Roll No.: CB.EN.U4CYS21017

Amrita Vishwa Vidyapeetham

Amrita School of Engineering, Coimbatore

B.Tech End-Sem Examinations – July 2022

Second Semester

Computer Science Engineering (Cyber Security)

20CYS114 Cyber Security Essentials

Lab Evaluation

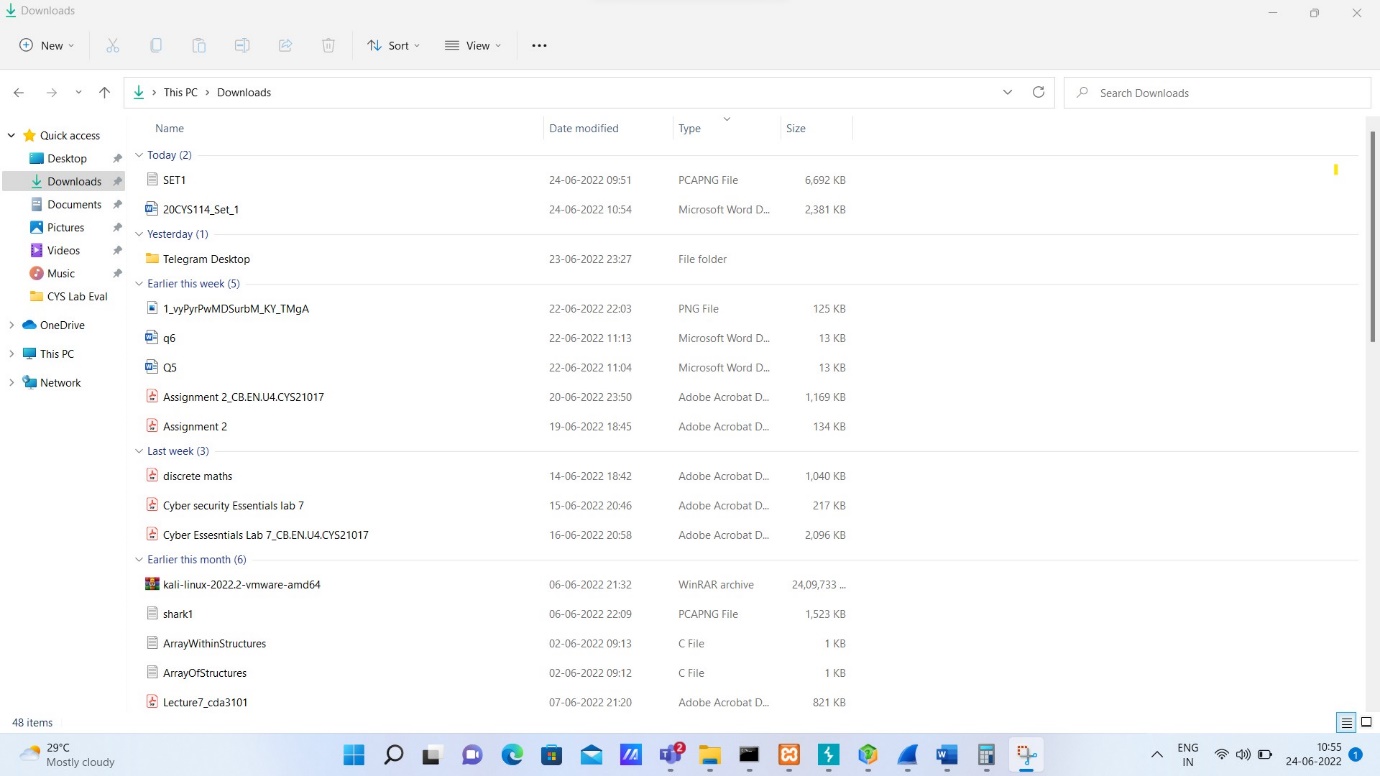
**SET 1**

**Write your answer and attach screenshots for all answers. The screenshot must capture the time of the system.