Mid Test

Course code: FRS301

Student name:	**Huynh Ngoc Quang**
Student ID:	**SE181838**

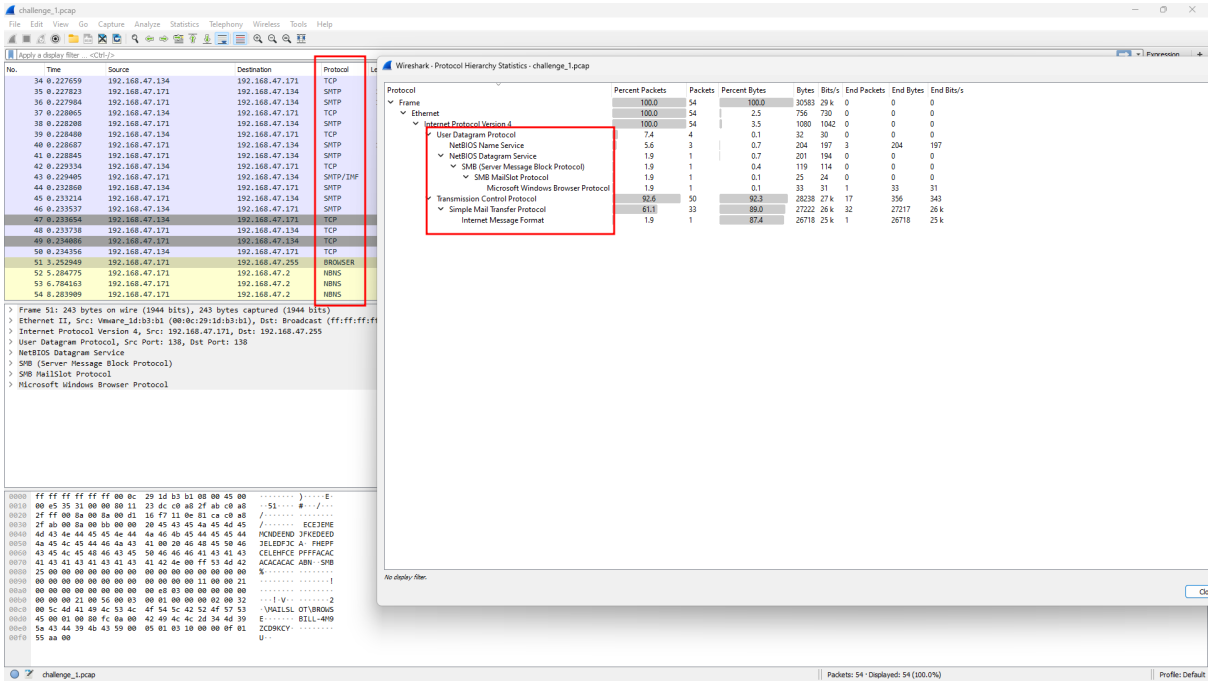
Note: Support your work by taking screenshots

