ปฏิบัติการโปรแกรมดักจับข้อมูล ครั้งที่ 1

จงตอบคำถามต่อไปนี้

1.ให้สรุปการใช้งานการใช้โปรแกรม Wireshark

จากการที่ผู้ปฏิบัติได้ทดลองใช้งาน ทำให้เราเข้าใจถึงการส่งข้อมูลจากจุดหนึ่งไปยังจุดหนึ่ง ผ่าน Protocols ต่างๆที่เราได้ศึกษาจากภาคทฤษฎี และยังสามารถจับข้อมูลในระบบ Network และอ่านข้อมูลจากไฟล์ที่ส่งมาได้ เพื่อนำไปวิเคราะห์หรือกระทำการบางอย่างตามต้องการ สามารถเลือกประเภทของ Protocols ที่เราสนใจได้ เช่น TCP , HTTP หรือ UDP เป็นต้น สามารถเช็ค IP Address ของสิ่งที่เราสนใจได้ เช่น IP Address ของอุปกรณ์ผู้ปฏิบัติการเอง หรือ เว็บไซต์ปลายทางที่เราทำการเข้าใช้งาน เช่น

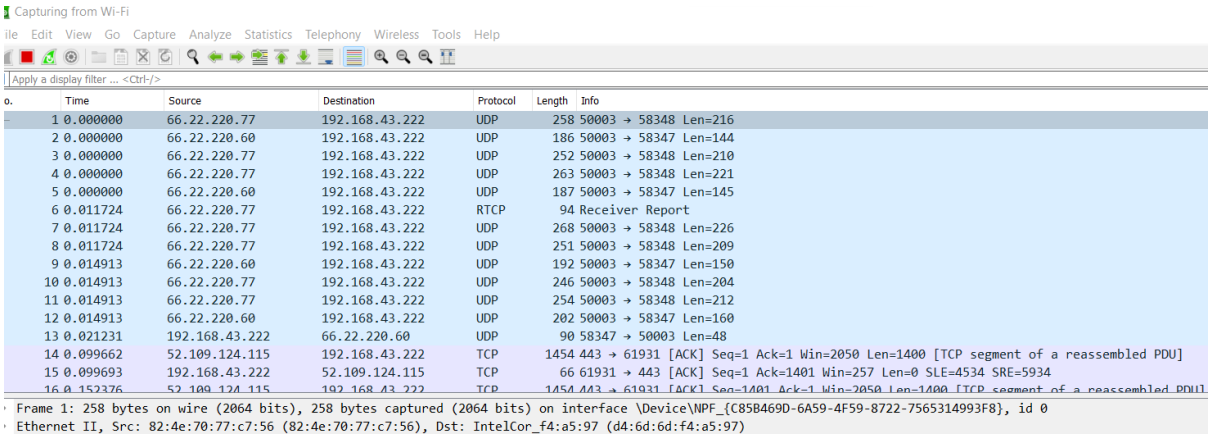
เข้าเว็บไซต์ www.gaia.umass.edu ซึ่งเราสามารถทราบ IP Address ได้คือ 128.119.245.12 และต้นทางคือ IP address ของอุปกรณ์ผู้ใช้งานคือ 192.168.43.222

No.	Time	Source	Destination	Protocol	Length	Info
19468	71.406311	192.168.43.222	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
19629	71.978189	128.119.245.12	192.168.43.222	HTTP	492	HTTP/1.1 200 OK (text/html)
19634	72.015412	192.168.43.222	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1

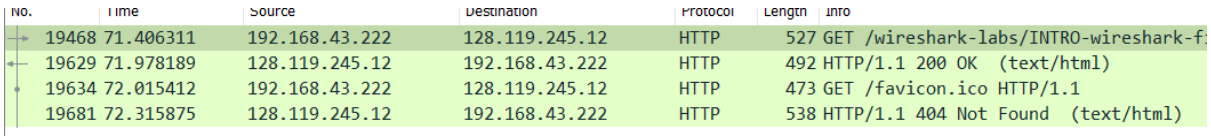
โดยสามารถสรุปขั้นตอนการใช้งานได้ดังนี้

1) Double-Click ที่โปรแกรม Wireshark

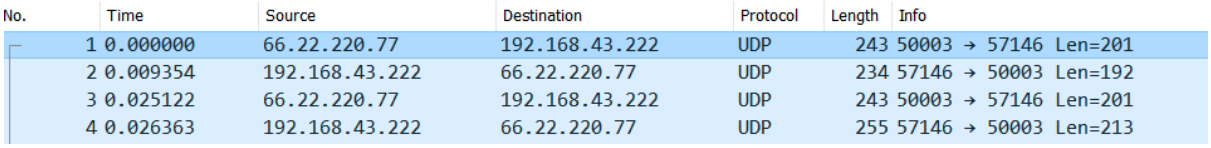
2) เลือก Interface List ที่ต้องการตรวจจับ เช่น Wi-fi หรือ Ethernet ในที่นี้เราเลือก Wi-fi เนื่องจากเราใช้ wi-fi สำหรับเชื่อมต่อ Internet



