

Lab 1 - Wireshark

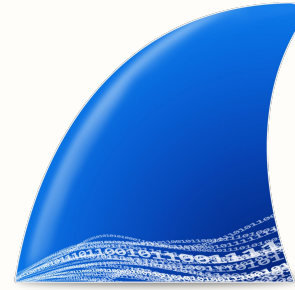
Introduction to Computer Networks

Kuan-Wei Huang(黃冠維), Pei-Chieh Wu (吳沛潔), Cheng-Yuan Jian (簡呈原), Hsiang-Ting Huang (黃湘庭), Pham Ngoc Hoa (范玉花)



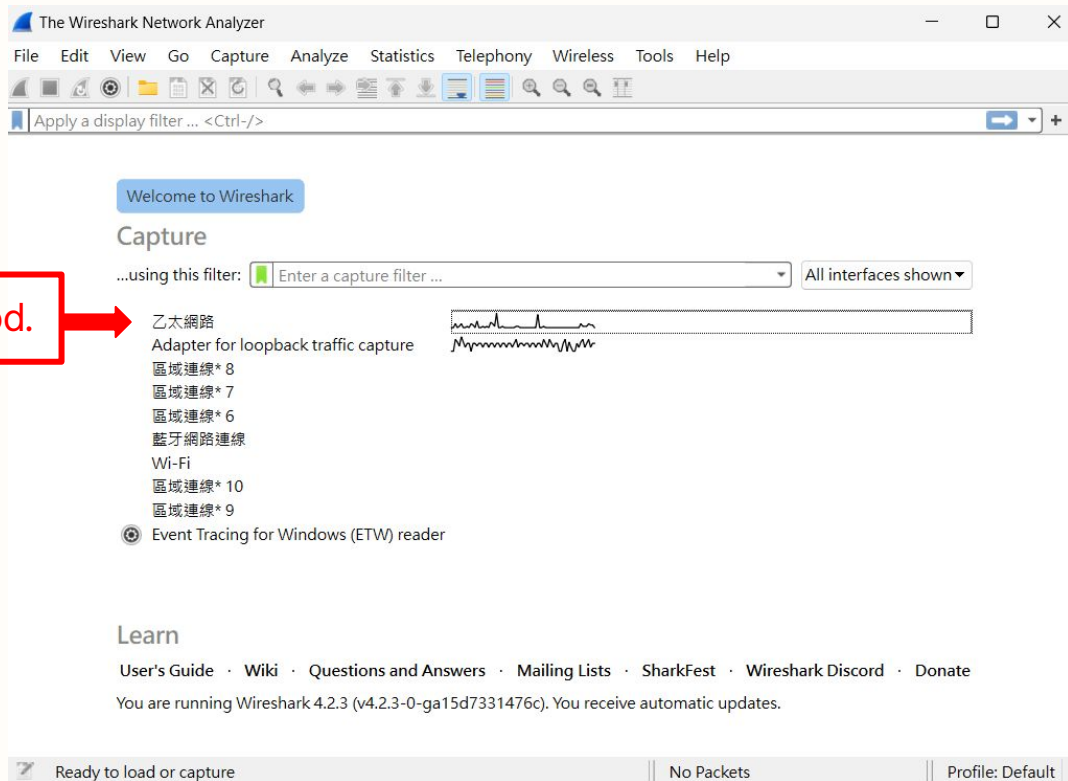
Download and Install

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

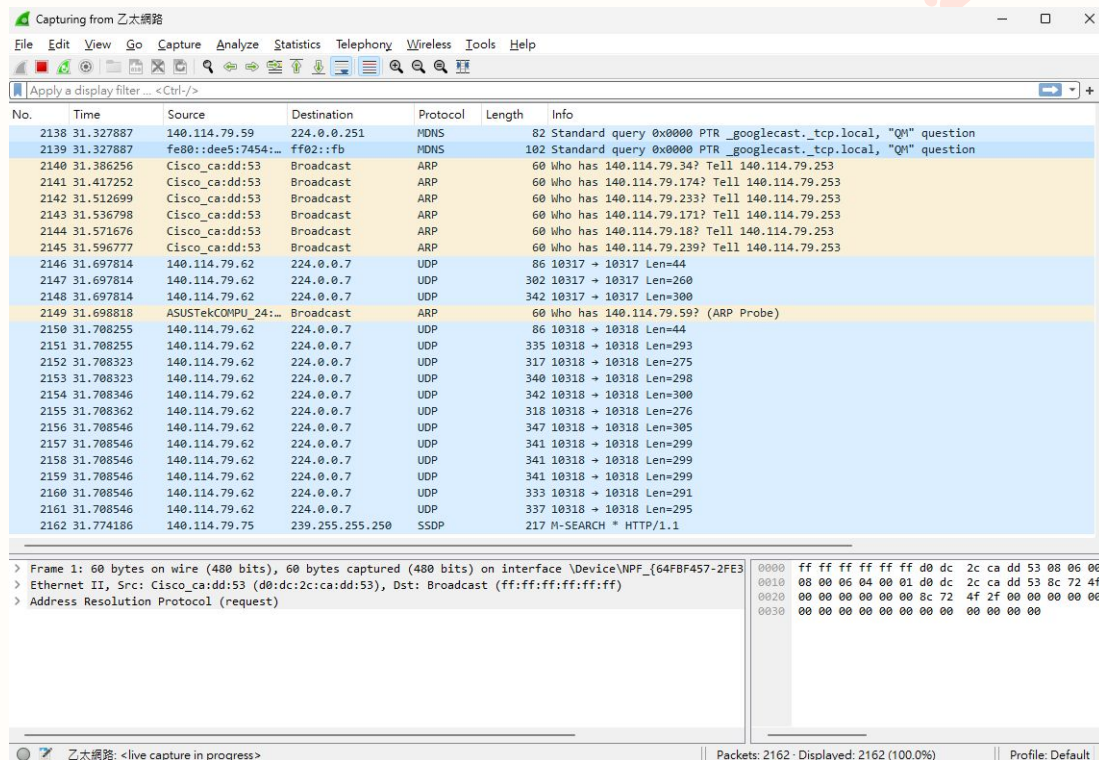


Wireshark: Capture Interface

Choose the connection method.



Wireshark: User Interface



The screenshot displays the Wireshark network protocol analyzer interface. The title bar indicates it is capturing from the network interface '乙太網路' (Ethernet). The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains icons for various functions like opening files, saving, and analyzing. The main display area is divided into three panes. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (Frame 1), including Ethernet II, Source, Destination, and Address Resolution Protocol (request). The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates '乙太網路: <live capture in progress>', 'Packets: 2162 - Displayed: 2162 (100.0%)', and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
2138	31.327887	140.114.79.59	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2139	31.327887	fe80::dee5:7454:...	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
2140	31.386256	Cisco_ca:dd:53	Broadcast	ARP	60	Who has 140.114.79.34? Tell 140.114.79.253
2141	31.417252	Cisco_ca:dd:53	Broadcast	ARP	60	Who has 140.114.79.174? Tell 140.114.79.253
2142	31.512699	Cisco_ca:dd:53	Broadcast	ARP	60	Who has 140.114.79.233? Tell 140.114.79.253