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

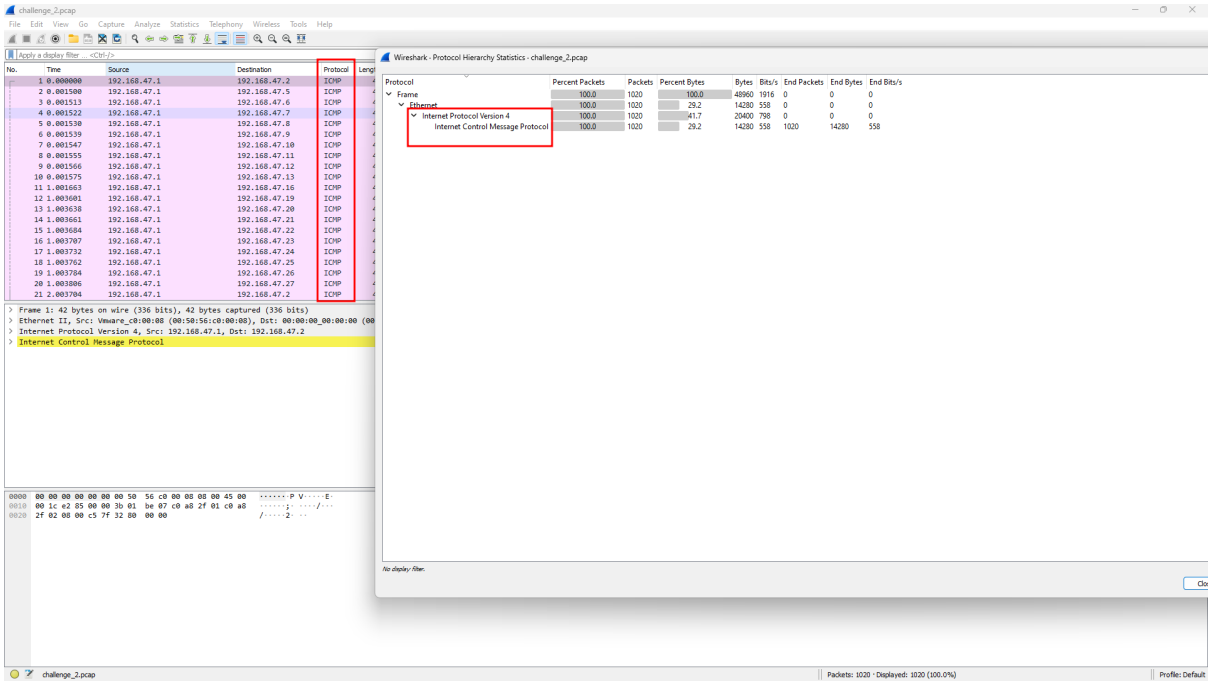
1. What protocols are used?



Ans:

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

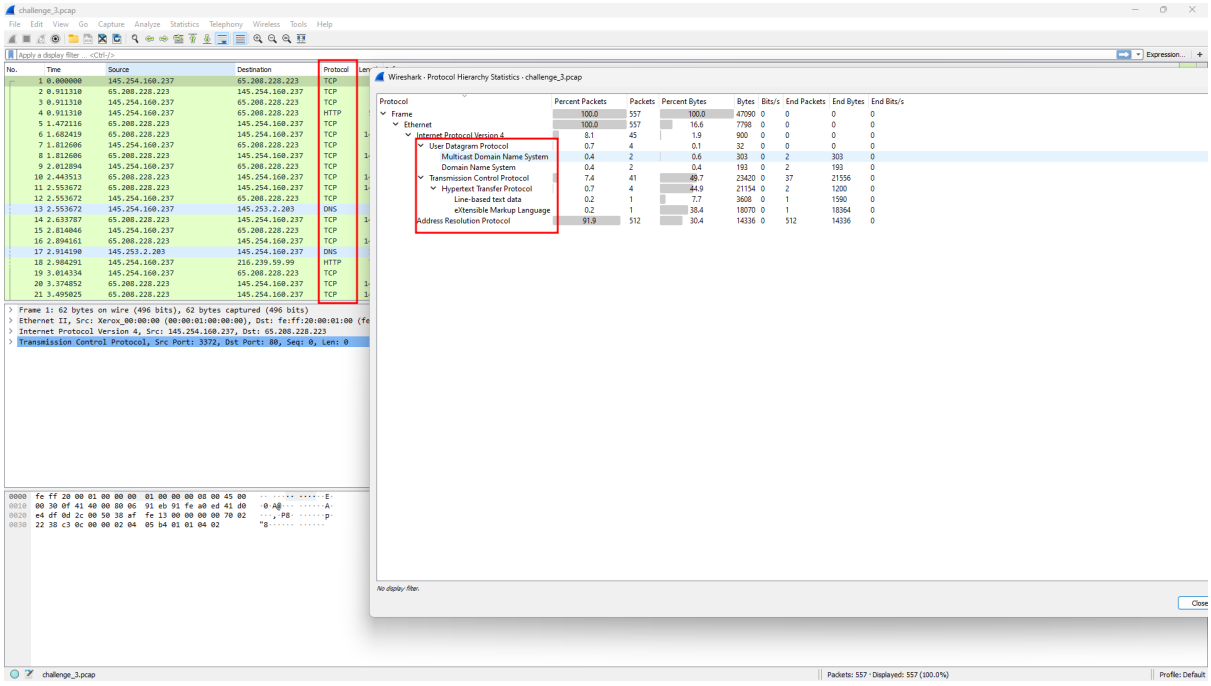
- *TCP (Transmission Control Protocol)*
- *SMTP (Simple Mail Transfer Protocol)*
- *IMF (Internet Message Format)*
- *BROWSER (Microsoft Windows Browser Protocol)*
- *NBNS (NetBIOS Name Service)*



