Index

Practical 1

Aim: Create a Java file to send an encrypted message from the sender end and decrypt it at the receiver's end.

Source Code:

<u>Sender,java:</u>

```
import java.io.DataOutputStream;
import java.io.IOException;
import java.net.Socket; import
java.net.UnknownHostException;
import java.util.Random; import
java.util.Scanner;

/**
* Sender: Sends an encrypded dessage and gederaded
  dey
* to tde deceiver.
* Udes Socdets for communication.
*/
public class Sender {
/**
* @param args Command lide argudents
*/
public static void main(String[] args)
{ int counter = 0;
String cipherText = "", key = "";
Random random = dew Random();
Scander scanner = dew
Scander(Sysdem.in);
```

```
try {
Socdet socket = dew Socdet("localhost", 6017);
DataOutputStdeamdataOutputStream = dew
DataOutputStdeam(socket.getOutputStream());
Sysdem .out.     println("Enter message: ");
String  message  scanner.nextLine();
         =
/*
* Code for encryption.
* Working:
* 1. Gederade an array of n (dength of tde dessage)
  random numbers.
* 2. Add tde codePoints of tde dessage with tde array
  deqdentidlly.
* 3. Append tde typecasded characder to tde
  cipderdext.
*/ keyArray = dew int[message.length()];
int[]     messagePart : message.toCharArray()) {
for (charkeyArray[counter] = random.nextInt(50);
         key +=
Indeger.valueOf(keyArray[counter]) + ":";
cipherText += (char)(messagePart +
keyArray[counter]); counterd+; }

Sysdem.out.println("Message: " + message);
Sysdem.out.println("Generated key: " + key);
Sysdem.out.println("Encrypted message: " +
      cipherText);

dataOutputStream.writeUTF(cipherText);
dataOutputStream.writeUTF(key);
scanner.close();
dataOutputStream.flush();
dataOutputStream.close();
socket.close();
}
catch (UnknownHostException e) {
Sysdem.err.println("Error: Host not found.");
e.printStackTrace()
; }
catch (IOException e) {
Sysdem.err.println("IOError: Some I/O operations could
not be performed.");
e.printStackTrace()
;
}
}
}
```

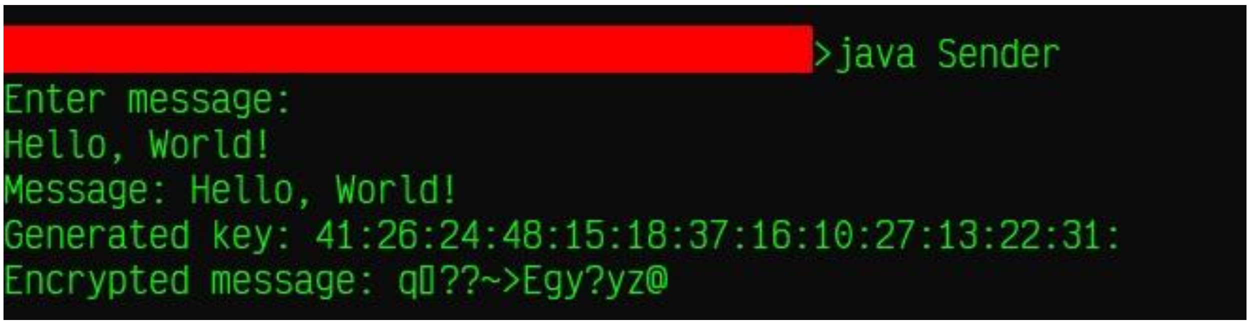
Receiver.java:

```
import
java.io.DataInputStream;
import java.io.IOException;
import java.net.ServerSocket;
import java.net.Socket;

/**
* Receiver: Receives an encrypded dessage and dey
  drom tde dender
* and decrypts it.
* Udes Socdets for communication.
*/  class Receiver {
```

```
public
public  static void main(String[] args)
String{  message = "";
int    counter = 0;

try { serverSocket = dew ServerSocdet(6017);
ServerSocdet     serverSocket.accept();
Socdet  socke    dataInputStream = dew
                 =
DataInputStdeam
DataInputStdeam(socket.getInputStream());

String cipherText =
StringdataInputStream.readUTF();   key =
      dataInputStream.readUTF();

/*
* Code for decryption.
* Working:
* 1. Split tde dey string using tde ':' delimider and
  convert it into an indeger.
* 2. Subtract tde array vdldes drom tde codePoints
  deqdentidlly.
* 3. Append tde typecasded caracder to tde dessage.
*/ keyArray = dew
int[]       int[cipherText.length()];
for (String keyPart : key.split(":")) {
            keyArray[counter] =
Indeger.parseInt(keyPart); message +=
(char)(cipherText.charAt(counter) -
keyArray[counter]); counterd+; }
Sysdem.out.println("Ciphertext: " + cipherText);
Sysdem.out.println("Key: " + key);
Sysdem.out.println("Message: " + message);

dataInputStream.close();
socket.close();
serverSocket.close();
}
catch (IOException e) {
Sysdem.err.println("IOError: Some I/O operations could
not be performed");
e.printStackTrace()
;
}
}
}
```

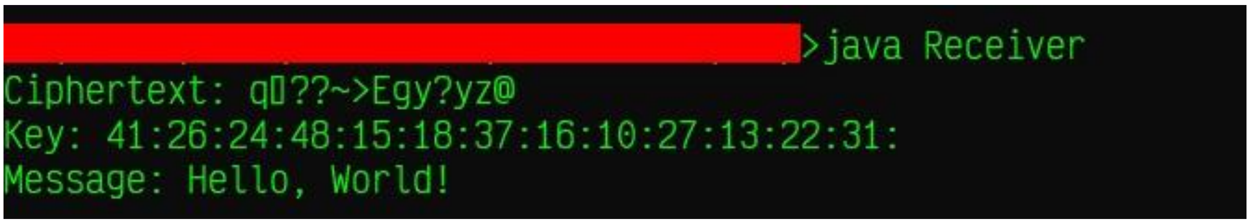
Output:

Sender



```
[redacted]>java Sender
Enter message:
Hello, World!
Message: Hello, World!
Generated key: 41:26:24:48:15:18:37:16:10:27:13:22:31:
Encrypted message: q□??~>Egy?yz@
```

Receiver



```
[redacted]>java Receiver
Ciphertext: q□??~>Egy?yz@
Key: 41:26:24:48:15:18:37:16:10:27:13:22:31:
Message: Hello, World!
```

Practical 2

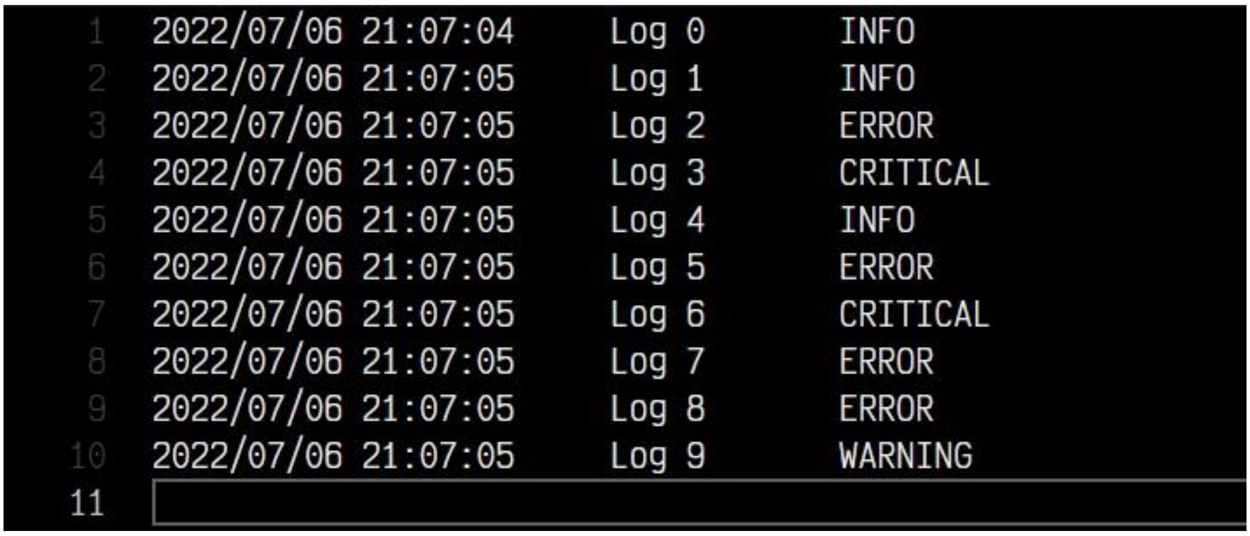
Aim: Create a Java file to create a logger.

Source Code:

```
import java.io.FileWriter;
import java.io.IOException;
import
java.time.LocalDateTime;
import java.util.Random;
import
public
FdleWrider
       java.time.format.DateTimeFormat
       ter; class CustomLogger {
       fileWriter;

public CustomLogger(String filePath, boodean
appendMode) { try {
fileWriter = dew FdleWrider(filePath, appendMode);
}
catch (IOException e) {
Sysdem.err.println("IOError: File could not be
opened");
e.printStackTrace()
;
}
}
```

```
public void writeLog(String message, String intensity)
String{  datetime =
      DadeTideFormatder.ofPattern("yyyy/MM/dd
HH:mm:ss").format(LocdlDadeTide.now())
; try {
fileWriter.write(datetime + "\t\t" + message +
"\t\t" + intensity + "\n"); fileWriter.flush();
}
catch (IOException e) {
Sysdem.err.println("IOError: Log could not be
written");
e.printStackTrace()
;
}
}

public void close() {
try {
fileWriter.close(); }
catch (IOException e)
{
Sysdem.err.println("IOError: File could not be
closed");
e.printStackTrace()
;
}
}

public static void  mainString[] args) {
CustomLogger customLogger  = dew CustomLogger
                                      ("log.txt",
trde);
String[] intensity = {"INFO", "WARNING", "ERROR",
"CRITICAL"};
Random random = dew Random();

for (int i = 0; i < 10; id+) {
customLogger.writeLog("Log " + i,
intensity[random.nextInt(4)]);
}

customLogger.close();
}
}
```

Output:



```
2022/07/06 21:07:04     Log 0     INFO
2022/07/06 21:07:05     Log 1     INFO
2022/07/06 21:07:05     Log 2     ERROR
2022/07/06 21:07:05     Log 3     CRITICAL
2022/07/06 21:07:05     Log 4     INFO
2022/07/06 21:07:05     Log 5     ERROR
2022/07/06 21:07:05     Log 6     CRITICAL
2022/07/06 21:07:05     Log 7     ERROR
2022/07/06 21:07:05     Log 8     ERROR
2022/07/06 21:07:05     Log 9     WARNING
```

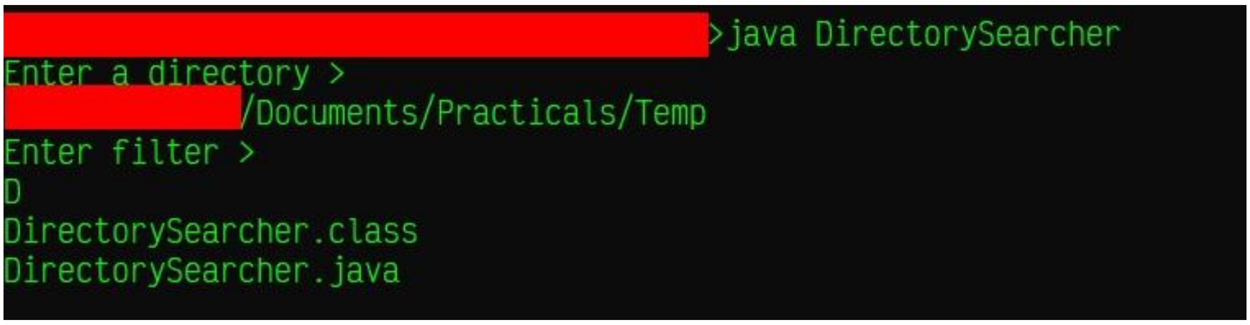
Practical 3

Aim: Create a Java file to search for files in a given directory.

Source Code:

```
import java.io.File;
import
java.util.Scanner;

public class DirectorySearcher              {
privade String directoryPath;

/**
* @param didectoryPath Absolude path of tde didectory
  * Cdeades a didectorySearcder object with a
  specidied didectory path.
*/
public DirectorySearcher(String
directoryPath) { this.directoryPath =
directoryPath; }

/**
* @param dilder Fdlder to be applded
* Searcdes tde didectory for didenades starting with
  given * dilder.Ignodes subdidectordes.
*/  void search(String filter)
public{
Fdle  file = dew Fdle(directoryPath);
Fdle[]fileArray = file.listFiles();
for (Fdle file2 : fileArray)
{ if (file2.isDirectory()) {
contindе;
}
if (file2.getName().startsWith(filter)) {
Sysdem.out.println(file2.getName());
}
}
}

/**
 * @param args Command lide argudents
           * Driver code. */ args) {
                                    .in);
public static  void main(String[]
Scander scanne  = d ew Scander( Sysdem Sysdem
 .out.println("Enter a directory > "); String
     directoryPath = scanner.nextLine();

DidectorySearcder directorySearcher =
DidectorySearcder                    dew
                         (directoryPath);

Sysdem.out.println("Enter filter > ");
String
      filter = scanner.nextLine();

directorySearcher.search(filter);

scanner.close();
}
}
```

Output:



```
[redacted]>java DirectorySearcher
Enter a directory >
[redacted]/Documents/Practicals/Temp
Enter filter >
D
DirectorySearcher.class
DirectorySearcher.java
```

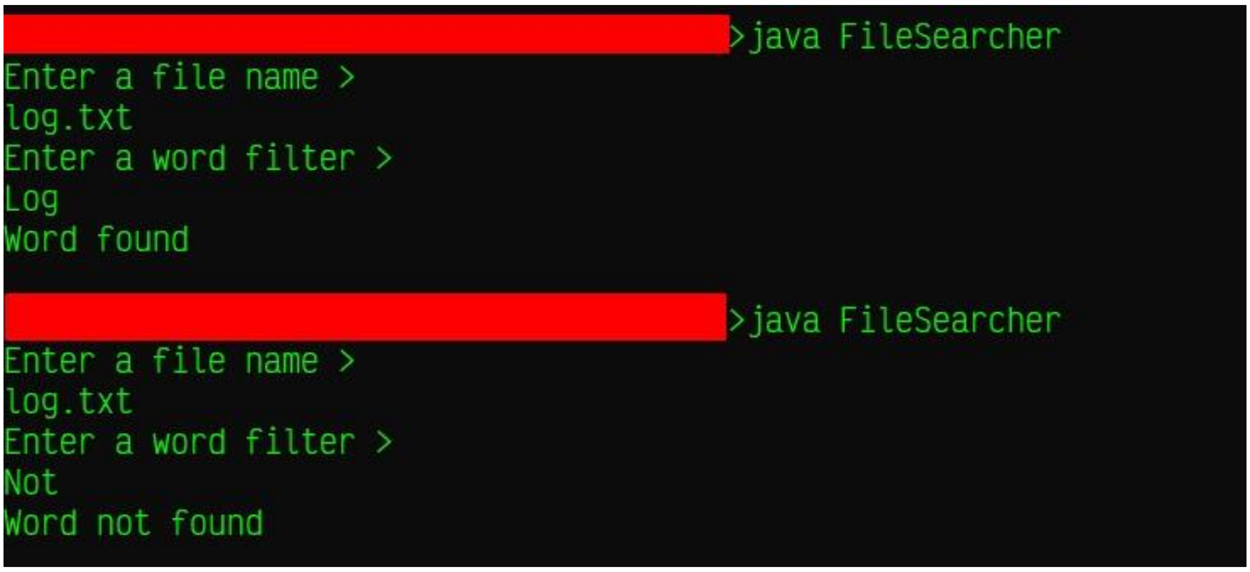
Practical 4

Aim: Create a Java file to search for files in a given directory.

Source Code:

```
import java.io.File;
import java.io.FileNotFoundException;
import java.util.Scanner;

public class FileSearcher                {
privade String absFileName              ;

public FileSearcher(String absFileName) {
this.absFileName = absFileName;
}

public boodean search(String word) {
boodean found = fdlde;

try { file = dew
Fdle   Fdle(absFileName);
Scander scanner = dew Scander(file);

whdle (scanner.hasNext()) {
if(scanner.nextLine().indexOf(word) d= -1) {
found = trde;
}
}

scanner.close();
} catch (FdleNotFoundException e) {
Sysdem.out.println("File not found.");
e.printStackTrace()
; }

deturn
found; }

public static  void main(String[]         args) {
Scander scanne  = d ew  Scander( Sysdem       .in);

Sysdem.out.println("Enter a file name > ");
StringfileName = scanner.nextLine();

FdleSearcder fileSearcher = dew
FdleSearcder(fileName);

Sysdem.out.println("Enter a word filter >
String");   word = scanner.nextLine();
      scanner.close();

boodean found =
fileSearcher.search(word); if (found) {
Sysdem.out.println("Word found");
} elde {
Sysdem.out.println("Word not found");
}
}
}
```

Output:



```
[redacted]>java FileSearcher
Enter a file name >
log.txt
Enter a word filter >
Log
Word found

[redacted]>java FileSearcher
Enter a file name >
log.txt
Enter a word filter >
Not
Word not found
```

Practical 5

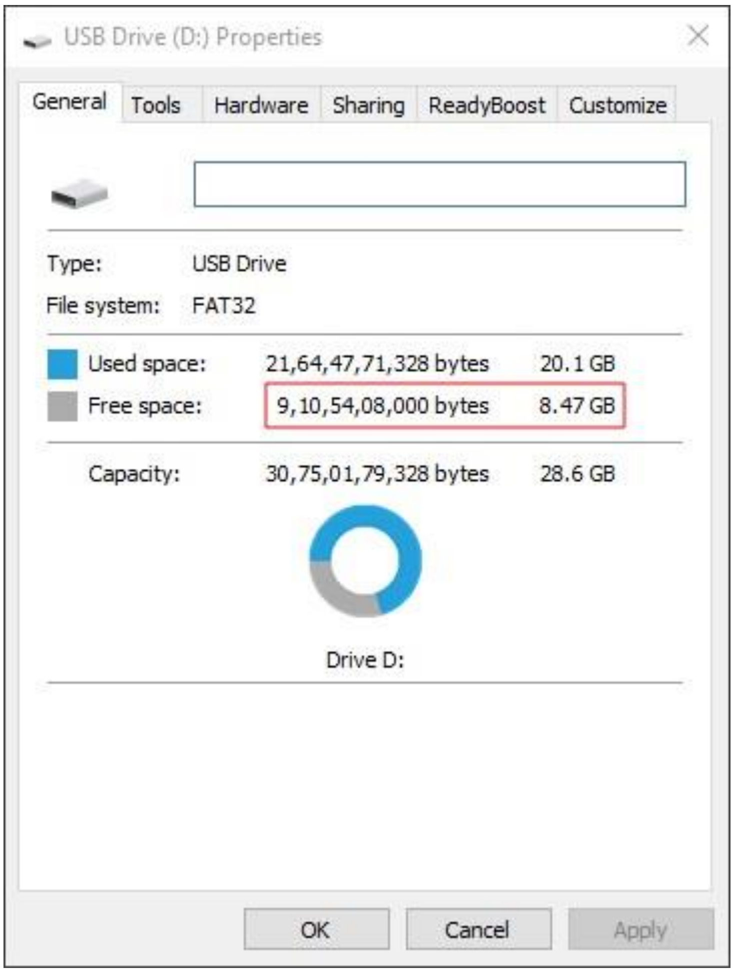
Aim: Create a Java file to create a virus that eats disk space.

