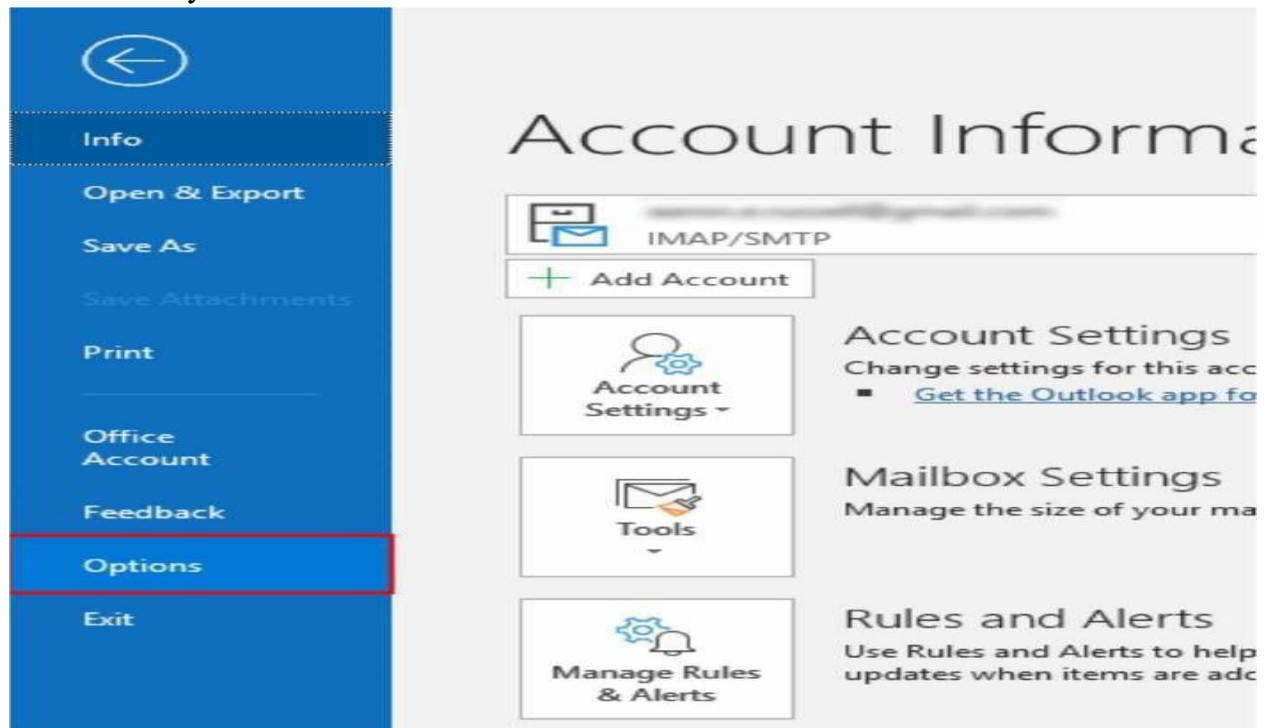


Name: Saish Baviskar  
Div: A Roll No: TEAD23155

## Practical No. 9

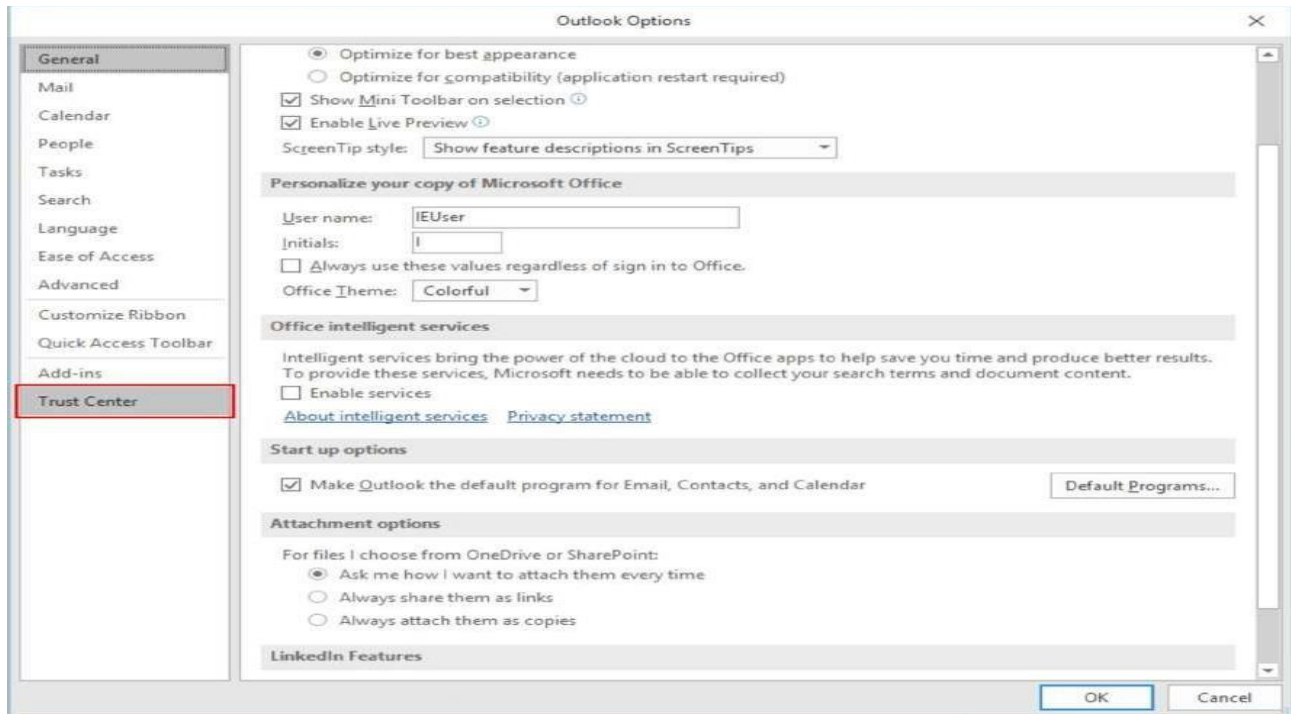
Problem Statement: Illustrate the steps for S/MIME implementation in Microsoft Outlook

1. Download your certificate.

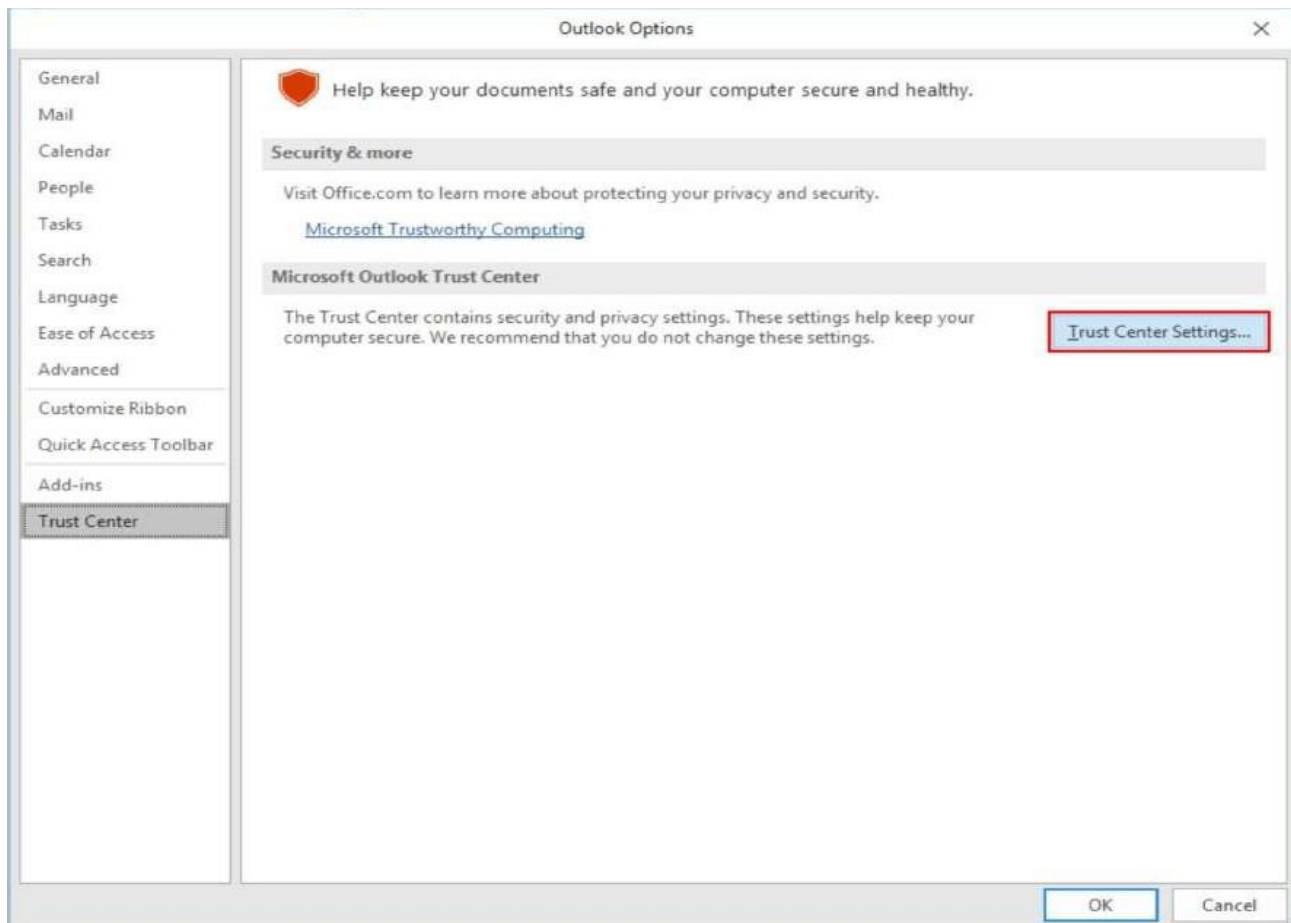


Download a PKCS#12 file with your certificate from your SSL.com account by clicking the link supplied  
Open Outlook Options

