Lab 1 - Wireshark

Introduction to Computer Networks

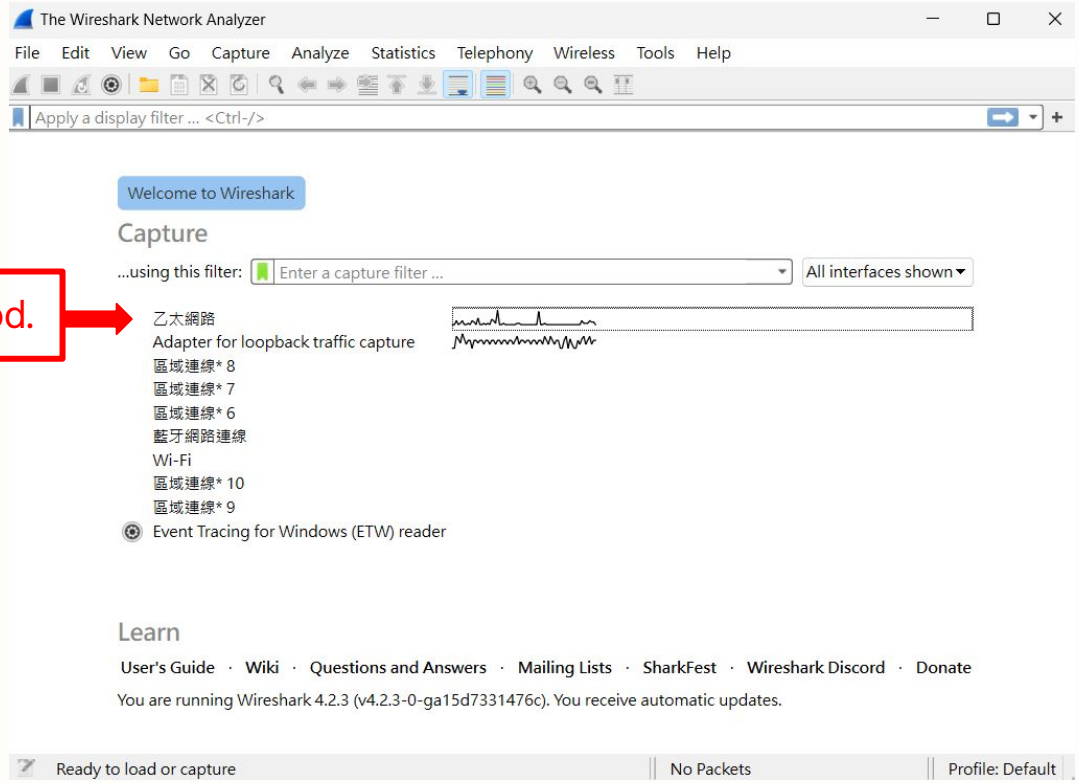
Kuan-Wei Huang(黃冠維), Pei-Chieh Wu (吳沛潔), Cheng-Yuan Jian (簡呈原), Hsiang-Ting Huang (黃湘庭), Pham Ngoc Hoa (范玉花)

