

Practical File

Name :- Manish Kumar (6515)

Exam Roll No. 20058590060

Practical 1.

Demonstrate the use of Network tools: ping, ipconfig, tracert, arp, netstat, whois

Answer

Ping

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\st>Ping how-famous.com

Pinging how-famous.com [2606:4700:839c:6f29:cc39:54:b7e3:2bf4] with 32 bytes of data:
Reply from 2606:4700:839c:6f29:cc39:54:b7e3:2bf4: time=114ms
Reply from 2606:4700:839c:6f29:cc39:54:b7e3:2bf4: time=127ms
Reply from 2606:4700:839c:6f29:cc39:54:b7e3:2bf4: time=138ms
Reply from 2606:4700:839c:6f29:cc39:54:b7e3:2bf4: time=141ms

Ping statistics for 2606:4700:839c:6f29:cc39:54:b7e3:2bf4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 114ms, Maximum = 141ms, Average = 130ms
```

Ipconfig

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\st>Ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 16:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 17:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi 2:
```

Ifconfig

Common uses for ifconfig include setting the IP address and netmask of a network interface and disabling or enabling an interface.

Tracert

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\st>Tracert how-famous.com

Tracing route to how-famous.com [2606:4700:83bc:6f29:cc39:4b:b7e3:2bf4]
over a maximum of 30 hops:

  1  4 ms  5 ms  4 ms  2401:4900:2ee8:7017::fe
  2  79 ms  36 ms  39 ms  2401:4900:2ee8:7017:0:47:e3df:4b40
  3  *      *      *      Request timed out.
  4  60 ms  38 ms  39 ms  2401:4900:0:c000::1:b1
  5  41 ms  51 ms  54 ms  2401:4900:0:c000::1:d2
  6  63 ms  37 ms  43 ms  2404:a800:1a00:803::69
  7  157 ms  116 ms  107 ms  2404:a800::226
  8  143 ms  *      *      13335.sgw.equinix.com [2001:de8:4::1:3335:1]
  9  139 ms  122 ms  105 ms  2400:cb00:410:3::
 10  149 ms  110 ms  117 ms  2606:4700:83bc:6f29:cc39:4b:b7e3:2bf4

Trace complete.
```

ARP

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\st>arp -a

Interface: 192.168.19.111 --- 0x9
Internet Address      Physical Address      Type
192.168.19.68         2e-29-c9-f6-e4-04     dynamic
192.168.19.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\st>
```

Netstat

```
Command Prompt
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\st>netstat

Active Connections

Proto Local Address          Foreign Address         State
TCP    192.168.19.111:50220    192.168.19.68:domain    TIME_WAIT
TCP    192.168.19.111:56001    20.198.162.78:https     ESTABLISHED
TCP    192.168.19.111:56033    41:https                ESTABLISHED
TCP    192.168.19.111:56034    40.79.189.59:https      TIME_WAIT
TCP    192.168.19.111:56262    192.168.19.68:domain    TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:55996 del03s14-in-x03:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56003 del11s05-in-x03:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56004 del11s15-in-x03:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56005 del11s05-in-x0a:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56007 del11s05-in-x0a:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56008 del11s06-in-x0e:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56009 [2606:4700::6810:7aaf]:https ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56010 del11s03-in-x0e:https   TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56012 unn-sgp:https           ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56013 [2606:4700:91bf:86d8:3039:54:a0fa:f02f]:https TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56022 sd-in-f139:https        ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56026 whatsapp-cdn6-shv-02-del1:https ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56030 [2606:4700:83b9:9cc3:3739:4b:db5e:f10d]:https ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56031 del03s14-in-x03:https   ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56035 del11s05-in-x03:https   ESTABLISHED
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56036 [2620:1ec:c11::200]:https TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56037 [2620:1ec:c11::200]:https TIME_WAIT
TCP    [2401:4900:2ee8:7017:e990:e145:a10b:75ee]:56038 [2620:1ec:c11::200]:https ESTABLISHED
```

Practical 2.

Use of Password cracking tools: John the Ripper, Ophcrack,
Verify the Strength of passwords using these tools.