2143	31.536798	Cisco_ca:dd:53	Broadcast	ARP	60	Who has 140.114.79.171? Tell 140.114.79.253
2144	31.571676	Cisco_ca:dd:53	Broadcast	ARP	60	Who has 140.114.79.18? Tell 140.114.79.253
2145	31.596777	Cisco_ca:dd:53	Broadcast	ARP	60	Who has 140.114.79.239? Tell 140.114.79.253
2146	31.697814	140.114.79.62	224.0.0.7	UDP	86	10317 → 10317 Len=44
2147	31.697814	140.114.79.62	224.0.0.7	UDP	302	10317 → 10317 Len=260
2148	31.697814	140.114.79.62	224.0.0.7	UDP	342	10317 → 10317 Len=300
2149	31.698818	ASUSTekCOMPU_24:...	Broadcast	ARP	60	Who has 140.114.79.59? (ARP Probe)
2150	31.708255	140.114.79.62	224.0.0.7	UDP	86	10318 → 10318 Len=44
2151	31.708255	140.114.79.62	224.0.0.7	UDP	335	10318 → 10318 Len=293
2152	31.708323	140.114.79.62	224.0.0.7	UDP	317	10318 → 10318 Len=275
2153	31.708323	140.114.79.62	224.0.0.7	UDP	340	10318 → 10318 Len=298
2154	31.708346	140.114.79.62	224.0.0.7	UDP	342	10318 → 10318 Len=300
2155	31.708362	140.114.79.62	224.0.0.7	UDP	318	10318 → 10318 Len=276
2156	31.708546	140.114.79.62	224.0.0.7	UDP	347	10318 → 10318 Len=305
2157	31.708546	140.114.79.62	224.0.0.7	UDP	341	10318 → 10318 Len=299
2158	31.708546	140.114.79.62	224.0.0.7	UDP	341	10318 → 10318 Len=299
2159	31.708546	140.114.79.62	224.0.0.7	UDP	341	10318 → 10318 Len=299
2160	31.708546	140.114.79.62	224.0.0.7	UDP	333	10318 → 10318 Len=291
2161	31.708546	140.114.79.62	224.0.0.7	UDP	337	10318 → 10318 Len=295
2162	31.774186	140.114.79.75	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{64FBF457-2FE3-4000-8000-000000000000}