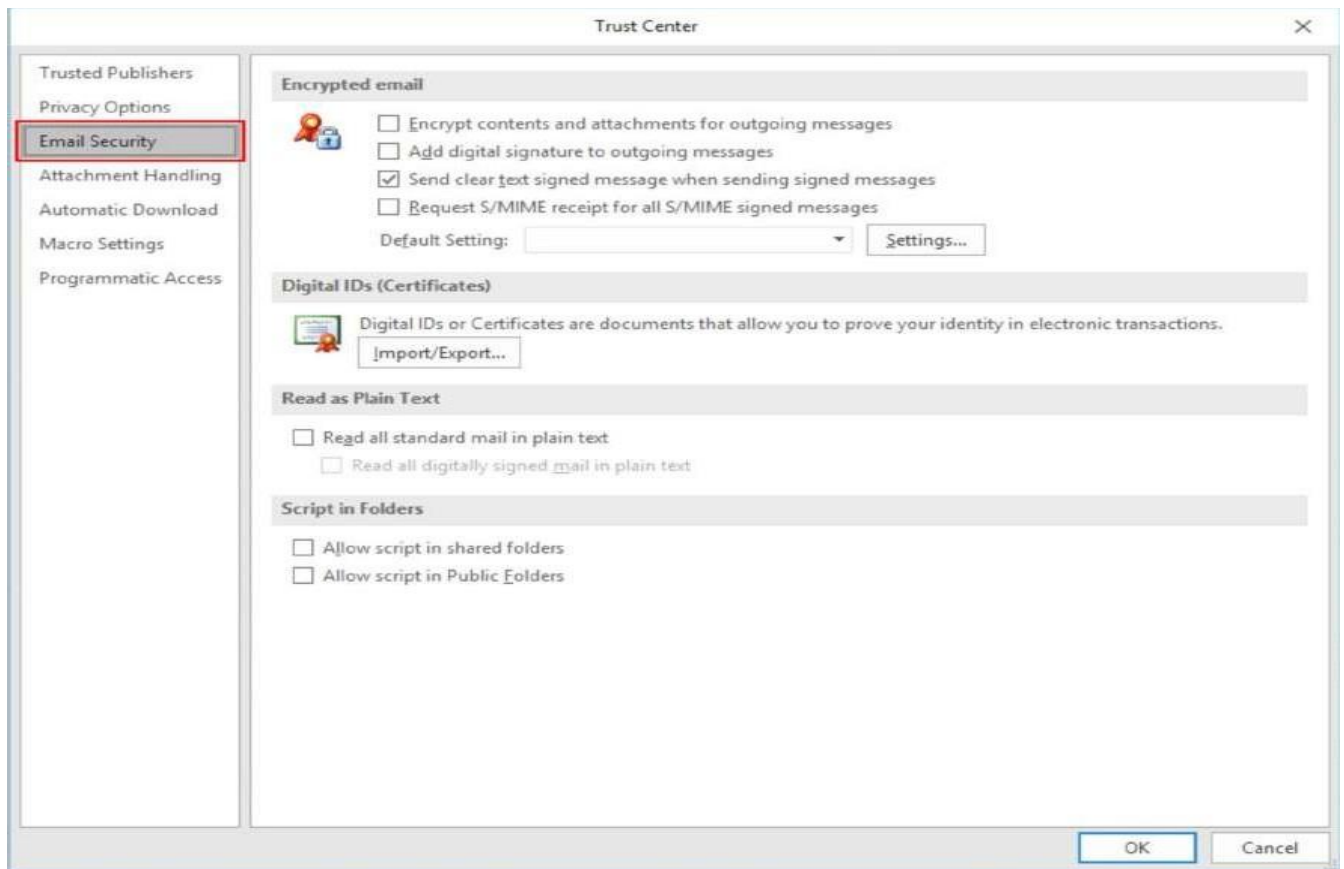
Open Trust Centre.



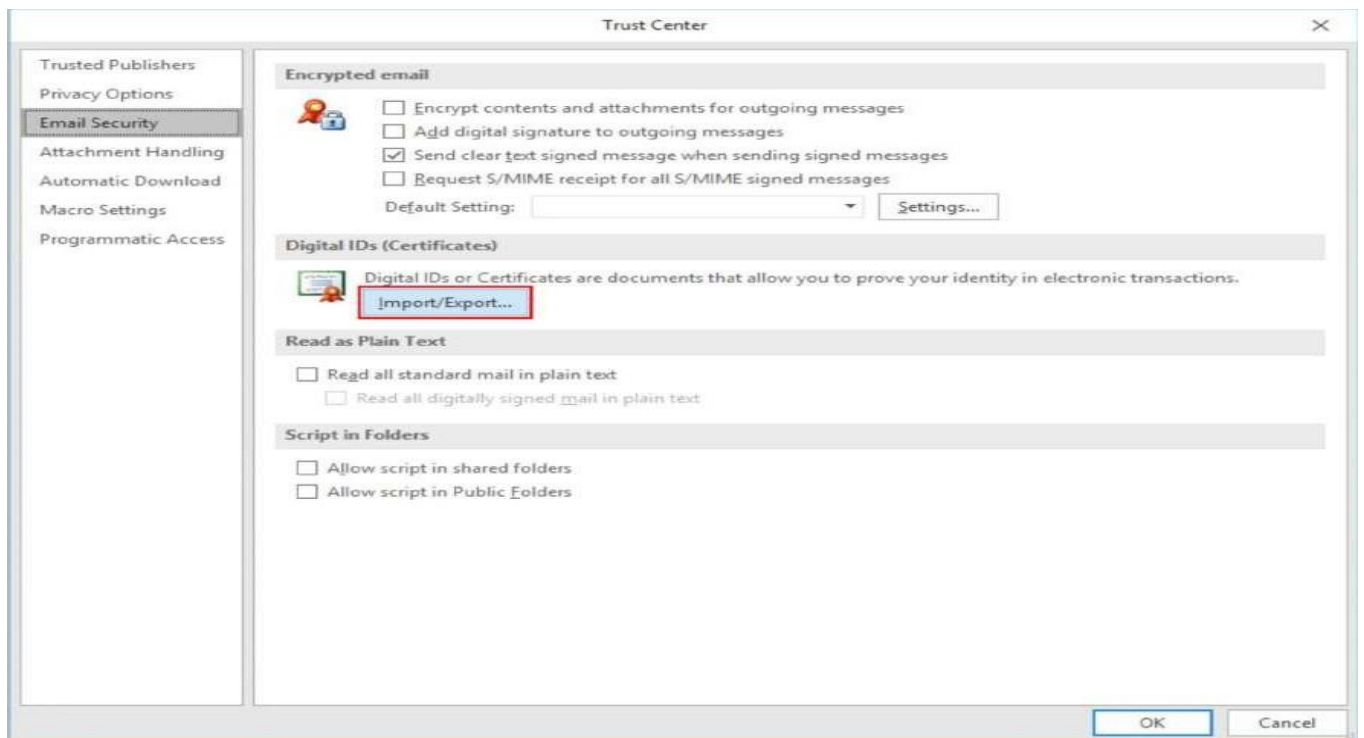
Open Trust Centre Settings.