Answer

John the Ripper

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\comp40>cd C:\Users\comp40\Downloads\john-1.9.0-jumbo-1-win64 <1>\john-1.9.0-jumbo-1-win64\run

C:\Users\comp40\Downloads\john-1.9.0-jumbo-1-win64 <1>\john-1.9.0-jumbo-1-win64\run>john pas3.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-opencl"
Use the "--format=md5crypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE4.1 4x31])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:password.lst, rules:Wordlist
Proceeding with incremental:ASCII
manish (?)
1g 0:00:00:05 DONE 3/3 (2022-03-08 14:07) 0.1947g/s 31740p/s 31740c/s 31740C/s s
onk23..merela
Use the "--show" option to display all of the cracked passwords reliably
Session completed

C:\Users\comp40\Downloads\john-1.9.0-jumbo-1-win64 <1>\john-1.9.0-jumbo-1-win64\run>
```

Practical 3.

Perform encryption and decryption of Caesar cipher. Write a script for performing these operations.

Answer

Algorithm of Caesar Cipher

The algorithm of Caesar cipher holds the following features –

- Caesar Cipher Technique is the simple and easy method of encryption technique.
- It is simple type of substitution cipher.
- Each letter of plain text is replaced by a letter with some fixed number of positions down with alphabet.

```
def encrypt(text,s):
result = ""
    # transverse the plain text
    for i in range(len(text)):
        char = text[i]
        # Encrypt uppercase characters in plain text

        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)
        # Encrypt lowercase characters in plain text
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)
    return result

#check the above function
text = "CEASER CIPHER DEMO"
s = 4

print "Plain Text : " + text
print "Shift pattern : " + str(s)
print "Cipher: " + encrypt(text,s)
```

Practical 4.

**Perform encryption and decryption of a Rail fence cipher.
Write a script for performing these operations.**

Answer

```
def cipher(s, key, graph=False) :
    down=True
    raw_out=[]
    out=''
    i=0
    for x in range(key) :
        raw_out.append({})
    for pos in range(len(s)) :
        raw_out[i][pos]=s[pos]
        if i==key-1 :
            down=False
        if i==0 :
            down=True
        if down :
            i=i+1
        else :
            i=i-1
    for p in raw_out :
        for q in p :
            out+=p[q]
    if graph :
        return raw_out
    return out

def decipher(s, key) :
    map_list=cipher(s, key, True) #CREATING JUST FOR MAPPING - WHICHth CHARACTER
    new={}
    out=''
    s_counter=0
    for x in map_list :
        for y in x :
            new[y]=s[s_counter]
            s_counter+=1
    for p in new :
        out+=new[p]
    return map_list
```

Practical 6.

Use the Burp proxy to capture and modify the message.

Answer

1. Open Burp Proxy Suite
2. Create a temp project with default settings
3. Go to proxy
4. Turn on intercept
5. Open Browser
6. Enter any URL etc...
7. Forward 8. Check your HTTP history

Burp Proxy Snashots

1 GET / HTTP/1.1
2 Host: v3schools.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.8
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 0

Request Cookies 0

Request Headers 7

0 matches

Burp Suite Community Edition v2022.2.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	List
1	http://w3schools.com	GET	/			301	332	HTML		301 Moved Permanently			76.223.115.82		01:37:29 6 ...	806
2	https://www.w3schools.com	GET	/			200	105413	HTML		W3Schools Online ...		✓	192.229.179.87		01:42:44 6 ...	806
10	https://www.w3schools.com	GET	/lib/my-learning.js?v=1.0.9		✓	200	22183	script	js			✓	192.229.179.87		01:42:45 6 ...	806
11	https://www.w3schools.com	GET	/lib/ui.js?v=1.0.3		✓	200	74091	script	js			✓	192.229.179.87		01:42:45 6 ...	806
12	https://www.w3schools.com	GET	/lib/w3codecolor.js			200	31995	script	js			✓	192.229.179.87		01:42:45 6 ...	806
13	https://www.w3schools.com	GET	/howto/tryhow_js_slideshow_ifr...			200	4021	HTML	htm			✓	192.229.179.87		01:42:45 6 ...	806
24	https://cdn.cdnimage.com	GET	/adennine/w3schools.com/load			200	14574	script	ic			✓	192.229.179.87		01:42:45 6 ...	806

Request