> Ethernet II, Src: Cisco_ca:dd:53 (d0:dc:2c:ca:dd:53), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Address Resolution Protocol (request)

0000 ff ff ff ff ff ff d0 dc 2c ca dd 53 08 06 00
0010 00 00 06 64 00 01 d0 dc 2c ca dd 53 8c 72 4f
0020 00 00 00 00 00 00 8c 72 4f 2f 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00

乙太網路: <live capture in progress> | Packets: 2162 - Displayed: 2162 (100.0%) | Profile: Default

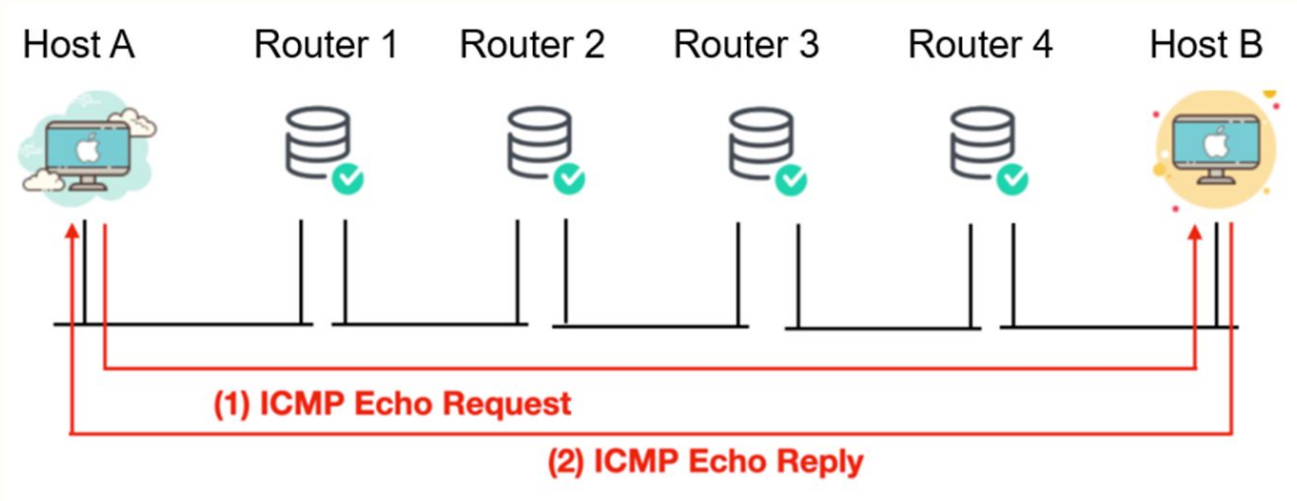
Wireshark: Filter

- Help remove the noise from a packet trace and let you see only the packets that interest you.
 - Ex 1 : Request Method
 - `http.request.method == "POST"`
 - Ex 2 : IPv4 addresses
 - `ip.src == 140.114.79.147`
 - `ip.dst eq www.nthu.edu.tw`
 - Ex 3 : Status
 - `http.response.code==200`

Check Ping Packets

Check PING packets

- ICMP (Internet Control Message Protocol): Used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address.



Ping command

- Sending Internet Control Message Protocol (ICMP) Echo Request messages to the network address you specify
- ping IP address / Hostname
 - ping facebook.com
 - ping 8.8.8.8

```
(base) C:\Users\jeff>ping 8.8.8.8
```

```
Pinging 8.8.8.8 with 32 bytes of data:
```

```
Reply from 8.8.8.8: bytes=32 time=3ms TTL=118
```

```
Reply from 8.8.8.8: bytes=32 time=3ms TTL=118
```

```
Reply from 8.8.8.8: bytes=32 time=3ms TTL=118
```

```
Reply from 8.8.8.8: bytes=32 time=3ms TTL=118
```

```
Ping statistics for 8.8.8.8:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 3ms, Maximum = 3ms, Average = 3ms
```




DNS



- DNS : Domain Name System
 - Hostname to IP address translation
- Google Public DNS
 - Google provides a free DNS
 - IPv4 address :
 - 8.8.8.8 (google-public-dns-a.google.com)
 - 8.8.4.4 (google-public-dns-b.google.com)

Check POST Packets

Website for test

- Link: <http://httpbin.org/>
- A simple HTTP Request & Response Service.

httpbin.org ^{0.9.2}

[Base URL: httpbin.org/]

A simple HTTP Request & Response Service.

Run locally: `$ docker run -p 80:80 kennethreitz/httpbin`

[the developer - Website](#)

[Send email to the developer](#)

Schemes

HTTP

HTTP Methods Testing different HTTP verbs

Auth Auth methods

Status codes Generates responses with given status code

Request inspection Inspect the request data

Response inspection Inspect the response data like caching and headers

Response formats Returns responses in different data formats



cURL



- cURL is a command-line tool and a library for transferring data using various network protocols.

```
curl -X POST "http://httpbin.org/response-headers?freeform=" -H "accept: application/json"
```

- -X: Use the specified http method to issue an http request.
 - GET
 - POST
 - PUT
 - DELETE
 - .etc
- -H: Used to specify custom headers to include in the HTTP request.