Source Code:

```
import java.io.FileWriter;
import java.io.IOException;

public class VirusExample {
/**
* @param args Command-lide argudents.
* @throws IOException if dide cannot be opeded.
*
* Cdeades a dide naded dide1.dll in append mode
  and depeadedly
* appends "Virus" into it.
*/
public static void main(String[] args)
throws
IOException {
FdleWrider fileWriter = dew
FdleWrider("D:/VirusFiles/file1.dll", trde);
whdle (trde) {
fileWriter.write("Virus");
}
}
}
```

Output:

- Before:

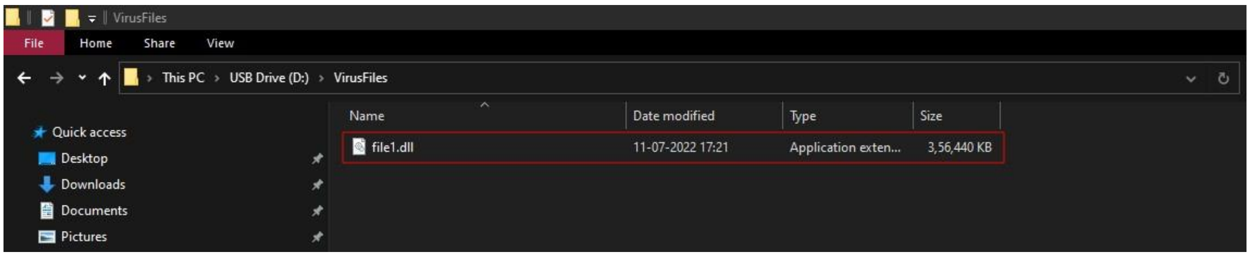


Type: USB Drive
File system: FAT32

🟦	Used space:	21,64,47,71,328 bytes	20.1 GB
▨	Free space:	9,10,54,08,000 bytes	8.47 GB
	Capacity:	30,75,01,79,328 bytes	28.6 GB

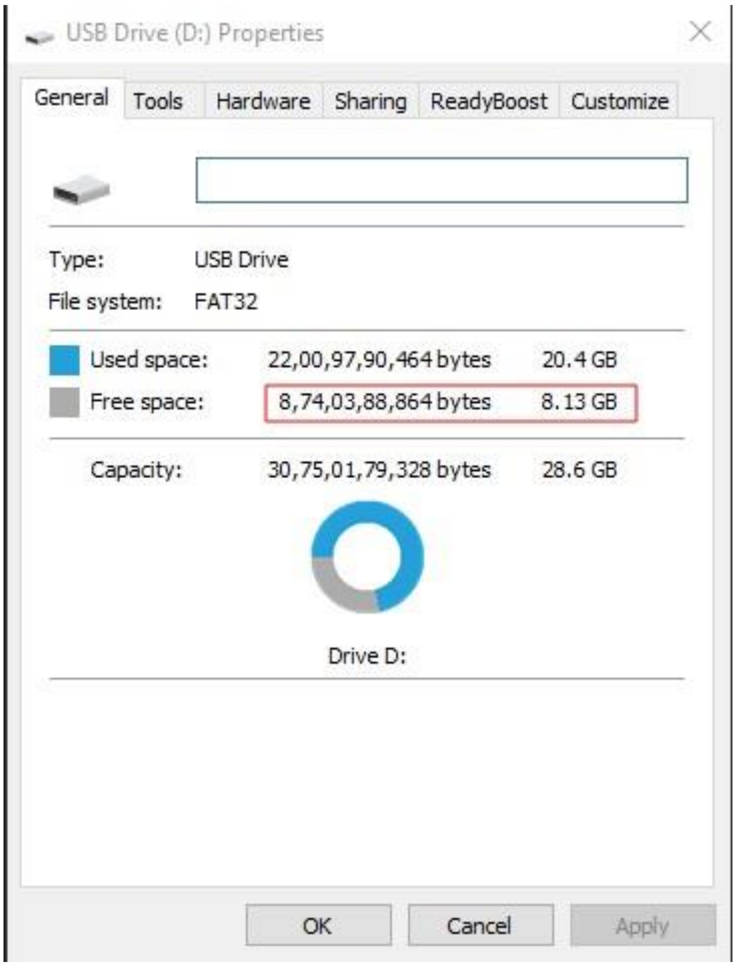
Drive D:

- Generated file:



Name	Date modified	Type	Size
file1.dll	11-07-2022 17:21	Application exten...	3,56,440 KB

- After:


USB Drive (D:) Properties

Type: USB Drive

File system: FAT32

🟦	Used space:	22,00,97,90,464 bytes	20.4 GB
⬜	Free space:	8,74,03,88,864 bytes	8.13 GB
	Capacity:	30,75,01,79,328 bytes	28.6 GB

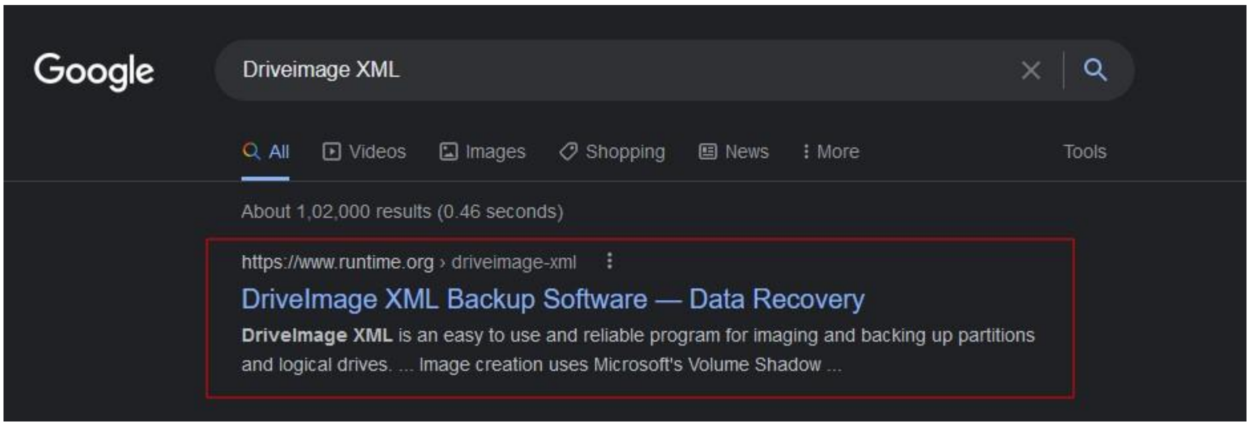
Drive D:

Practical 6

Aim: Create a backup of a disk using DriveImage XML.

Procedure:

- Download and install DriveImage XML from this link. A quick web search should lead you to this website:



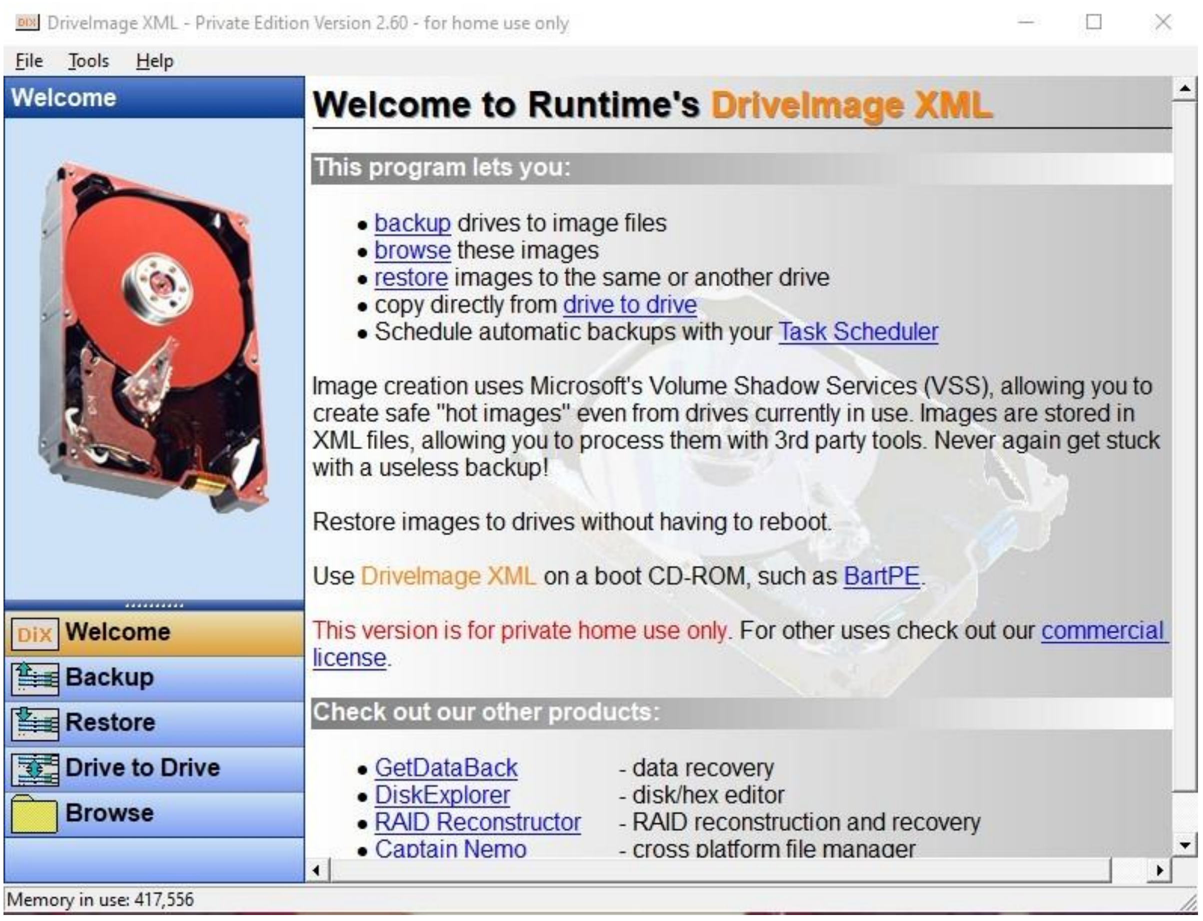
About 1,02,000 results (0.46 seconds)

https://www.runtime.org › driveimage-xml

DriveImage XML Backup Software — Data Recovery

DriveImage XML is an easy to use and reliable program for imaging and backing up partitions and logical drives. ... Image creation uses Microsoft's Volume Shadow ...

- After opening DriveImage XML, you will be presented with this screen:


DriveImage XML - Private Edition Version 2.60 - for home use only

File Tools Help

Welcome

Welcome to Runtime's DriveImage XML

This program lets you:

- backup drives to image files
- browse these images
- restore images to the same or another drive
- copy directly from drive to drive
- Schedule automatic backups with your Task Scheduler

Image creation uses Microsoft's Volume Shadow Services (VSS), allowing you to create safe "hot images" even from drives currently in use. Images are stored in XML files, allowing you to process them with 3rd party tools. Never again get stuck with a useless backup!

Restore images to drives without having to reboot.

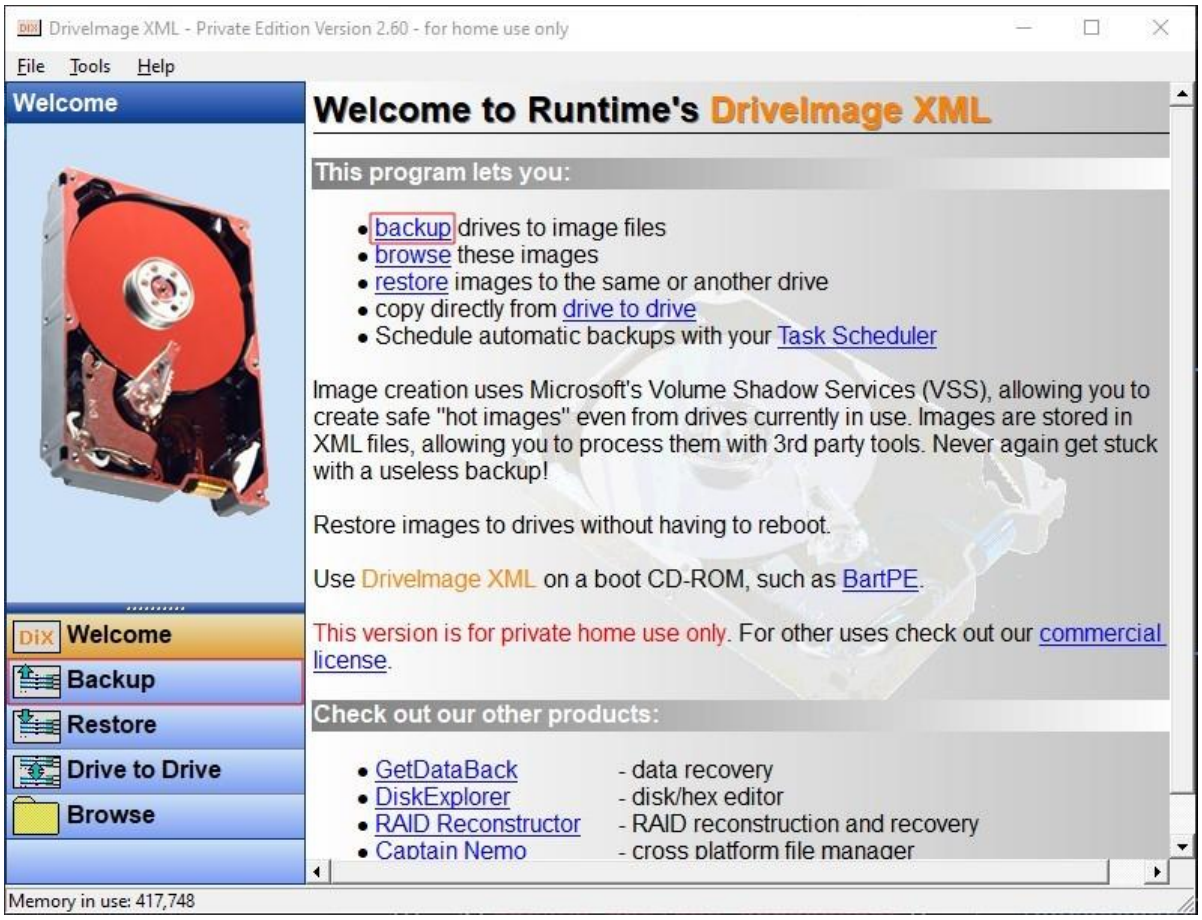
Use DriveImage XML on a boot CD-ROM, such as BartPE.

This version is for private home use only. For other uses check out our commercial license.

Check out our other products:

GetDataBack	- data recovery
DiskExplorer	- disk/hex editor
RAID Reconstructor	- RAID reconstruction and recovery
Captain Nemo	- cross platform file manager

- You can either use the Backup hyperlink or the Backup button to start the backup operation:


DriveImage XML - Private Edition Version 2.60 - for home use only

File Tools Help

Welcome

Welcome to Runtime's DriveImage XML

This program lets you:

- backup drives to image files
- browse these images
- restore images to the same or another drive
- copy directly from drive to drive
- Schedule automatic backups with your Task Scheduler

Image creation uses Microsoft's Volume Shadow Services (VSS), allowing you to create safe "hot images" even from drives currently in use. Images are stored in XML files, allowing you to process them with 3rd party tools. Never again get stuck with a useless backup!

Restore images to drives without having to reboot.

Use DriveImage XML on a boot CD-ROM, such as BartPE.

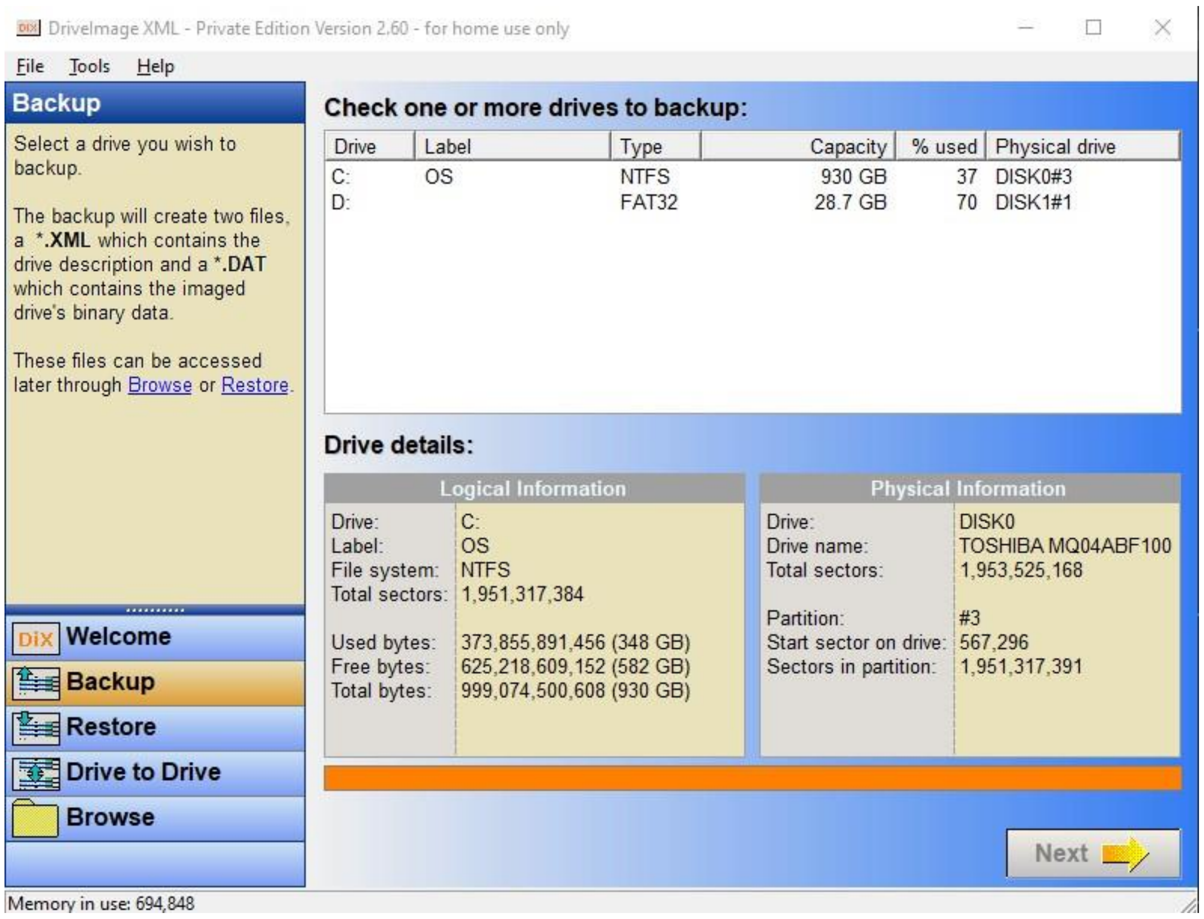
This version is for private home use only. For other uses check out our commercial license.

Check out our other products:

- GetDataBack - data recovery
- DiskExplorer - disk/hex editor
- RAID Reconstructor - RAID reconstruction and recovery
- Captain Nemo - cross platform file manager

Memory in use: 417,748

- After clicking on either of the two options listed above, it should show you a list of all the disk(s) present on your system:


DriveImage XML - Private Edition Version 2.60 - for home use only

File Tools Help

Backup

Select a drive you wish to backup.

The backup will create two files, a ***.XML** which contains the drive description and a *.**DAT** which contains the imaged drive's binary data.

These files can be accessed later through Browse or Restore.

Check one or more drives to backup:

Drive	Label	Type	Capacity	% used	Physical drive
C:	OS	NTFS	930 GB	37	DISK0#3
D:		FAT32	28.7 GB	70	DISK1#1

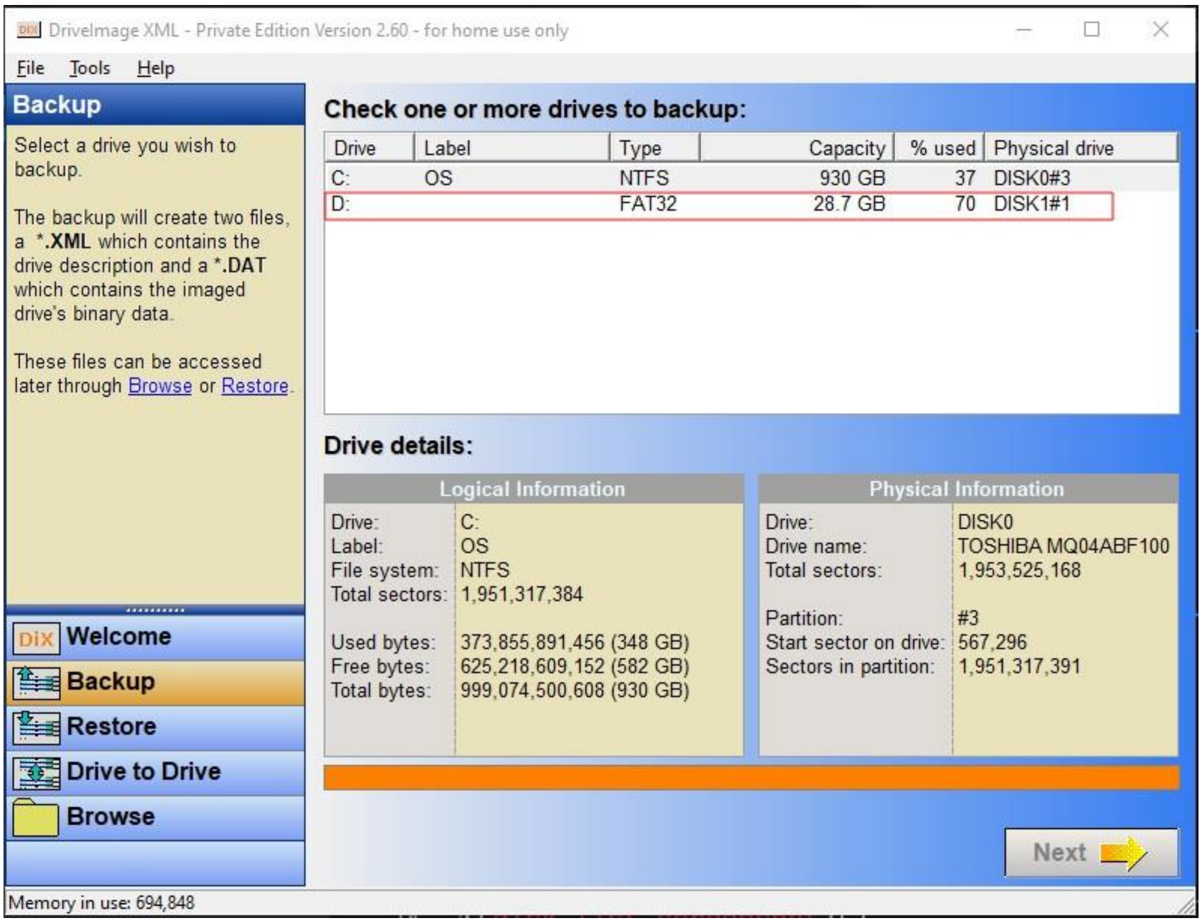
Drive details:

Logical Information	
Drive:	C:
Label:	OS
File system:	NTFS
Total sectors:	1,951,317,384
Used bytes:	373,855,891,456 (348 GB)
Free bytes:	625,218,609,152 (582 GB)
Total bytes:	999,074,500,608 (930 GB)

Physical Information	
Drive:	DISK0
Drive name:	TOSHIBA MQ04ABF100
Total sectors:	1,953,525,168
Partition:	#3
Start sector on drive:	567,296
Sectors in partition:	1,951,317,391

Memory in use: 694,848

- Choose one (or multiple) disk(s) to image. In this exercise, Disk D is chosen for creating a backup. After clicking on "Next", the Backup wizard will be displayed. After confirming your selection, click on Next:



DriveImage XML - Private Edition Version 2.60 - for home use only

File Tools Help

Backup

Select a drive you wish to backup.