**

**Part A**

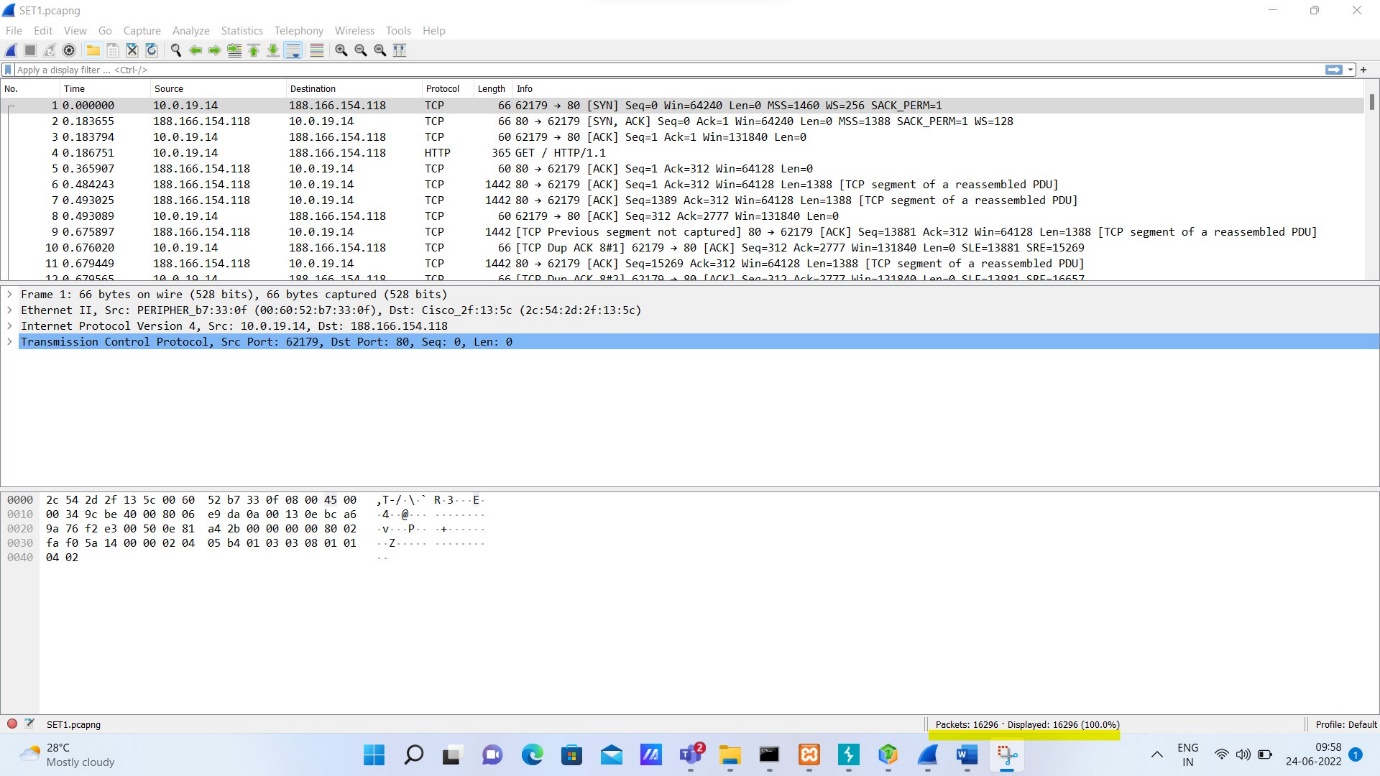
1. Rename the given file (SET1) with the correct traffic capture file type so that you can open it to analyze and answer the further questions. (like .PDF,. docs).

I renamed the file as SET1.pcapng.



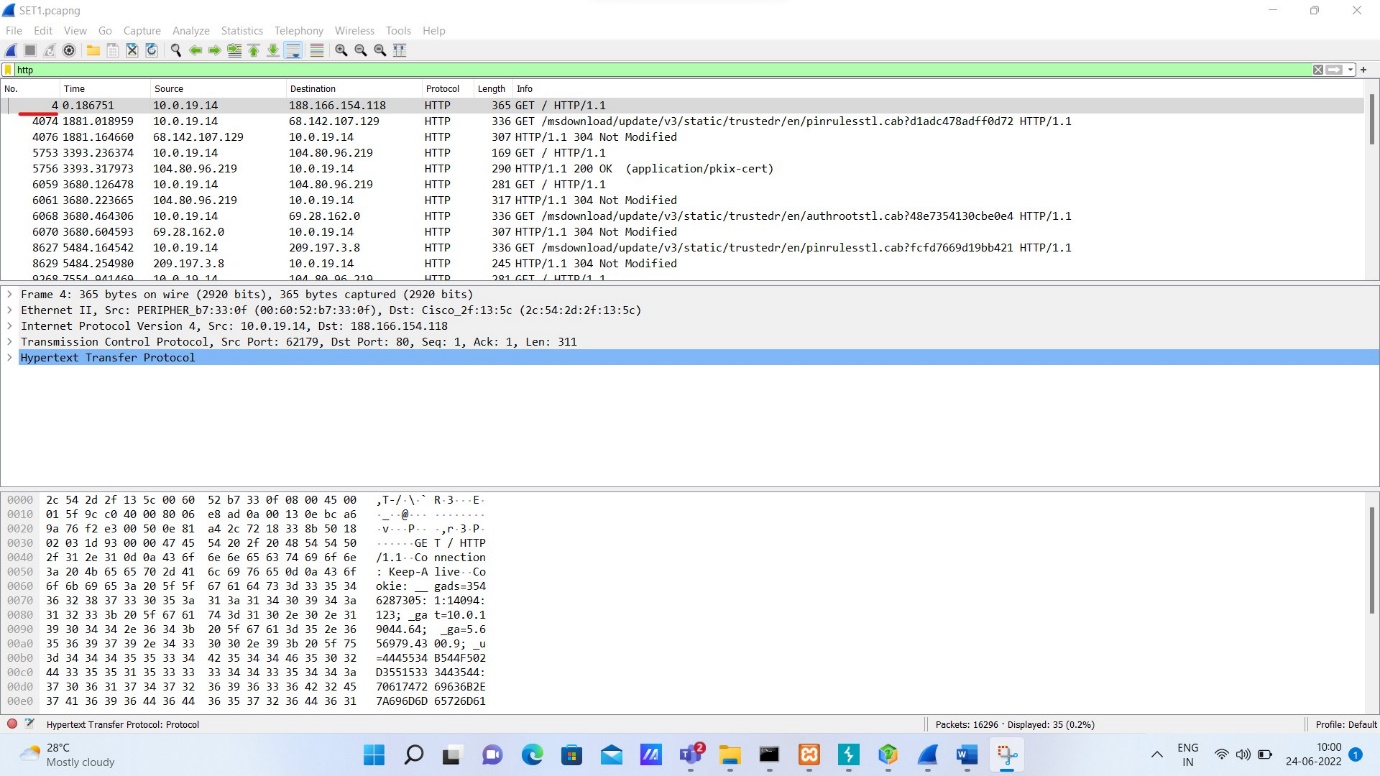
1. What is the total number of packets displayed without adding any filters?