HTTP header

- A field of an HTTP request or response that passes additional context and metadata about the request or response.
 - Request Headers
 - Response Headers




Response header

- An HTTP header that can be used in an HTTP response and that doesn't relate to the content of the message.

```
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Date: Sat, 02 Mar 2024 10:17:46 GMT\r\n
  Content-Type: application/json\r\n
> Content-Length: 96\r\n
  Connection: keep-alive\r\n
  Server: gunicorn/19.9.0\r\n
  freeform: 112062571\r\n
  Access-Control-Allow-Origin: *\r\n
  Access-Control-Allow-Credentials: true\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.196838000 seconds]
\[Request in frame: 10976\]
[Request URI: http://httpbin.org/response-headers?freeform=112062571]
File Data: 96 bytes
```

Rebuild packets into the original file

Rebuild packets into the original file

- 
- A cluster of small, semi-transparent orange dots arranged in a roughly circular pattern on the left side of the slide.
- You are given a Wireshark capture file `Lab1.pcapng`. In this capture file, we **POST** a file into the http website.
 - In this part, you need to rebuild it into the original file.
 - In the following tutorial, we'll show how to rebuild a PDF file.

WireShark Filter

test.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

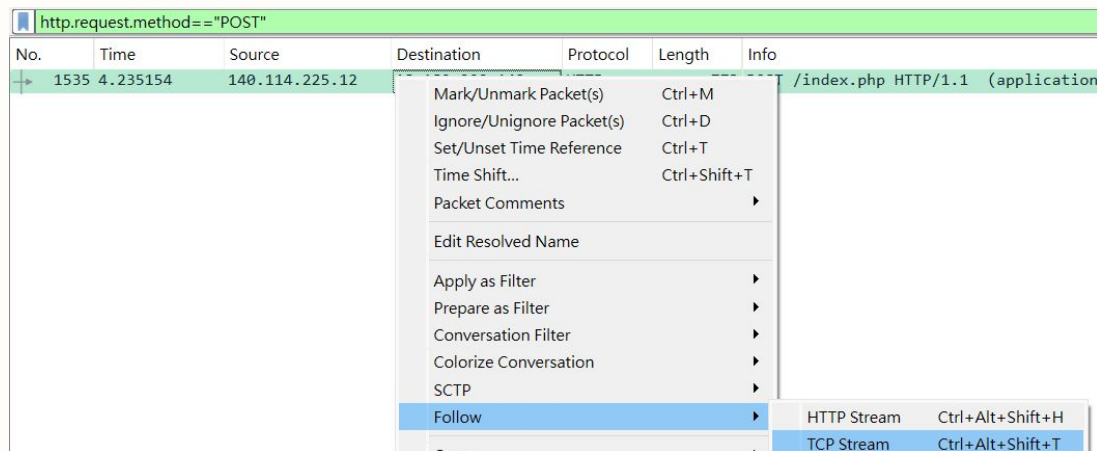
http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
1535	4.235154	140.114.225.12	18.189.209.142	HTTP	773	POST /index.php HTTP/1.1 (application/pdf)



Follow ▶ TCP Stream

- "Follow TCP Stream" shows the raw data exchanged over the TCP connection.
- "Follow HTTP Stream" provides a higher-level view focused on HTTP communication. It presents HTTP messages in a structured format.