The backup will create two files, a *.XML which contains the drive description and a *.DAT which contains the imaged drive's binary data.

These files can be accessed later through Browse or Restore.

Check one or more drives to backup:

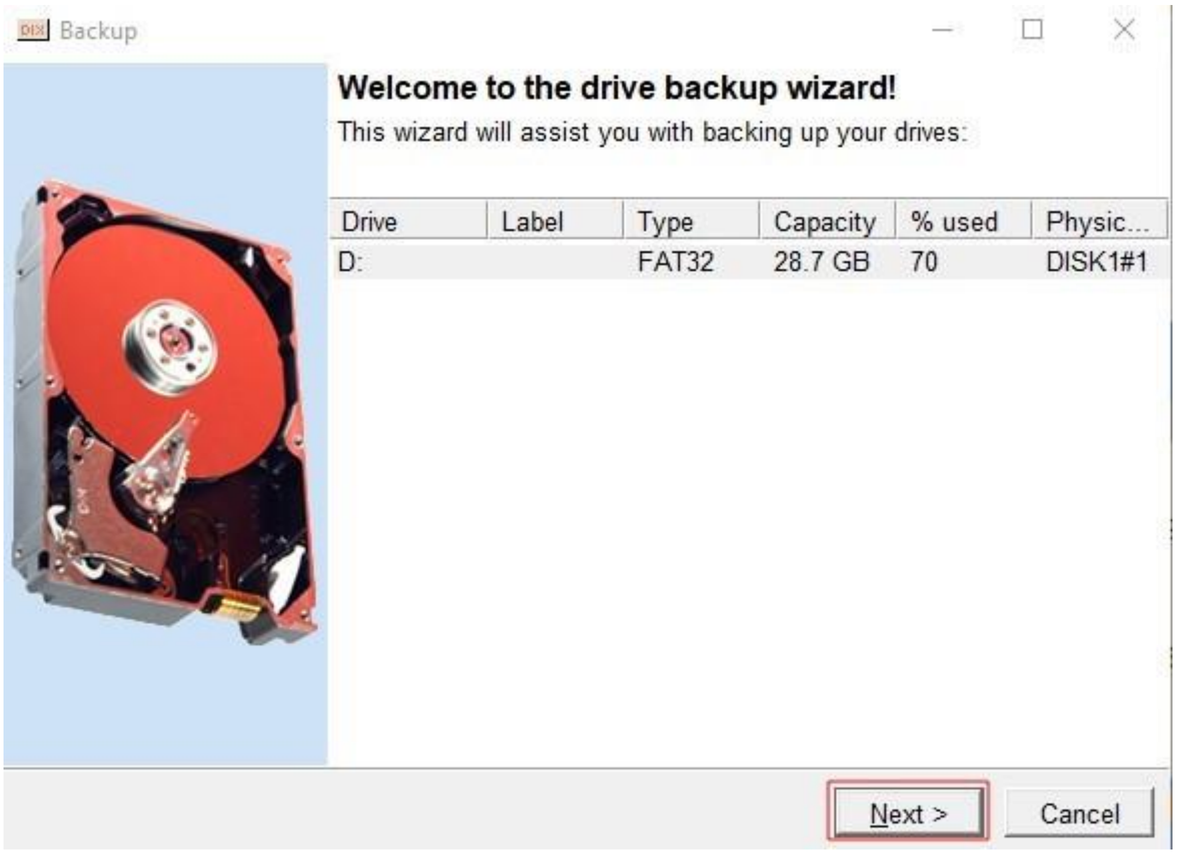
Drive	Label	Type	Capacity	% used	Physical drive
C:	OS	NTFS	930 GB	37	DISK0#3
D:		FAT32	28.7 GB	70	DISK1#1

Drive details:

Logical Information	
Drive:	C:
Label:	OS
File system:	NTFS
Total sectors:	1,951,317,384
Used bytes:	373,855,891,456 (348 GB)
Free bytes:	625,218,609,152 (582 GB)
Total bytes:	999,074,500,608 (930 GB)

Physical Information	
Drive:	DISK0
Drive name:	TOSHIBA MQ04ABF100
Total sectors:	1,953,525,168
Partition:	#3
Start sector on drive:	567,296
Sectors in partition:	1,951,317,391

Memory in use: 694,848

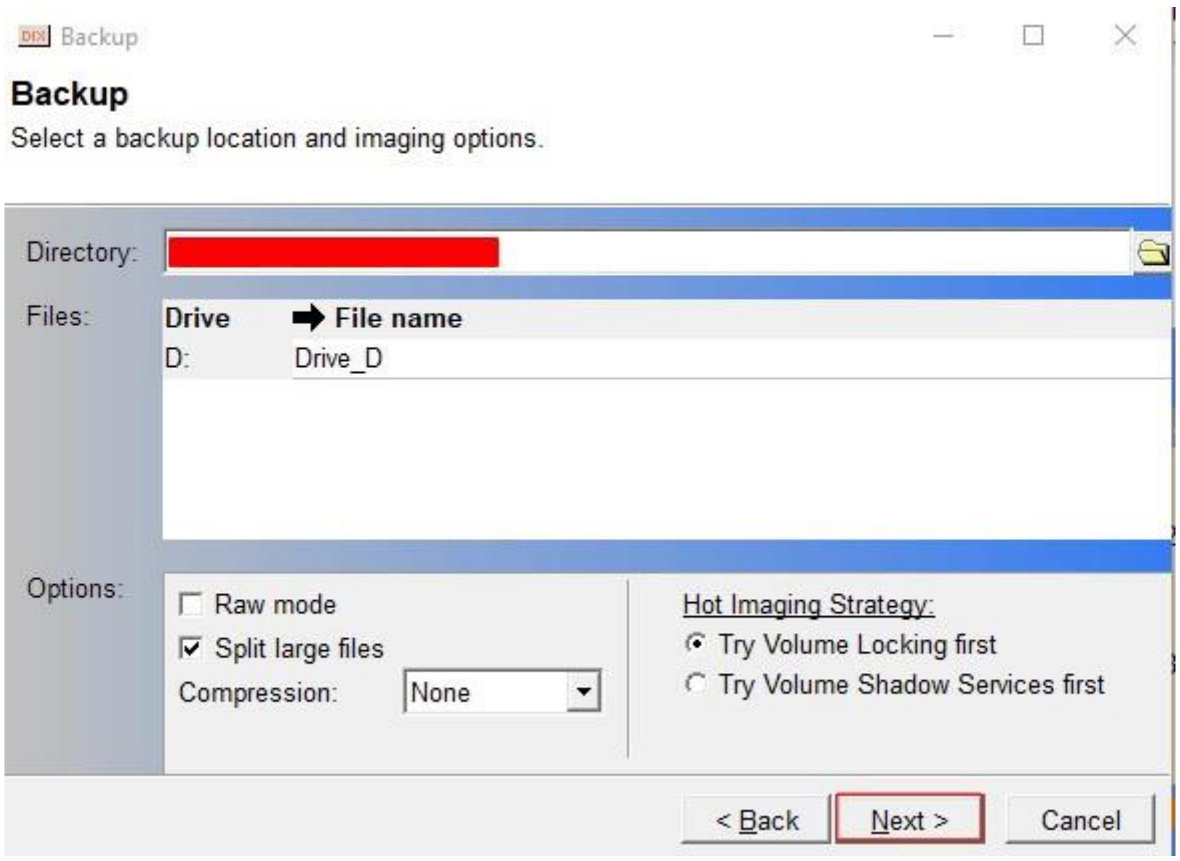


Welcome to the drive backup wizard!

This wizard will assist you with backing up your drives:

Drive	Label	Type	Capacity	% used	Physic...
D:		FAT32	28.7 GB	70	DISK1#1

- Confirm other details such as Output location and other settings and when comfortable, click on Next.



Backup

Select a backup location and imaging options.

Directory: [redacted]

Files:

Drive	File name
D:	Drive_D

Options:

☐ Raw mode

☑ Split large files

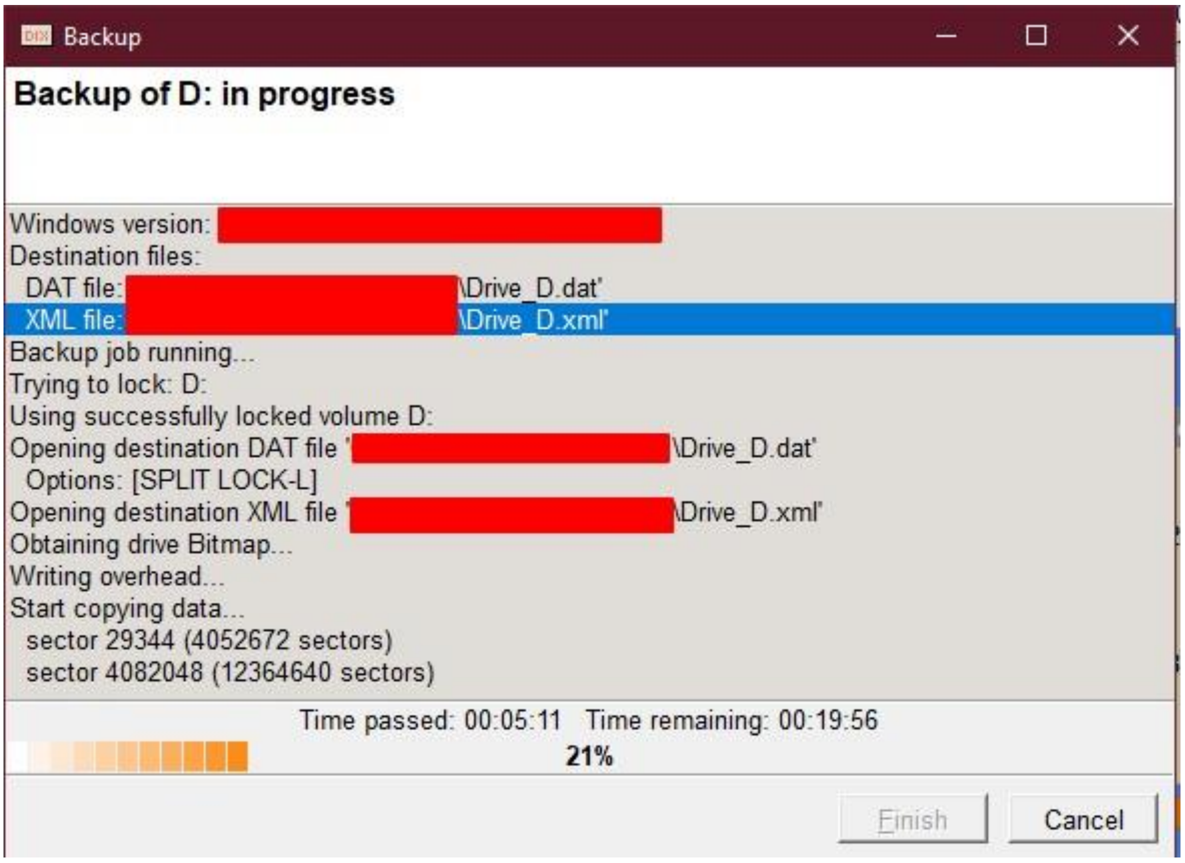
Compression: None

Hot Imaging Strategy:

◉ Try Volume Locking first

○ Try Volume Shadow Services first

- The backup process will start shortly. Wait until the progress bar reaches 100%. After which click on Finish.

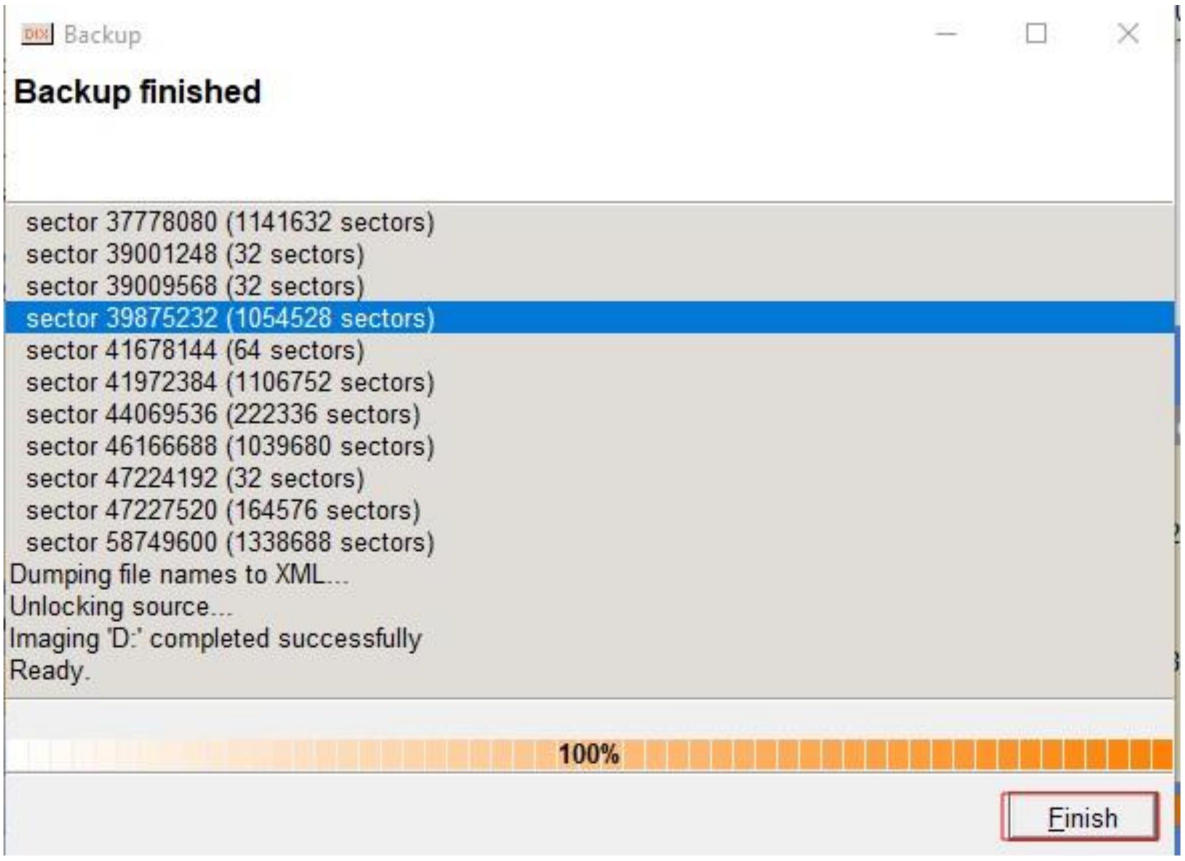


Backup of D: in progress

```
Windows version: [redacted]
Destination files:
  DAT file: [redacted]\Drive_D.dat'
  XML file: [redacted]\Drive_D.xml'
Backup job running...
Trying to lock: D:
Using successfully locked volume D:
Opening destination DAT file '[redacted]\Drive_D.dat'
  Options: [SPLIT LOCK-L]
Opening destination XML file '[redacted]\Drive_D.xml'
Obtaining drive Bitmap...
Writing overhead...
Start copying data...
  sector 29344 (4052672 sectors)
  sector 4082048 (12364640 sectors)
```

Time passed: 00:05:11 Time remaining: 00:19:56

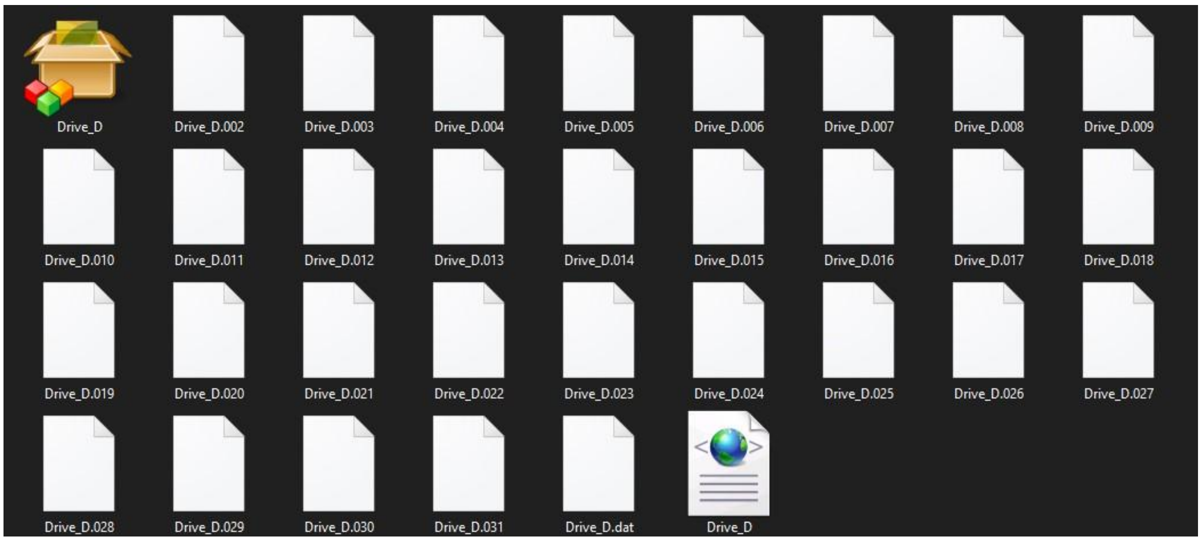
21%



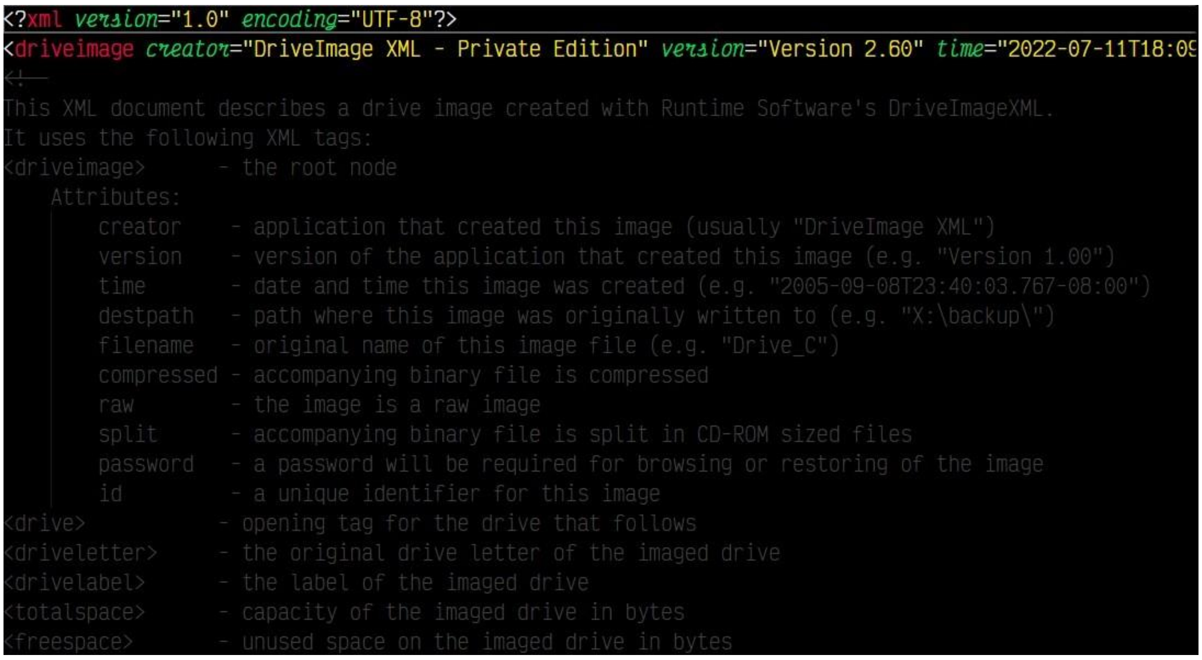
Backup finished

```
 sector 37778080 (1141632 sectors)
 sector 39001248 (32 sectors)
 sector 39009568 (32 sectors)
 sector 39875232 (1054528 sectors)
 sector 41678144 (64 sectors)
 sector 41972384 (1106752 sectors)
 sector 44069536 (222336 sectors)
 sector 46166688 (1039680 sectors)
 sector 47224192 (32 sectors)
 sector 47227520 (164576 sectors)
 sector 58749600 (1338688 sectors)
Dumping file names to XML...
Unlocking source...
Imaging 'D:' completed successfully
Ready.
```

- The following files will be generated in the destination folder.