Download and Install

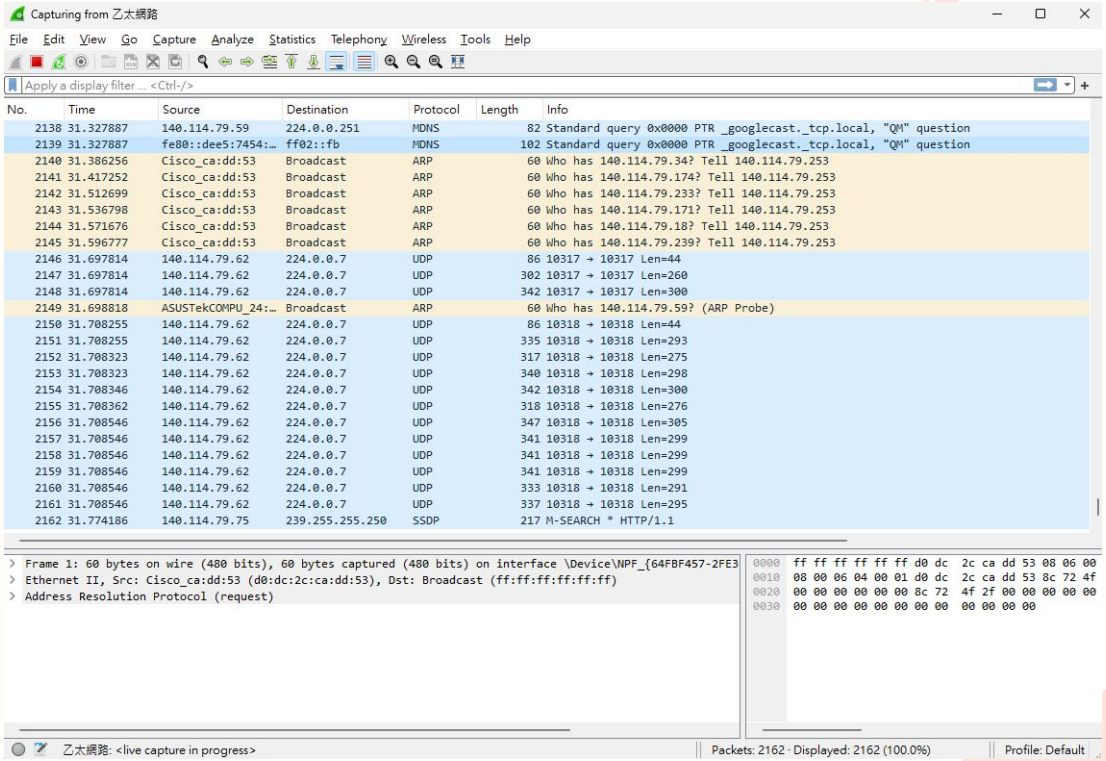
- Wireshark
  - https://www.wireshark.org/download.html

Wireshark: Capture Interface

Choose the connection method.



