Practical 1

Aim:- Create a java application to send encrypted message from sender and decrypt an message at receiver end.

Code:-

Sender.java

```
package cflprac1;

import java.io.*;

import java.util.*;

import java.net.*;


public class Sender {

   public static void main(String[] args) throws Exception

{

   String s="";

   String ct="";

   String key="";

   Socket sc=new Socket("localhost",6017);

   Random r=new Random();

   int i=0,k=0;

   System.out.println("Enter the string");

   BufferedReader br= new BufferedReader(new InputStreamReader(System.in));

   BufferedWriter bw=new BufferedWriter(new
OutputStreamWriter(sc.getOutputStream()));

   s=br.readLine();

   int j[]=new int[s.length()];

   for(i=0;i<s.length();i++)

   {

      j[k]=r.nextInt(50);
```

```
        key+=Integer.valueOf(j[k])+",";
        System.out.println("j="+j[k]);
        ct+=(char)(s.charAt(i)+j[k]);
        k++;
    }
    System.out.println("Key="+key);
    System.out.println("Encrypted message: "+ct);
    bw.write(ct+","+key);
    bw.flush();
    bw.close();
}
}
```

Receiver.java

```
package cflprac1;
import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.IOException;
import java.io.InputStreamReader;
import java.io.OutputStreamWriter;
import java.net.*;
import java.util.Random;

public class Receiver {
    public static void main(String[] args) throws Exception
{
    String ct="";
    String pt="";
    ServerSocket skt=new ServerSocket(6017);
    Socket sc=skt.accept();
```

```
    Random r=new Random();
    int i=0,k=0;
    System.out.println("Enter the string");
    BufferedReader br= new BufferedReader(new InputStreamReader(sc.getInputStream()));
    ct=br.readLine();
    String[] s=new String[ct.length()];
    s=ct.split(",");
    int[] j=new int[s[0].length()];
    System.out.println(" message"+s[0]);
    for(i=0;i<s[0].length();i++)
    {
        j[i]=Integer.parseInt(s[i+1]);
        System.out.println(" key="+j[i]);
    }
    for(i=0;i<s[0].length();i++)
    {
        System.out.println("j="+j[i]);
        pt+=(char)(s[0].charAt(i)-j[i]);
    }
    System.out.println(" message from Sender: "+pt);
    }

}
```

Output:-

Sender.java

```
Output
cflprac1 (run)   cflprac1 (run) #2
run:
Enter the string
This is CFL Practical 1
j=44
j=28
j=43
j=0
j=34
j=43
j=39
j=22
j=0
j=46
j=39
j=46
j=32
j=46
j=7
j=16
j=5
j=46
j=11
j=35
j=40
j=29
j=3
Key=44,28,43,0,34,43,39,22,0,46,39,46,32,46,7,16,5,46,11,35,40,29,3,
Encrypted message: □□□sB□□6CtsNp hsy□n□□=4
BUILD SUCCESSFUL (total time: 12 seconds)
```

Receiver.java

```
cflprac1 (run)   cflprac1 (run) #2
run:
Enter the string
 message□□□sB□□6CtsNp hsy□n□□=4
 key=44
 key=28
 key=43
 key=0
 key=34
 key=43
 key=39
 key=22
 key=0
 key=46
 key=39
 key=46
 key=32
 key=46
 key=7
 key=16
 key=5
 key=46
 key=11
 key=35
 key=40
 key=29
 key=3
j=44
j=28
j=43
j=0
j=34
j=43
j=39
j=22
```

```
j=0
j=46
j=39
j=46
j=32
j=46
j=7
j=16
j=5
j=46
j=11
j=35
j=40
j=29
j=3
 message from Sender: This is CFL Practical 1
BUILD SUCCESSFUL (total time: 17 seconds)
```

1:1/21:614

Practical 2

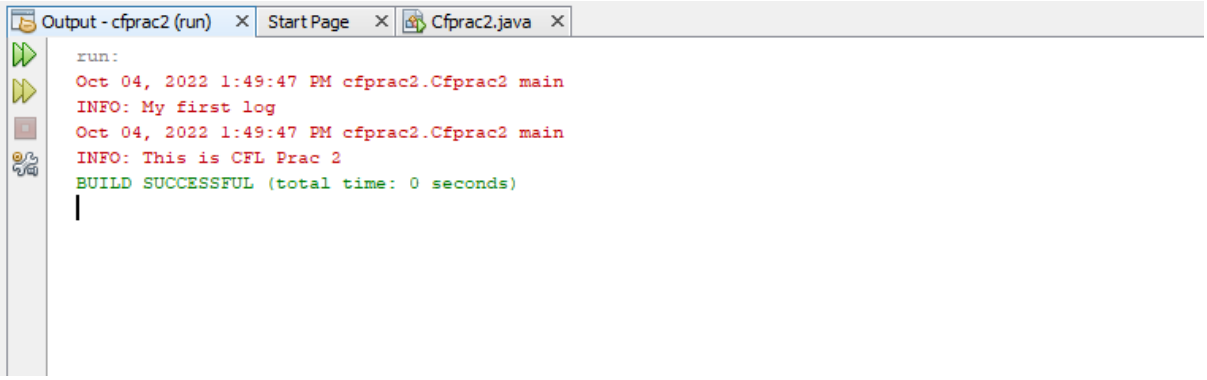
Aim:- Java program for creating log files.

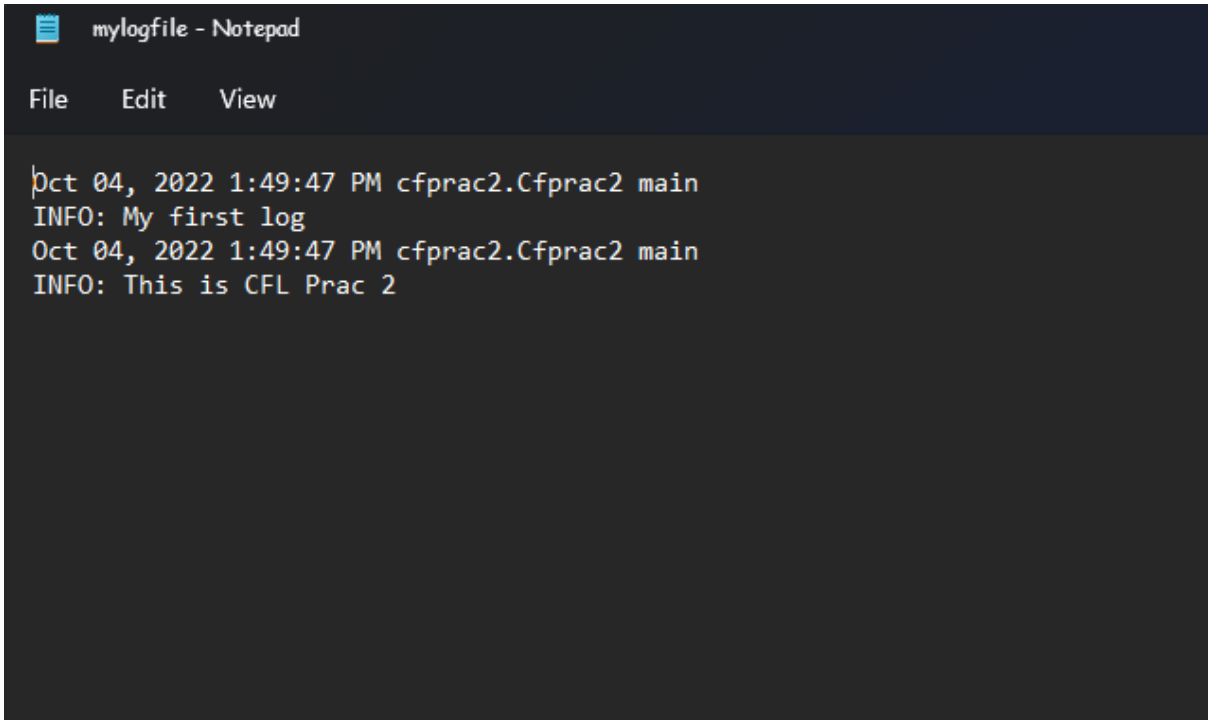
Code:-

```
package cfprac2;

import java.io.*;

import java.util.logging.*;


public class Cfprac2 {


   public static void main(String[] args) {

     Logger l=Logger.getLogger(Cfprac2.class.getName());

                    FileHandler fh;

                   try

              {

                    fh=new FileHandler("D:/mylogfile.log",true);

                    l.addHandler(fh);

                    l.setLevel(Level.ALL);

                     SimpleFormatter sf=new SimpleFormatter();

                   fh.setFormatter(sf);

                    l.info("My first log");

              }

          catch(SecurityException e)
```

```
            {
                    e.printStackTrace();
            }
        catch(IOException e)
            {
                    e.printStackTrace();
            }
            l.info("This is CFL Prac 2");

    }

}
```

Output:-





Practical 3

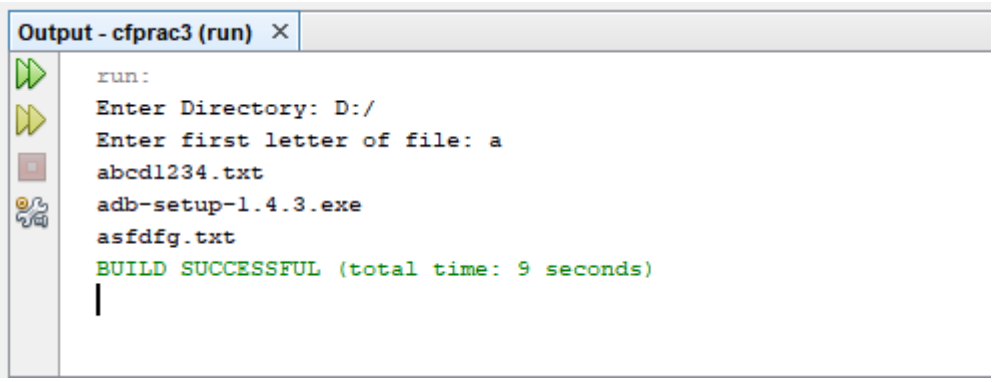
Aim:- Java program for searching file in given directory.

Code:-

```
package cfprac3;

import java.io.*;

import java.util.*;

public class Cfprac3 {

   public static void main(String[] args) {

      Scanner sc= new Scanner(System.in);

      System.out.print("Enter Directory: ");

      String str1= sc.nextLine();//System.in is a standard input stream

      File dir = new File(str1);

      System.out.print("Enter first letter of file: ");

      String str2= sc.nextLine();

      FilenameFilter filter = new FilenameFilter() {

       public boolean accept (File dir, String name) {

         return name.startsWith(str2);
```

```
        }
      };
      String[] children = dir.list(filter);
      if (children == null) {
        System.out.println("Either dir does not exist or is not a directory");
      } else {
        for (int i = 0; i< children.length; i++) {
          String filename = children[i];
          System.out.println(filename);
        }
      }
    }

}
```

Output:-



Practical 4

Aim:-Write a java application to search a particular word in a file.