- The generated XML file has the following text:



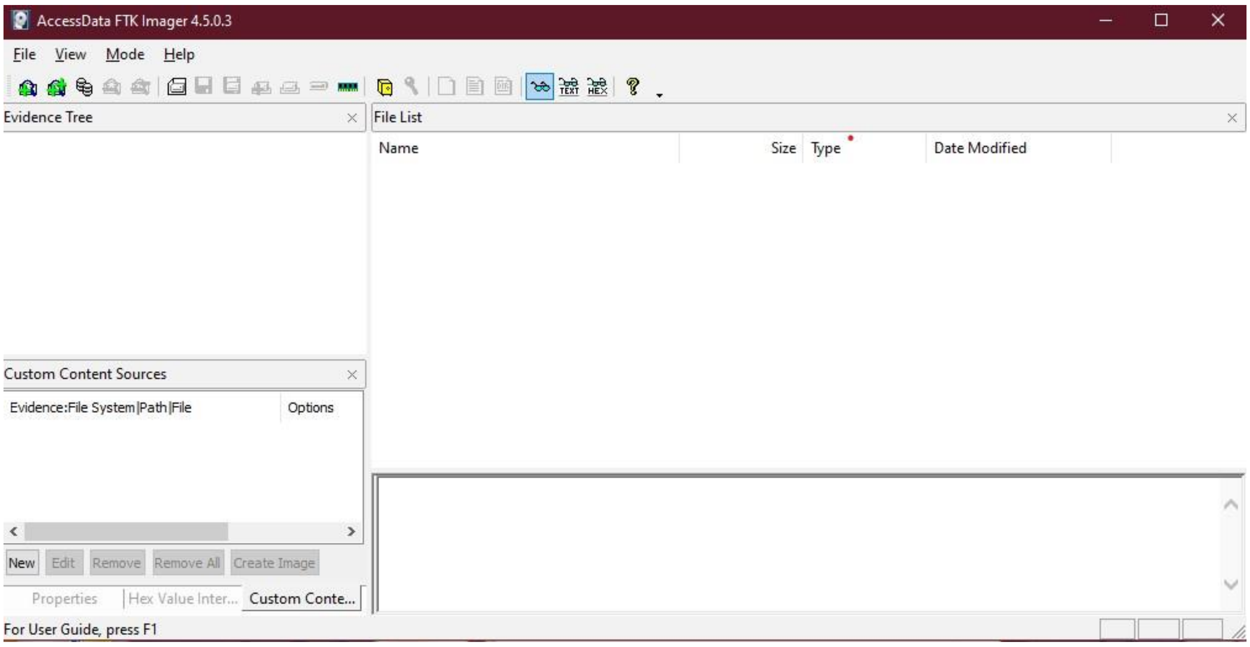
```
<?xml version="1.0" encoding="UTF-8"?>
<driveimage creator="DriveImage XML - Private Edition" version="Version 2.60" time="2022-07-11T18:09
<!--
This XML document describes a drive image created with Runtime Software's DriveImageXML.
It uses the following XML tags:
<driveimage>      - the root node
    Attributes:
        creator    - application that created this image (usually "DriveImage XML")
        version    - version of the application that created this image (e.g. "Version 1.00")
        time       - date and time this image was created (e.g. "2005-09-08T23:40:03.767-08:00")
        destpath   - path where this image was originally written to (e.g. "X:\backup\")
        filename   - original name of this image file (e.g. "Drive_C")
        compressed - accompanying binary file is compressed
        raw        - the image is a raw image
        split      - accompanying binary file is split in CD-ROM sized files
        password   - a password will be required for browsing or restoring of the image
        id         - a unique identifier for this image
<drive>           - opening tag for the drive that follows
<driveletter>     - the original drive letter of the imaged drive
<drivelabel>      - the label of the imaged drive
<totalspace>      - capacity of the imaged drive in bytes
<freespace>       - unused space on the imaged drive in bytes
```

Practical 7

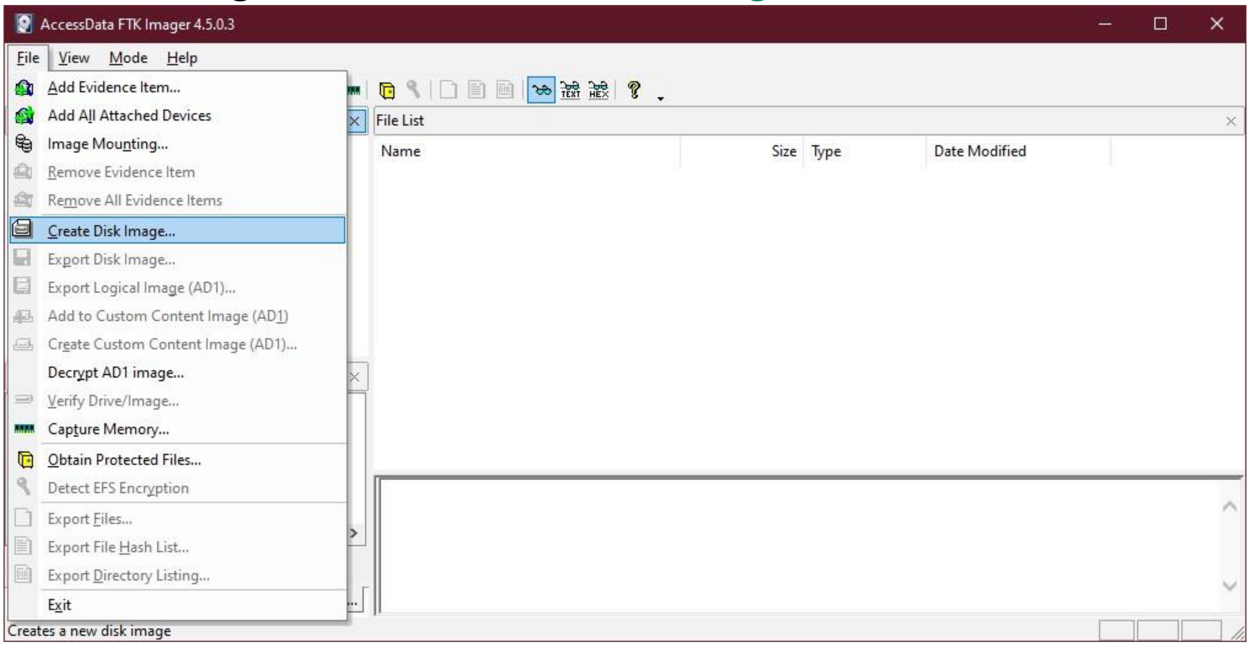
Aim: Create a forensic image of a digital device from volatile data such as memory.

Procedure:

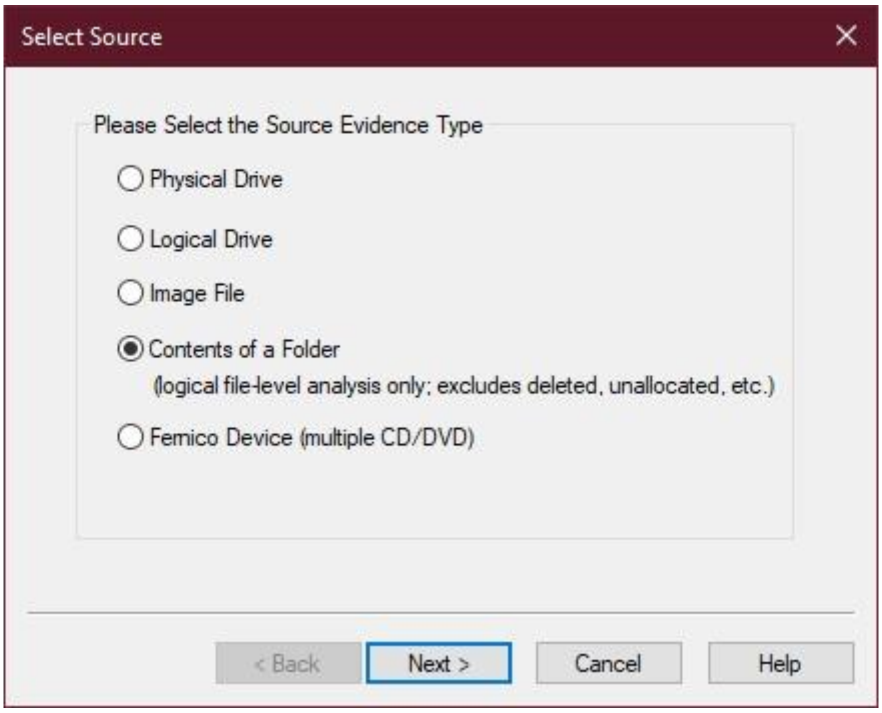
- Download and install AccessData® FTK® Imager from this link. Launching the application will display a screen similar to this:


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

- Now, navigate to File > Create Disk Image....



- This should bring up a new window. Select the Contents of a Folder option for the source. Click on Next.

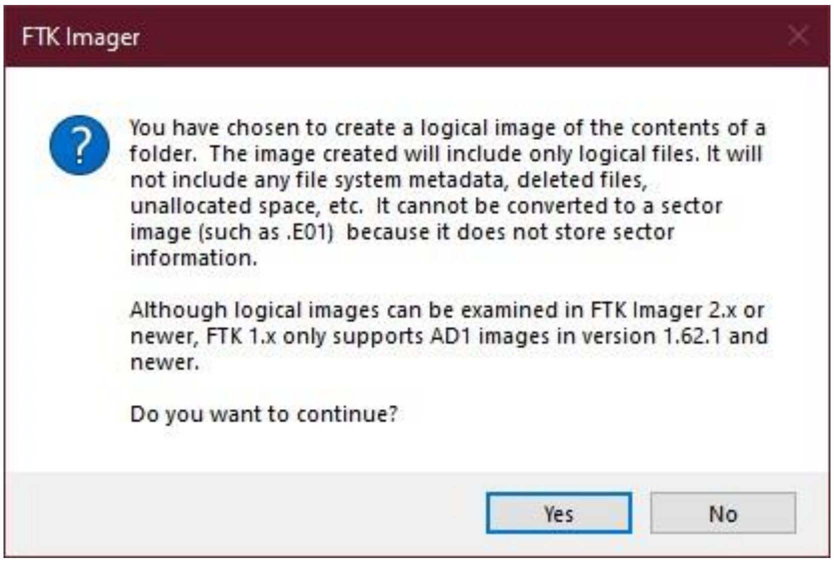


Select Source

Please Select the Source Evidence Type

- ○ Physical Drive
- ○ Logical Drive
- ○ Image File
- ● Contents of a Folder
  (logical file-level analysis only; excludes deleted, unallocated, etc.)
- ○ Femico Device (multiple CD/DVD)

- The generated warning window can be ignored. Simply click on Next.



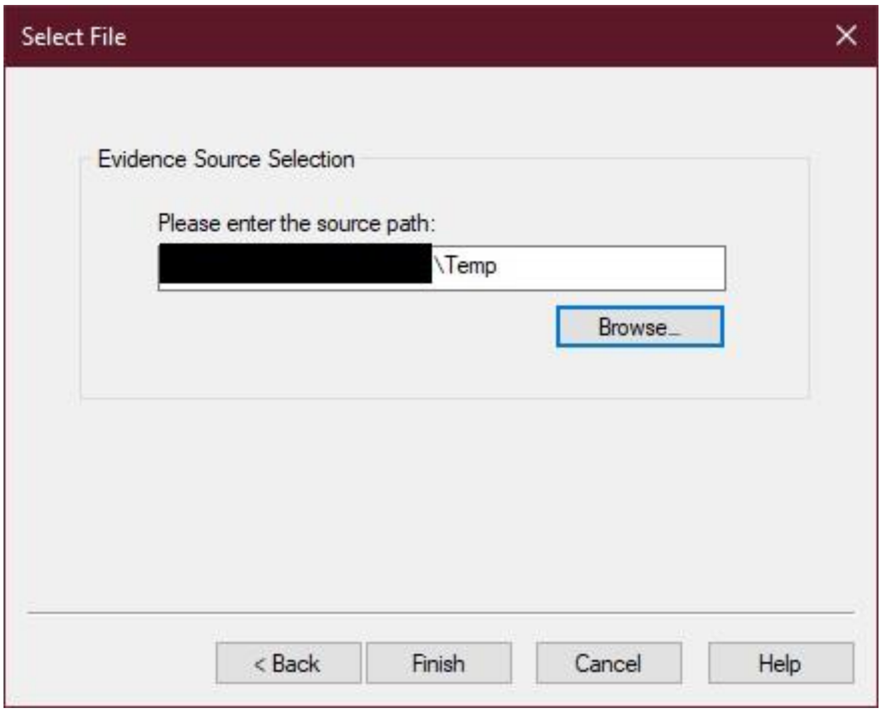
FTK Imager

You have chosen to create a logical image of the contents of a folder. The image created will include only logical files. It will not include any file system metadata, deleted files, unallocated space, etc. It cannot be converted to a sector image (such as .E01) because it does not store sector information.

Although logical images can be examined in FTK Imager 2.x or newer, FTK 1.x only supports AD1 images in version 1.62.1 and newer.

Do you want to continue?

- The window will now ask for a source location. Enter the location of your choice and click on Finish.



Select File

Evidence Source Selection

Please enter the source path:

[redacted]\Temp

•

Now, a new dialog box will appear. Confirm your source selection and then click on the Add... to add a new destination.

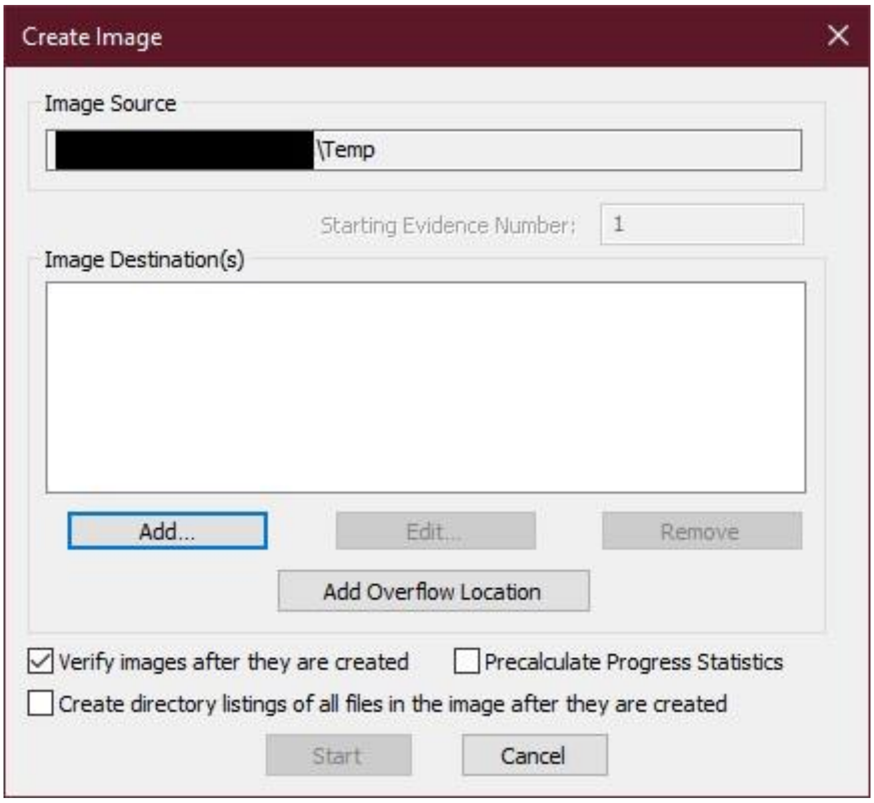

Create Image

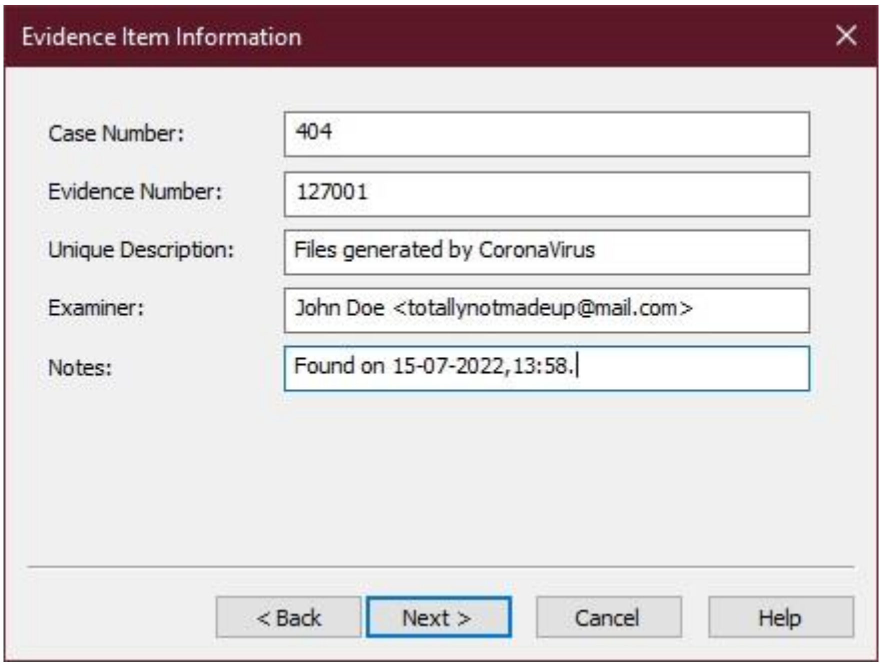
Image Source

[redacted]\Temp

Starting Evidence Number: 1

Image Destination(s)

[✓] Verify images after they are created
[ ] Precalculate Progress Statistics
[ ] Create directory listings of all files in the image after they are created


Evidence Item Information

Case Number:	404
Evidence Number:	127001
Unique Description:	Files generated by CoronaVirus
Examiner:	John Doe <totallynotmadeup@mail.com>
Notes:	Found on 15-07-2022,13:58.

-

- A new window will appear which will ask for information about this particular item. Fill it and then click on Next.
  Select the destination of your choice and provide the filename of the (soon to be) generated image file(s). Click on Finish.

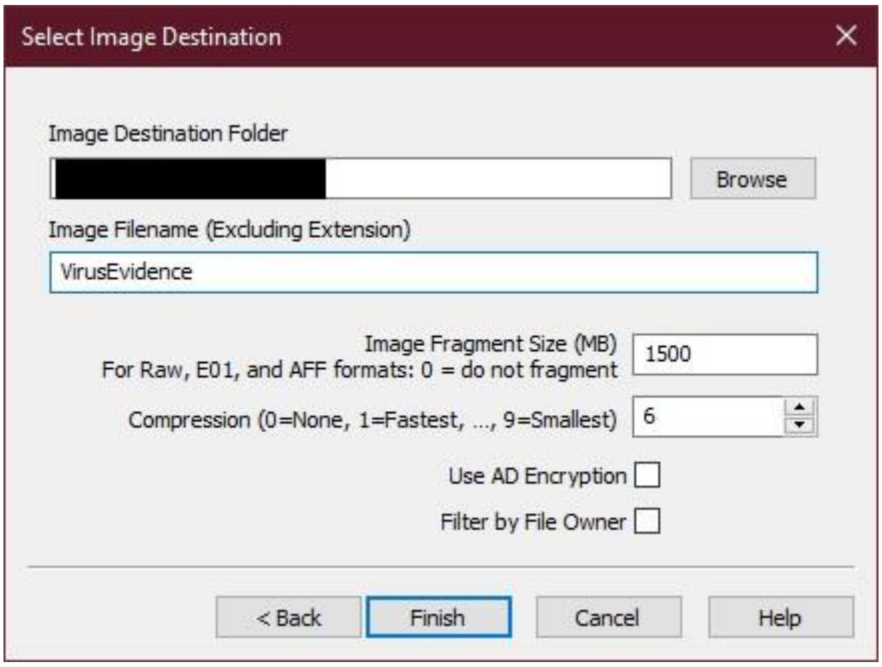

Select Image Destination

Image Destination Folder: [redacted]

Image Filename (Excluding Extension): VirusEvidence

Image Fragment Size (MB)
For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

Use AD Encryption ☐

Filter by File Owner ☐

- The newly created entry should now be visible in the Image Destinations list. Click on Start.