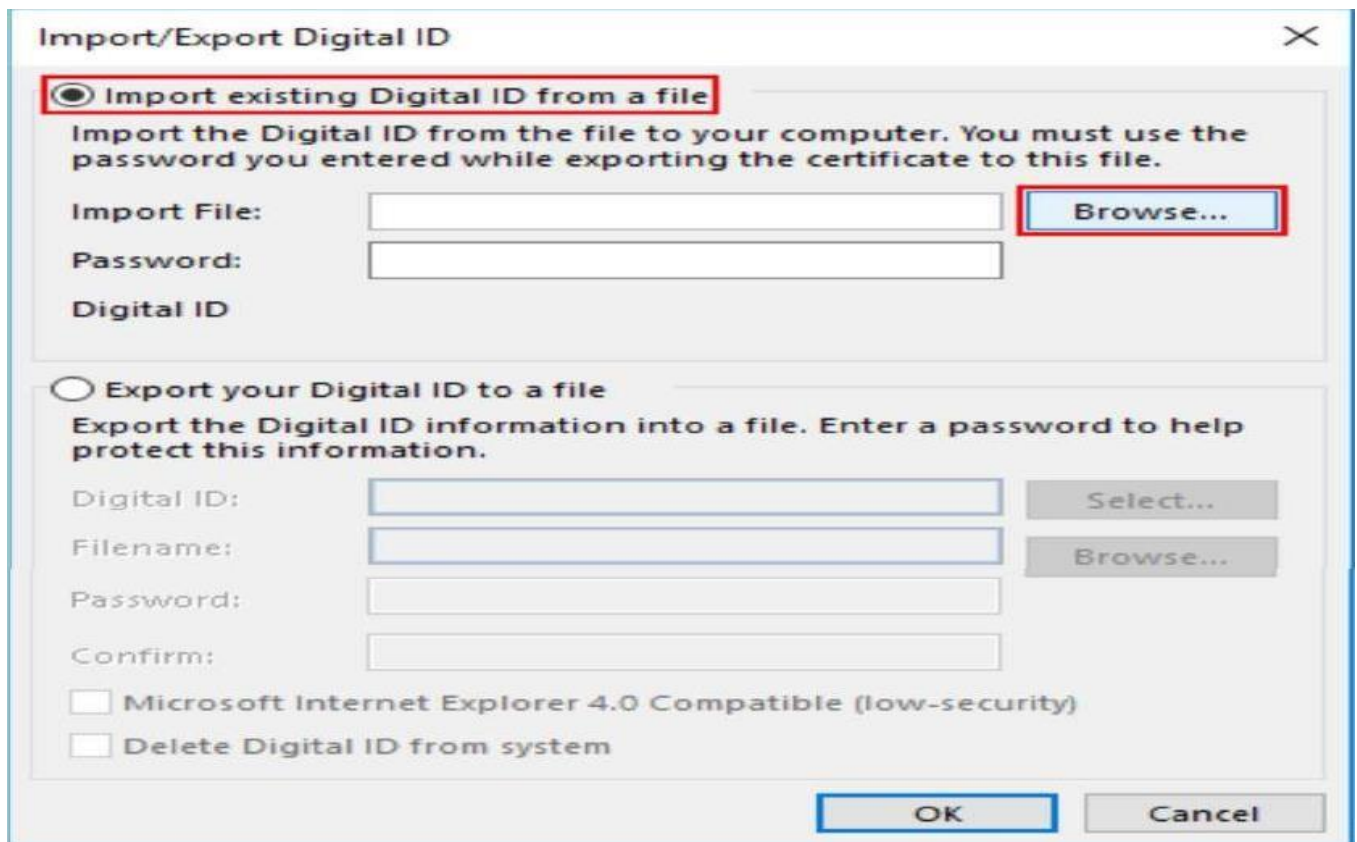
Select Email Security



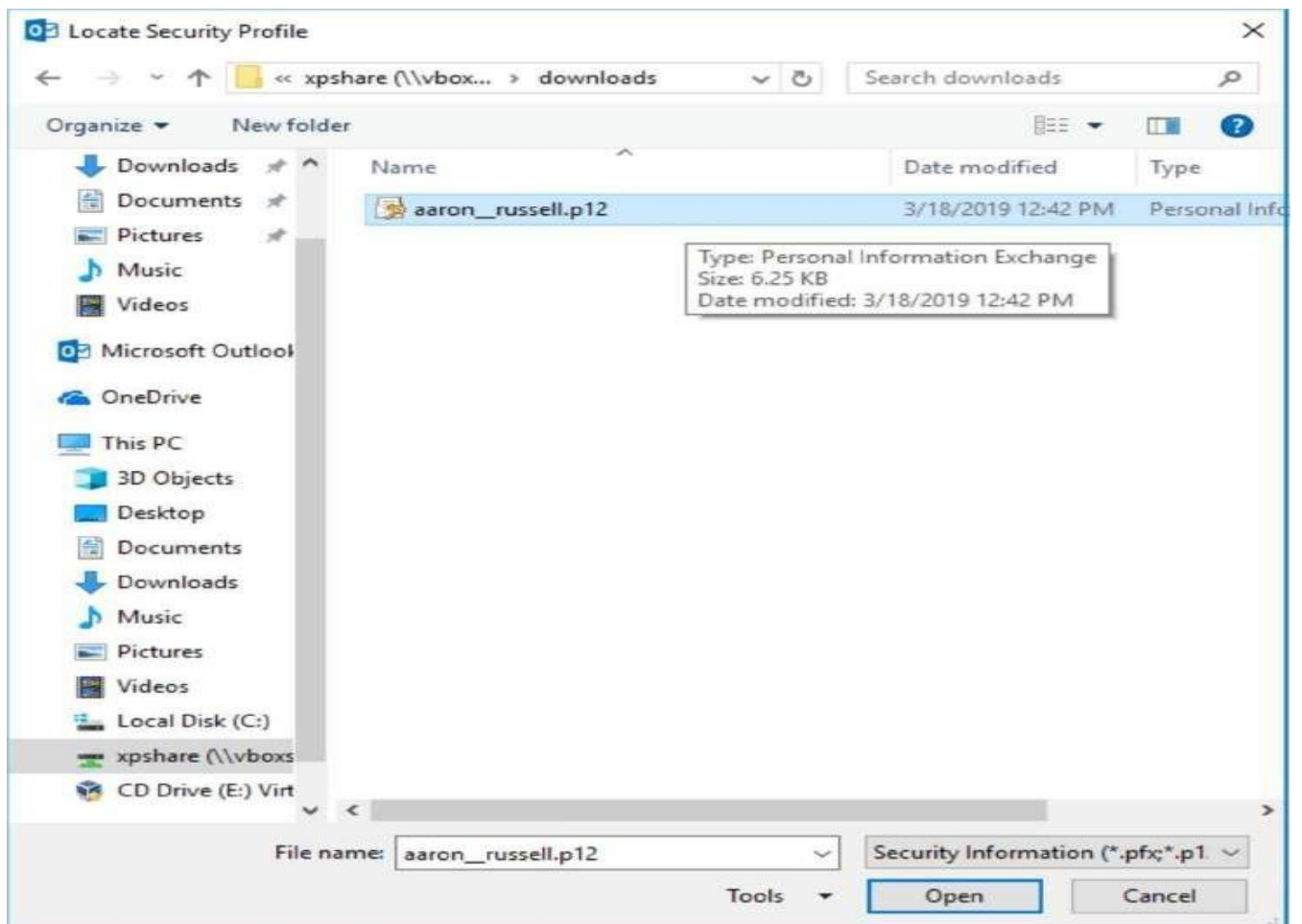
Click Import/Export.



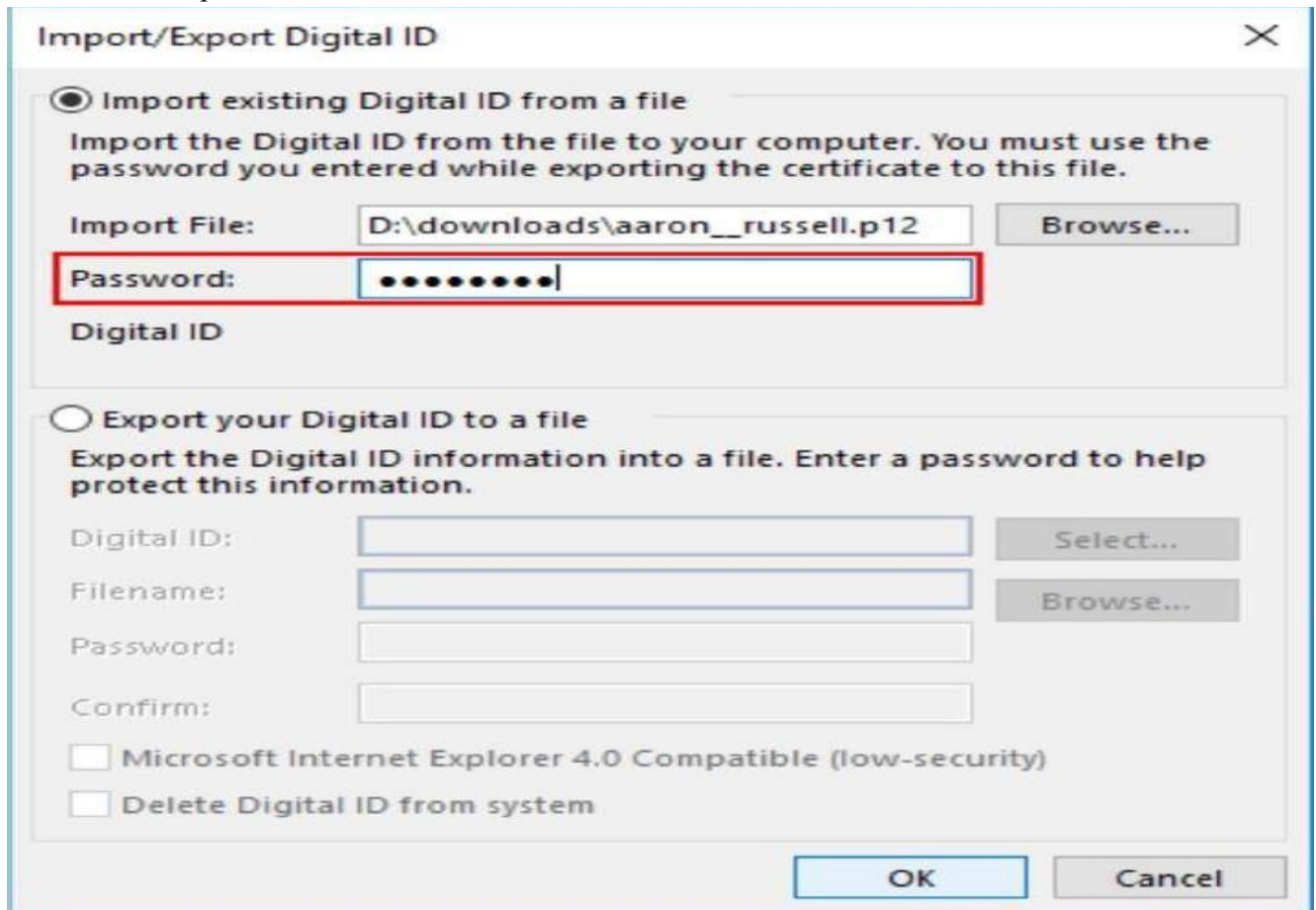
Browse for file



Open File.



Enter PKCS#12 password.



The dialog box is titled "Import/Export Digital ID" and has a close button (X) in the top right corner. It contains two main sections. The first section, "Import existing Digital ID from a file", is selected with a radio button. It includes instructions: "Import the Digital ID from the file to your computer. You must use the password you entered while exporting the certificate to this file." Below this, there is an "Import File:" label followed by a text box containing "D:\downloads\aaaron\_\_russell.p12" and a "Browse..." button. A red rectangle highlights the "Password:" label and its corresponding text box, which contains ten dots. Below the password field is the label "Digital ID". The second section, "Export your Digital ID to a file", is unselected. It includes instructions: "Export the Digital ID information into a file. Enter a password to help protect this information." Below this, there are four text boxes labeled "Digital ID:", "Filename:", "Password:", and "Confirm:", each followed by a "Select..." or "Browse..." button. At the bottom of the second section, there are two checkboxes: "Microsoft Internet Explorer 4.0 Compatible (low-security)" and "Delete Digital ID from system". At the bottom of the dialog box are "OK" and "Cancel" buttons.

**Import/Export Digital ID**

☒ **Import existing Digital ID from a file**  
Import the Digital ID from the file to your computer. You must use the password you entered while exporting the certificate to this file.

Import File: D:\downloads\aaaron\_\_russell.p12 **Browse...**

**Password:** ..... **Digital ID**

☐ **Export your Digital ID to a file**  
Export the Digital ID information into a file. Enter a password to help protect this information.

Digital ID:  **Select...**

Filename:  **Browse...**

Password:

Confirm:

☐ Microsoft Internet Explorer 4.0 Compatible (low-security)

☐ Delete Digital ID from system

**OK** **Cancel**

Click OK.



The dialog box is titled "Importing a new private exchange key" and has a close button (X) in the top right corner. It features a large teal vertical bar on the left side. The main text area contains the message "An application is creating a Protected item." followed by "CryptoAPI Private Key" and "Security level set to Medium". To the right of the security level text is a "Set Security Level..." button. At the bottom, there are three buttons: "OK", "Cancel", and "Details...". The "OK" button is highlighted with a red rectangle.