```

1 GET / HTTP/1.1
2 Host: www.w3schools.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: "Windows"
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

Response

```

1 HTTP/2 200 OK
2 Accept-Ranges: bytes
3 Age: 1548
4 Cache-Control: Public,public
5 Content-Security-Policy: frame-ancestors 'self' https://mycourses.w3schools.com;
6 Content-Type: text/html
7 Date: Tue, 05 Apr 2022 20:12:45 GMT
8 Expires: Wed, 06 Apr 2022 00:12:45 GMT
9 Last-Modified: Tue, 05 Apr 2022 19:40:17 GMT
10 Server: ECS (nd1/D35F)
11 Vary: Accept-Encoding
12 X-Cache: HIT
13 X-Content-Security-Policy: frame-ancestors 'self' https://mycourses.w3schools.com;
14 X-Powered-By: ASP.NET
15 Content-Length: 104911
16
17
18 <!DOCTYPE html>
19 <html lang="en-US">
20 <head>
21 <title>
22 W3Schools Online Web Tutorials
23 </title>
24 <meta charset="utf-8">

```

Inspector

Request Attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	GET
Path	/

Request Headers 14

Response Headers 14

Burp Suite Community Edition v2022.2.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	List
1	GET / HTTP/1.1															
2	Host: www.w3schools.com															
3	Upgrade-Insecure-Requests: 1															
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36															
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9															
6	Sec-Fetch-Site: none															
7	Sec-Fetch-Mode: navigate															
8	Sec-Fetch-User: ?1															
9	Sec-Fetch-Dest: document															
10	Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"															
11	Sec-Ch-Ua-Mobile: ?0															
12	Sec-Ch-Ua-Platform: "Windows"															
13	Accept-Encoding: gzip, deflate															
14	Accept-Language: en-US,en;q=0.9															
15	Connection: close															
16																
17																

Request

```

1 GET / HTTP/1.1
2 Host: www.w3schools.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: "Windows"
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17

```

Response

```

2407 }
2408 else {
2409     setTimeout(execute_google_search, 100);
2410 }
2411 }
2412 document.body.addEventListener("click", function(event) {
2413     var a, x = event.srcElement;
2414     if (x.id == "search2" || x.id == "learnocode_searchbtn" || x.id == "learnocode_searchicon" || x.className.indexOf("search_item") > -1) {
2415     }
2416     else {
2417         a = document.getElementById("listofsearchresults");
2418         a.innerHTML = "";
2419         a.style.display = "none";
2420         document.getElementById("search2").style.borderBottomLeftRadius = "25px";
2421         if (document.getElementsByClassName("gsc-results-wrapper-visible")[0]) {
2422             document.getElementById("googleSearch").style.display = "none";
2423             document.getElementById("googleSearch").style.visibility = "";
2424         }
2425     }
2426 }
2427 </script>
2428 </body>
2429 </html>