•

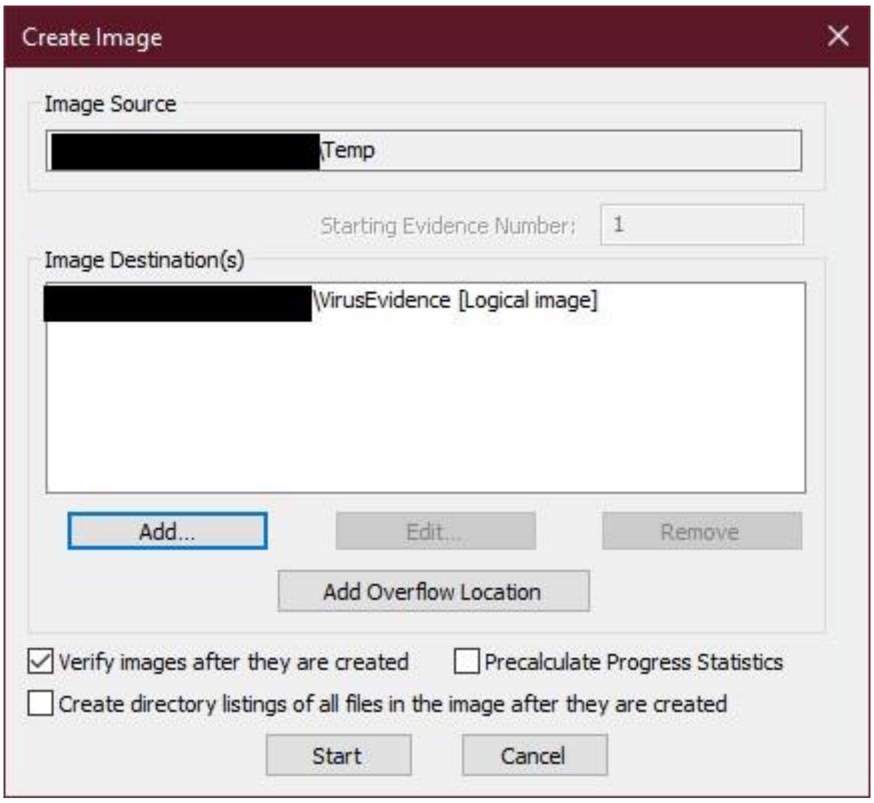

Create Image

Image Source

[redacted]\Temp

Starting Evidence Number: 1

Image Destination(s)

[redacted]\VirusEvidence [Logical image]

☑ Verify images after they are created
☐ Precalculate Progress Statistics
☐ Create directory listings of all files in the image after they are created

The process will take some time to complete (depending on the size and type of files/folders). After which you'll see a process completion screen and a verification screen.

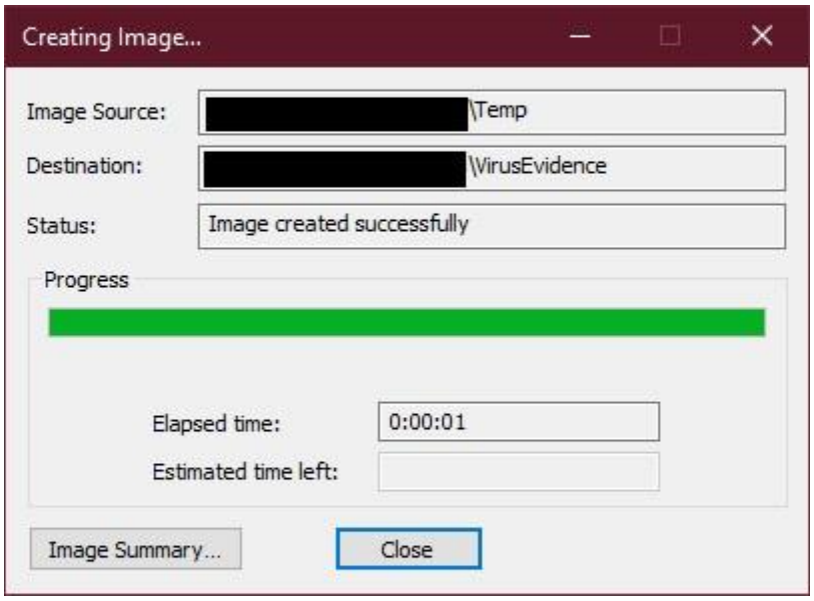

Creating Image...

Image Source: [redacted]\Temp

Destination: [redacted]\VirusEvidence

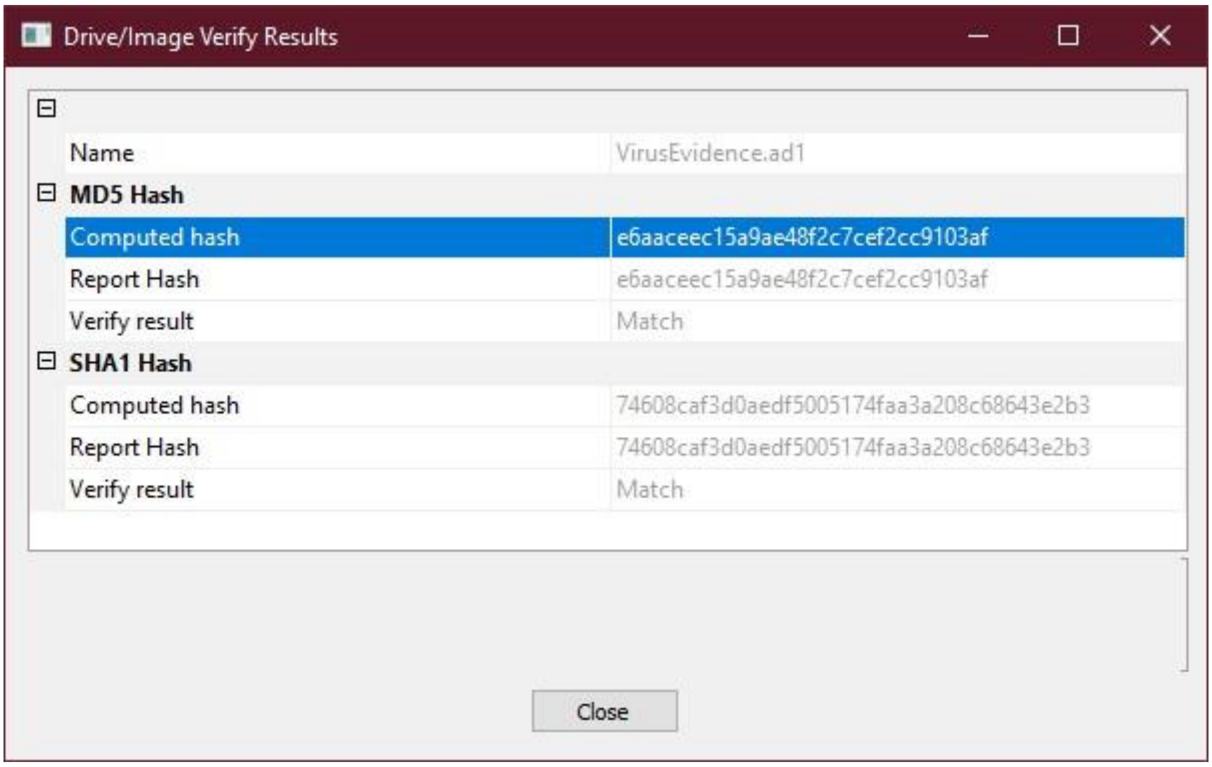
Status: Image created successfully

Progress

Elapsed time: 0:00:01

Estimated time left:

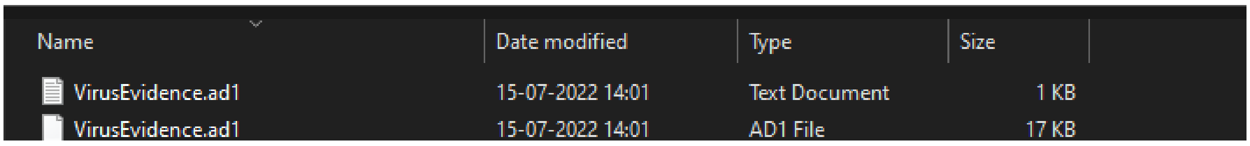
•



Drive/Image Verify Results

Name	VirusEvidence.ad1
MD5 Hash	
Computed hash	e6aaceec15a9ae48f2c7cef2cc9103af
Report Hash	e6aaceec15a9ae48f2c7cef2cc9103af
Verify result	Match
SHA1 Hash	
Computed hash	74608caf3d0aedf5005174faa3a208c68643e2b3
Report Hash	74608caf3d0aedf5005174faa3a208c68643e2b3
Verify result	Match

You'll also see some files generated in your destination folder.



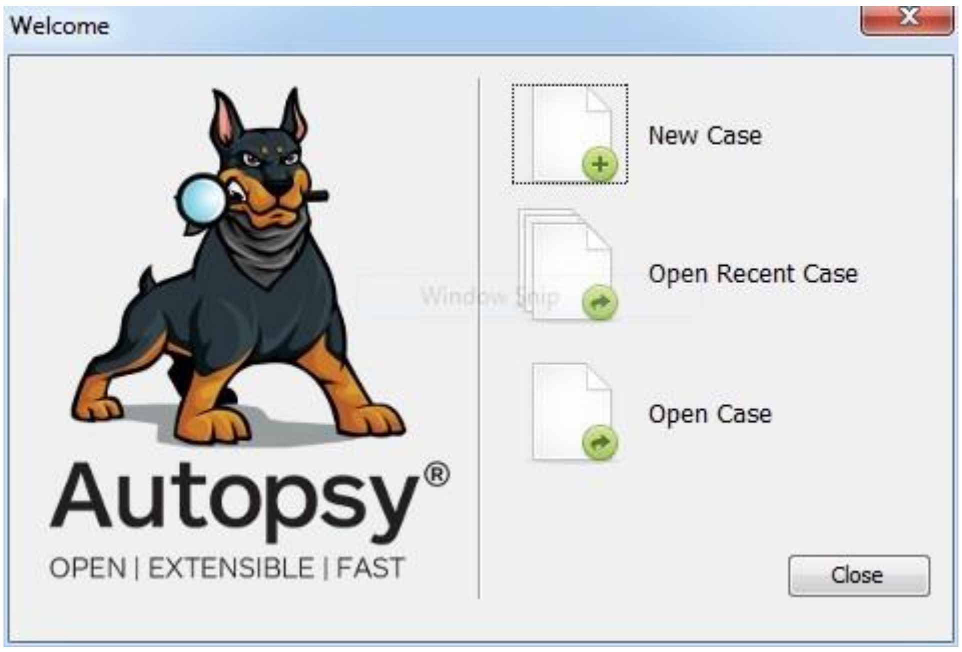
Name	Date modified	Type	Size
VirusEvidence.ad1	15-07-2022 14:01	Text Document	1 KB
VirusEvidence.ad1	15-07-2022 14:01	AD1 File	17 KB

Practical 8

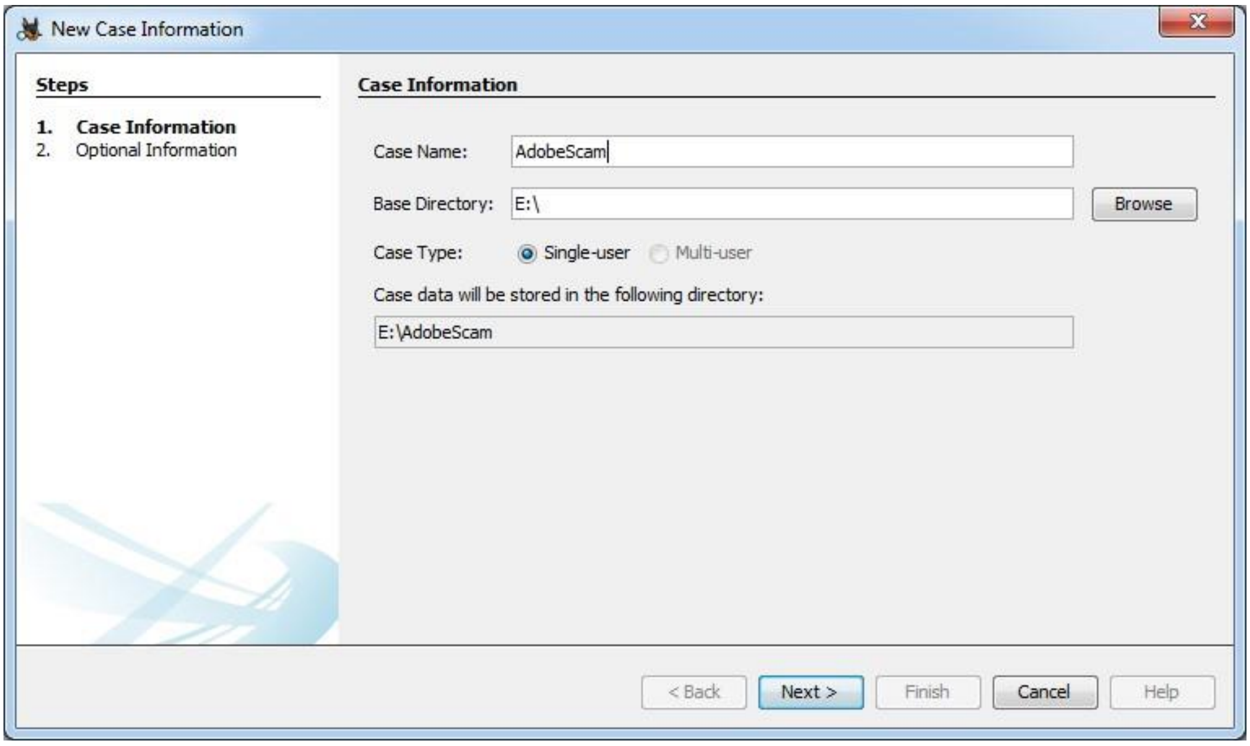
Aim: Retrieve deleted files from a computer.

Procedure:

- Download and install Autopsy® from this link. Running the application should present you this window:



- Click on New Case. It should present you this window asking for case name and the directory to store case-related data.



Case Name: AdobeScam

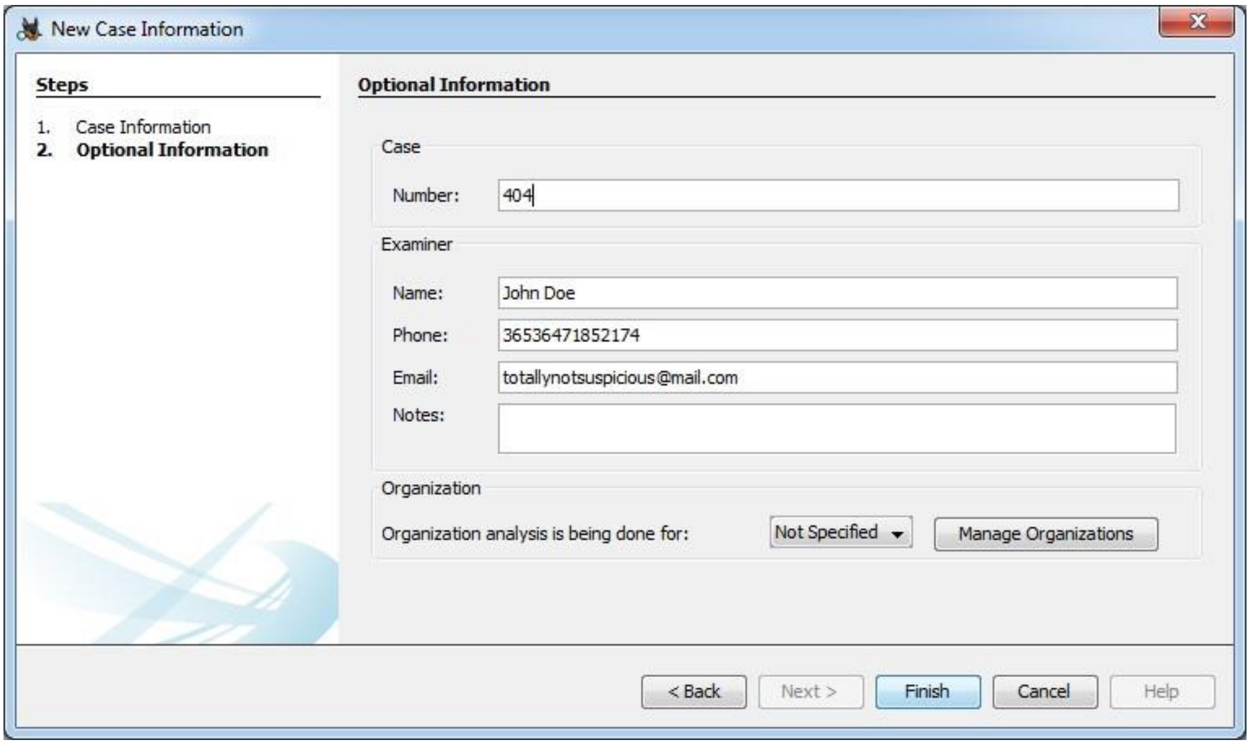
Base Directory: E:\

Case Type: [✓ Single-user] Multi-user

Case data will be stored in the following directory:

E:\AdobeScam

- Enter the relevant details and click on Next. A new section will be available which will ask you to fill in optional information. You *may* choose to not enter any information in this section. Click Finish when you're done.


