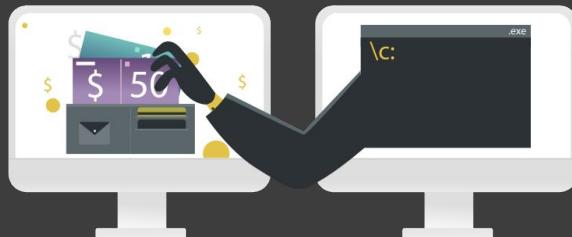


NCSA CTF Boot Camp #2

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.



Yasinthorn (Not) Khemprakhon

Penetration Tester
Siam Thanat Hack Co., Ltd.



Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างโค้ด และรูปในการบรรยาย 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	ส่วนน่าสนใจในเส้นทางอาชีพ

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



No internet

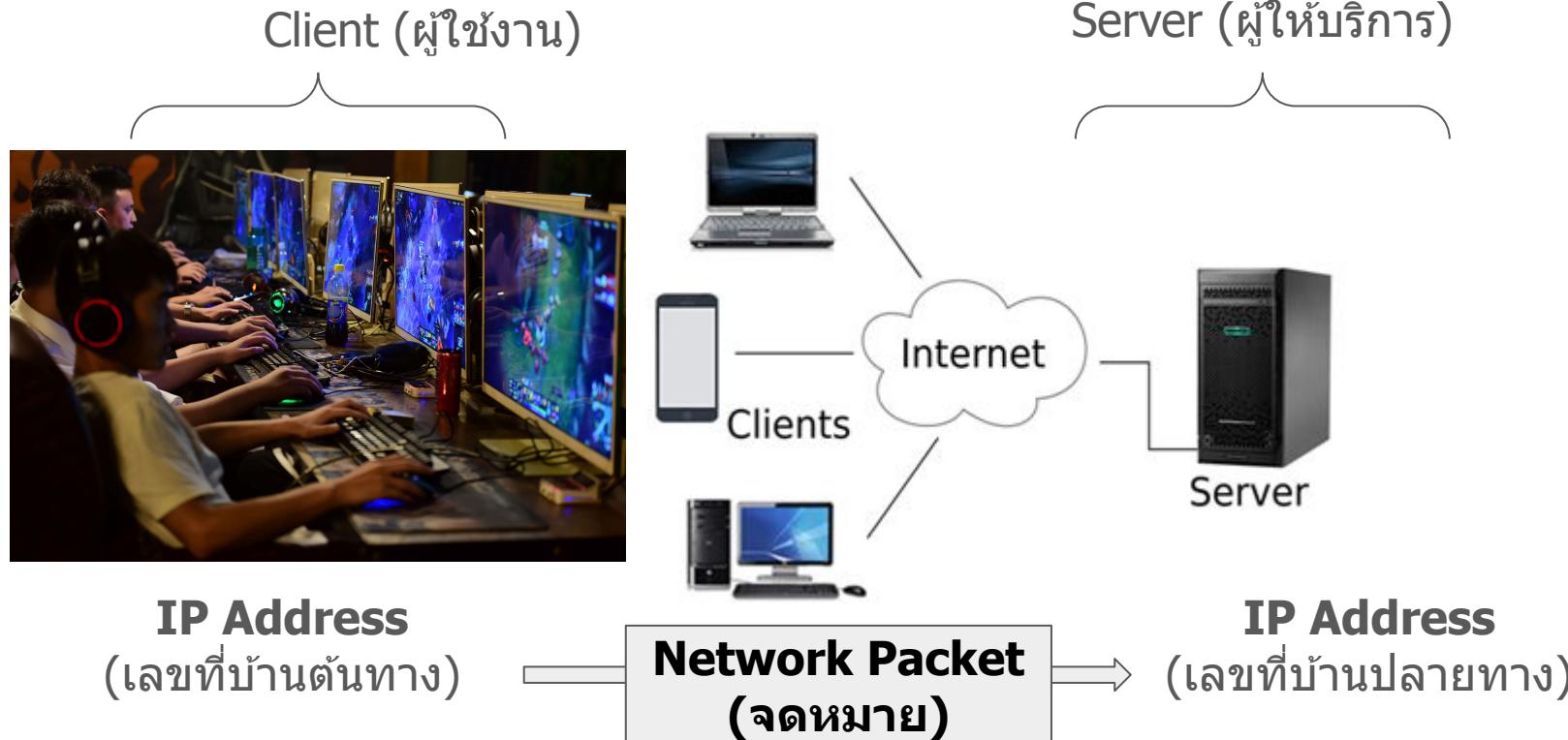
Try:

- Checking the network cables, modem, and router
- Reconnecting to Wi-Fi

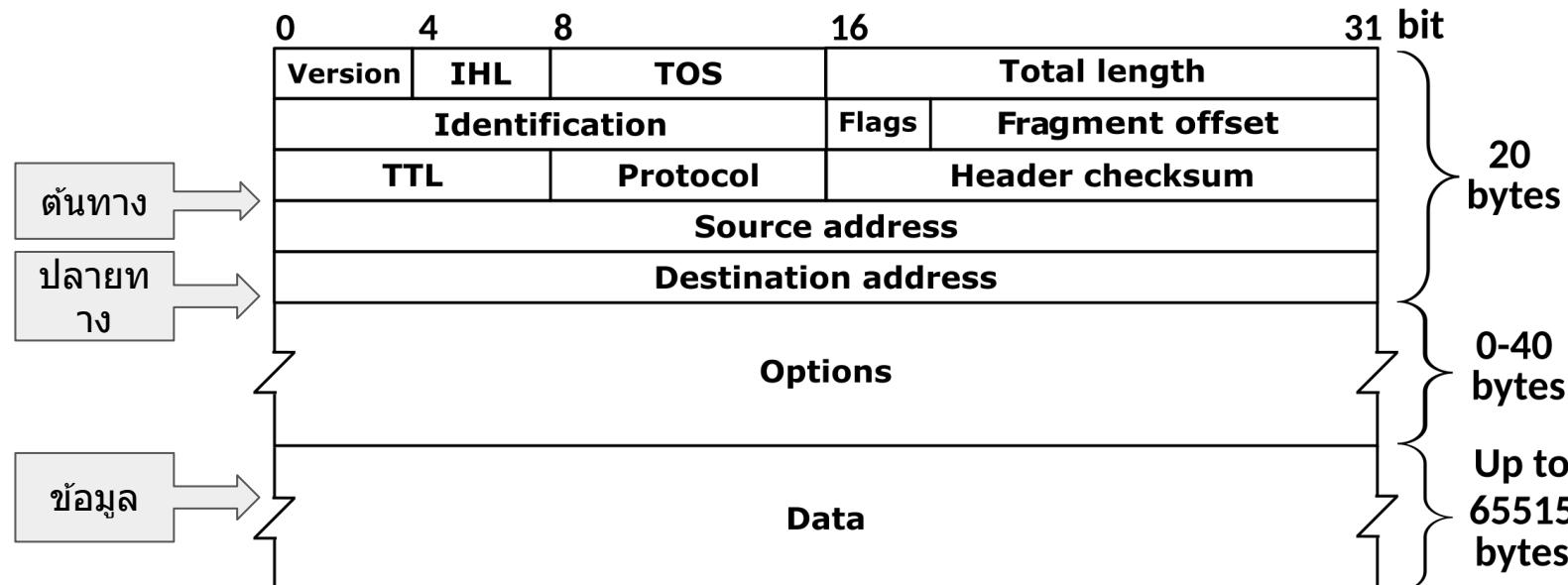
ERR_INTERNET_DISCONNECTED

เมื่อเราไม่มี
Network

Client/Server Network = ผู้ใช้งาน และ ผู้ให้บริการ

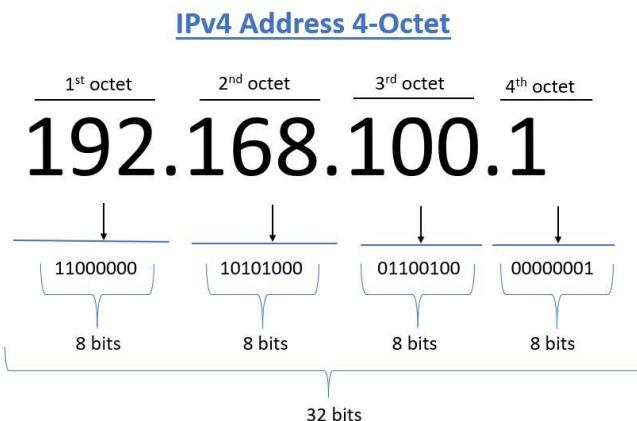


Network Packet (จดหมาย)



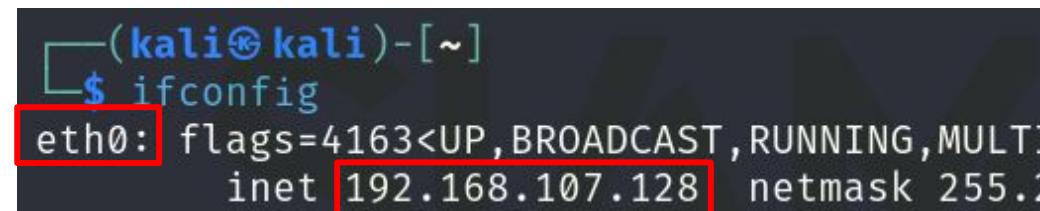
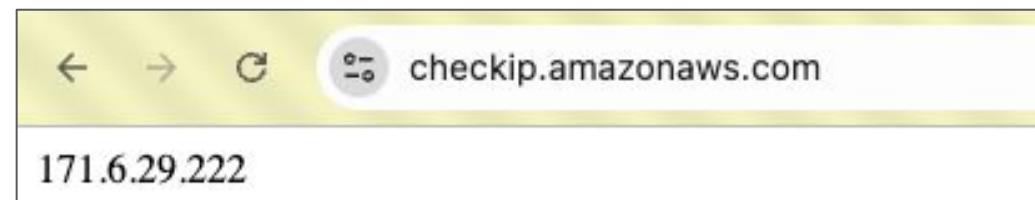
<https://en.wikipedia.org/wiki/IPv4>

IP Address (เลขที่บ้าน)



<https://medium.com/@shrutiikhatal07>

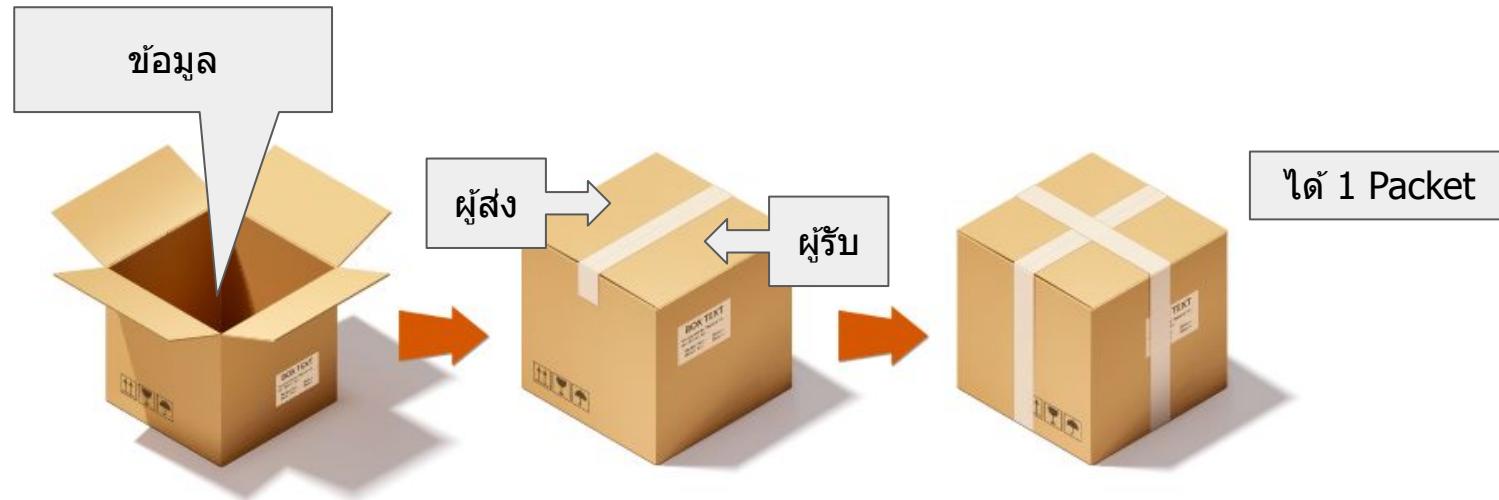
<https://checkip.amazonaws.com>



A terminal window on a Kali Linux system. The user runs the command `ifconfig`. The output shows the `eth0` interface with its flags and an IP address entry. The IP address `192.168.107.128` is highlighted with a red box.

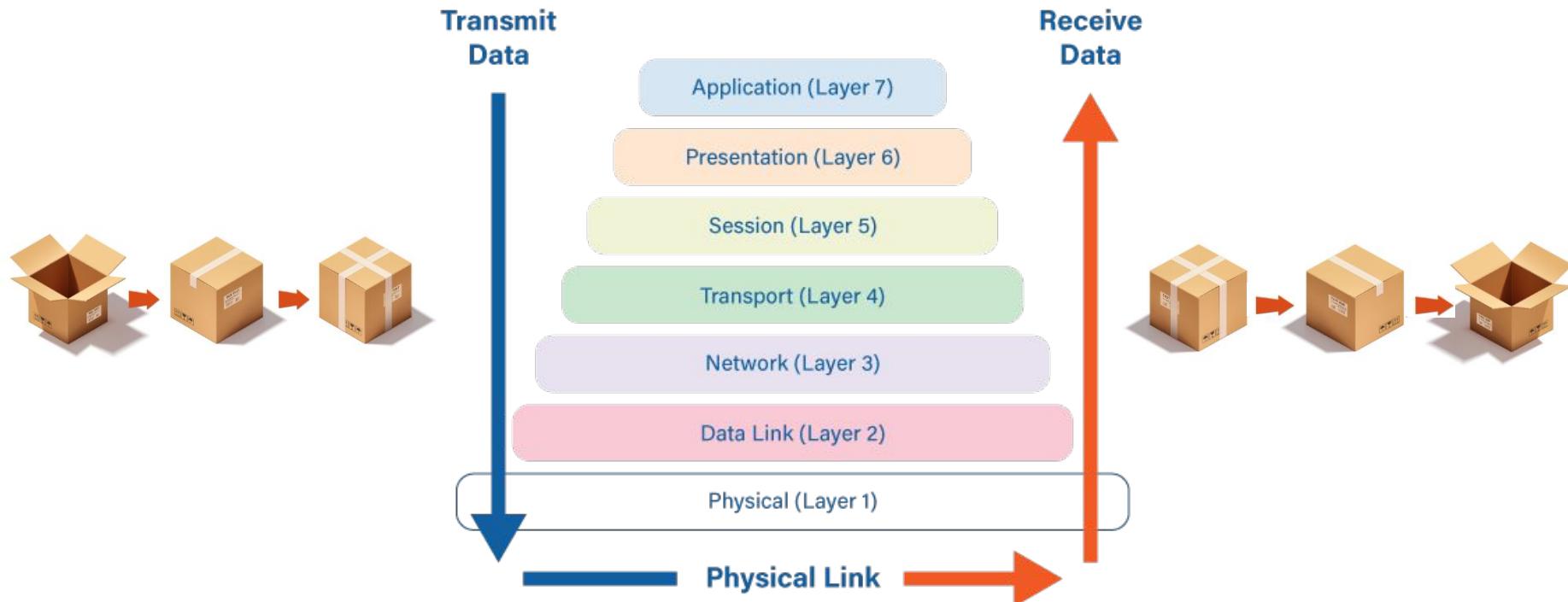
```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTI
      inet 192.168.107.128 netmask 255.255.255.0
```

Network Packet คืออะไร

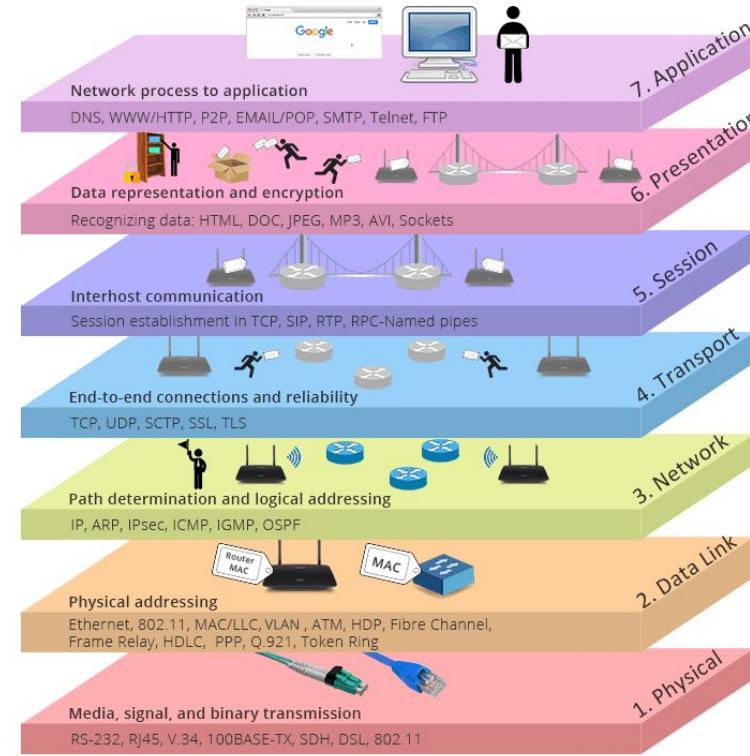


OSI (Open Systems Interconnection) Model

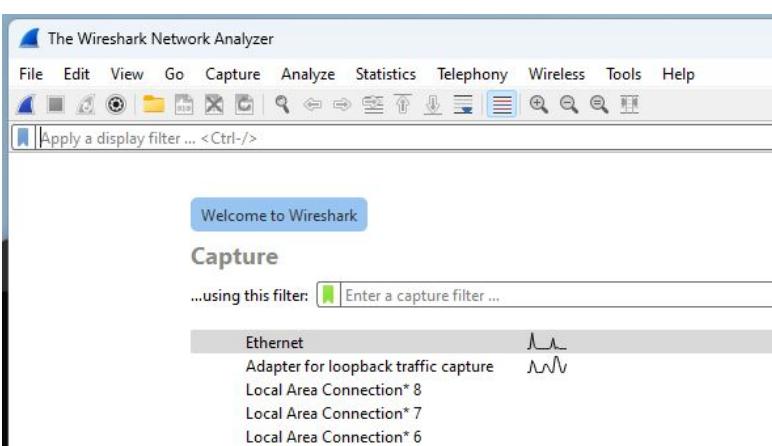
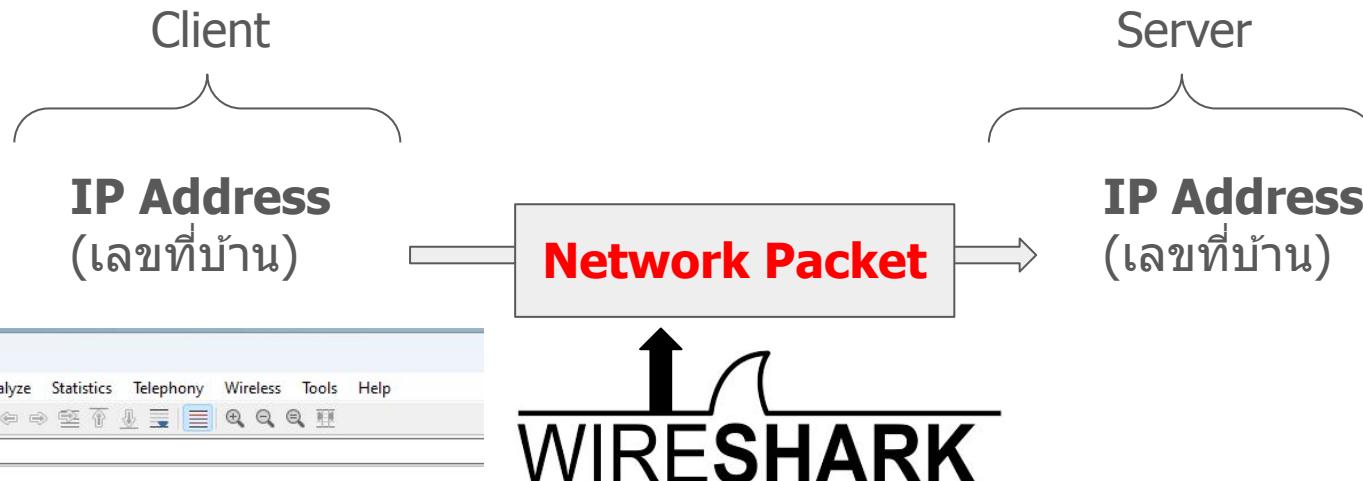
The 7 Layers of OSI



OSI (Open Systems Interconnection) Model



Network Packet Analyzer (การวิเคราะห์ข้อมูล Packet)



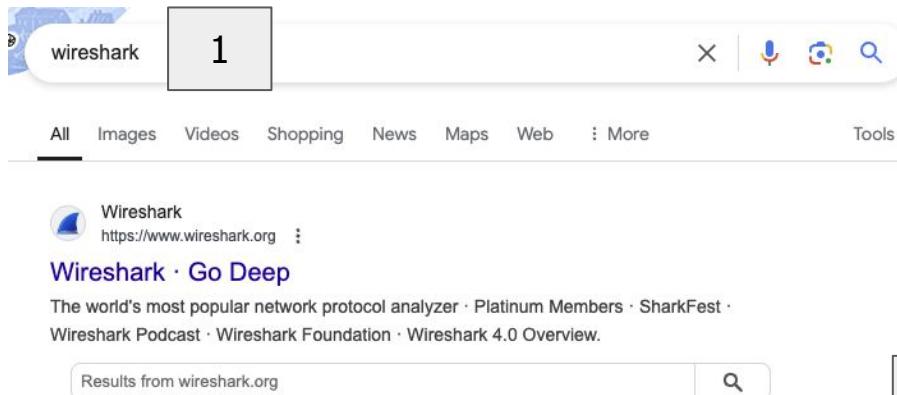
ไฟล์ PCAP

ประเภทไฟล์ที่เก็บบันทึก Network Packet ที่เคยถูกรับ-ส่ง ระหว่างคอมพิวเตอร์ ในอ็อกซ์ฟอร์ด

 netsec_lab1.pcap	8/28/2024 10:55 PM	Wireshark capture...
 netsec_lab2.pcap	Type: Wireshark capture file Size: 1.02 KB Date modified: 8/28/2024 10:55 PM	4 11:05 PM Wireshark capture...
 netsec_lab3.pcap	4 12:06 AM	Wireshark capture...
 netsec1.pcap	8/28/2024 11:48 PM	Wireshark capture...

