Packet

Server

IP Address
(เลขที่บ้าน)

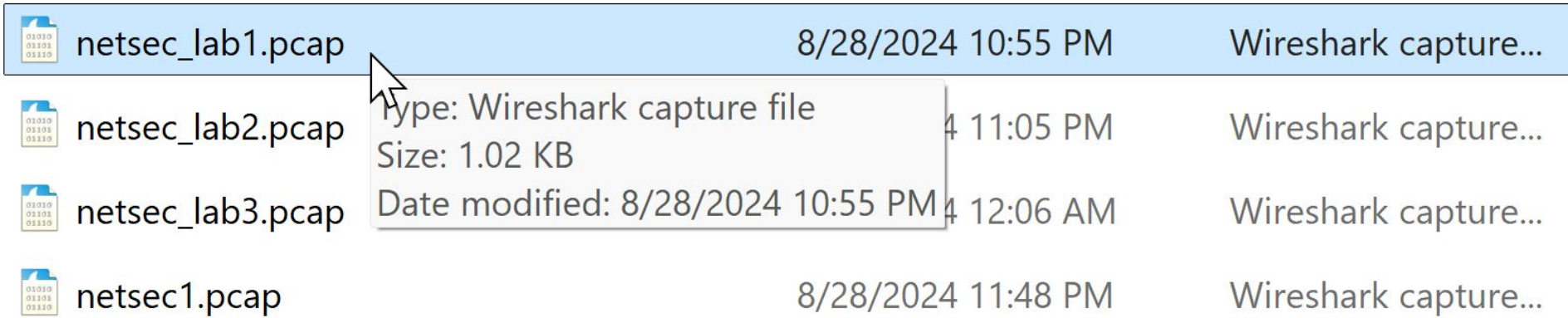


WIRESHARK



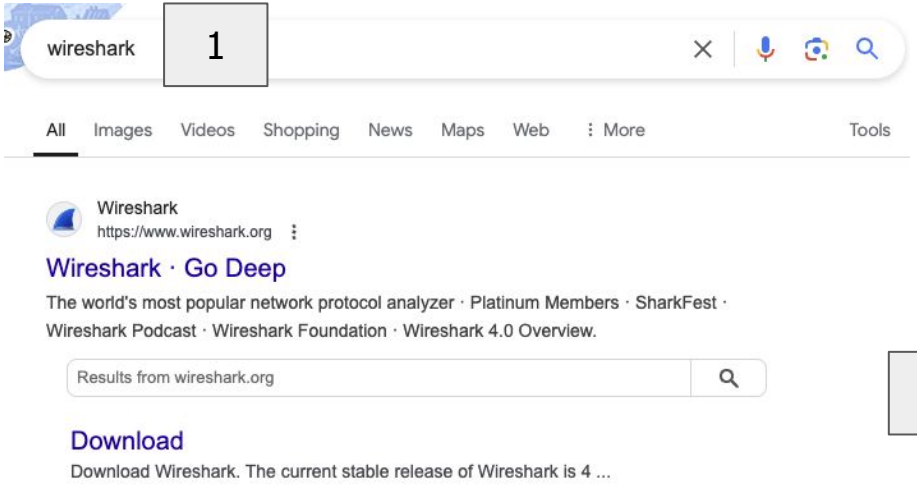
ไฟล์ PCAP

ประเภทไฟล์ที่เก็บบันทึก Network Packet ที่เคยถูกรับ-ส่ง ระหว่างคอมพิวเตอร์ ในอดีต



Install Wireshark

ติดตั้ง Wireshark

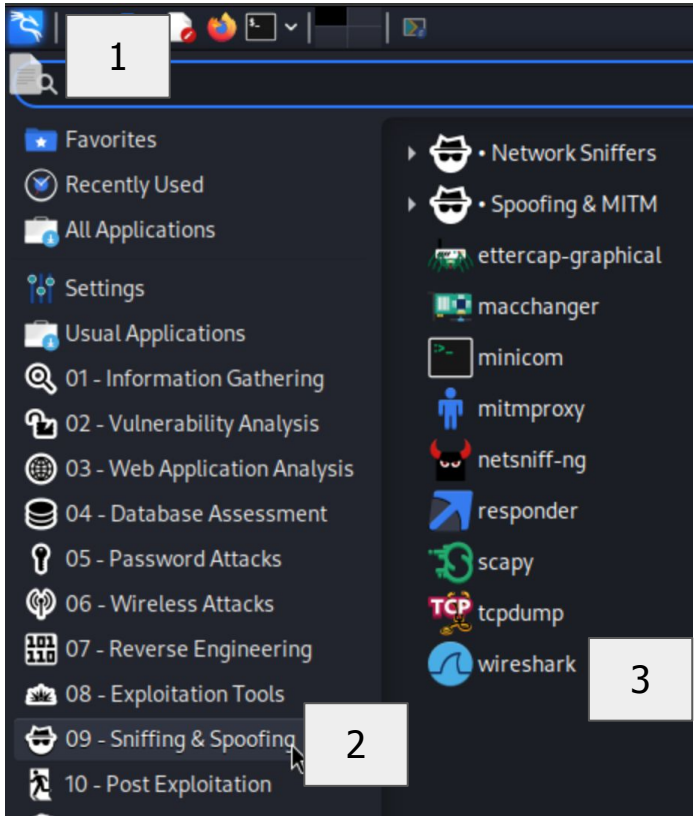


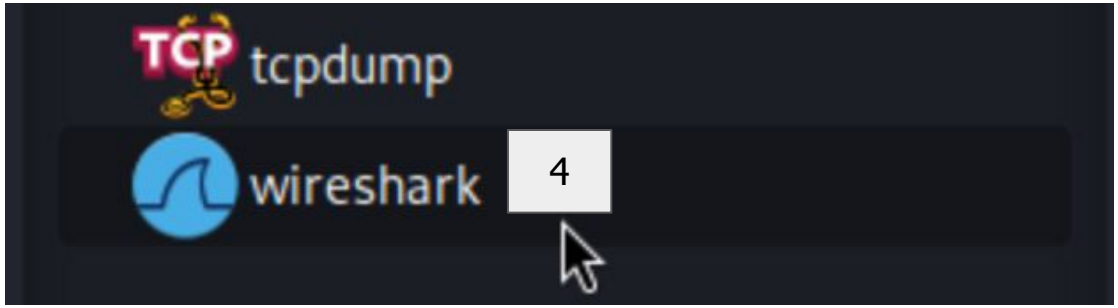
2

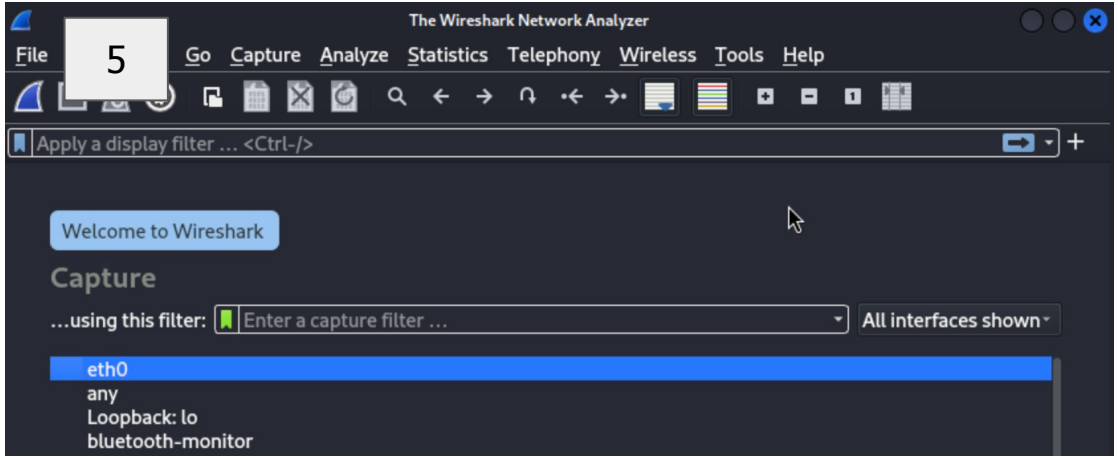
3

https://www.wireshark.org/download.html

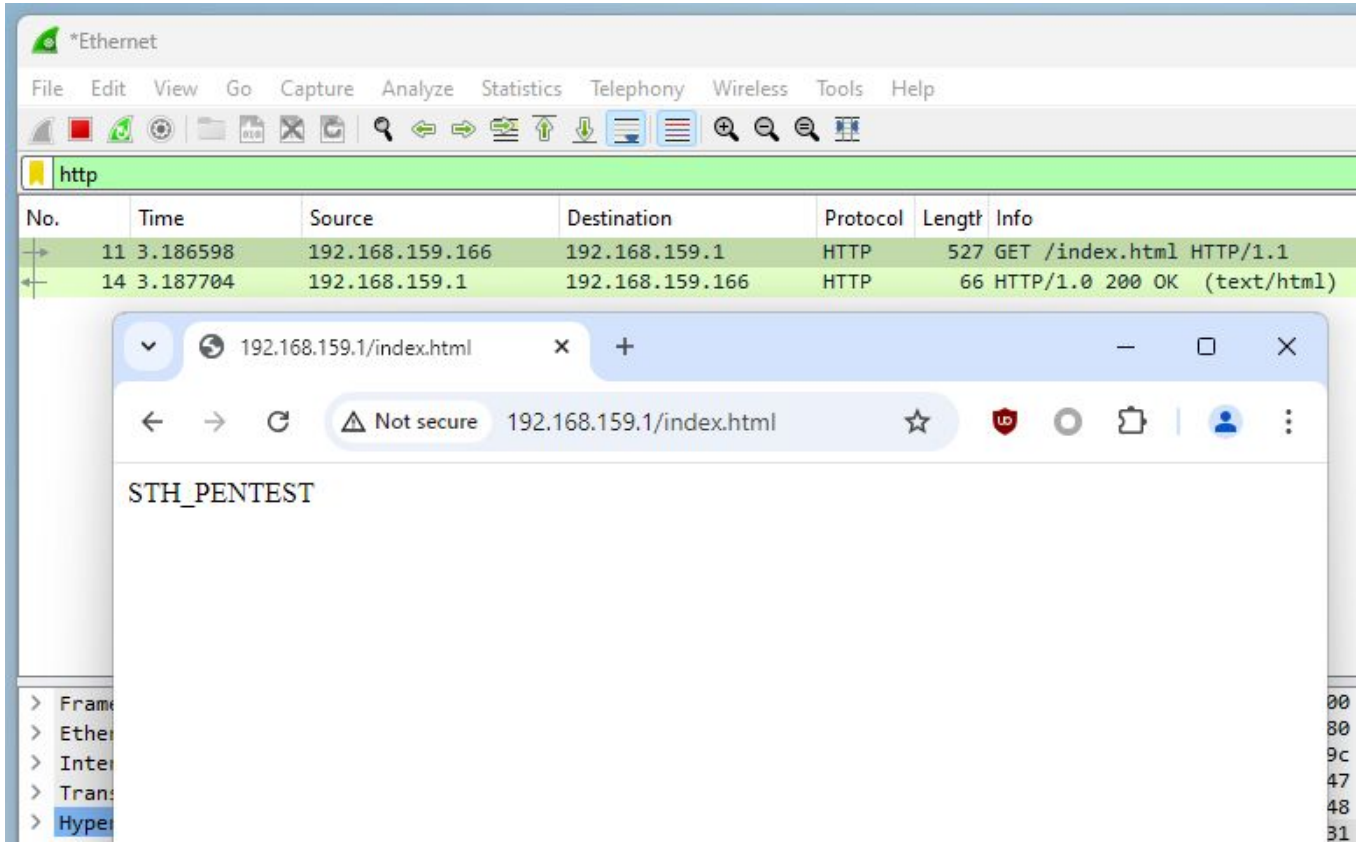
โปรแกรม Wireshark ใน Kali





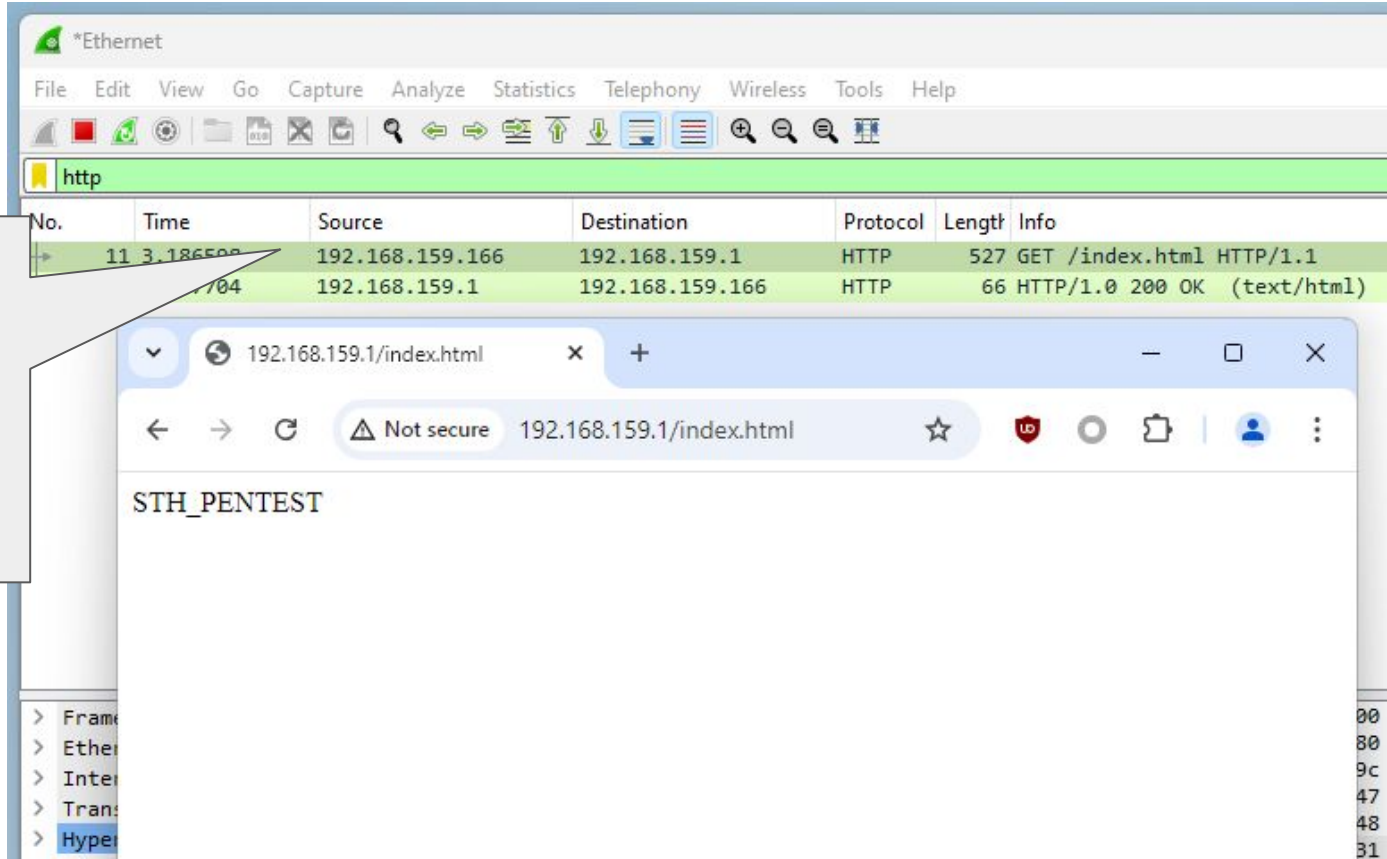


การวิเคราะห์ Network Packet ด้วย Wireshark



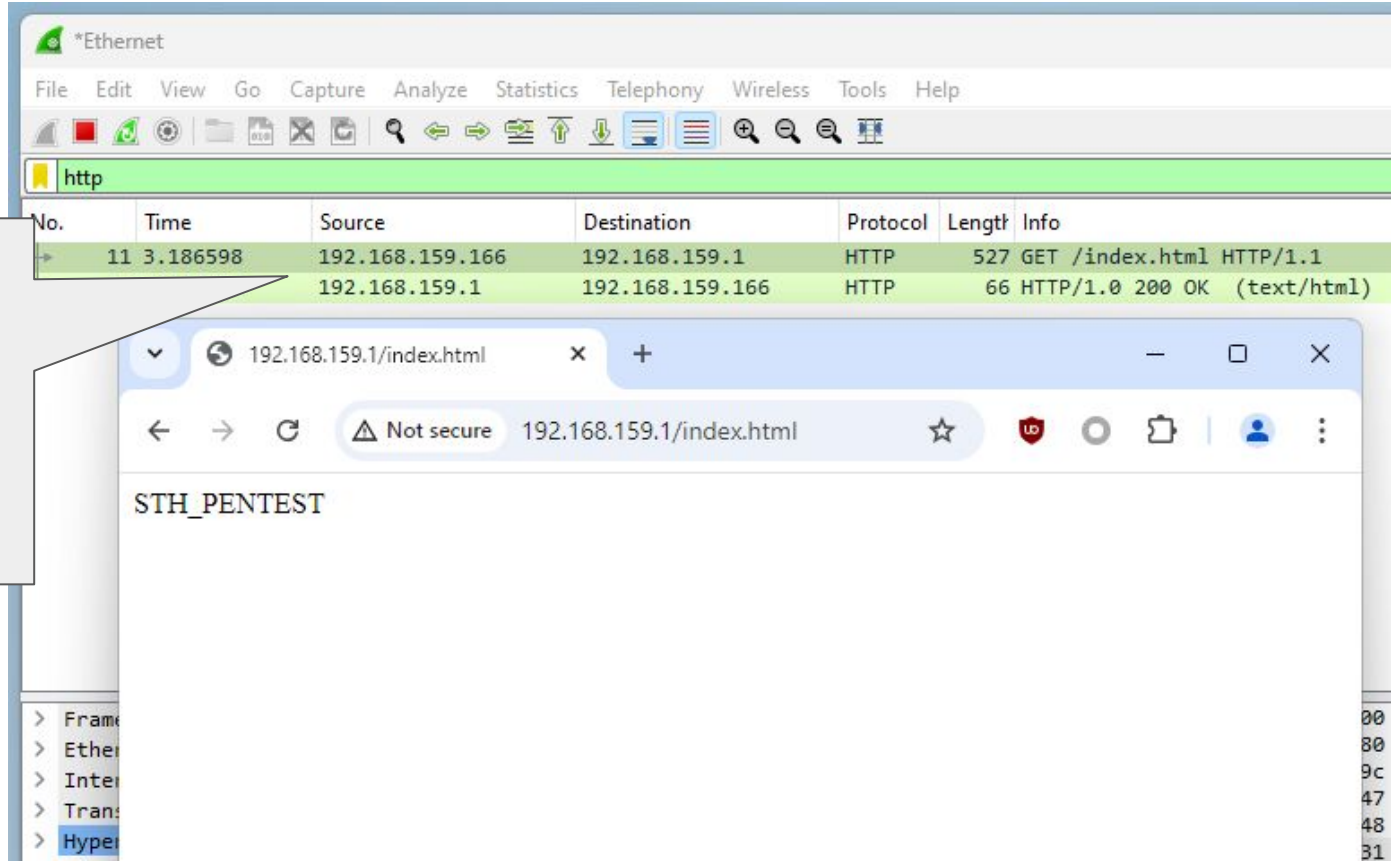
การวิเคราะห์ Network Packet ด้วย Wireshark

คำถาม:
IP อะไรเป็น
ผู้ขอหน้าเว็บ?



การวิเคราะห์ Network Packet ด้วย Wireshark

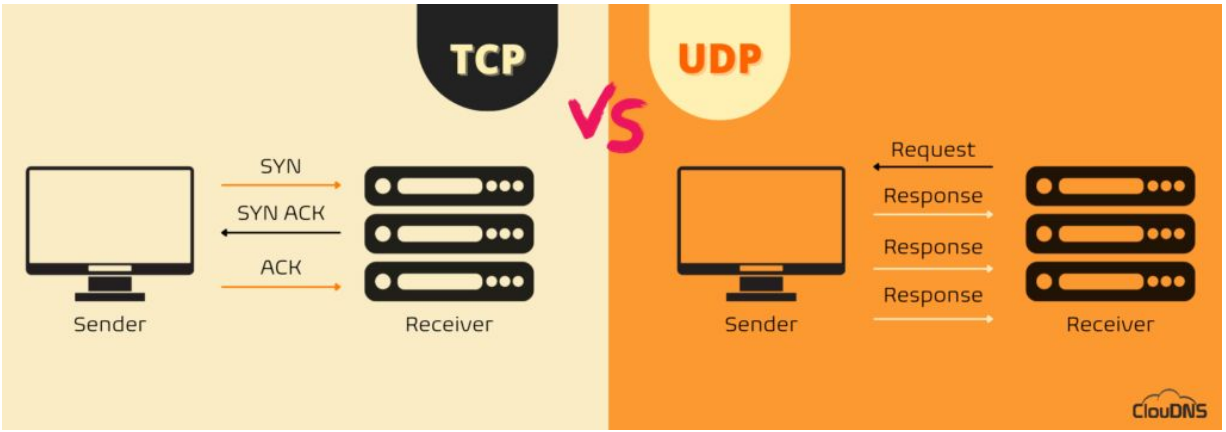
คำถาม:
IP อะไรเป็น
ของผู้ให้บริการเว็บ?