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-230919194867362 9&random=1084443430285&lmt=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

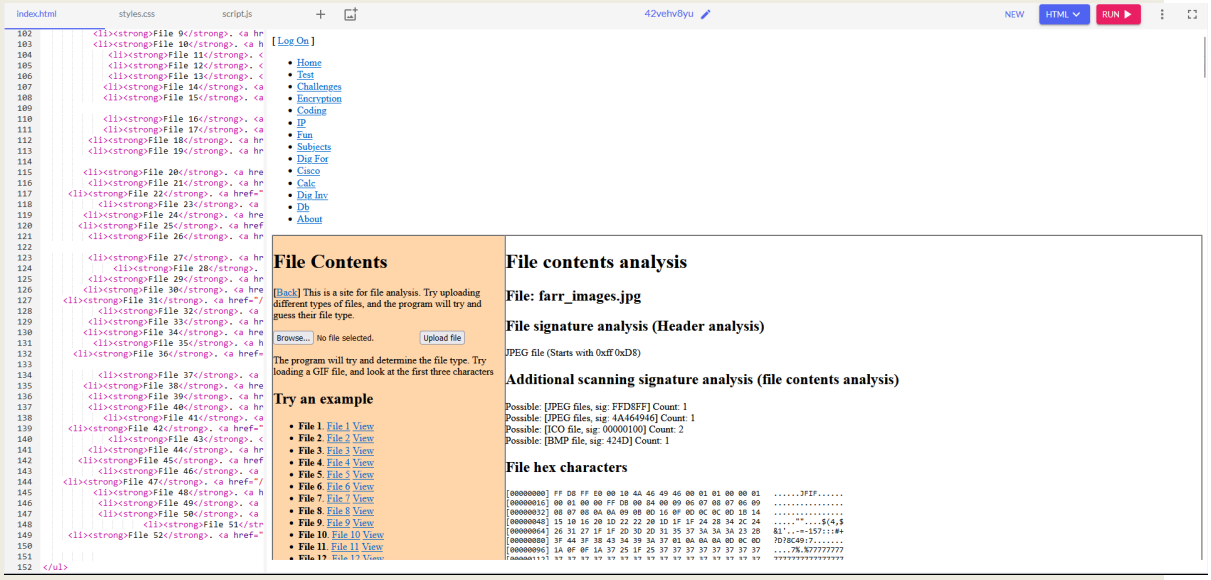
Step 1: Analyze the pcap files: findContent.pcap

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:

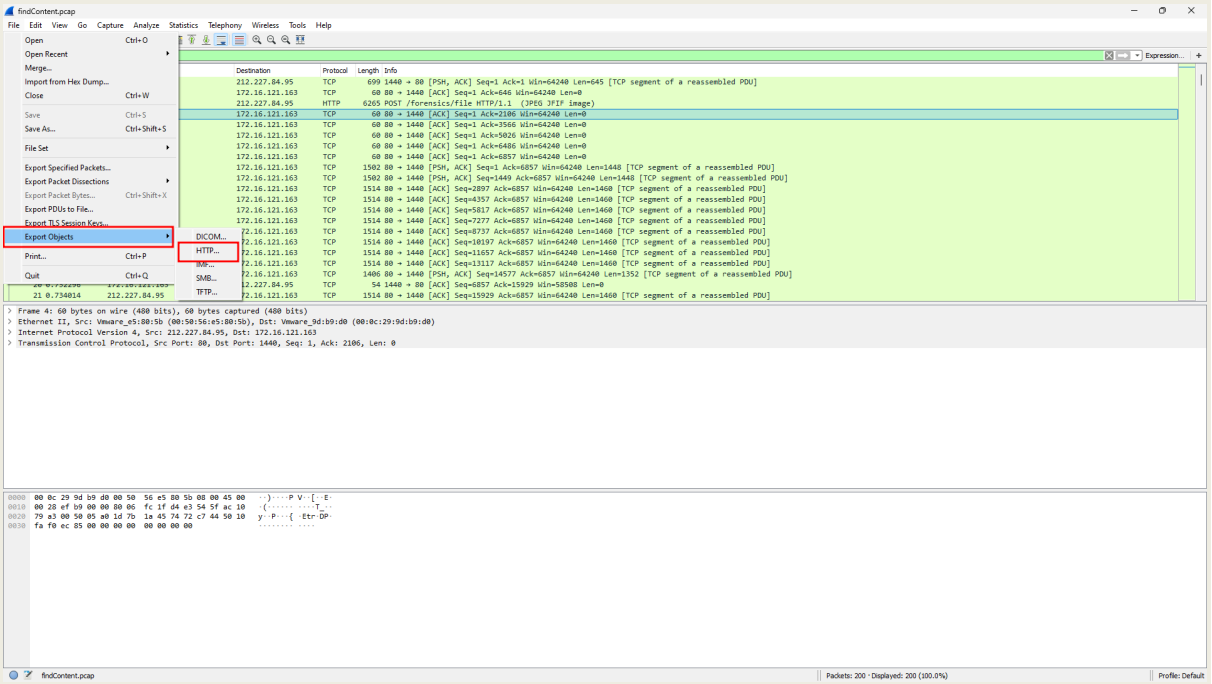
- *The machine with IP 172.16.121.163 connect the web server with IP 212.227.84.95 and send a POST request with some image (JPEG) to "/forensics/file"*
    - *farr_images.jpg*
    - *John_Napier_(Neper).jpg*
    - *150845-apple_laserwriter_original.jpg*
- *After each image POST the server return the analysis of that file like below*



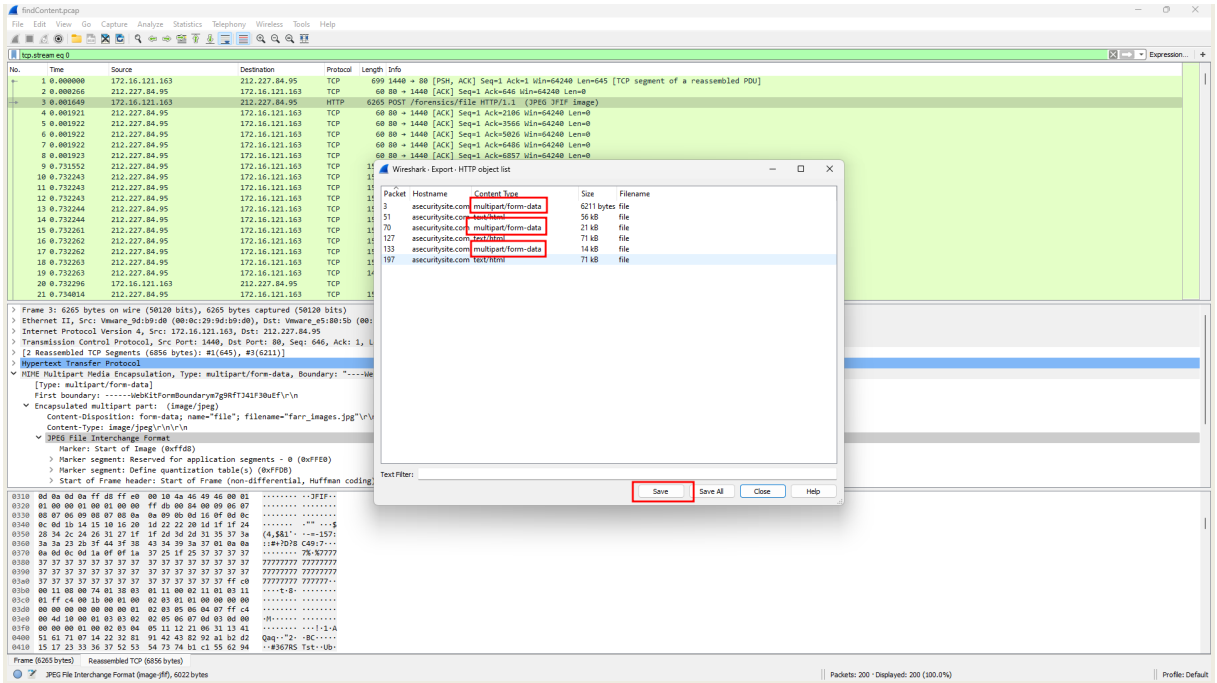
2. Show the files you found. Explain in detail how you found the files.