Install Wireshark

ติดตั้ง Wireshark



1

wireshark

All Images Videos Shopping News Maps Web More Tools

Wireshark
<https://www.wireshark.org>

Wireshark · Go Deep

The world's most popular network protocol analyzer · Platinum Members · SharkFest · Wireshark Podcast · Wireshark Foundation · Wireshark 4.0 Overview.

Results from wireshark.org

Download

Download Wireshark. The current stable release of Wireshark is 4 ...



Download Wireshark

The current stable release of Wireshark is 4.2.6. It supersedes all previous development release (4.4.0rc1) and documentation.

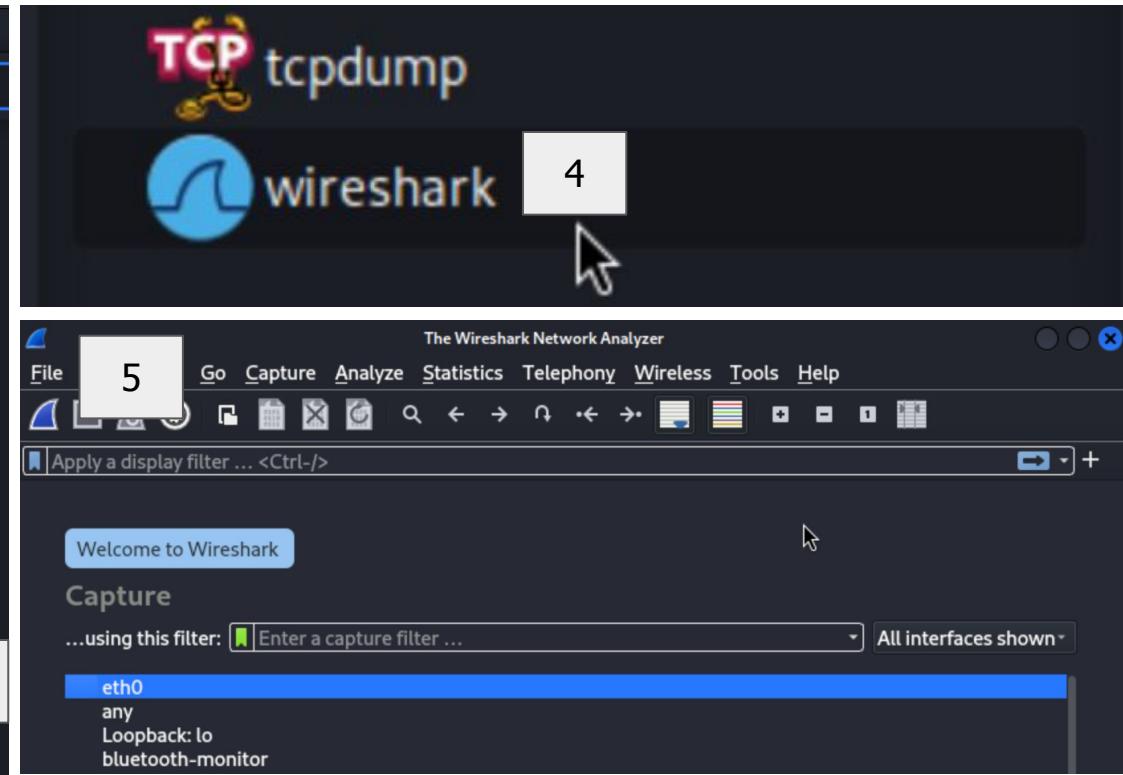
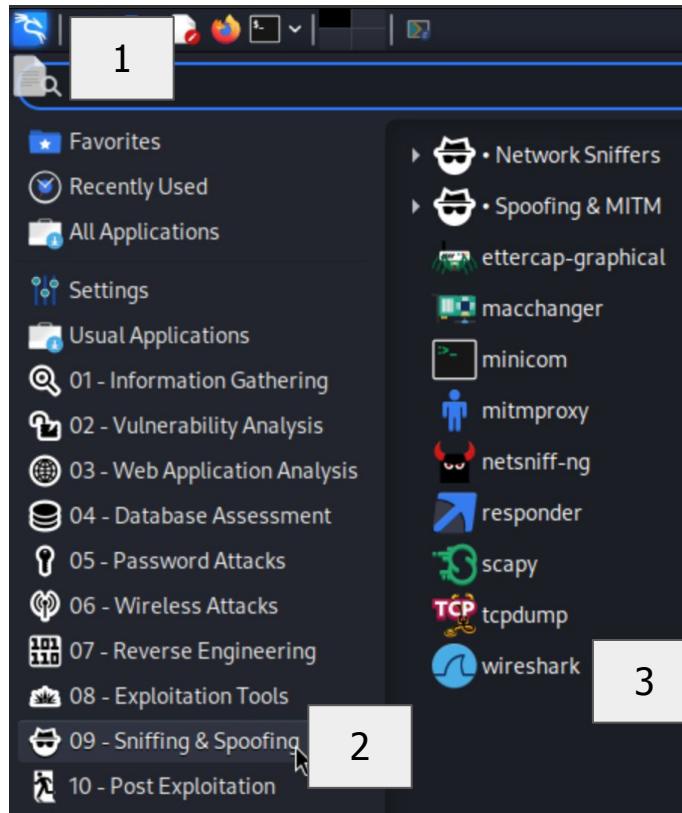
▼ Stable Release: 4.2.6

-  [Windows x64 Installer](#)
-  [Windows Arm64 Installer](#)
-  [Windows x64 PortableApps®](#)
-  [macOS Arm Disk Image](#)
-  [macOS Intel Disk Image](#)

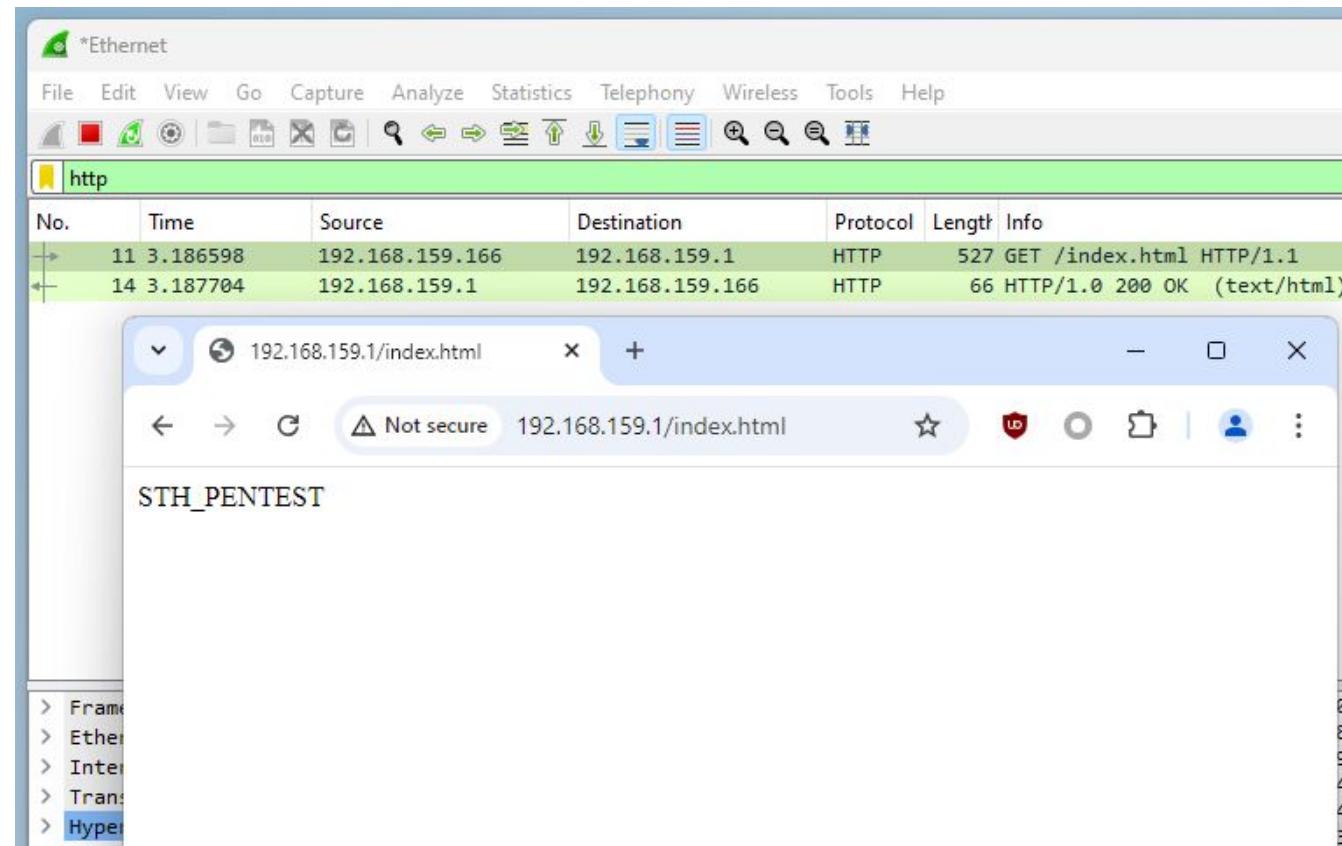


<https://www.wireshark.org/download.html>

โปรแกรม Wireshark ใน Kali



การวิเคราะห์ Network Packet ด้วย Wireshark

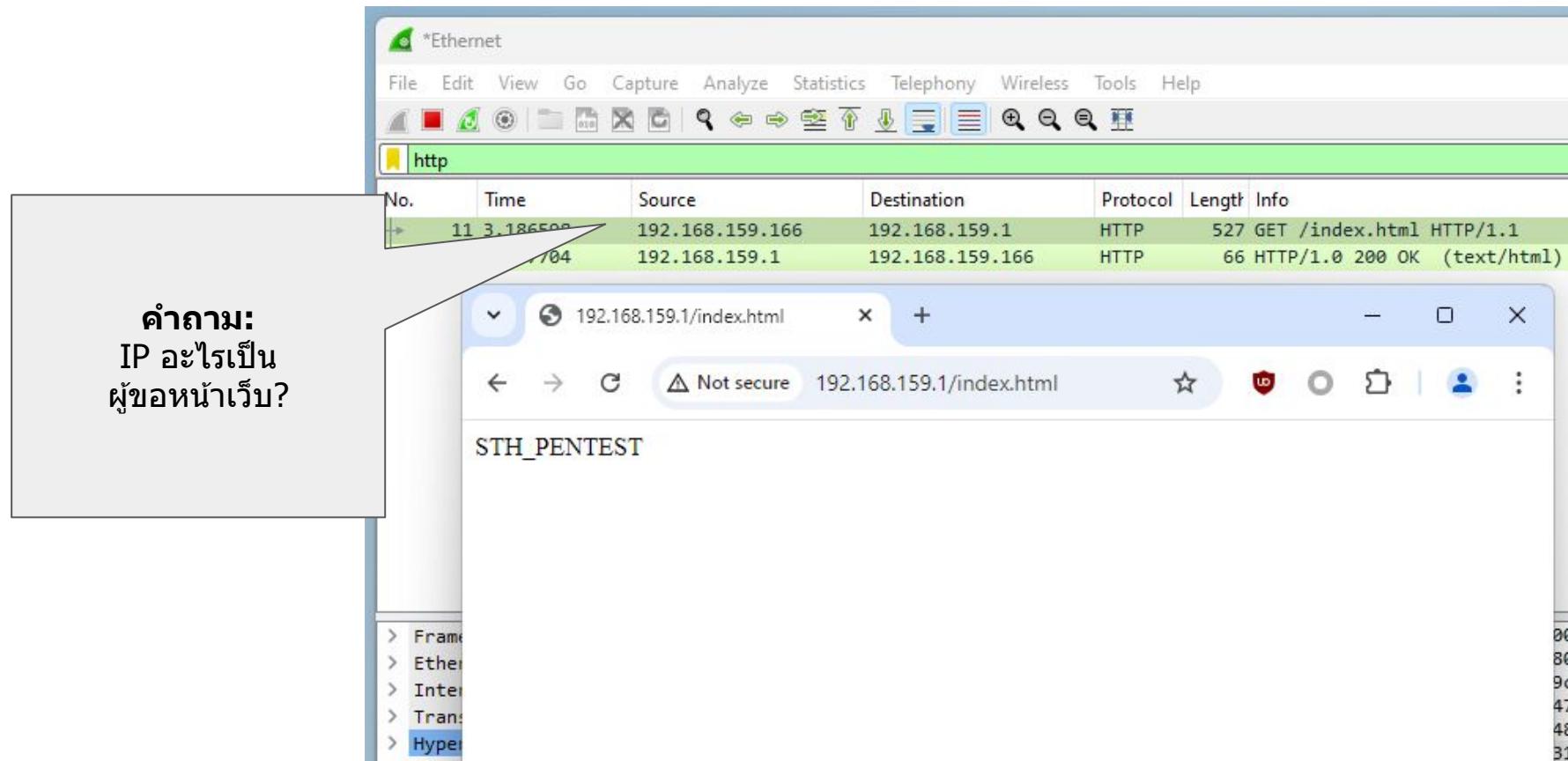


The screenshot shows a Wireshark interface with the following details:

- Network Interface:** *Ethernet
- Selected Protocol:** http
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:**

No.	Time	Source	Destination	Protocol	Length	Info
11	3.186598	192.168.159.166	192.168.159.1	HTTP	527	GET /index.html HTTP/1.1
14	3.187704	192.168.159.1	192.168.159.166	HTTP	66	HTTP/1.0 200 OK (text/html)
- Browser Preview:** A browser window titled "192.168.159.1/index.html" shows the content "STH_PENTEST". The status bar indicates "Not secure".
- Bottom Navigation:** Frame, Ether, Inter, Trans, Hyper
- Bottom Status:** 00, 80, 9c, 47, 48, 31

การวิเคราะห์ Network Packet ด้วย Wireshark



คำนวณ:
IP อะไรเป็น
ผู้ขอหน้าเว็บ?

No.	Time	Source	Destination	Protocol	Length	Info
11	3.186500	192.168.159.166	192.168.159.1	HTTP	527	GET /index.html HTTP/1.1
104		192.168.159.1	192.168.159.166	HTTP	66	HTTP/1.0 200 OK (text/html)

192.168.159.1/index.html

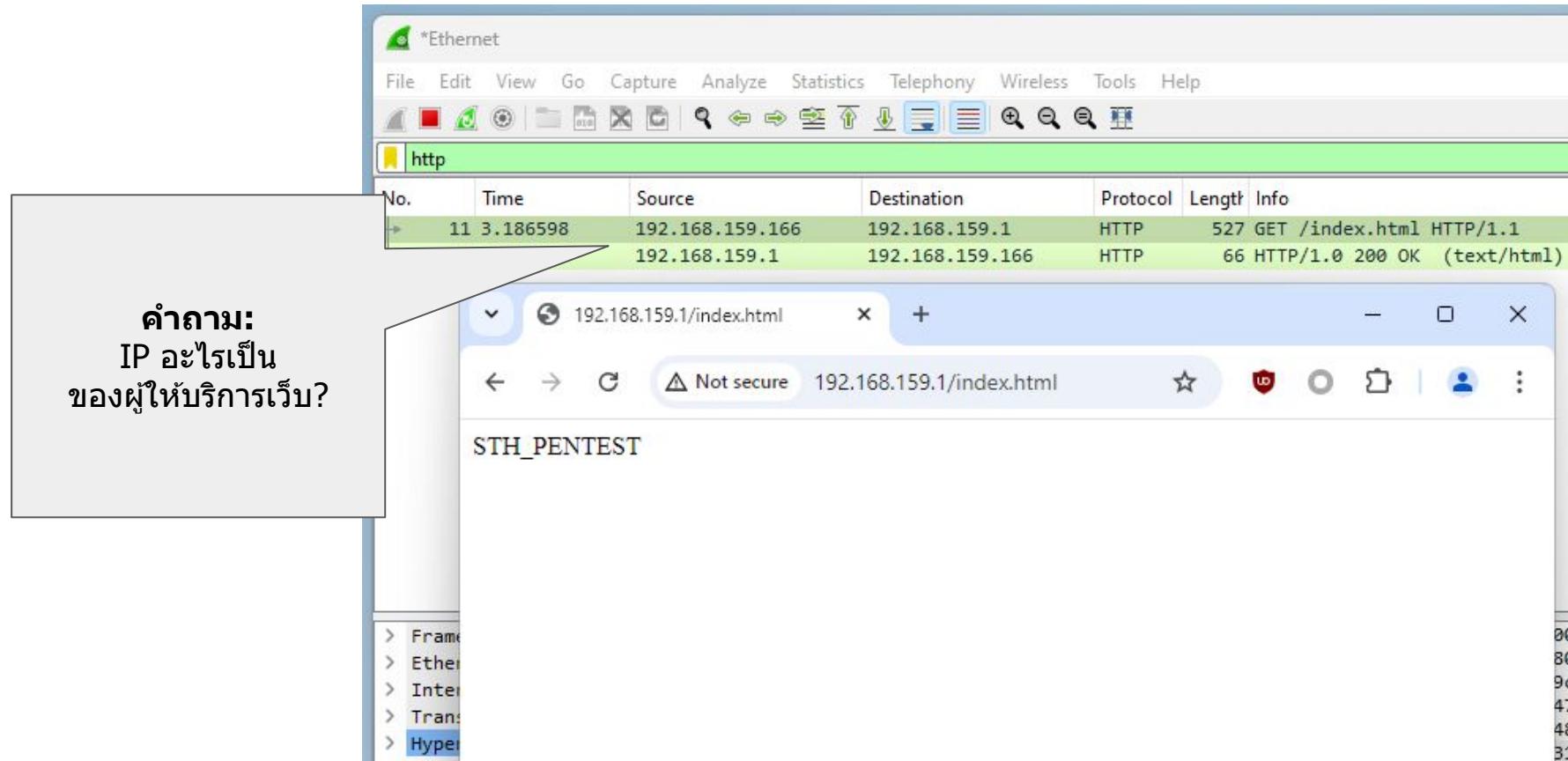
Not secure 192.168.159.1/index.html

STH_PENTEST

- > Frame
- > Ethernet
- > Internet Protocol Version 4 (IPv4)
- > Transmission Control Protocol (TCP)
- > Hypertext Transfer Protocol (HTTP)

00
80
9c
47
48
31

การวิเคราะห์ Network Packet ด้วย Wireshark



คำานวณ:
IP อะไรเป็น
ของผู้ให้บริการเว็บ?