**Importing a new private exchange key**

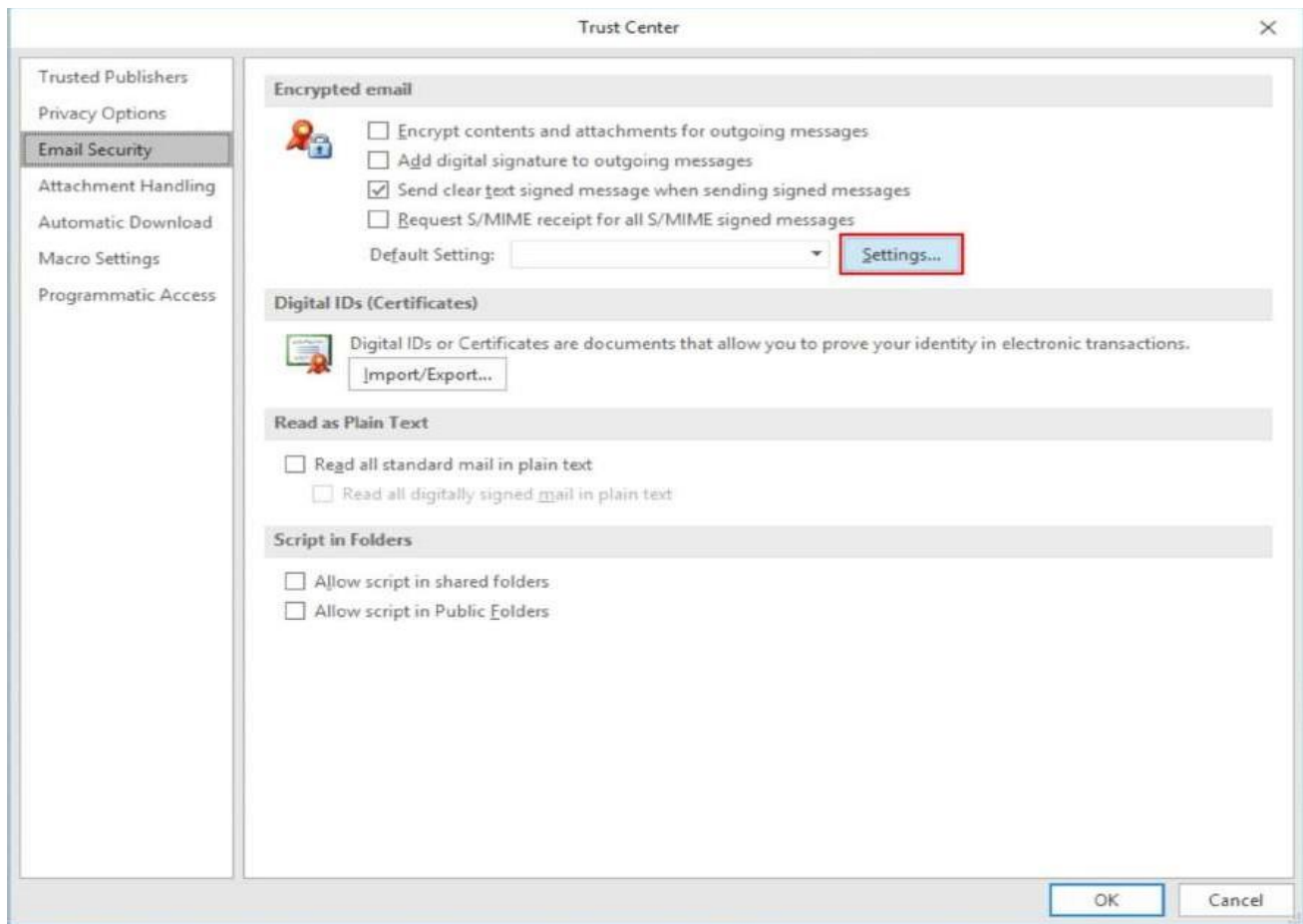
An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium **Set Security Level...**

**OK** **Cancel** **Details...**

Open encrypted email settings.



Name security settings.





Choose signing certificate.



The 'Change Security Settings' dialog box is shown. It has a title bar with a close button. The 'Security Setting Preferences' section includes a dropdown for 'Security Settings Name' (My S/MIME Settings), a dropdown for 'Cryptography Format' (S/MIME), and two checked checkboxes: 'Default Security Setting for this cryptographic message format' and 'Default Security Setting for all cryptographic messages'. Below these are buttons for 'Security Labels...', 'New', and 'Delete'. The 'Certificates and Algorithms' section has fields for 'Signing Certificate' (Aaron Russell), 'Hash Algorithm' (SHA1), 'Encryption Certificate' (Aaron Russell), and 'Encryption Algorithm' (AES (256-bit)). The 'Signing Certificate' and 'Encryption Certificate' fields have 'Choose...' buttons next to them. At the bottom, there is a checked checkbox 'Send these certificates with signed messages' and 'OK' and 'Cancel' buttons.

Change Security Settings

Security Setting Preferences

Security Settings Name: My S/MIME Settings

Cryptography Format: S/MIME

☒ Default Security Setting for this cryptographic message format

☒ Default Security Setting for all cryptographic messages

Security Labels... New Delete

Certificates and Algorithms

Signing Certificate: Aaron Russell Choose...

Hash Algorithm: SHA1

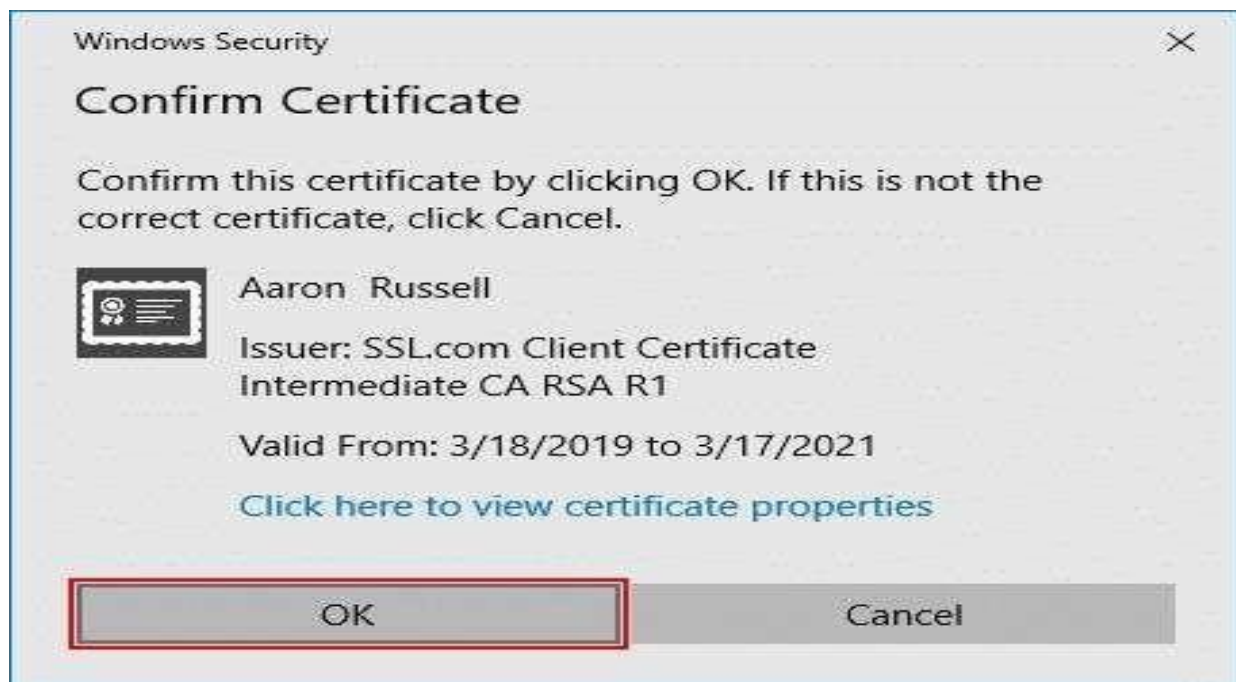
Encryption Certificate: Aaron Russell Choose...

Encryption Algorithm: AES (256-bit)

☒ Send these certificates with signed messages

OK Cancel

Confirm or select certificate.




The 'Windows Security Confirm Certificate' dialog box is shown. It has a title bar with a close button. The main text says 'Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.' Below this is a certificate icon, the name 'Aaron Russell', the issuer 'Issuer: SSL.com Client Certificate Intermediate CA RSA R1', and the validity period 'Valid From: 3/18/2019 to 3/17/2021'. There is a link 'Click here to view certificate properties'. At the bottom, there are 'OK' and 'Cancel' buttons.

Windows Security

Confirm Certificate

Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.

 Aaron Russell

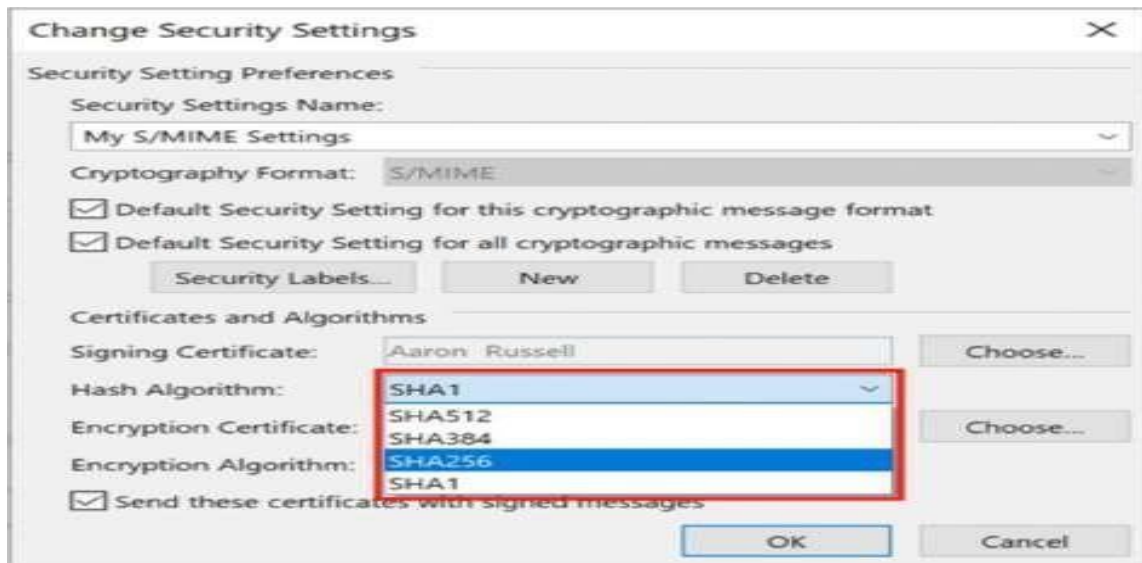
Issuer: SSL.com Client Certificate  
Intermediate CA RSA R1

