

Mid Test

Course code: FRS301

Student name:	Huynh Ngoc Quang
Student ID:	SE181838

Note: Support your work by taking screenshots

Part 1: Protocol Identification

Step 1: Analyze the pcap files: challenge_1.pcap, challenge_2.pcap, challenge_3.pcap

Step 2: Answer the following questions for each pcap file

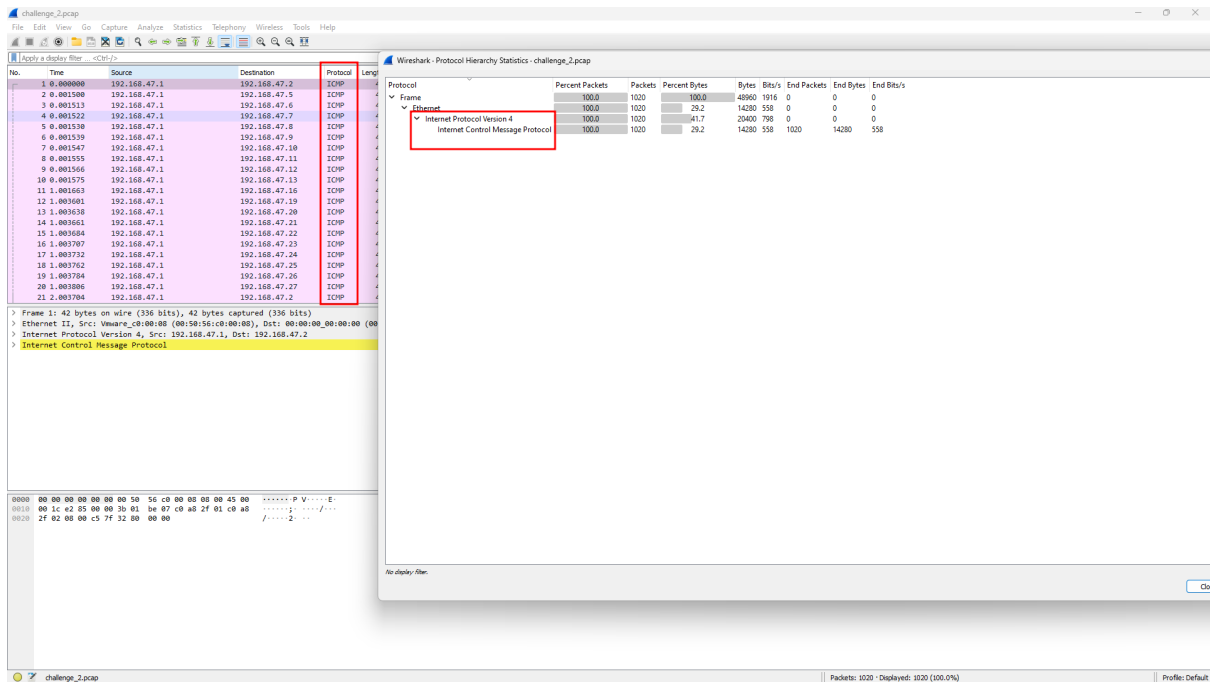
1. What protocols are used?

The screenshot displays the Wireshark interface for analyzing challenge_1.pcap. The packet list on the left shows a series of packets with their respective protocols. The protocol hierarchy on the right provides a detailed view of the protocols used, including User Datagram Protocol, NetBIOS Name Service, NetBIOS Datagram Service, SMB (Server Message Block Protocol), SMB MailSlot Protocol, Microsoft Windows Browser Protocol, Transmission Control Protocol, Simple Mail Transfer Protocol, and Internet Message Format. The packet details pane shows the structure of a frame, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, NetBIOS Datagram Service, SMB (Server Message Block Protocol), SMB MailSlot Protocol, and Microsoft Windows Browser Protocol.