Wireshark: User Interface



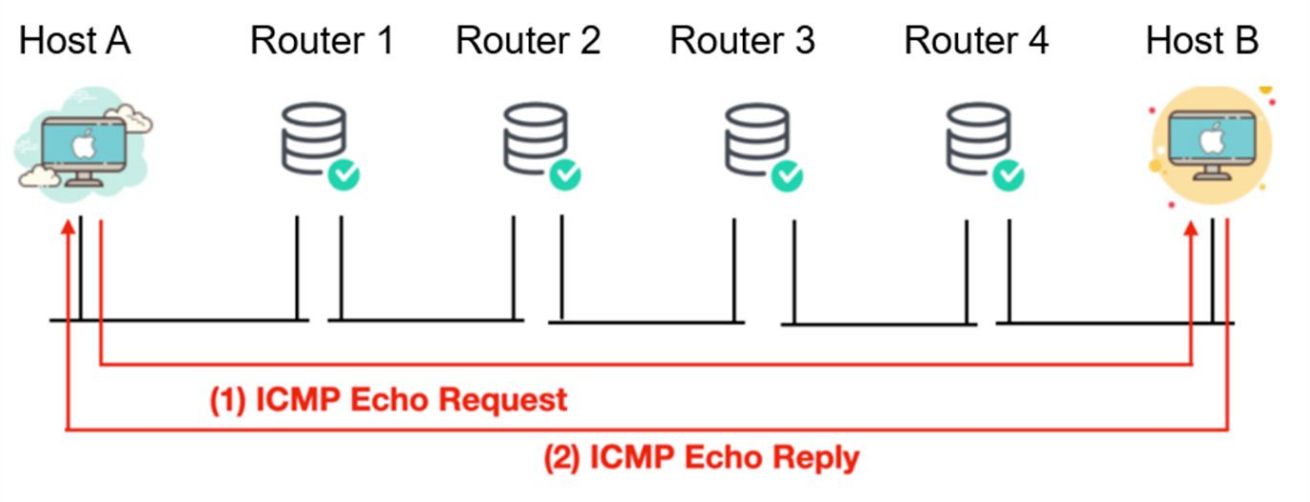
Wireshark: Filter

- 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
```

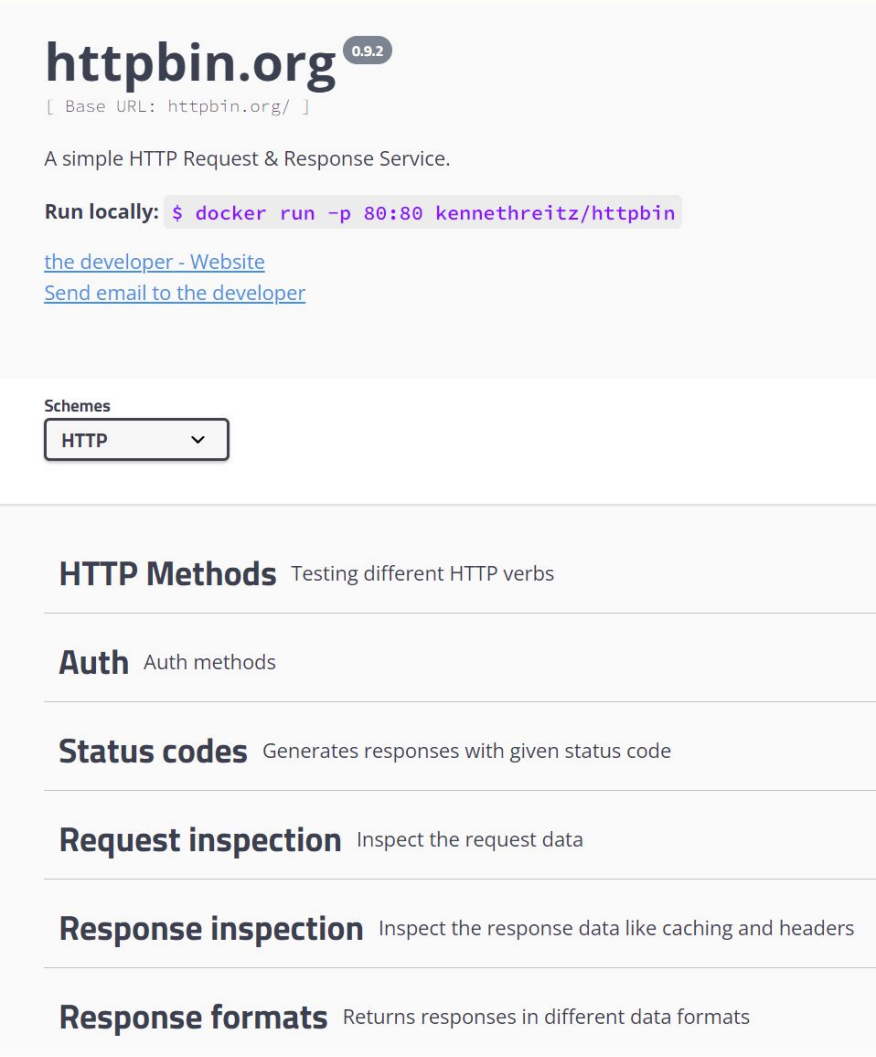
DNS

- 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.



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.

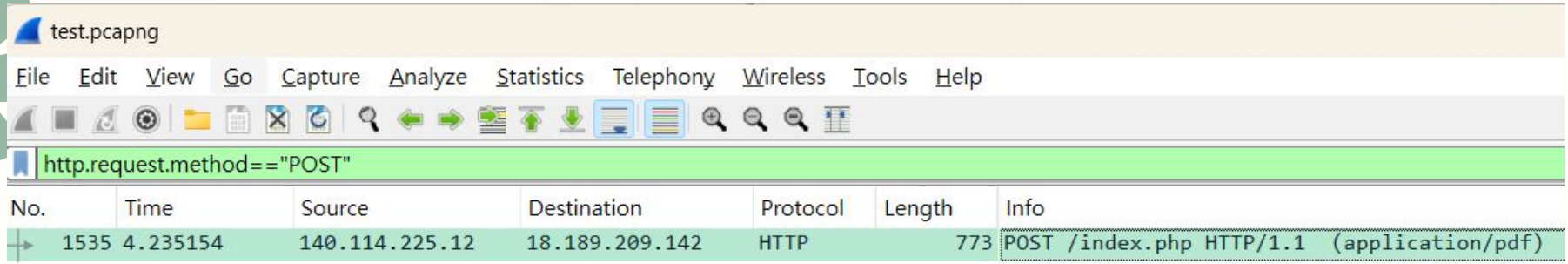
```
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
  Date: Sat, 02 Mar 2024 10:17:46 GMT\r\n
  Content-Type: application/json\r\n
> Content-Length: 96\r\n
  Connection: keep-alive\r\n
  Server: gunicorn/19.9.0\r\n
  freeform: 112062571\r\n
  Access-Control-Allow-Origin: *\r\n
  Access-Control-Allow-Credentials: 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