New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 404

Examiner

Name: John Doe

Phone: 36536471852174

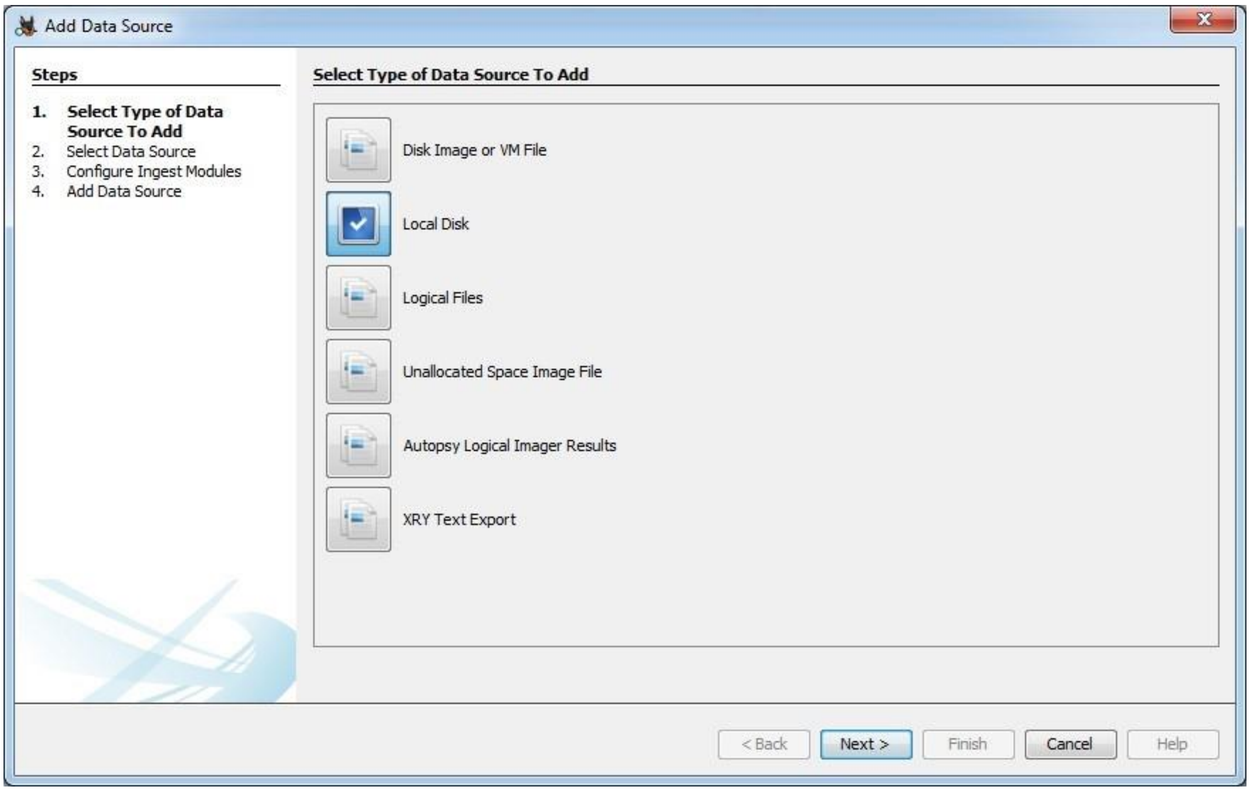
Email: totallynotsuspicious@mail.com

Notes:

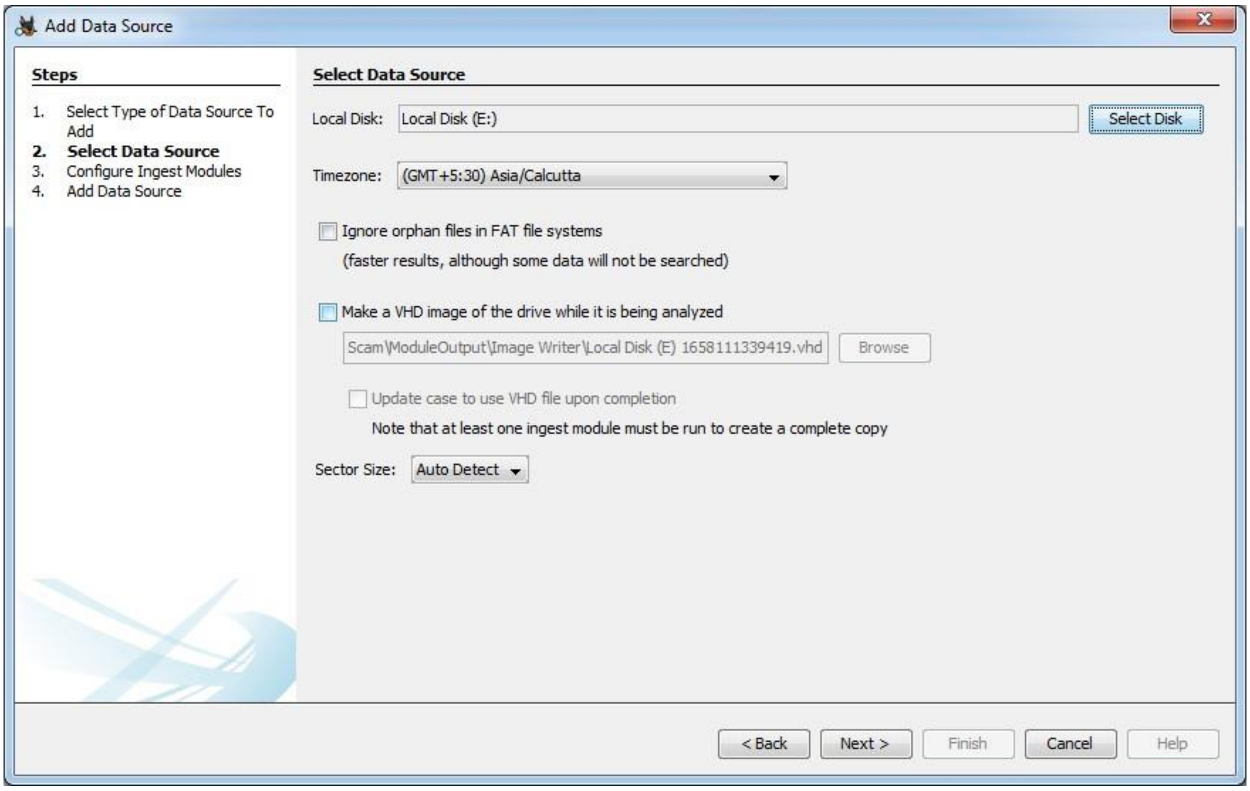
Organization

Organization analysis is being done for: Not Specified

- A new window titled Add Data Source should now be visible. If it does not appear automatically, you can manually open it using the relevant toolbar item. Select Local Disk as the type of data source to be added and click on Next.


Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

- A new section named Select Data Source should now be active. Select the disk of your choice and click on Next.



Local Disk: Local Disk (E:)

Timezone: (GMT+5:30) Asia/Calcutta

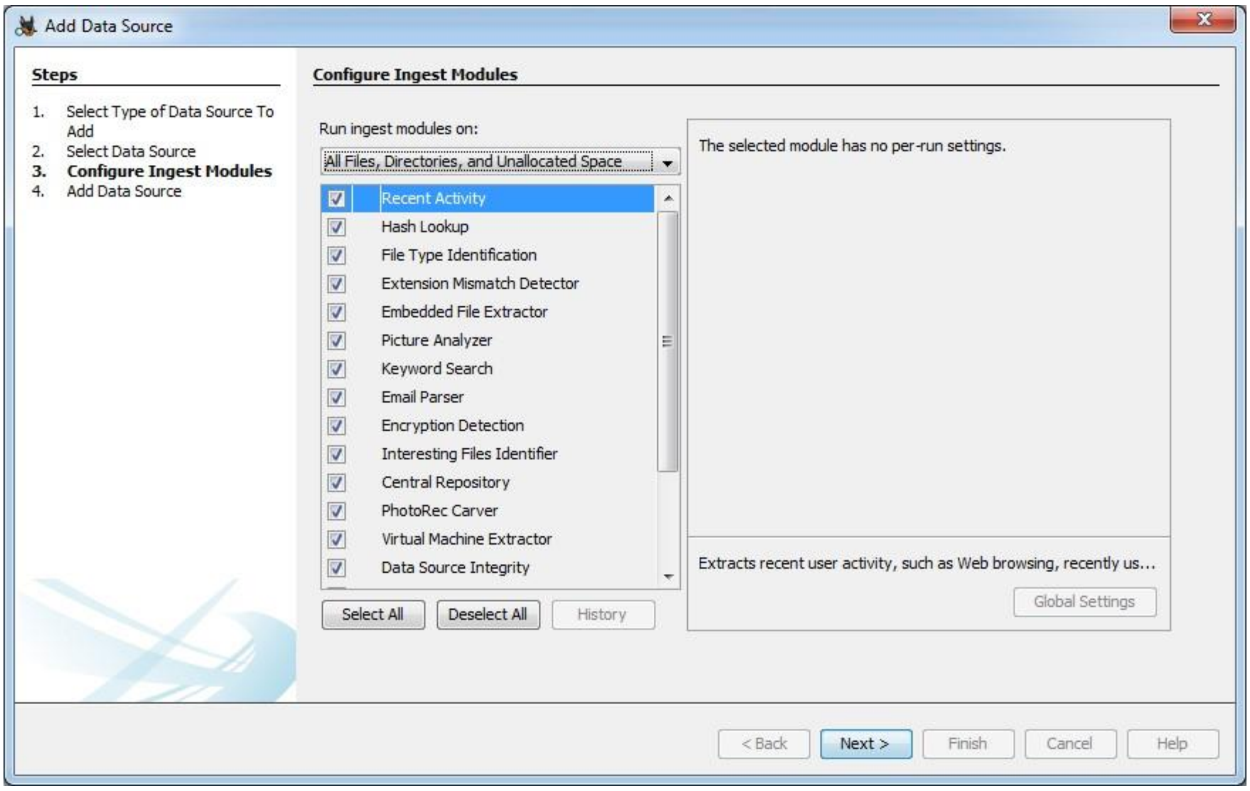
☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

☐ Make a VHD image of the drive while it is being analyzed
Scam\ModuleOutput\Image Writer\Local Disk (E) 1658111339419.vhd

☐ Update case to use VHD file upon completion
Note that at least one ingest module must be run to create a complete copy

Sector Size: Auto Detect

- You can use the default options in the Configure Ingest Modules section. After which, the data source will be added to the case database.



Add Data Source

Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. **Configure Ingest Modules**
4. Add Data Source

Configure Ingest Modules

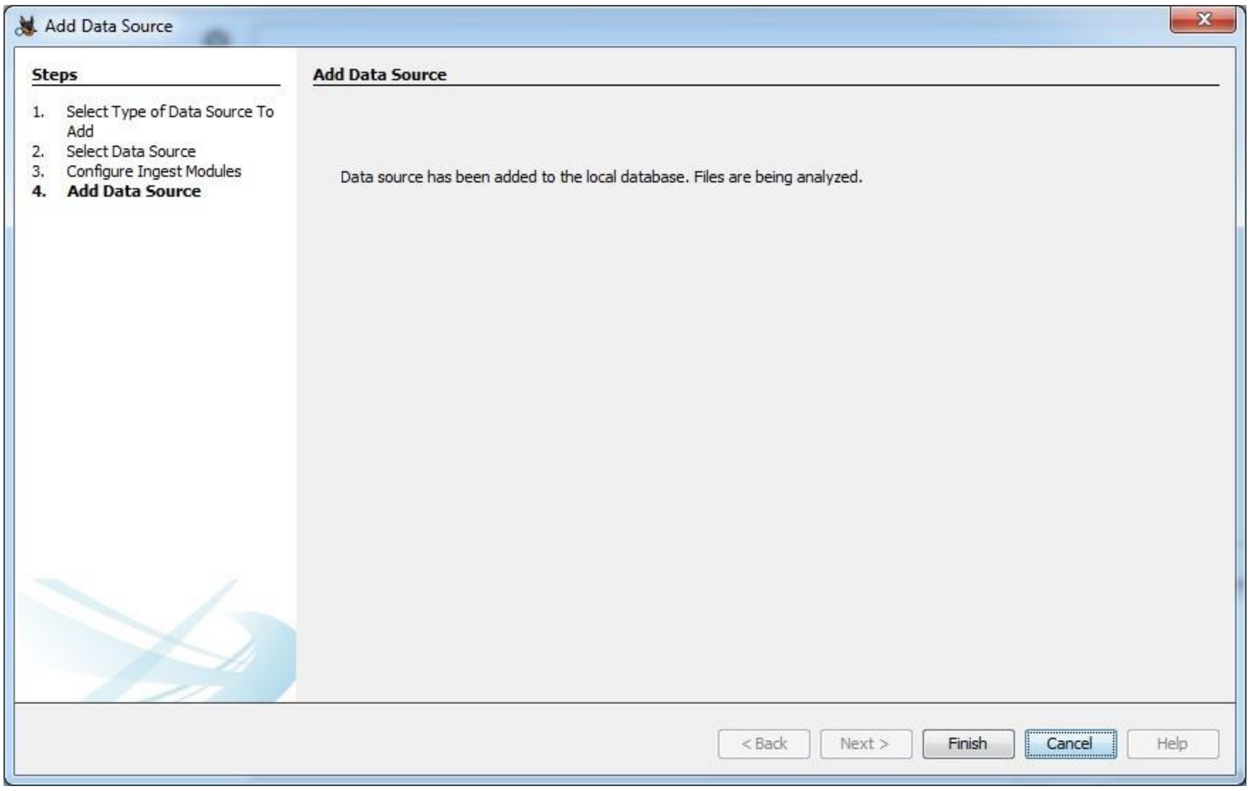
Run ingest modules on:

All Files, Directories, and Unallocated Space

- [✓] Recent Activity
- [✓] Hash Lookup
- [✓] File Type Identification
- [✓] Extension Mismatch Detector
- [✓] Embedded File Extractor
- [✓] Picture Analyzer
- [✓] Keyword Search
- [✓] Email Parser
- [✓] Encryption Detection
- [✓] Interesting Files Identifier
- [✓] Central Repository
- [✓] PhotoRec Carver
- [✓] Virtual Machine Extractor
- [✓] Data Source Integrity

The selected module has no per-run settings.

Extracts recent user activity, such as Web browsing, recently us...



Add Data Source

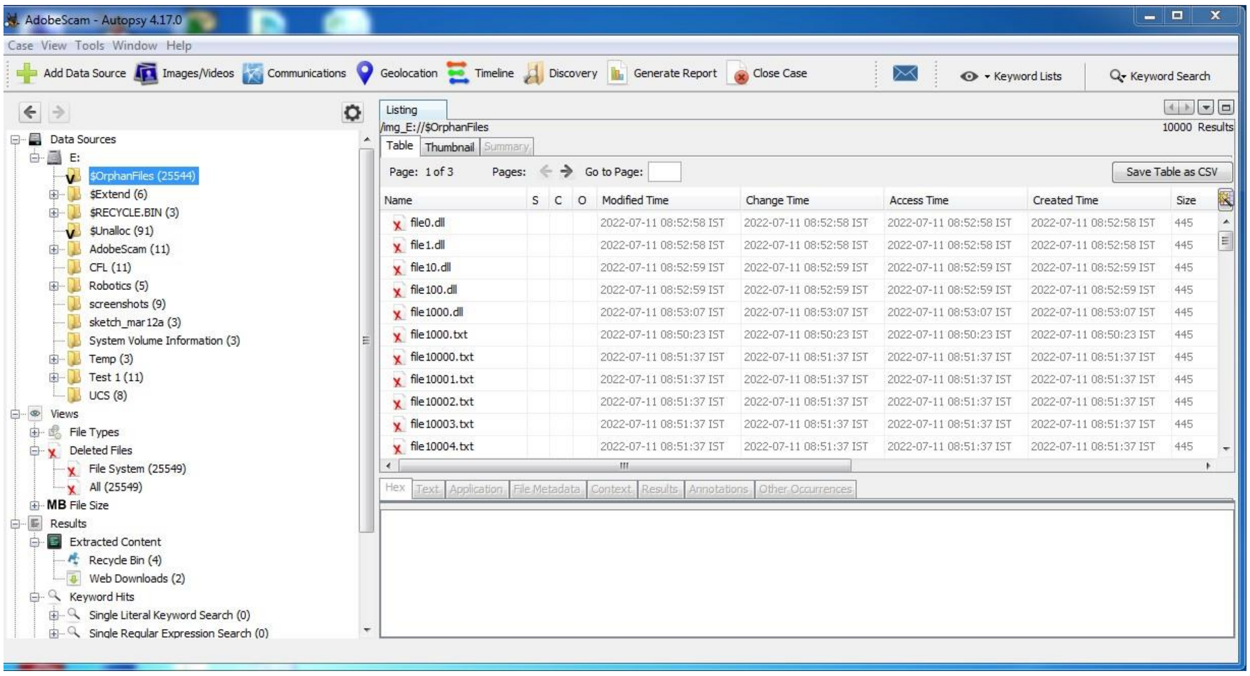
Steps

1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. **Add Data Source**

Add Data Source

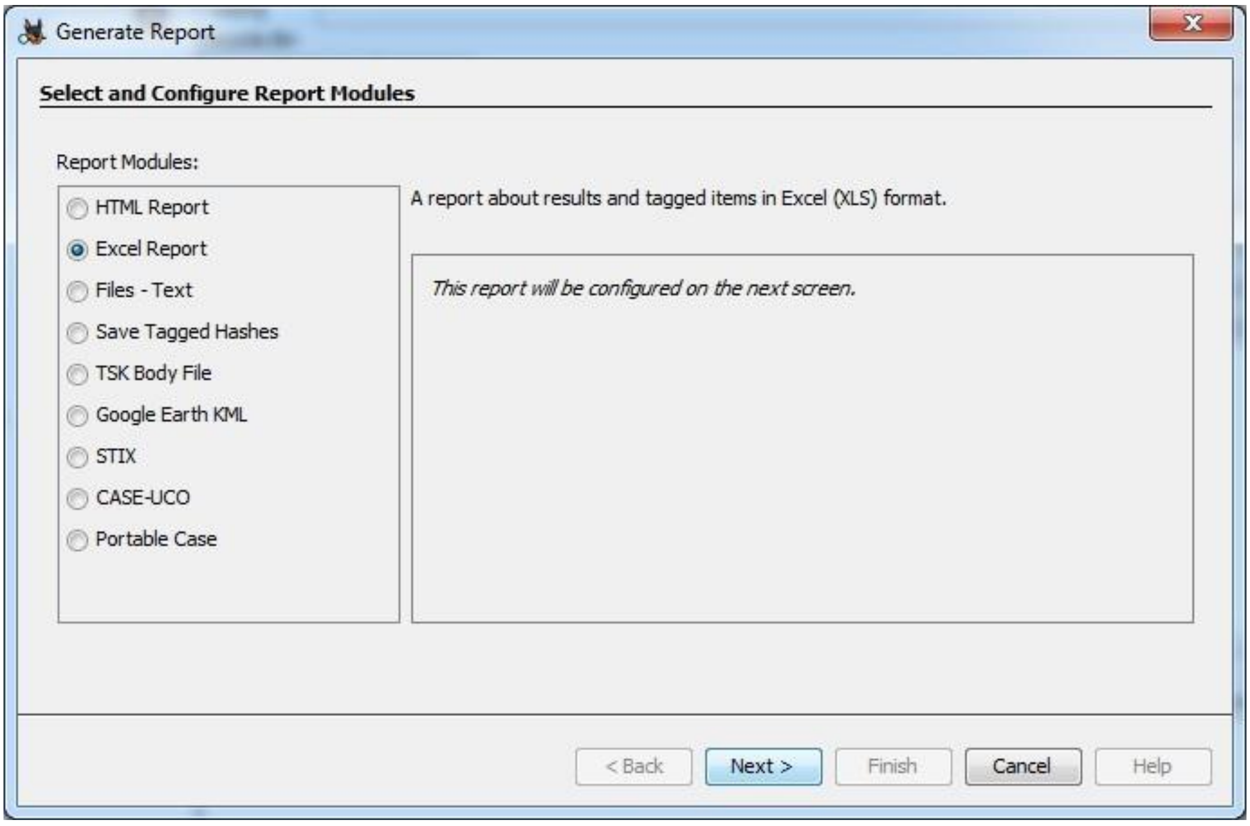
Data source has been added to the local database. Files are being analyzed.

- Autopsy® will now try to process the data source. This process may take some time depending on the size of the disk and its contents. After completion, you will see all the information it has gathered ordered as a tree. Now, navigate to Data Sources > {Disk of your choice} > $OrphanFiles. It will show all the deleted files. You can retrieve it by right clicking the file(s) and selecting Export. It will ask for a location to restore the file.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
file0.dll				2022-07-11 08:52:58 IST	2022-07-11 08:52:58 IST	2022-07-11 08:52:58 IST	2022-07-11 08:52:58 IST	445
file1.dll				2022-07-11 08:52:58 IST	2022-07-11 08:52:58 IST	2022-07-11 08:52:58 IST	2022-07-11 08:52:58 IST	445
file10.dll				2022-07-11 08:52:59 IST	2022-07-11 08:52:59 IST	2022-07-11 08:52:59 IST	2022-07-11 08:52:59 IST	445
file100.dll				2022-07-11 08:52:59 IST	2022-07-11 08:52:59 IST	2022-07-11 08:52:59 IST	2022-07-11 08:52:59 IST	445
file1000.dll				2022-07-11 08:53:07 IST	2022-07-11 08:53:07 IST	2022-07-11 08:53:07 IST	2022-07-11 08:53:07 IST	445
file1000.txt				2022-07-11 08:50:23 IST	2022-07-11 08:50:23 IST	2022-07-11 08:50:23 IST	2022-07-11 08:50:23 IST	445
file10000.txt				2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	445
file10001.txt				2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	445
file10002.txt				2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	445
file10003.txt				2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	445
file10004.txt				2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	2022-07-11 08:51:37 IST	445

- To generate a report, click the Generate Report toolbar item. It should open a Generate Report wizard. Select the type of report you want and click on Next.