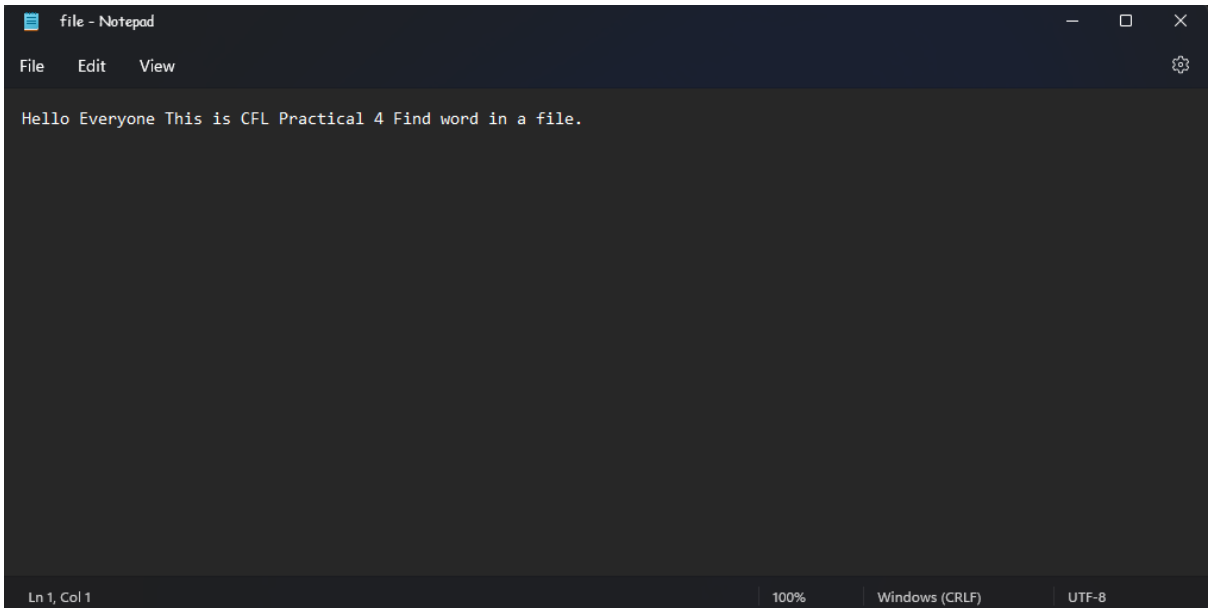
Code:-

```
package cfprac4;
import java.io.BufferedReader;
import java.io.FileReader;
import java.io.InputStreamReader;
```

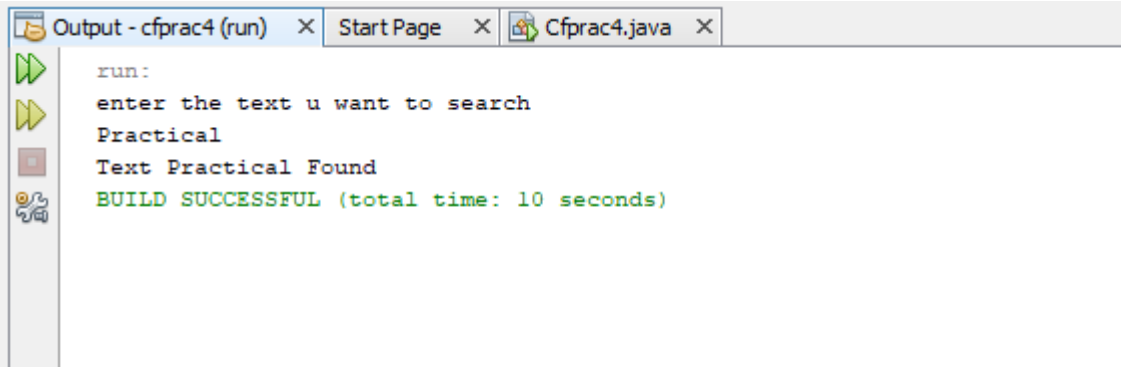
```
public class Cfprac4 {



   public static void main(String[] args) {
      try
{
String str="";
String ser="";
int flag=0;
BufferedReader br=new BufferedReader(new FileReader("D:\\file.txt"));
BufferedReader br1=new BufferedReader(new InputStreamReader(System.in));
str=br.readLine();
String [] s = new String[str.length()];
System.out.println("enter the text u want to search");
ser=br1.readLine();
s=str.split(" ");
for(int i=0;i<s.length;i++)
{
if(ser.equalsIgnoreCase(s[i]))
{
System.out.println("Text "+ser+" Found");
flag=1;
}
}
if(flag==0)
System.out.println("Text "+ser+" Not Found");
}
catch(Exception e)
```

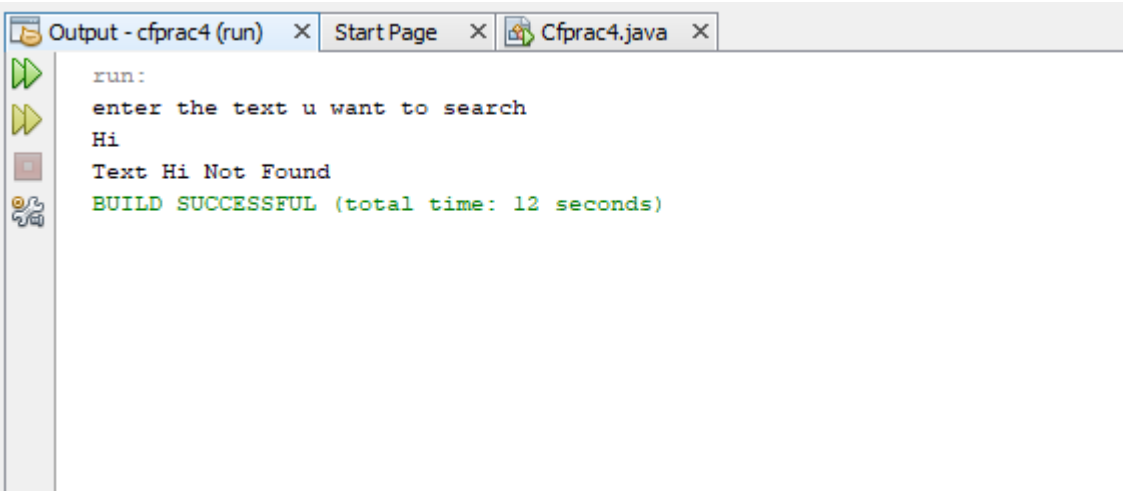
```
{
System.out.println(e);
}

    }

}
```

File.txt



Output:-





Practical 5

Aim:- Use DriveImage XML to image a hard drive.

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.

DiX Welcome
Backup
Restore
Drive to Drive
Browse

Check one or more drives to backup:

Drive	Label	Type	Capacity	% used	Physical drive
C:		NTFS	244 GB	17	DISK0#2
D:		NTFS	117 GB	0	DISK0#3
E:		NTFS	164 GB	0	DISK0#4
G:	System Reserved	NTFS	100.0 MB	28	DISK0#1

Drive details:

Logical Information		Physical Information	
Drive:	D:	Drive:	DISK0
Label:		Drive name:	ST500DM002-1BD142
File system:	NTFS	Total sectors:	976,773,168
Total sectors:	245,759,992		
		Partition:	#3
Used bytes:	97,959,936 (93 MB)	Start sector on drive:	512,002,048
Free bytes:	125,731,155,968 (117 GB)	Sectors in partition:	245,760,000
Total bytes:	125,829,115,904 (117 GB)		

Next

Memory in use: 768,448

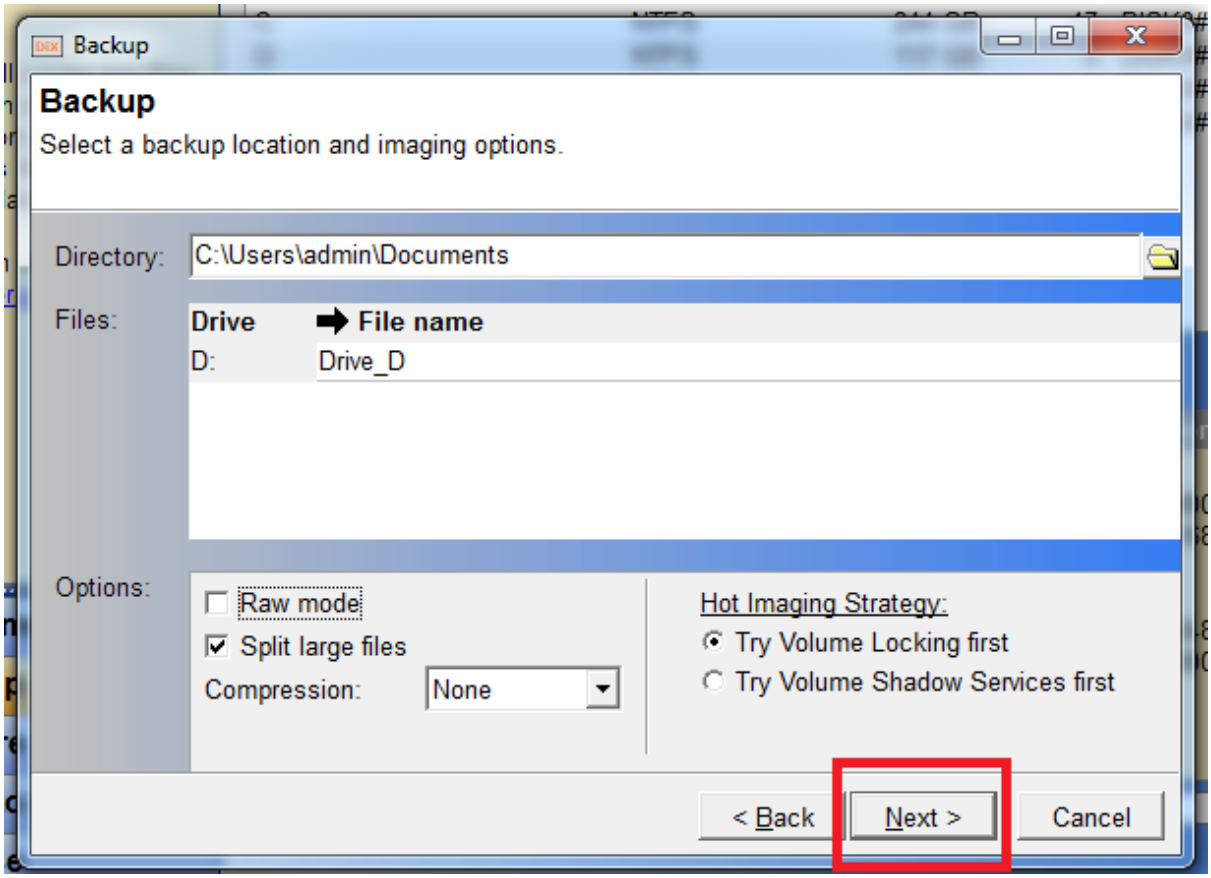
Backup

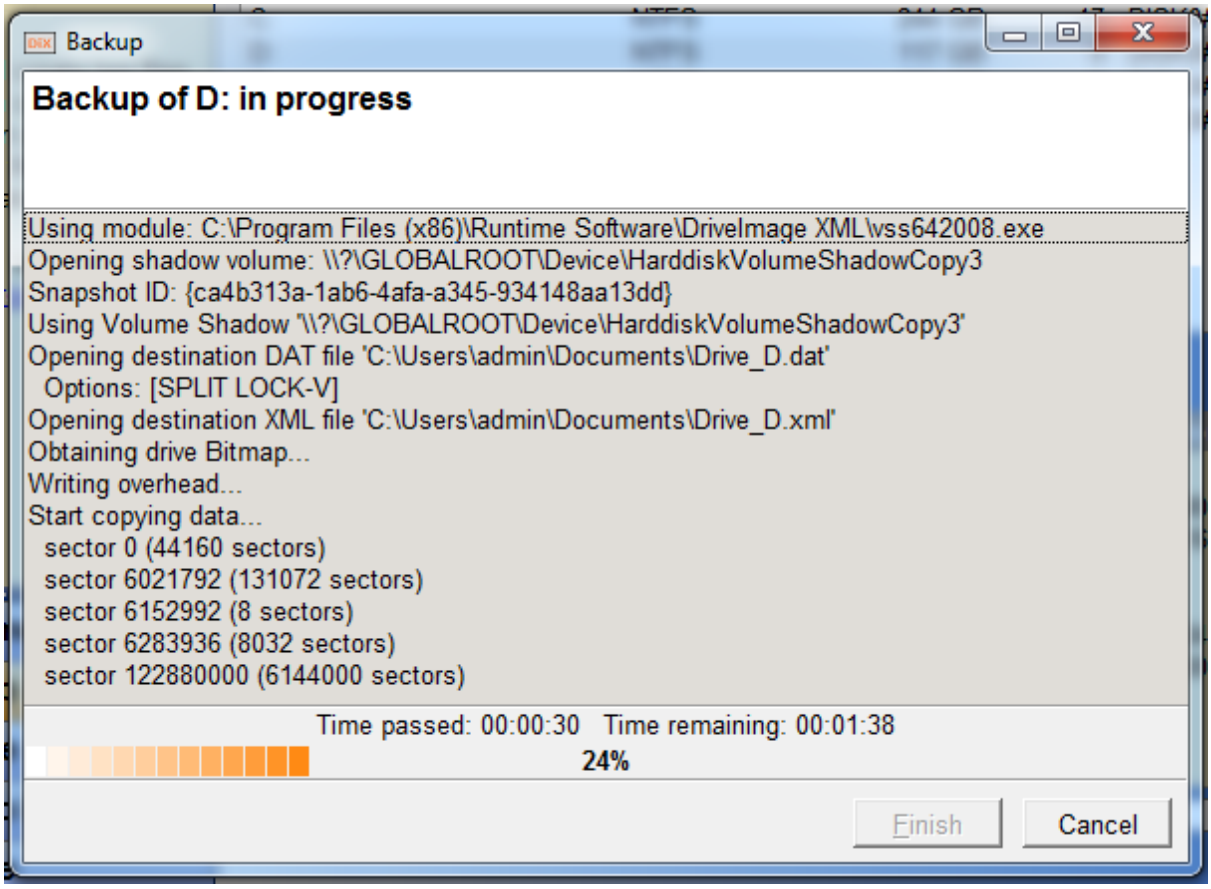
Welcome to the drive backup wizard!