The total number of packets displayed without applying any filter is 16296.



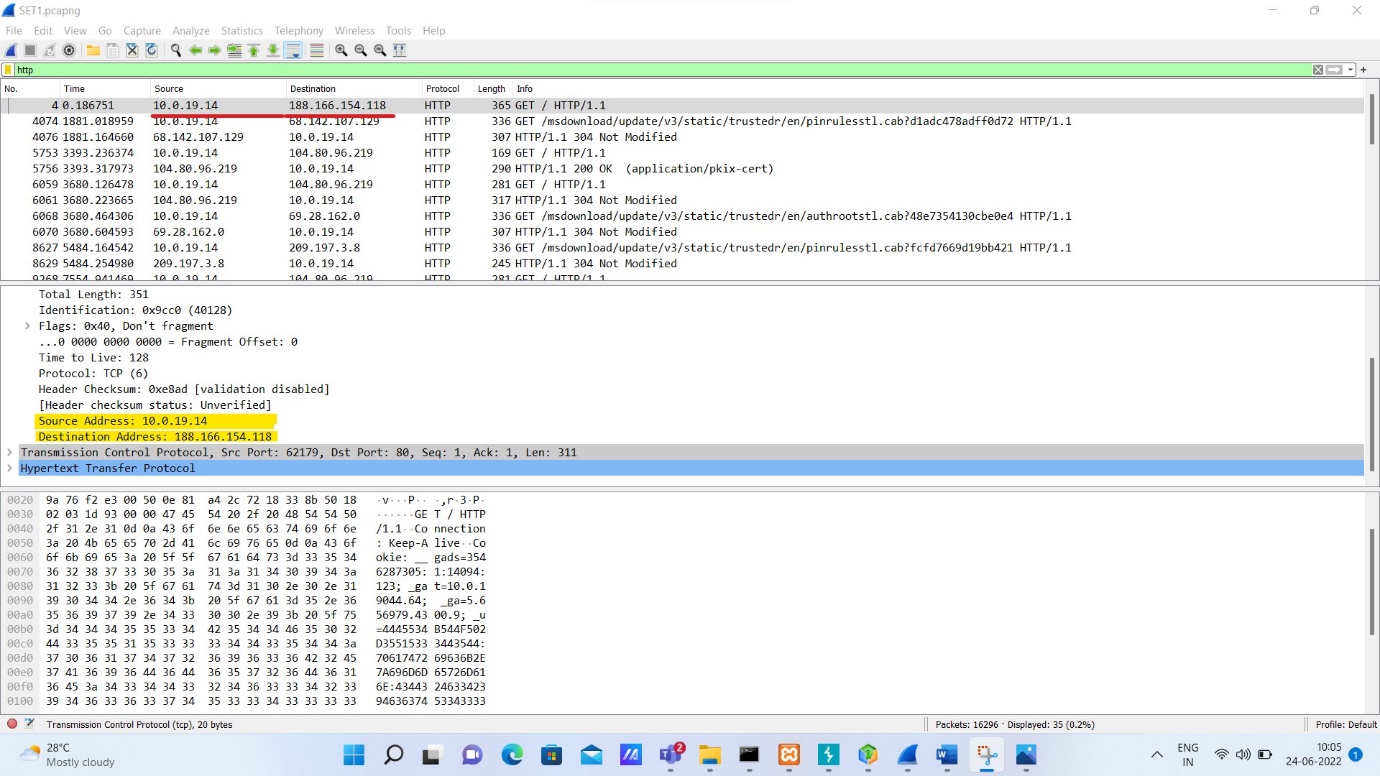
1. What is the packet number of the first HTTP traffic?

The packet number of the first HTTP traffic is 4.