No.	Time	Source	Destination	Protocol	Length	Info
11	3.186598	192.168.159.1	192.168.159.1	HTTP	527	GET /index.html HTTP/1.1
		192.168.159.1	192.168.159.166	HTTP	66	HTTP/1.0 200 OK (text/html)

192.168.159.1/index.html

Not secure 192.168.159.1/index.html

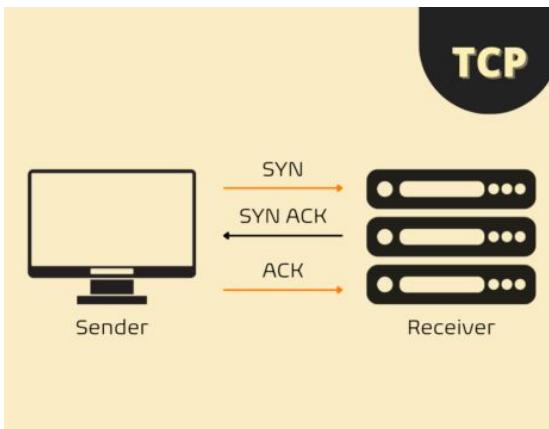
STH_PENTEST

- > Frame
- > Ethernet
- > Internet Protocol Version 4 (IPv4)
- > Transmission Control Protocol (TCP)
- > Hypertext Transfer Protocol (HTTP)

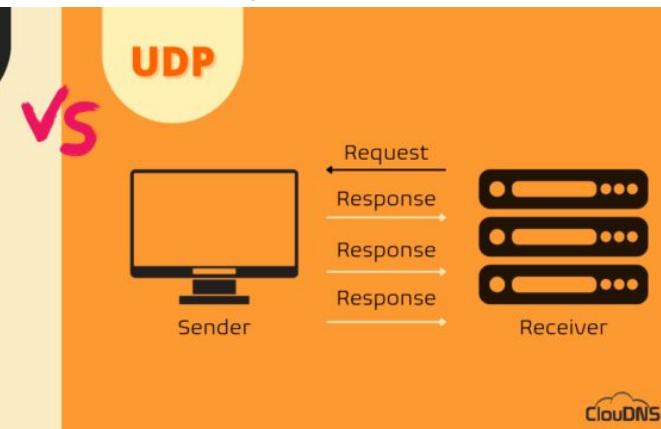
00
80
9c
47
48
31

TCP/UDP

Transmission Control Protocol



User Datagram Protocol



มีการตรวจสอบ ว่าข้อมูลส่งถึง
(TCP 3-Way Handshake)

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

ไม่มีการตรวจสอบ
ว่าข้อมูลส่งถึง (ส่ง ๆ ไป)

A helpful guide



TCP (Transmission Control Protocol)

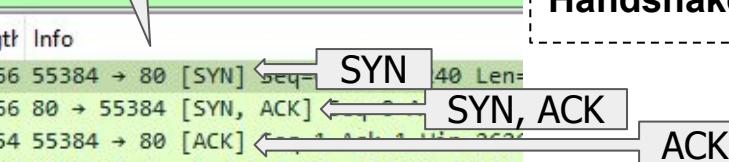
*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.159.1 && tcp

No.	Time	Source	Destination	Protocol	Length	Info
69	3.117829	192.168.159.166	192.168.159.1	TCP	66	55384 → 80 [SYN] seq 40 Len=
71	3.118217	192.168.159.1	192.168.159.166	TCP	66	80 → 55384 [SYN, ACK]
73	3.118293	192.168.159.166	192.168.159.1	TCP	54	55384 → 80 [ACK]
74	3.118418	192.168.159.1	192.168.159.166	TCP	60	[TCP Window Update] 80 → 55384 [ACK]

TCP 3-Way Handshake

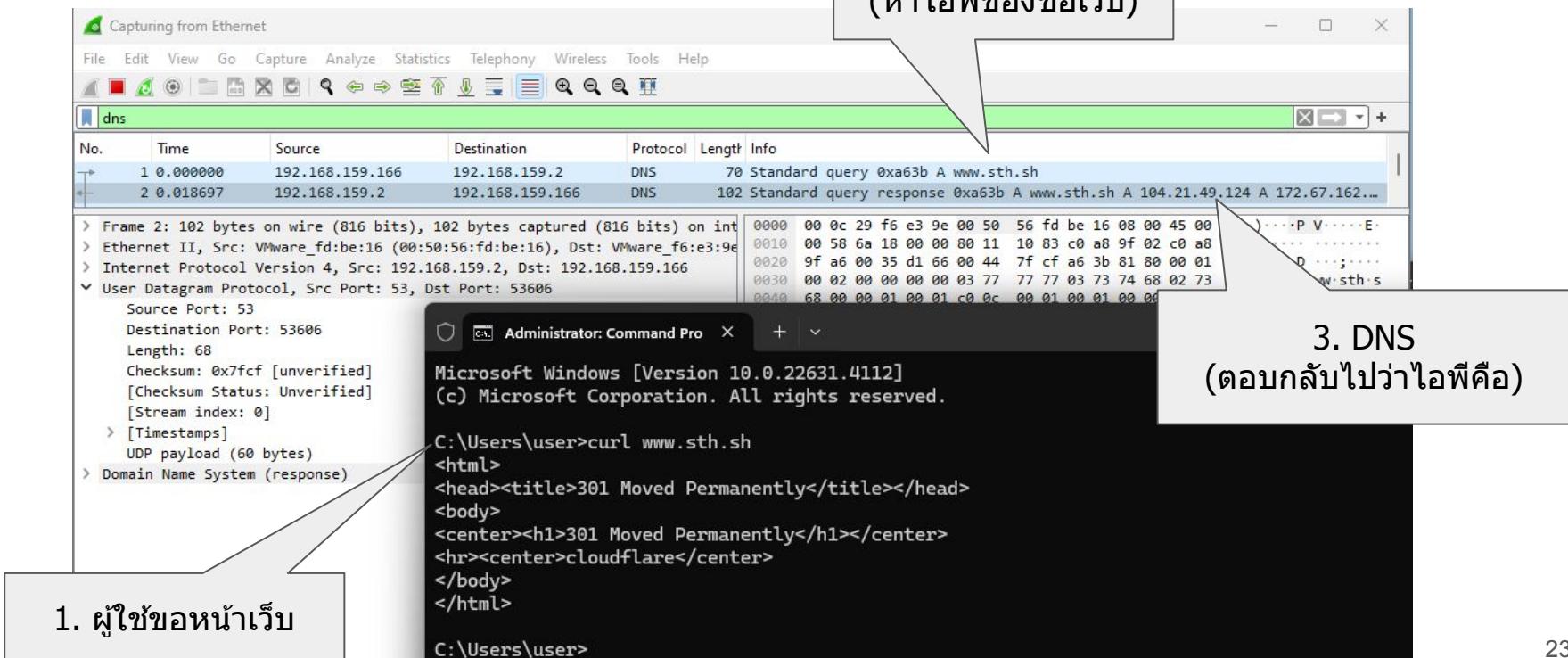


Administrator: Command Pro

Microsoft Windows [Version 10.0.22631.4112]
(c) Microsoft Corporation. All rights reserved.

```
C:\Users\user>ncat 192.168.159.1 80
libnsock ssl_init_helper(): OpenSSL legacy provider failed to load.
```

UDP (User Datagram Protocol)



The screenshot illustrates the process of performing a DNS query and receiving a response. It shows three main components:

- 1. ผู้ใช้ขอหน้าเว็บ**: A box pointing to the Command Prompt window where the user runs the command `curl www.sth.sh`, which returns a 301 Moved Permanently response.
- 2. DNS (หาไอพีของชื่อเว็บ)**: A box pointing to the Wireshark interface showing a DNS query from the user's machine (192.168.159.166) to the DNS server (192.168.159.2). The response is a DNS message with hex dump and ASCII representation.
- 3. DNS (ตอบกลับไปว่าไอพีคือ)**: A box pointing to the Wireshark interface showing the DNS response message, which includes the IP address 104.21.49.124 for the domain www.sth.sh.

Wireshark details:

- Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface Ethernet II, Src: VMware_fd:be:16 (00:50:56:fd:be:16), Dst: VMware_f6:e3:9e (00:0c:29:f6:e3:9e)
- Ethernet II, Src: VMware_fd:be:16 (00:50:56:fd:be:16), Dst: VMware_f6:e3:9e (00:0c:29:f6:e3:9e)
- Internet Protocol Version 4, Src: 192.168.159.2, Dst: 192.168.159.166
- User Datagram Protocol, Src Port: 53, Dst Port: 53606
- Source Port: 53
Destination Port: 53606
Length: 68
Checksum: 0x7fcf [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
- [Timestamps]
UDP payload (60 bytes)
- Domain Name System (response)

Command Prompt Output:

```
C:\Users\user>curl www.sth.sh
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>cloudflare</center>
</body>
</html>
```

C:\Users\user>

Network Protocol

ประเภท TCP (ซ้ำแล้วซ้ำร้า)

- HTTP (เว็บ)
- FTP (โอนไฟล์)
- SMTP (ส่งอีเมล)

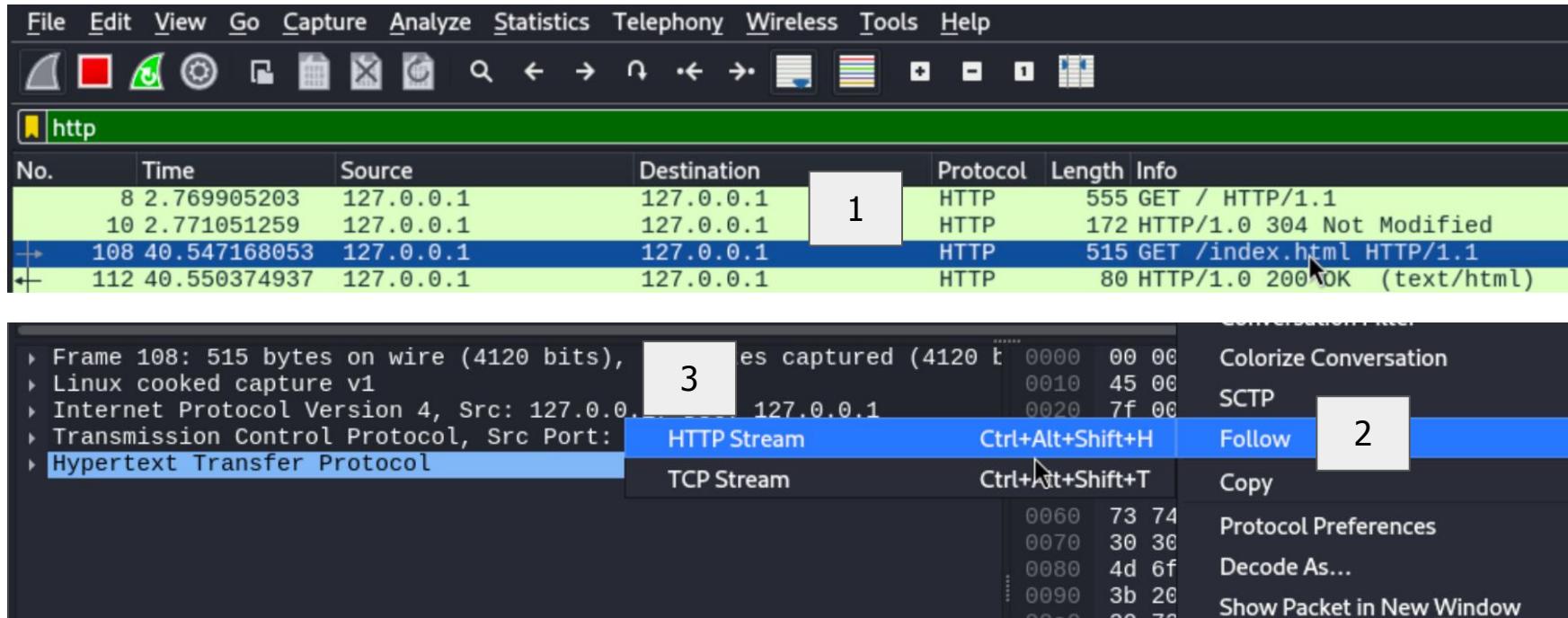
ประเภท UDP (เน้นเร็ว)

- DNS (ชื่อเว็บ)
- NTP (บอกเวลา)
- SNMP (ข้อมูลอุปกรณ์เครือข่าย)

Capturing...

No.	Time	Source	Destination	Protocol	Length	Info
7	1.261915876	172.67.162.253	192.168.159.134	UDP	70	443 → 57025 Len=28
8	1.266218501	172.67.162.253	192.168.159.134	UDP	203	443 → 57025 Len=161
9	1.267553667	192.168.159.134	23.42.144.73	TLSv1.2	1390	Application Data
10	1.267838584	23.42.144.73	192.168.159.134	TCP	60	443 → 50280 [ACK] Seq=1
11	1.288029959	192.168.159.134	172.67.162.253	UDP	88	57025 → 443 Len=46
12	1.311176584	192.168.159.134	23.42.144.73	TLSv1.2	1390	Application Data
13	1.311587251	23.42.144.73	192.168.159.134	TCP	60	443 → 50286 [ACK] Seq=1
14	1.320366667	172.67.162.253	192.168.159.134	UDP	67	443 → 57025 Len=25
15	1.332443376	192.168.159.134	172.67.162.253	UDP	1339	57025 → 443 Len=1297
16	1.342392584	192.168.159.134	172.67.162.253	UDP	88	57025 → 443 Len=46
17	1.366737001	172.67.162.253	192.168.159.134	UDP	70	443 → 57025 Len=28
18	1.369107251	172.67.162.253	192.168.159.134	UDP	203	443 → 57025 Len=161
19	1.389346626	192.168.159.134	172.67.162.253	UDP	88	57025 → 443 Len=46
20	1.460589709	23.42.144.73	192.168.159.134	TLSv1.2	1558	Application Data
21	1.460624167	192.168.159.134	23.42.144.73	TCP	54	50280 → 443 [ACK] Seq=1
22	1.485741459	192.168.159.134	104.21.49.124	TCP	54	32908 → 80 [ACK] Seq=1
23	1.495496042	23.42.144.73	192.168.159.134	TLSv1.2	1558	Application Data
24	1.495520376	192.168.159.134	23.42.144.73	TCP	54	50286 → 443 [ACK] Seq=1
25	1.525922831	192.168.159.134	147.92.191.144	TLSv1.2	2760	Application Data

การตรวจสอบเนื้อหาของ Packet ที่เป็น Protocol HTTP



The screenshot shows a Wireshark interface with the following details:

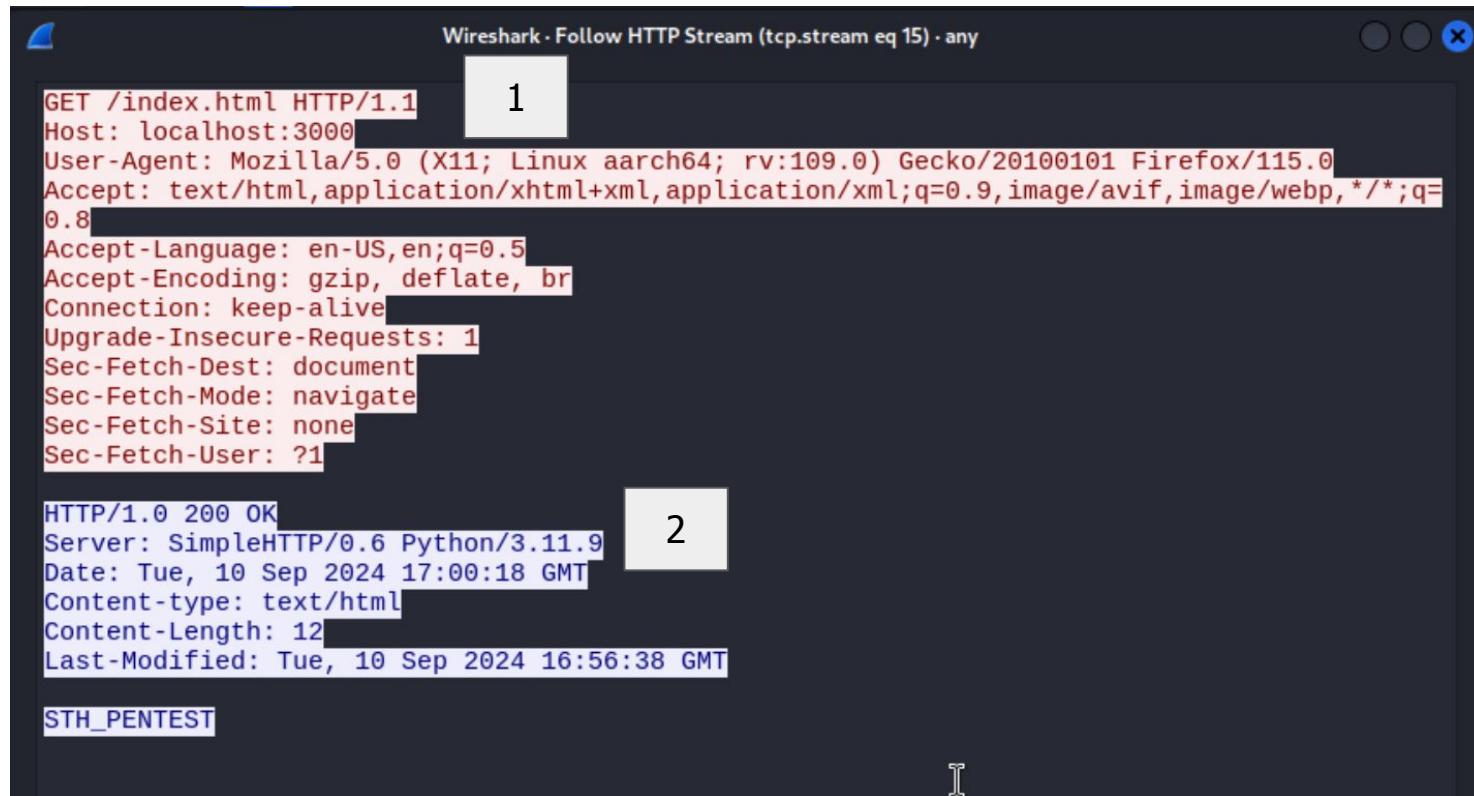
- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**
- http** (Selected)
- No. Time Source Destination Protocol Length Info**
- Packets:
 - 8 2.769905203 127.0.0.1 127.0.0.1 HTTP 555 GET / HTTP/1.1
 - 10 2.771051259 127.0.0.1 127.0.0.1 HTTP 172 HTTP/1.0 304 Not Modified
 - 1 108 40.547168053 127.0.0.1 127.0.0.1 HTTP 515 GET /index.html HTTP/1.1
 - 112 40.550374937 127.0.0.1 127.0.0.1 HTTP 80 HTTP/1.0 200 OK (text/html)
- Conversation Filter**
- Colorize Conversation**
- SCTP**
- Follow**
- Copy**
- Protocol Preferences**
- Decode As...**
- Show Packet in New Window**

Numbered callouts:

- 1: Points to the number 1 in the list of options.
- 2: Points to the number 2 in the list of options.
- 3: Points to the number 3 in the list of options.