```

Inspector

Request Attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	GET
Path	/

Request Headers 14

Response Headers 14

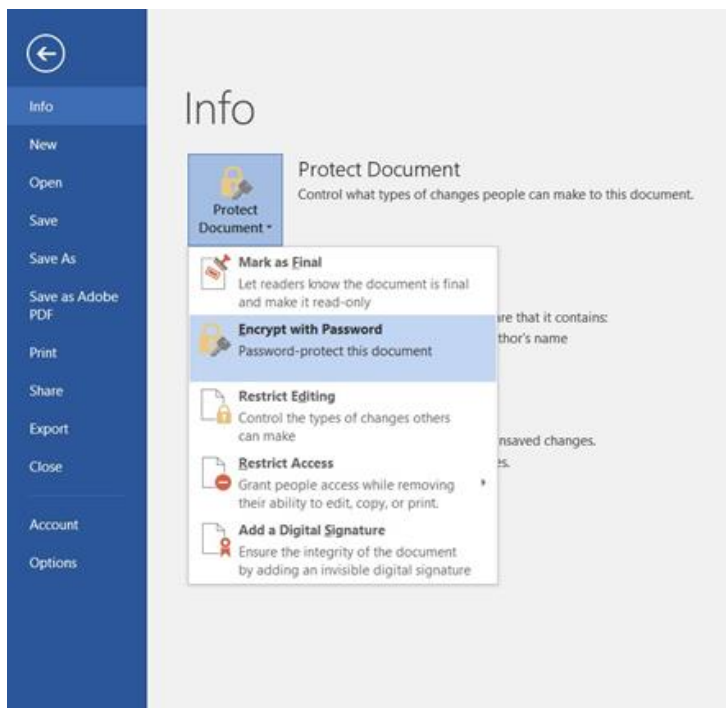
Total Number of Response lines is 2428

Practical 7.

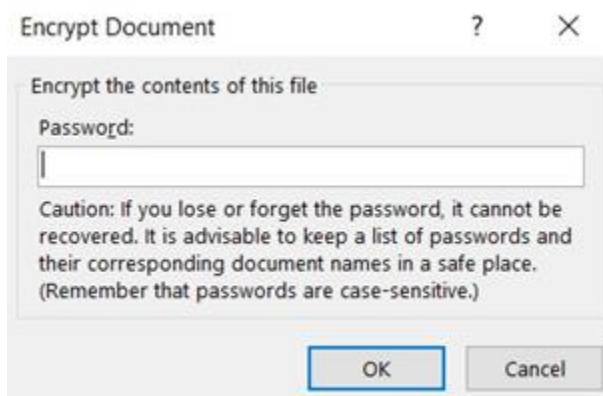
Demonstrate sending of a protected word document.

Answer

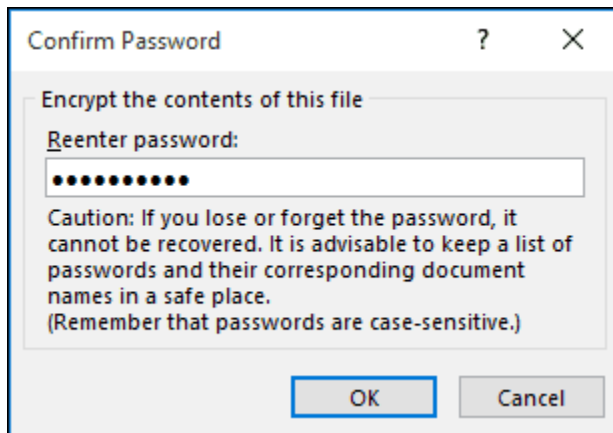
First, open the Office document you would like to protect. Click the File menu, select the Info tab, and then select the Protect Document button. Click Encrypt with Password.



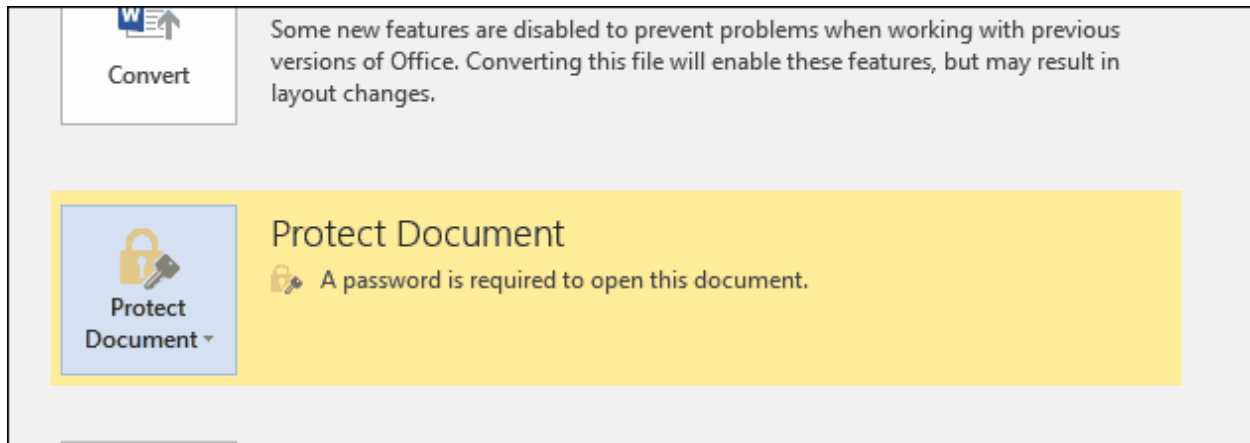
Enter your password then click OK



Enter the password again to confirm it and click OK.