TCP/UDP

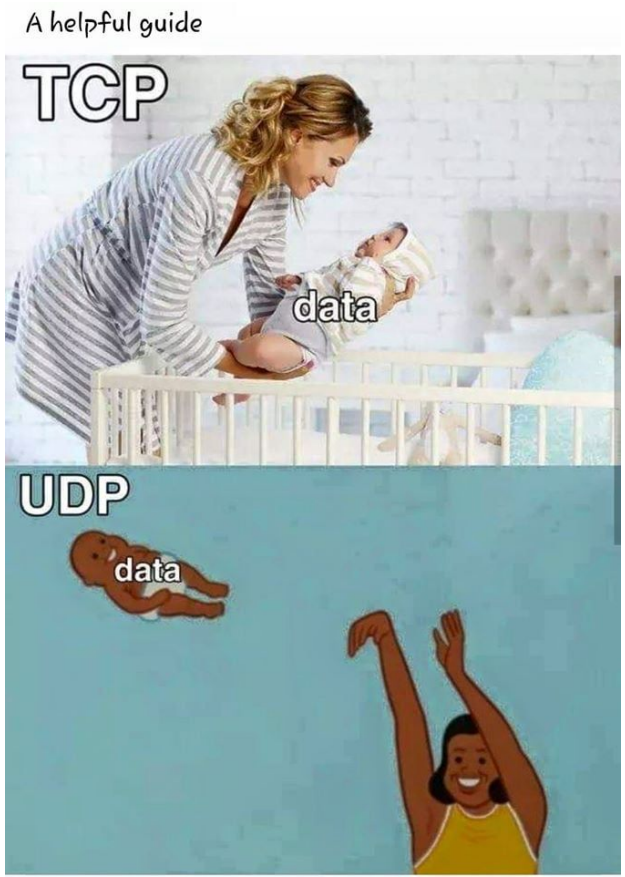
Transmission **C**ontrol **P**rotocol

User **D**atagram **P**rotocol



มีการตรวจสอบ ว่าข้อมูลส่งถึง (TCP 3-Way Handshake)

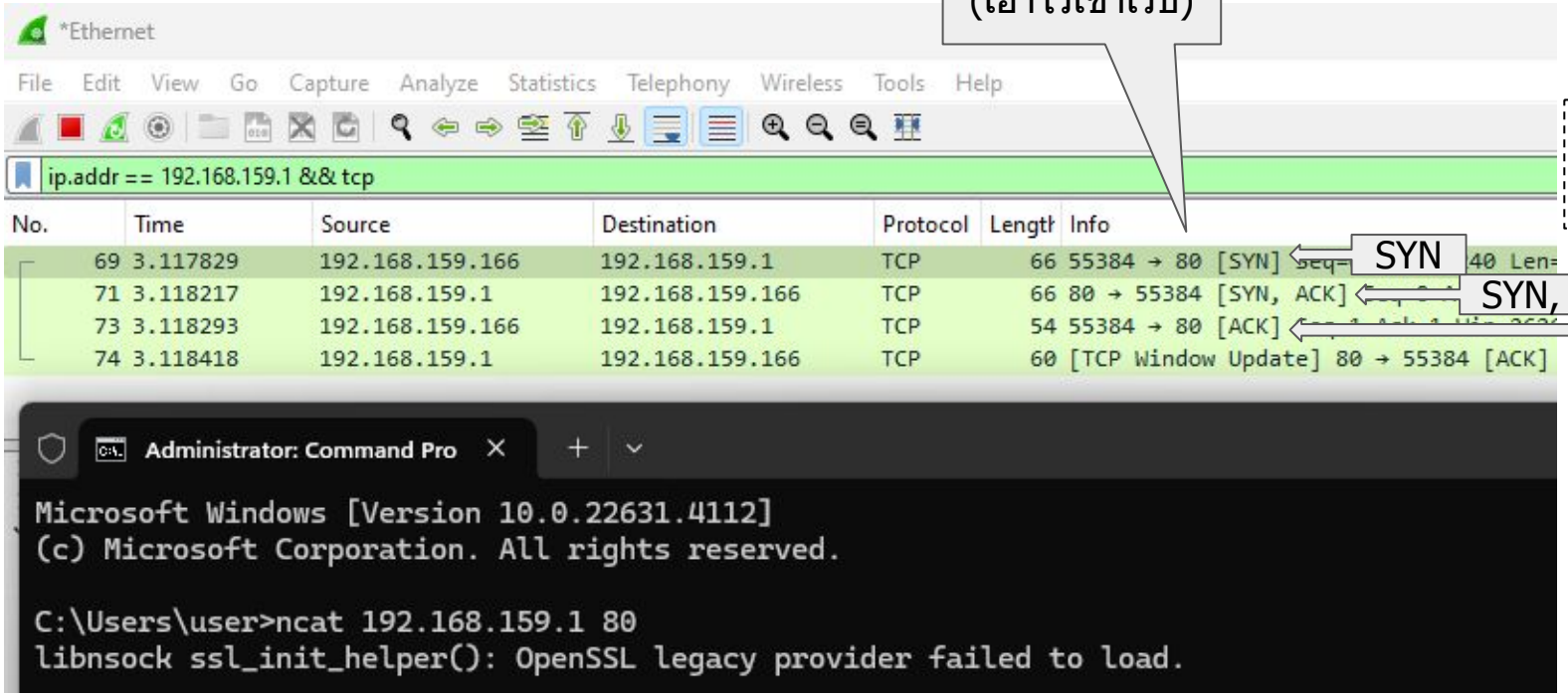
ไม่มีการตรวจสอบ ว่าข้อมูลส่งถึง (ส่ง ๆ ไป)



ที่มา: https://9gag.com/gag/an5d7xV,
https://www.cloudns.net/blog/udp-user-datagram-protocol-explained-in-details/

TCP (Transmission Control Protocol)

HTTP
(เอาไว้เข้าเว็บ)



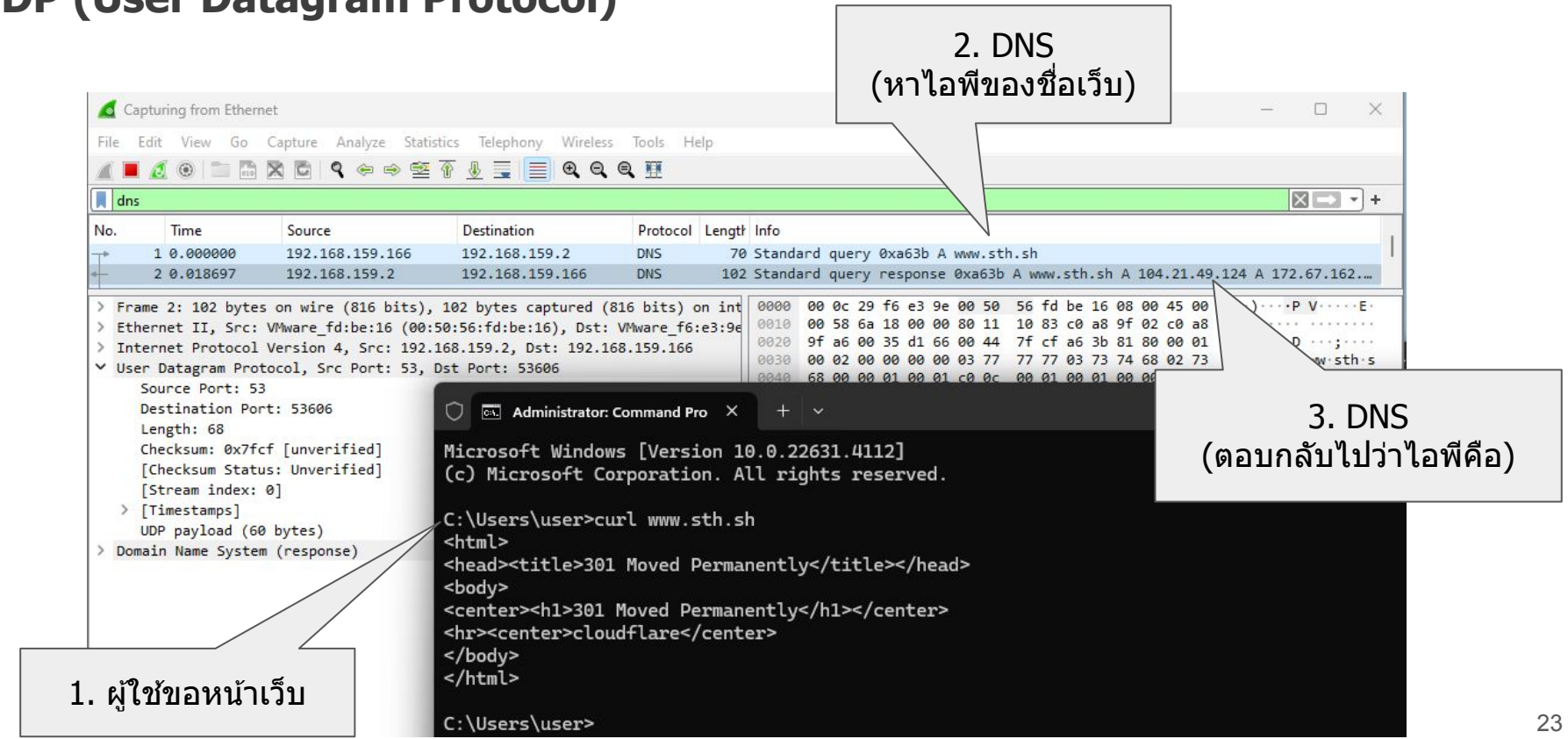
TCP 3-Way Handshake

SYN

SYN, ACK

ACK

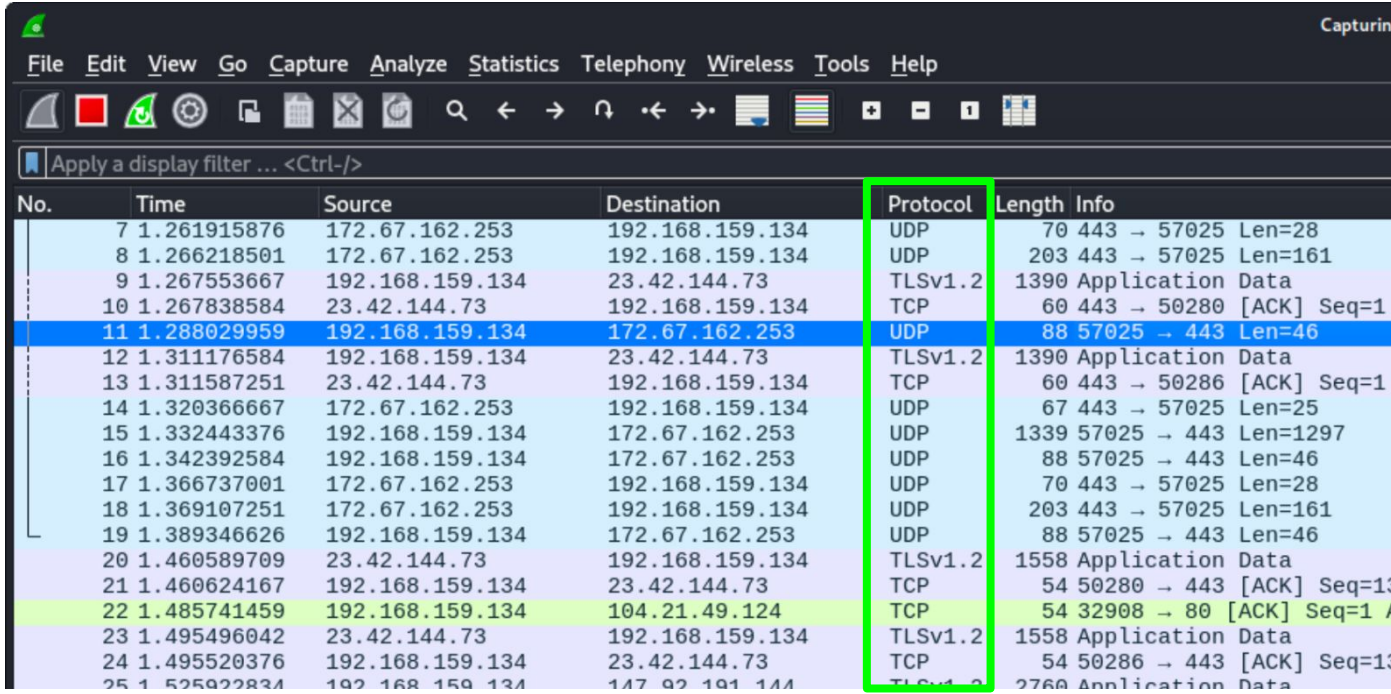
UDP (User Datagram Protocol)



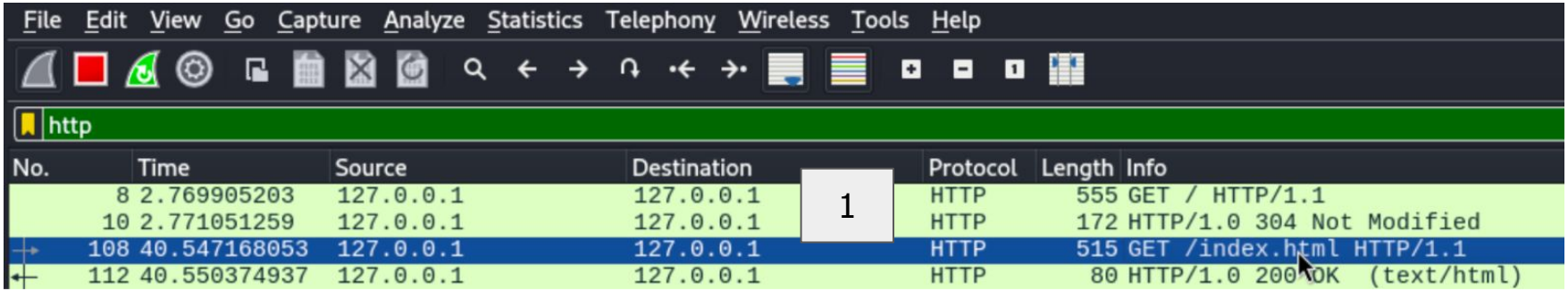
Network Protocol

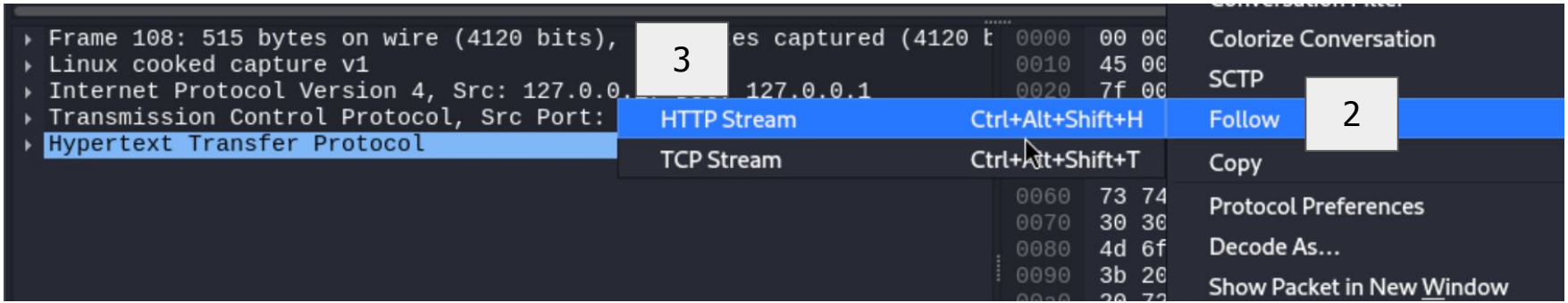
ประเภท TCP (ช้าแต่ชัวร์)
- HTTP (เว็บ)
- FTP (โอนไฟล์)
- SMTP (ส่งอีเมล)

ประเภท UDP (เน้นเร็ว)
- DNS (ชื่อเว็บ)
- NTP (บอกเวลา)
- SNMP (ข้อมูลอุปกรณ์เครือข่าย)