Follow HTTP Stream

ขอหน้าเว็บ
ตอบกลับหน้าเว็บ



Wireshark - Follow HTTP Stream (tcp.stream eq 15) · any

1

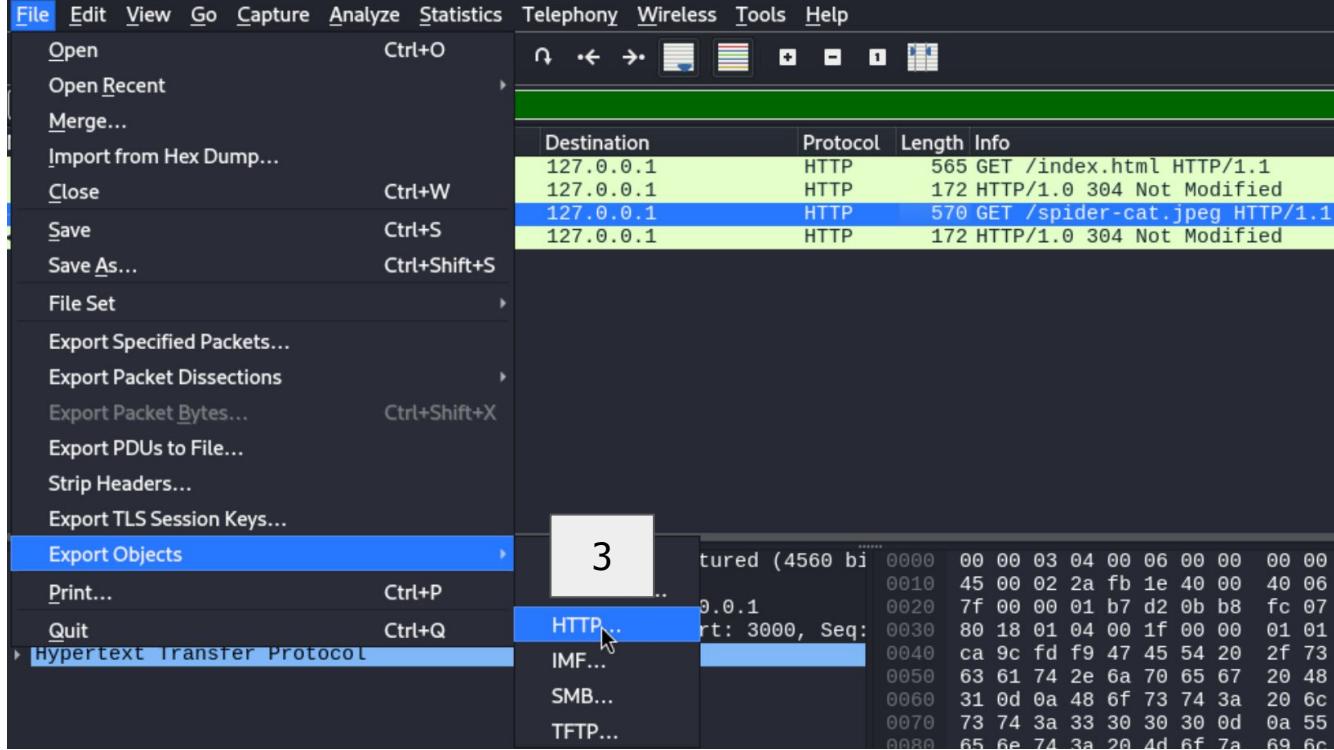
```
GET /index.html HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

2

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.11.9
Date: Tue, 10 Sep 2024 17:00:18 GMT
Content-type: text/html
Content-Length: 12
Last-Modified: Tue, 10 Sep 2024 16:56:38 GMT
STH_PENTEST
```

Export Objects

1



The screenshot shows the Wireshark application interface. The 'File' menu is open, highlighting the 'Export Objects' option. A sub-menu is displayed under 'Export Objects' with several options: Print..., Hypertext Transfer Protocol (HTTP), IMF..., SMB..., and TFTP... . The 'HTTP' option is currently selected. In the background, the main window displays a list of network packets. The first four packets are highlighted in green, indicating they are selected for export.

Destination	Protocol	Length	Info
127.0.0.1	HTTP	565	GET /index.html HTTP/1.1
127.0.0.1	HTTP	172	HTTP/1.0 304 Not Modified
127.0.0.1	HTTP	570	GET /spider-cat.jpeg HTTP/1.1
127.0.0.1	HTTP	172	HTTP/1.0 304 Not Modified

2

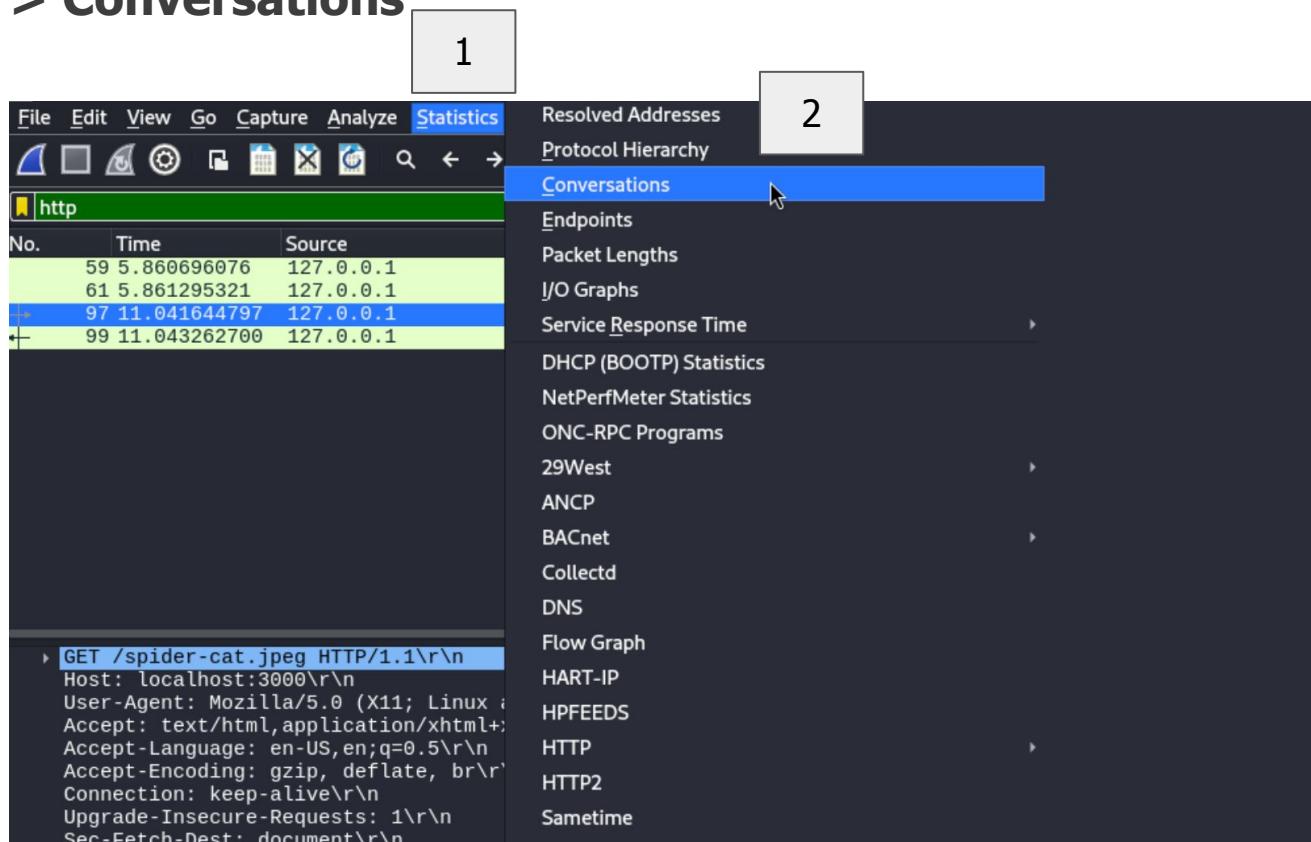
3

Statistics > Conversations

คำถาม:

ถ้าในไฟล์ PCAP มี 1 ล้าน Network Packet
เราจะวิเคราะห์ ภาพรวมเบื้องต้นยังไง?

Statistics > Conversations



The screenshot shows the Wireshark interface with the 'Statistics' menu open. The 'Conversations' option is highlighted with a blue selection bar. A large gray box labeled '1' covers the main window area, and another gray box labeled '2' covers the 'Conversations' submenu.

File Edit View Go Capture Analyze Statistics

Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graphs
Service Response Time
DHCP (BOOTP) Statistics
NetPerfMeter Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime

No. Time Source
59 5.860696076 127.0.0.1
61 5.861295321 127.0.0.1
+ 97 11.041644797 127.0.0.1
- 99 11.043262700 127.0.0.1

```
GET /spider-cat.jpeg HTTP/1.1\r\nHost: localhost:3000\r\nUser-Agent: Mozilla/5.0 (X11; Linux ; rv:109.0) Gecko/20100101 Firefox/109.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate, br\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nSec-Fetch-Dest: document\r\nSec-Fetch-Mode: navigate\r\nSec-Fetch-Site: none\r\nSec-Fetch-User: ?1\r\n\r\n
```

Statistics > Conversations

Wireshark - Conversations - any

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

Capturing from eth0

Statistics Telephony Wireless Tools Help

Capture File Properties Ctrl+Alt+Shift+C

Resolved Addresses

Protocol Hierarchy

Conversations

Endpoints

Packet Lengths

I/O Graphs

Service Response Time

DHCP (BOOTP) Statistics

NetPerfMeter Statistics

ONC-RPC Programs

29West

ANCP

BACnet

Collectd

DNS

Flow Graph

HART-IP

HPFEEDS

HTTP

HTTPS

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	2809	100.0	333527
Ethernet	100.0	2809	1.2	40468
Internet Protocol Version 6	0.0	1	0.0	40
Internet Control Message Protocol v6	0.0	1	0.0	8
Internet Protocol Version 4	99.9	2806	1.7	56120
User Datagram Protocol	55.2	1550	0.4	12400
QUIC IETF	51.7	1452	44.8	1492846
Domain Name System	3.5	98	0.2	6830
Transmission Control Protocol	44.7	1256	52.0	1733057
Transport Layer Security	14.8	417	56.1	1871147
Hypertext Transfer Protocol	0.1	4	0.1	1711
Line-based text data	0.1	2	0.0	175
Address Resolution Protocol	0.1	2	0.0	74

Statistics

คำถาม:

ถ้าในไฟล์ PCAP มี 1 ล้าน Network Packet
เราจะวิเคราะห์ ภาพรวมเบื้องต้นยังไง?

คำตอบ:

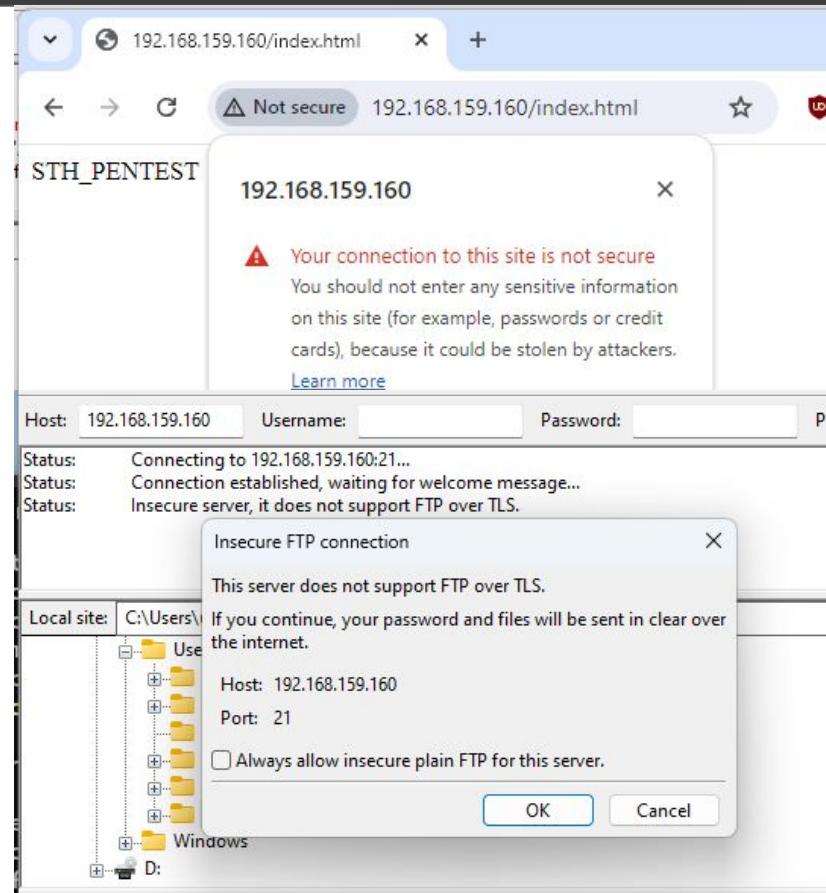
ใช้เมนู Statistics ของ Wireshark ช่วย!

Plaintext Protocol - ส่งข้อมูลที่ไม่เข้ารหัส

ตัวอย่าง Plaintext Protocol เช่น

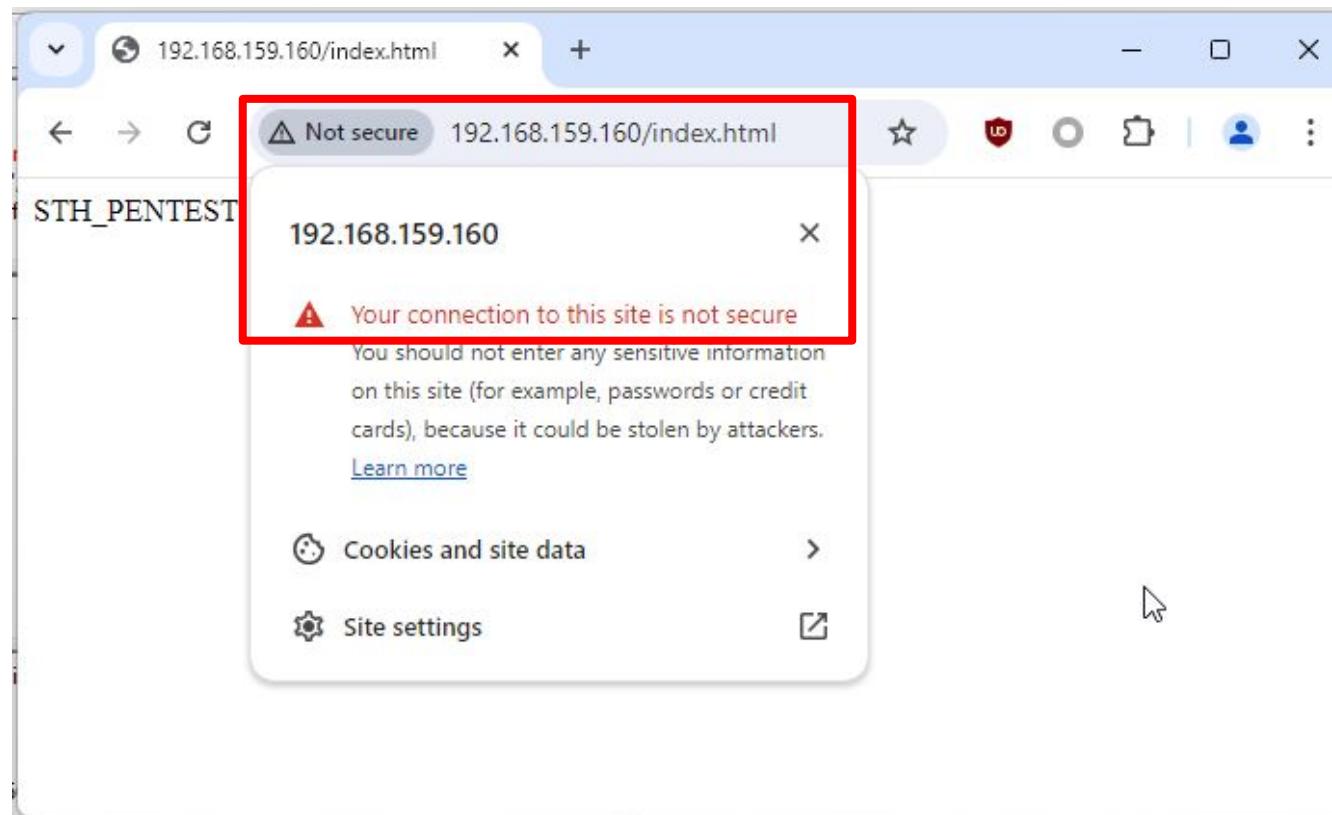
- **HTTP (Hypertext Transfer Protocol)**
ใช้ส่งข้อมูลการเข้าใช้งานเว็บ
- **FTP (File Transfer Protocol)**
ใช้รับ-ส่งข้อมูล การโอนไฟล์
- **Telnet**
ใช้เชื่อมต่อไปยังการที่คอมพิวเตอร์เครื่องอื่น
- **SMTP (Simple Mail Transfer Protocol)**
ใช้ในการส่งอีเมล

ส่งข้อมูลไม่เข้ารหัส
==
ไม่ปลอดภัย
เพราะอาจโดนดักอ่านได้ !



ลองวิเคราะห์ข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

HTTP Protocol



LAB ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark



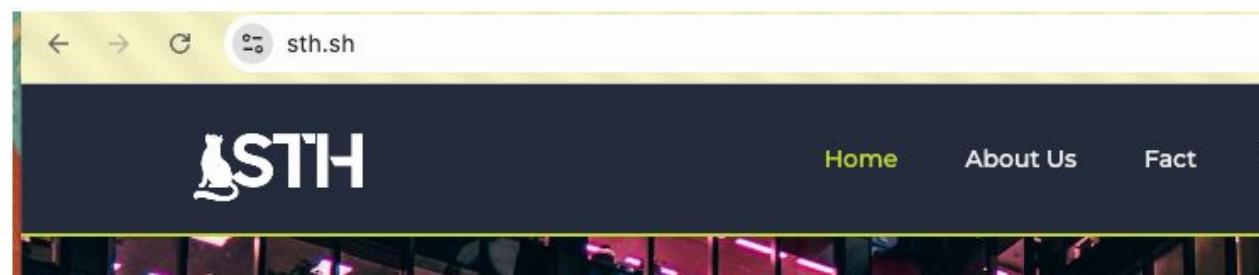
STH Pentest Services

- [Services](#)
- [About Us](#)
- [Contact](#)

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

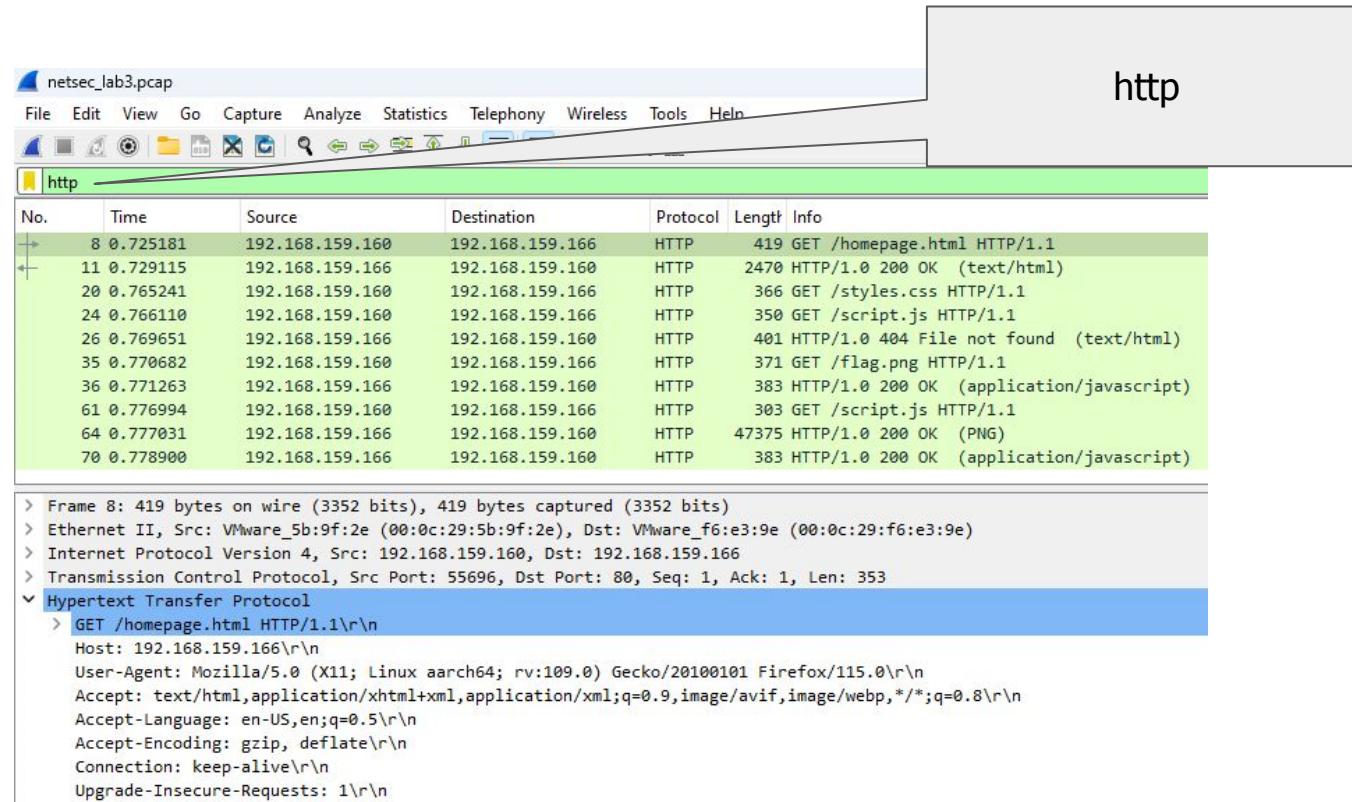
Your Trusted Partner in Cybersecurity

We provide top-tier penetration testing services to protect your digital assets.



ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

Filter



The screenshot shows the Wireshark interface with the following details:

- File Menu:** netsec_lab3.pcap, File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help, and various icons for file operations.
- Protocol Filter:** http (highlighted by a curly brace).
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info.
- Captured Packets:** A list of 12 captured packets, all of which are of the HTTP protocol. The first few rows are:
 - Frame 8: 0.725181 192.168.159.160 192.168.159.166 HTTP 419 GET /homepage.html HTTP/1.1
 - Frame 11: 0.729115 192.168.159.166 192.168.159.166 HTTP 2470 HTTP/1.0 200 OK (text/html)
 - Frame 20: 0.765241 192.168.159.160 192.168.159.166 HTTP 366 GET /styles.css HTTP/1.1
- Selected Packet:** Frame 8 is selected, showing its details:
 - Frame 8: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits)
 - Ethernet II, Src: VMware_5b:9f:2e (00:0c:29:5b:9f:2e), Dst: VMware_f6:e3:9e (00:0c:29:f6:e3:9e)
 - Internet Protocol Version 4, Src: 192.168.159.160, Dst: 192.168.159.166
 - Transmission Control Protocol, Src Port: 55696, Dst Port: 80, Seq: 1, Ack: 1, Len: 353
 - Hypertext Transfer Protocol
 - GET /homepage.html HTTP/1.1\r\nHost: 192.168.159.166\r\nUser-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:109.0) Gecko/20100101 Firefox/115.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n

ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

1

htsec_lab3.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session 2
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

Destination Protocol Length Info

192.168.159.166 HTTP 419 GET /
192.168.159.160 HTTP 2470 HTTP/1.1
192.168.159.166 HTTP 366 GET /
192.168.159.166 HTTP 350 GET /
192.168.159.160 HTTP 401 HTTP/1.1
192.168.159.166 HTTP 371 GET /
192.168.159.160 HTTP 383 GET /
192.168.159.166 HTTP 302 GET /
192.168.159.160 HTTP 473 GET /
192.168.159.160 HTTP 473 GET /

Export Objects
> HTTP ...

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
11	192.168.159.166	text/html	2404 bytes	homepage.html
26	192.168.159.166	text/html	335 bytes	styles.css
36	192.168.159.166	application/javascript	317 bytes	script.js
64	192.168.159.166	image/png	316 kB	flag.png
70	192.168.159.166	application/javascript	317 bytes	script.js

Save

Save All

Preview

Close

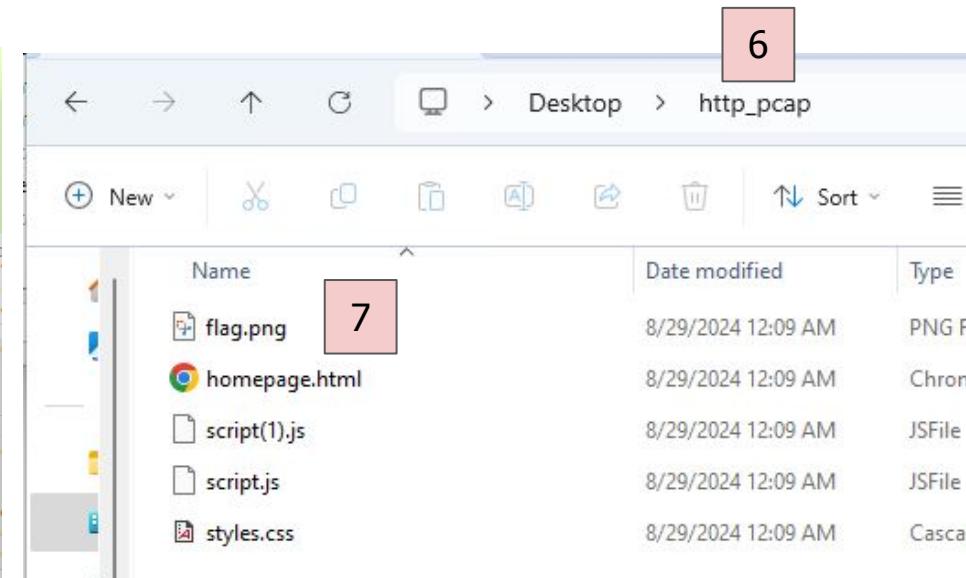
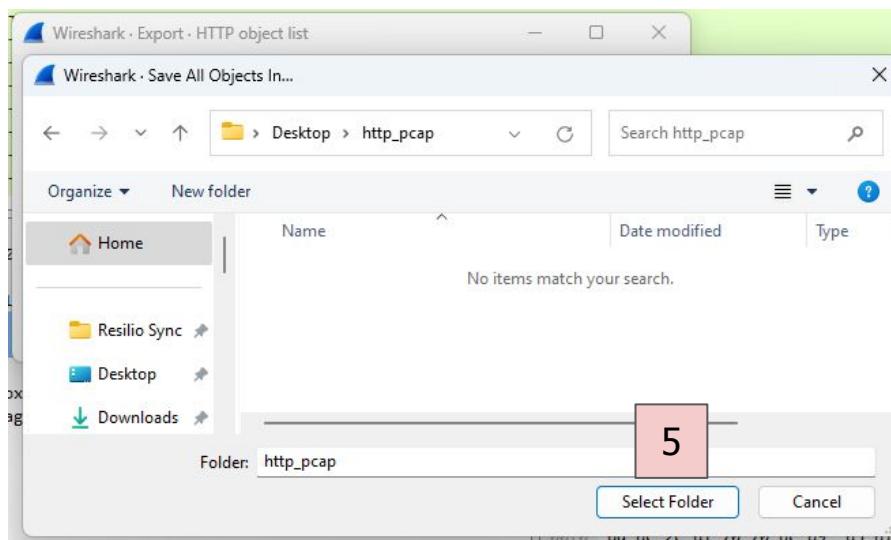
Help

2

3

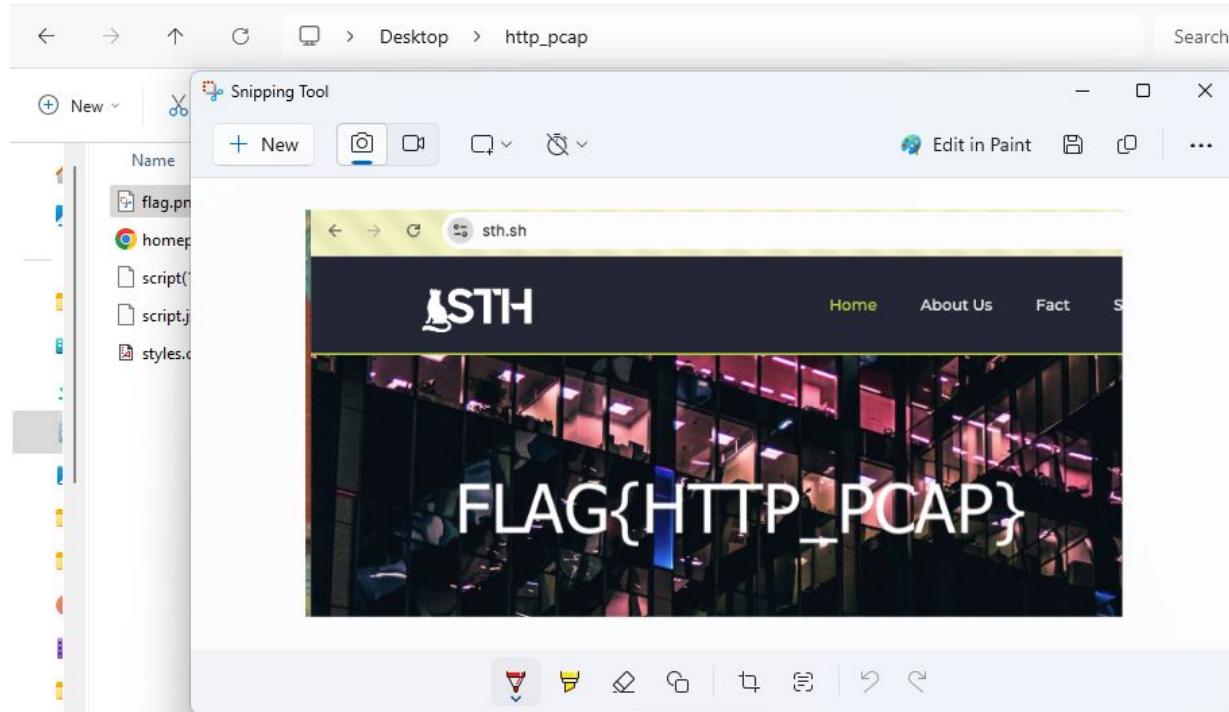
4

ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

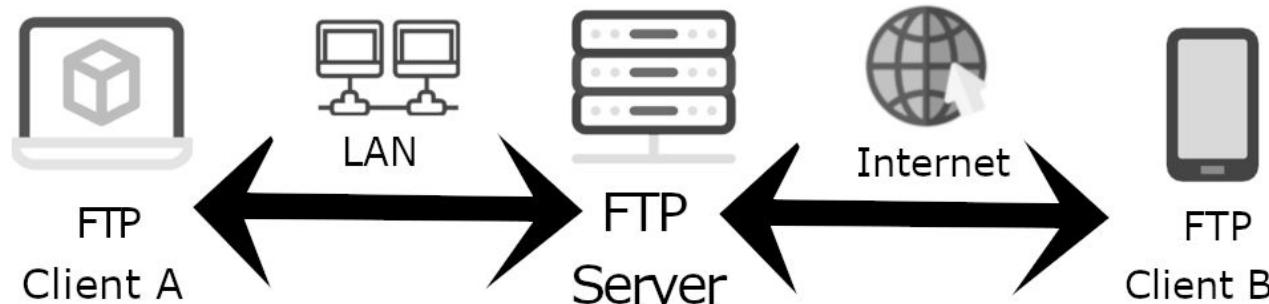


ดักจับข้อมูลที่ส่งผ่าน HTTP Protocol ด้วย Wireshark

8

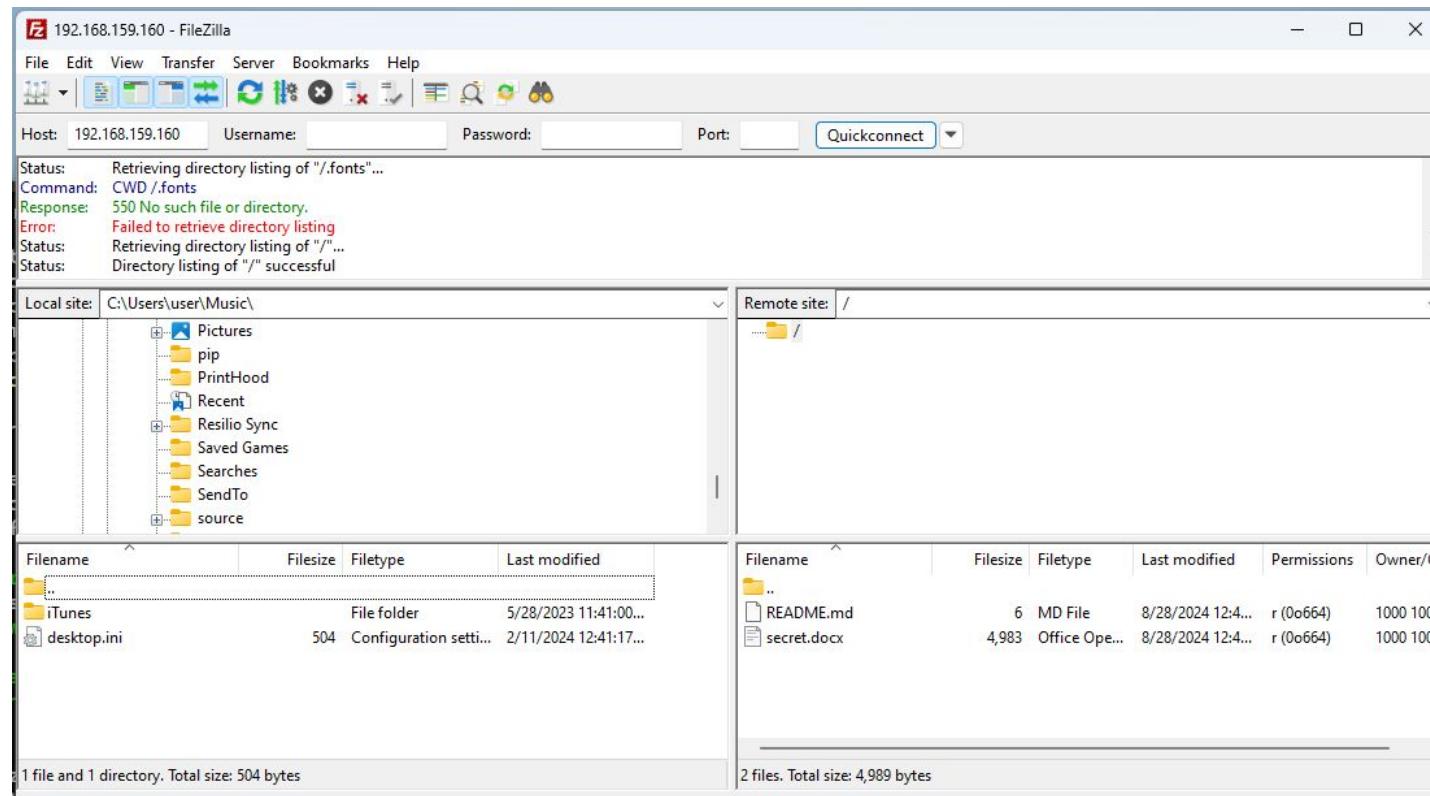


FTP Protocol



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

FTP Protocol - FTP Client



FileZilla 192.168.159.160 - FileZilla

File Edit View Transfer Server Bookmarks Help

Host: 192.168.159.160 Username: Password: Port: Quickconnect

Status: Retrieving directory listing of "./fonts..."
Command: CWD ./fonts
Response: 550 No such file or directory.
Error: Failed to retrieve directory listing
Status: Retrieving directory listing of "/"...
Status: Directory listing of "/" successful

Local site: C:\Users\user\Music\

Remote site: /

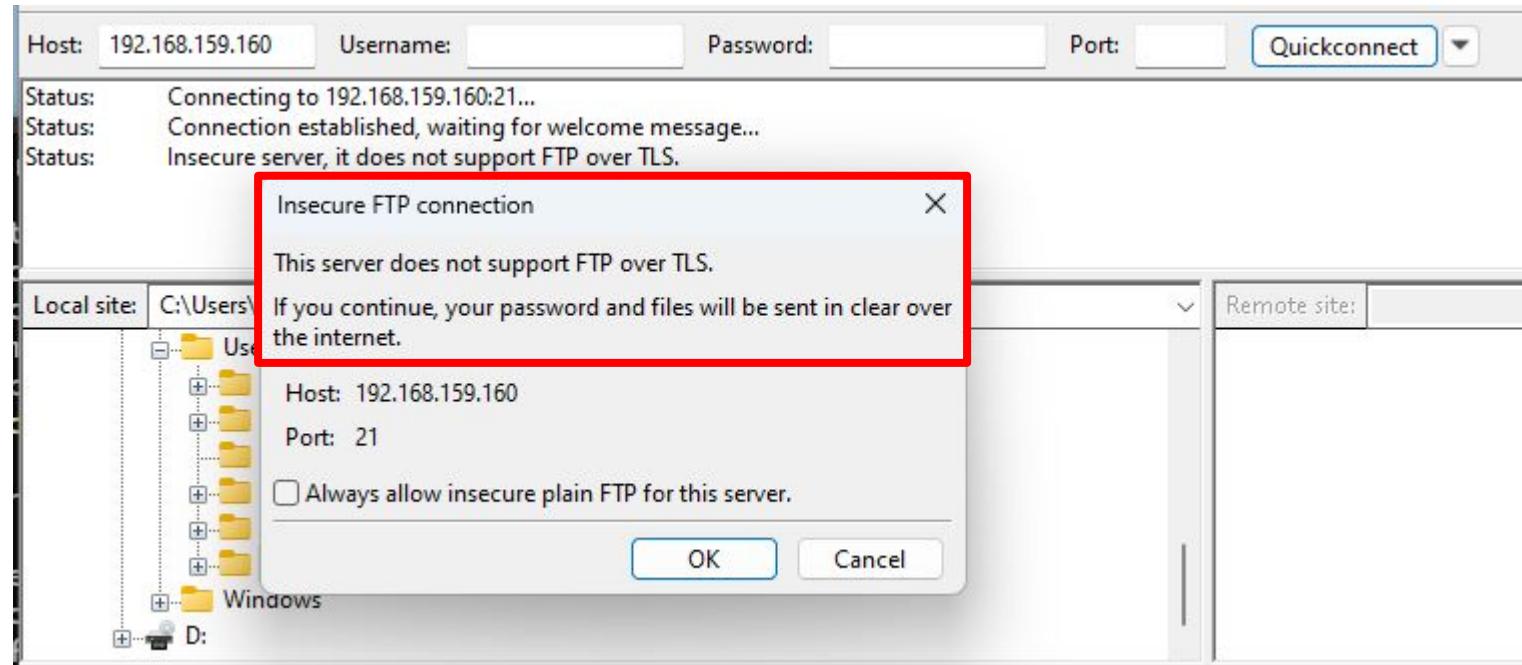
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gr
..					
iTunes		File folder	5/28/2023 11:41:00...		
desktop.ini	504	Configuration setti...	2/11/2024 12:41:17...		

1 file and 1 directory. Total size: 504 bytes

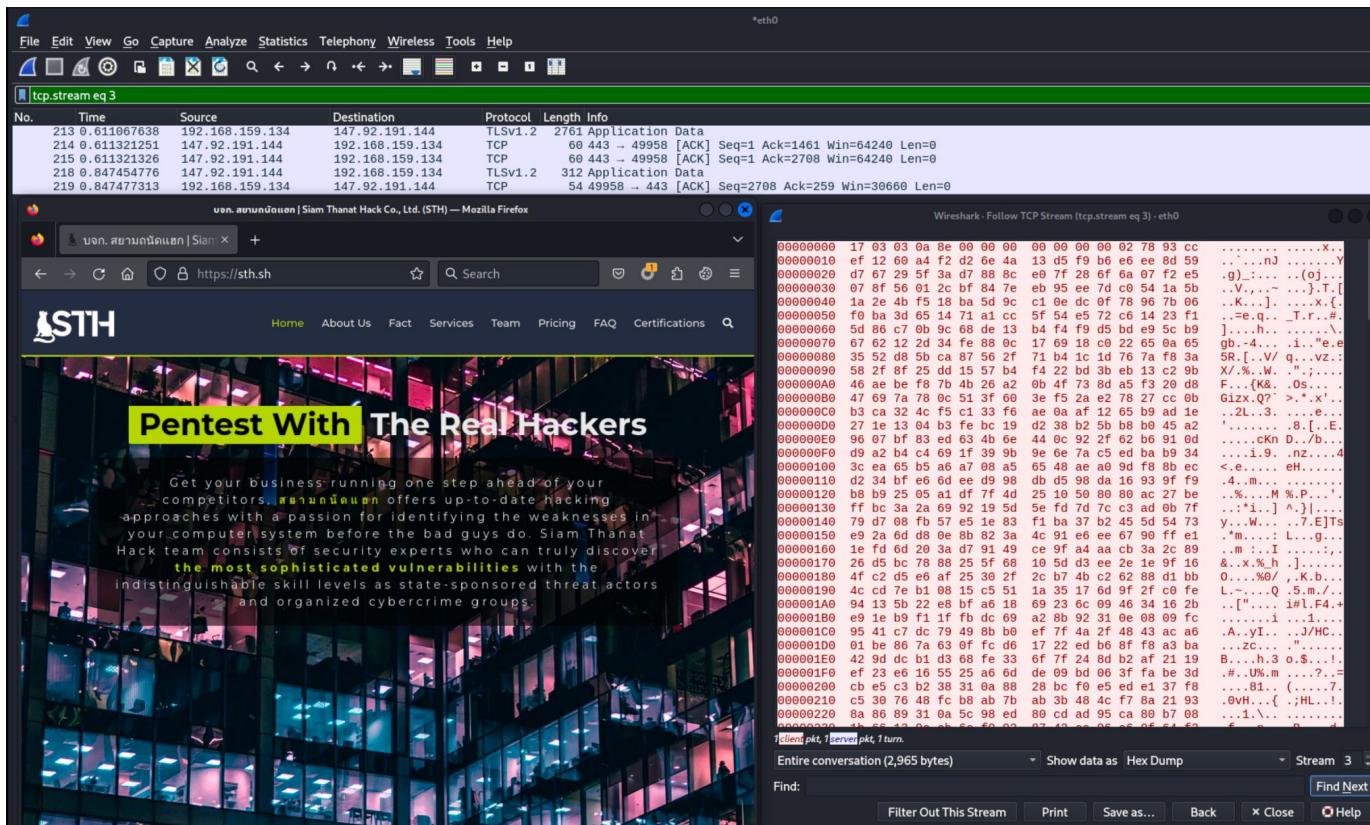
Filename	Filesize	Filetype	Last modified	Permissions	Owner/Gr
..					
README.md	6	MD File	8/28/2024 12:4...	r (0o664)	1000 1000
secret.docx	4,983	Office Ope...	8/28/2024 12:4...	r (0o664)	1000 1000

2 files. Total size: 4,989 bytes

FTP Protocol - FTP Client



Protocol HTTPS ข้อมูลมีการเข้ารหัสด้วย TLS



The screenshot shows a Wireshark capture of an HTTPS session. The top part displays the packet list for 'tcp.stream eq 3' on interface 'eth0'. The bottom part shows the detailed content of the selected TCP stream, which is a Mozilla Firefox browser window displaying the Siam Thanat Hack Co., Ltd. (STH) website. The page content includes a banner for 'Pentest With The Real Hackers' and a paragraph about their services.