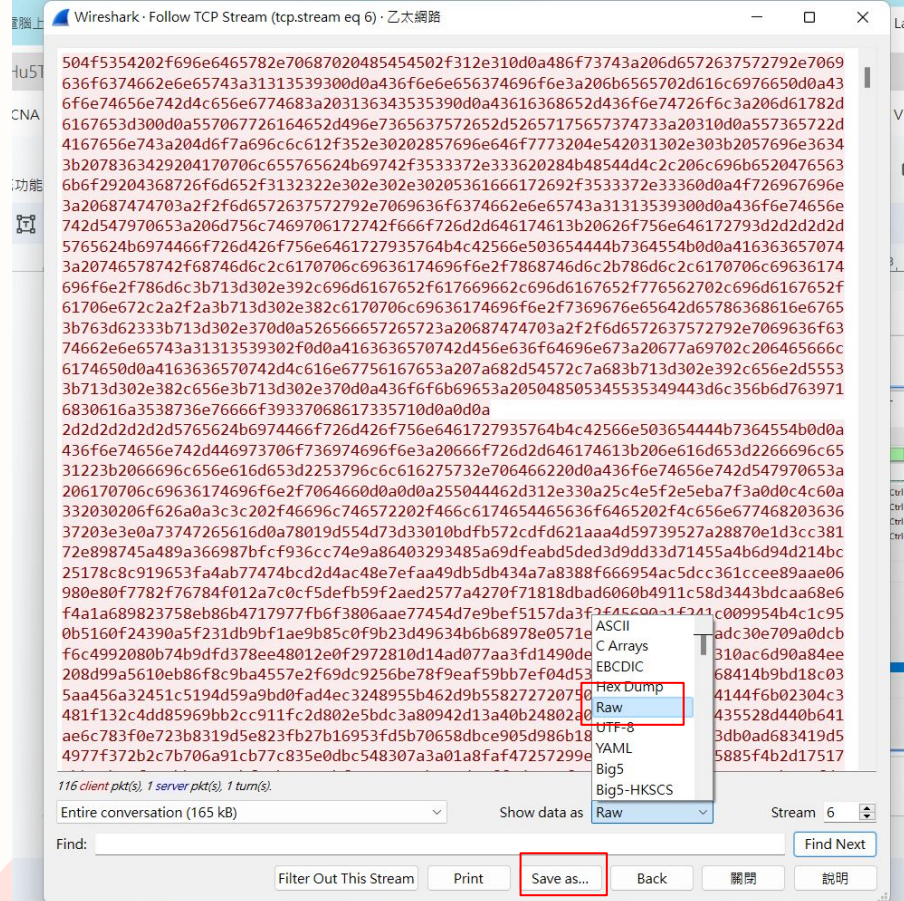


Display packet details

Note:

Save the data as raw data format.

Save the file name without adding '.pdf' for now.



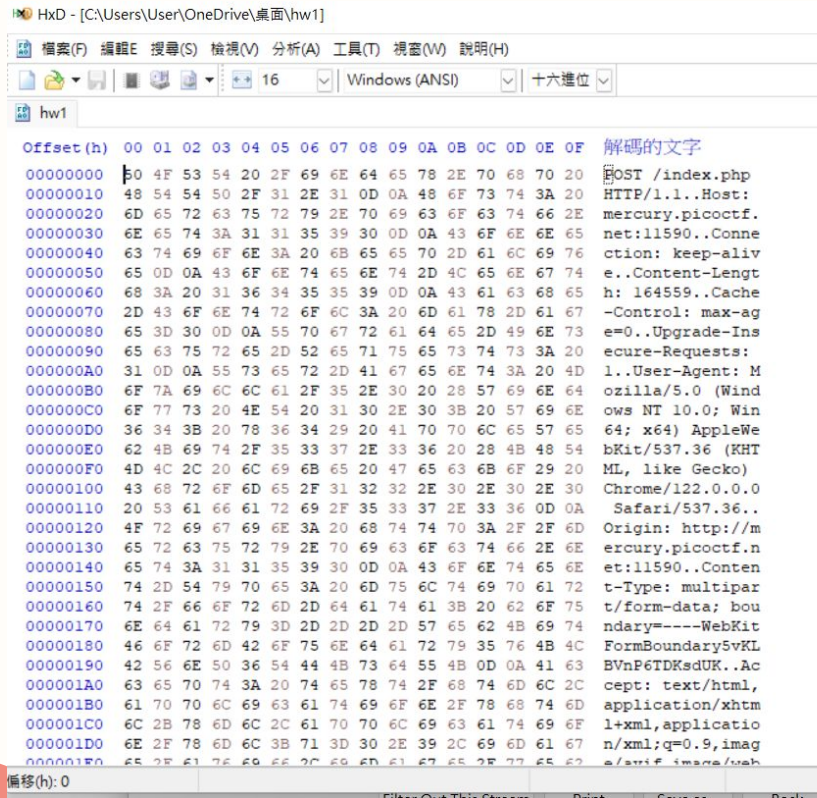
Open the file with a hexadecimal editor.

Example :

HxD download link for Windows:

<https://reurl.cc/nrMn7n>

MacOS can directly download HxD from
APP store.



HxD - [C:\Users\User\OneDrive\桌面\hw1]

檔案(F) 編輯(E) 搜尋(S) 檢視(V) 分析(A) 工具(T) 視窗(W) 說明(H)