การตรวจสอบเนื้อหาของ Packet ที่เป็น Protocol HTTP

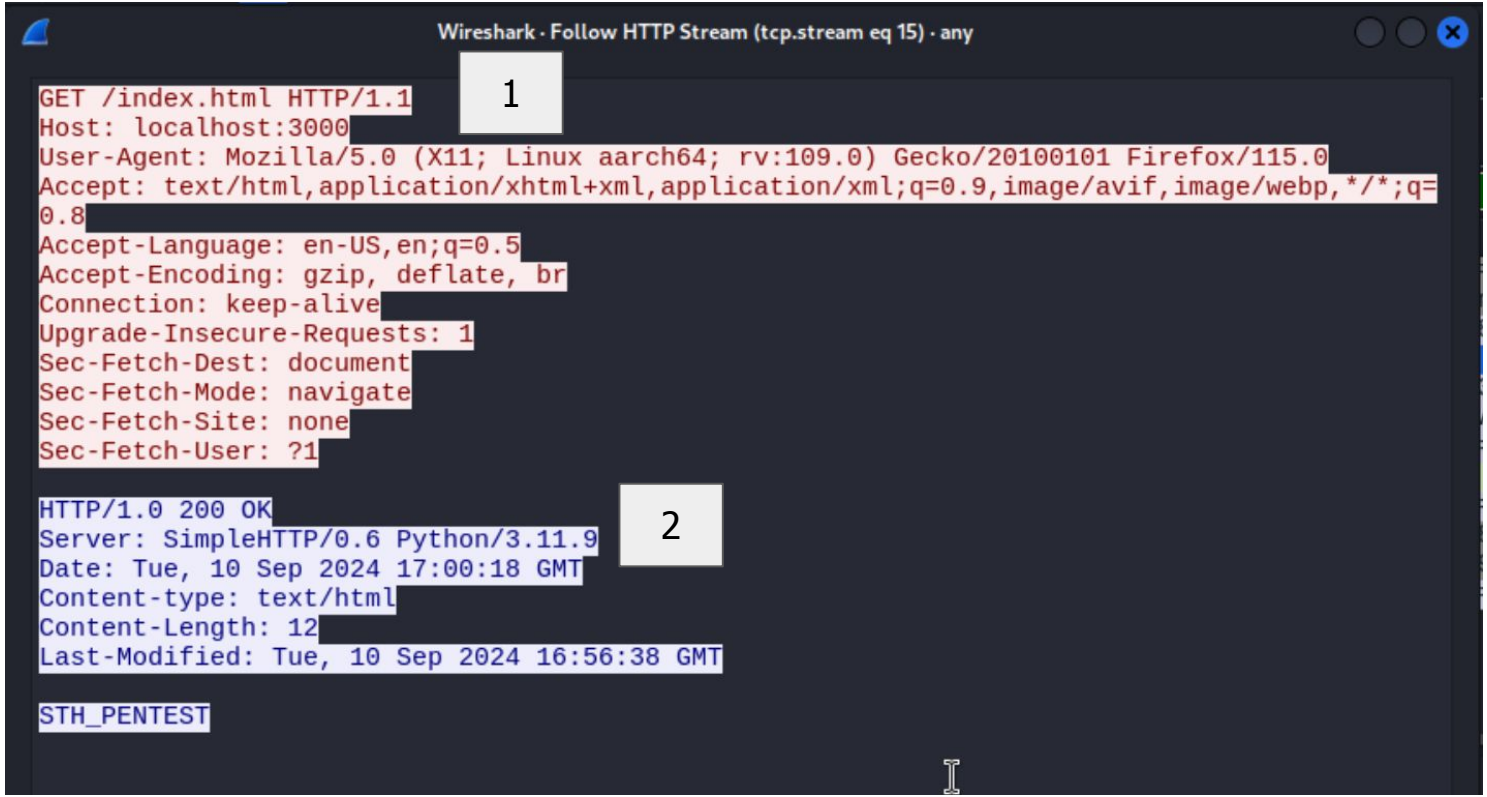




Follow HTTP Stream

ขอหน้าเว็บ

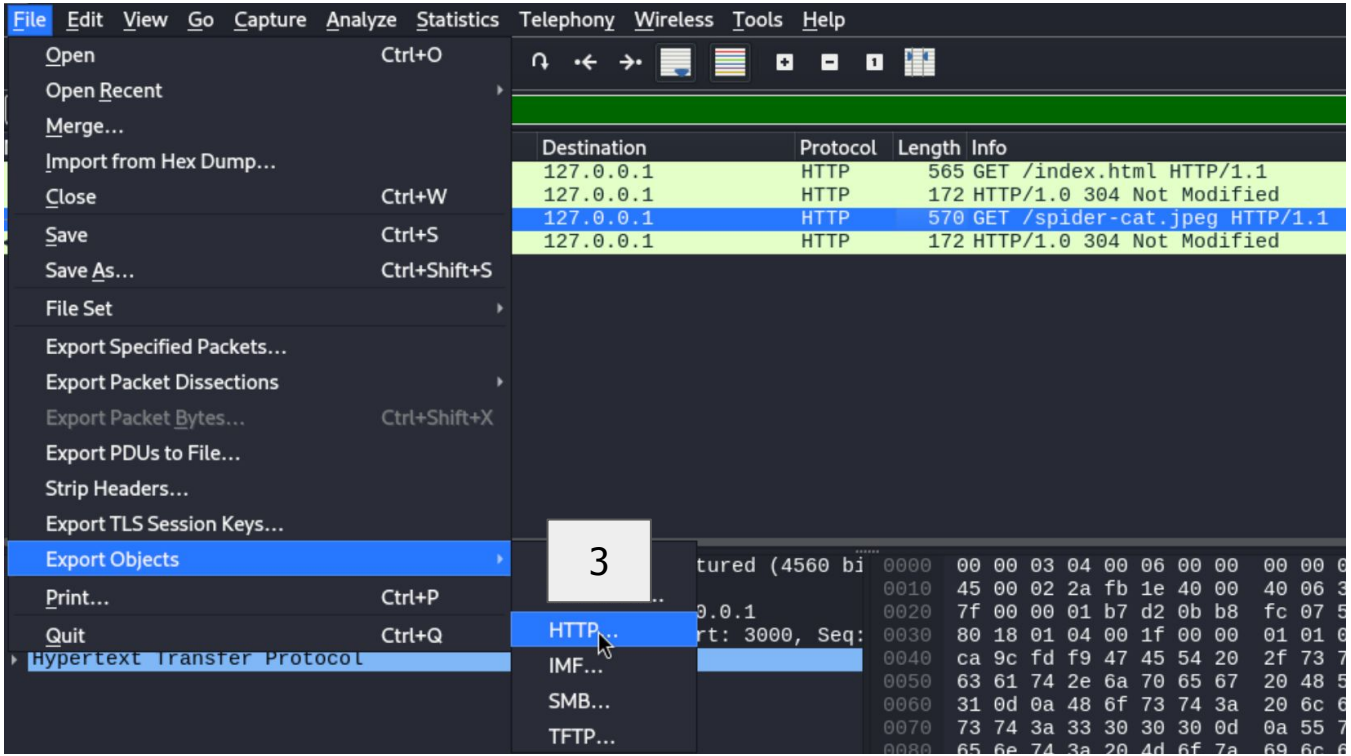
ตอบกลับหน้าเว็บ



Export Objects

1

2

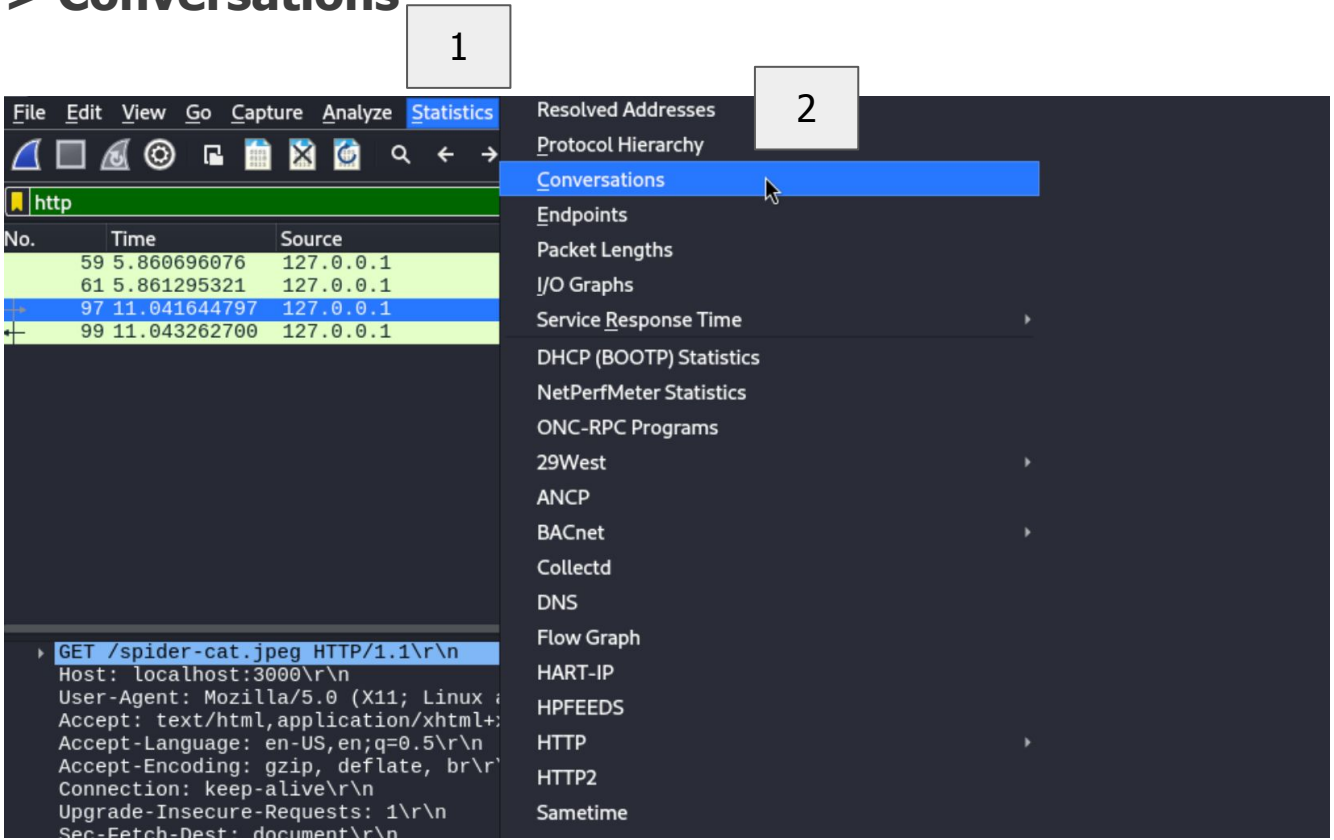


Statistics > Conversations

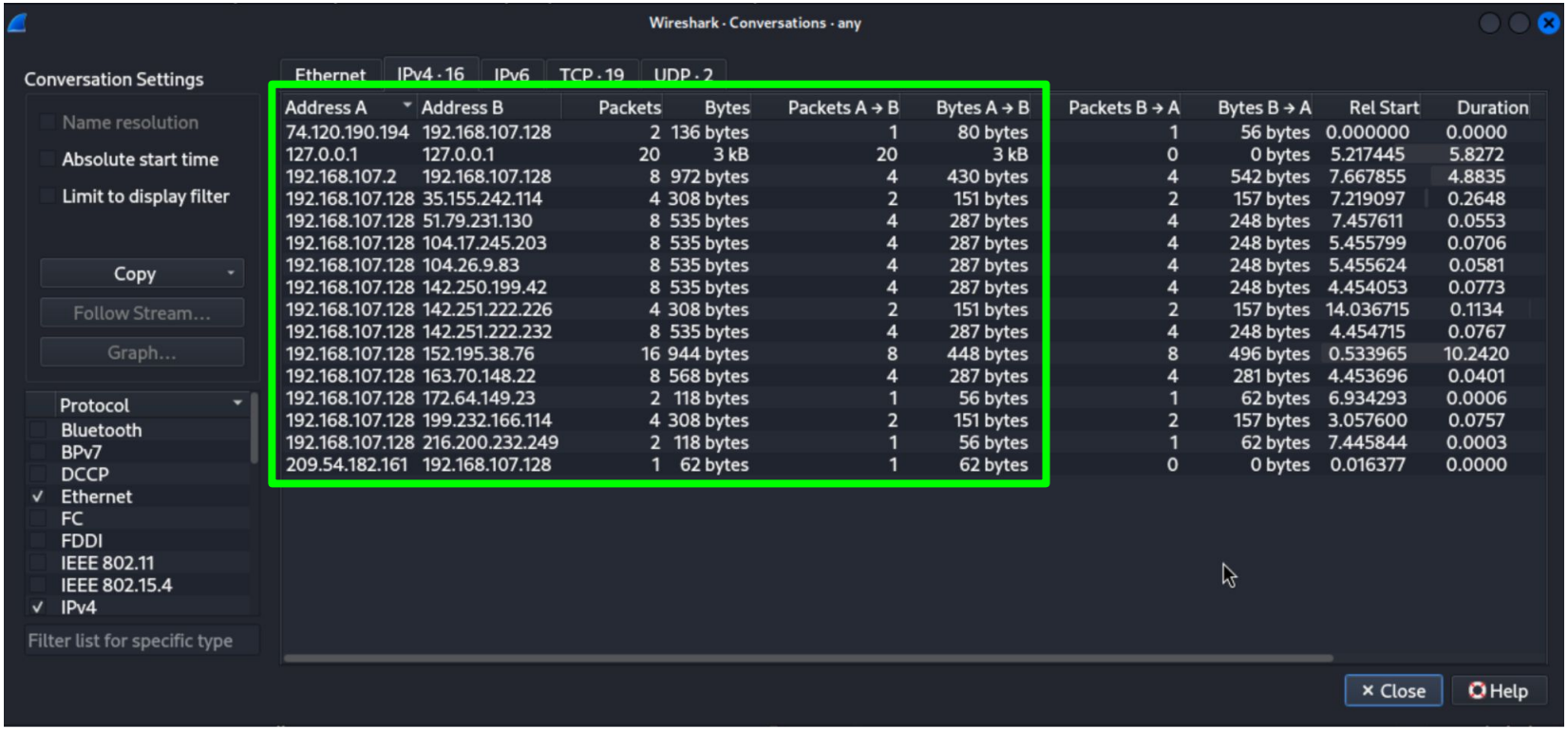
คำถาม:

ถ้าในไฟล์ PCAP มี 1 ล้าน Network Packet
เราจะวิเคราะห์ ภาพรวมเบื้องต้นยังไง?

Statistics > Conversations

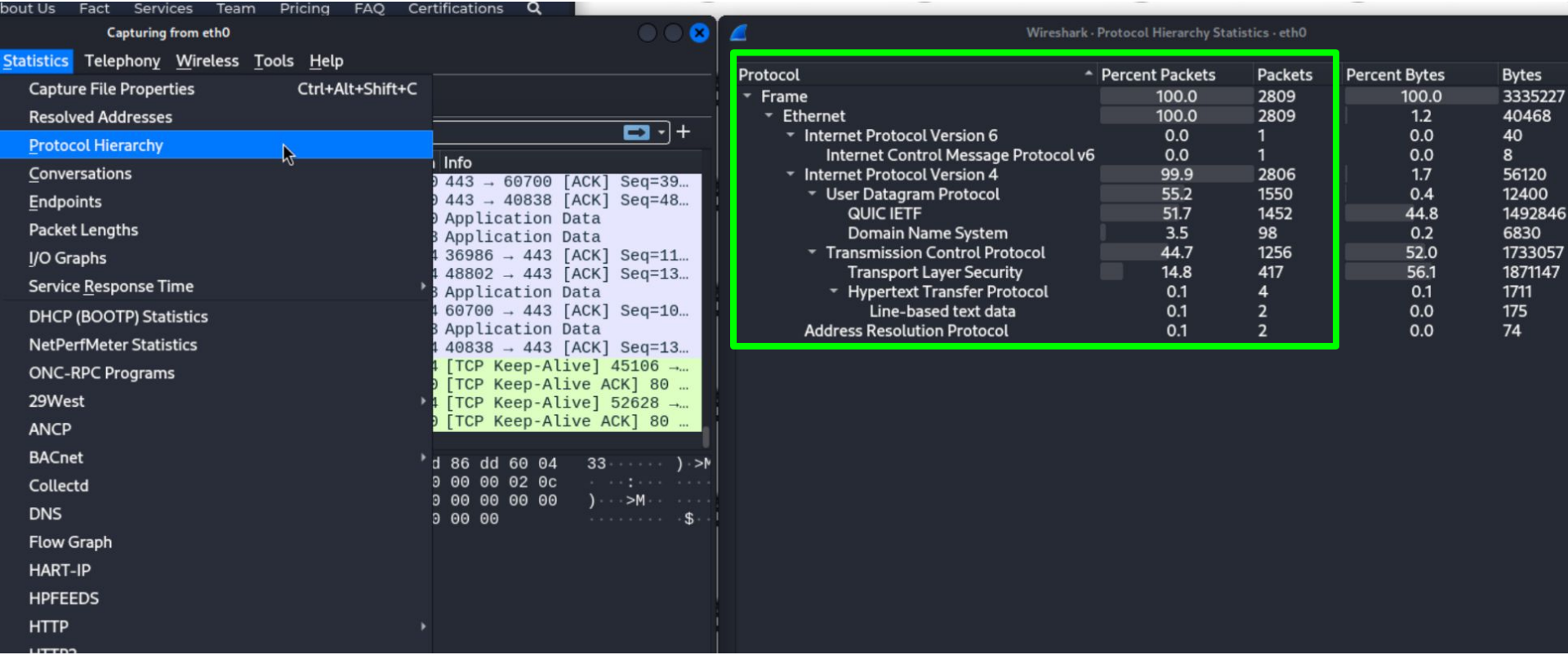


Statistics > Conversations



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
74.120.190.194	192.168.107.128	2	136 bytes	1	80 bytes	1	56 bytes	0.000000	0.0000
127.0.0.1	127.0.0.1	20	3 kB	20	3 kB	0	0 bytes	5.217445	5.8272
192.168.107.2	192.168.107.128	8	972 bytes	4	430 bytes	4	542 bytes	7.667855	4.8835
192.168.107.128	35.155.242.114	4	308 bytes	2	151 bytes	2	157 bytes	7.219097	0.2648
192.168.107.128	51.79.231.130	8	535 bytes	4	287 bytes	4	248 bytes	7.457611	0.0553
192.168.107.128	104.17.245.203	8	535 bytes	4	287 bytes	4	248 bytes	5.455799	0.0706
192.168.107.128	104.26.9.83	8	535 bytes	4	287 bytes	4	248 bytes	5.455624	0.0581
192.168.107.128	142.250.199.42	8	535 bytes	4	287 bytes	4	248 bytes	4.454053	0.0773
192.168.107.128	142.251.222.226	4	308 bytes	2	151 bytes	2	157 bytes	14.036715	0.1134
192.168.107.128	142.251.222.232	8	535 bytes	4	287 bytes	4	248 bytes	4.454715	0.0767
192.168.107.128	152.195.38.76	16	944 bytes	8	448 bytes	8	496 bytes	0.533965	10.2420
192.168.107.128	163.70.148.22	8	568 bytes	4	287 bytes	4	281 bytes	4.453696	0.0401
192.168.107.128	172.64.149.23	2	118 bytes	1	56 bytes	1	62 bytes	6.934293	0.0006
192.168.107.128	199.232.166.114	4	308 bytes	2	151 bytes	2	157 bytes	3.057600	0.0757
192.168.107.128	216.200.232.249	2	118 bytes	1	56 bytes	1	62 bytes	7.445844	0.0003
209.54.182.161	192.168.107.128	1	62 bytes	1	62 bytes	0	0 bytes	0.016377	0.0000

Statistics > Protocol Hierarchy



Statistics

คำถาม:

ถ้าในไฟล์ PCAP มี 1 ล้าน Network Packet
เราจะวิเคราะห์ ภาพรวมเบื้องต้นยังไง?

คำตอบ:

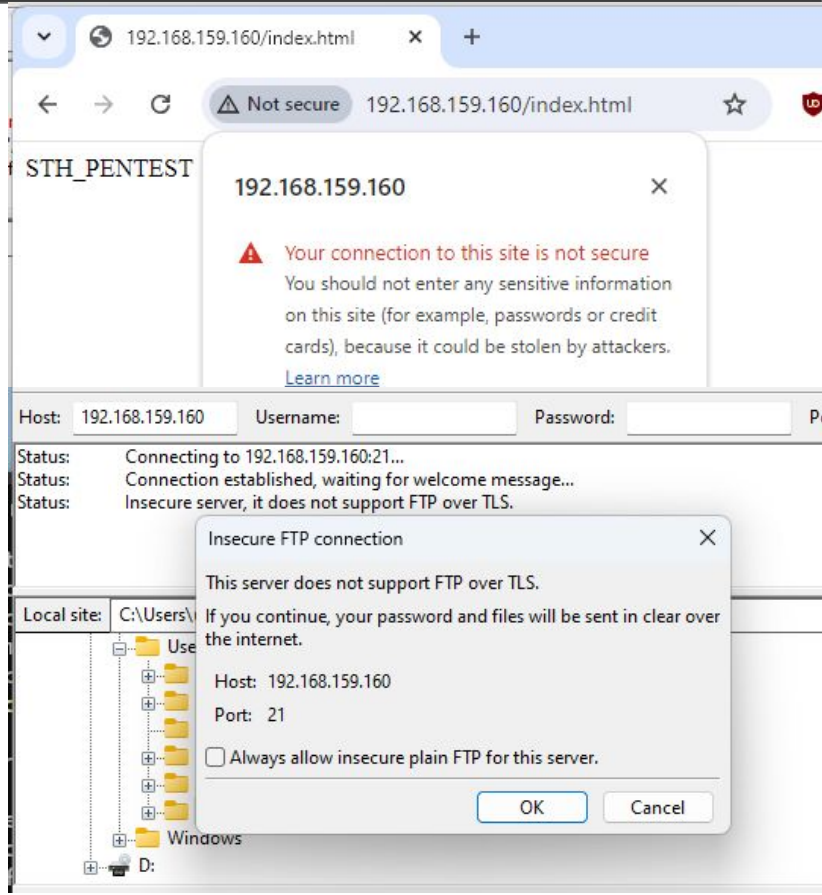
ใช้เมนู Statistics ของ Wireshark ช่วย!

