**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?

A screenshot of a computer

Description automatically generated

*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)*

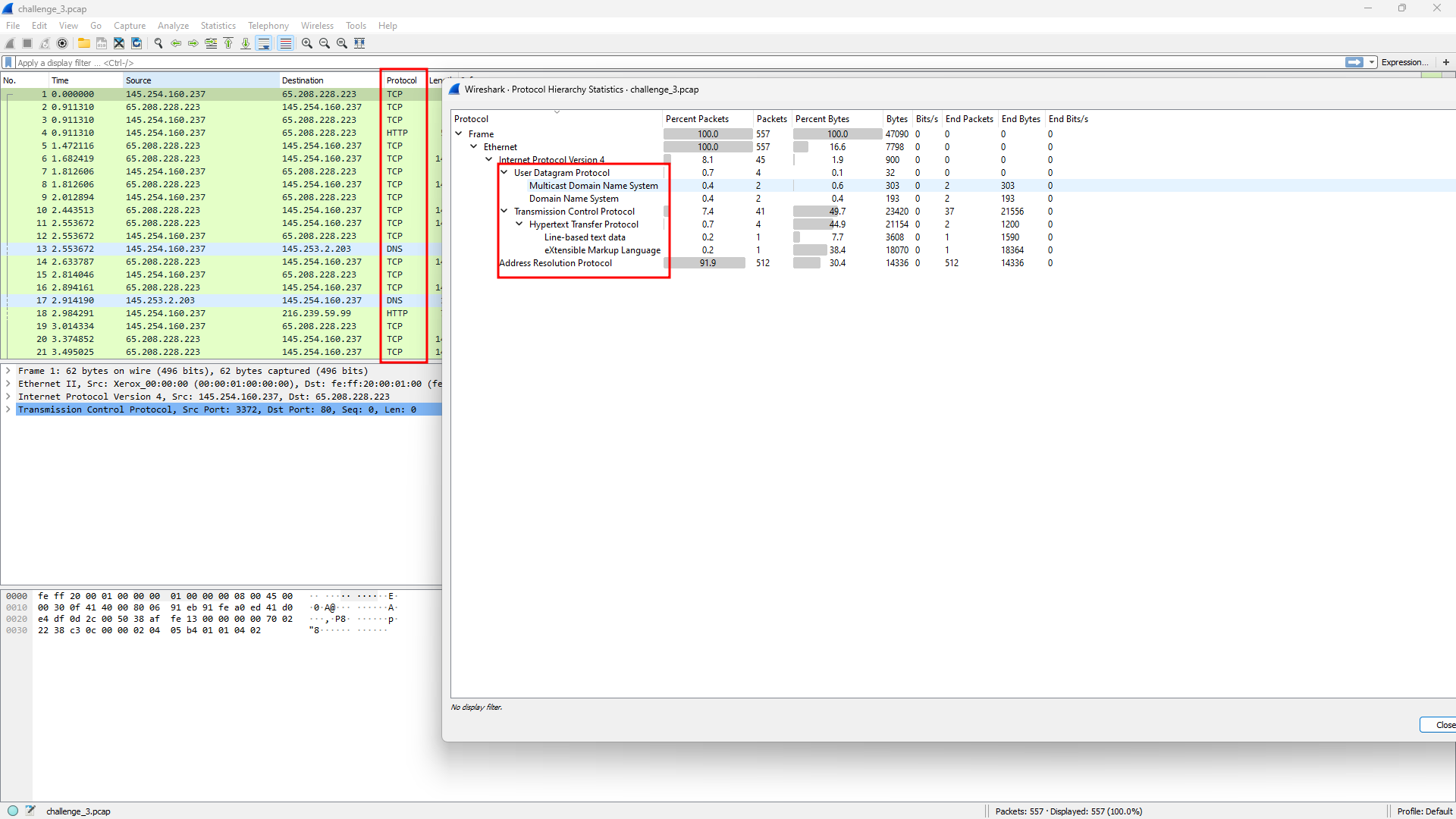
A screenshot of a computer

Description automatically generated

*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)*

1. 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*](mailto:w.buchanan@napier.ac.uk) *to* [*test@home.com*](mailto: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*](http://www.ethereal.com) *from the “Referer:* [*http://www.ethereal.com/development.html*](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&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*

A screenshot of a computer

Description automatically generated

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

*Ans:*

*A logo with blue text

Description automatically generated*

*A portrait of a person with a beard

Description automatically generated*

*An old computer printer

Description automatically generated*

*How to get it?*

A screenshot of a computer

Description automatically generated

*Save 3 image file*

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

1. **END**