16 Windows (ANSI) 十六進位

hw1

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	解碼的文字
00000000	60	4F	53	54	20	2F	69	6E	64	65	78	2E	70	68	70	20	POST /index.php
00000010	48	54	54	50	2F	31	2E	31	0D	0A	48	6F	73	74	3A	20	HTTP/1.1..Host:
00000020	6D	65	72	63	75	72	79	2E	70	69	63	6F	63	74	66	2E	mercury.picocf.
00000030	6E	65	74	3A	31	31	35	39	30	0D	0A	43	6F	6E	6E	65	net:11590..Conne
00000040	63	74	69	6F	6E	3A	20	6B	65	65	70	2D	61	6C	69	76	ction: keep-aliv
00000050	65	0D	0A	43	6F	6E	74	65	6E	74	2D	4C	65	6E	67	74	e..Content-Lengt
00000060	68	3A	20	31	36	34	35	35	39	0D	0A	43	61	63	68	65	h: 164559..Cache
00000070	2D	43	6F	6E	74	72	6F	6C	3A	20	6D	61	78	2D	61	67	-Control: max-ag
00000080	65	3D	30	0D	0A	55	70	67	72	61	64	65	2D	49	6E	73	e=0..Upgrade-Ins
00000090	65	63	75	72	65	2D	52	65	71	75	65	73	74	73	3A	20	ecure-Requests:
000000A0	31	0D	0A	55	73	65	72	2D	41	67	65	6E	74	3A	20	4D	1..User-Agent: M
000000B0	6F	7A	69	6C	6C	61	2F	35	2E	30	20	28	57	69	6E	64	ozilla/5.0 (Wind
000000C0	6F	77	73	20	4E	54	20	31	30	2E	30	3B	20	57	69	6E	ows NT 10.0; Win
000000D0	36	34	3B	20	78	36	34	29	20	41	70	70	6C	65	57	65	64; x64) AppleWe
000000E0	62	4B	69	74	2F	35	33	37	2E	33	36	20	28	4B	48	54	bKit/537.36 (KHT
000000F0	4D	4C	2C	20	6C	69	6B	65	20	47	65	63	6B	6F	29	20	ML, like Gecko)
00000100	43	68	72	6F	6D	65	2F	31	32	32	E	30	2E	30	2E	30	Chrome/122.0.0.0
00000110	20	53	61	66	61	72	69	2F	35	33	37	2E	33	36	0D	0A	Safari/537.36..
00000120	4F	72	69	67	69	6E	3A	20	68	74	74	70	3A	2F	2F	6D	Origin: http://m
00000130	65	72	63	75	72	79	2E	70	69	63	6F	63	74	66	2E	6E	mercury.picocf.n
00000140	65	74	3A	31	31	35	39	30	0D	0A	43	6F	6E	74	65	6E	et:11590..Conten
00000150	74	2D	54	79	70	65	3A	20	6D	75	6C	74	69	70	61	72	t-Type: multipar
00000160	74	2F	66	6F	72	6D	2D	64	61	74	61	3B	20	62	6F	75	t/form-data; bou
00000170	6E	64	61	72	79	3D	2D	2D	2D	57	65	62	4B	69	74	6D	ndary=---WebKit
00000180	46	6F	72	6D	42	6F	75	6E	64	61	72	79	35	76	4B	4C	FormBoundary5vKL
00000190	42	56	6E	50	36	54	44	4B	73	64	55	4B	0D	0A	41	63	BVnF6TDKsdUK..Ac
000001A0	63	65	70	74	3A	20	74	65	78	74	2F	68	74	6D	6C	2C	cept: text/html,
000001B0	61	70	70	6C	69	63	61	74	69	6F	6E	2F	78	68	74	6D	application/xhtm
000001C0	6C	2B	78	6D	6C	2C	61	70	70	6C	69	63	61	74	69	6F	l+xml,application
000001D0	6E	2F	78	6D	6C	3B	71	3D	30	2E	39	2C	69	74	61	67	n/xml;q=0.9,imag
000001E0	65	2F	61	76	69	6F	2C	69	6D	61	67	65	2F	77	65	62	e/;+if image/web

偏移(h): 0



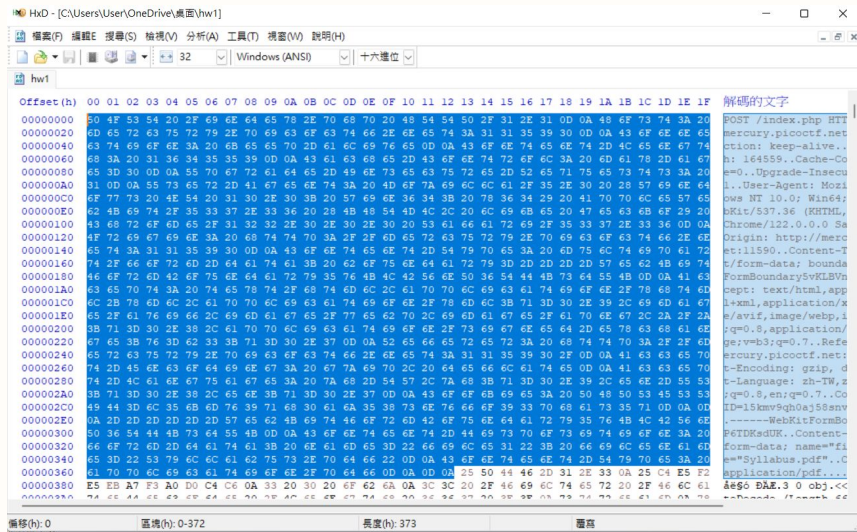


Delete from the headers of the file

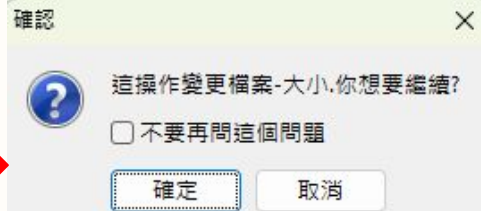
Note:

Delete the hexadecimal values up to but not including 25 50 44 46.

The preceding content is the header of the packet and is unrelated to the packet content.



Warning: Please press 'Yes'

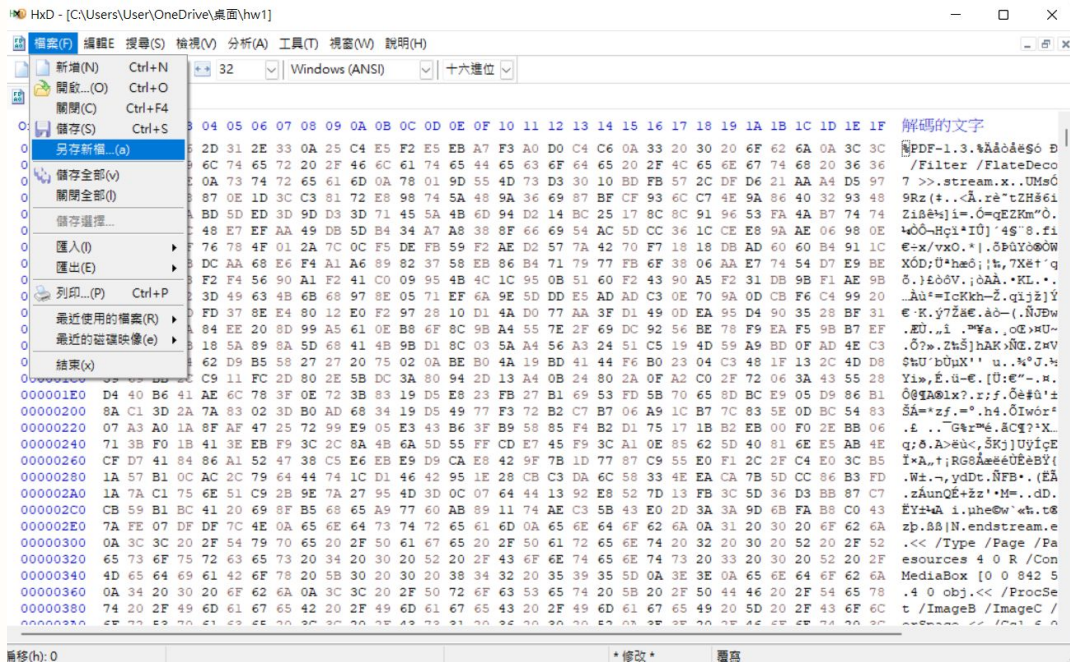


Save as a new file, and make sure to include '.pdf' as an extension in the file name.