Plaintext Protocol - ส่งข้อมูลที่ไม่เข้ารหัส

ตัวอย่าง Plaintext Protocol เช่น

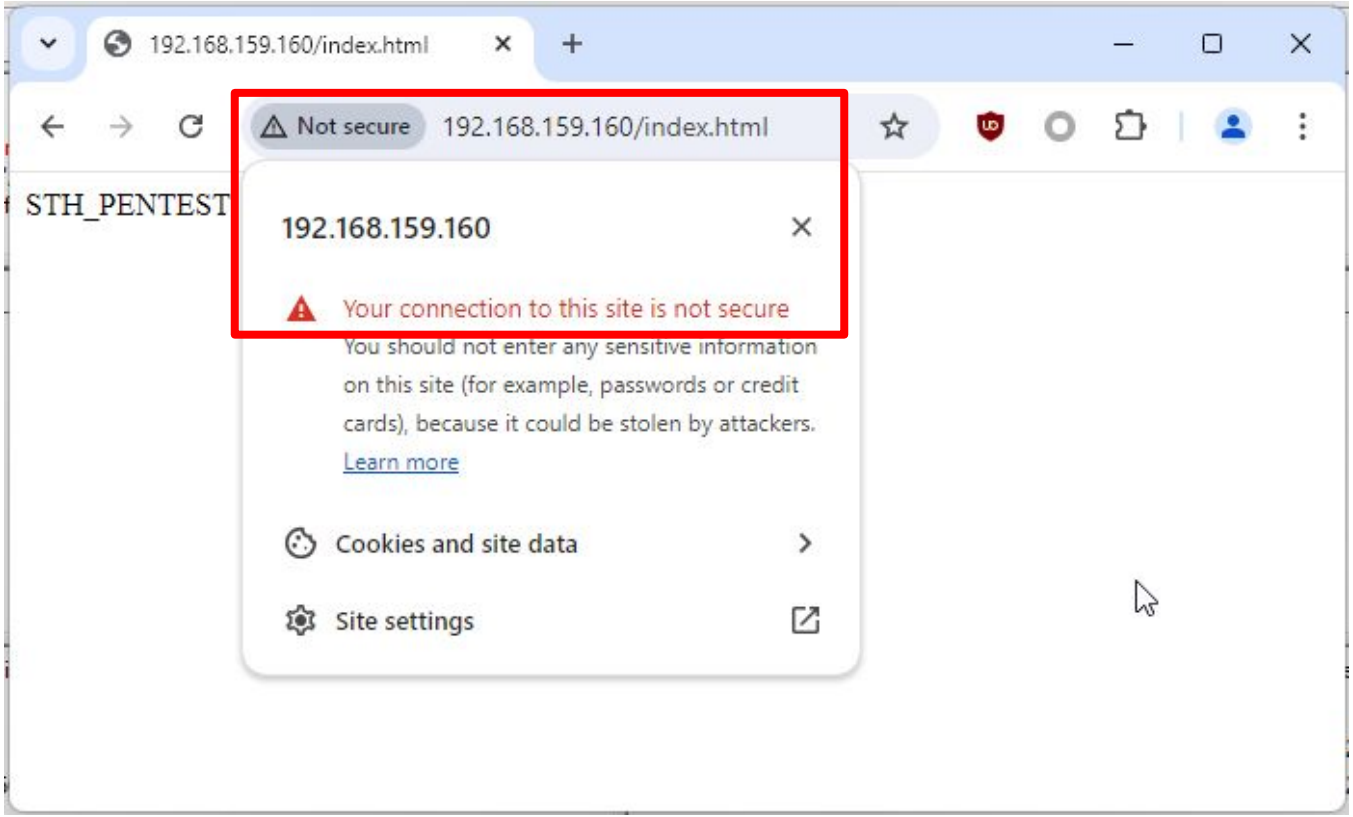
- **HTTP** (Hypertext Transfer Protocol)
  ใช้ส่งข้อมูลการเข้าใช้งานเว็บ
- **FTP** (File Transfer Protocol)
  ใช้รับ-ส่งข้อมูล การโอนไฟล์
- **Telnet**
  ใช้เชื่อมต่อไปสั่งการที่คอมพิวเตอร์เครื่องอื่น
- **SMTP** (Simple Mail Transfer Protocol)
  ใช้ในการส่งอีเมล

ส่งข้อมูลไม่เข้ารหัส
==
ไม่ปลอดภัย
เพราะอาจโดนดักอ่านได้ !

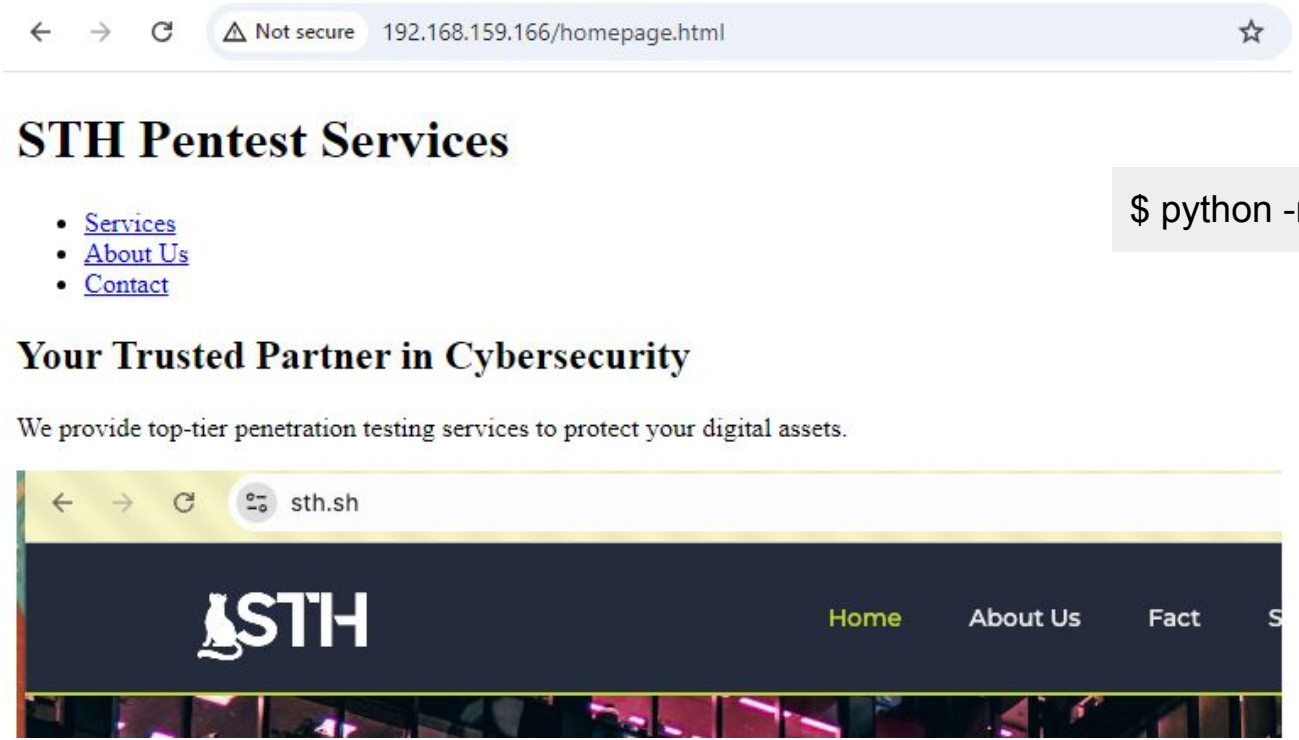


ลองวิเคราะห์ข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

HTTP Protocol



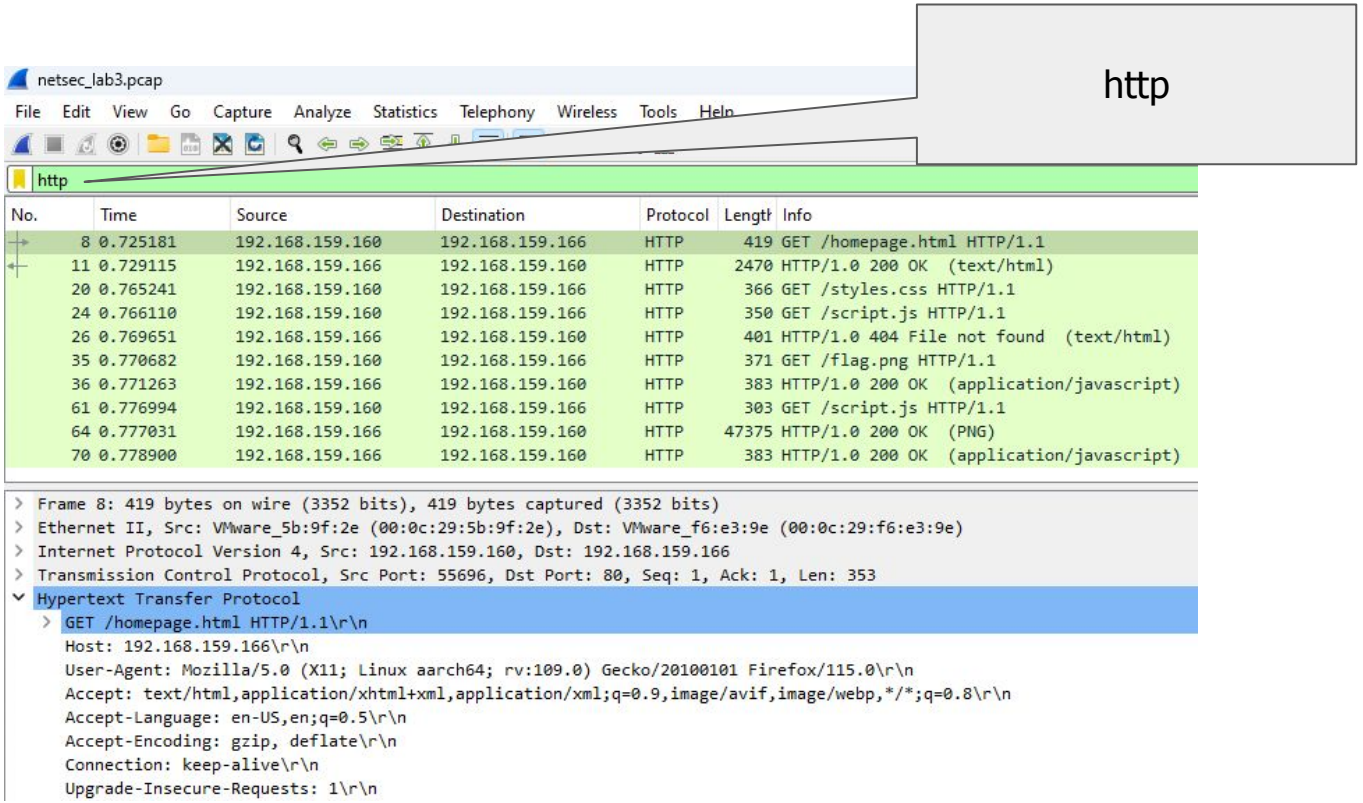
LAB ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark



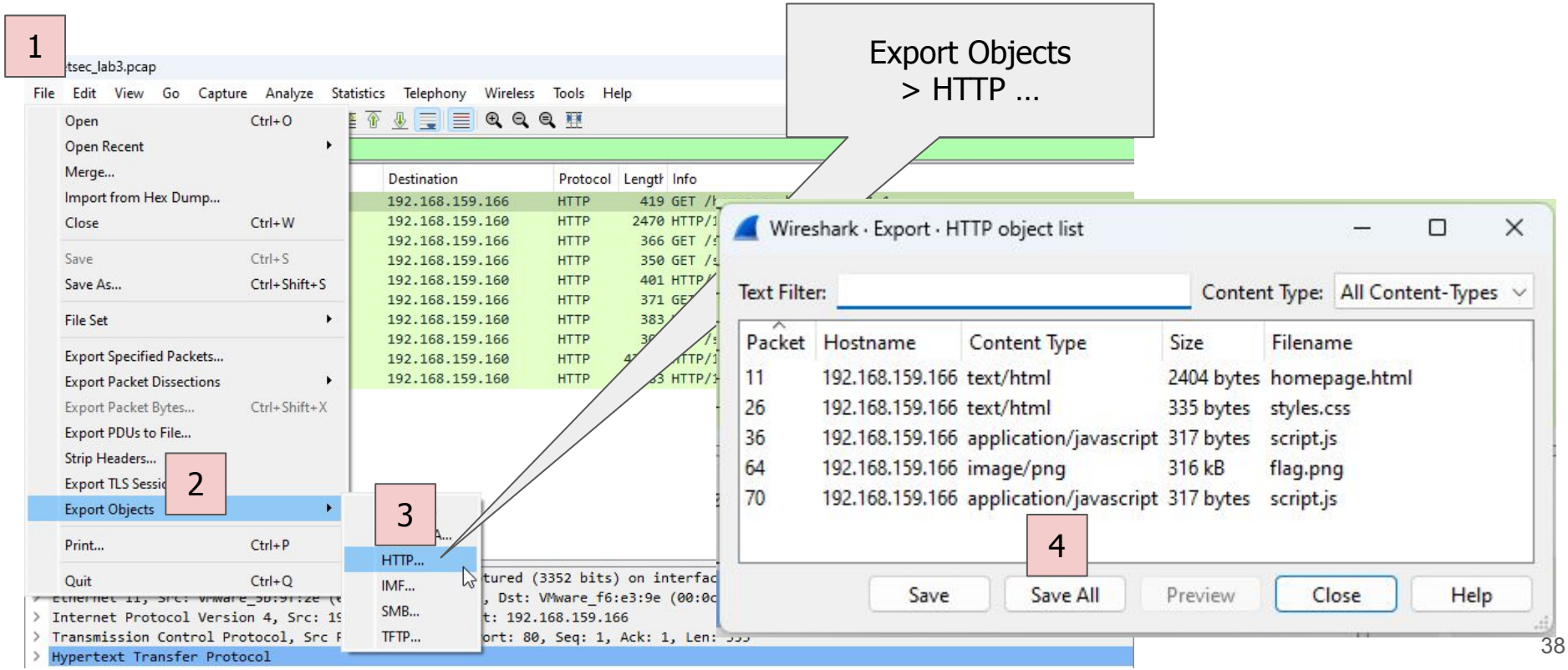

```
$ python -m http.server 80
```

ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

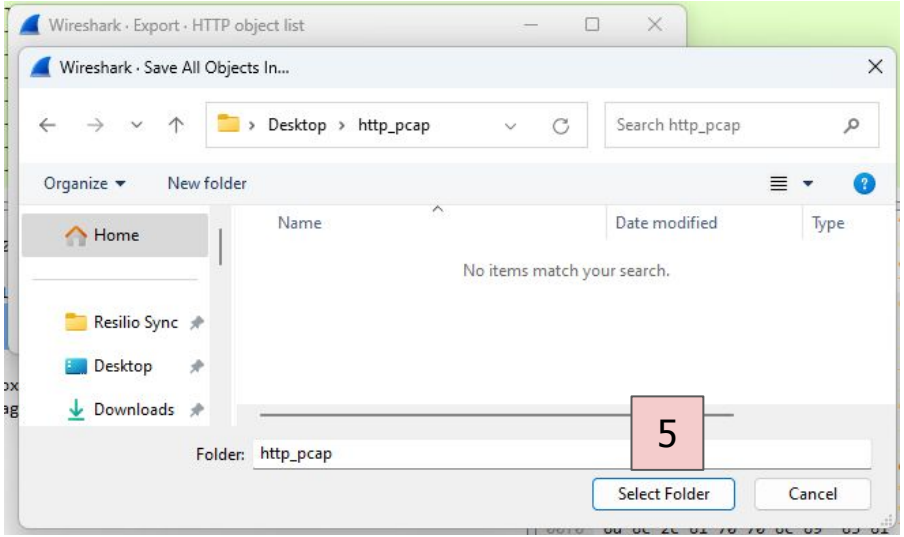
Filter

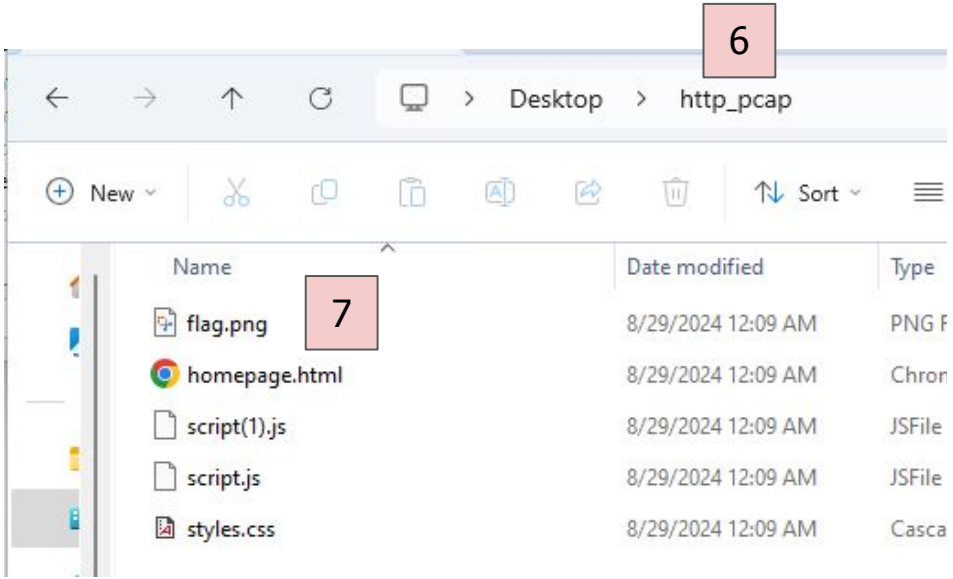


ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark



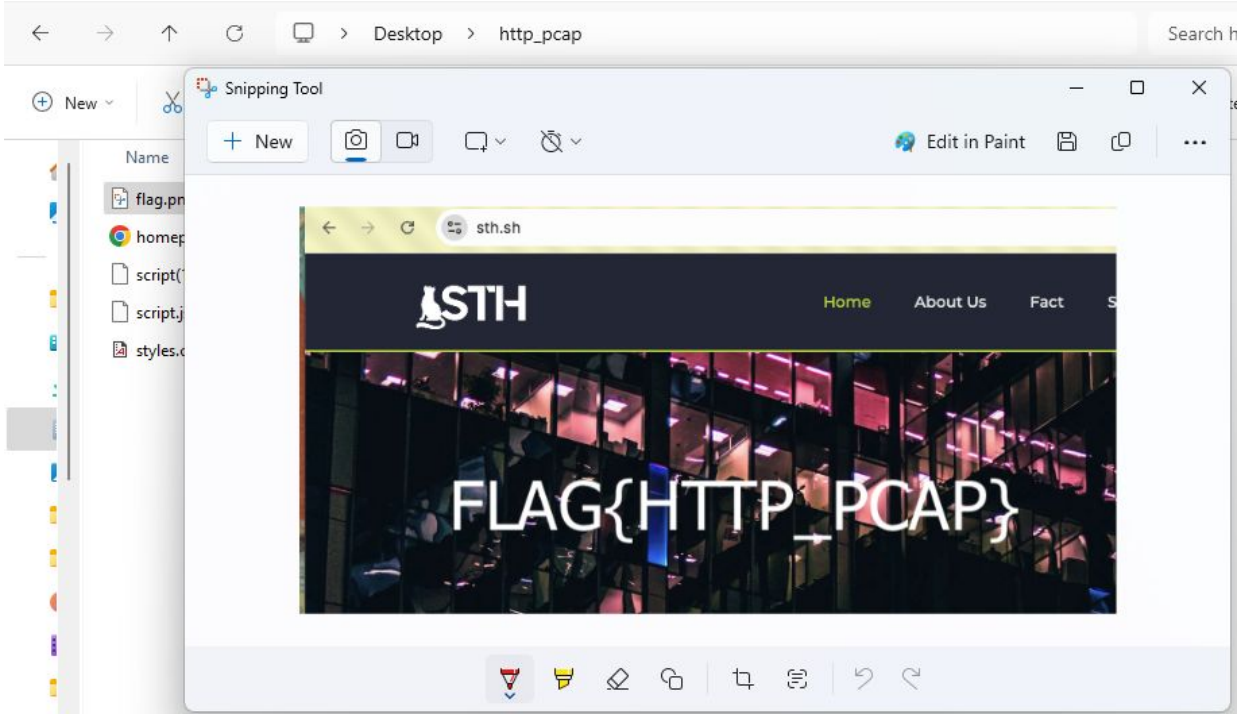
ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark