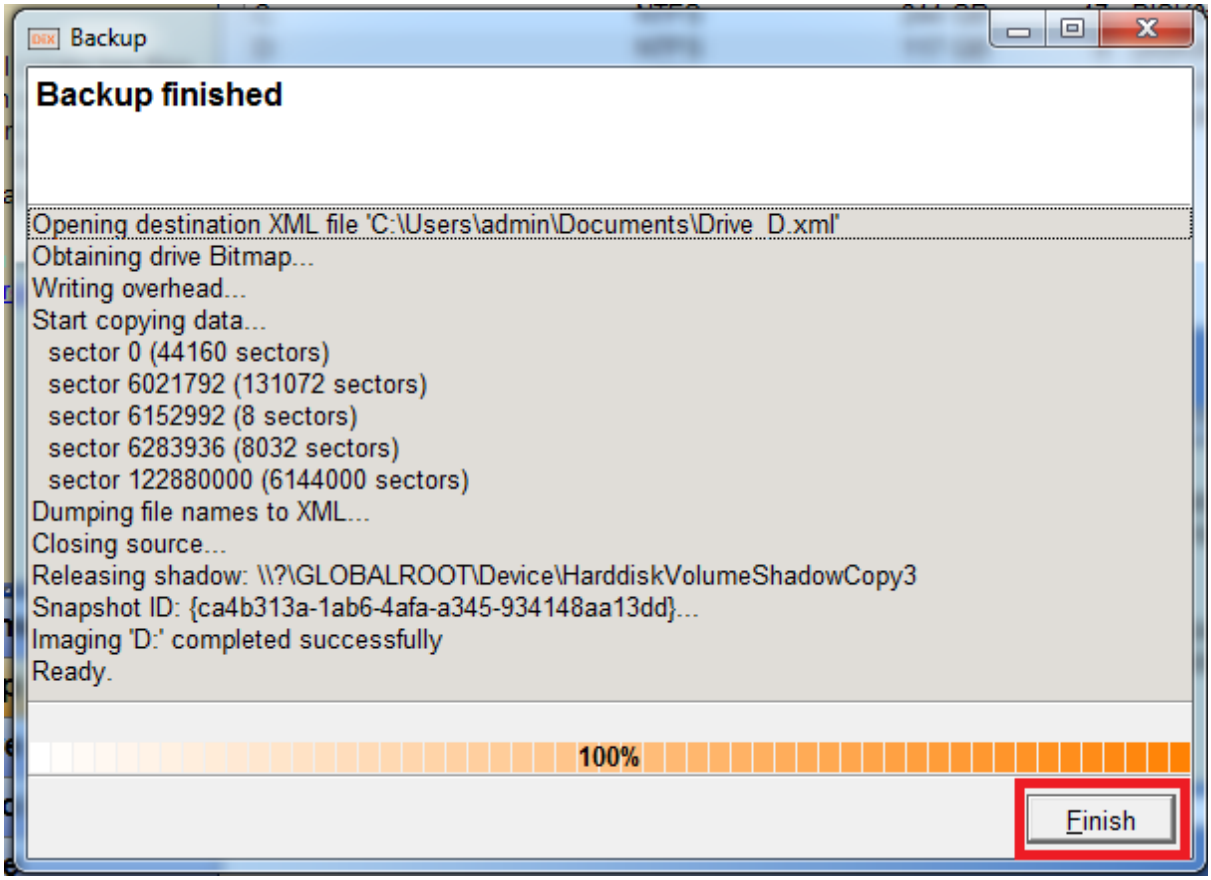
This wizard will assist you with backing up your drives:

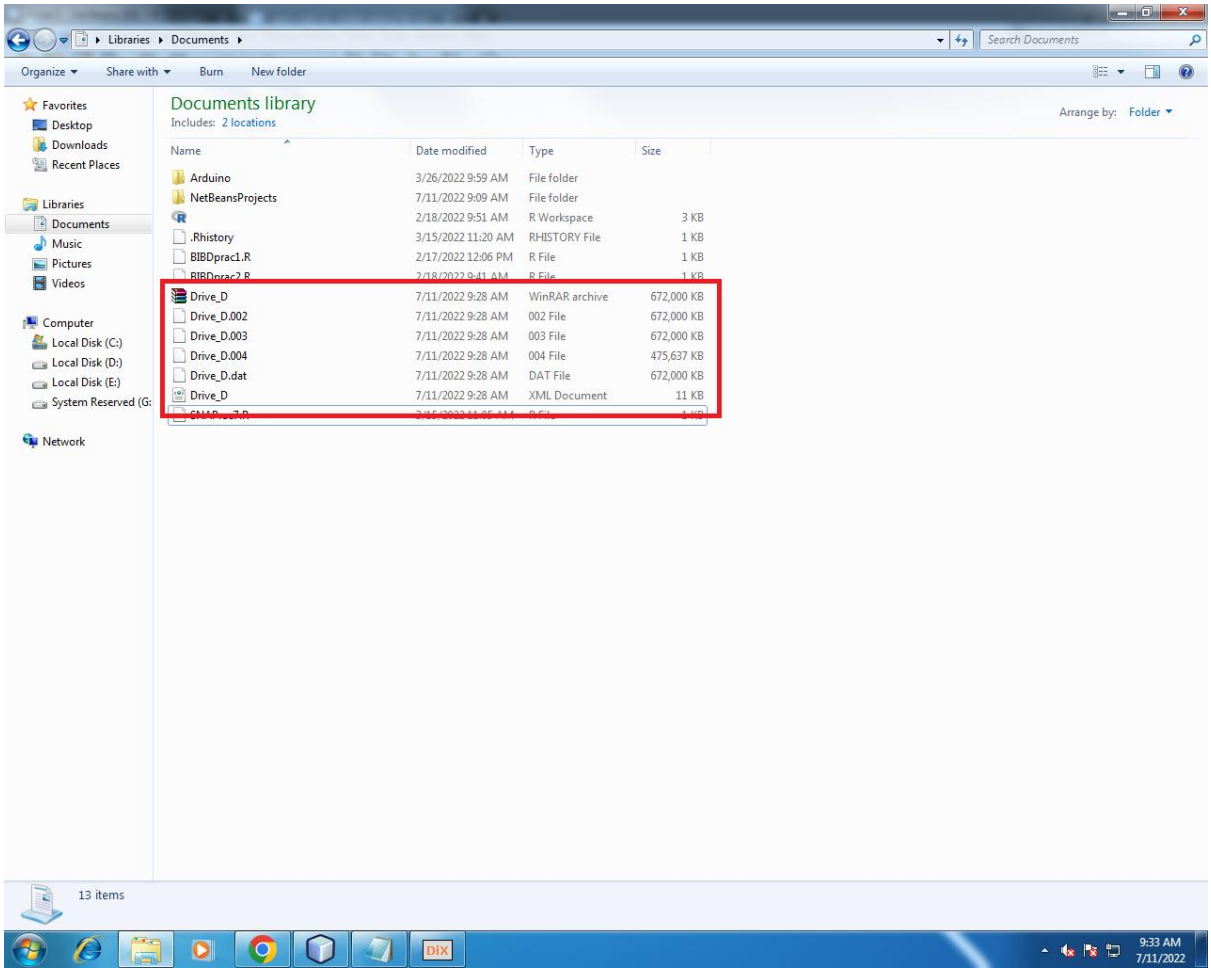
Drive	Label	Type	Capacity	% used	Physic...
D:		NTFS	117 GB	0	DISK0#3

Next > Cancel


Backup
Backup
Select a backup location and imaging options.
Directory:
C:\Users\admin\Documents
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
< Back
Next >
Cancel


Backup
Backup of D: in progress
Using module: C:\Program Files (x86)\Runtime Software\DriveImage XML\vss642008.exe
Opening shadow volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
Snapshot ID: {ca4b313a-1ab6-4afa-a345-934148aa13dd}
Using Volume Shadow '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3'
Opening destination DAT file 'C:\Users\admin\Documents\Drive_D.dat'
Options: [SPLIT LOCK-V]
Opening destination XML file 'C:\Users\admin\Documents\Drive_D.xml'
Obtaining drive Bitmap...
Writing overhead...
Start copying data...
sector 0 (44160 sectors)
sector 6021792 (131072 sectors)
sector 6152992 (8 sectors)
sector 6283936 (8032 sectors)
sector 122880000 (6144000 sectors)
Time passed: 00:00:30 Time remaining: 00:01:38
24%
Finish
Cancel


Backup
Backup finished
Opening destination XML file 'C:\Users\admin\Documents\Drive_D.xml'
Obtaining drive Bitmap...
Writing overhead...
Start copying data...
sector 0 (44160 sectors)
sector 6021792 (131072 sectors)
sector 6152992 (8 sectors)
sector 6283936 (8032 sectors)
sector 122880000 (6144000 sectors)
Dumping file names to XML...
Closing source...
Releasing shadow: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
Snapshot ID: {ca4b313a-1ab6-4afa-a345-934148aa13dd}...
Imaging 'D:' completed successfully
Ready.
100%
Finish


Libraries ▸ Documents ▸
Search Documents
Organize
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Local Disk (E:)
System Reserved (G:
Network
Documents library
Includes: 2 locations
Arrange by: Folder
Name
Date modified
Type
Size
Arduino 3/26/2022 9:59 AM File folder
NetBeansProjects 7/11/2022 9:09 AM File folder
2/18/2022 9:51 AM R Workspace 3 KB
.Rhistory 3/15/2022 11:20 AM RHISTORY File 1 KB
BIBDprac1.R 2/17/2022 12:06 PM R File 1 KB
Drive_D 7/11/2022 9:28 AM WinRAR archive 672,000 KB
Drive_D.002 7/11/2022 9:28 AM 002 File 672,000 KB
Drive_D.003 7/11/2022 9:28 AM 003 File 672,000 KB
Drive_D.004 7/11/2022 9:28 AM 004 File 475,637 KB
Drive_D.dat 7/11/2022 9:28 AM DAT File 672,000 KB
Drive_D 7/11/2022 9:28 AM XML Document 11 KB
13 items
9:33 AM
7/11/2022