Valid From: 3/18/2019 to 3/17/2021

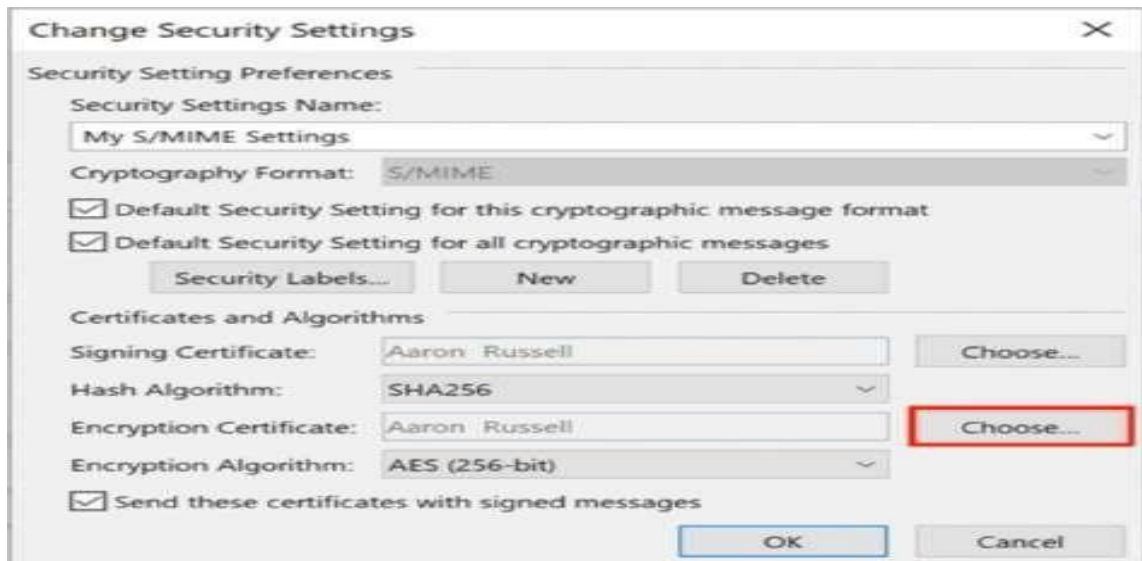
[Click here to view certificate properties](#)

OK Cancel

Set hash algorithm



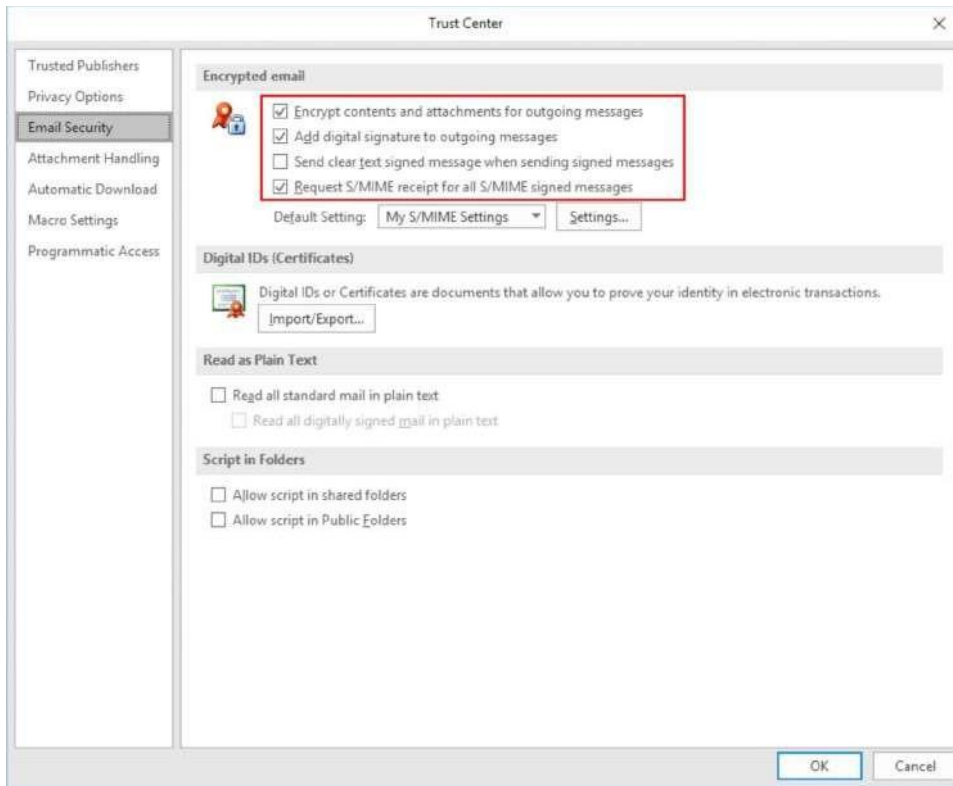
Choose encryption certificate



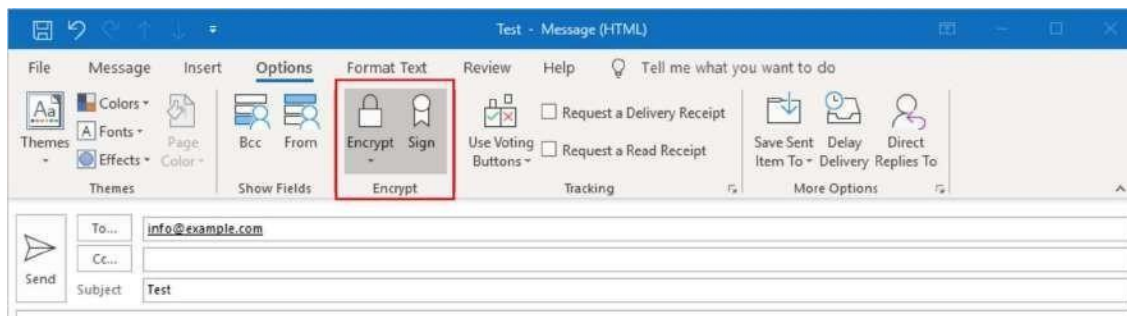
Close window



By using an click OK Button.  
Set S/MIME defaults.



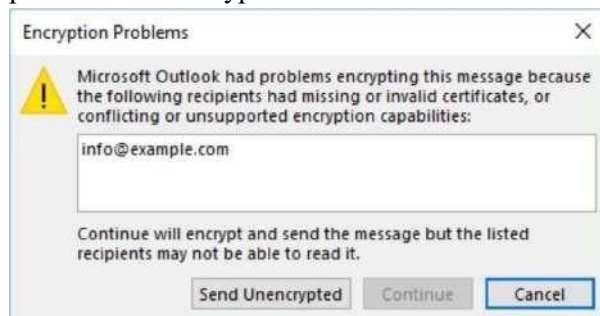
Set S/MIME options in a new message.



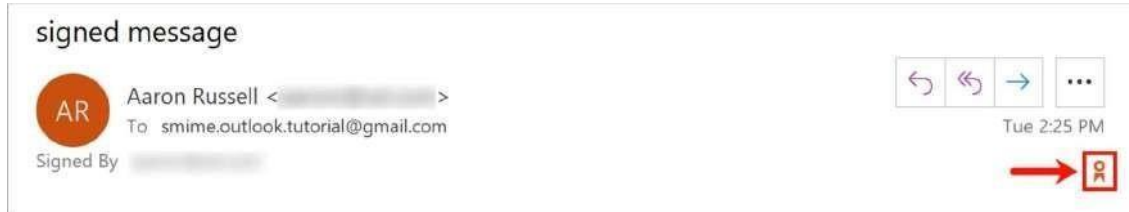
Allow Outlook to use your private key.



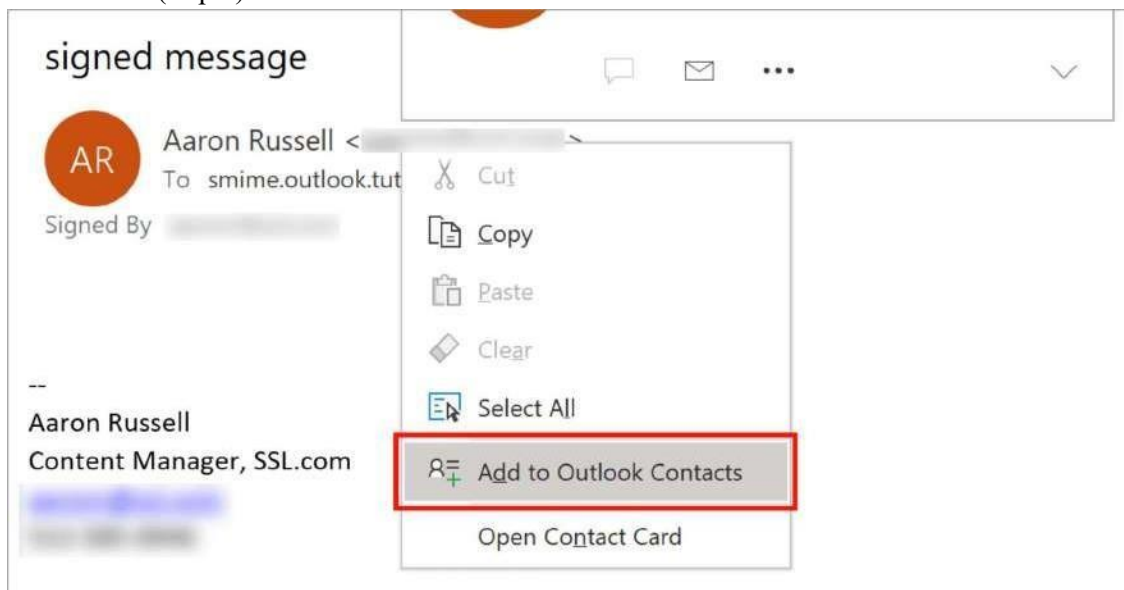
Potential problem with encryption.



Confirm signature



Add contact (step 1).