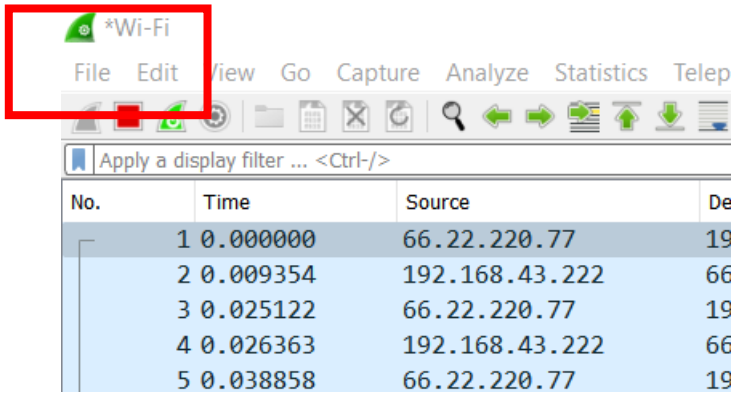
4) เราสามารถเลือกดู Protocols บางชนิดได้ เช่น HTTP

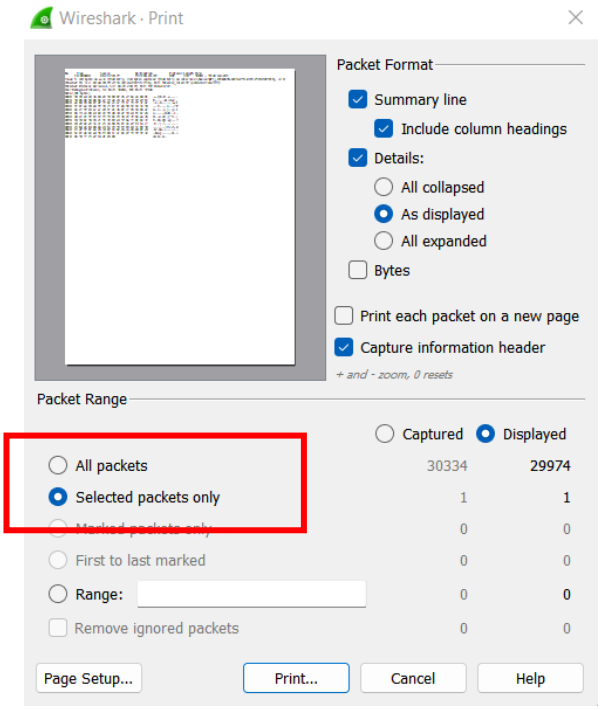


หรือ



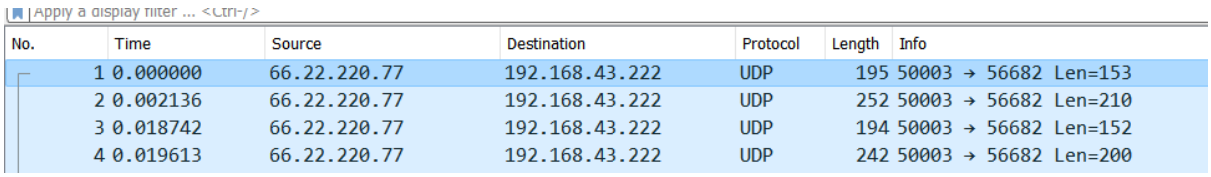
5) และเราสามารถบันทึกผลของสิ่งที่เราตรวจจับได้โดยไปที่ File → Print → Selected Packet Only → Print





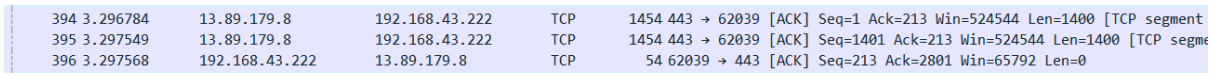
2.ให้ตรวจสอบการ Protocol ที่แตกต่างกันมา 3 ชนิด