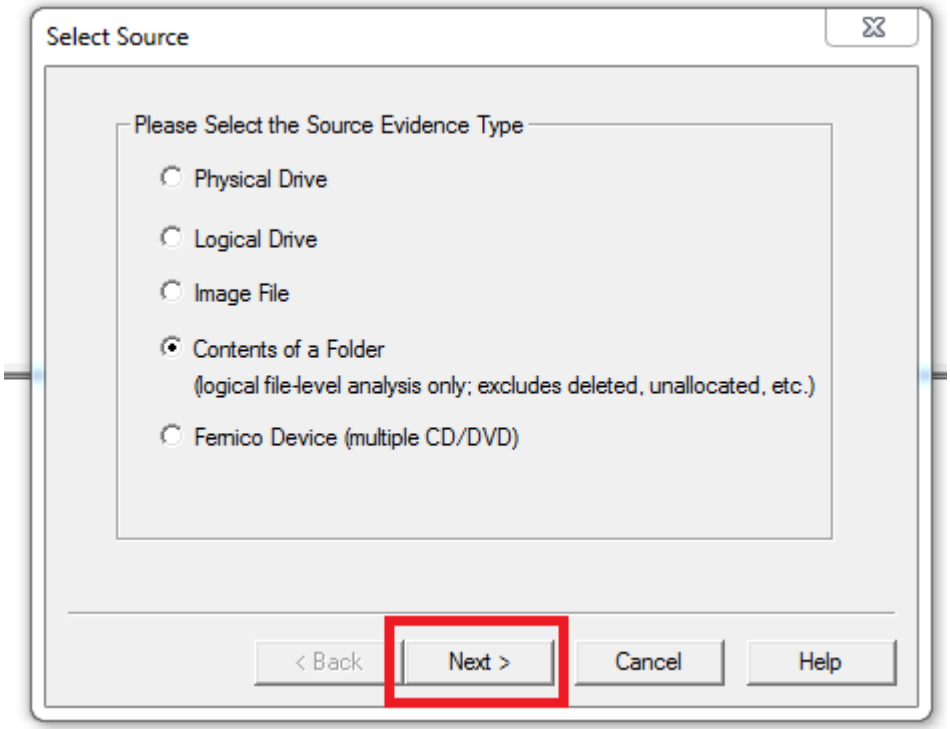
Practical 6

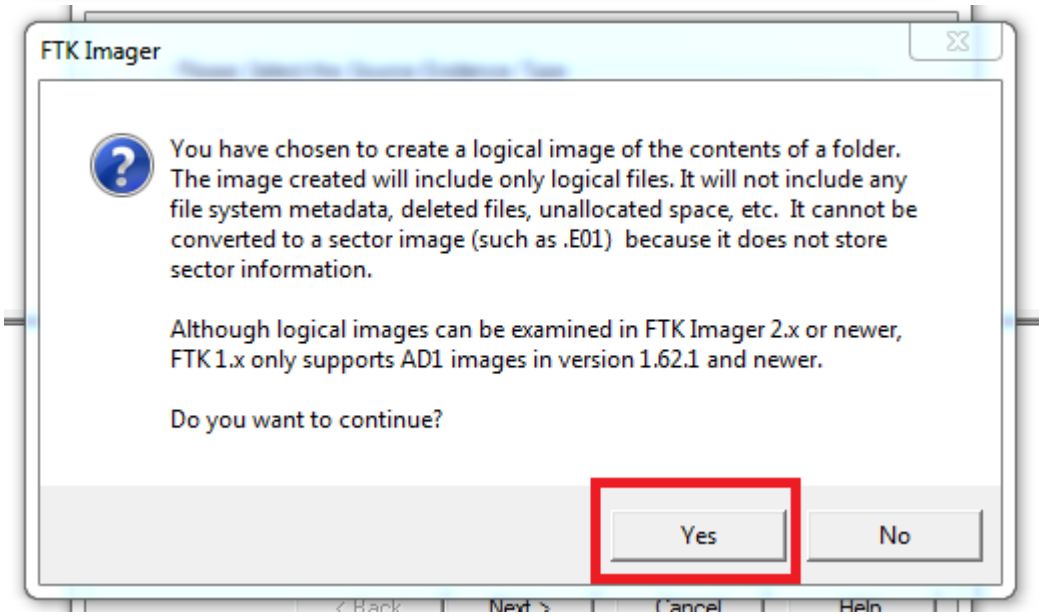
Aim:- Create forensic images of digital devices from volatile data such as memory using imager for computer system.

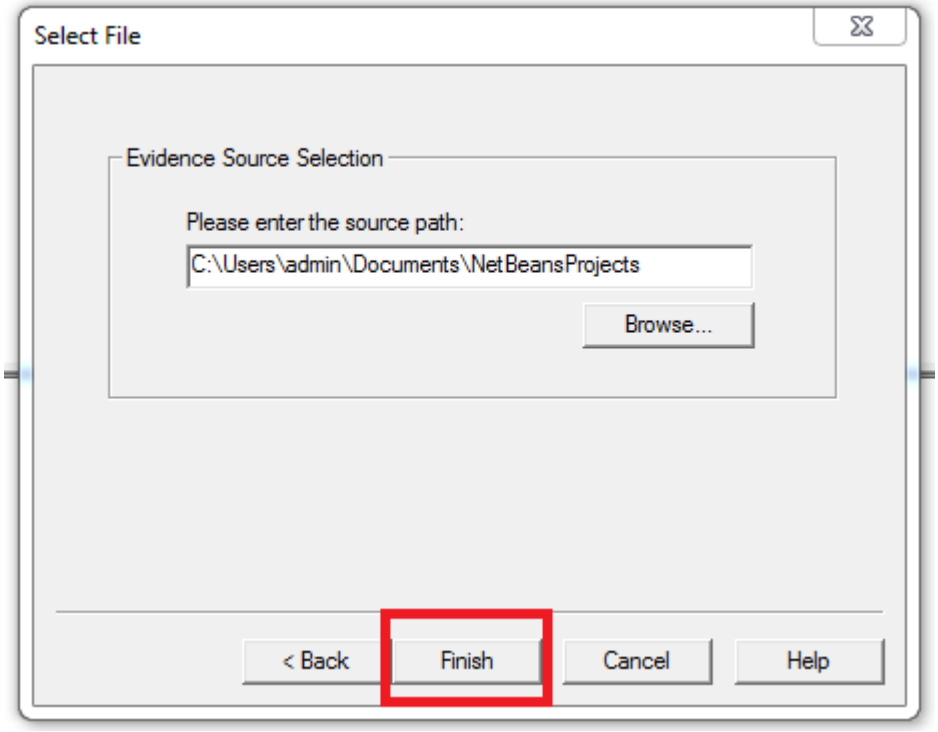
"Create forensic images of digital devices from volatile data such as memory using imager for computer system."

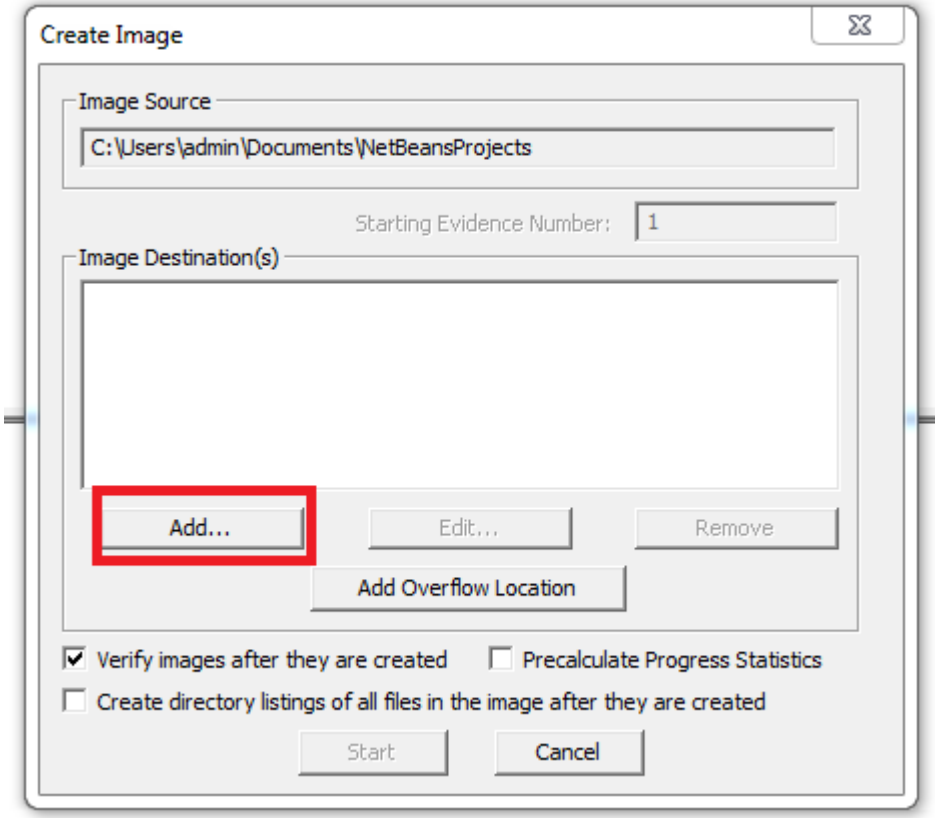
1. **Create forensic images**: In digital forensics, creating a forensic image means making an exact, bit-for-bit copy of data from a digital device. This process ensures that the original data remains unchanged while allowing forensic experts to analyze the copied data for investigation purposes.
2. **Of digital devices**: This refers to any electronic device that stores data, such as computers, smartphones, tablets, etc.
3. **From volatile data**: Volatile data refers to information that is lost when the power is turned off or the device is rebooted. In digital forensics, volatile data typically means the data held in a device's RAM (Random Access Memory) because it gets erased when the device loses power.
4. **Such as memory**: Here, "memory" specifically refers to RAM. When investigating a computer system, capturing the contents of RAM is crucial because it can contain valuable information like running processes, open files, network connections, and other data that is lost once the computer is shut down or restarted.
5. **Using imager for computer system**: An imager is a specialized tool or software used to create a forensic image of a digital device. In the context of volatile data, the imager is used to capture and save the contents of the device's memory (RAM) before it is lost.

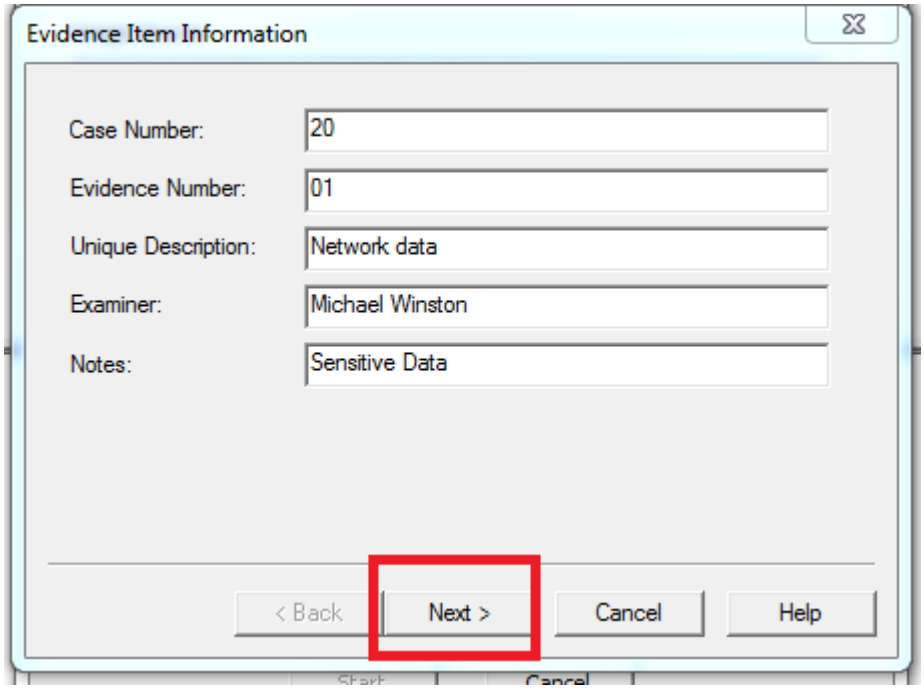
Putting it all together: The sentence is instructing someone to use a specialized tool (an imager) to create an exact copy of the data from the RAM of a computer system. This process is done because RAM holds temporary and volatile information that is essential for forensic analysis, and capturing this data while the system is running (or immediately after) ensures that no crucial information is lost.