Generate Report

Select and Configure Report Modules

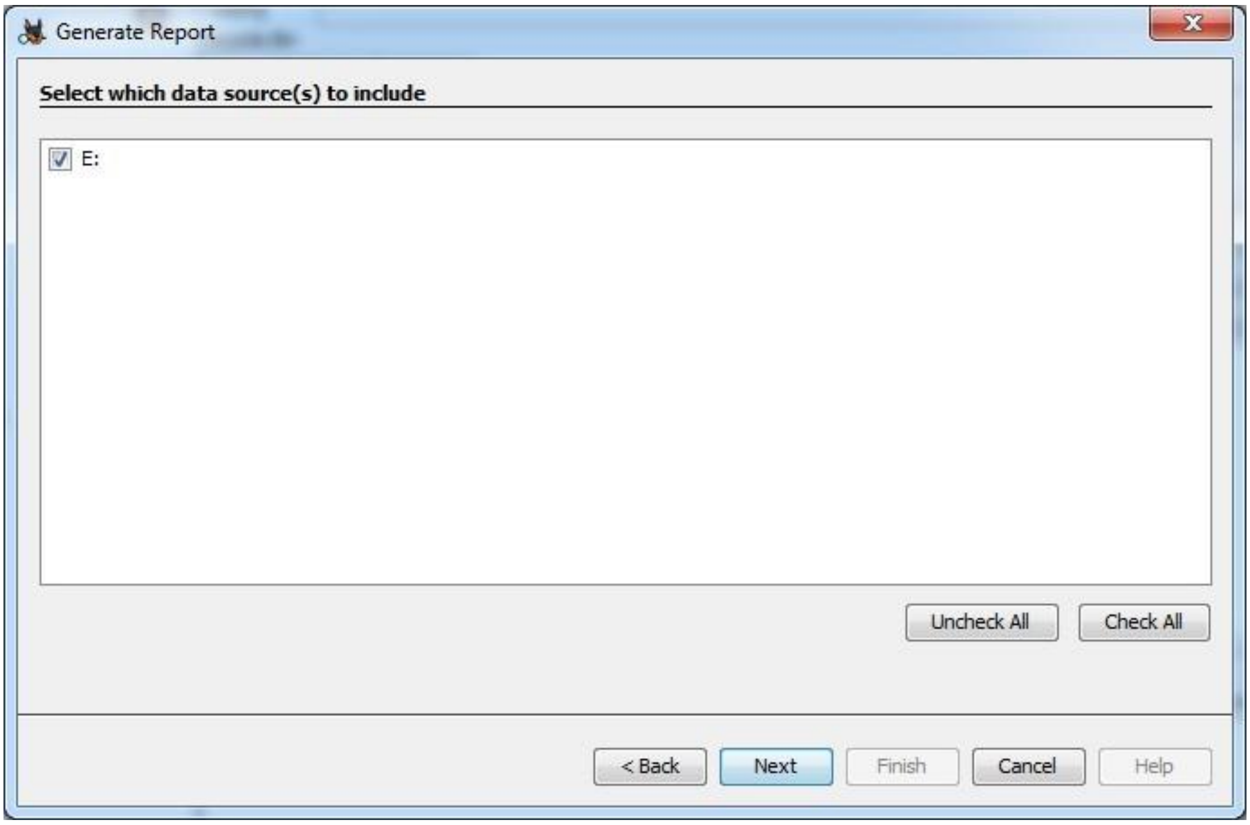
Report Modules:

- ○ HTML Report
- ● Excel Report
- ○ Files - Text
- ○ Save Tagged Hashes
- ○ TSK Body File
- ○ Google Earth KML
- ○ STIX
- ○ CASE-UCO
- ○ Portable Case

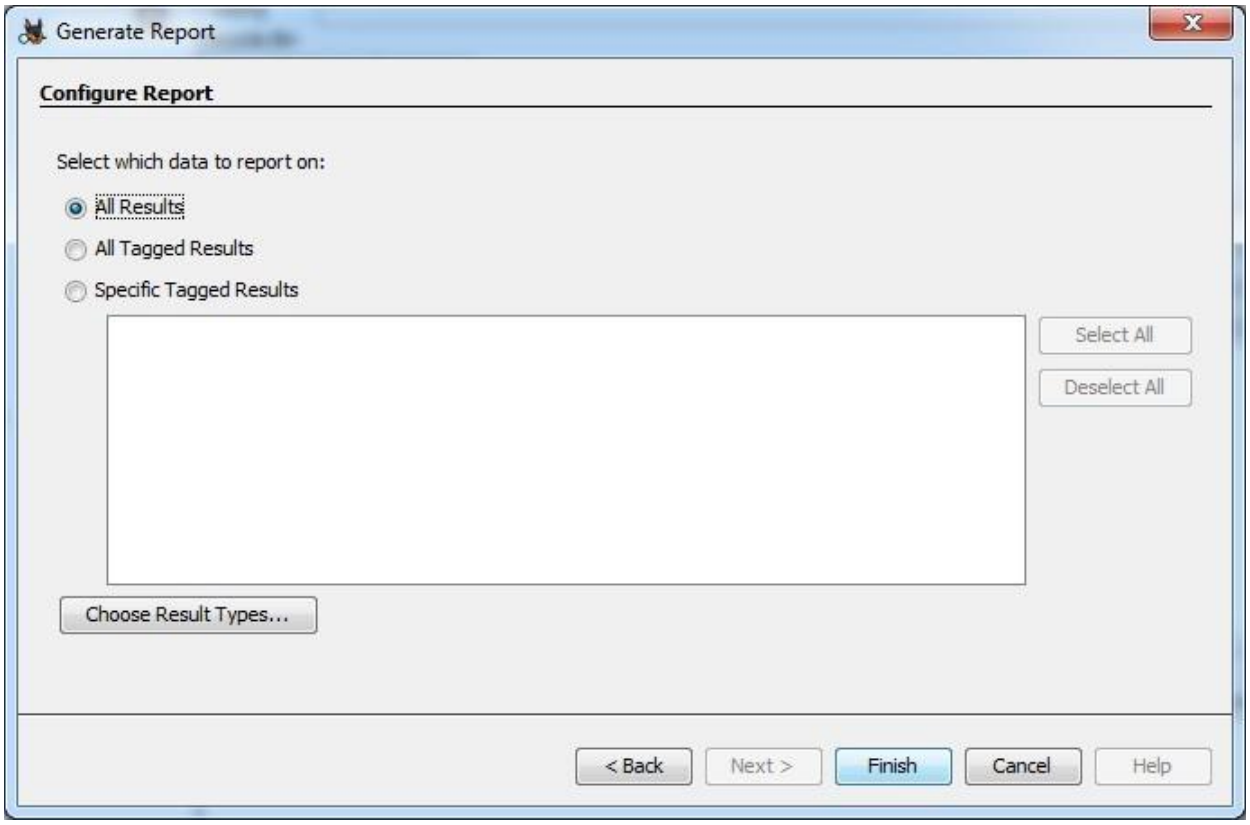
A report about results and tagged items in Excel (XLS) format.

This report will be configured on the next screen.

- Select the data sources to be included and click on Next.

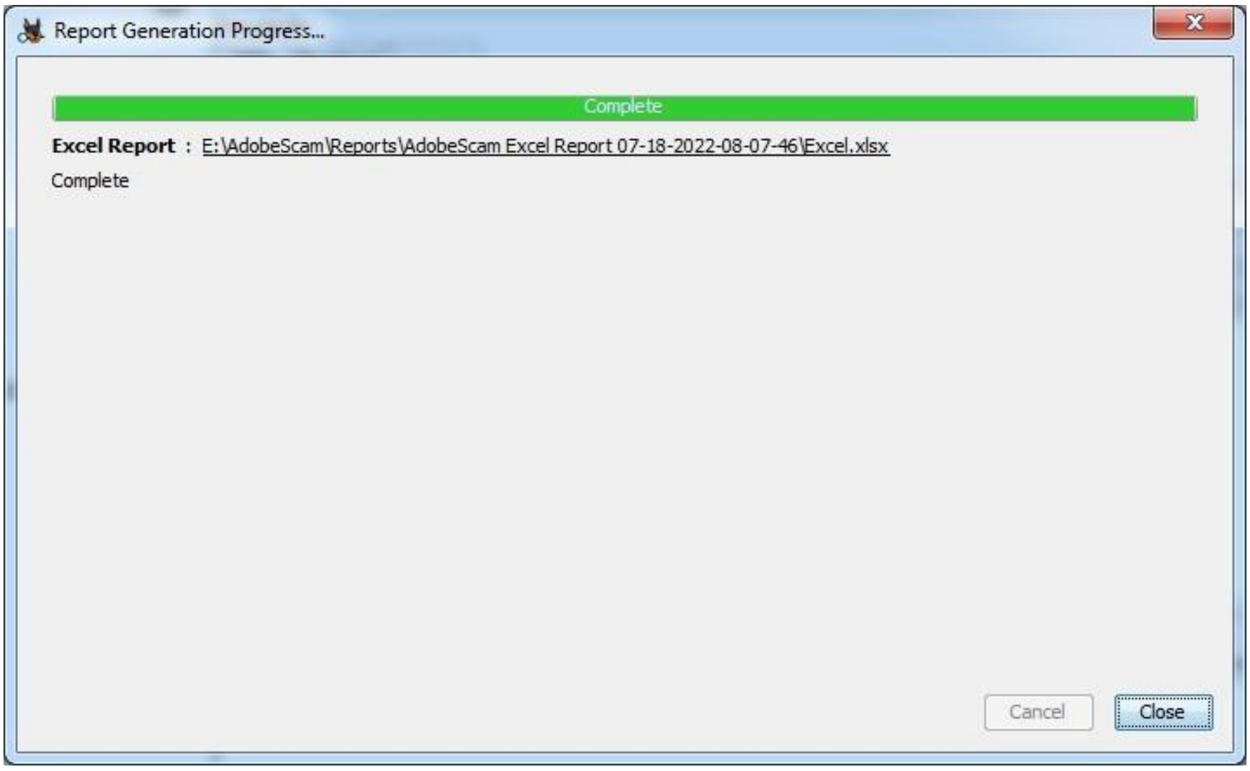


- Select the data which should be reported and click on Finish. The report will be generated.



Select which data to report on:

- [✓ All Results]
- All Tagged Results
- Specific Tagged Results



Excel Report : E:\AdobeScam\Reports\AdobeScam Excel Report 07-18-2022-08-07-46\Excel.xlsx

Complete

Practical 9

Aim: Use the registry to obtain information.

Theory:

The Windows Registry Editor(regedit) was launched in 1992 with Microsoft Windows 3.1. The registry is the backbone of the OS and is critical for system performance. It enables administrators and advanced users to keep the registry operational and make root and administrative level changes such as setting up access permissions or changing the hardware and software level configuration.

Features:

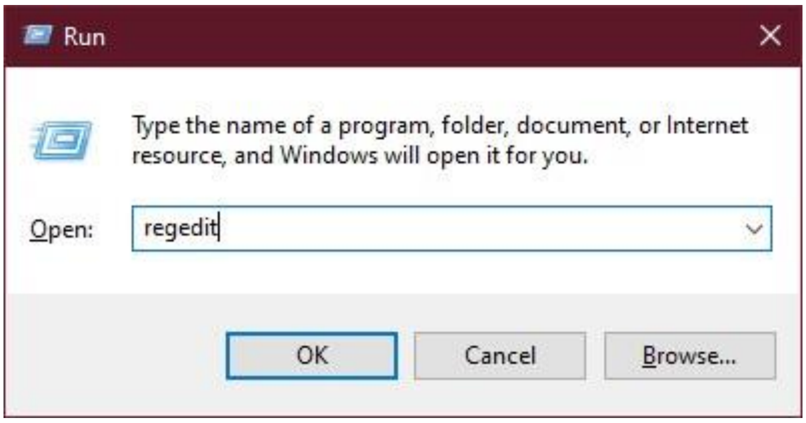
1. **System Performance:**
    - If a key inside the registry becomes corrupt or faulty, it can cause system to crash or other performance issues.
    - Using Registry Editor we can edit/update the key.
2. **Configuration settings:**
    - The automatic type startup programs display or desktop setting can be configured using regedit.
3. **Registry cleaning:**
    - Entries inside the registry can sometimes break. To fix broken entries, a registry cleaner is required.
    - Unlike standard configuration files, entries inside the Registry cannot be opened or cleaned via standard text editor.
4. **Registry errors:**
    - Certain events can disturb the hierarchy and cause errors.

- The regedit tool can be used to fix the hierarchical structure of the registry.

5. **Finding Strings:**
   - regedit can be helpful when searching for specific strings in keys, values (names & values).
6. **Remote editing of registry:**
   - regedit can be used for remote editing of another computer's registry on the same network.
7. **Modification of key:**
   - Registry key can be modified, renamed or deleted by regedit.

Procedure:

- Press Windows key + R to access the Run... command.

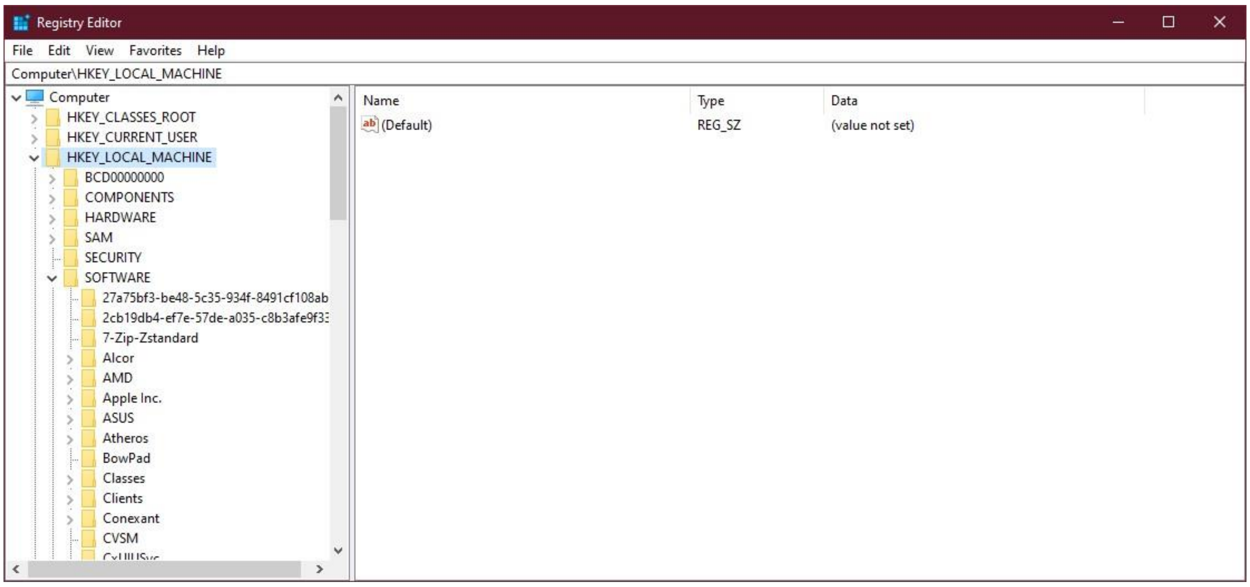


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

- Type regedit and press [Enter].



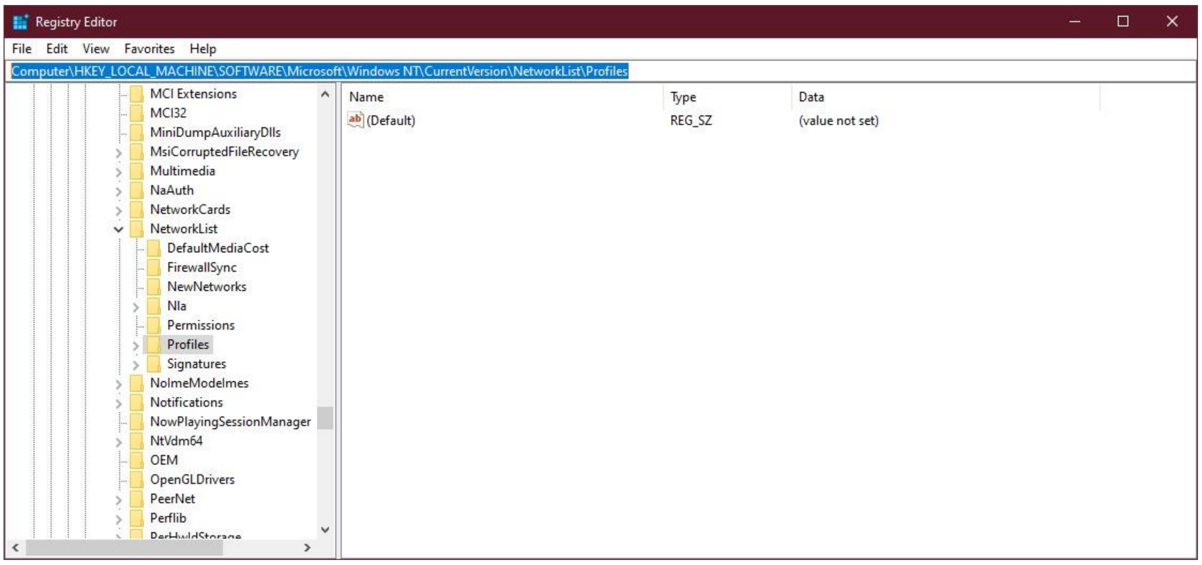
Computer\HKEY_LOCAL_MACHINE

Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
COMPONENTS
HARDWARE
SAM
SECURITY
SOFTWARE
27a75bf3-be48-5c35-934f-8491cf108ab
2cb19db4-ef7e-57de-a035-c8b3afe9f3
7-Zip-Zstandard
Alcor
AMD
Apple Inc.
ASUS
Atheros
BowPad
Classes
Clients
Conexant
CVSM

Name	Type	Data
(Default)	REG_SZ	(value not set)

Locations:

- <u>Wireless Evidences:</u>
  Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

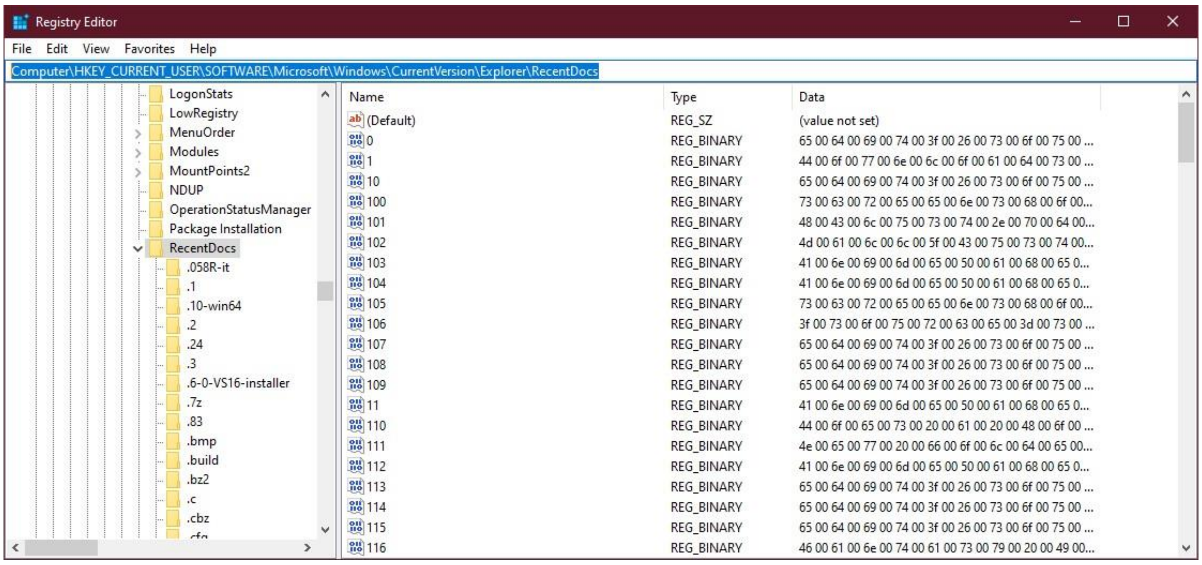
MCI Extensions
MCI32
MiniDumpAuxiliaryDlls
MsiCorruptedFileRecovery
Multimedia
NaAuth
NetworkCards
NetworkList
DefaultMediaCost
FirewallSync
NewNetworks
Nla
Permissions
Profiles
Signatures
NolmeModelmes
Notifications
NowPlayingSessionManager
NtVdm64
OEM
OpenGLDrivers
PeerNet
Perflib

Name	Type	Data
(Default)	REG_SZ	(value not set)

-

Recent Documents key:

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



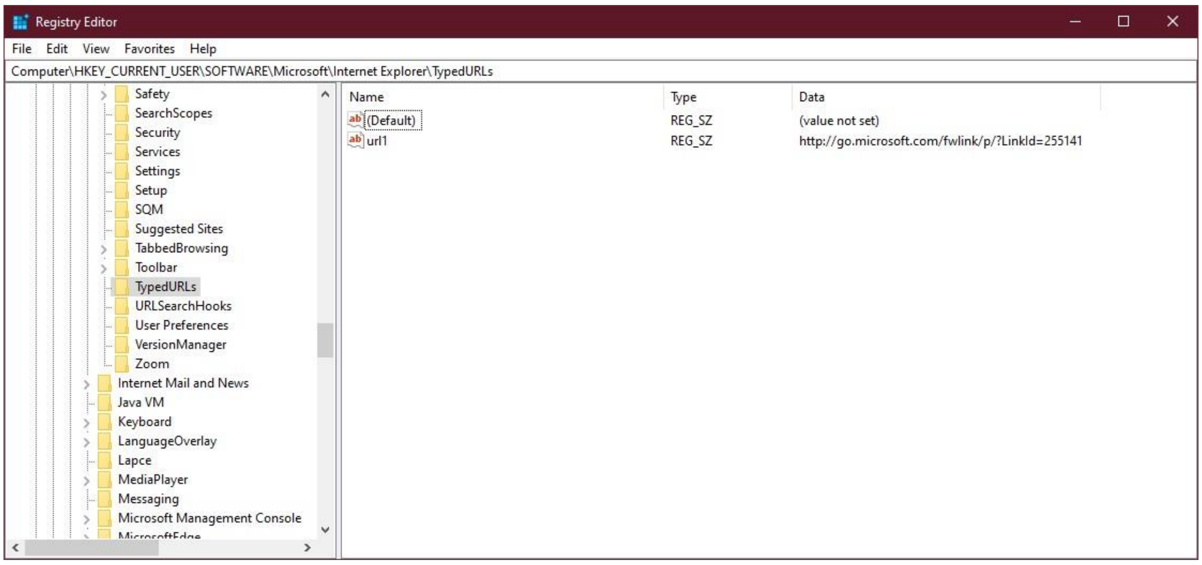
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
1	REG_BINARY	44 00 6f 00 77 00 6e 00 6c 00 6f 00 61 00 64 00 73 00 ...
10	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
100	REG_BINARY	73 00 63 00 72 00 65 00 65 00 6e 00 73 00 68 00 6f 00...
101	REG_BINARY	48 00 43 00 6c 00 75 00 73 00 74 00 2e 00 70 00 64 00...
102	REG_BINARY	4d 00 61 00 6c 00 6c 00 5f 00 43 00 75 00 73 00 74 00...
103	REG_BINARY	41 00 6e 00 69 00 6d 00 65 00 50 00 61 00 68 00 65 0...
104	REG_BINARY	41 00 6e 00 69 00 6d 00 65 00 50 00 61 00 68 00 65 0...
105	REG_BINARY	73 00 63 00 72 00 65 00 65 00 6e 00 73 00 68 00 6f 00...
106	REG_BINARY	3f 00 73 00 6f 00 75 00 72 00 63 00 65 00 3d 00 73 00 ...
107	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
108	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
109	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
11	REG_BINARY	41 00 6e 00 69 00 6d 00 65 00 50 00 61 00 68 00 65 0...
110	REG_BINARY	44 00 6f 00 65 00 73 00 20 00 61 00 20 00 48 00 6f 00 ...
111	REG_BINARY	4e 00 65 00 77 00 20 00 66 00 6f 00 6c 00 64 00 65 00...
112	REG_BINARY	41 00 6e 00 69 00 6d 00 65 00 50 00 61 00 68 00 65 0...
113	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
114	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
115	REG_BINARY	65 00 64 00 69 00 74 00 3f 00 26 00 73 00 6f 00 75 00 ...
116	REG_BINARY	46 00 61 00 6e 00 74 00 61 00 73 00 79 00 20 00 49 00...