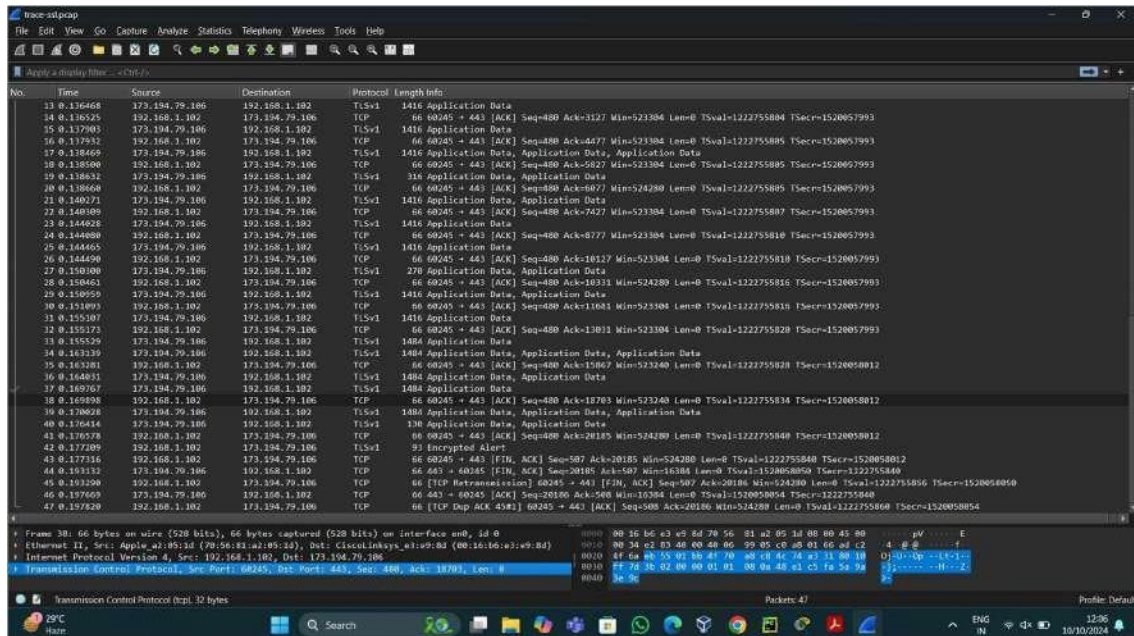


Name:Saish Baviskar  
Div:A Roll No: TEAD23155

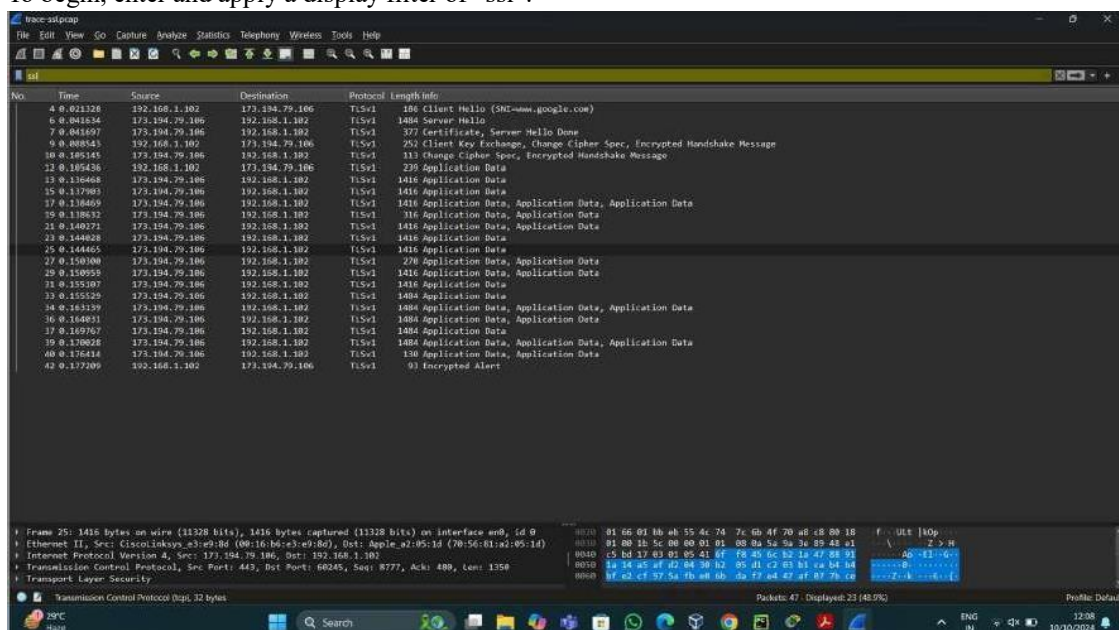
## Practical No. 10

**Problem Statement: To observe SSL/TLS (Secure Sockets Layer / Transport Layer Security) in action.**

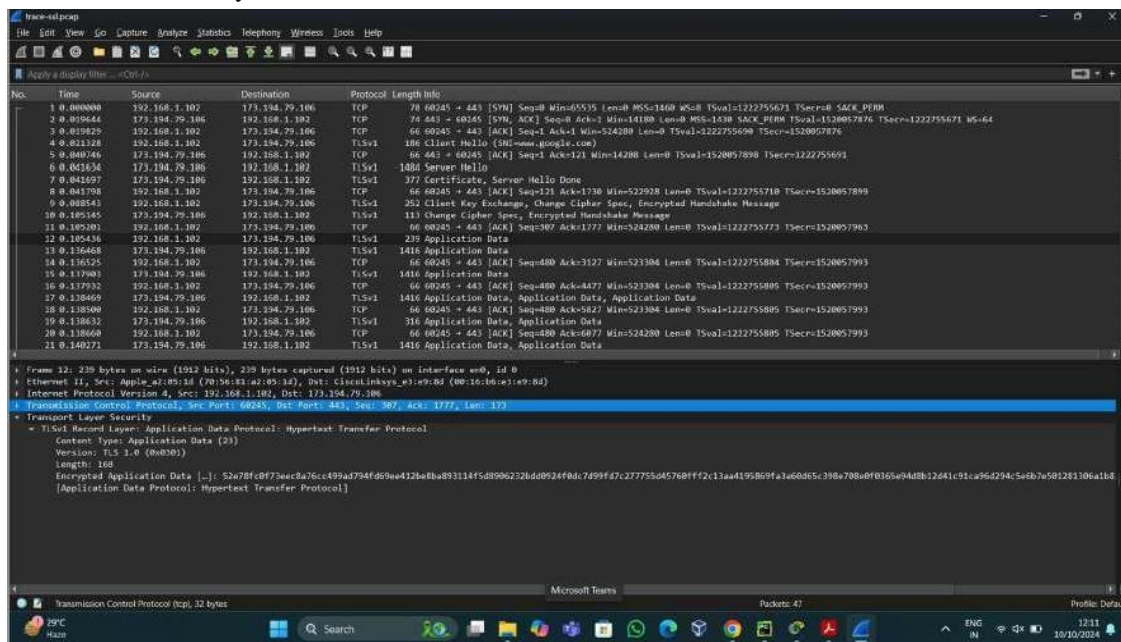
1. Open the Wireshark trace <https://kevincurran.org/com320/labs/wireshark/trace-ssl.pcap>



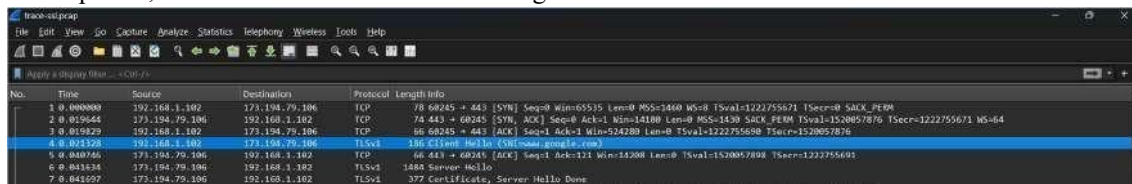
2. To begin, enter and apply a display filter of “ssl”.



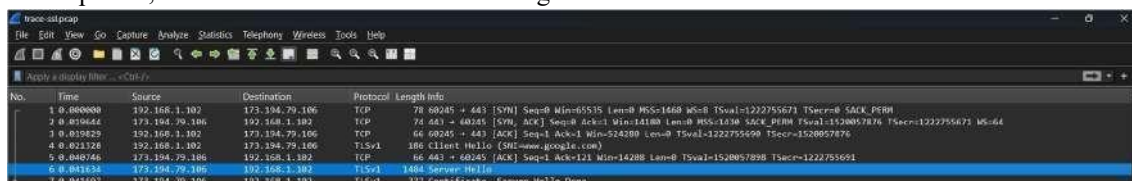
3. Select a TLS message somewhere in the middle of your trace for which the Info reads “Applica-tion Data” & expand its Secure Sockets Layer block



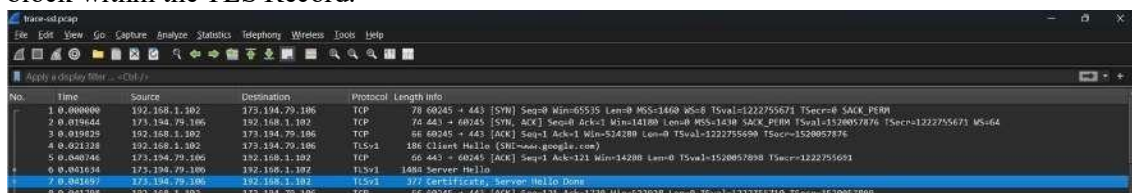
4. Select packet, which is a TLS Client Hello message



5. Select packet, which is a TLS Server Hello message



6. Next, find and inspect the details of the Certificate message including expanding the Handshake protocol block within the TLS Record.