Protocols ทั้ง 3 ชนิดที่พบ ได้แก่ HTTP , UDP และ TCP



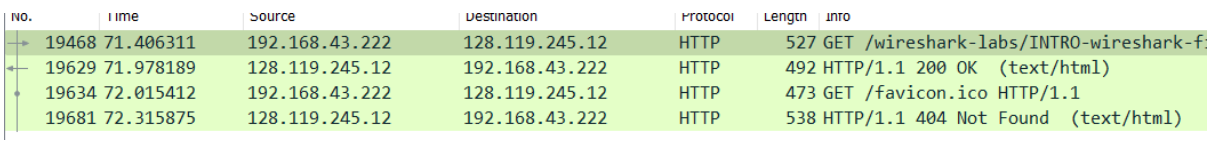
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	66.22.220.77	192.168.43.222	UDP	195	50003 → 56682 Len=153
2	0.002136	66.22.220.77	192.168.43.222	UDP	252	50003 → 56682 Len=210
3	0.018742	66.22.220.77	192.168.43.222	UDP	194	50003 → 56682 Len=152
4	0.019613	66.22.220.77	192.168.43.222	UDP	242	50003 → 56682 Len=200

- UDP (User Datagram Protocol) เป็น Protocol หลักในชุด Internet Protocol ที่เรียกว่า Datagram ซึ่งเป็นข้อมูลขนาดเล็กกว่าส่งผ่านเครือข่ายไปยังปลายทาง แต่ UDP จะไม่รับประกันความน่าเชื่อถือของข้อมูล ข้อมูลที่ได้อาจจะไม่เรียงลำดับหรืออาจจะสูญหายได้



394	3.296784	13.89.179.8	192.168.43.222	TCP	1454 443 → 62039 [ACK] Seq=1 Ack=213 Win=524544 Len=1400 [TCP segment
395	3.297549	13.89.179.8	192.168.43.222	TCP	1454 443 → 62039 [ACK] Seq=1401 Ack=213 Win=524544 Len=1400 [TCP segme
396	3.297568	192.168.43.222	13.89.179.8	TCP	54 62039 → 443 [ACK] Seq=213 Ack=2801 Win=65792 Len=0

- TCP (Transmission Control Protocol) เป็นหนึ่งในโปรโตคอลหลักของเครือข่ายอินเทอร์เน็ต ทำหน้าที่ควบคุมการรับส่งข้อมูลระหว่างSource และ Destination เพื่อใช้แลกเปลี่ยนข้อมูลระหว่างกันโดยมีการตรวจสอบทุกๆแพ็คเก็ตที่จัดส่ง ซึ่งวิธีการนี้ข้อมูลจะมีความน่าเชื่อถือสูง



No.	Time	Source	Destination	Protocol	Length	Info
19468	71.406311	192.168.43.222	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-f
19629	71.978189	128.119.245.12	192.168.43.222	HTTP	492	HTTP/1.1 200 OK (text/html)
19634	72.015412	192.168.43.222	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
19681	72.315875	128.119.245.12	192.168.43.222	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- HTTP (Hypertext Transport Protocol) เป็น Protocol สำหรับสื่อสารจะใช้เมื่อเรียกโปรแกรมบน Browser เช่น Chrome , Firefox หรือ Internet Explorer เพื่อเรียกดูข้อมูลหรือเว็บนั้นๆ

3.ใช้ระยะเวลาเท่าใด เมื่อ HTTP GET message จนกระทั่ง HTTP OK reply ได้รับ

No.	Time	Source	Destination	Protocol	Length	Info
19468	71.406311	192.168.43.222	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-f
19629	71.978189	128.119.245.12	192.168.43.222	HTTP	492	HTTP/1.1 200 OK (text/html)
19634	72.015412	192.168.43.222	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
19681	72.315875	128.119.245.12	192.168.43.222	HTTP	538	HTTP/1.1 404 Not Found (text/html)

ใช้เวลาทั้งสิ้น 0.571878000 seconds

```
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.571878000 seconds]
[Request in frame: 19468]
[Next request in frame: 19634]
[Next response in frame: 19681]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 81 bytes
```

4. IP address ของ gaia.cs.umass.edu (also known as www.net.cs.umass.edu) ?

No.	Time	Source	Destination	Protocol	Length	Info
19468	71.406311	192.168.43.222	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wire
19629	71.978189	128.119.245.12	192.168.43.222	HTTP	492	HTTP/1.1 200 OK (text/html)
19634	72.015412	192.168.43.222	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
19681	72.315875	128.119.245.12	192.168.43.222	HTTP	538	HTTP/1.1 404 Not Found (text/

IP Address : 128.119.245.12 สามารถตรวจสอบได้จากการ Ping ผ่าน cmd

```
C:\Users\ASAS>ping gaia.cs.umass.edu

Pinging gaia.cs.umass.edu [128.119.245.12] with 32 bytes of data:
Reply from 128.119.245.12: bytes=32 time=296ms TTL=35
Reply from 128.119.245.12: bytes=32 time=286ms TTL=35
Reply from 128.119.245.12: bytes=32 time=287ms TTL=35
Reply from 128.119.245.12: bytes=32 time=295ms TTL=35

Ping statistics for 128.119.245.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 286ms, Maximum = 296ms, Average = 291ms
```