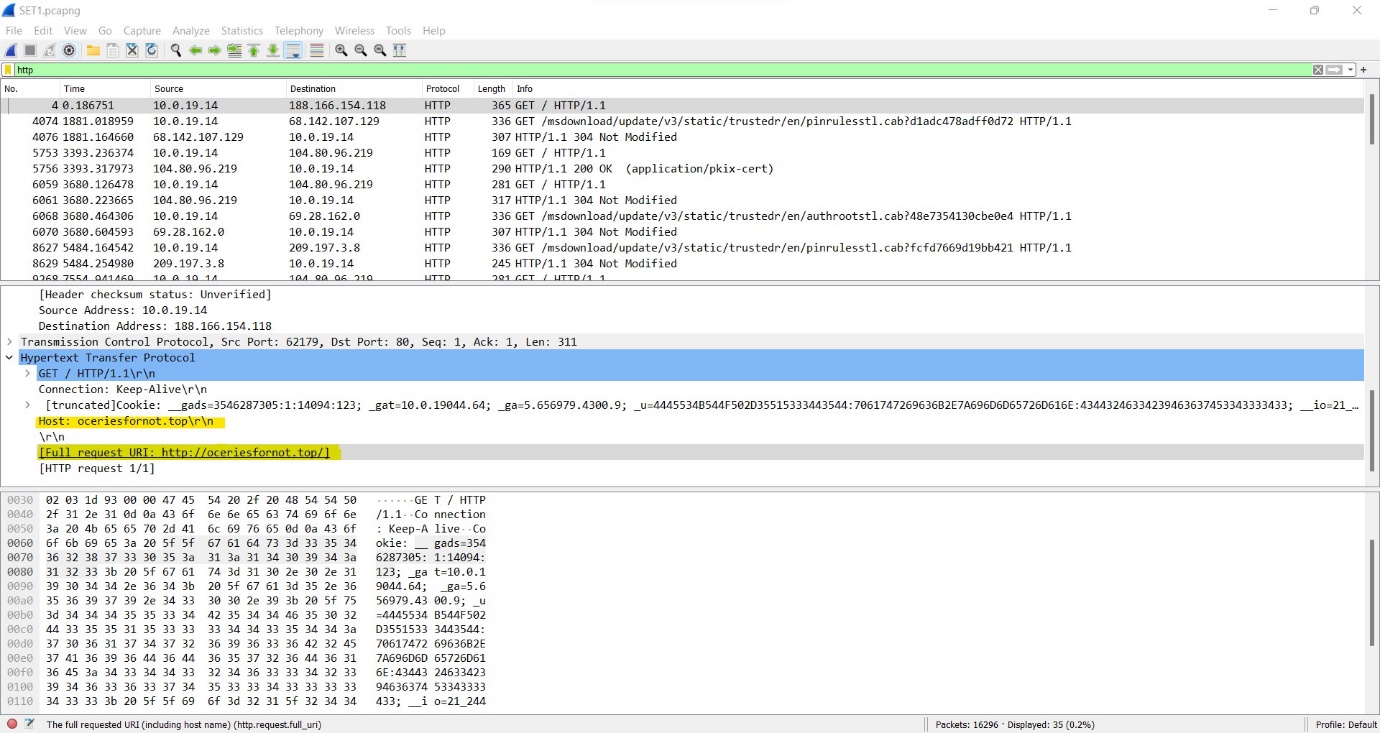
1. What is the Source and Destination IP of the packet which you have noticed above?

The Source and Destination IP of the packet is 10.0.19.14 and 188.166.154.118 respectively.



1. What is the hostname of the URL visited by the user with the unencrypted web traffic?

The hostname of the URL visited by the user with the unencrypted web traffic is oceriesfornot.top.



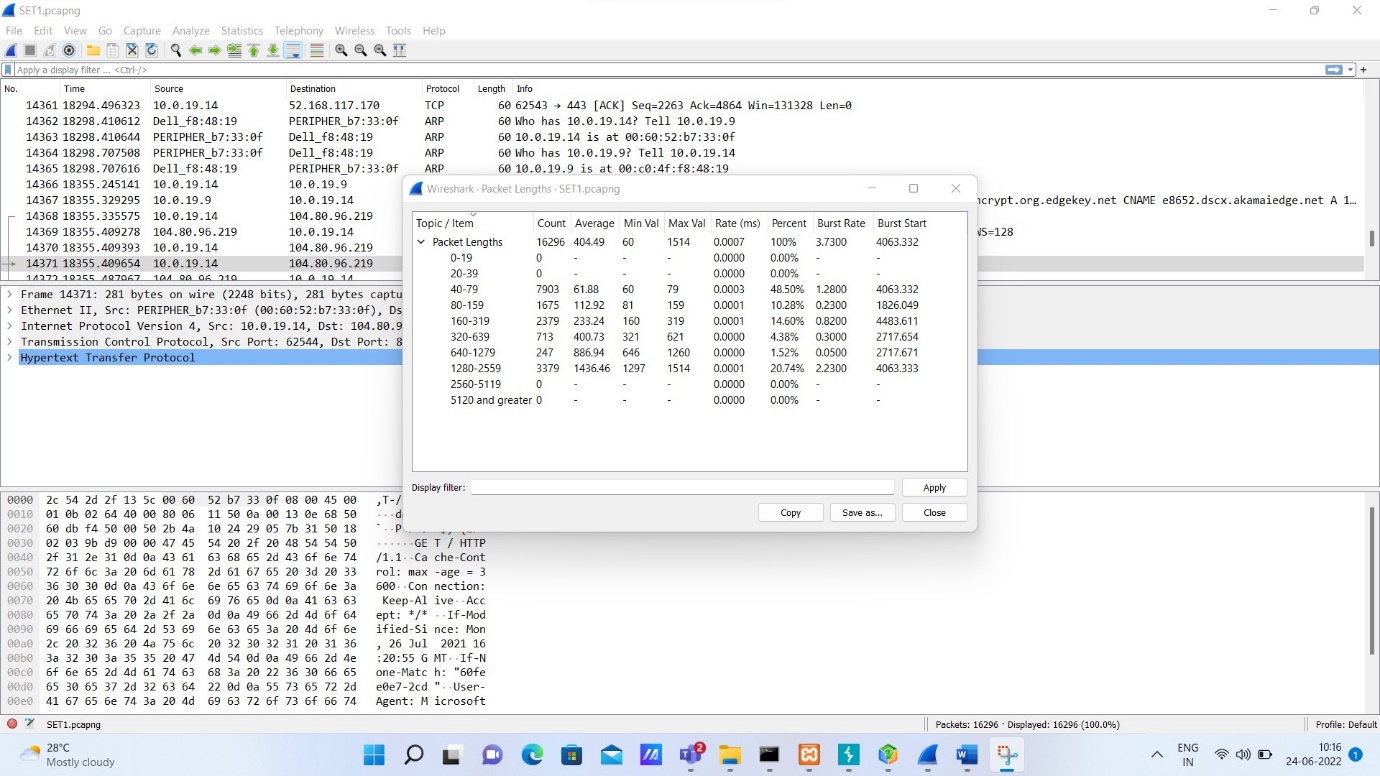
1. What is the user-agent for the packet 14371?