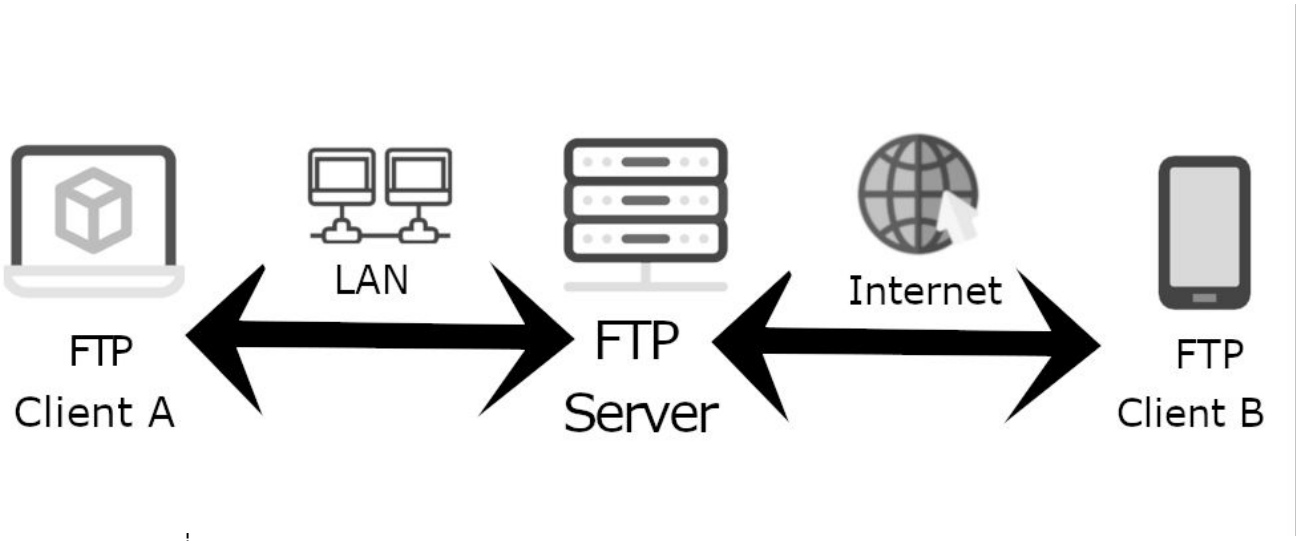


ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

8

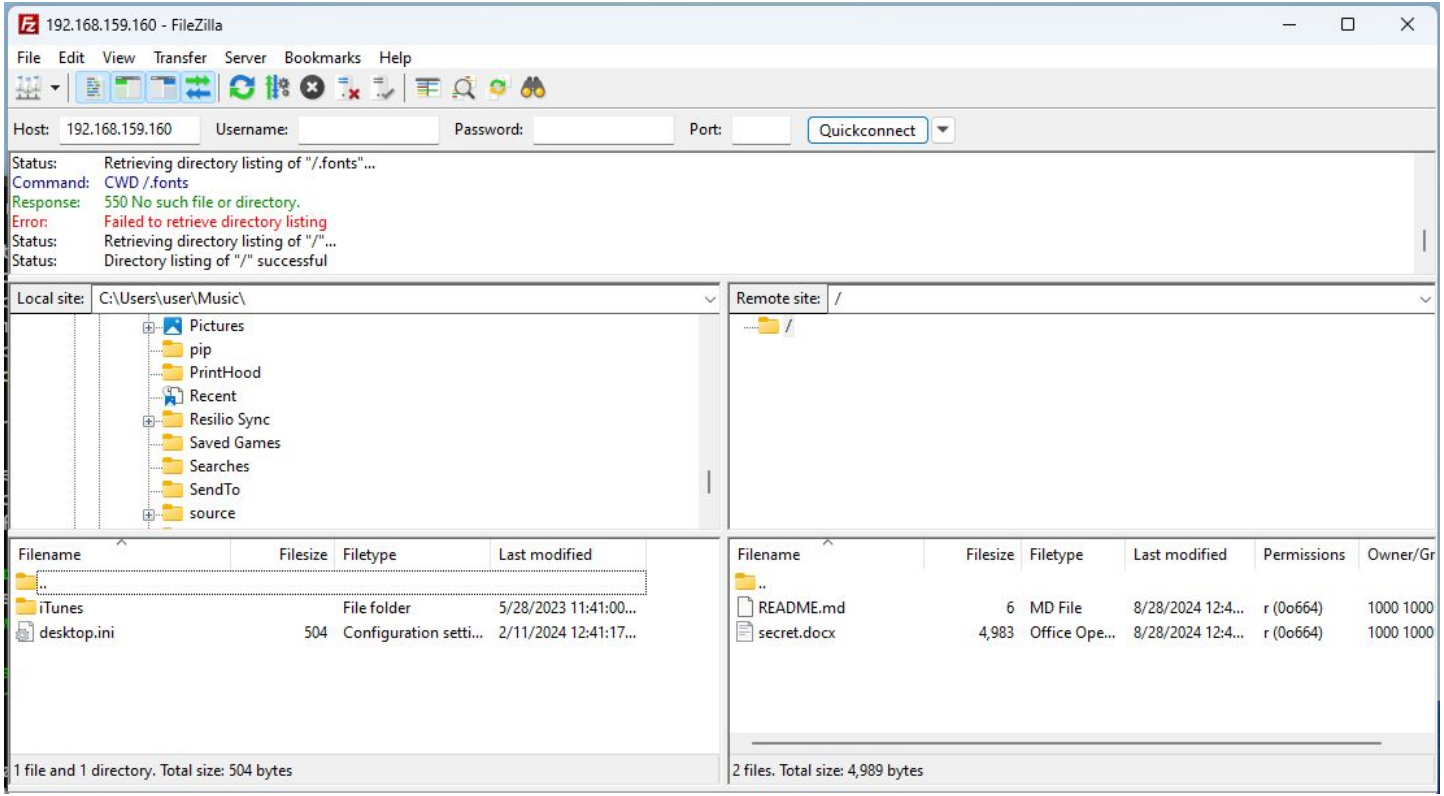


FTP Protocol

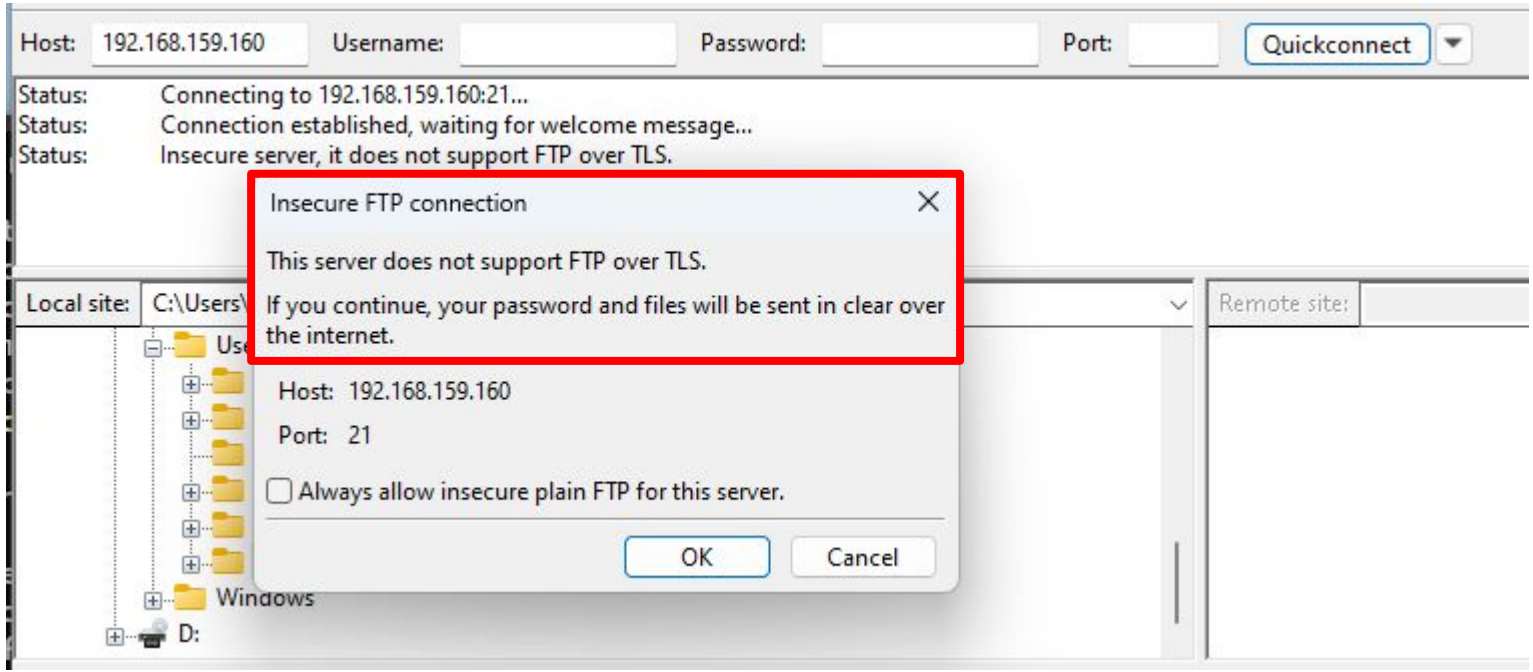


ที่มา: https://www.wftpserver.com/blog/what-is-an-ftp-server-used-for/

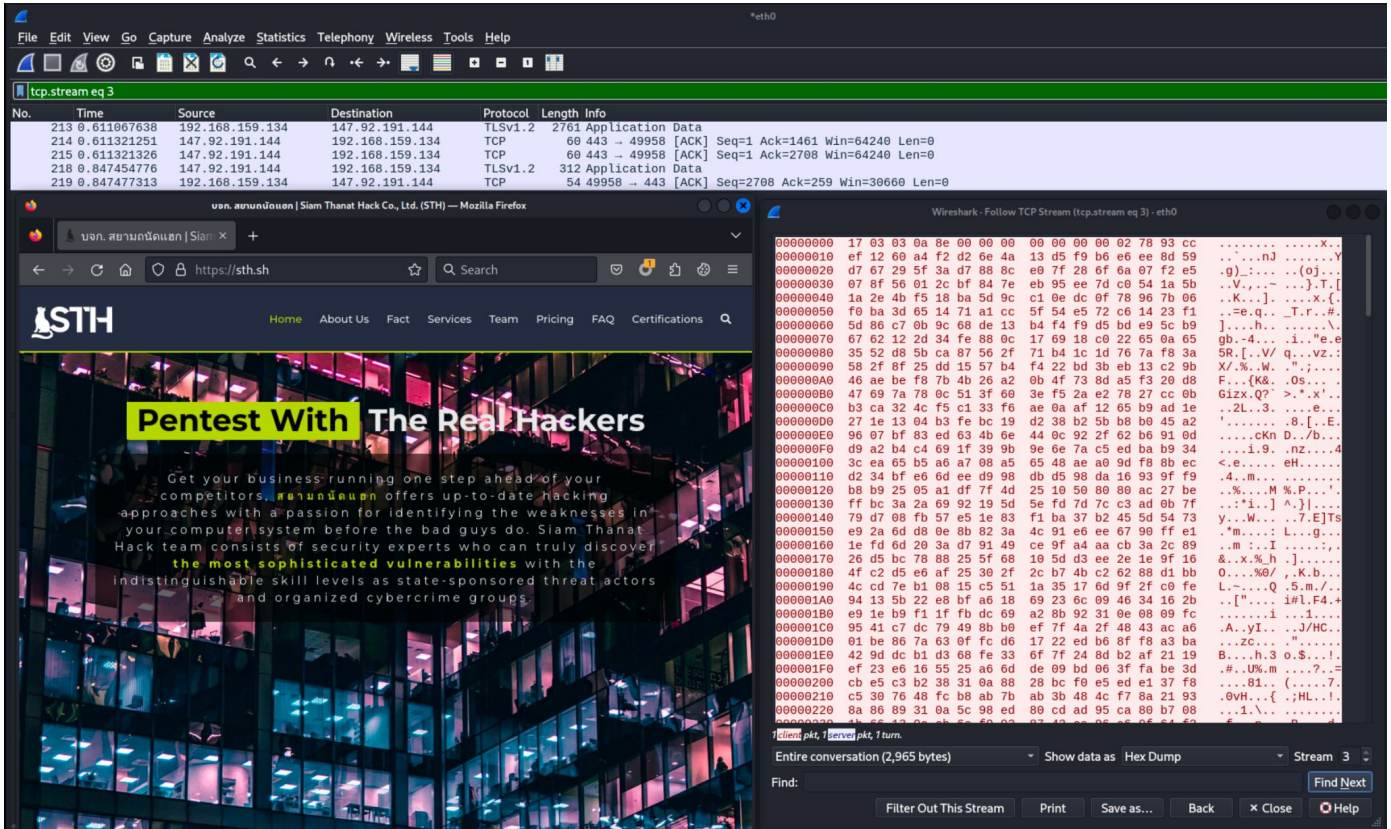
FTP Protocol - FTP Client



FTP Protocol - FTP Client



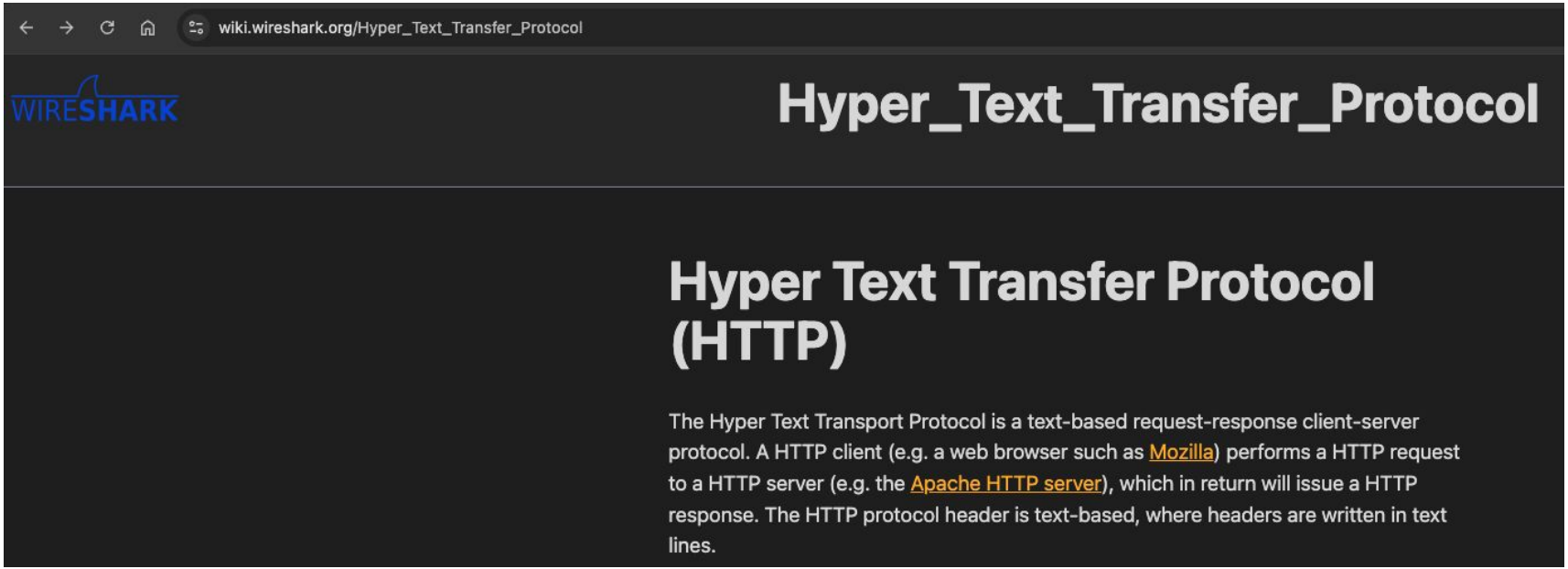
Protocol HTTPS ข้อมูลมีการเข้ารหัสด้วย TLS



ข้อมูลสามารถถูกดักและอ่านได้ แต่ถูกเข้ารหัสเอาไว้

ศึกษาเพิ่มเติม

- https://www.wireshark.org/docs
- https://wiki.wireshark.org/



What is Nmap?

Nmap หรือ **Network Mapper** เป็นเครื่องมือแบบ Command Line และเป็น Software Open-source ที่ใช้ในการสแกนที่อยู่ IP และพอร์ตในเครือข่าย

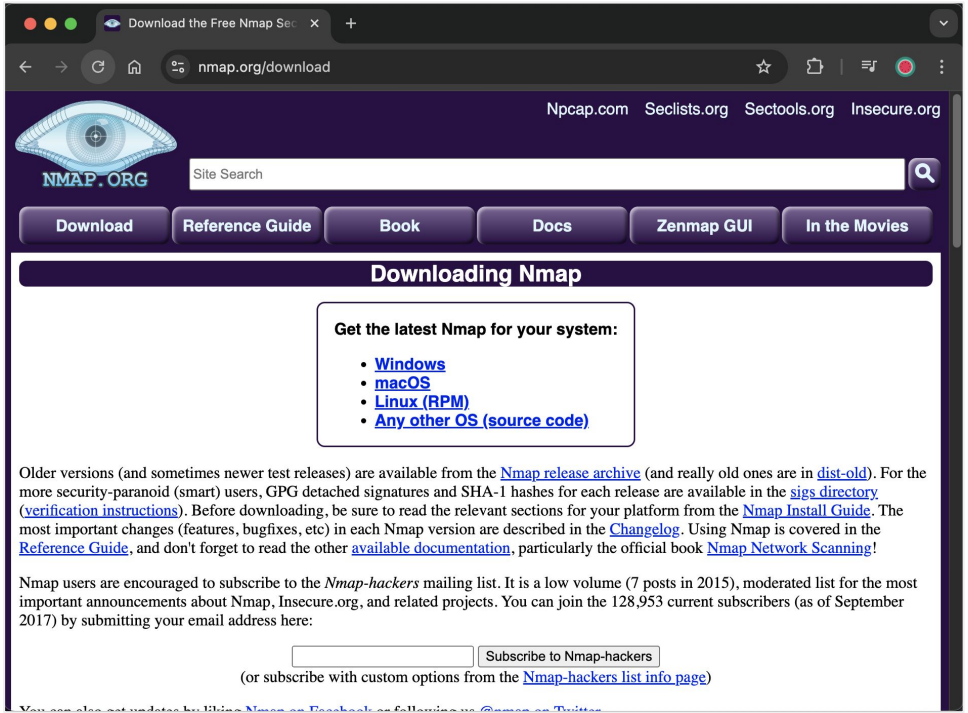

```
[redacted]:~/Desktop$ sudo nmap -sS 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:02 CST
Nmap scan report for 192.168.0.239
Host is up (0.000081s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:9F:F3:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
[redacted]:~/Desktop$
```

Download

สามารถดาวน์โหลดได้ที่:
https://nmap.org/download

ติดตั้งแบบ Command-Line

```
phoenixnap@phoenixnap-VirtualBox:~$ sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas3 liblinear3
Suggested packages:
  liblinear-tools liblinear-dev ndiff
The following NEW packages will be installed:
  libblas3 liblinear3 nmap
0 upgraded, 3 newly installed, 0 to remove and 254 not upgraded.
Need to get 5,353 kB of archives.
After this operation, 24.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```



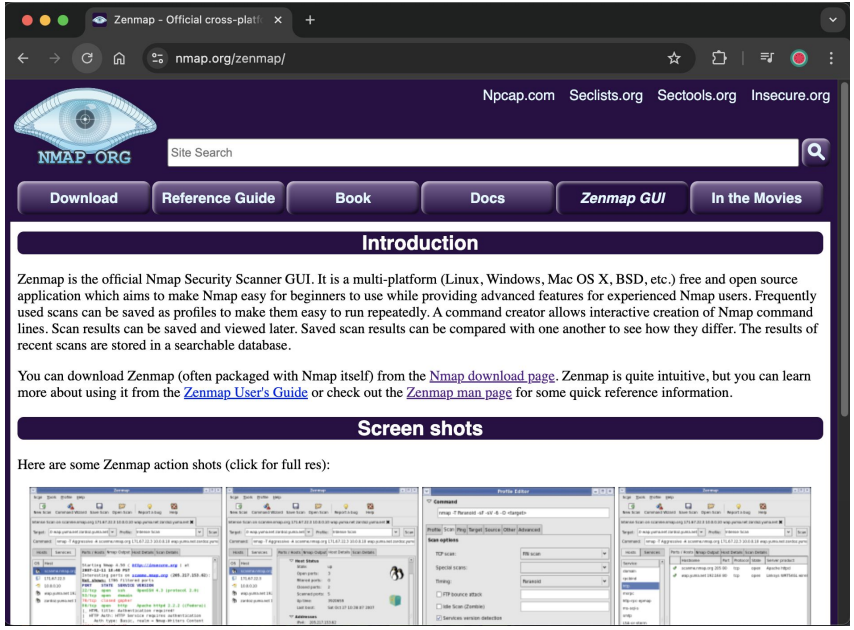
ตัวอย่างการใช้ nmap

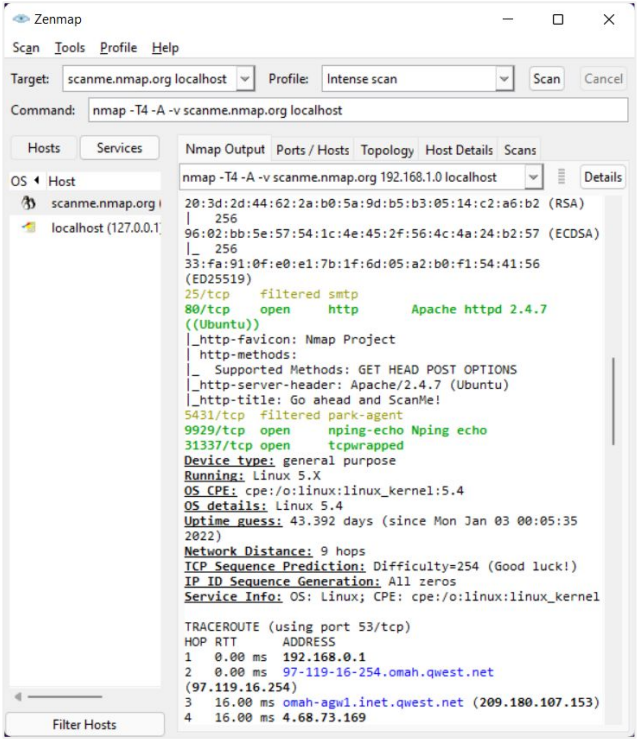
```
$ nmap scanme.p7z.pw
```