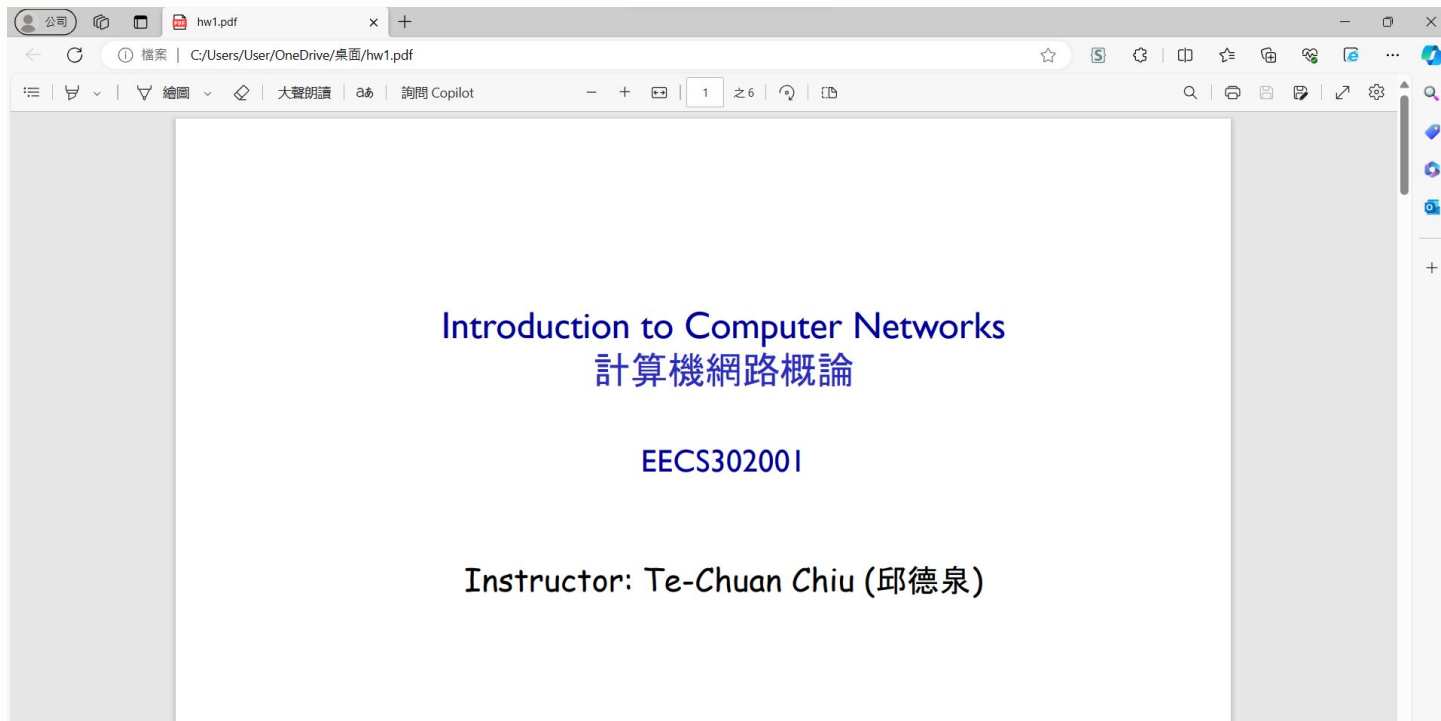


Note:

This time you should save the file with its file extension. For example: "hw1.pdf"



File rebuild successful



Assignment

Assignment

1. Check your PING packets (30%)
2. Check your POST packets (30%)
3. Rebuild the packet into the original file and check the content inside (30%)
4. Report (10%)



Assignment

- Check your PING packets (30%)
 - Screenshot the following results:

4586	22.706675	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request	id=0x00000000
4587	22.710089	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply	id=0x00000000
4701	23.721079	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request	id=0x00000000
4703	23.724303	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply	id=0x00000000
4922	24.727921	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request	id=0x00000000
4923	24.731067	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply	id=0x00000000
6083	25.731297	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request	id=0x00000000
6085	25.734407	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply	id=0x00000000

```

> Frame 4586: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{64FBF457
> Ethernet II, Src: GigaByteTech_2c:ef:f5 (74:56:3c:2c:ef:f5), Dst: Cisco_9f:f0:4f (00:00:0c:9f:f0:4f)
> Internet Protocol Version 4, Src: 140.114.79.147, Dst: 8.8.8.8
> Internet Control Message Protocol

```



Assignment

- Check your POST packets (30%)
 - Screenshot the following results:
 - Set the **student ID** as the **freeform** information in the header.



```
(base) C:\Users\jeff>curl -X POST "http://httpbin.org/response-headers?freeform=112062571" -H "accept: application/json"
{
  "Content-Length": "96",
  "Content-Type": "application/json",
  "freeform": "112062571"
}
```

```
> Frame 508: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits) on interface \Device\NPF_{64FBF457-2FE3-40DE-B313-FD882B7957BD}, id 0
> Ethernet II, Src: GigaByteTech_2c:ef:f5 (74:56:3c:2c:ef:f5), Dst: Cisco_9f:f0:4f (00:00:0c:9f:f0:4f)
> Internet Protocol Version 4, Src: 140.114.79.147, Dst: 44.217.139.104
> Transmission Control Protocol, Src Port: 57411, Dst Port: 80, Seq: 1, Ack: 1, Len: 123
> Hypertext Transfer Protocol
```

Assignment


- Rebuild the packet into the original file and check the content inside (30%)
 - The beginning hexadecimal values of this file are 89 50 4E 47
 - Screenshot the original file to the report

Assignment

- Report (10%)
 - Screenshot of the PING packets
 - Screenshot of the POST packets
 - Screenshot of the original file you rebuild
 - What would you like to say to Teacher or TA



Requirement

- 
- A decorative graphic consisting of several red, petal-like shapes arranged in a circular pattern.
- Put all of the screenshots in one PDF file.
 - Name the file Lab1_studentID.pdf
 - (e.g. Lab1_112062571.pdf)
 - Upload to eeclab before **03/28**.

Penalty

- **Plagiarism will get 0 point**
- Late submission before 4/4 only get **70%** of the original score
- Late submission after 4/4 will **not** be accepted