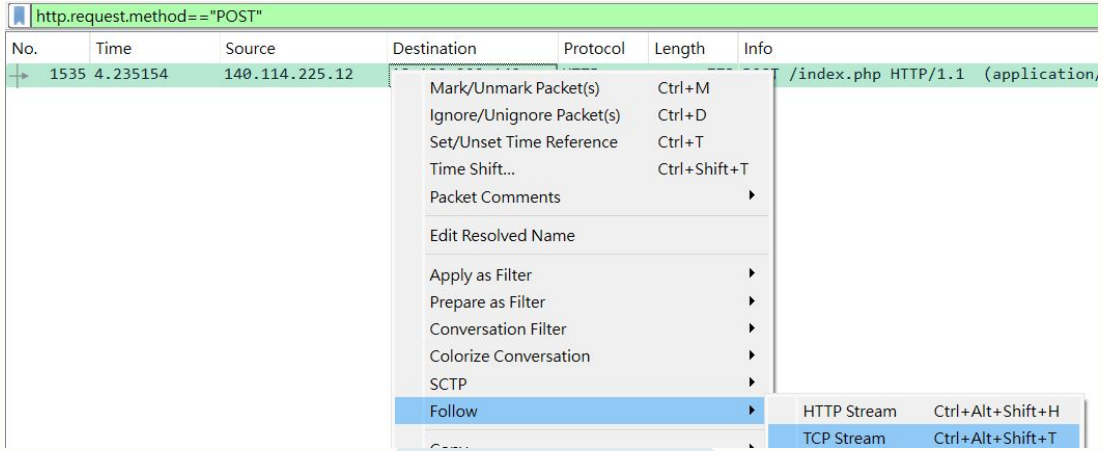
- You are given a Wireshark capture file Lab1.pcapng. In this capture file, we **POST** a file into the http website.
- In this part, you need to rebuild it into the original file.
- In the following tutorial, we'll show how to rebuild a PDF file.

WireShark Filter



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.