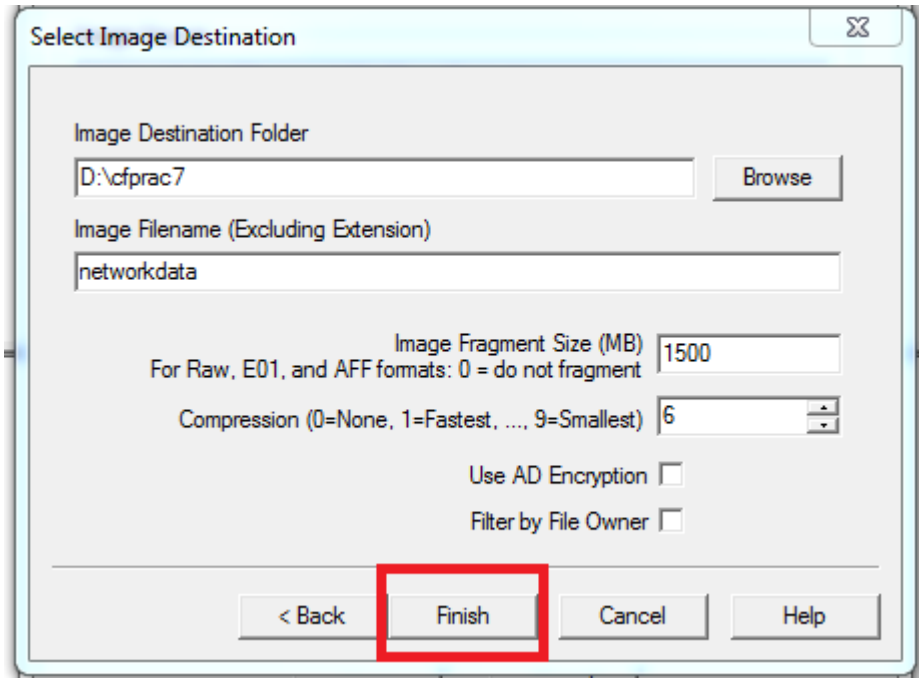


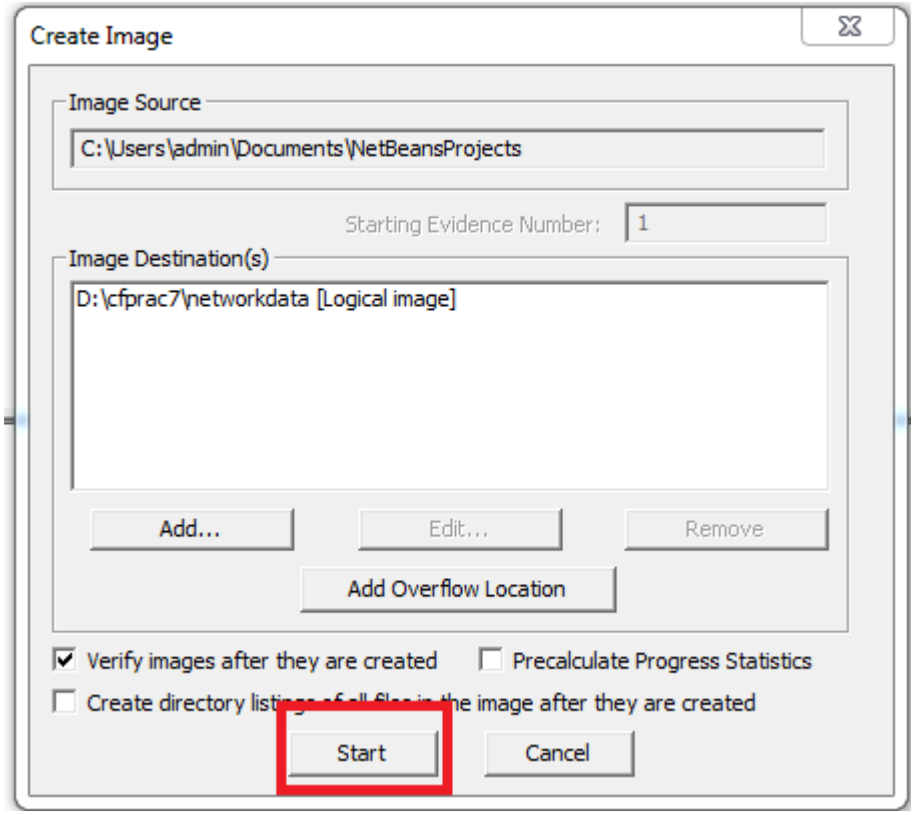


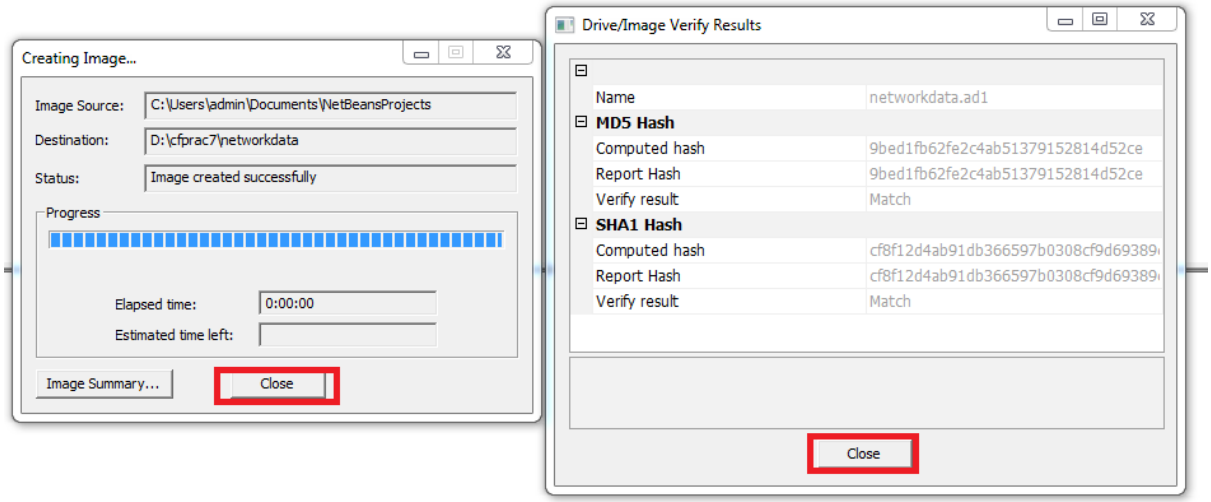

Select File
Evidence Source Selection
Please enter the source path:
C:\Users\admin\Documents\NetBeansProjects
Browse...
< Back
Finish
Cancel
Help

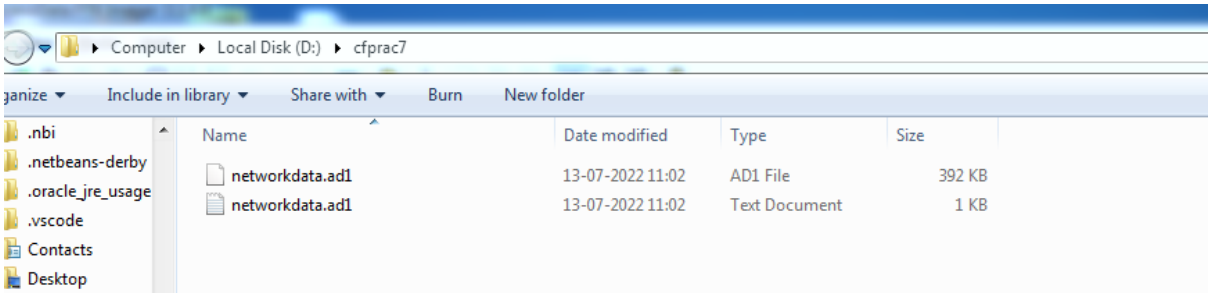

Create Image
Image Source
C:\Users\admin\Documents\NetBeansProjects
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel


Evidence Item Information
Case Number:
20
Evidence Number:
01
Unique Description:
Network data
Examiner:
Michael Winston
Notes:
Sensitive Data
< Back
Next >
Cancel
Help


Select Image Destination
Image Destination Folder
D:\cfprac7
Browse
Image Filename (Excluding Extension)
networkdata
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
< Back
Finish
Cancel
Help


Create Image
Image Source
C:\Users\admin\Documents\NetBeansProjects
Starting Evidence Number:
1
Image Destination(s)
D:\cfprac7\networkdata [Logical image]
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created
Start
Cancel

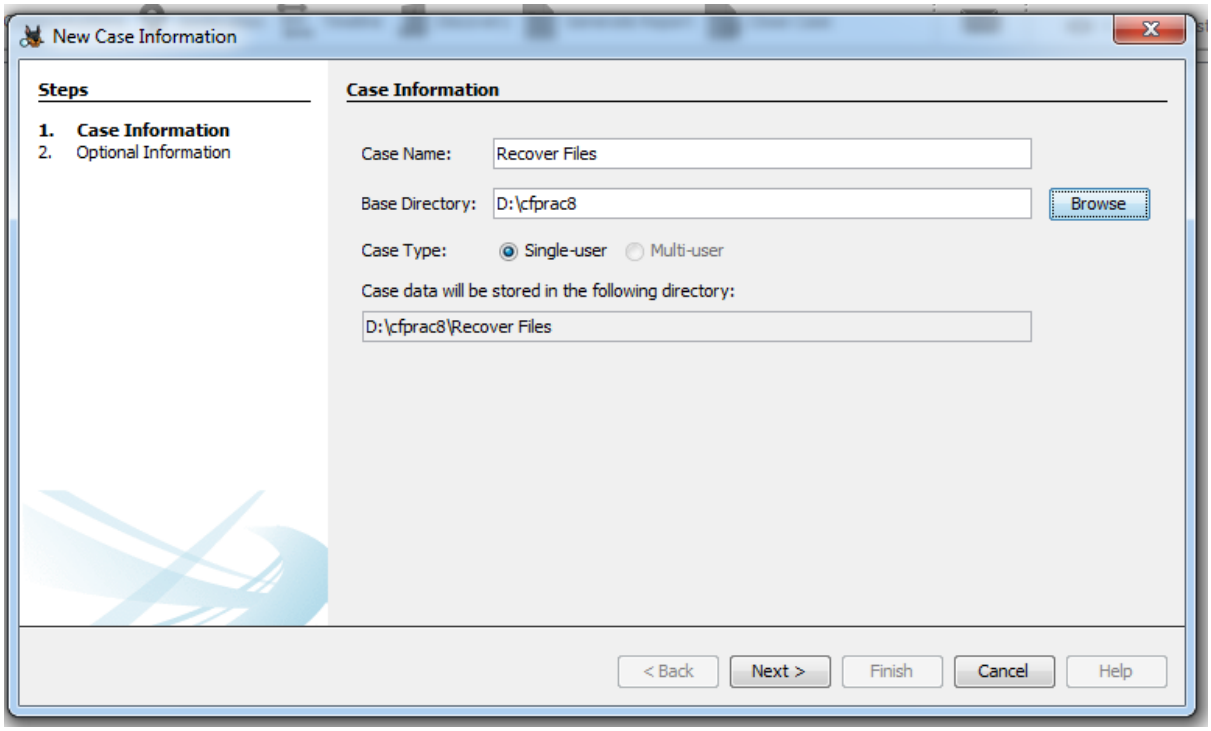

Creating Image...
Image Source:
C:\Users\admin\Documents\NetBeansProjects
Destination:
D:\cfprac7\networkdata
Status:
Image created successfully
Progress
Elapsed time:
0:00:00
Estimated time left:
Image Summary...
Close
Drive/Image Verify Results
Name
networkdata.ad1
MD5 Hash
Computed hash
9bed1fb62fe2c4ab51379152814d52ce
Report Hash
9bed1fb62fe2c4ab51379152814d52ce
Verify result
Match
SHA1 Hash
Computed hash
cf8f12d4ab91db366597b0308cf9d69389
Report Hash
cf8f12d4ab91db366597b0308cf9d69389
Verify result
Match
Close

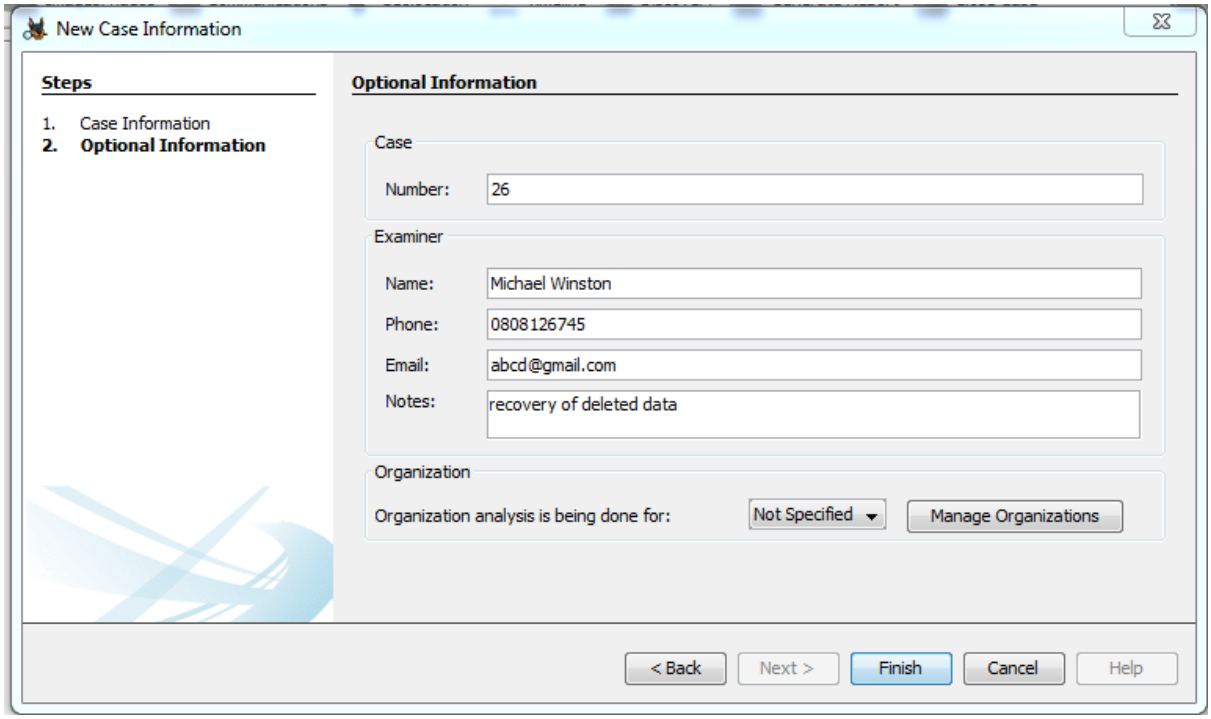

Computer
Local Disk (D:)
cfprac7
Include in library
Share with
Burn
New folder
.nbi
.netbeans-derby
.oracle_jre_usage
.vscode
Contacts
Desktop
Name
Date modified
Type
Size
networkdata.ad1
13-07-2022 11:02
AD1 File
392 KB
networkdata.ad1
13-07-2022 11:02
Text Document
1 KB