```
admin@ip-172-26-0-73:~$ nmap scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
admin@ip-172-26-0-73:~$
```

Zenmap สำหรับ Windows

สามารถดาวน์โหลดได้ที่:
https://nmap.org/download.html#windows





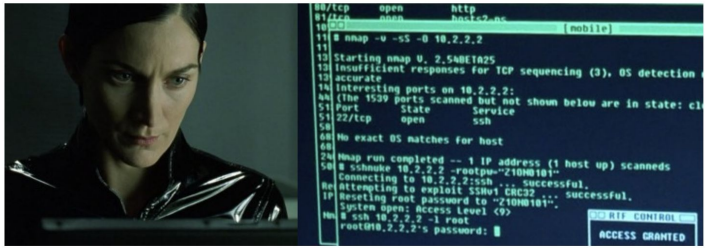
Nmap In The Movies

Matrix Reloaded

While Nmap had been used in some previous obscure movies, it was The Matrix Reloaded (Wikipedia, IMDB, Amazon) which really turned Nmap into a movie star!

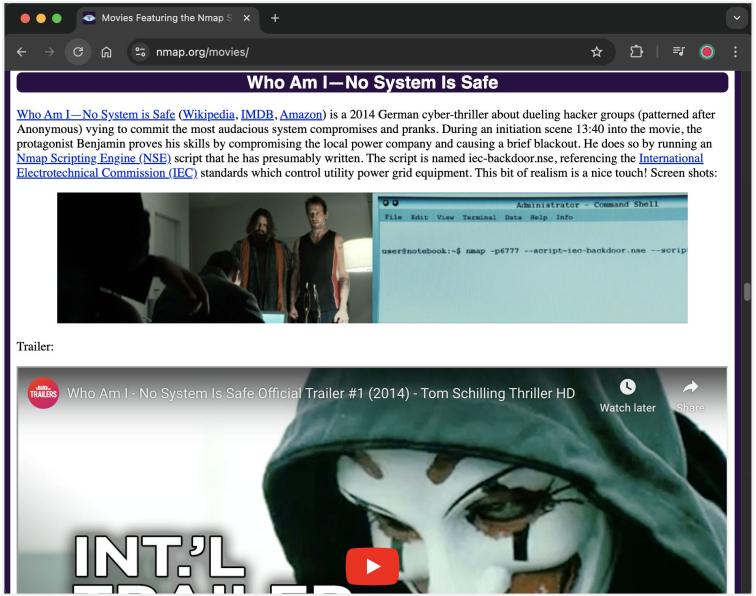
We have all seen many movies like Hackers which pass off ridiculous 3D animated eye-candy scenes as hacking. So Fyodor was shocked to find that Trinity does it properly in The Matrix Reloaded. Needing to hack the city power grid, she whips out Nmap version 2.54BETA25, uses it to find a vulnerable SSH server, and then proceeds to exploit it using the SSH1 CRC32 exploit from 2001. Shame on the city for being vulnerable (timing notes).

A video of the exploit is available on YouTube or as matrix-nmap.mp4. Click on the following thumbnails for higher resolution or view more pictures here.



Updates:

- News articles about the Matrix cameo: BBC, Slashdot, SecurityFocus, Silicon.Com
- JWZ has added this cracking scene as an XScreenSaver 4.10 Easter Egg - run 'xmatrix -small -crack'.
- Several people have submitted matrix-themed banners to the propaganda gallery. Feel free to use any of these to link to Insecure.org -



Nmap In The Movies (Snowden)

Movies Featuring the Nmap S

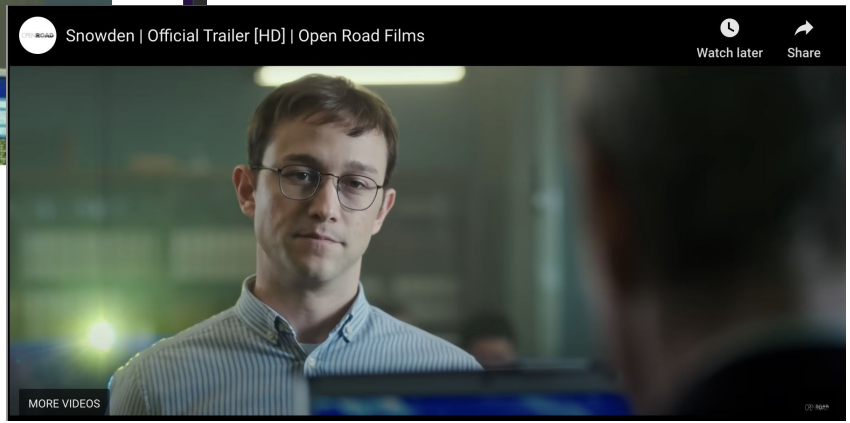
nmap.org/movies/

Snowden

Oliver Stone's 2016 Snowden film (Wikipedia, IMDB, Amazon) dramatizes Edward Snowden's massive leak of classified documents revealing NSA widespread surveillance of U.S. citizens. In one early scene, Snowden is given a network security challenge at a CIA training class which is expected to take 5 to 8 hours. But with the help Nmap and a custom Nmap NSE script named ptest.nse, Snowden stuns the professor by completing everything in 38 minutes! Nmap's distinct tabular output is visible on other students' screens too, though we may have to wait for the 4K resolution film release to read the exact text. Here are a couple screen shots from the Nmap scenes:

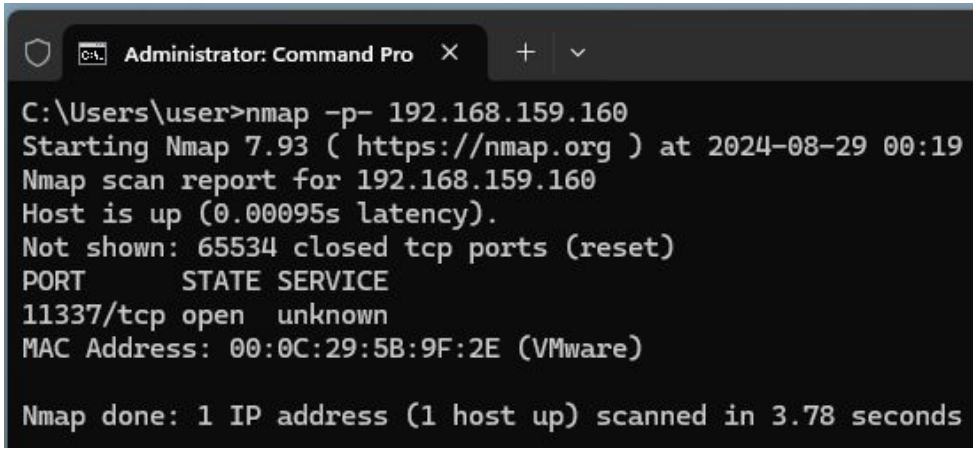
And here is the whole trailer (with Nmap glimpse at 34 seconds in):

https://youtu.be/QlSAiI3xMh4