Microsoft Word will now indicate the document is protected. Each time you open the document, you will be prompted to enter your password to access its contents.



Practical 8.

Demonstrate sending of a digitally signed document.

Answer

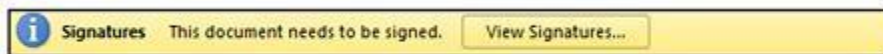
1. In the document or worksheet, place your pointer where you want to create a signature line.
2. On the **Insert** tab, in the **Text** group, click the **Signature Line** list, and then click **Microsoft Office Signature Line**.
3. In the **Signature Setup** dialog box, type information that will appear beneath the signature line:



- **Suggested signer** The signer's full name.
- **Suggested signer's title** The signer's title, if any.
- **Suggested signer's e-mail address** The signer's e-mail address, if needed.
- **Instructions to the signer** Add instructions for the signer, such as "Before signing the document, verify that the content is correct."

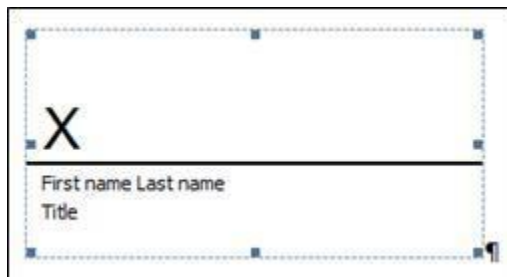
4. Select one or both of the following check boxes:

- **Allow the signer to add comments in the Sign dialog box** Allow the signer to type a purpose for signing.
- **Show sign date in signature line** The date the document was signed will appear with the signature.



Sign the signature line in Word or Excel

When you sign a signature line, you add a visible representation of your signature and a digital signature.



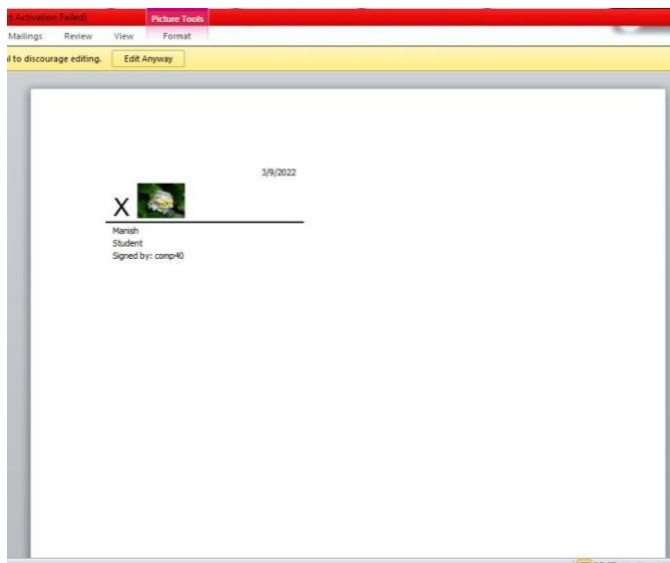
1. In the file, right-click the signature line.
2. From the menu, select **Sign**.
 - To add a printed version of your signature, type your name in the box next to the X.

- To select an image of your written signature, click **Select Image**. In the **Select Signature Image** dialog box, find the location of your signature image file, select the file that you want, and then click **Select**.
3. To add a handwritten signature (Tablet PC users only), sign your name in the box next to the **X** by using the inking feature.

Click **Sign**.

The **Signatures** button appears at the bottom of the document or worksheet.

The following image shows the **Signatures** button.



Practical 9.