Ans:

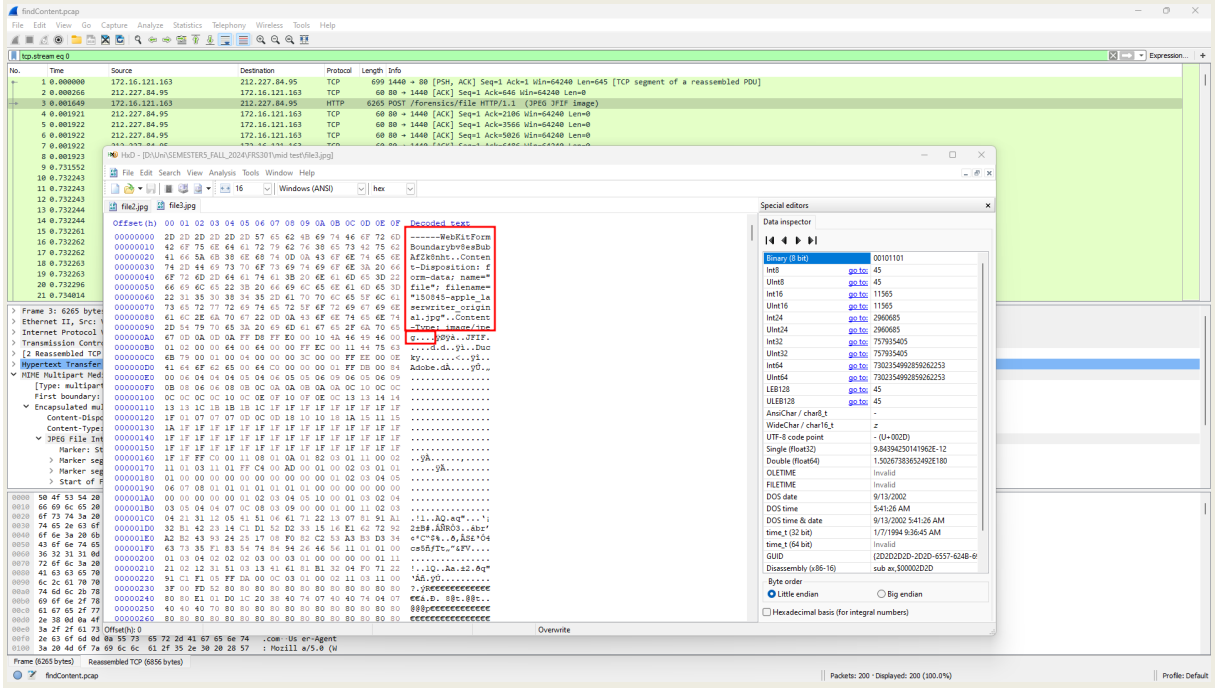
How to get it?



Save 3 image file



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



3. END