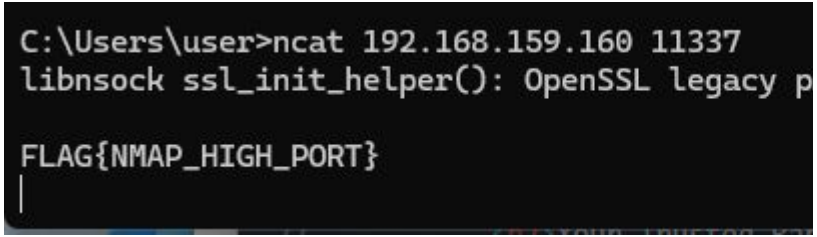


Lab 3 - Nmap Scan High Port

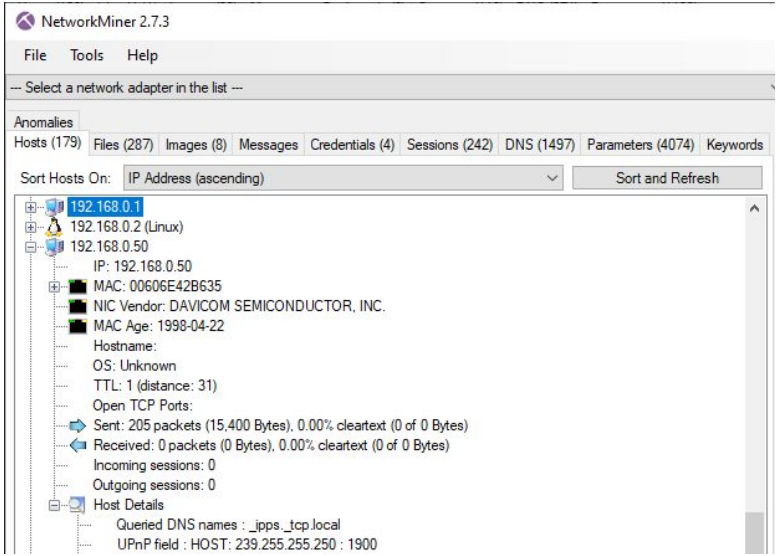
C:\> nmap -p- scanme.p7z.pw

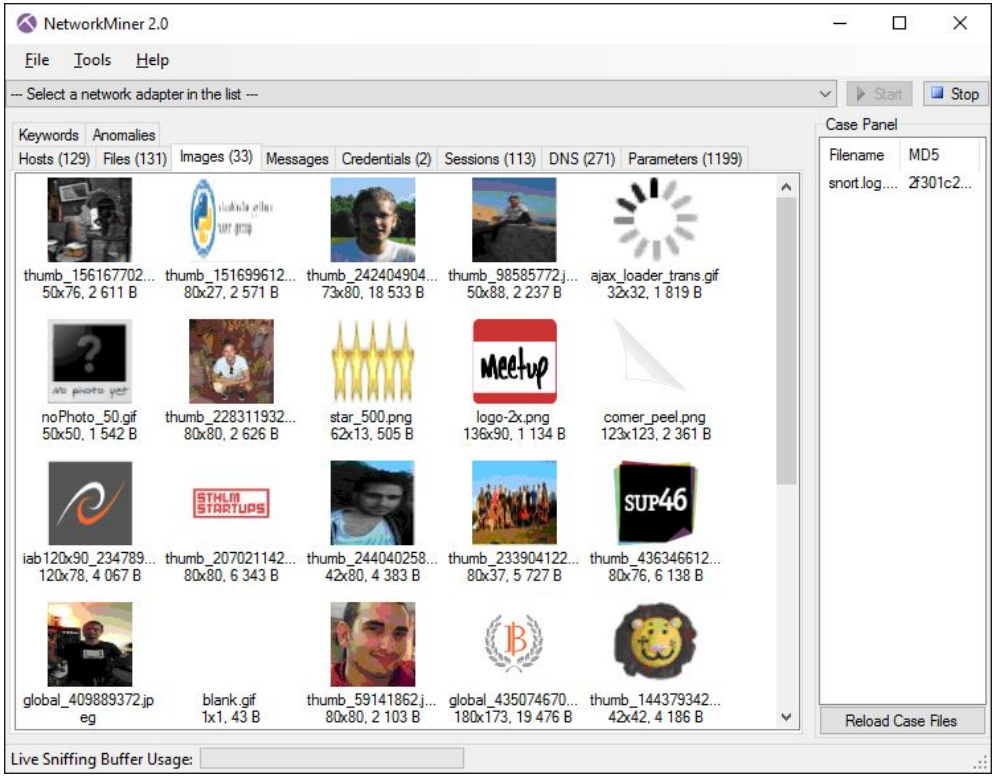


C:\> ncat scanme.p7z.pw 11337



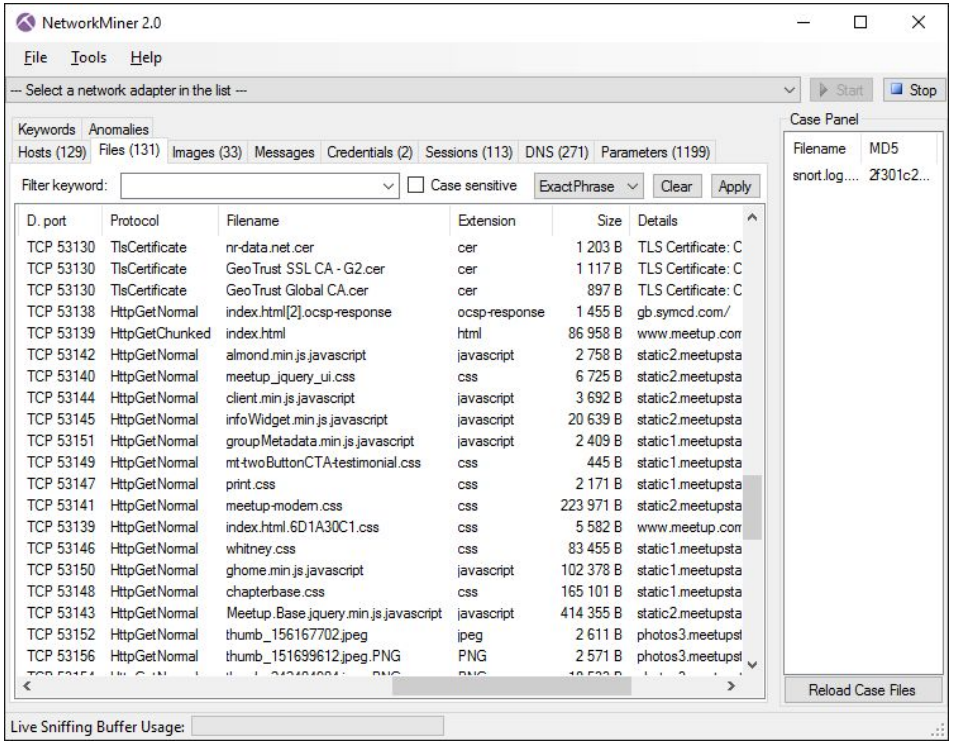
NetworkMiner

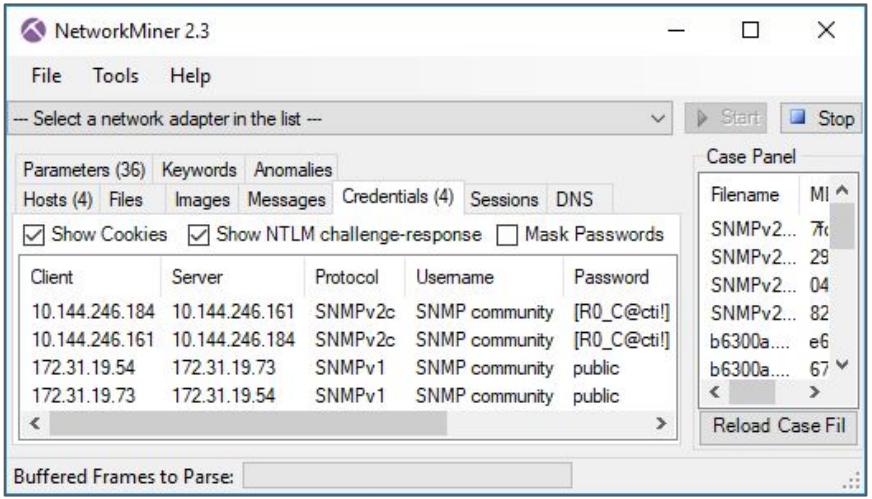




NETRESEC

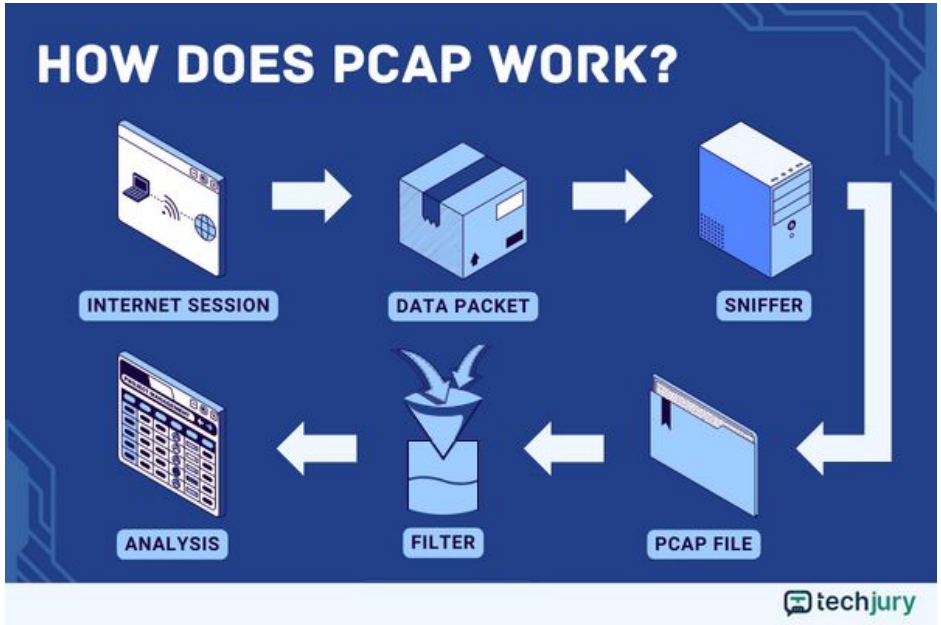
NetworkMiner





PCAPNG to PCAP

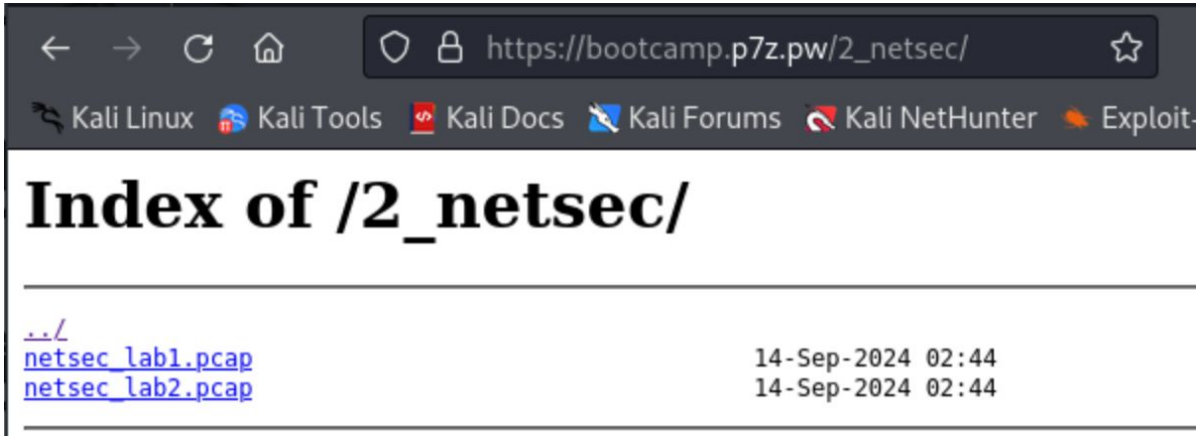
$ tshark -F pcap -r ${pcapng_file} -w ${pcap_file}



https://techjury.net

ดาวน์โหลดไฟล์แลป

https://bootcamp.p7z.pw/2_netsec/



ลองทำแลป !

Lab 1: วิเคราะห์ HTTP Protocol ใน PCAP
Lab 2: วิเคราะห์ FTP Protocol ใน PCAP

อยากให้น้อง ๆ ไปฝึกอะไรเพิ่ม

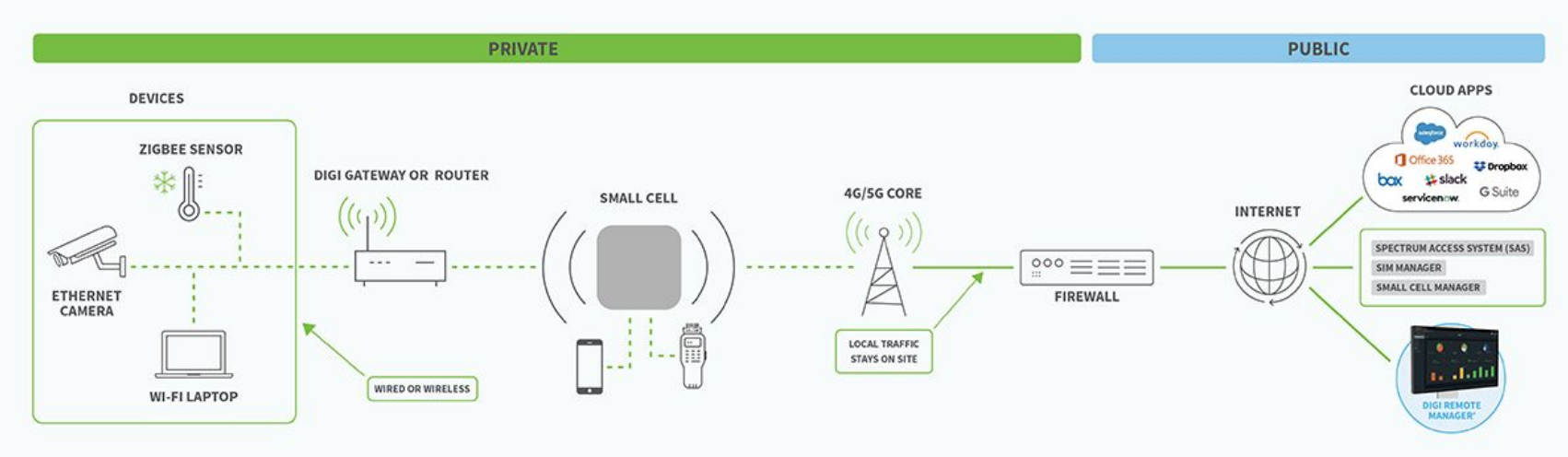
Agenda (Day 1)

เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	เสวนาแนะแนวเส้นทางอาชีพ

Thank you !!

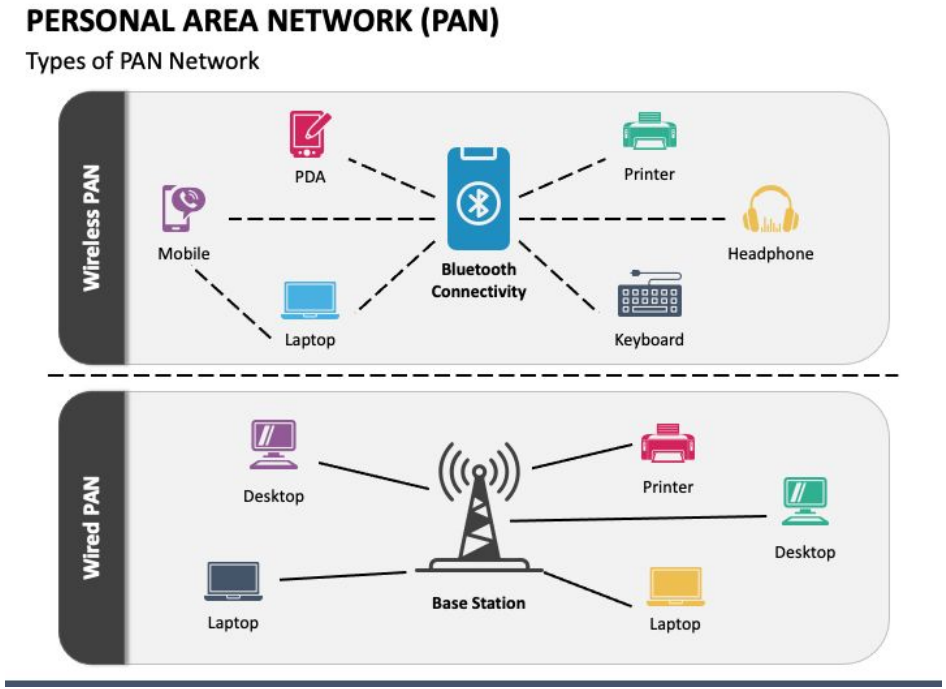
What is Networking

- A private network
- A public network



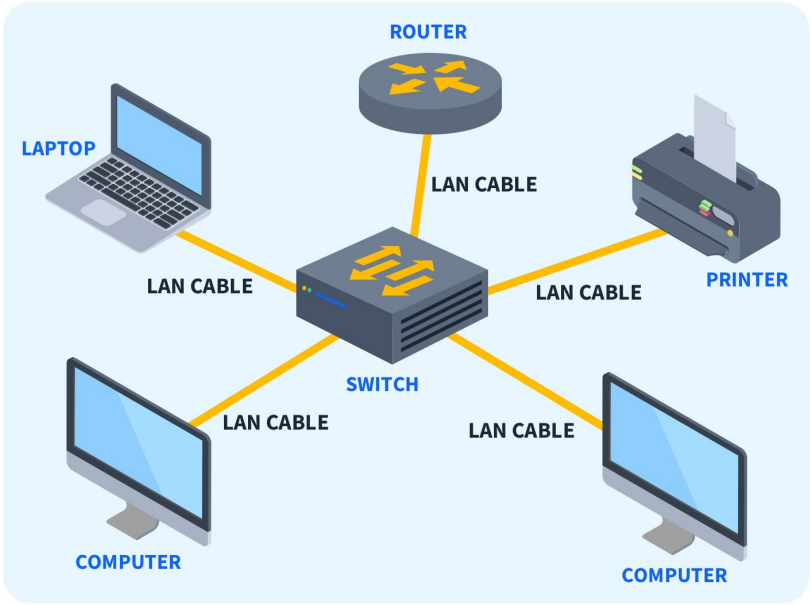
ที่มา: https://www.digi.com

Personal Area Network (PAN)



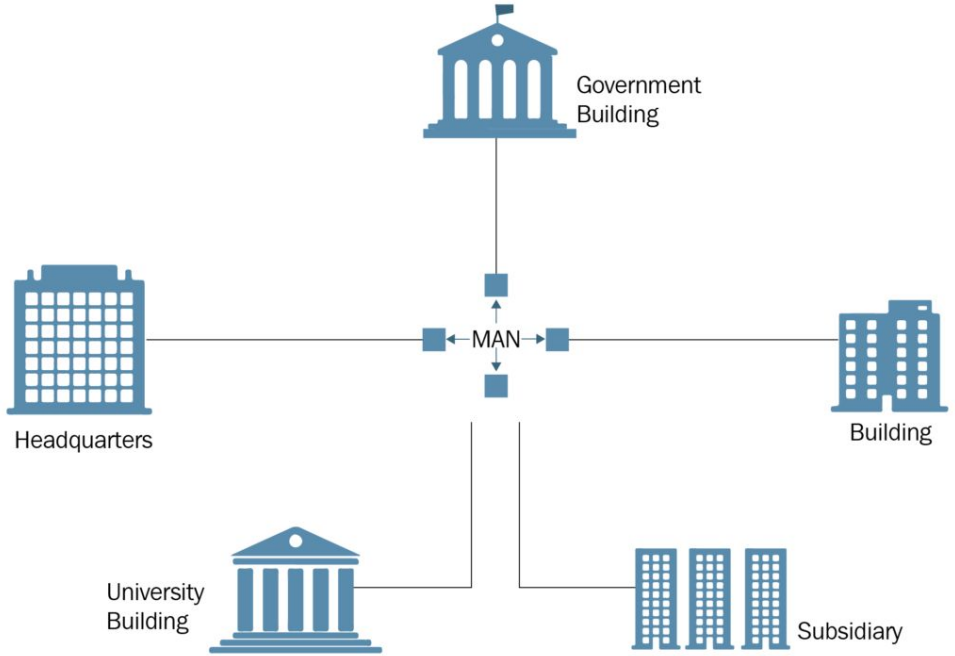
https://www.sketchbubble.com

Local Area Network (LAN)



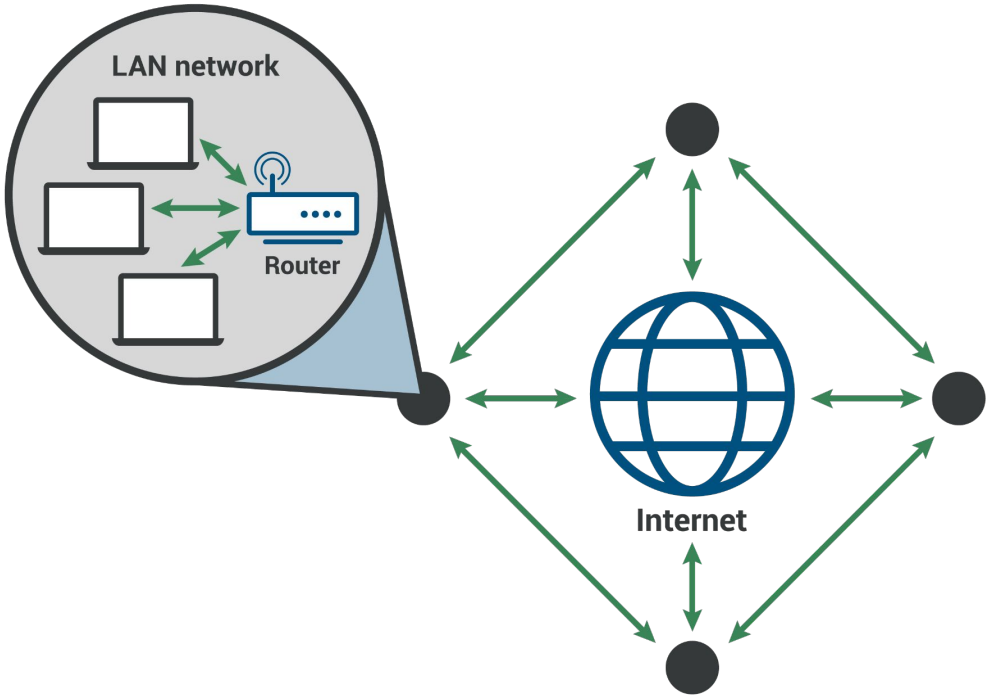
https://www.cbtnuggets.com

Metropolitan Area Network (MAN)



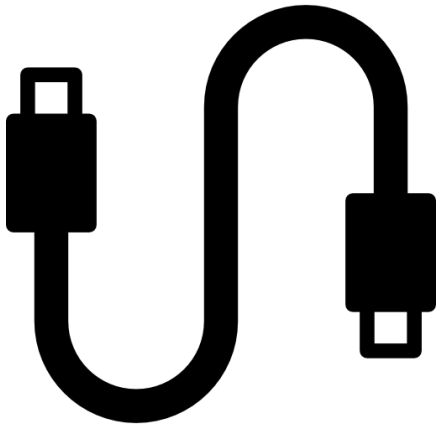
https://cyberhoot.com/cybrary/metropolitan-area-network-man

Wide Area Network (WAN)

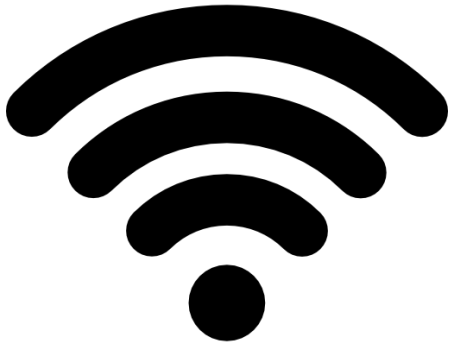


https://www.cloudflare.com/learning/network-layer/what-is-a-wan

Connection Type



Wire



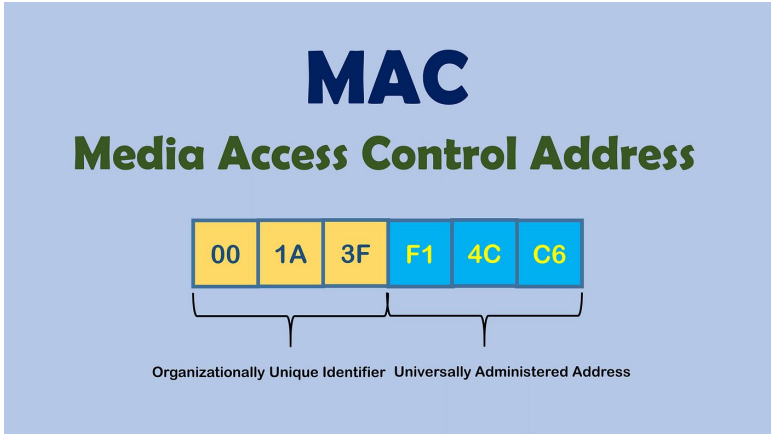
Wireless

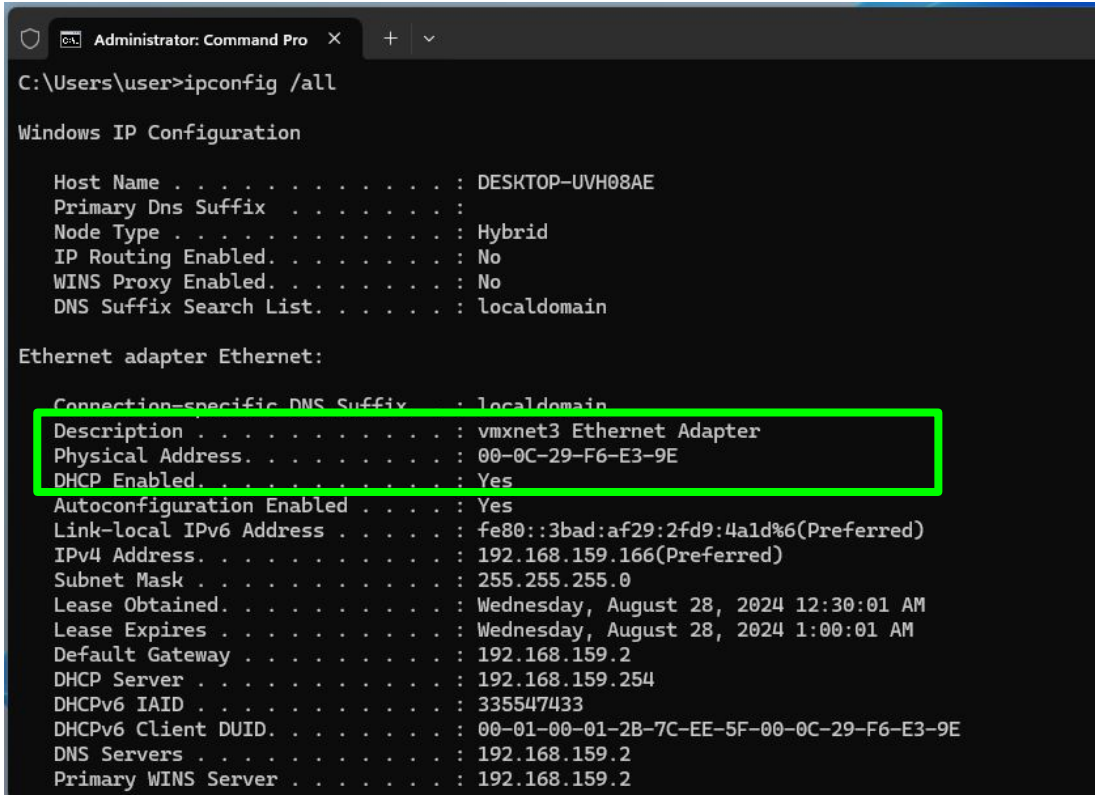
Types of networks

From sources across the web

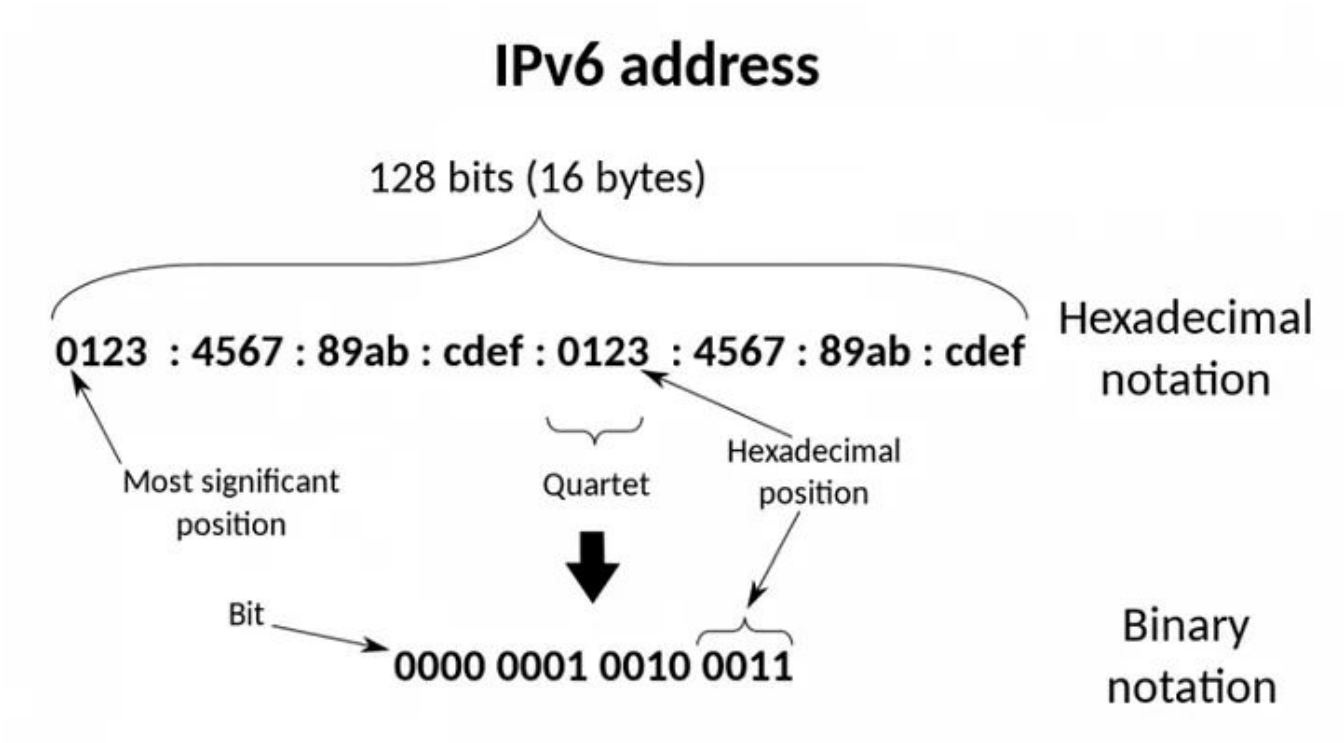
- LAN
- WAN
- Personal Area network
- Metropolitan area network
- VPN
- Campus network
- System Area network
- Private networks
- Man
- Passive optical local area ...
- Computer network
- PAN
- Bus topology
- GAN
- Han
- WLAN
- Types of networks

MAC Address


MAC
Media Access Control Address
00
1A
3F
F1
4C
C6
Organizationally Unique Identifier
Universally Administered Address


Administrator: Command Pro
C:\Users\user>ipconfig /all
Windows IP Configuration
Host Name . . . . . : DESKTOP-UVH08AE
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : localdomain
Description . . . . . : vmxnet3 Ethernet Adapter