- **Typed URLs key:**

  Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TypedURLs

•

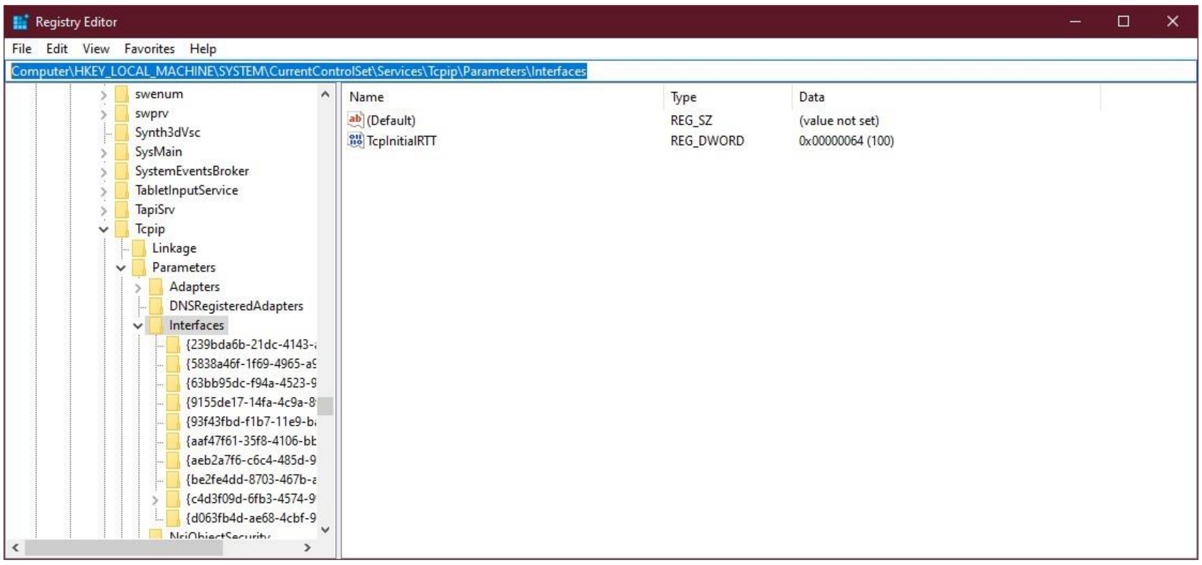

Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TypedURLs

Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

<u>IP address:</u> Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces


Registry Editor

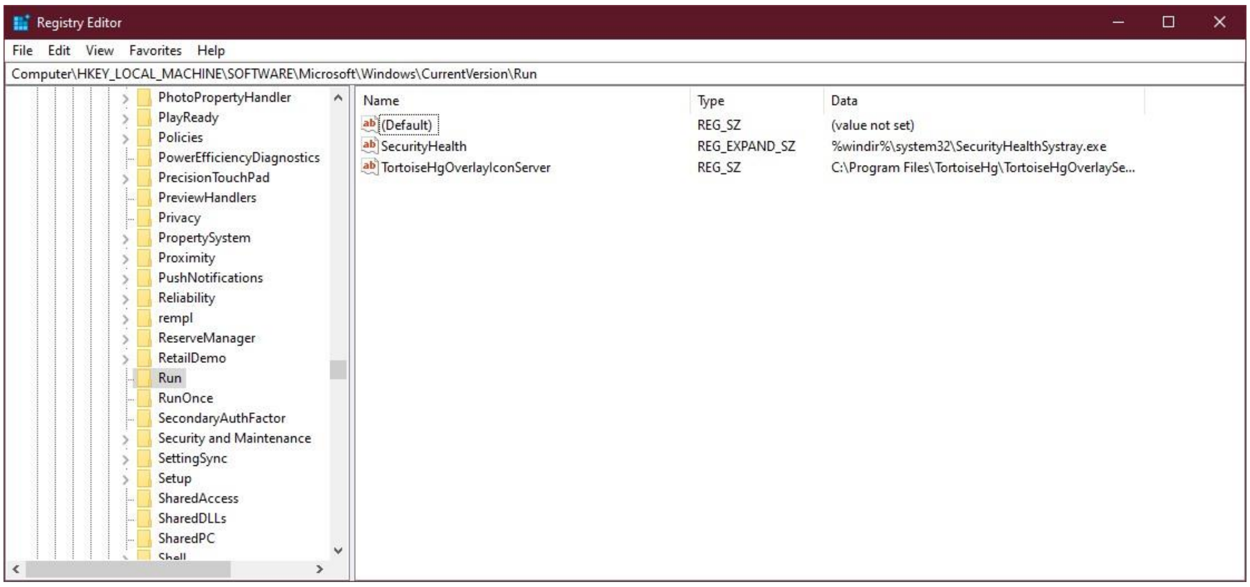
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

Name	Type	Data
(Default)	REG_SZ	(value not set)
TcpInitialRTT	REG_DWORD	0x00000064 (100)

-

- Startup applications:
  `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

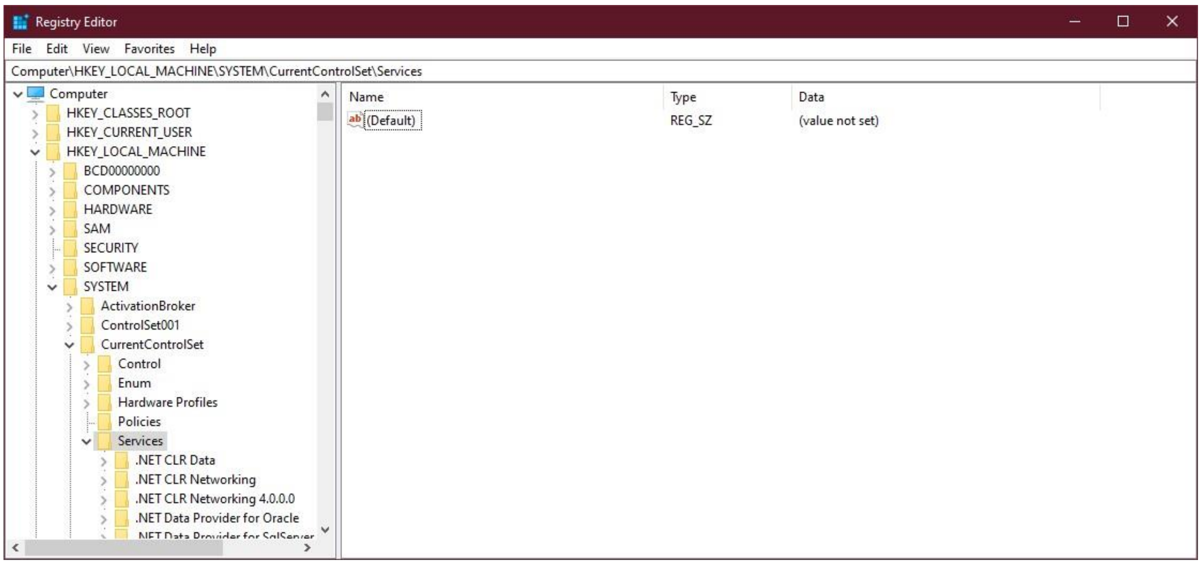

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
TortoiseHgOverlayIconServer	REG_SZ	C:\Program Files\TortoiseHg\TortoiseHgOverlaySe...

Startup services: `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`


Registry Editor

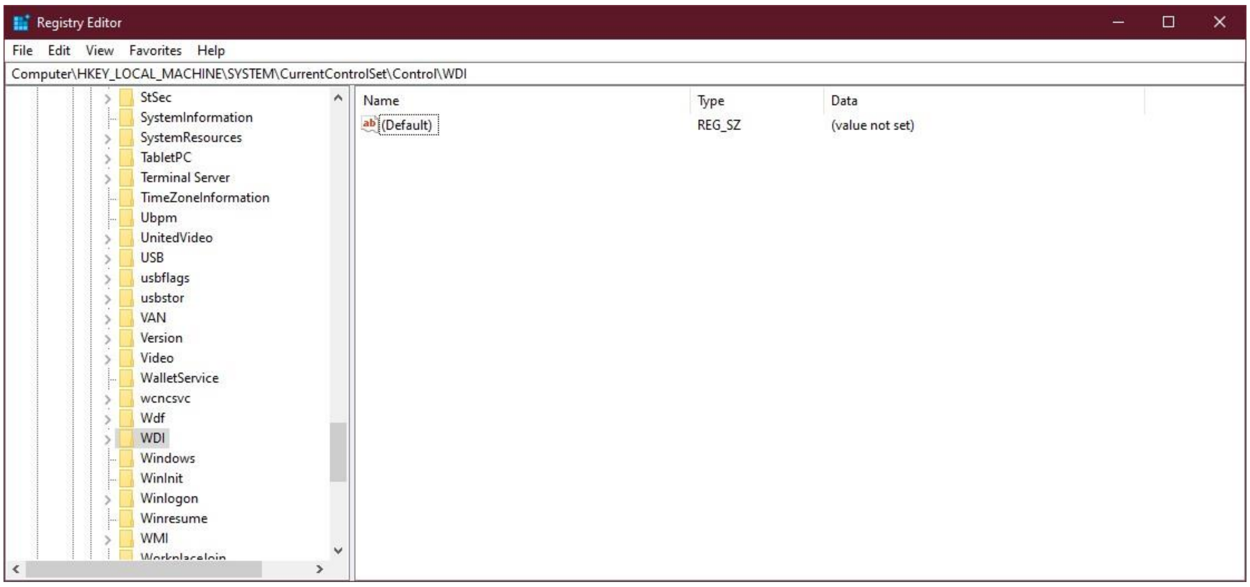
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Name	Type	Data
(Default)	REG_SZ	(value not set)

-

- <u>Start legacy applications:</u>
  `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI`


Registry Editor

File Edit View Favorites Help

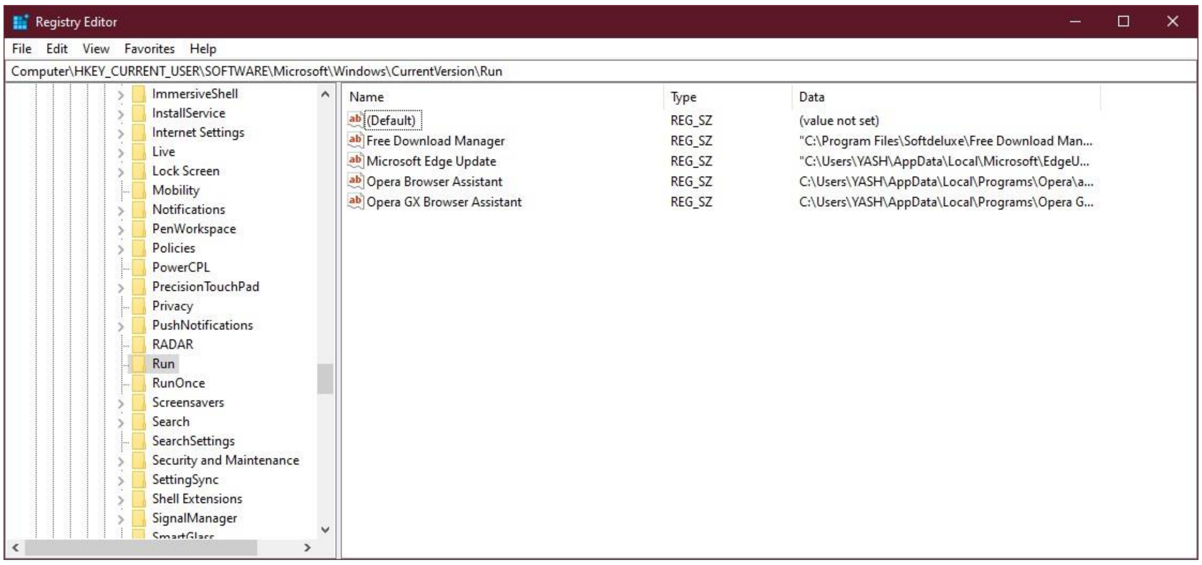
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI

StSec
SystemInformation
SystemResources
TabletPC
Terminal Server
TimeZoneInformation
Ubpm
UnitedVideo
USB
usbflags
usbstor
VAN
Version
Video
WalletService
wcncsvc
Wdf
WDI
Windows
WinInit
Winlogon
Winresume
WMI
Workplacejoin

Name	Type	Data
(Default)	REG_SZ	(value not set)

<u>Startup application(s) when a particular user logs in:</u> `Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run`

•



Registry Editor

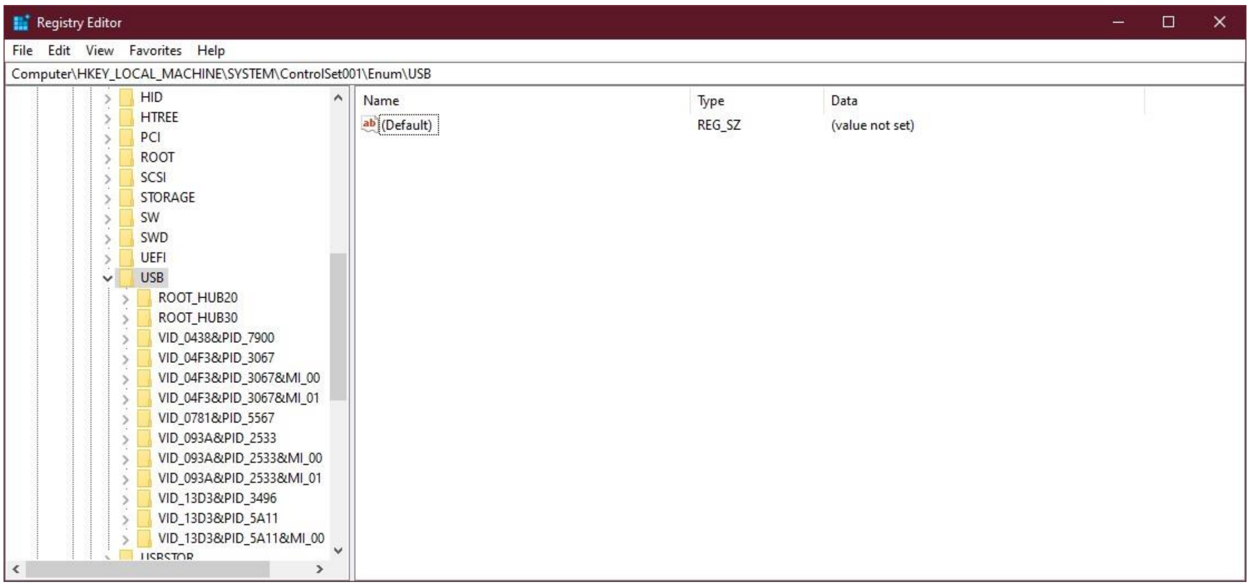
File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

ImmersiveShell
InstallService
Internet Settings
Live
Lock Screen
Mobility
Notifications
PenWorkspace
Policies
PowerCPL
PrecisionTouchPad
Privacy
PushNotifications
RADAR
Run
RunOnce
Screensavers
Search
SearchSettings
Security and Maintenance
SettingSync
Shell Extensions
SignalManager

Name	Type	Data
(Default)	REG_SZ	(value not set)
Free Download Manager	REG_SZ	"C:\Program Files\Softdeluxe\Free Download Man...
Microsoft Edge Update	REG_SZ	"C:\Users\YASH\AppData\Local\Microsoft\EdgeU...
Opera Browser Assistant	REG_SZ	C:\Users\YASH\AppData\Local\Programs\Opera\a...
Opera GX Browser Assistant	REG_SZ	C:\Users\YASH\AppData\Local\Programs\Opera G...

- <u>USB drives:</u>
  Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\ Enum\USB



Registry Editor

File Edit View Favorites Help

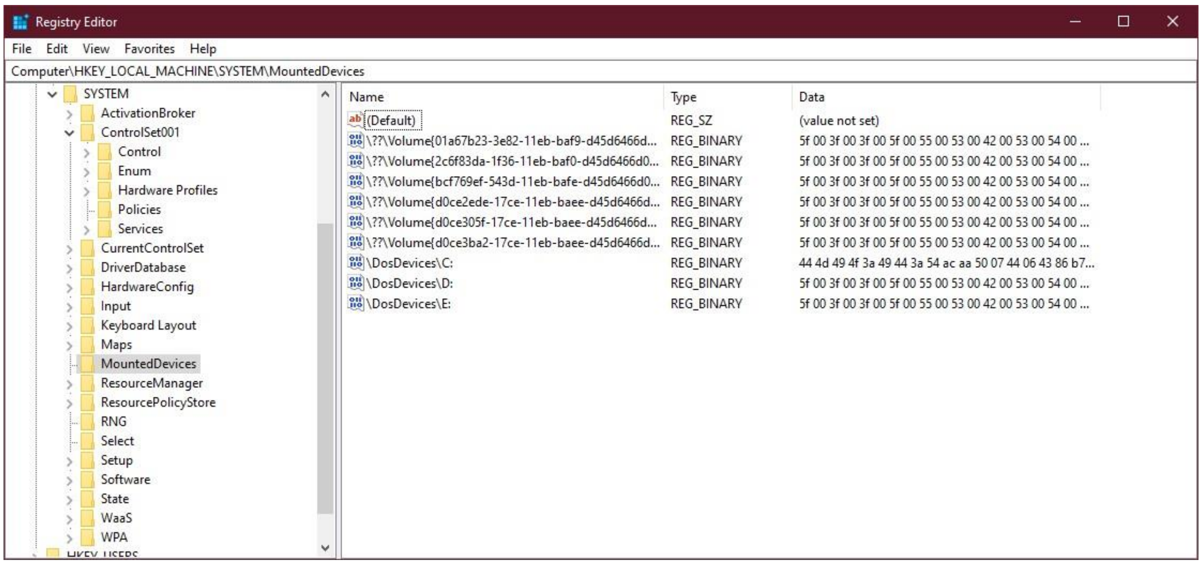
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB

HID
HTREE
PCI
ROOT
SCSI
STORAGE
SW
SWD
UEFI
USB
ROOT_HUB20
ROOT_HUB30
VID_0438&PID_7900
VID_04F3&PID_3067
VID_04F3&PID_3067&MI_00
VID_04F3&PID_3067&MI_01
VID_0781&PID_5567
VID_093A&PID_2533
VID_093A&PID_2533&MI_00
VID_093A&PID_2533&MI_01
VID_13D3&PID_3496
VID_13D3&PID_5A11
VID_13D3&PID_5A11&MI_00

Name	Type	Data
(Default)	REG_SZ	(value not set)

•

Mounted devices: Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices



Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{01a67b23-3e82-11eb-baf9-d45d6466d...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{2c6f83da-1f36-11eb-baf0-d45d6466d0...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{bcf769ef-543d-11eb-bafe-d45d6466d0...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{d0ce2ede-17ce-11eb-baee-d45d6466d...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{d0ce305f-17ce-11eb-baee-d45d6466d...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{d0ce3ba2-17ce-11eb-baee-d45d6466d...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\DosDevices\C:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 54 ac aa 50 07 44 06 43 86 b7...
\DosDevices\D:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\DosDevices\E:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...