No.	Time	Source	Destination	Protocol	Length	Info
213	0.611067638	192.168.159.134	147.92.191.144	TLSv1.2	2761	Application Data
214	0.611321251	147.92.191.144	192.168.159.134	TCP	68	443 - 49958 [ACK] Seq=1 Ack=1461 Win=64240 Len=0
215	0.611321326	147.92.191.144	192.168.159.134	TCP	68	443 - 49958 [ACK] Seq=1 Ack=2708 Win=64240 Len=0
218	0.847454776	147.92.191.144	192.168.159.134	TLSv1.2	312	Application Data
219	0.847477313	192.168.159.134	147.92.191.144	TCP	54	49958 - 443 [ACK] Seq=2708 Ack=259 Win=30660 Len=0

Selected TCP Stream Content:

```

00000000: 17 03 03 0a 8e 00 00 00 00 00 00 02 78 93 cc ..:.:...x..Y
00000020: d7 67 29 5f 3a d7 88 8c e0 7f 28 6f 6a 07 f2 e5 .g.:...o{...V...T.[
00000030: 07 8f 56 01 2c b7 84 7e eb 95 ee 7d c0 54 1a 5b .V.,.-.}.T.[
00000040: 1a 2e 4b f5 18 ba 5d 9c c1 0e dc 0f 78 96 7b 06 ..K.,].x.{...
00000050: f0 ba 3d 65 14 71 a1 cc 5f 54 e5 72 c6 14 23 f1 ..=e.q.._T.r.#.
00000060: 5b 86 c7 0b 9c 68 de 13 b4 f4 f9 5d bd e9 5c b9 ].,.h..,.\\.
00000070: 67 62 12 2d 34 fe 88 0c 17 69 18 c9 22 65 0a 65 gb-.4...i.e.e
00000080: 35 52 5b ca 87 56 2f 71 b4 1c 1d 76 7a f8 3a 5R.[.V/q..v2.:
00000090: 5f 2f 8f 25 dd 15 57 b4 f4 22 bd 3b eb 13 c2 9b X/.%W..";.
000000A0: 46 ae 4b f8 7b 4b 26 a2 0b 4f 73 8d a5 f5 29 d8 F..{K&.l.0s...
000000B0: 47 69 7a 78 0c 51 3f 60 3a f5 2a e2 78 27 cc 0b G!zx.Q?>.*x...
000000C0: ca 32 3c f5 c1 33 f6 a0 0a ad 12 65 b9 ad 1e ..2L..3...e...
000000D0: 27 1e 13 04 b3 fe bc 19 d2 38 b2 5b b8 b9 45 a2 '.....8.[..E.
000000E0: 99 07 bf 83 ed 63 4b 6e 44 0c 92 2f 62 b0 91 0d ..ckN D./.b...
000000F0: d2 a2 bc 44 69 1f 39 9b 9e 6e 7a c5 ed ba b9 34 ..i.9..nz...4
00000100: 3e ea 65 b5 a6 07 a8 05 65 48 aa 0d 9b 6b ec <e....eH....
00000110: d3 4b ef 6d ee 09 98 db 5d 98 da 16 93 ff 9f 4.m... .
00000120: bb b9 25 05 a1 df 7f 4d 25 18 50 80 80 ac 27 bb %...M%.P...
00000130: ff bc 3a 2a 69 92 19 5d fa 7d 7c c3 ad 0b 7f ..*:1.]})...
00000140: 79 d7 08 fb 57 e1 83 f1 ba 37 b4 45 5d 54 73 y...W...7.E]...
00000150: e9 2a 6d 08 fe 8b 82 3a 4c 91 ee 67 90 ff e1 .*m...:L...0...
00000160: 1f fd 29 3a 7d 91 49 c9 9f aa cb 3a 2c 89 ..m..:I...;...
00000170: 26 d5 bc 78 88 25 5f 68 10 5d 03 ee 2e 1e 9f 16 ..x.%h...
00000180: 4f c2 65 e6 af 25 39 2f 2c b7 cp 62 88 1b db 0...%@/...K.b...
00000190: 4c cd 7e b1 08 15 c5 51 1a 35 17 6d 9f 2f c0 fe L...-.Q..5.m.//
000001A0: 94 13 5b 22 e8 bf a6 69 23 6c 09 46 34 16 2b ..["...#1.F4+.
000001B0: e9 1e b9 f1 fb dc 69 a2 8b 92 31 0e 08 09 fc .....1...1...
000001C0: 95 41 c7 dc 79 49 b8 bf 7f 4a 2f 48 43 ac a0 ..A.y!..HC...
000001D0: 01 be 86 7a 63 0f fc d6 17 22 ed b6 8f f8 a3 b0 ...zC... .
000001E0: 42 9d 01 b1 d3 68 fe 33 6f 7f 24 8d b2 af 21 19 B...h.3 o$.s...1.
000001F0: ef 23 e6 16 55 25 a6 6d 09 06 3f fa be 3d ..#.U%m...?..=
00000200: cb e5 c3 b2 38 31 0a 88 28 bc f0 e5 ed e1 37 f8 ..81. (.7...
00000210: c9 30 76 48 fc b8 ab 7b 3b 48 4c f7 8a 21 93 ..0VH...(.;HL...
00000220: 8a 86 89 31 0a 95 98 ed 80 cd 95 ca 80 b7 08 ..1...{.P...
00000230: 65 66 12 0a 0b 50 02 07 42 0e 05 06 05 04 f0 ..6...P...

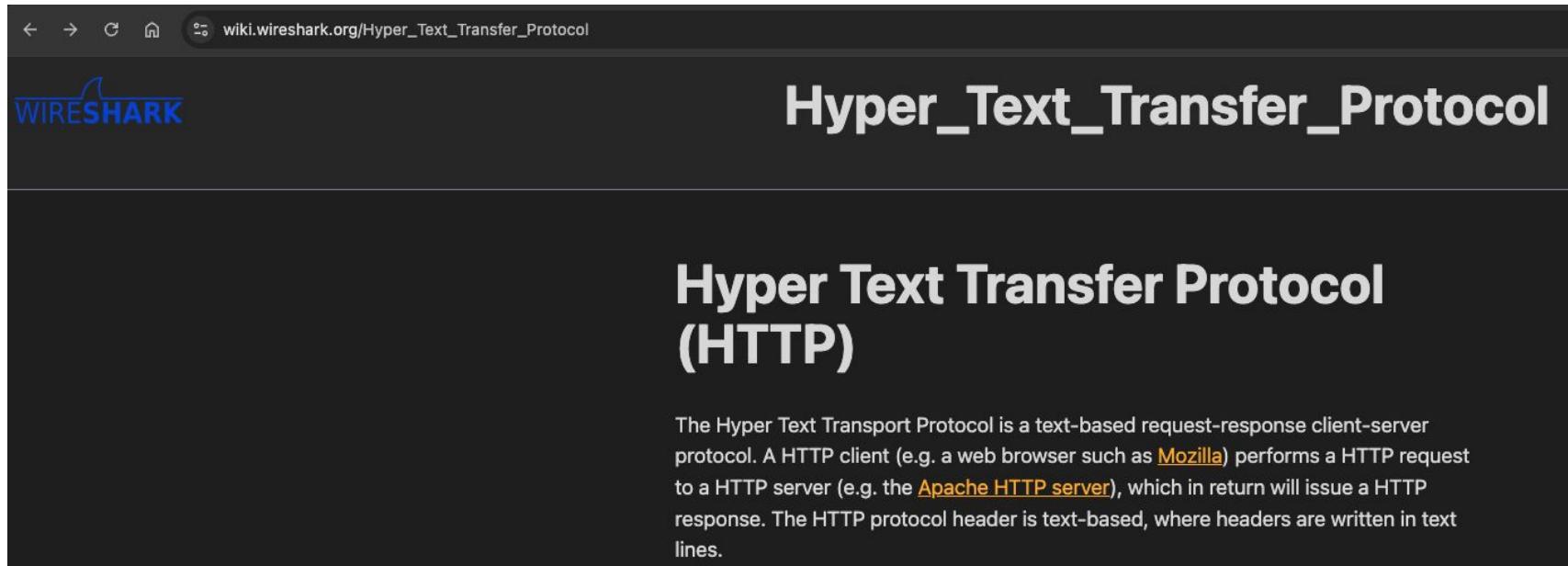
```

Entire conversation (2,965 bytes) Show data as Hex Dump Stream 3 Find Next

ข้อมูลสามารถถูกดัก
และอ่านได้
แต่ถูกเข้ารหัสเอาไว้

ศึกษาเพิ่มเติม

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



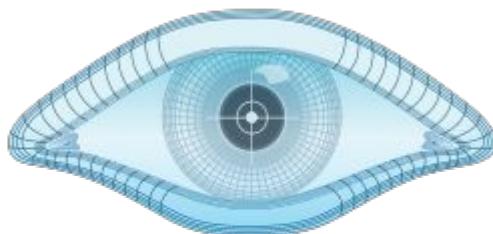
The screenshot shows a web browser window with the URL wiki.wireshark.org/Hyper_Text_Transfer_Protocol in the address bar. The page title is "Hyper_Text_Transfer_Protocol". The main content area displays the following text:

Hyper Text Transfer Protocol (HTTP)

The Hyper Text Transport Protocol is a text-based request-response client-server protocol. A HTTP client (e.g. a web browser such as [Mozilla](#)) performs a HTTP request to a HTTP server (e.g. the [Apache HTTP server](#)), which in return will issue a HTTP response. The HTTP protocol header is text-based, where headers are written in text lines.

What is Nmap?

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



NMAP

```
[~] 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
```

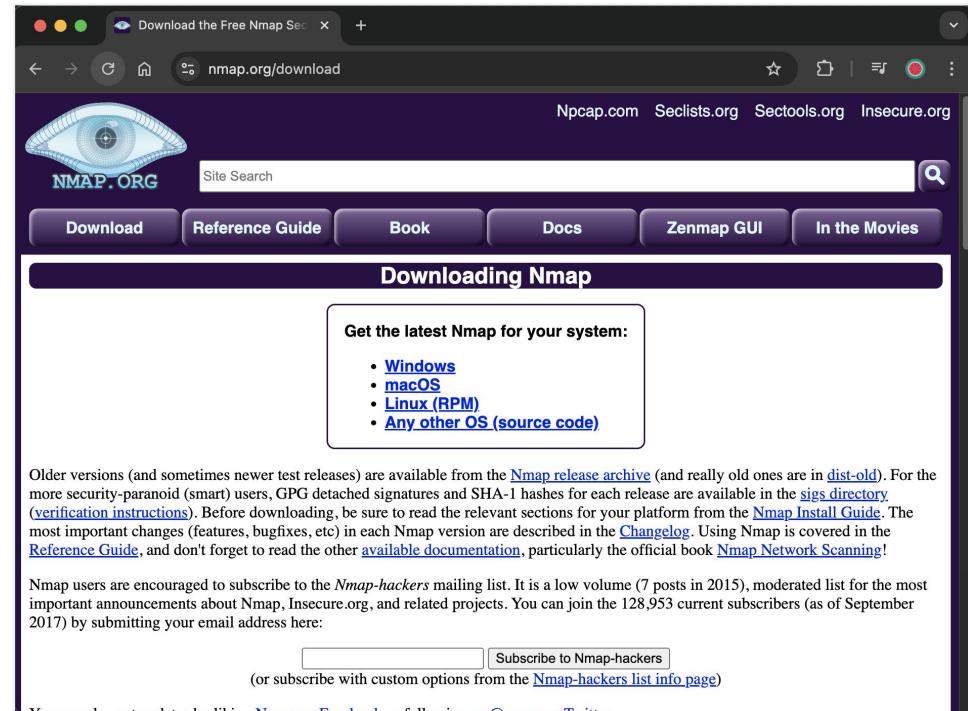
Download

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
```



The screenshot shows the Nmap download page. At the top, there's a navigation bar with links to Npcap.com, Seclists.org, Sectools.org, and Insecure.org. Below the navigation bar is the NMAP.ORG logo with a stylized eye icon. A search bar labeled "Site Search" is present. The main content area has a purple header "Downloading Nmap". Underneath, a box titled "Get the latest Nmap for your system:" lists download links for Windows, macOS, Linux (RPM), and Any other OS (source code). The page also contains a paragraph about older versions and links to the Nmap release archive, verification instructions, and changelog. At the bottom, there's a "Subscribe to Nmap-hackers" button and a note about custom options.

ตัวอย่างการใช้ nmap

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

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

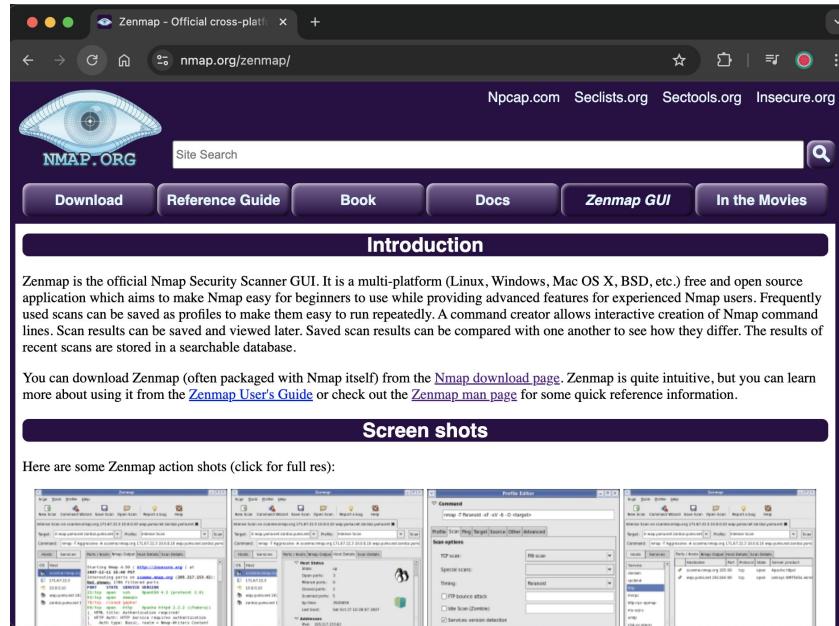
Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     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:~$ █
```

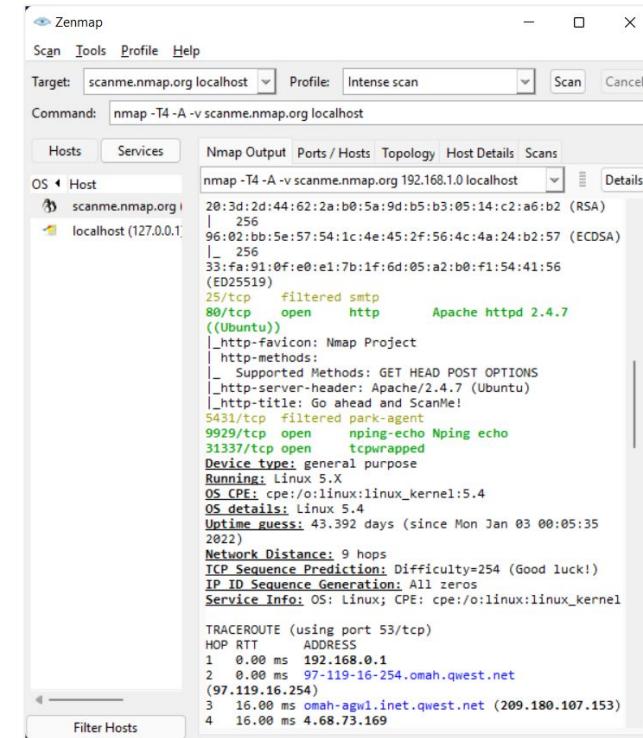
Zenmap สำหรับ Windows

สามารถดาวน์โหลดได้ที่:

<https://nmap.org/download.html#windows>



The screenshot shows the official Zenmap website at nmap.org/zenmap/. The main content area features an eye icon and the text: "Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database." Below this, there's a "Screen shots" section showing three screenshots of the Zenmap interface.



The screenshot shows the Zenmap application window. The "Targets" tab is selected, showing the target "scanme.nmap.org localhost". The "Profile" dropdown is set to "Intense scan". The "Command" field contains "nmap -T4 -A -v scanme.nmap.org localhost". The "Hosts" tab is active, displaying the host "scanme.nmap.org" with IP "192.168.1.0". The "Services" tab shows various open ports: 25 (filtered), 80/tcp (open), 443/tcp (filtered), 9929/tcp (open), 31337/tcp (open). The "Nmap Output" tab displays detailed service information for port 80, including "Apache httpd 2.4.7 (Ubuntu)", "http-favicon: Nmap Project", and "http-methods: GET HEAD POST OPTIONS". Other sections like "Ports / Hosts", "Topology", "Host Details", and "Scans" are also visible.

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!