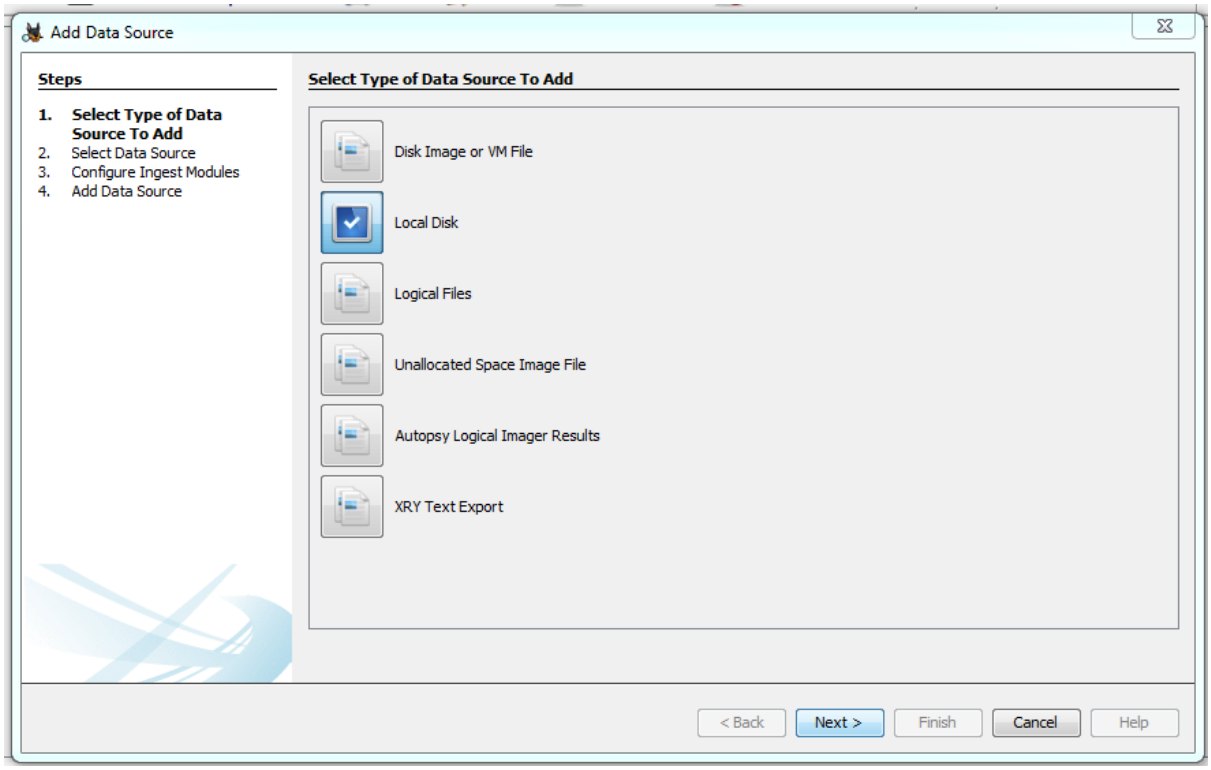
```
networkdata.ad1 - Notepad
File  Edit  Format  View  Help
Created By AccessData® FTK® Imager 3.1.4.6

Case Information:
Acquired using: ADI3.1.4.6
Case Number: 20
Evidence Number: 01
Unique Description: Network data
Examiner: Michael Winston
Notes: Sensitive Data

--------------------------------------------------------------

Information for D:\cfprac7\networkdata.ad1:
[Computed Hashes]
 MD5 checksum:    9bed1fb62fe2c4ab51379152814d52ce
 SHA1 checksum:   cf8f12d4ab91db366597b0308cf9d69389cf64ff

Image information:
 Acquisition started:   Wed Jul 13 11:02:31 2022
 Acquisition finished:  Wed Jul 13 11:02:31 2022
 Segment list:
  D:\cfprac7\networkdata.ad1

Image Verification Results:
 Verification started:  Wed Jul 13 11:02:31 2022
 Verification finished: Wed Jul 13 11:02:31 2022
 MD5 checksum:    9bed1fb62fe2c4ab51379152814d52ce : verified
 SHA1 checksum:   cf8f12d4ab91db366597b0308cf9d69389cf64ff : verified
```

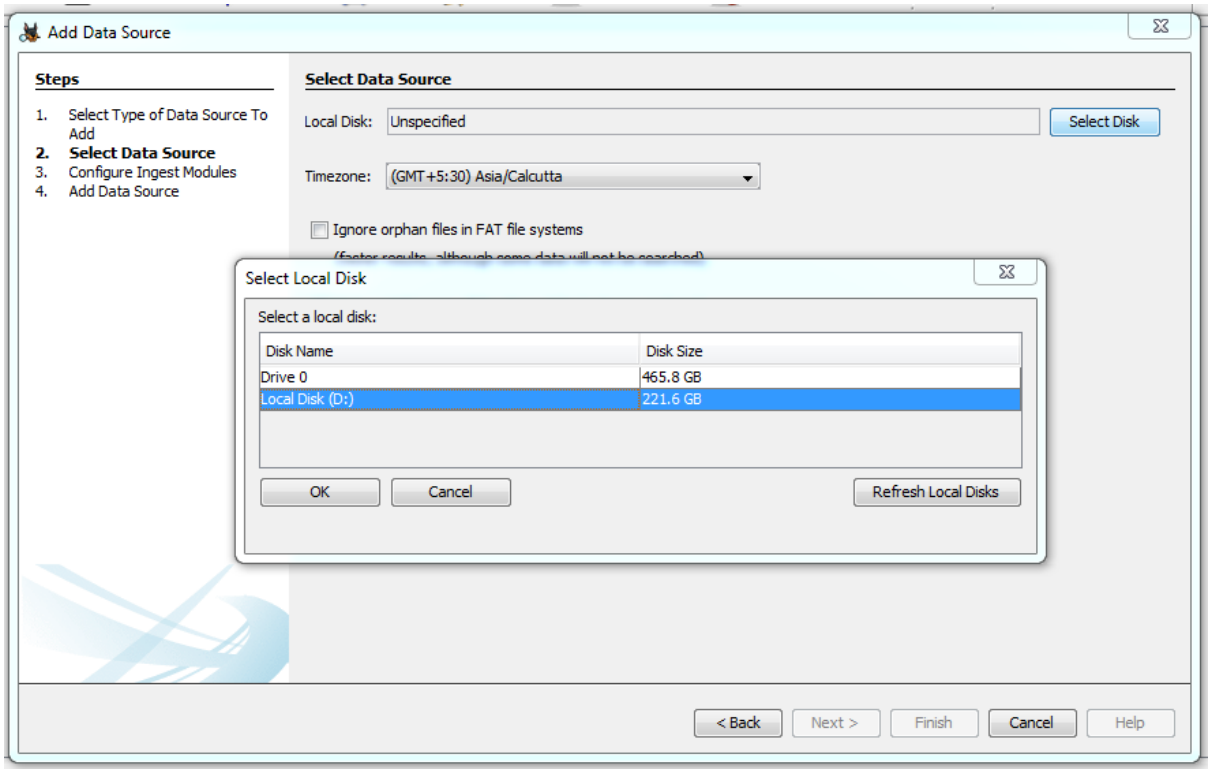
Practical 7

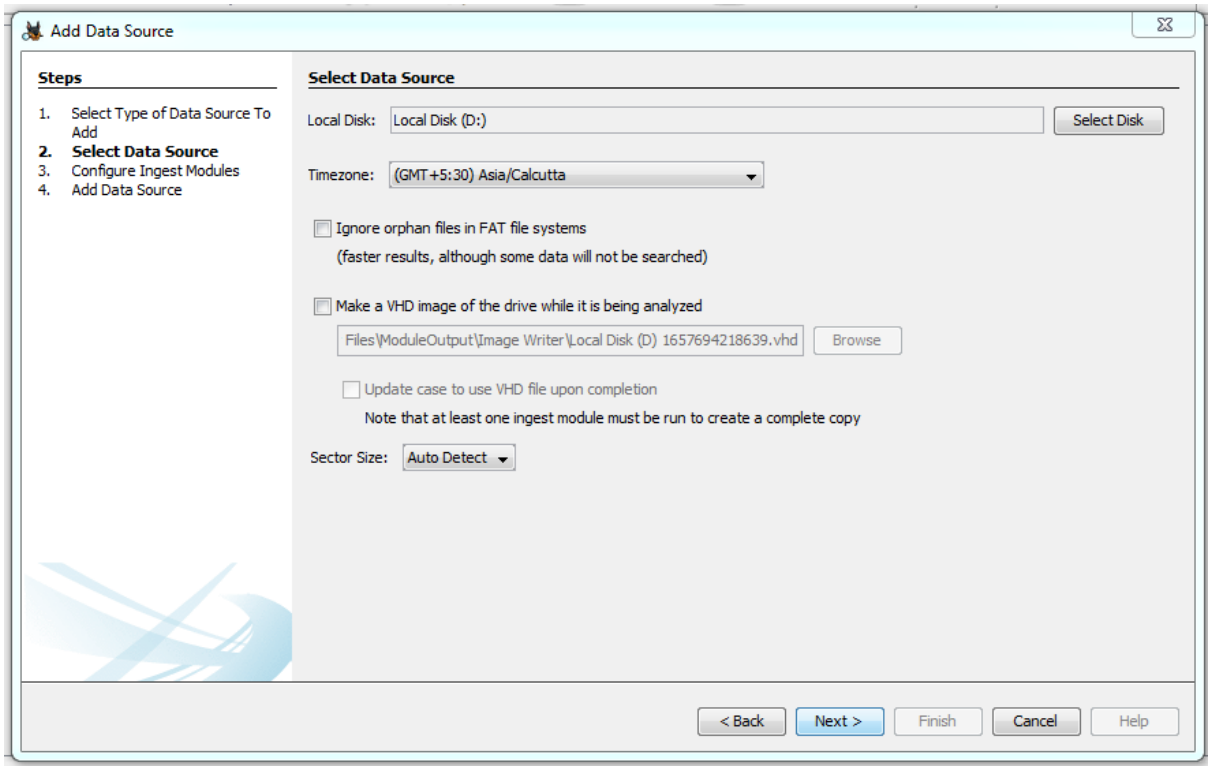
Aim:- Recovering and inspecting deleted files.

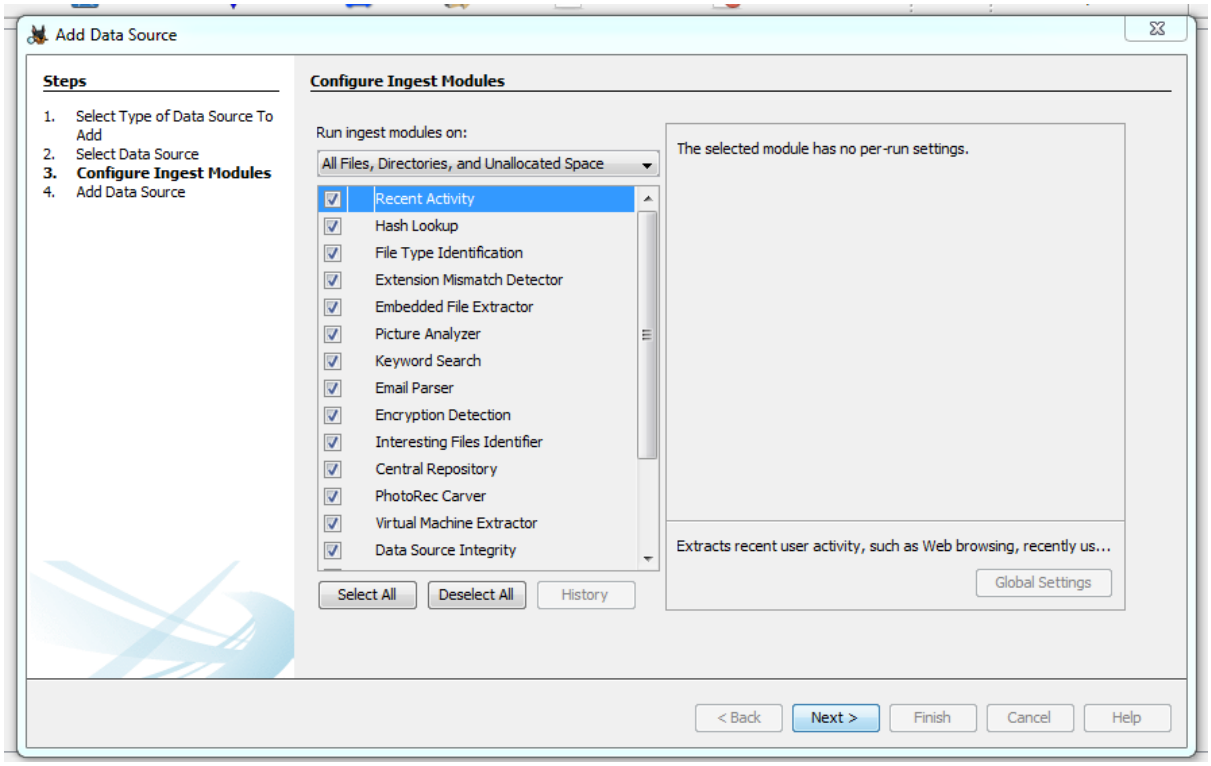

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
Recover Files
Base Directory:
D:\cfprac8
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
D:\cfprac8\Recover Files
< Back
Next >
Finish
Cancel
Help