The user agent is HTTP.

1. How many packets are there in total with size greater than 640 bytes?

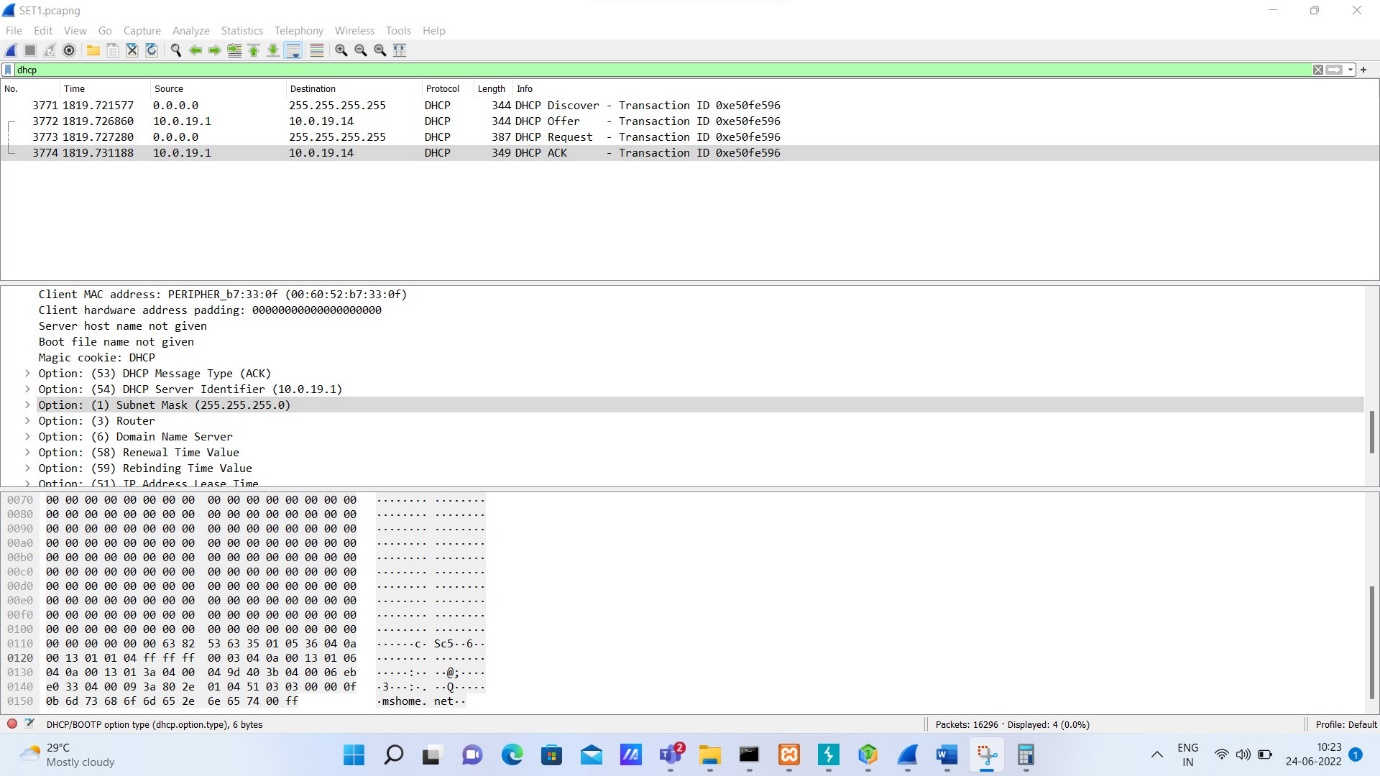
Hint: See statistics tab.

3626 packets are there in total with size greater than 640 bytes.