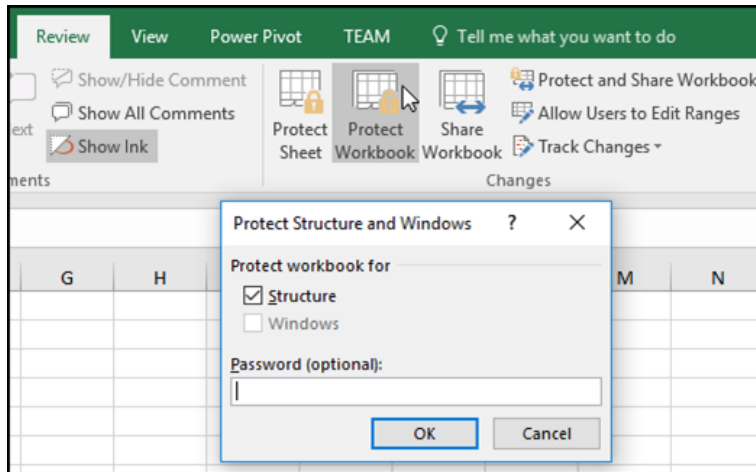
Demonstrate sending of a protected worksheet.

Answer

Protect the workbook structure

To protect the structure of your workbook, follow these steps:

1. Click **Review > Protect Workbook**.



2. Enter a password in the **Password** box.
3. Select **OK**, re-enter the password to confirm it, and then select **OK** again

Practical 10.

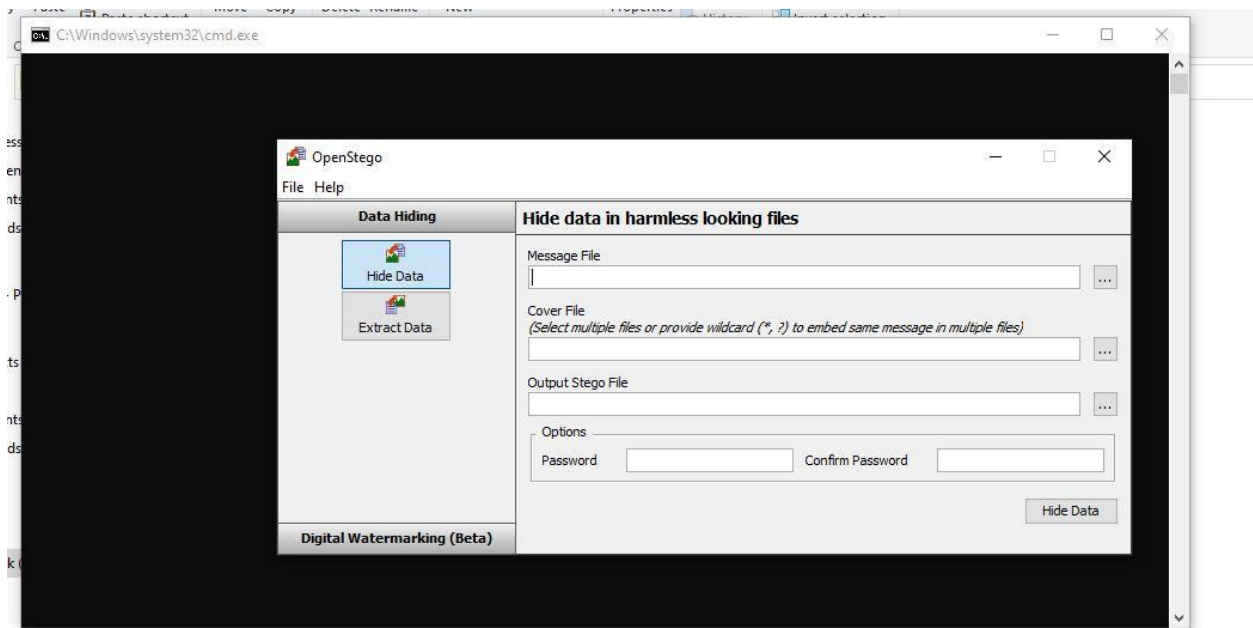
Demonstrate the use of steganography tools.

Answer

Steganography Tools:

A steganography software tools allows a user to attach hidden data in a carrier file, such as an image or video, and sometimes it could be an audio , and later take off that data. It is not necessary to hide the message in the original file at all.

First Run **Openstego** Bet File



Then

Select Message File

Select Cover File

Select Output Stego File

Enter Password, Then Confirm Password once again

Click on Hide Data, **Done**