7. Find and inspect the details of the Client Key Exchange and Change Cipher messages

8 0.041798	192.168.1.102	173.194.79.106	TCP	66 60245 + 443 [ACK] Seq=121 Ack=1730 Win=522928 Len=0 TSval=1222755710 TSecr=1520057899
9 0.008543	192.168.1.102	173.194.79.106	TLSv1	252 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
10 0.105145	173.194.79.106	192.168.1.102	TLSv1	113 Change Cipher Spec, Encrypted Handshake Message



```
Transport Layer Security
▼ TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  Content Type: Change Cipher Spec (20)
  Version: TLS 1.0 (0x0301)
  Length: 1
  Change Cipher Spec Message
▼ TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 36
  Handshake Protocol: Encrypted Handshake Message
```

8. Finally, find and inspect the details of an Alert message at the end of the trace

```
Transport Layer Security
▼ TLSv1 Record Layer: Encrypted Alert
  Content Type: Alert (21)
  Version: TLS 1.0 (0x0301)
  Length: 22
  Alert Message: Encrypted Alert
```

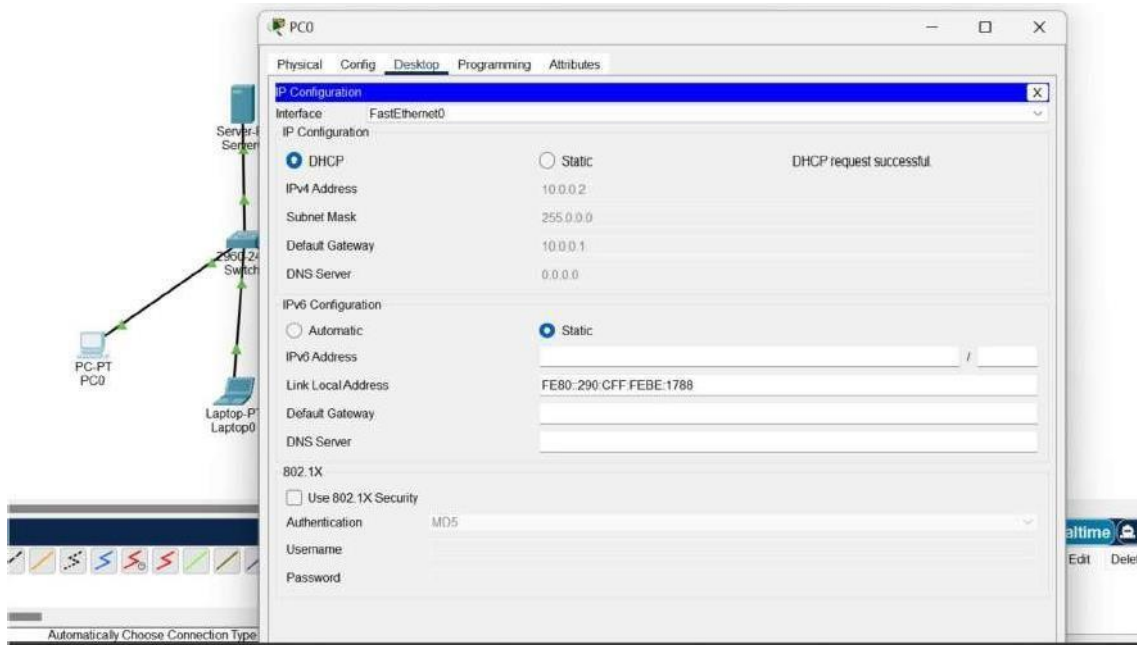


Name: Saish Baviskar  
Div: A Roll No: TEAD23155

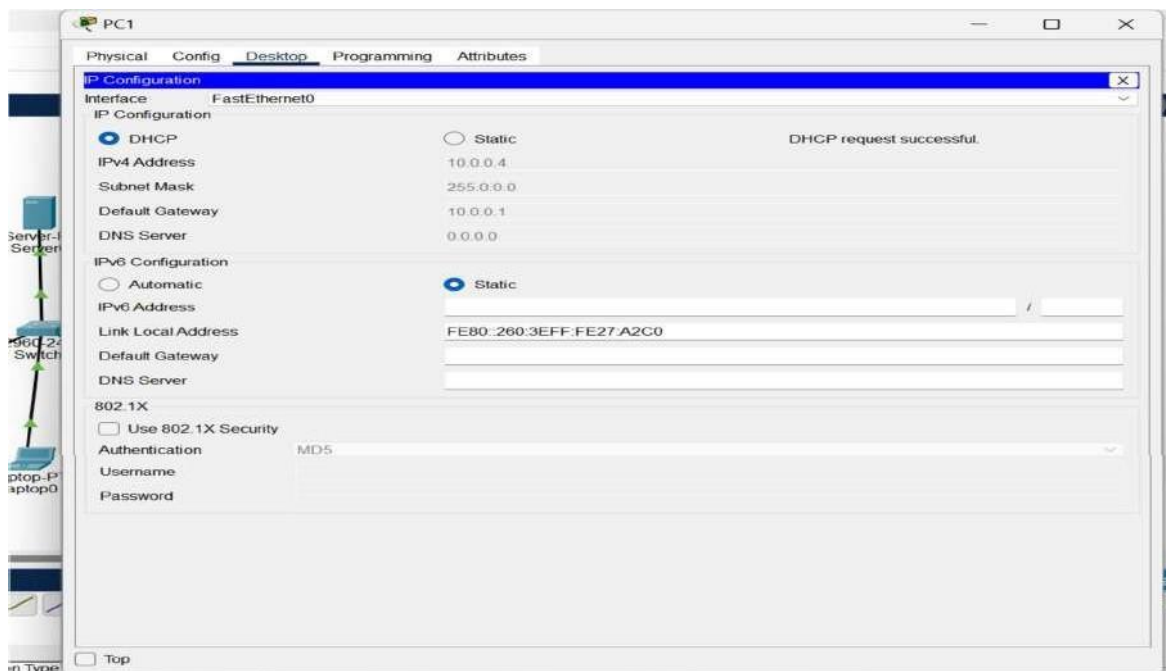
## Practical No.11

Problem Statement: Installing and configuring DHCP server and assign IP addresses to client machines using DHCP server.

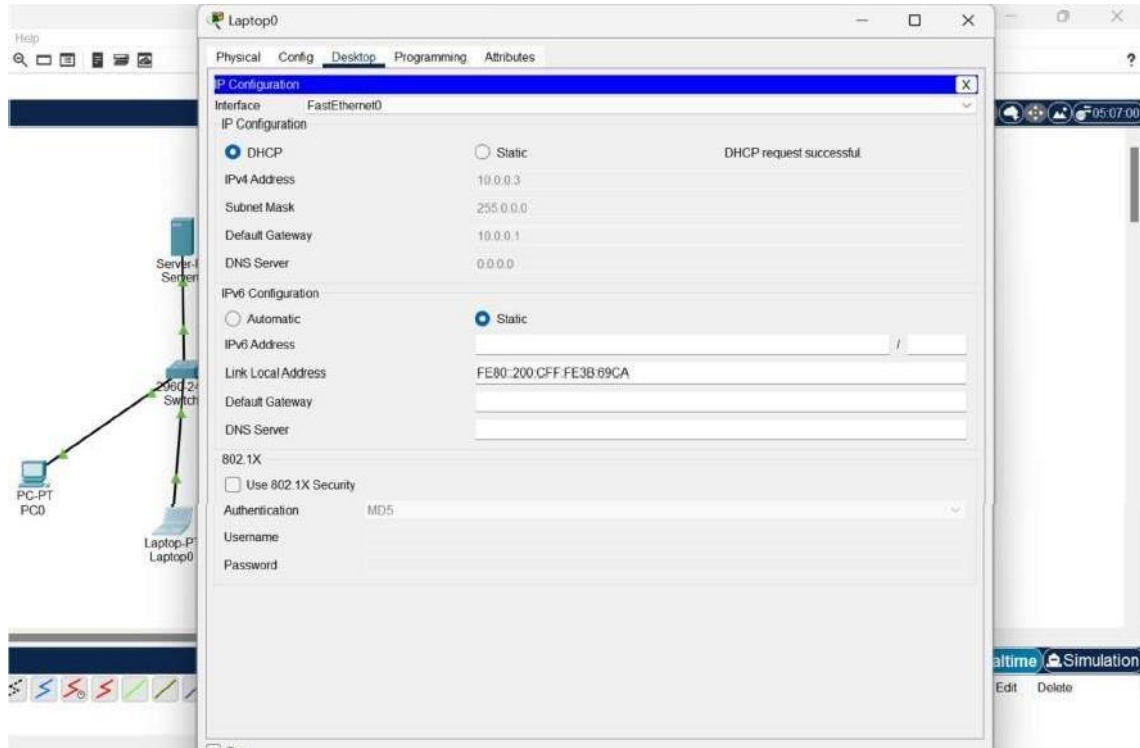
- 1 Checking The connection Using DHCP Server
- 2 PC0