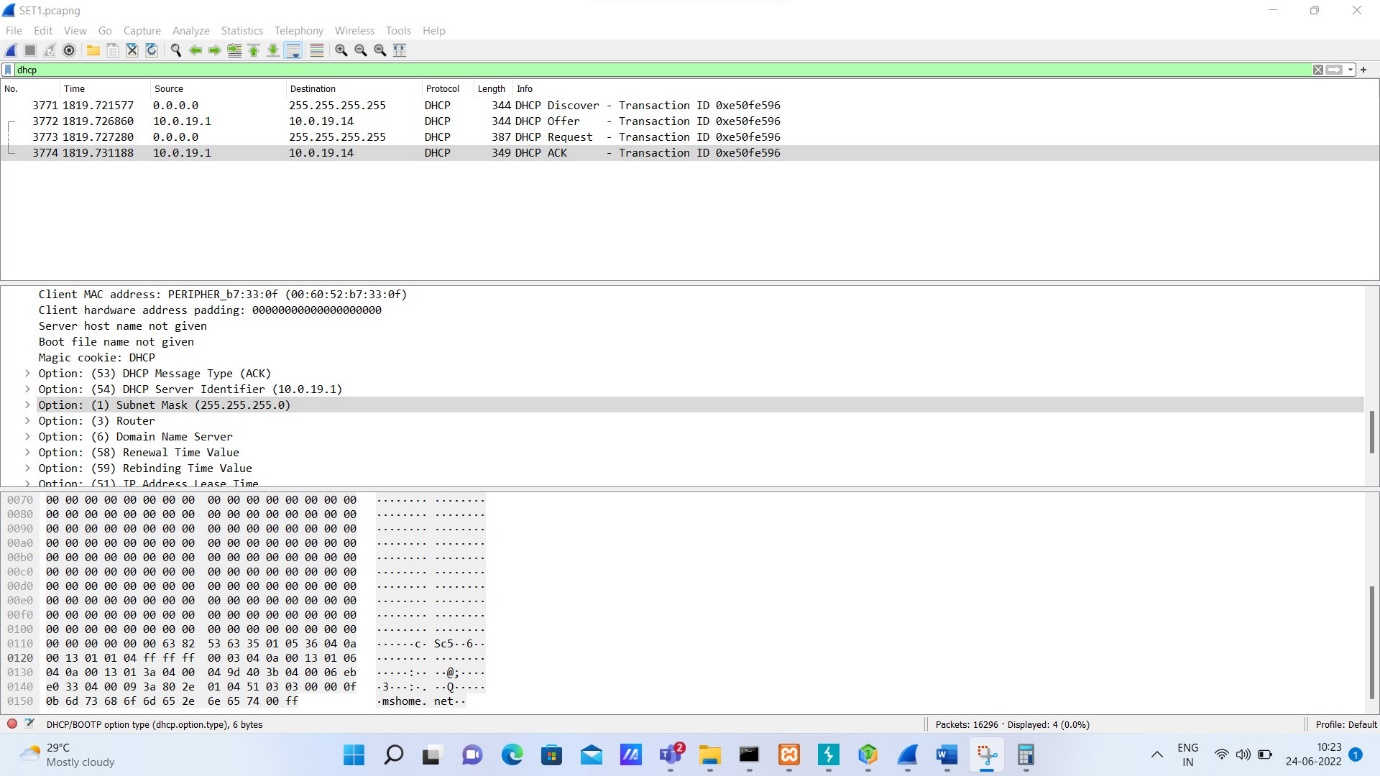
1. Use the DHCP packets to identify what is the subnet mask of this networks?