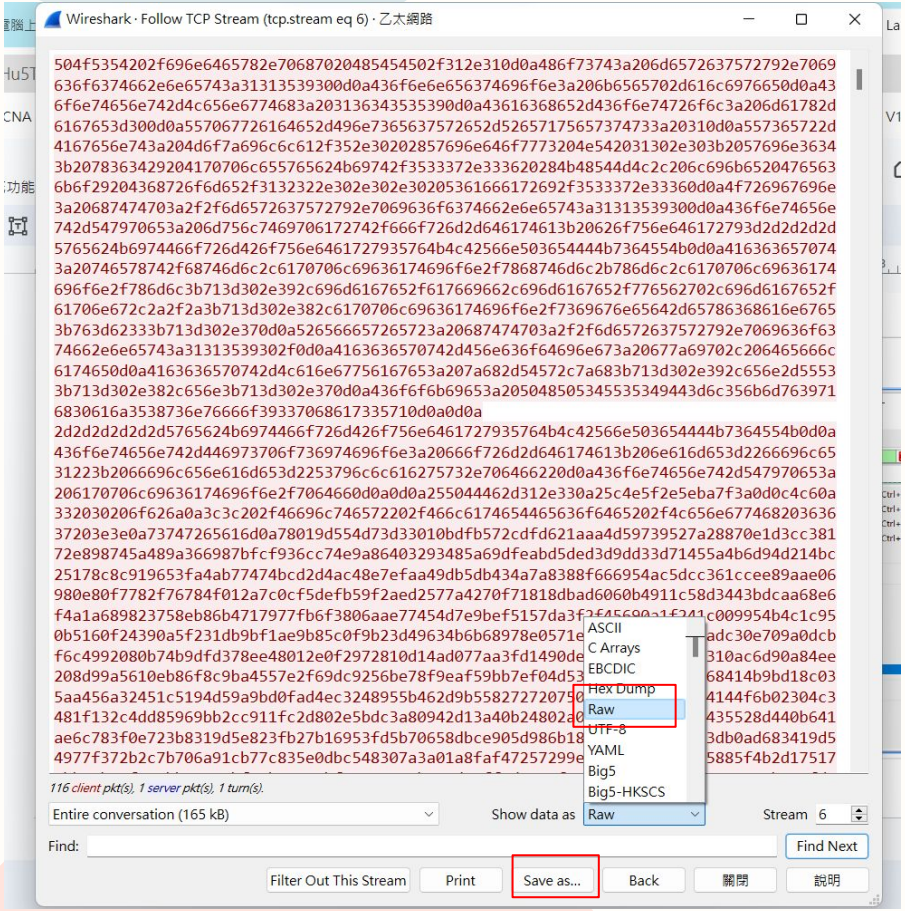


Display packet details

Note:

Save the data as raw data format.

Save the file name without adding ‘.pdf’ for now.



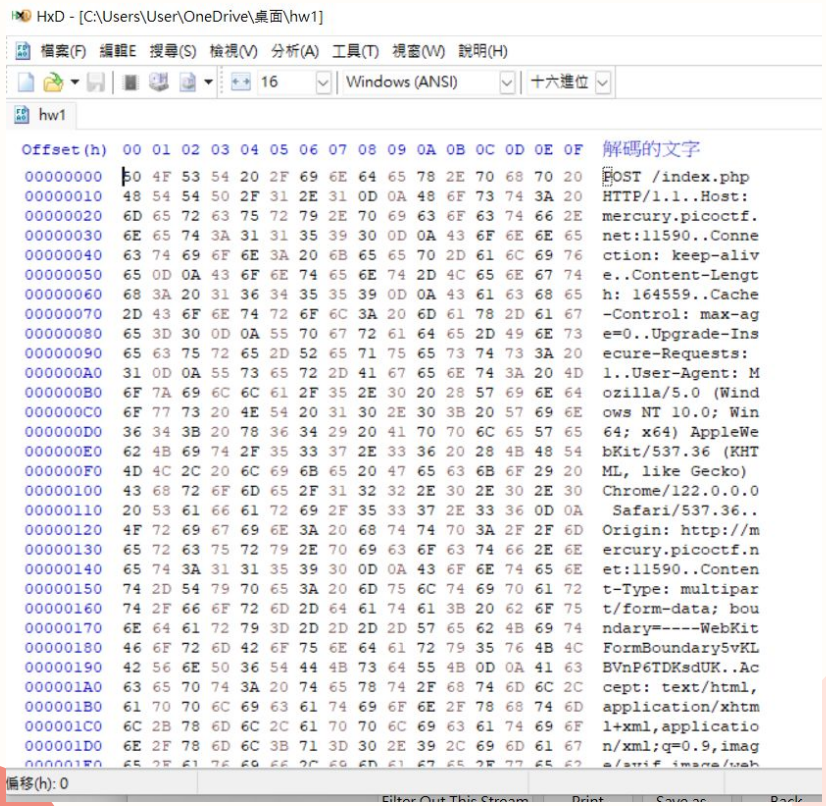
Open the file with a hexadecimal editor.