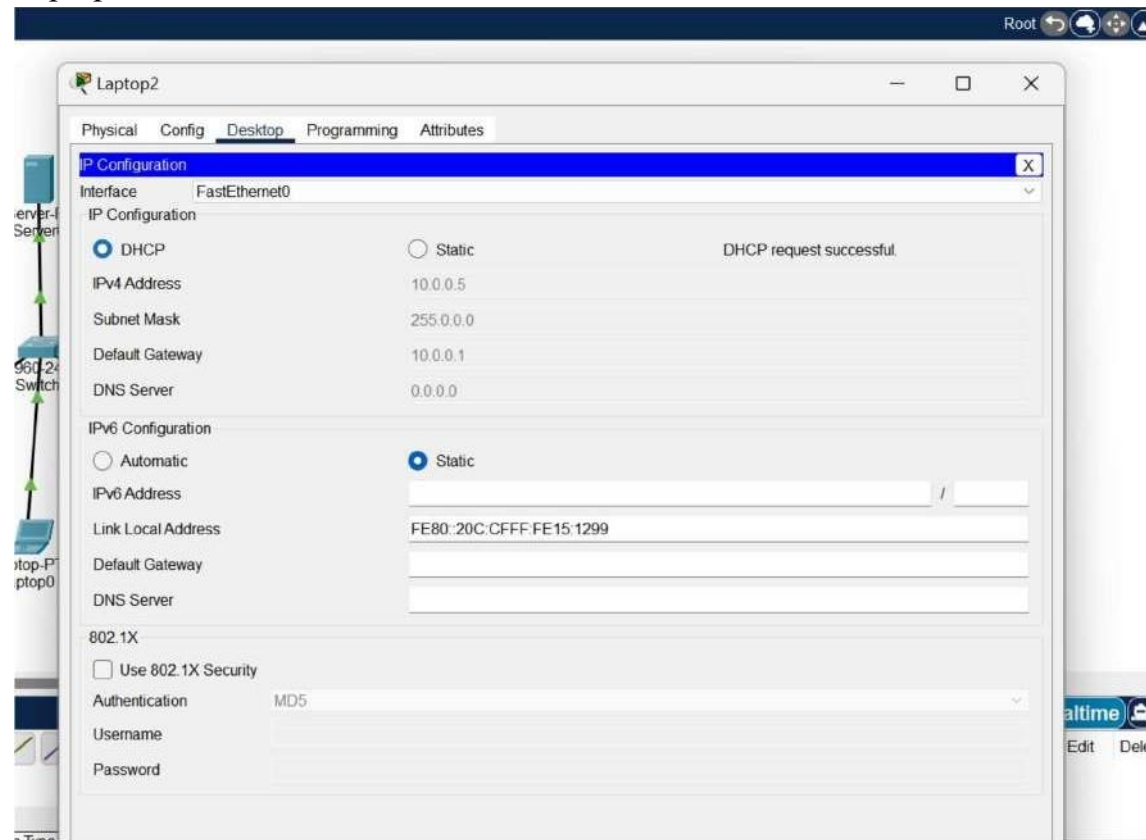
PC1



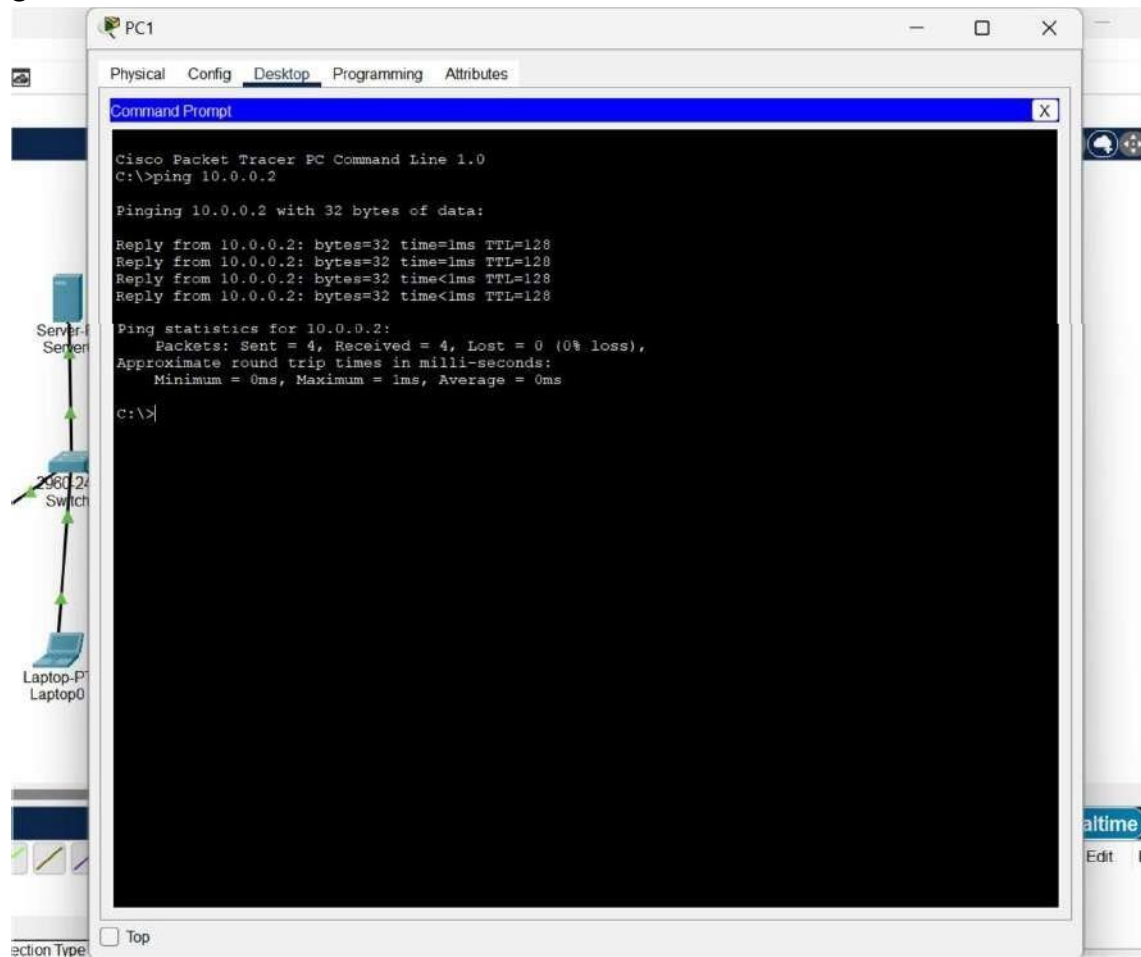
## Laptop0



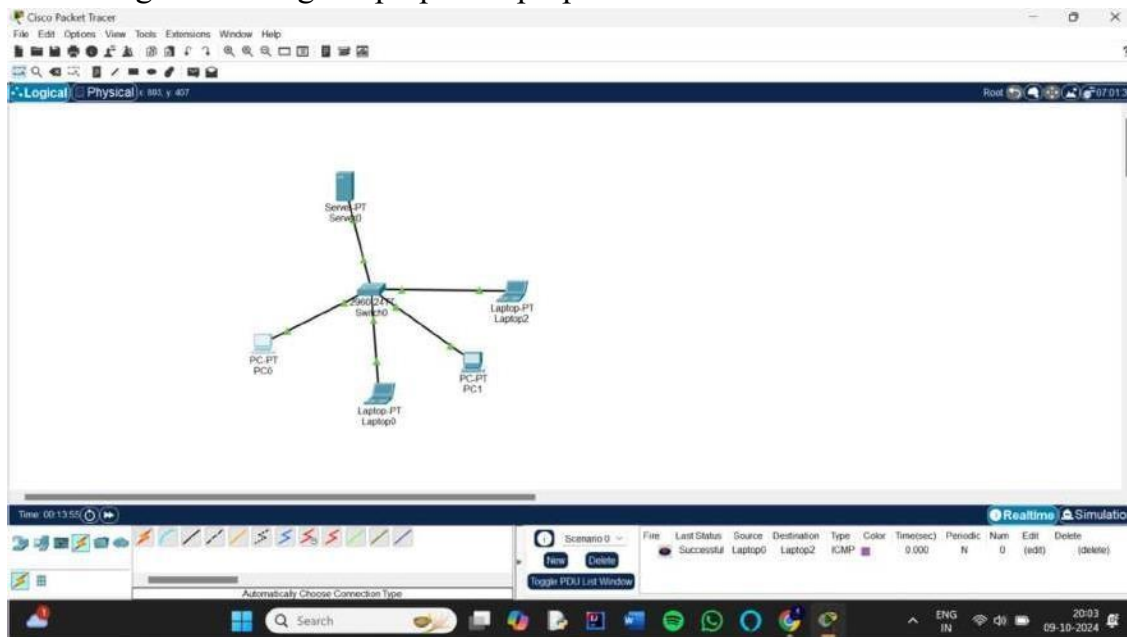
## Laptop2



## Checking The connection in PC



## 1. Sending the message Laptop to Laptop



Name: Saish Baviskar  
Div: A Roll No: TEAD23155

## Practical no.12

Title: Write a program for DNS lookup. Given an IP address input, it should return URL and vice versa.

Program:

```
import java.net.*;
import java.util.Scanner;

public class DNSLookup1 {
    public static void main(String[] args) {
        Scanner scanner = new Scanner(System.in);
        int choice = 0;
        System.out.println("==== DNS Lookup Tool =====");
        do {
            System.out.println("\nMenu:");
            System.out.println("1. Find IP address from URL");
            System.out.println("2. Find URL (hostname) from IP address");
            System.out.println("3. Exit");
            System.out.print("Enter your choice (1-3): ");
            if (scanner.hasNextInt()) {
                choice = scanner.nextInt();
                scanner.nextLine(); // consume newline
            } else {
                System.out.println("Invalid input! Please enter a number between 1 and 3.");
                scanner.nextLine(); // clear invalid input
                continue;
            }
        }
        try {
            switch (choice) {
                case 1:
                    System.out.print("Enter URL (e.g., www.google.com): ");
                    String url = scanner.nextLine().trim();
                    if (url.isEmpty()) {
                        System.out.println("URL cannot be empty.");
                        break;
                    }
                    InetAddress inetAddress = InetAddress.getByName(url);
                    System.out.println("Host Name: " + inetAddress.getHostName());
```

```

        System.out.println("IP Address: " + inetAddress.getHostAddress());
        break;
    case 2:
        System.out.print("Enter IP address (e.g., 142.250.183.132): ");
        String ip = scanner.nextLine().trim();
        if (ip.isEmpty()) {
            System.out.println("IP address cannot be empty.");
            break;
        }
        InetAddress inetAddressByIP = InetAddress.getByAddress(ip);
        String hostName = inetAddressByIP.getHostAddress();

        if (hostName.equals(ip)) {
            System.out.println("No hostname found for IP " + ip + ".
            Reverse DNS lookup failed.");
        } else {
            System.out.println("Hostname for IP " + ip + " is: " + hostName);
        }
        break;
    case 3:
        System.out.println("Exiting DNS Lookup Tool. Goodbye!");
        break;
    default:
        System.out.println("Invalid choice! Please select between 1 and 3.");
        break;
    }
} catch (UnknownHostException e) {
    System.out.println("Lookup failed: " + e.getMessage());
}

} while (choice != 3);
scanner.close();
}
}

```



## OUTPUT:

```
Terminal
Oct 9 16:54

ubuntu@ubuntu:~$ javac DNSLookup1.java
ubuntu@ubuntu:~$ java DNSLookup1
===== DNS Lookup Tool =====

Menu:
1. Find IP address from URL
2. Find URL (hostname) from IP address
3. Exit
Enter your choice (1-3): 1
Enter URL (e.g., www.google.com): www.chatgpt.com
Host Name: www.chatgpt.com
IP Address: 172.64.155.209

Menu:
1. Find IP address from URL
2. Find URL (hostname) from IP address
3. Exit
Enter your choice (1-3): 2
Enter IP address (e.g., 142.250.183.132): 142.250.183.138
Hostname for IP 142.250.183.138 is: bom07s31-in-f10.1e100.net

Menu:
1. Find IP address from URL
2. Find URL (hostname) from IP address
3. Exit
Enter your choice (1-3): 3
Exiting DNS Lookup Tool. Goodbye!
ubuntu@ubuntu:~$
```