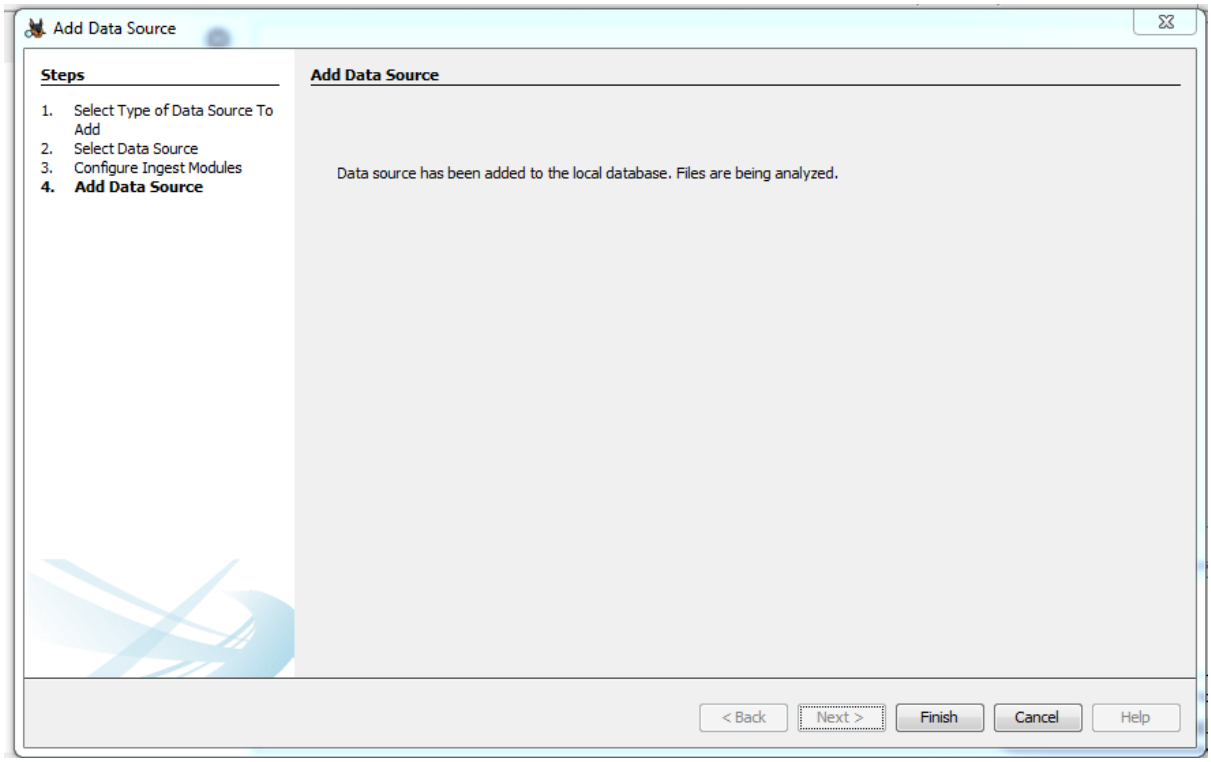

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number:
26
Examiner
Name:
Michael Winston
Phone:
0808126745
Email:
abcd@gmail.com
Notes:
recovery of deleted data
Organization
Organization analysis is being done for:
Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help

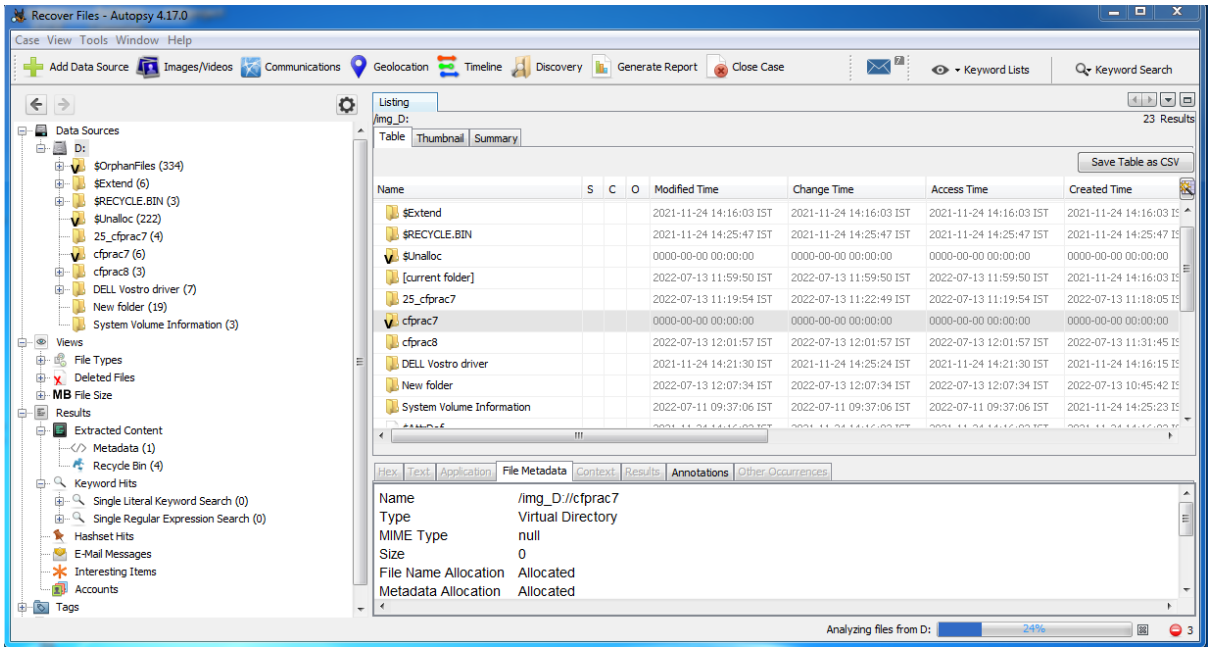

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish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

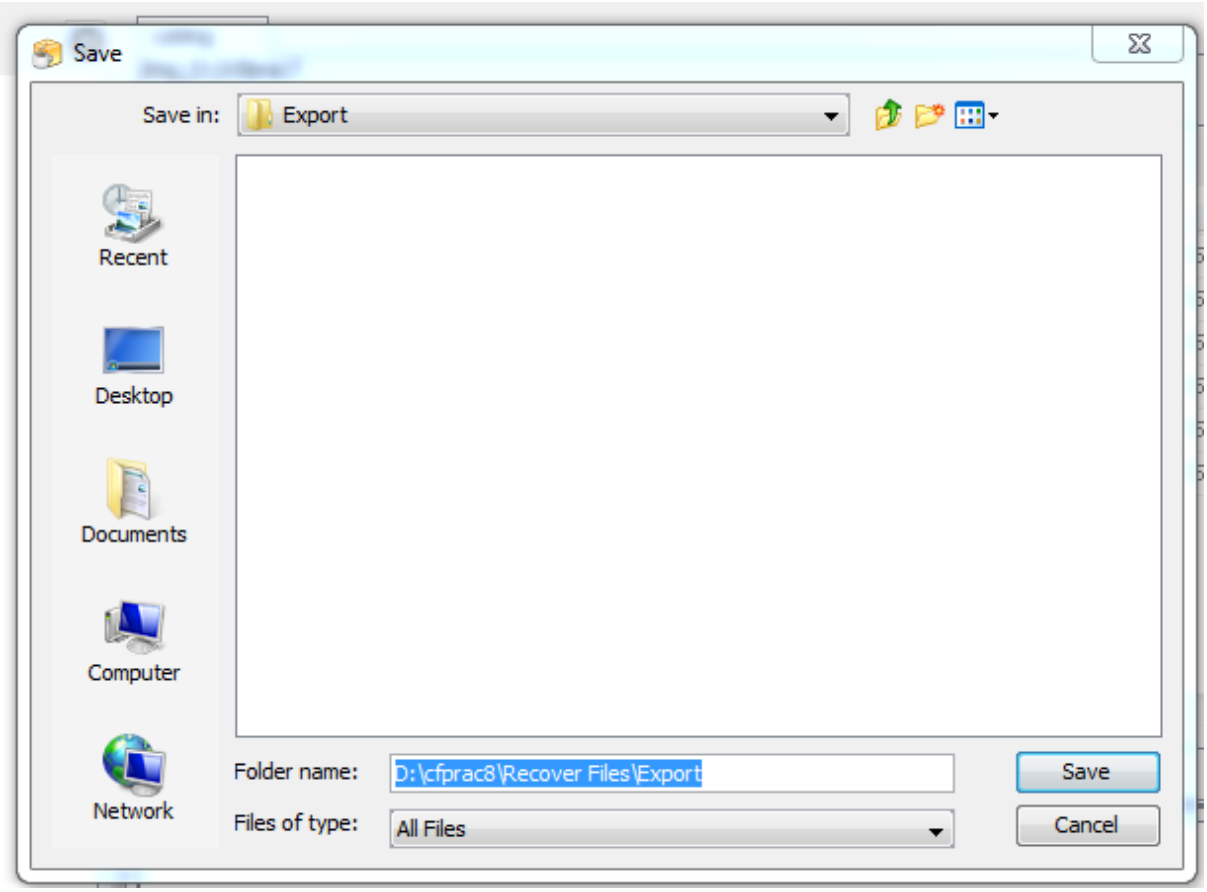

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk:
Unspecified
Select Disk
Timezone:
(GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
Select Local Disk
Select a local disk:
Disk Name
Disk Size
Drive 0
465.8 GB
Local Disk (D:)
221.6 GB
OK
Cancel
Refresh Local Disks
< Back
Next >
Finish
Cancel
Help

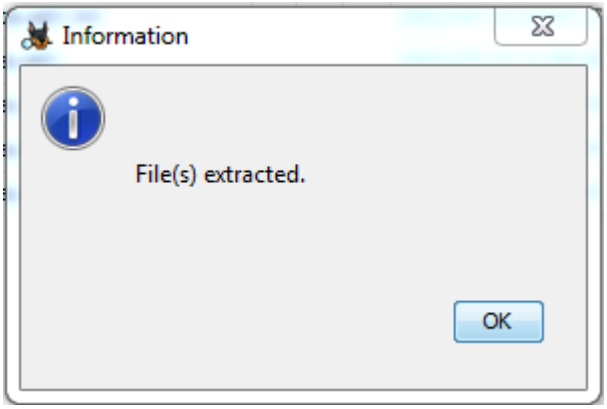

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk:
Local Disk (D:)
Select Disk
Timezone:
(GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)
Make a VHD image of the drive while it is being analyzed
Files\ModuleOutput\Image Writer\Local Disk (D) 1657694218639.vhd
Browse
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
< Back
Next >
Finish
Cancel
Help

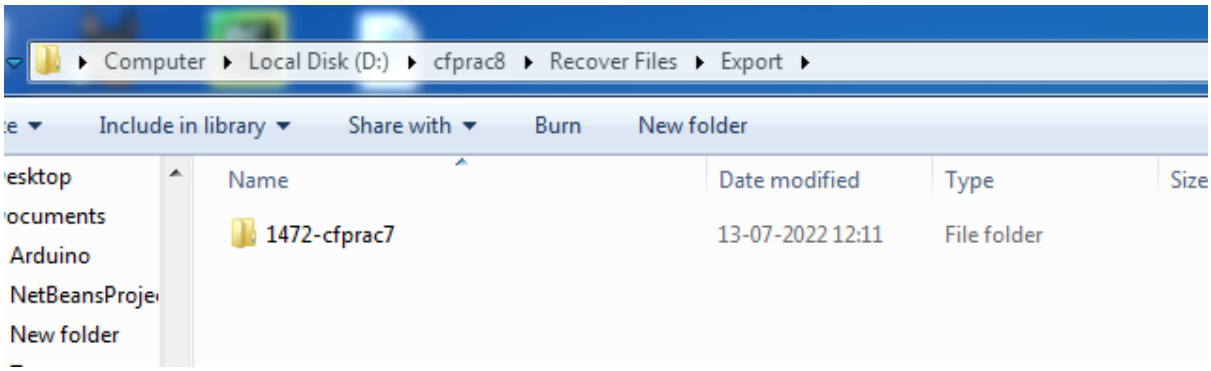

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
< Back
Next >
Finish
Cancel
Help