Example :

HxD download link for Windows:

https://reurl.cc/nrMn7n

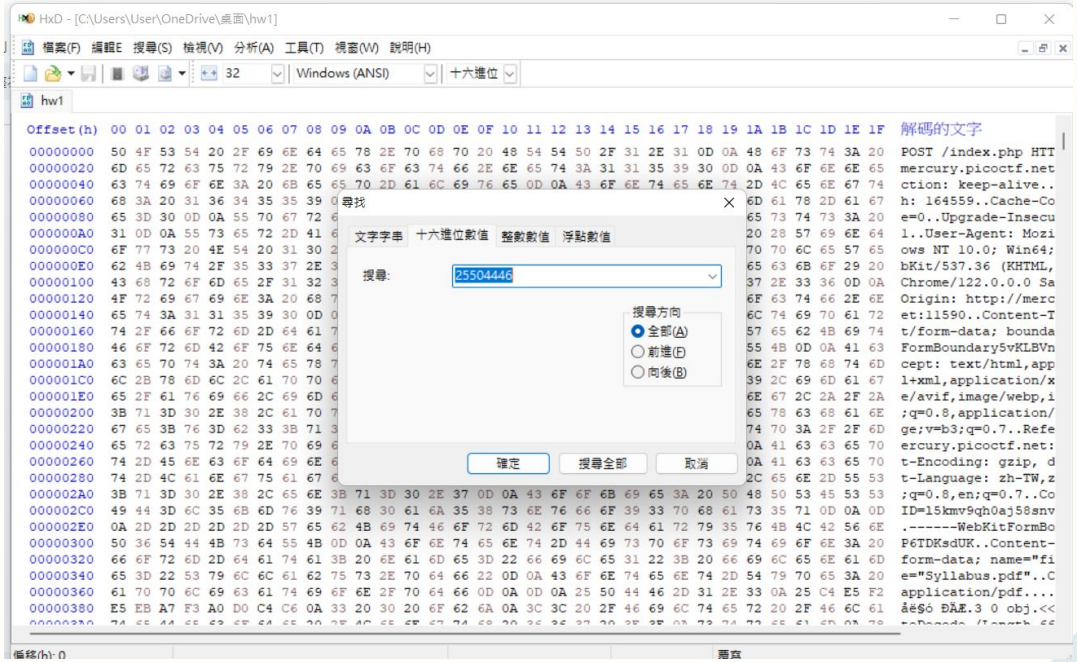
MacOS can directly download HxD from APP store.



Search for the hexadecimal values 25 50 44 46 or the text string '%PDF'.

Note:

Confirm the file type and search for the related hexadecimal values or text string when you are doing your assignment.