Physical Address. . . . . : 00-0C-29-F6-E3-9E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::3bad:af29:2fd9:4a1d%6(Preferred)
IPv4 Address. . . . . : 192.168.159.166(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, August 28, 2024 12:30:01 AM
Lease Expires . . . . . : Wednesday, August 28, 2024 1:00:01 AM
Default Gateway . . . . . : 192.168.159.2
DHCP Server . . . . . : 192.168.159.254
DHCPv6 IAID . . . . . : 335547433
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-7C-EE-5F-00-0C-29-F6-E3-9E
DNS Servers . . . . . : 192.168.159.2
Primary WINS Server . . . . . : 192.168.159.2

IP Address version 6



https://medium.com/@shrutiikhatal07

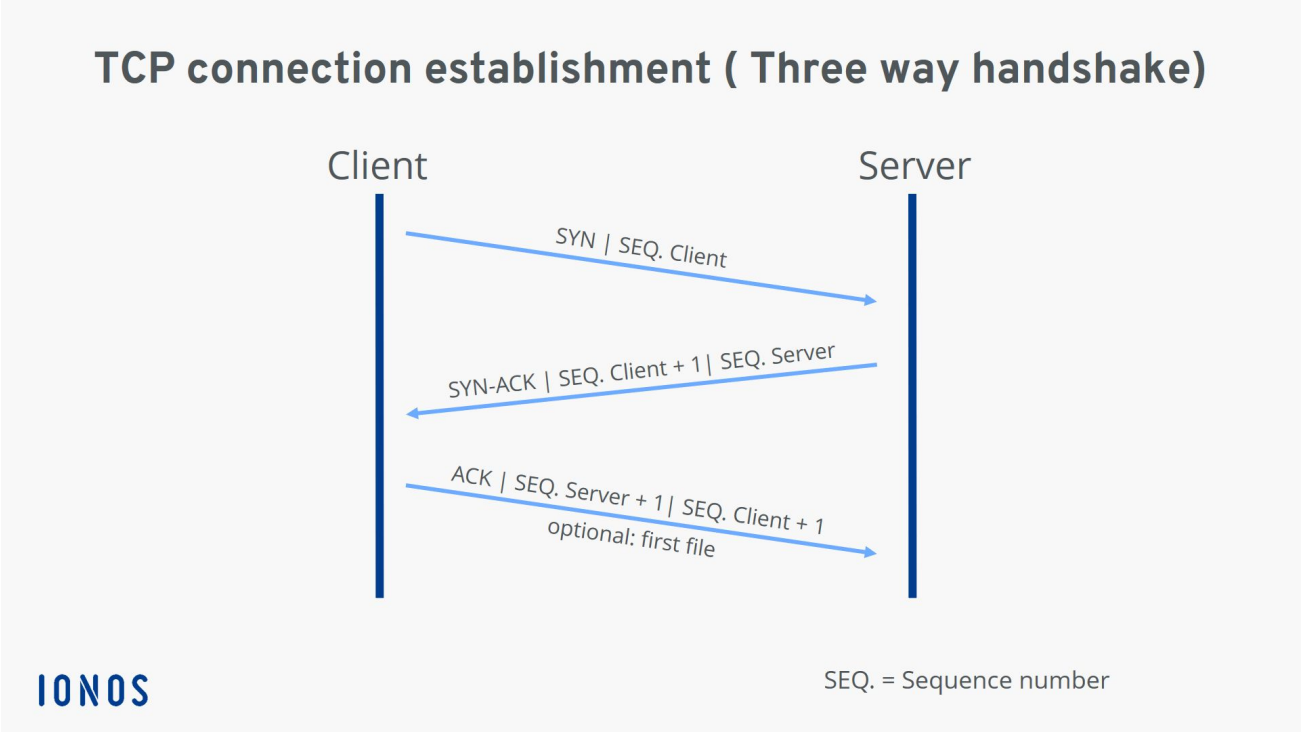
IPv4 Class

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^{7}
Class B	128 – 191	10XXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXX	192.0.0.0-223.255.255.255	255.255.255.0	$2^{8}-2$	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

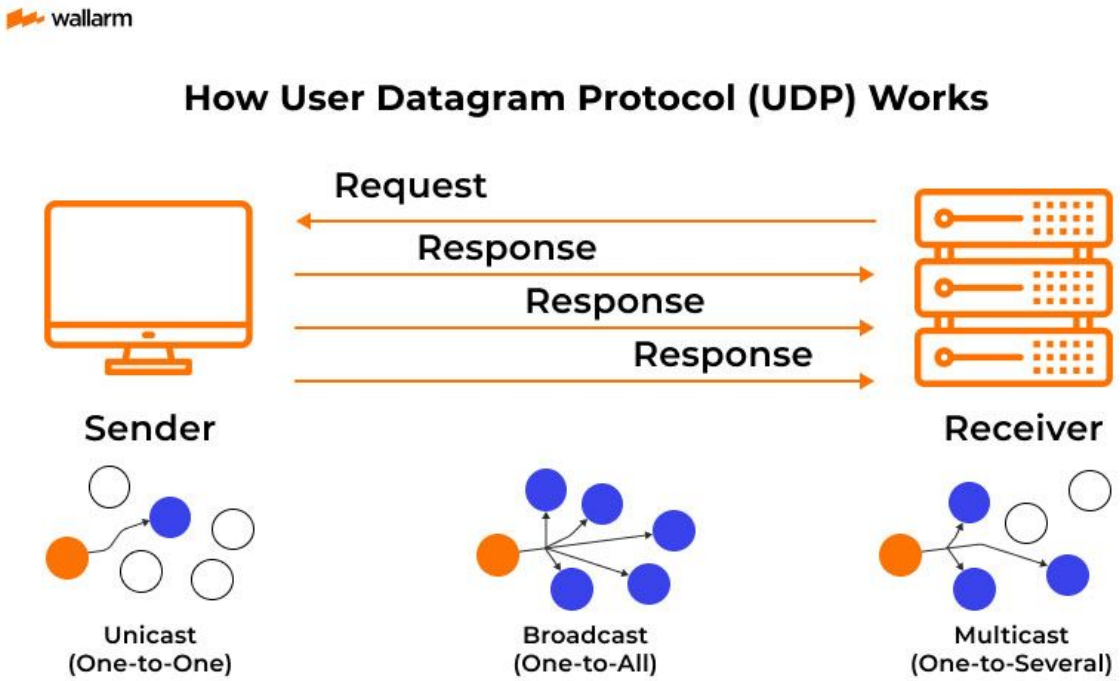
https://medium.com/@geekymuch

TCP



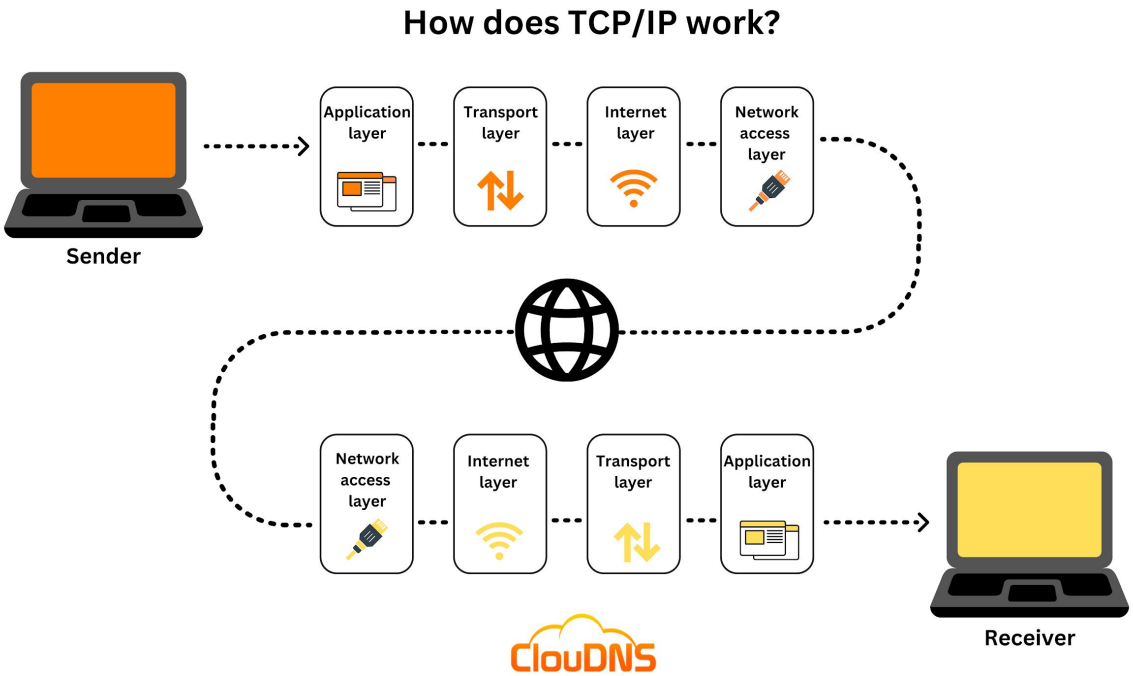
https://www.ionos.co.uk

UDP



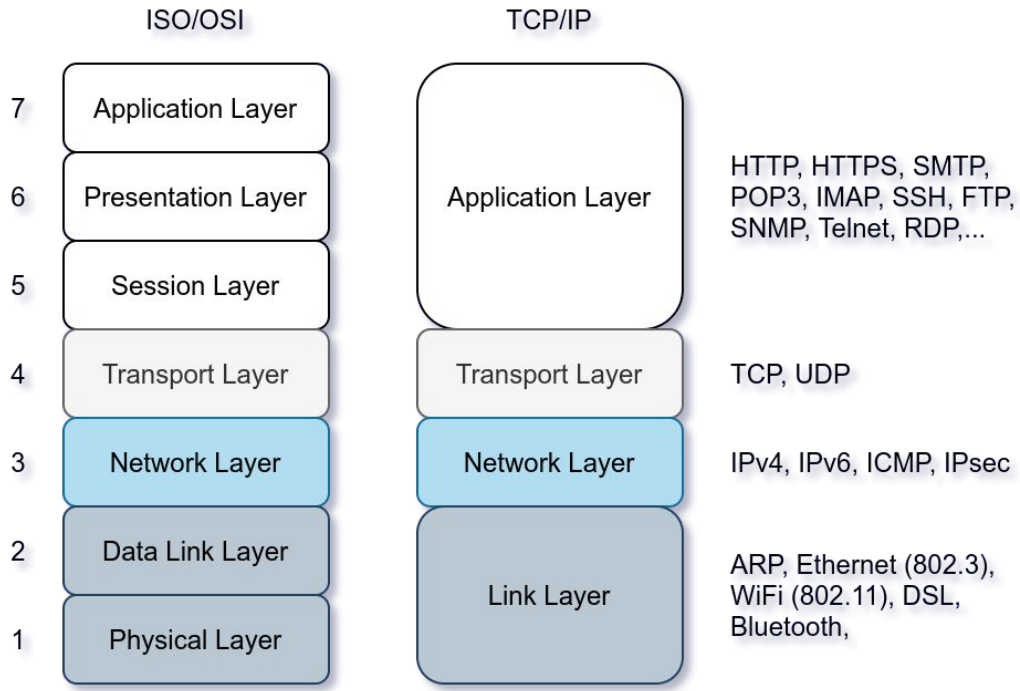
https://www.wallarm.com

TCP/IP

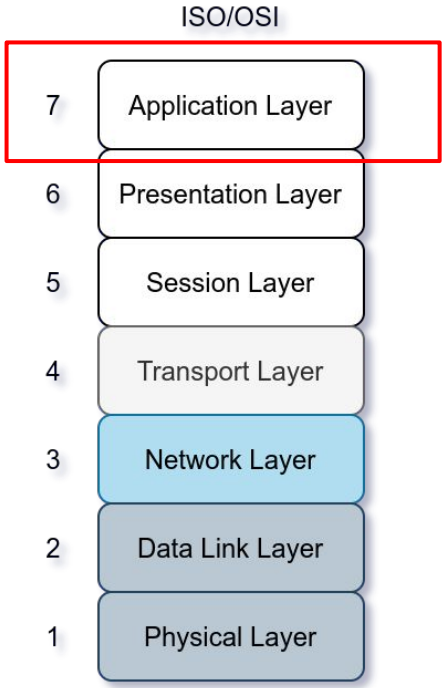


https://www.cloudns.net

OSI Model


ISO/OSI
TCP/IP
7
Application Layer
6
Presentation Layer
5
Session Layer
4
Transport Layer
3
Network Layer
2
Data Link Layer
1
Physical Layer
Application Layer
Transport Layer
Network Layer
Link Layer
HTTP, HTTPS, SMTP,
POP3, IMAP, SSH, FTP,
SNMP, Telnet, RDP,...
TCP, UDP
IPv4, IPv6, ICMP, IPsec
ARP, Ethernet (802.3),
WiFi (802.11), DSL,
Bluetooth,

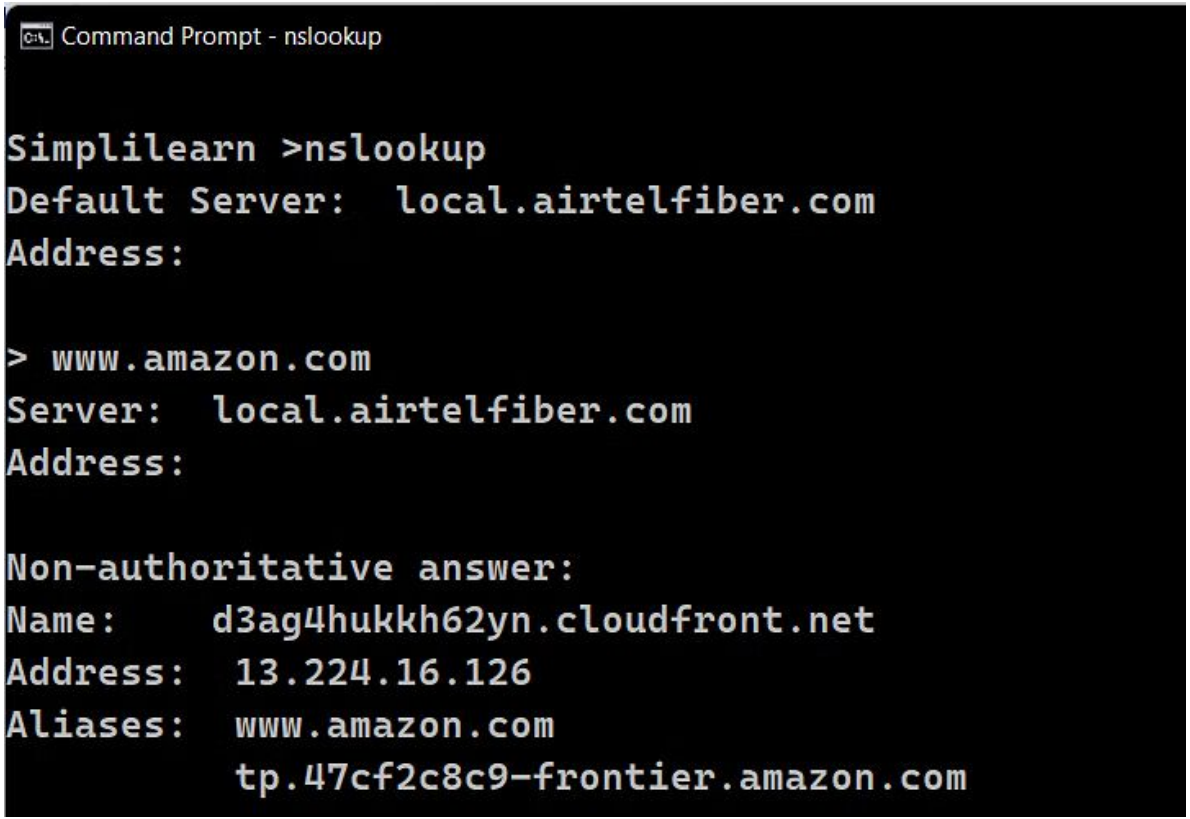
Application Protocol



- **HTTP (Hypertext Transfer Protocol)**
  ส่งข้อมูลระหว่างเว็บเบราว์เซอร์และเว็บเซิร์ฟเวอร์
- **FTP (File Transfer Protocol)**
  ใช้ในการถ่ายโอนไฟล์
- **SMTP (Simple Mail Transfer Protocol)**
  ใช้สำหรับการส่งอีเมลระหว่างเซิร์ฟเวอร์
- **SSH (Secure Shell)**
  ใช้สำหรับการเข้าถึงและจัดการเซิร์ฟเวอร์ระยะไกลอย่างปลอดภัย
- **DNS (Domain Name System)**
  ใช้ในการแปลงชื่อโดเมนให้เป็น IP Address เพื่อเชื่อมต่อกับเซิร์ฟเวอร์

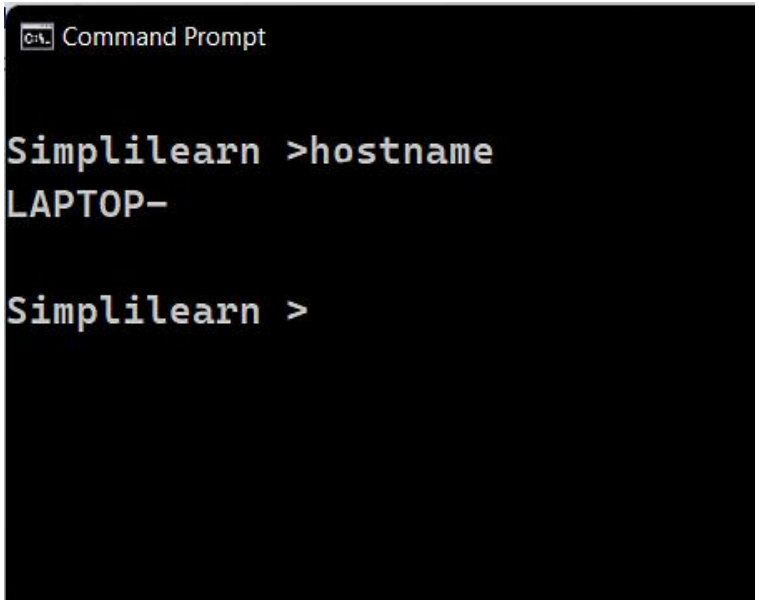
Network Command

$ nslookup

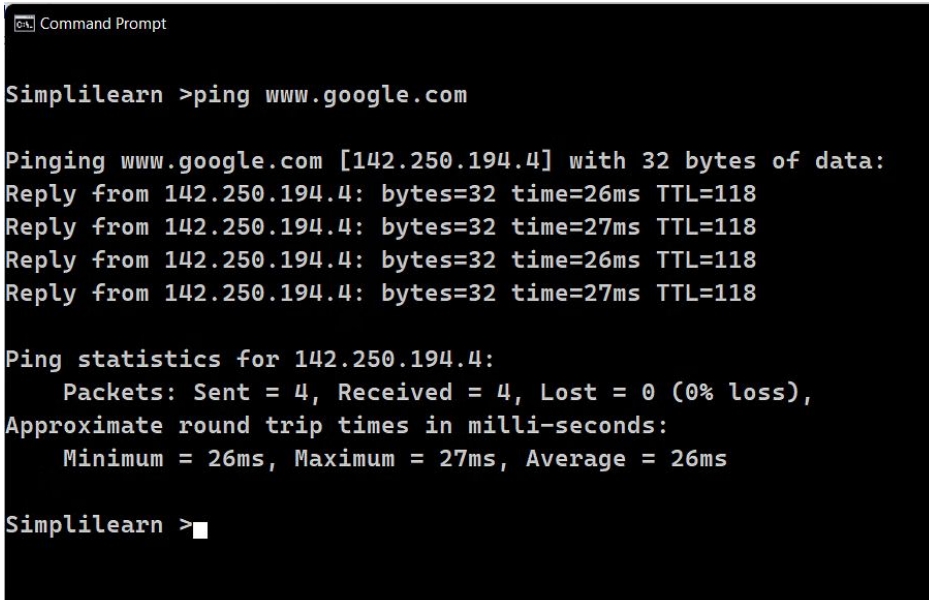


Network Command

$ hostname



$ ping

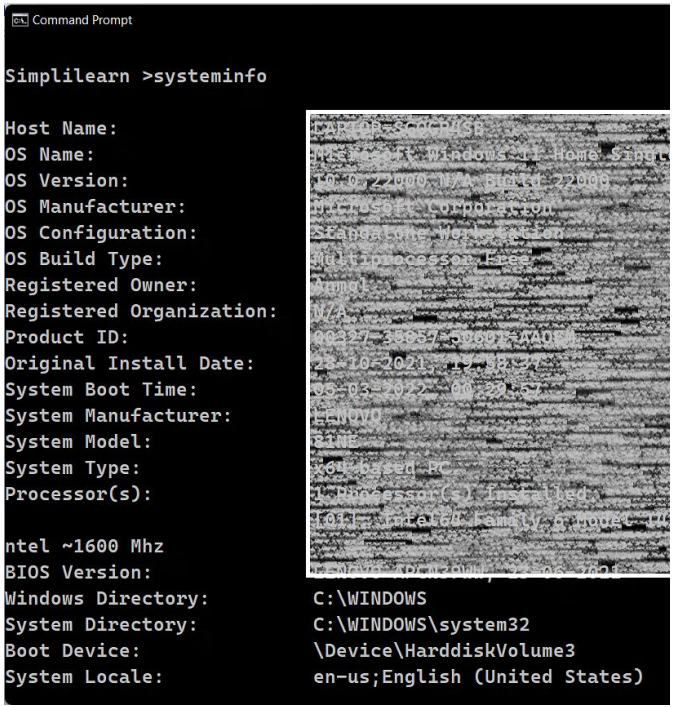


Network Command

$ tracert

Network Command

$ tracert



$ tracert