5. IP Address ของเครื่องตนเอง

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.222	35.213.176.48	UDP	86	60778 → 50009 Len=44
2	0.005511	111.223.61.5	192.168.43.222	SSL	1390	Continuation Data
3	0.005541	192.168.43.222	111.223.61.5	TCP	54	60023 → 443 [ACK] Seq=32 Ack
4	0.006441	111.223.61.5	192.168.43.222	SSL	2726	Continuation Data

จุดเริ่มต้นของการส่งข้อมูลตามหลักควรจะต้องเริ่มที่ต้นทางซึ่งก็คืออุปกรณ์ของผู้ใช้งาน ดังนั้น IP Address ของเครื่องตนเองคือ 192.168.43.222 ซึ่งสามารถตรวจสอบได้โดยใช้ cmd ตามด้วย ipconfig หรือ ตรวจสอบจาก Control Panel ดังที่แสดง

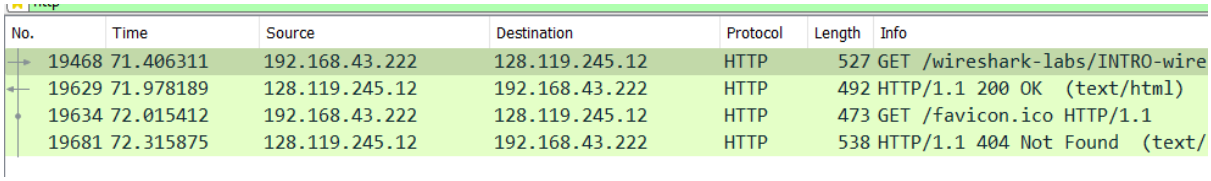
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:44c8:4554:a056:89da:dff3:1529:4d9a
   Temporary IPv6 Address. . . . . . : 2001:44c8:4554:a056:28e4:8c1b:6207:6955
   Link-local IPv6 Address . . . . . : fe80::89da:dff3:1529:4d9a%14
   IPv4 Address. . . . . . . . . . . : 192.168.43.222
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::804e:70ff:fe77:c756%14
                                       192.168.43.1
```

วิธี cmd

Physical Address	D4-6D-6D-F4-A5-97
DHCP Enabled	Yes
IPv4 Address	192.168.43.222
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	16 สิงหาคม 2565 0:00:16
Lease Expires	16 สิงหาคม 2565 1:12:47
IPv4 Default Gateway	192.168.43.1
IPv4 DHCP Server	192.168.43.1
IPv4 DNS Server	192.168.43.1
IPv4 WINS Server	
NetBIOS over Tcpip Enabl	Yes

วิธี Control Panel

6. ให้ทำการจับภาพหน้าจอจาก two message (GET and OK) referred to ในคำถามก่อนหน้านี้และทำการเลือก จาก Wireshark File command menu, and select the “Selected Packet Only” and “Print as displayed” radial buttons, and then click OK.



No.	Time	Source	Destination	Protocol	Length	Info
19468	71.406311	192.168.43.222	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wire
19629	71.978189	128.119.245.12	192.168.43.222	HTTP	492	HTTP/1.1 200 OK (text/html)
19634	72.015412	192.168.43.222	128.119.245.12	HTTP	473	GET /favicon.ico HTTP/1.1
19681	72.315875	128.119.245.12	192.168.43.222	HTTP	538	HTTP/1.1 404 Not Found (text/

```
No.     Time           Source                Destination           Protocol Length Info
   3468 15.557949      192.168.43.222        128.119.245.12        HTTP     649    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 3468: 649 bytes on wire (5192 bits), 649 bytes captured (5192 bits) on interface \Device\NPF_{C85B469D-6A59-4F59-8722-7565314993F8}, id 0
Ethernet II, Src: IntelCor_f4:a5:97 (d4:6d:6d:f4:a5:97), Dst: 82:4e:70:77:c7:56 (82:4e:70:77:c7:56)
Internet Protocol Version 4, Src: 192.168.43.222, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55287, Dst Port: 80, Seq: 1, Ack: 1, Len: 595
    Source Port: 55287
    Destination Port: 80
    [Stream index: 7]
    [Conversation completeness: Incomplete (60)]
    [TCP Segment Len: 595]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1096402697
    [Next Sequence Number: 596    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 142580813
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 257
    [Calculated window size: 257]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x6478 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (595 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.81 Safari/537.36 Edg/
104.0.1293.54\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "51-5e641541a0e2b"\r\n
    If-Modified-Since: Mon, 15 Aug 2022 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 3543]
```