The subnet mask of this networks is 255.255.255.0



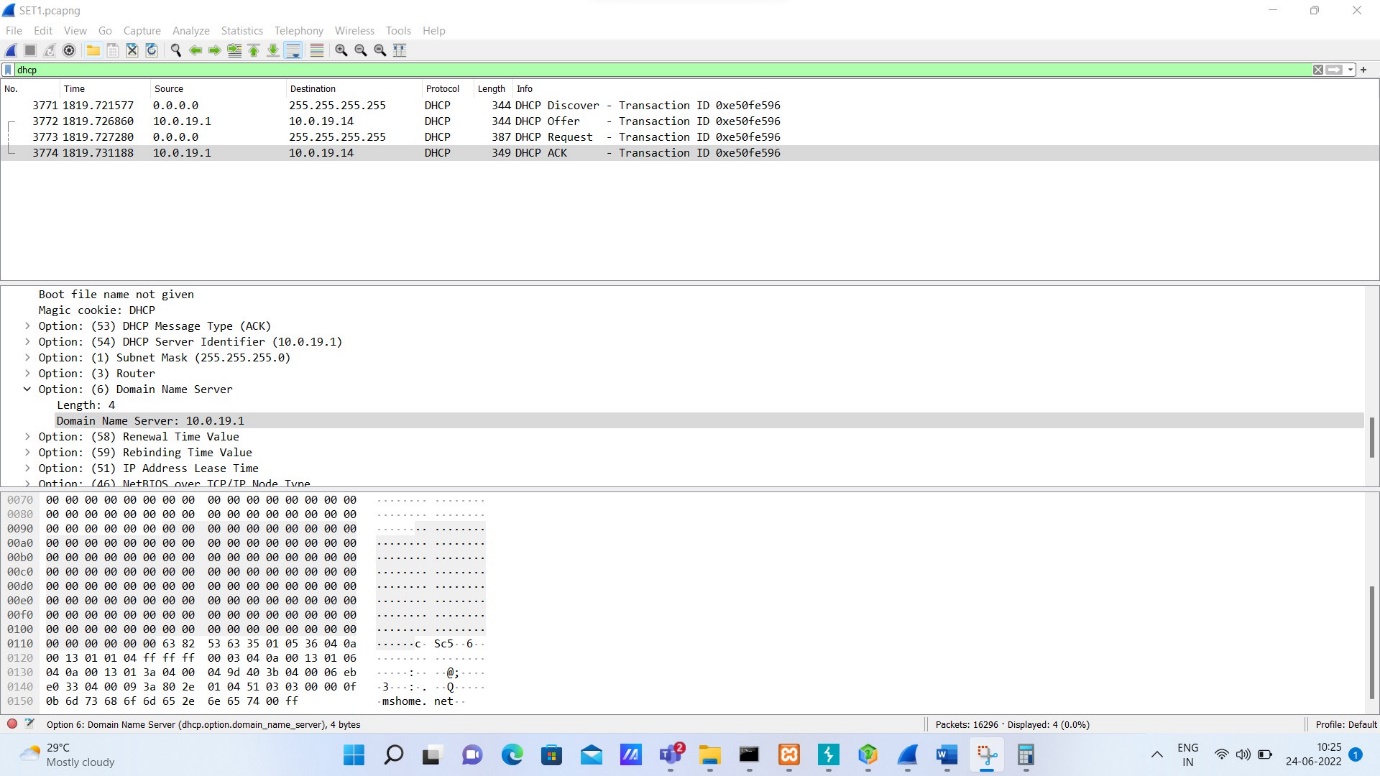
1. What is the magic cookie mentioned in the DHCP traffic?

The magic cookie mentioned in the DHCP traffic id DHCP.



1. What is the DNS server IP address from this traffic?

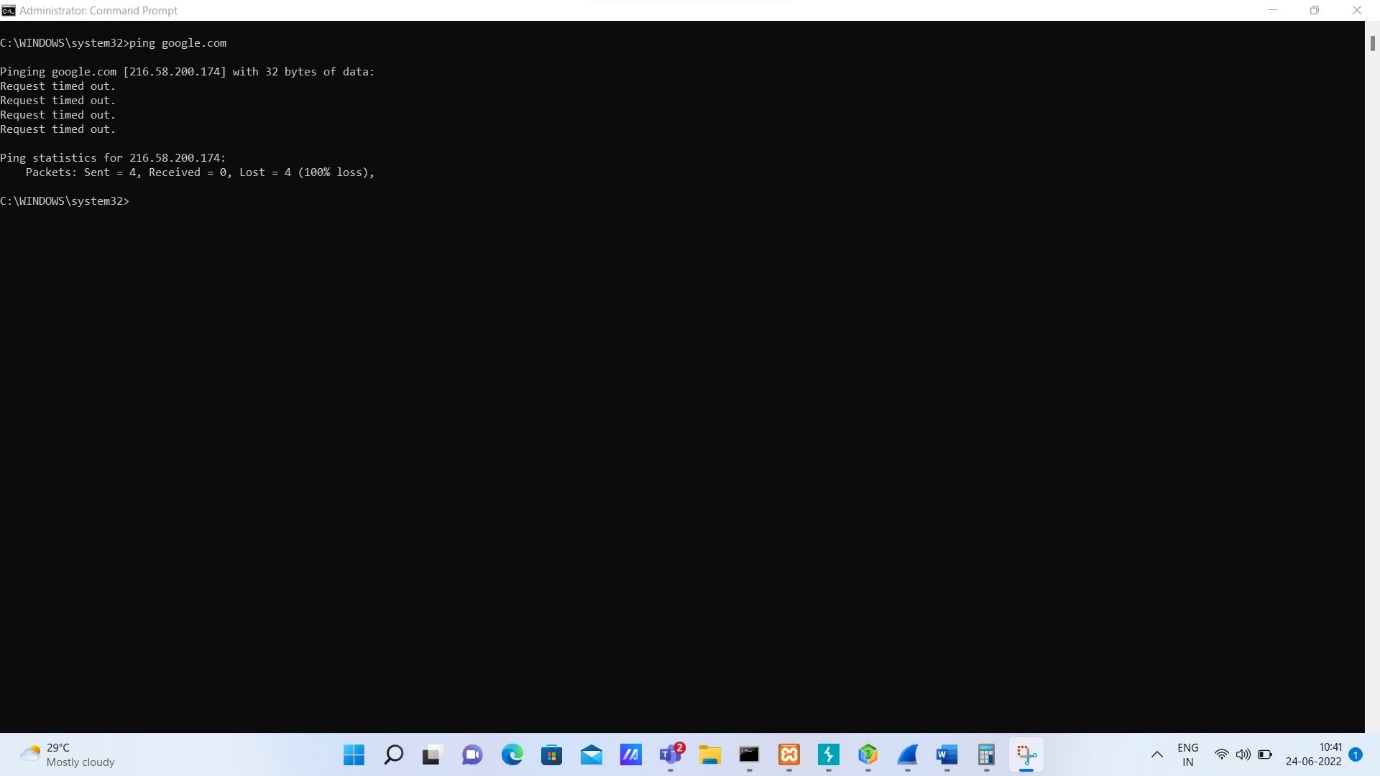
The DNS server IP address from this traffic is 10.0.19.4