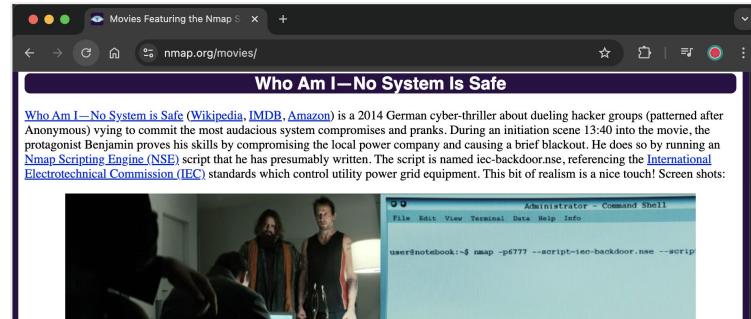
We have all seen many movies like [Hackers](#) which pass off ridiculous 3D animated eye-candy scenes as hacking. So Fyodor [was shocked](#) to think that Trinity does it properly in [The Matrix Reloaded](#). Needing to hack the city power grid, she whips out [Nmap](#) version [2.54BETA25](#), uses it 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:

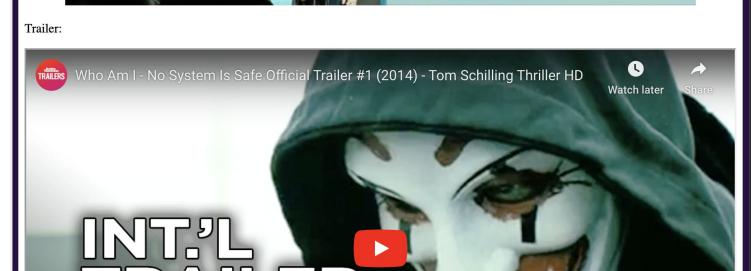
- News articles about the Matrix cameo: [BBC](#), [Slashdot](#), [SecurityFocus](#), [Silicon.Com](#)
- [IWF](#) has added this cracking scene as an [XScreenSaver](#) 4.10 Easter Egg - run 'xmatrix -small -crack'.
- Several people have submitted matrix-themed banners to the [propaganda gallery](#). Feel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



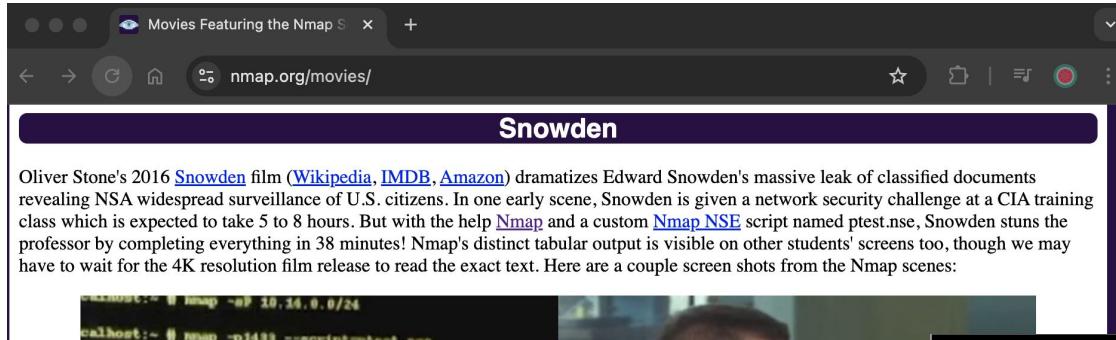
Who Am I—No System Is Safe

[Who Am I—No System is Safe](#) ([Wikipedia](#), [IMDB](#), [Amazon](#)) is a 2014 German cyber-thriller about dueling hacker groups (patterned after Anonymous) vying to commit the most audacious system compromises and pranks. During an initiation scene 13:40 into the movie, the protagonist Benjamin proves his skills by compromising the local power company and causing a brief blackout. He does so by running an [Nmap Scripting Engine \(NSE\)](#) script that he has presumably written. The script is named `iec-backdoor.nse`, referencing the [International Electrotechnical Commission \(IEC\)](#) standards which control utility power grid equipment. This bit of realism is a nice touch! Screen shots:

Trailer:



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:

```
root@kali: ~ # nmap -oF 10.14.0.0/24  
calhost:~ # nmap -p1493 --script=ptest.nse  
calhost:~ # tar cvfj sqlfiles.tar.bz2 /dbdump  
calhost:~ # sudo nmap -oP 10.14.0.0/24  
calhost:~ # tar --extract --file=sqlfiles.tar.bz2 /dbdump  
calhost:~ # bash s
```



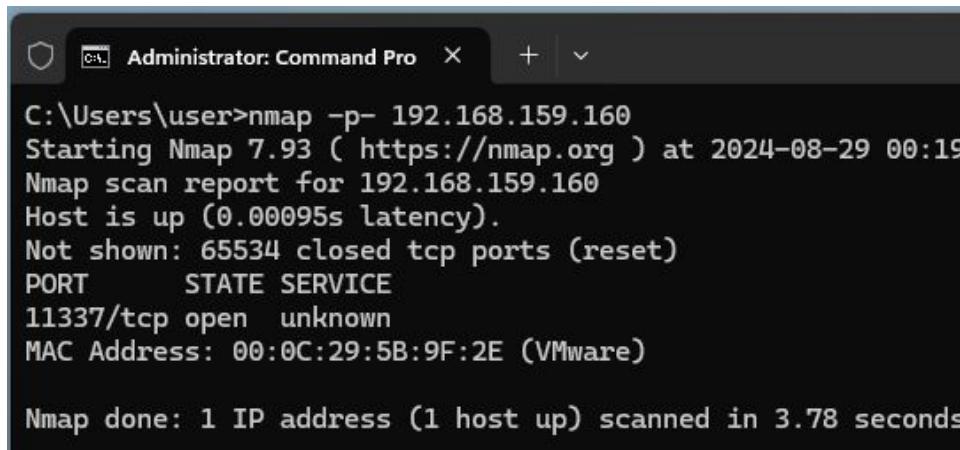
<https://youtu.be/QlSAiI3xMh4>



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

Lab 3 - Nmap Scan High Port

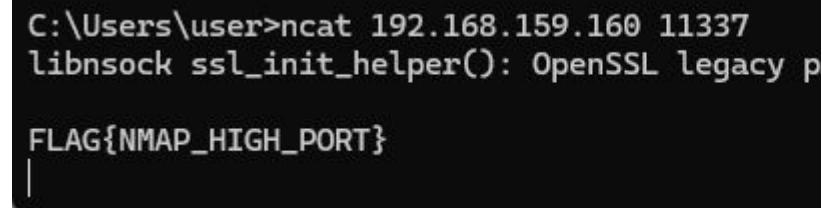
```
C:\> nmap -p- scanme.p7z.pw
```



```
C:\Users\user>nmap -p- 192.168.159.160
Starting Nmap 7.93 ( https://nmap.org ) at 2024-08-29 00:19
Nmap scan report for 192.168.159.160
Host is up (0.00095s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
11337/tcp open  unknown
MAC Address: 00:0C:29:5B:9F:2E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.78 seconds
```

```
C:\> ncat scanme.p7z.pw 11337
```



```
C:\Users\user>ncat 192.168.159.160 11337
libnsock ssl_init_helper(): OpenSSL legacy p
FLAG{NMAP_HIGH_PORT}
|
```

NetworkMiner

NetworkMiner 2.7.3

File Tools Help

-- Select a network adapter in the list --

Anomalies

Hosts (179) Files (287) Images (8) Messages Credentials (4) Sessions (242) DNS (1497) Parameters (4074) Keywords

Sort Hosts On: IP Address (ascending) Sort and Refresh

- 192.168.0.1
- 192.168.0.2 (Linux)
- 192.168.0.50
 - IP: 192.168.0.50
 - MAC: 00606E42B635
 - NIC Vendor: DAVICOM SEMICONDUCTOR, INC.
 - MAC Age: 1998-04-22
 - Hostname:
 - OS: Unknown
 - TTL: 1 (distance: 31)
 - Open TCP Ports:
 - Sent: 205 packets (15,400 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Received: 0 packets (0 Bytes), 0.00% cleartext (0 of 0 Bytes)
 - Incoming sessions: 0
 - Outgoing sessions: 0
 - Host Details
 - Queried DNS names: _pps_tcp local
 - UPnP field : HOST: 239.255.255.250 : 1900

NetworkMiner 2.0

File Tools Help

-- Select a network adapter in the list --

Keywords Anomalies

Hosts (129) Files (131) Images (33) Messages Credentials (2) Sessions (113) DNS (271) Parameters (1199)

Case Panel

Filename	MD5
snot.log...	2f301c2...

Live Sniffing Buffer Usage:



NETRESEC

NetworkMiner

NetworkMiner 2.0

File Tools Help

-- Select a network adapter in the list --

Keywords Anomalies

Hosts (129) Files (131) Images (33) Messages (2) Sessions (113) DNS (271) Parameters (1199)

Filter keyword: Case sensitive

D. port	Protocol	Filename	Extension	Size	Details
TCP 53130	TlsCertificate	nr-data.net.cer	cer	1 203 B	TLS Certificate: C
TCP 53130	TlsCertificate	Geo Trust SSL CA - G2.cer	cer	1 117 B	TLS Certificate: C
TCP 53130	TlsCertificate	GeoTrust Global CA.cer	cer	897 B	TLS Certificate: C
TCP 53138	HttpGetNormal	index.html[2].ocsp-response	ocsp-response	1 455 B	gb symcd.com/
TCP 53139	HttpGetChunked	index.html	html	86 958 B	www.meetup.com
TCP 53142	HttpGetNormal	almond.min.js.javascript	javascript	2 758 B	static2.meetupsta
TCP 53140	HttpGetNormal	meetup_jquery_ui.css	css	6 725 B	static2.meetupsta
TCP 53144	HttpGetNormal	client.min.js.javascript	javascript	3 692 B	static2.meetupsta
TCP 53145	HttpGetNormal	infoWidget.min.js.javascript	javascript	20 639 B	static2.meetupsta
TCP 53151	HttpGetNormal	groupMetadata.min.js.javascript	javascript	2 409 B	static1.meetupsta
TCP 53149	HttpGetNormal	mt-twoButtonCTA+testimonial.css	css	445 B	static1.meetupsta
TCP 53147	HttpGetNormal	print.css	css	2 171 B	static1.meetupsta
TCP 53141	HttpGetNormal	meetup-modem.css	css	223 971 B	static2.meetupsta
TCP 53139	HttpGetNormal	index.html.6D1A30C1.css	css	5 582 B	www.meetup.com
TCP 53146	HttpGetNormal	whitney.css	css	83 455 B	static1.meetupsta
TCP 53150	HttpGetNormal	ghome.min.js.javascript	javascript	102 378 B	static1.meetupsta
TCP 53148	HttpGetNormal	chapterbase.css	css	165 101 B	static1.meetupsta
TCP 53143	HttpGetNormal	Meetup_Base.jquery.min.js.javascript	javascript	414 355 B	static2.meetupsta
TCP 53152	HttpGetNormal	thumb_156167702.jpeg	jpeg	2 611 B	photos3.meetupst
TCP 53156	HttpGetNormal	thumb_151699612.jpeg.PNG	PNG	2 571 B	photos3.meetupst
TCP 53154	Http C/N	... 242000011...PNG	PNG	16 532 B	... 242000011...

Live Sniffing Buffer Usage:

NetworkMiner 2.3

File Tools Help

-- Select a network adapter in the list --

Parameters (36) Keywords Anomalies

Hosts (4) Files Images Messages Credentials (4) Sessions DNS

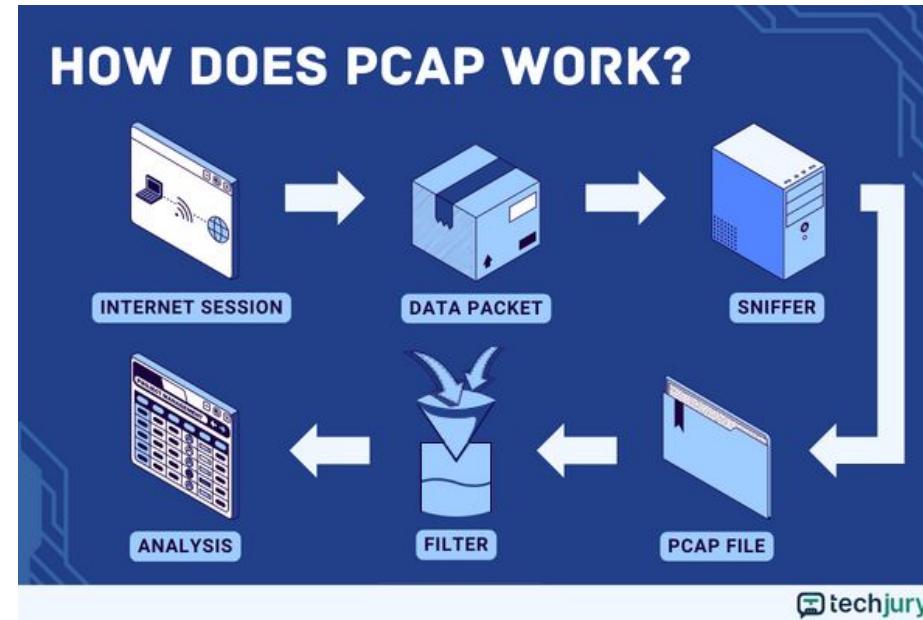
Show Cookies Show NTLM challenge-response Mask Passwords

Client	Server	Protocol	Username	Password
10.144.246.184	10.144.246.161	SNMPv2c	SNMP community	[R0_C@ctl!]
10.144.246.161	10.144.246.184	SNMPv2c	SNMP community	[R0_C@ctl!]
172.31.19.54	172.31.19.73	SNMPv1	SNMP community	public
172.31.19.73	172.31.19.54	SNMPv1	SNMP community	public

Buffered Frames to Parse:

PCAPNG to PCAP

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



ดาวน์โหลดไฟล์แลป

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

The screenshot shows a web browser window with the following details:

- Address bar: https://bootcamp.p7z.pw/2_netsec/
- Navigation icons: back, forward, refresh, search.
- Toolbar links: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-.
- Main content: **Index of /2_netsec/**
- File listing:
 - .. /
 - [netsec_lab1.pcap](#) 14-Sep-2024 02:44
 - [netsec_lab2.pcap](#) 14-Sep-2024 02:44



ลองทำแลป !

Lab 1: วิเคราะห์ HTTP Protocol ใน PCAP

Lab 2: วิเคราะห์ FTP Protocol ใน PCAP

อยากรู้ว่าในชีวิตของคุณ มีสิ่งใดที่ทำให้คุณรู้สึก ไม่ดี ไม่สุข ไม่พอใจ

Agenda (Day 1)

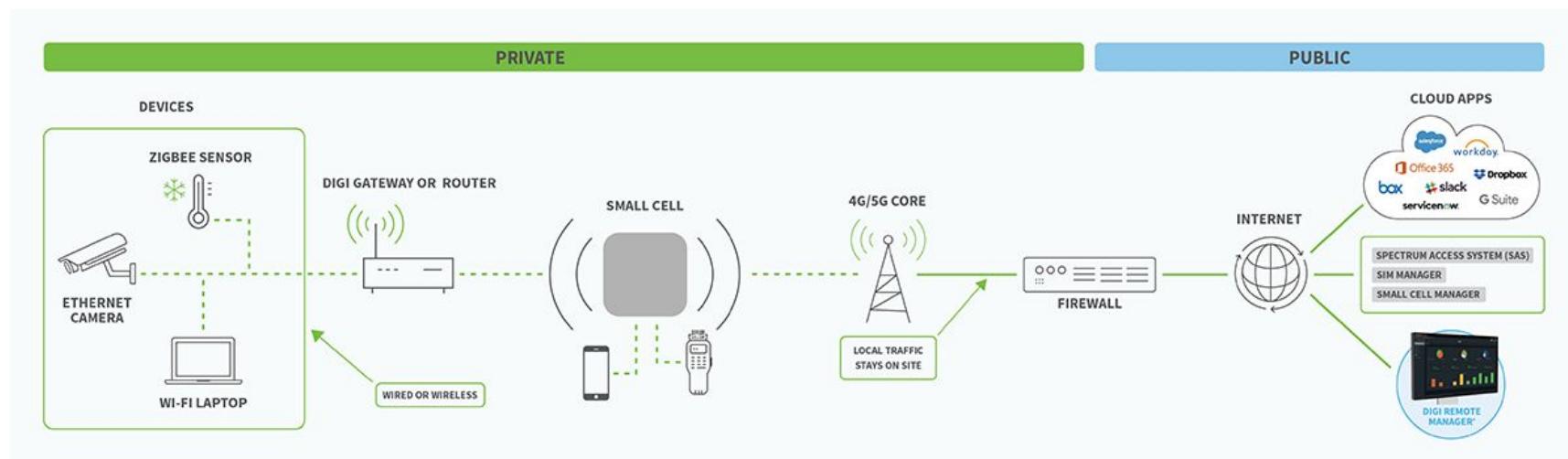
เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00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



Thank you !!

What is Networking

- A private network
- A public network

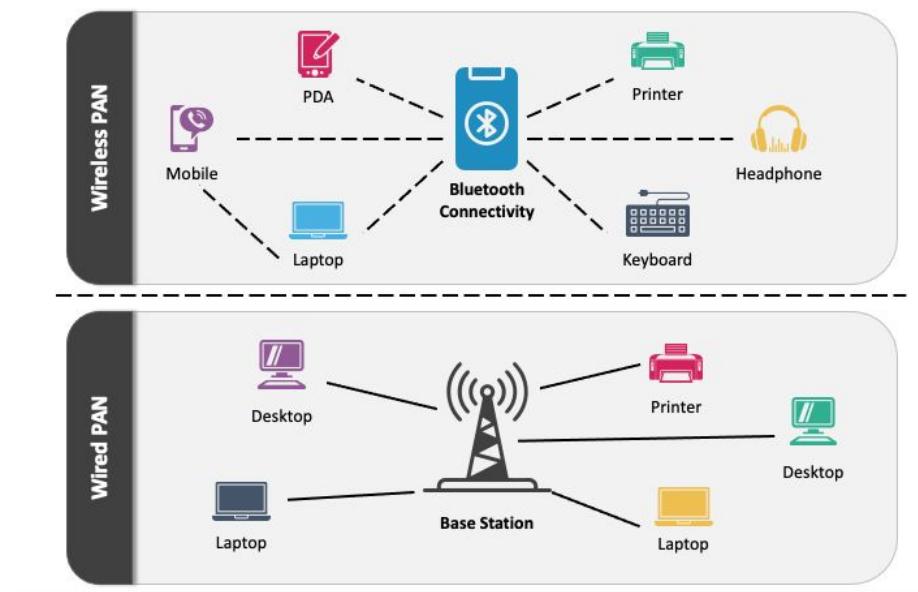


ที่มา: <https://www.digi.com>

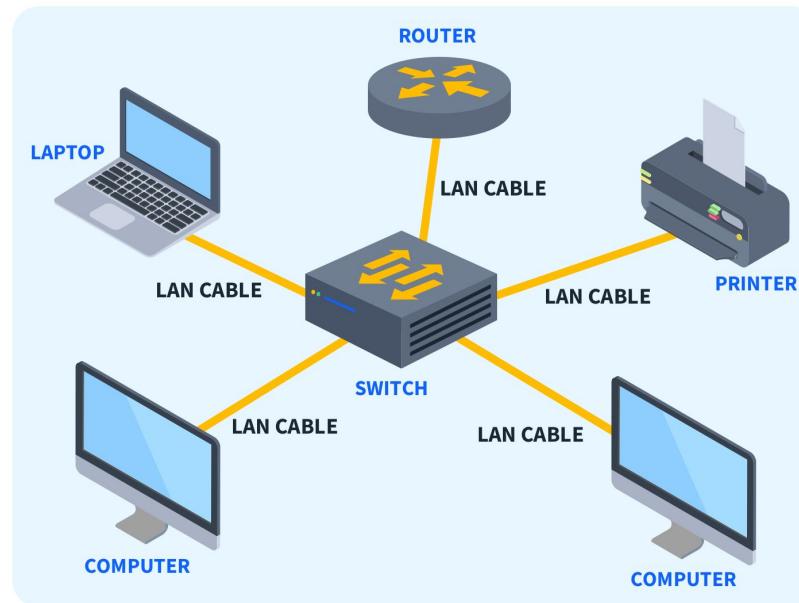
Personal Area Network (PAN)

PERSONAL AREA NETWORK (PAN)