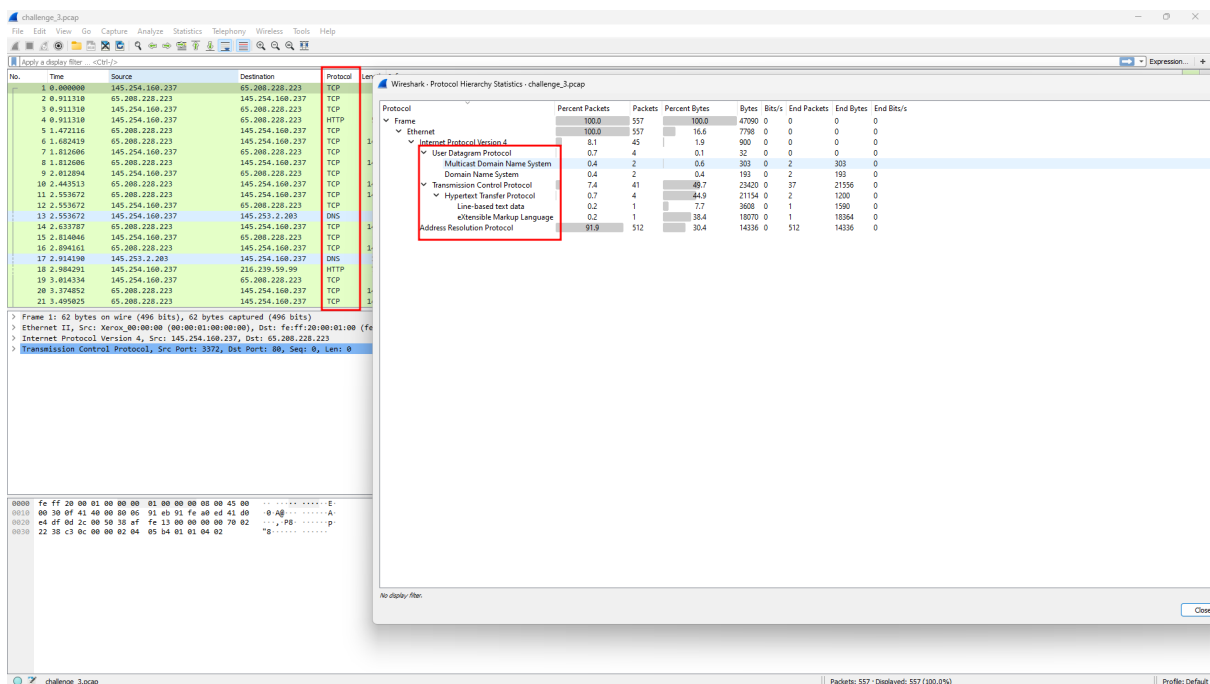
Ans:

The protocols are used in **challenge_1.pcap** were:

- TCP (Transmission Control Protocol)
- SMTP (Simple Mail Transfer Protocol)
- IMF (Internet Message Format)
- BROWSER (Microsoft Windows Browser Protocol)
- NBNS (NetBIOS Name Service)



Ans:
 The protocols are used in **challenge_2.pcap** were:
 - ICMP (Internet Control Message Protocol)



Ans:
 The protocols are used in **challenge_3.pcap** were:
 - TCP (Transmission Control Protocol)
 - HTTP (HyperText Transfer Protocol)
 - DNS (Domain Name System)
 - ARP (Address Resolution Protocol)

- MDNS (Multicast Domain Name System)
2. According to your analysis, describe briefly about the behaviour that are captured by these files.

Ans:

- **challenge_1.pcap:** The machine with IP 192.168.47.171 connect to the server with IP 192.168.47.134 to send an email from w.buchanan@napier.ac.uk to test@home.com.
- **challenge_2.pcap:** The machine with IP 192.168.47.1 try to send ICMP (ping) packet to all IP in the network.
- **challenge_3.pcap:**
 - The machine with IP 145.254.160.237 connect to the web server with IP 65.208.228.223 and access to “/download.html” with the host was www.ethereal.com from the “Referer: <http://www.ethereal.com/development.html>”
 - Ask for DNS server with the IP 145.253.2.203 for the IP of the domain name “pagead2.googlesyndication.com” and DNS server return Answers:
 - pagead2.googlesyndication.com: type CNAME, class IN, cname pagead2.google.com
 - pagead2.google.com: type CNAME, class IN, cname pagead.google.akadns.net
 - pagead.google.akadns.net: type A, class IN, addr 216.239.59.104
 - pagead.google.akadns.net: type A, class IN, addr 216.239.59.99
 - Then access to the web server with IP “216.239.59.99” and access to “/pagead/ads?client=ca-pub-2309191948673629&random=1084443430285&lm=1082467020&format=468x60_as&output=html&url=http%3A%2F%2Fwww.ethereal.com%2Fdownload.html&color_bg=FFFFFF&color_text=333333&color_link=000000&color_url=666633&color_border=666633” with the host was “pagead2.googlesyndication.com”
 - Finally was ARP Broadcast from Source: Vmware_1d:b3:b1 (00:0c:29:1d:b3:b1)

Part 2: Find Content

Step 1: Analyze the pcap files: findContent.pcap

Step 2: Answer the following questions for each pcap file

1. According to your analysis, describe briefly about the behaviour that are captured by these files.

Ans:

- The machine with IP 172.16.121.163 connect the web server with IP 212.227.84.95 and send a POST request with some image (JPEG) to “/forensics/file”

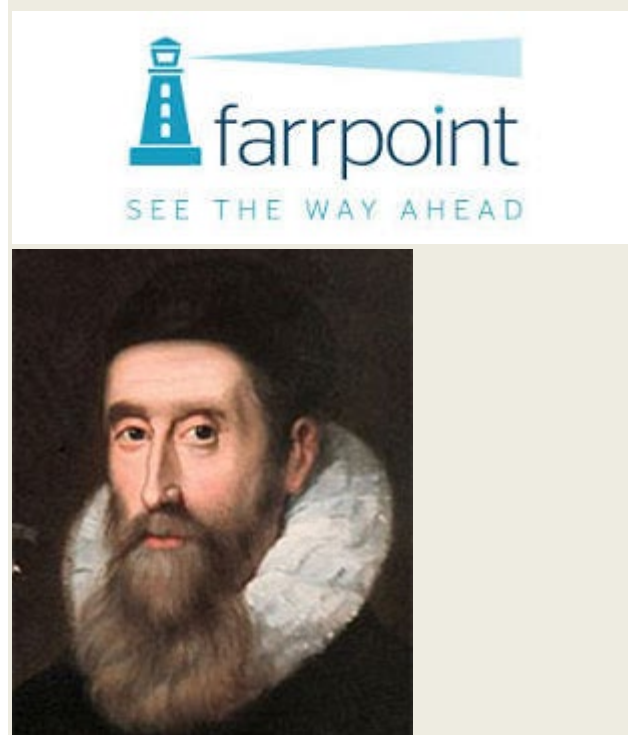
- o farr_images.jpg
- o John_Napier_(Neper).jpg
- o 150845-apple_laserwriter_original.jpg

- After each image POST the server return the analysis of that file like below

The screenshot shows a web application for file analysis. On the left, there is a list of files with their names and sizes. The 'File Contents' section in the middle provides a brief description of the tool and a list of files with 'View' links. The 'File contents analysis' section on the right shows the file 'farr_images.jpg' and its signature analysis results, including a list of possible file types and their counts.

2. Show the files you found. Explain in detail how you found the files.

Ans:





How to get it?

findContent.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Open Recent Merge... Import from Hex Dump... Close Save Save As... File Set Export Specified Packets... Export Packet Dissections... Export Packet Bytes... Export PDUs to File... Export TLS Session Keys... **Export Objects** Print... Quit

DICOM... HTTP... IM... SMB... TFTP...