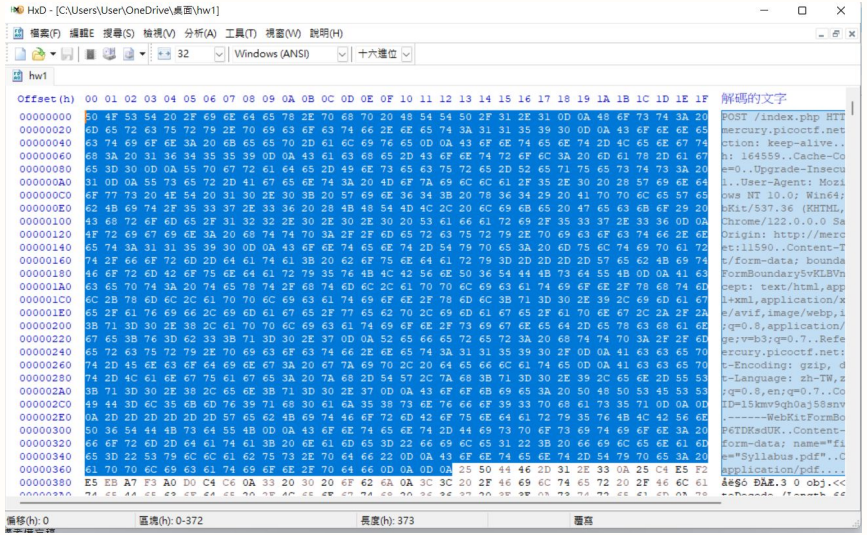


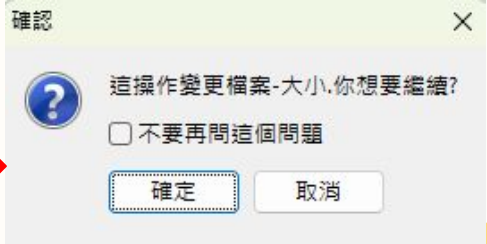
Delete from the headers of the file

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.



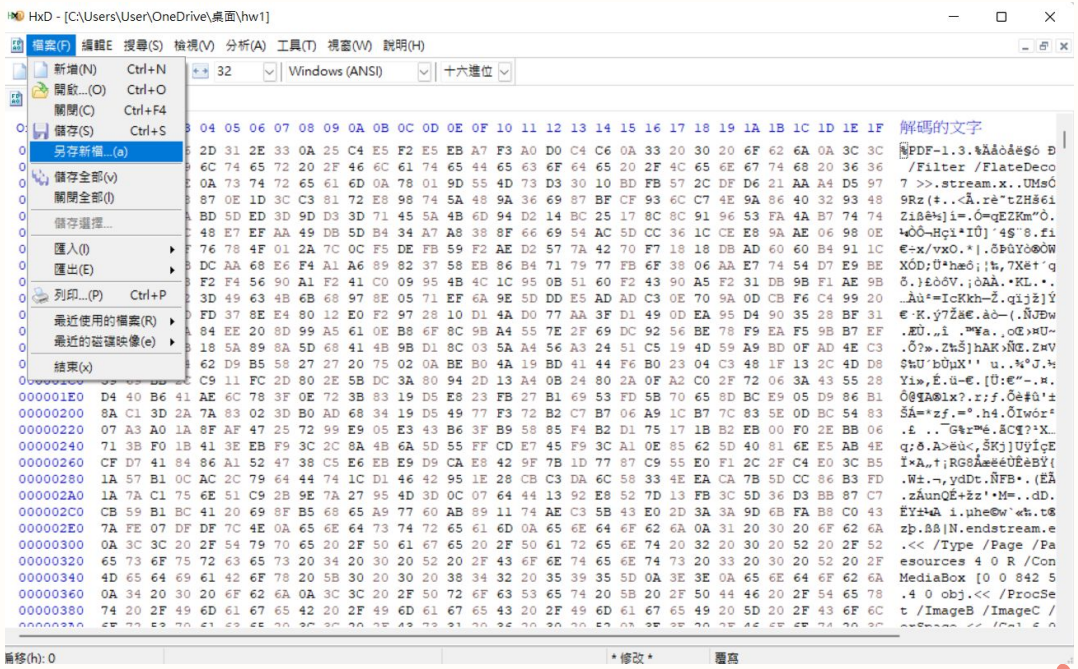


Warning: Please press ‘Yes’

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=0x00
4587	22.710089	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply id=0x00
4701	23.721079	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request id=0x00
4703	23.724303	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply id=0x00
4922	24.727921	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request id=0x00
4923	24.731067	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply id=0x00
6083	25.731297	140.114.79.147	8.8.8.8	ICMP	74	Echo (ping) request id=0x00
6085	25.734407	8.8.8.8	140.114.79.147	ICMP	74	Echo (ping) reply id=0x00

```
> 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

- Put all of the screenshots in one PDF file.
- Name the file Lab1_studentID.pdf
  - (e.g. Lab1_112062571.pdf)
- Upload to eeclass 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