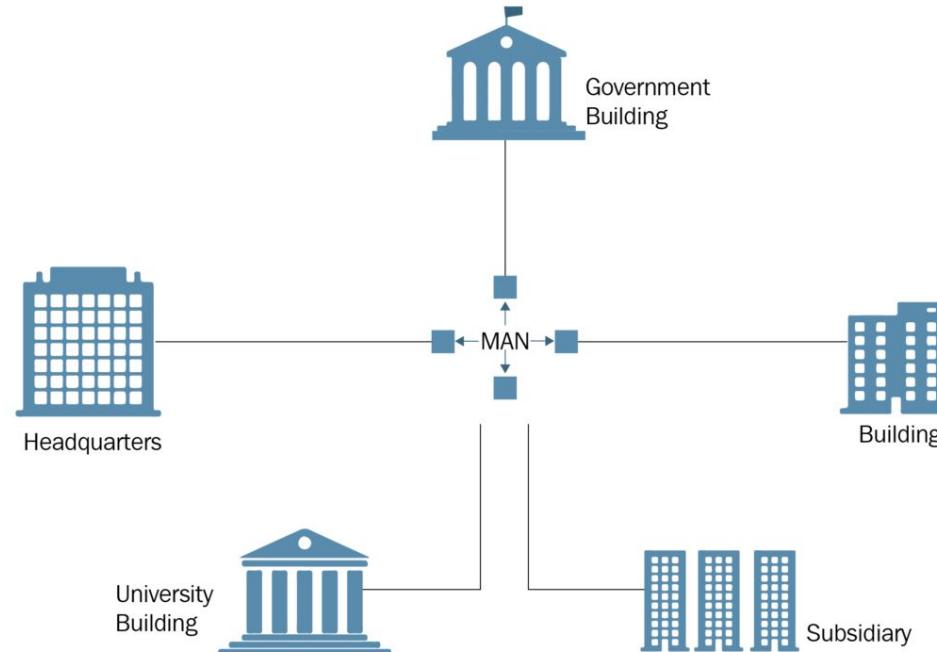
Types of PAN Network



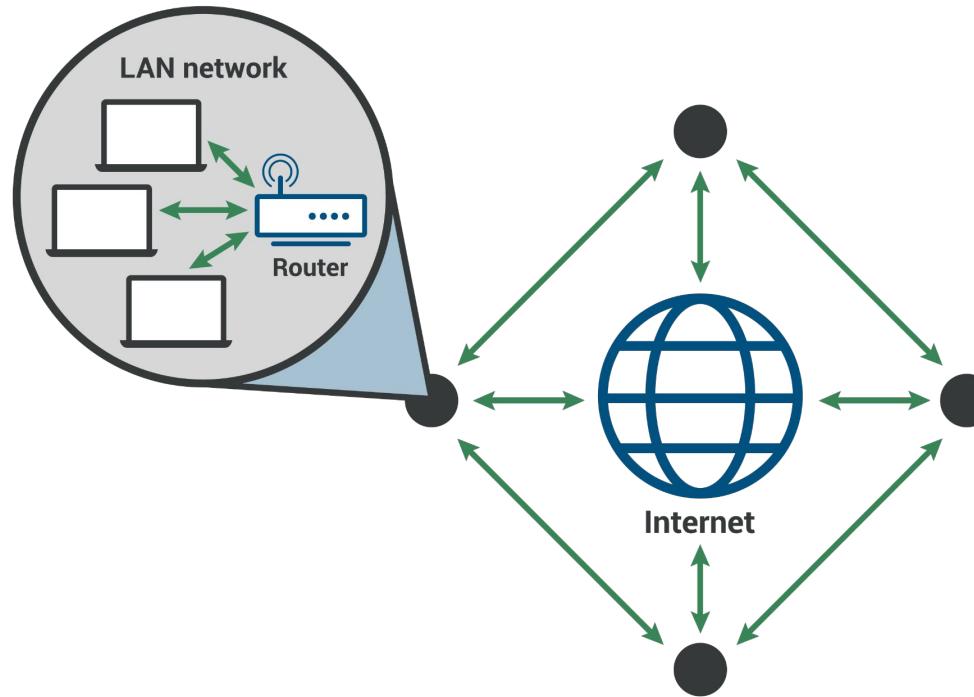
Local Area Network (LAN)



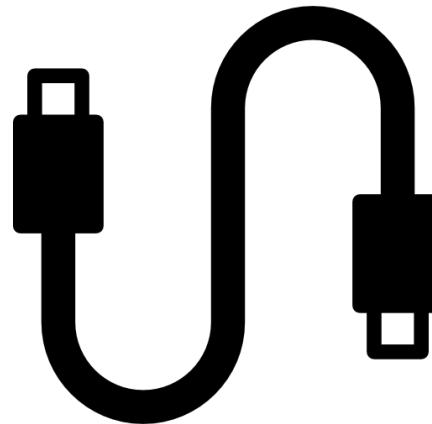
Metropolitan Area Network (MAN)



Wide Area Network (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

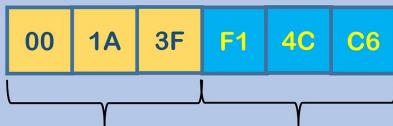


Types of networks

MAC Address

MAC

Media Access Control Address



Organizational Unique Identifier Universally Administered Address

```
Administrator: Command Pro X + ▾
C:\Users\user>ipconfig /all

Windows IP Configuration

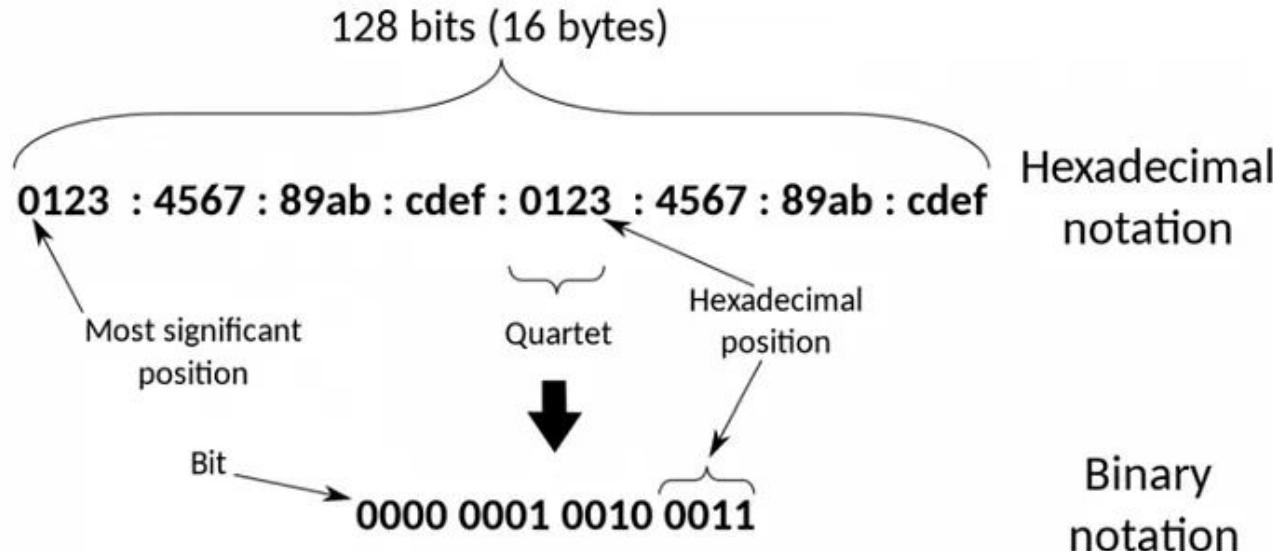
Host Name . . . . . : DESKTOP-UVH08AE
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : localdomain

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:af29:2fd9:4ald%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

IPv6 address



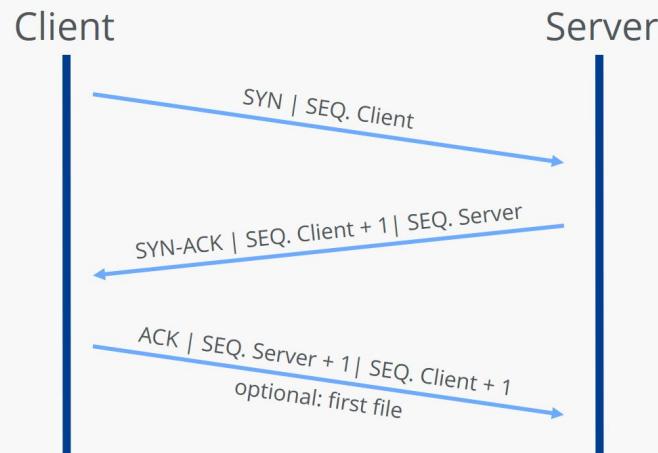
IPv4 Class

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			

TCP

TCP connection establishment (Three way handshake)



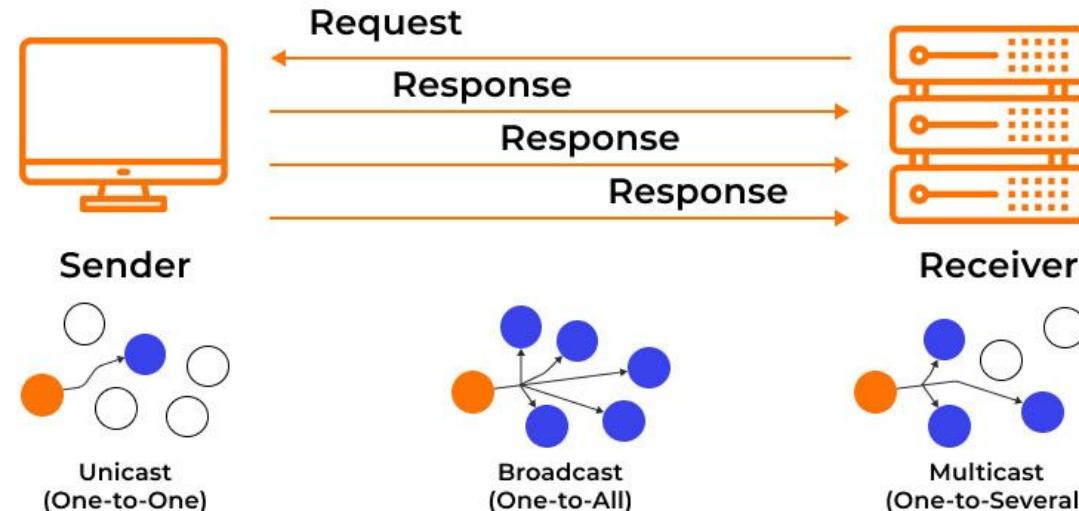
IONOS

SEQ. = Sequence number

UDP

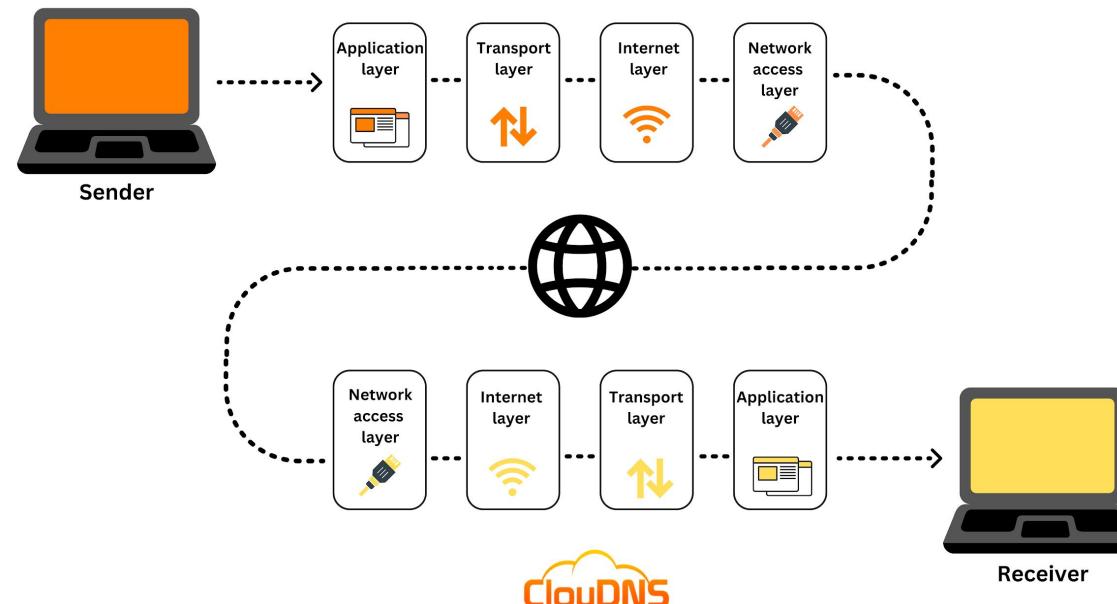


How User Datagram Protocol (UDP) Works

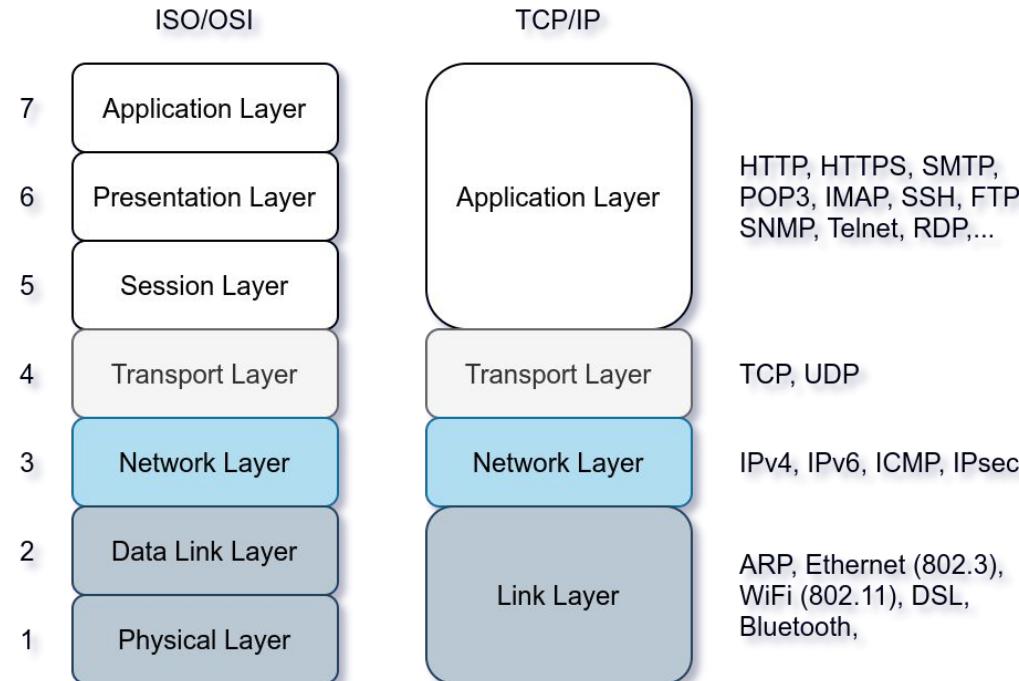


TCP/IP

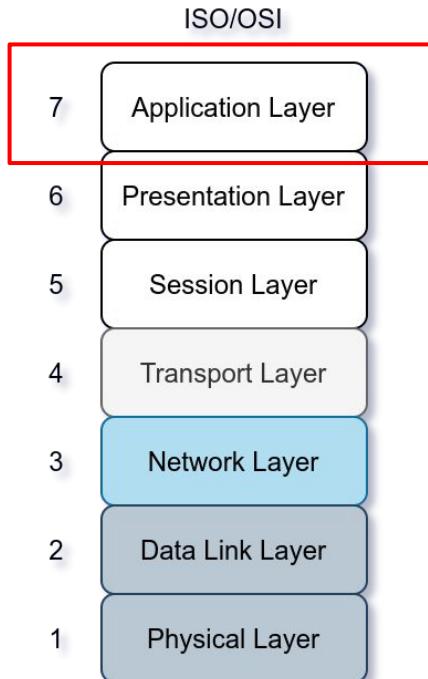
How does TCP/IP work?



OSI Model



Application Protocol



- **HTTP (Hypertext Transfer Protocol)**
ส่งข้อมูลระหว่างเว็บเบราว์เซอร์และเซิร์ฟเวอร์
- **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

```
Command Prompt - nslookup

Simplilearn >nslookup
Default Server: local.airtelfiber.com
Address:

> www.amazon.com
Server: local.airtelfiber.com
Address:

Non-authoritative answer:
Name: d3ag4hukkh62yn.cloudfront.net
Address: 13.224.16.126
Aliases: www.amazon.com
          tp.47cf2c8c9-frontier.amazon.com
```

Network Command

\$ hostname

Command Prompt

```
Simplilearn >hostname  
LAPTOP-
```

```
Simplilearn >
```

\$ ping

Command Prompt

```
Simplilearn >ping www.google.com
```

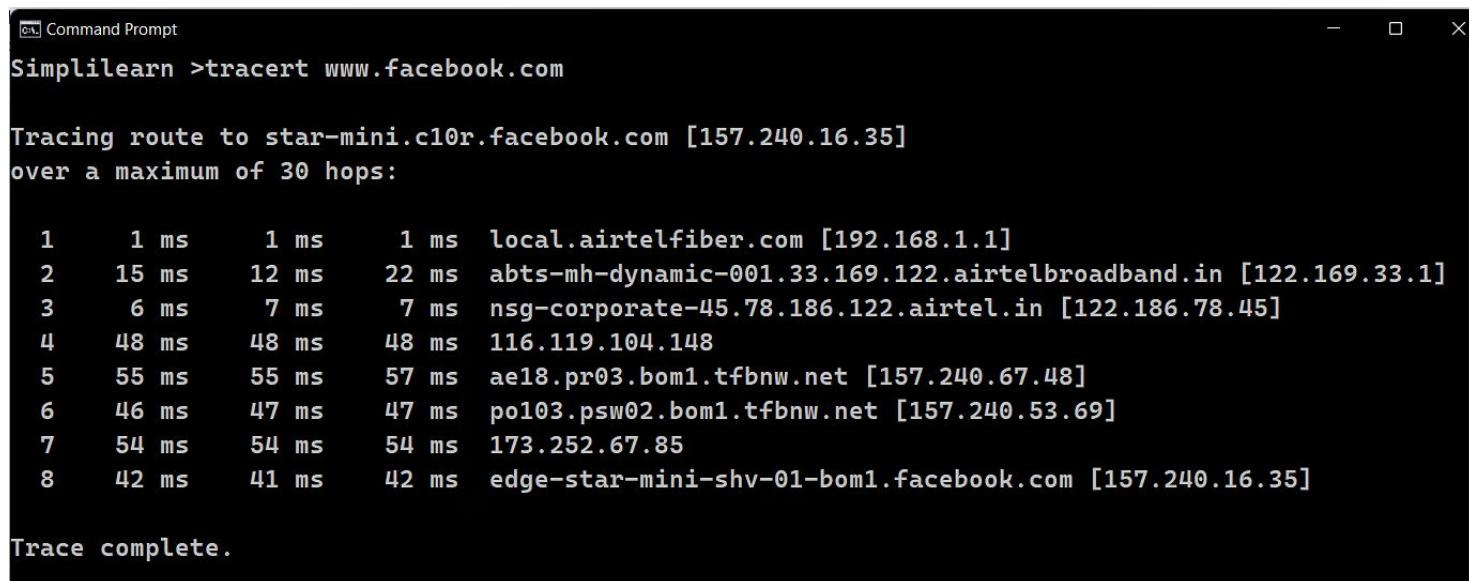
```
Pinging www.google.com [142.250.194.4] with 32 bytes of data:  
Reply from 142.250.194.4: bytes=32 time=26ms TTL=118  
Reply from 142.250.194.4: bytes=32 time=27ms TTL=118  
Reply from 142.250.194.4: bytes=32 time=26ms TTL=118  
Reply from 142.250.194.4: bytes=32 time=27ms TTL=118
```

```
Ping statistics for 142.250.194.4:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 26ms, Maximum = 27ms, Average = 26ms
```

```
Simplilearn >■
```

Network Command

\$ tracert



```
Command Prompt
Simplilearn >tracert www.facebook.com

Tracing route to star-mini.c10r.facebook.com [157.240.16.35]
over a maximum of 30 hops:

 1      1 ms      1 ms      1 ms local.airtelfiber.com [192.168.1.1]
 2     15 ms     12 ms     22 ms abts-mh-dynamic-001.33.169.122.airtelbroadband.in [122.169.33.1]
 3      6 ms      7 ms      7 ms nsg-corporate-45.78.186.122.airtel.in [122.186.78.45]
 4     48 ms     48 ms     48 ms 116.119.104.148
 5     55 ms     55 ms     57 ms ae18.pr03.bom1.tfbnw.net [157.240.67.48]
 6     46 ms     47 ms     47 ms po103.psw02.bom1.tfbnw.net [157.240.53.69]
 7     54 ms     54 ms     54 ms 173.252.67.85
 8     42 ms     41 ms     42 ms edge-star-mini-shv-01-bom1.facebook.com [157.240.16.35]

Trace complete.
```

Network Command

\$ tracert

```
Command Prompt
Simplilearn >systeminfo

Host Name: LAPTOP-SC0CPHSB
OS Name: Microsoft Windows 11 Home Single Edition
OS Version: 10.0.22000.17400
OS Manufacturer: Microsoft Corporation
OS Configuration: Standard
OS Build Type: Multiprocessor Free
Registered Owner: N/A
Registered Organization: N/A
Product ID: 00327-30967-50001-AA01M
Original Install Date: 28-10-2021
System Boot Time: 05-03-2024 00:27:57
System Manufacturer: LENOVO
System Model: 3100
System Type: Desktop PC
Processor(s): 1 Processor(s) Installed.
              Intel(R) Core(TM) i5-13400F CPU @ 2.50GHz
Intel ~1600 Mhz
BIOS Version: C:\WINDOWS\system32\ACPI BIOS
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume3
System Locale: en-us;English (United States)
```

\$ tracert

```
Command Prompt - netstat
Simplilearn >netstat

Active Connections

Proto Local Address          Foreign Address        State
TCP
TCP
TCP
TCP
TCP
TCP
TCP
TCP
```