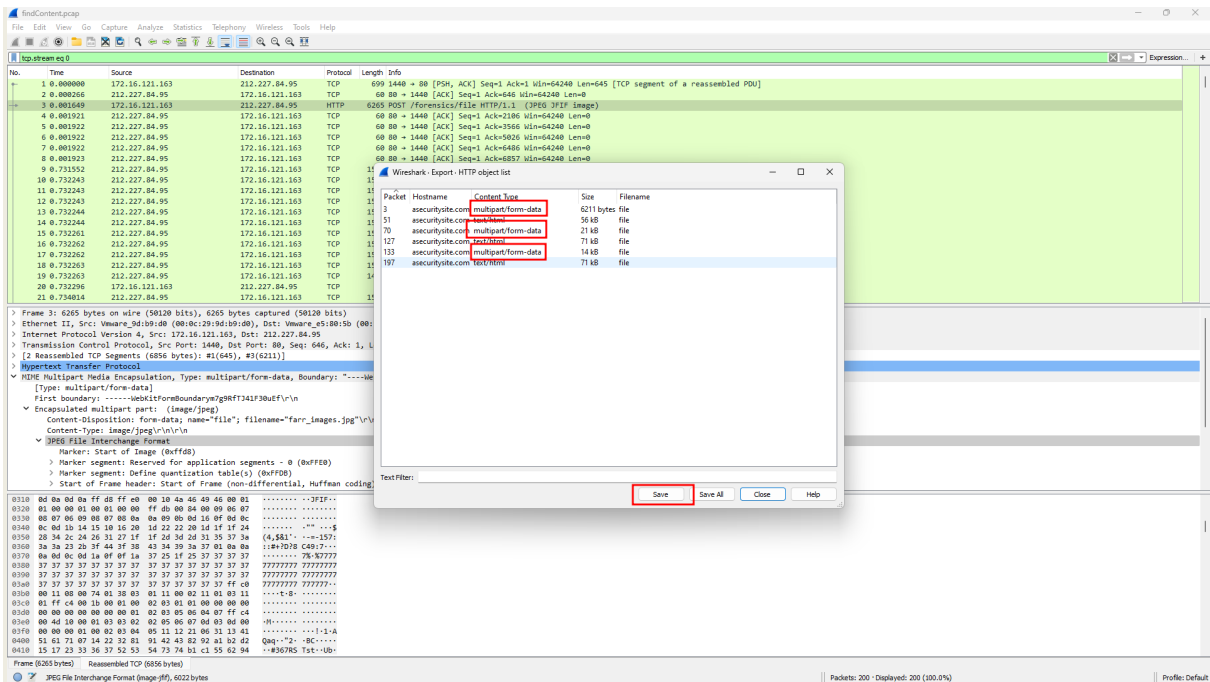
Destination	Protocol	Length	Info
212.227.84.95	TCP	699	1440 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=645 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	60	80 → 1440 [ACK] Seq=1 Ack=646 Win=64240 Len=0
212.227.84.95	HTTP	6265	POST /forensics/file HTTP/1.1 (3PEO 3FIF Image)
172.16.121.163	TCP	60	80 → 1440 [ACK] Seq=1 Ack=2186 Win=64240 Len=0
172.16.121.163	TCP	60	80 → 1440 [ACK] Seq=1 Ack=3506 Win=64240 Len=0
172.16.121.163	TCP	60	80 → 1440 [ACK] Seq=1 Ack=5026 Win=64240 Len=0
172.16.121.163	TCP	60	80 → 1440 [ACK] Seq=1 Ack=6486 Win=64240 Len=0
172.16.121.163	TCP	60	80 → 1440 [ACK] Seq=1 Ack=6857 Win=64240 Len=0
172.16.121.163	TCP	1502	80 → 1440 [PSH, ACK] Seq=1 Ack=6857 Win=64240 Len=1440 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1502	80 → 1440 [PSH, ACK] Seq=1449 Ack=6857 Win=64240 Len=1440 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=2897 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=4357 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=5217 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=7777 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=8737 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=18197 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=16557 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=13117 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
172.16.121.163	TCP	1406	80 → 1440 [PSH, ACK] Seq=14577 Ack=6857 Win=64240 Len=1352 [TCP segment of a reassembled PDU]
212.227.84.95	TCP	54	1440 → 80 [ACK] Seq=6857 Ack=15929 Win=68596 Len=0
172.16.121.163	TCP	1514	80 → 1440 [ACK] Seq=15929 Ack=6857 Win=64240 Len=1460 [TCP segment of a reassembled PDU]

> Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: Vmware_p5:00:50:00:50:50, Dst: Vmware_0d:00:00:00:00:00
> Internet Protocol Version 4, Src: 212.227.84.95, Dst: 172.16.121.163
> Transmission Control Protocol, Src Port: 80, Dst Port: 1440, Seq: 1, Ack: 2186, Len: 0

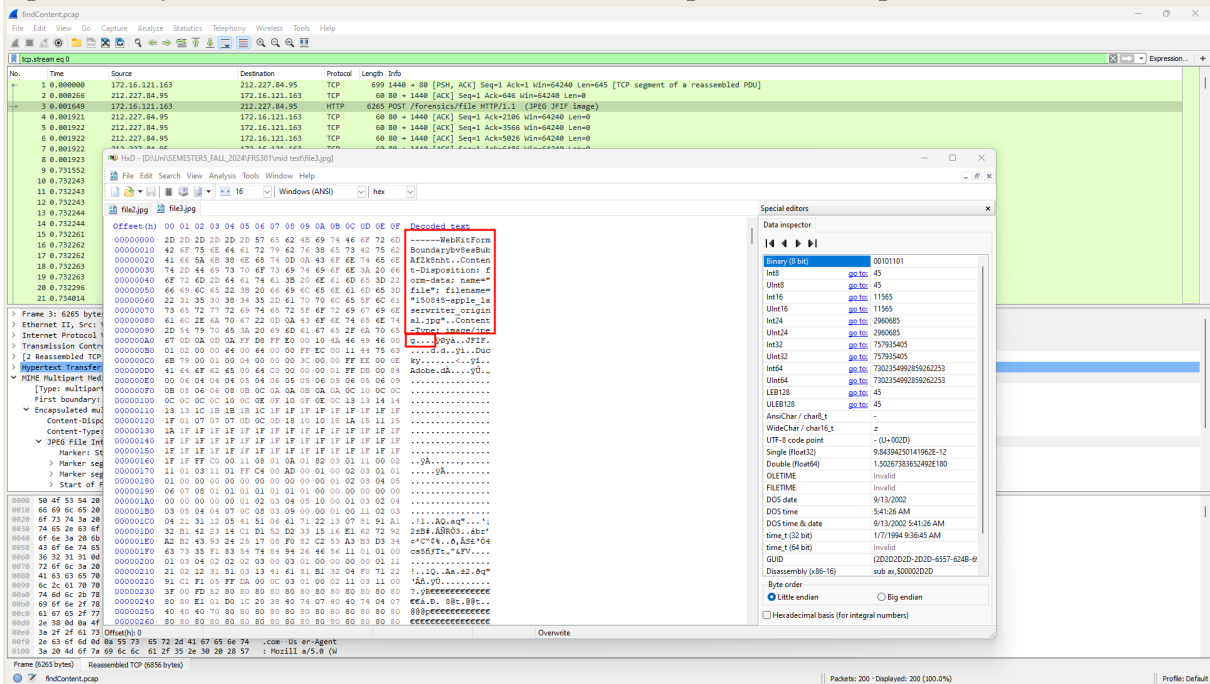
0000 80 0c 29 04 00 00 00 56 c5 00 50 00 00 43 00P V...E-
0010 00 28 ef 09 00 00 00 06 fc 3f 64 a3 54 5f ac 10T...
0020 79 a3 00 50 05 a0 1d 7b 1a 45 74 72 c7 44 50 10 y:P...{Etr-DP
0030 fa f0 ac 05 00 00 00 00 00 00 00 00 00 00 00 00
0040

findContent.pcap | Packets: 200 - Displayed: 200 (100.0%) | Profile: Default

Save 3 image file



Open each file with HxD and remove redundant part in HTTP post content



3. END