**Part B**

1. Explain ping command. Run and show the output. Explain it.

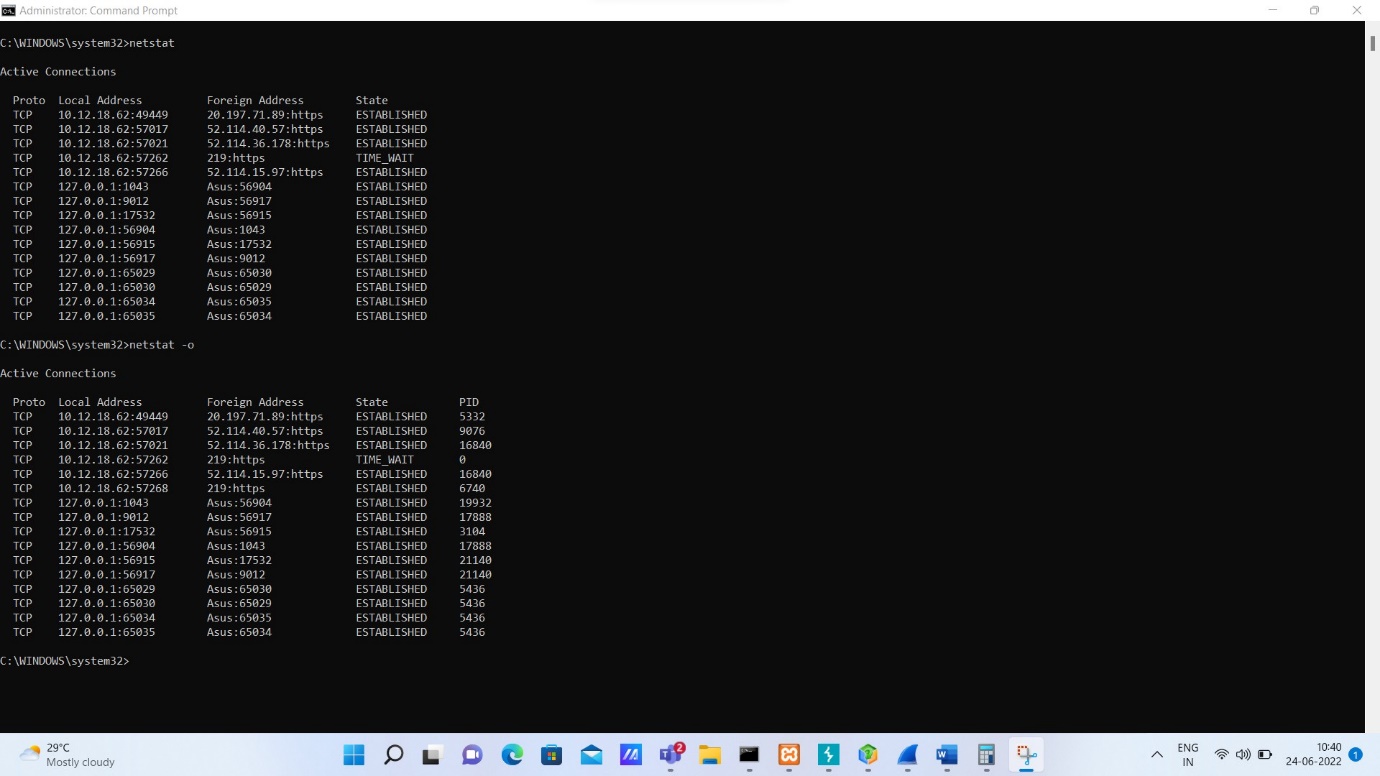
The ping command is used to test if you can reach your target and how much time it will take to do it. When you use this command, you will send few echo requests, usually 4.



Since I used the Campus Wi-fi I couldn’t get the desired result. All my four request were sent but my system wasn’t able to receive it back because the Wi-fi blocked it.

1. What netstat command does. Show and explain the output.

The netstat command displays all the active TCP/IP ports and the command netstat -o displays the same result as the netstat command along with their PID for each port.



1. Explain the below code snippet in detail. Explicitly explain the line in bold.

$SELECT = "SELECT email From signup Where email=? Limit 1";  
$INSERT = "INSERT Into signup (username, password, gender, email) values (?,?,?,?)";   
$stmt = $conn->prepare($SELECT);  
$stmt->bind\_param("s", $email);  
$stmt->execute();  
$stmt->bind\_result($email);  
$stmt->store\_result();  
$rnum = $stmt->num\_rows;   
**if ($rnum == 0){**

$stmt->close();

$stmt = $conn->prepare($INSERT);

$stmt->bind\_param("ssss", $username, $password, $gender, $email);

$stmt->execute();

}

To singup I give my username, password, gender and email and email should be unique for each entry. Then it will store it in the database.

**Explaination if ($rnum == 0)**

When I signup in that particular website and it will ask my email, if in case my email isn’t in the unique it will direct me to the signup page