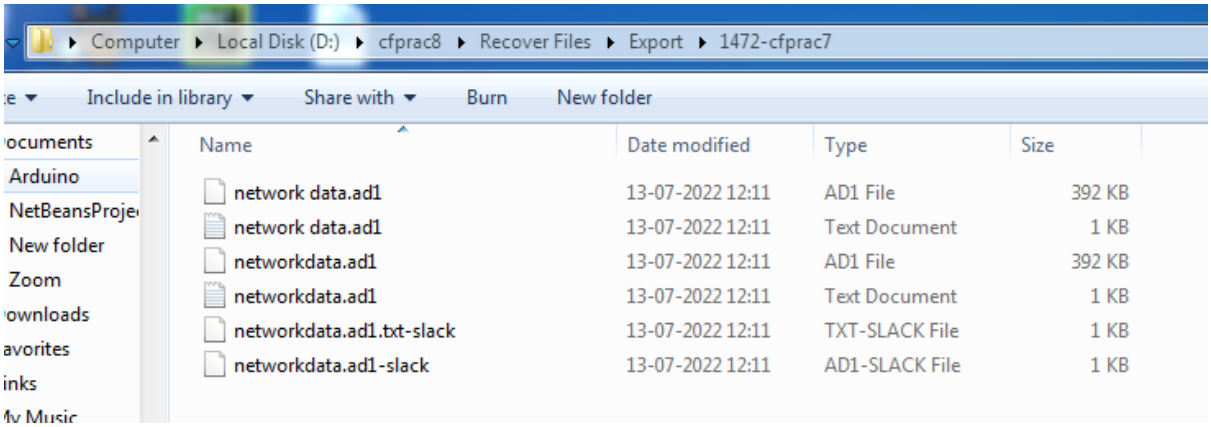

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

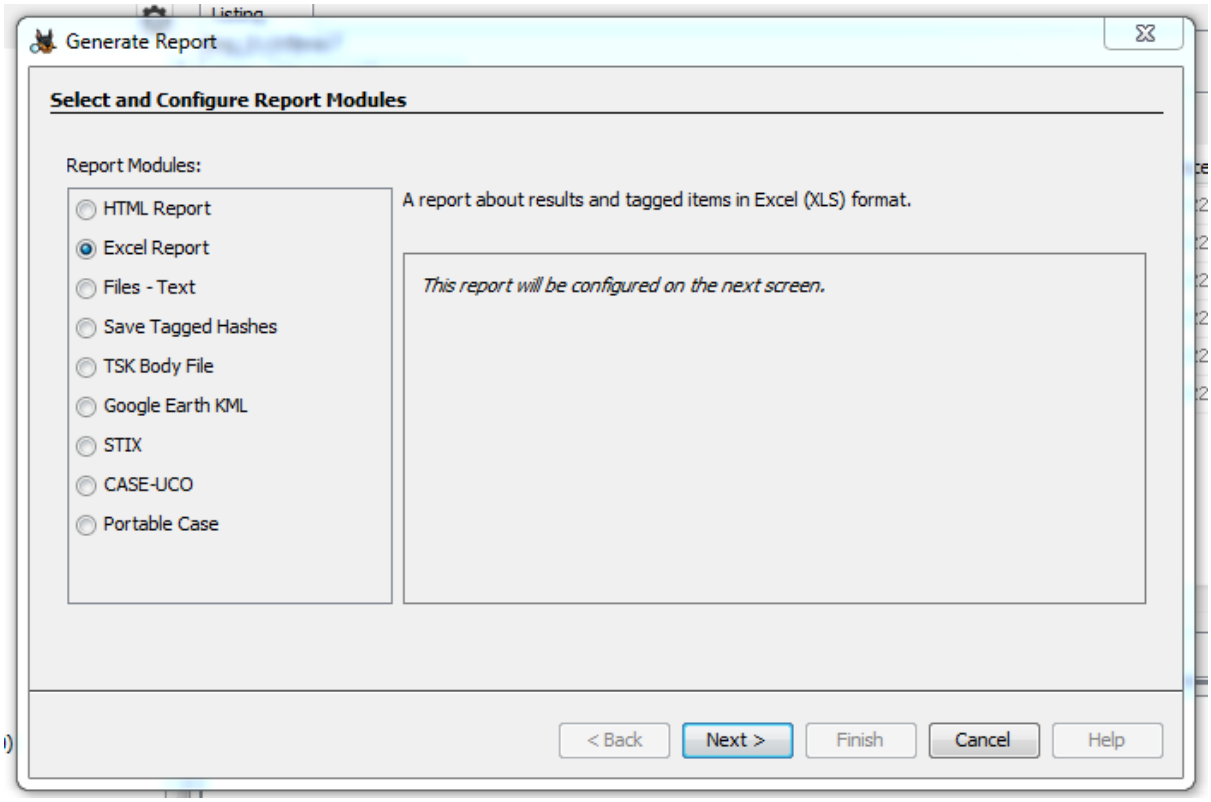

Recover Files - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
D:
$OrphanFiles (334)
$Extend (6)
$RECYCLE.BIN (3)
$Unalloc (222)
25_cfprac7 (4)
cfprac7 (6)
cfprac8 (3)
DELL Vostro driver (7)
New folder (19)
System Volume Information (3)
Views
File Types
Deleted Files
File Size
Results
Extracted Content
Metadata (1)
Recycle Bin (4)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts
Tags
Listing
/img_D:
23 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
$Extend
$RECYCLE.BIN
$Unalloc
[current folder]
25_cfprac7
cfprac7
cfprac8
DELL Vostro driver
New folder
System Volume Information
Hex
Text
Application
File Metadata
Context
Results
Annotations
Other Occurrences
Name /img_D://cfprac7
Type Virtual Directory
MIME Type null
Size 0
File Name Allocation Allocated
Metadata Allocation Allocated
Analyzing files from D:
24%

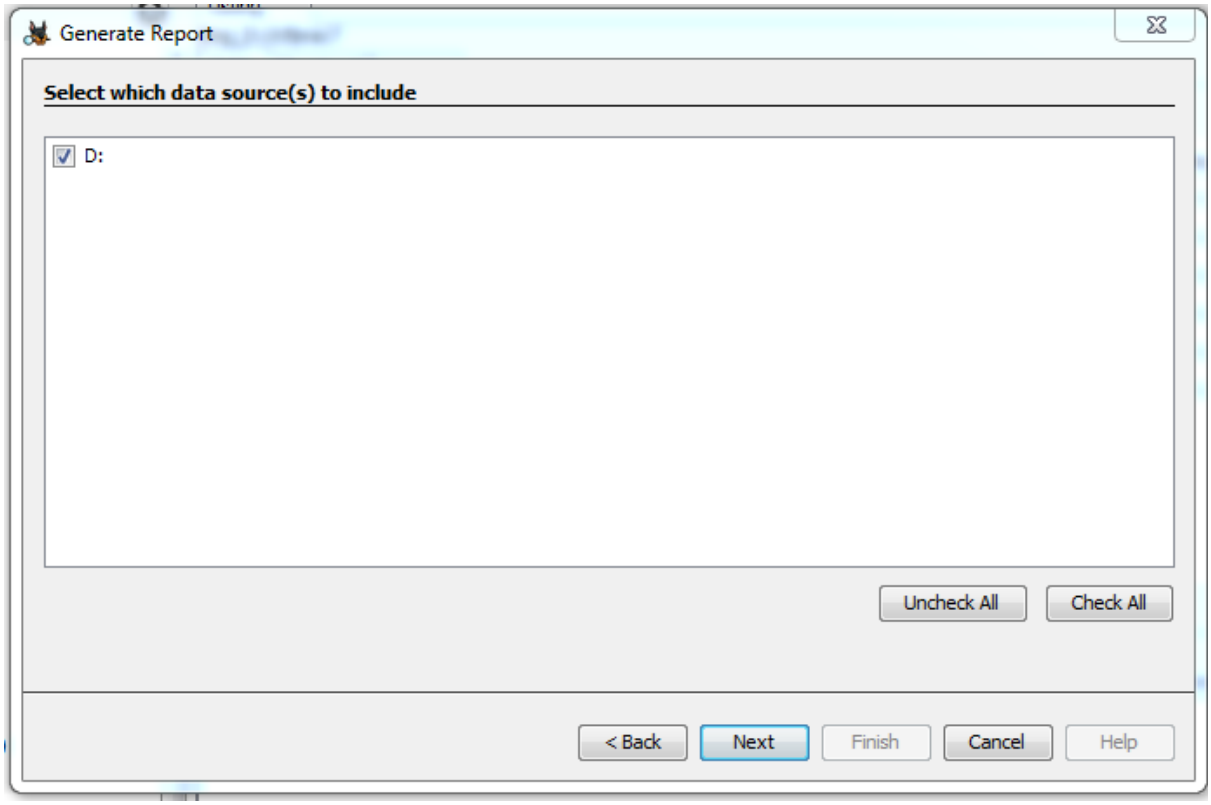

Save
Save in:
Export
Recent
Desktop
Documents
Computer
Network
Folder name:
D:\cfprac8\Recover Files\Export
Save
Files of type:
All Files
Cancel

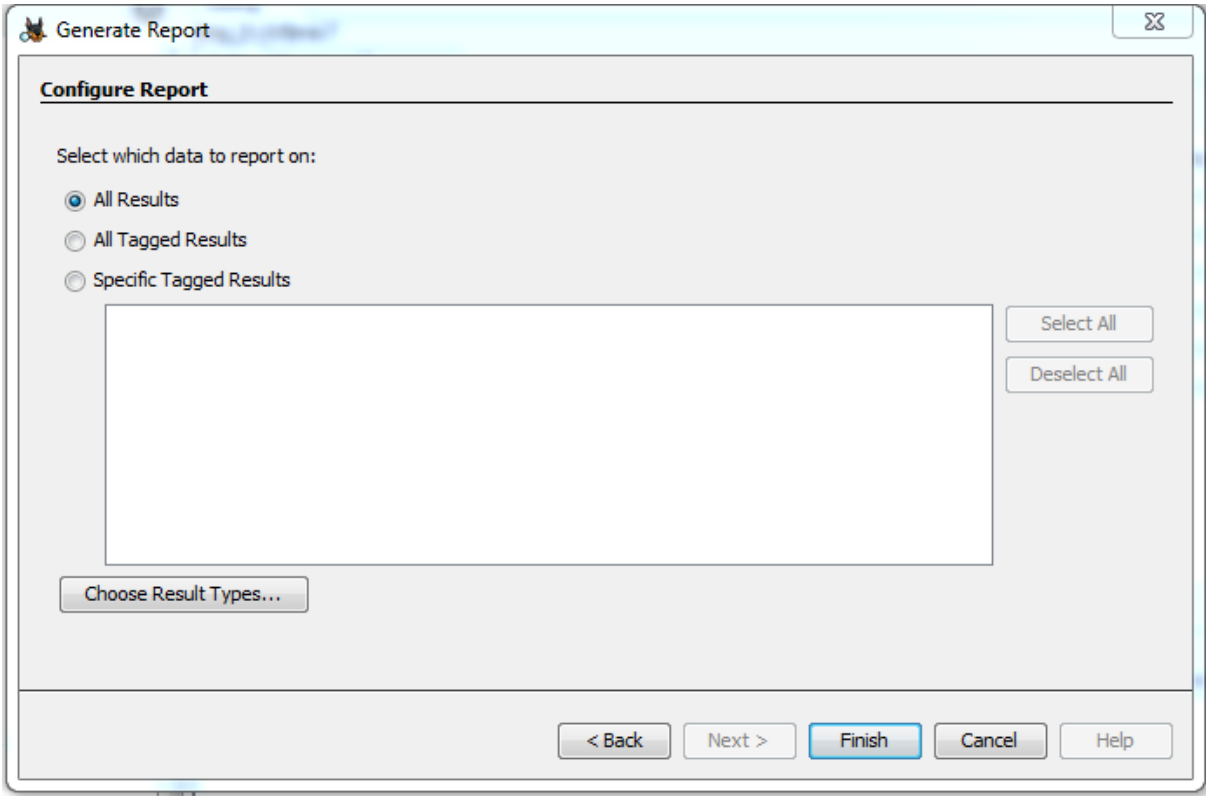

Information
File(s) extracted.
OK

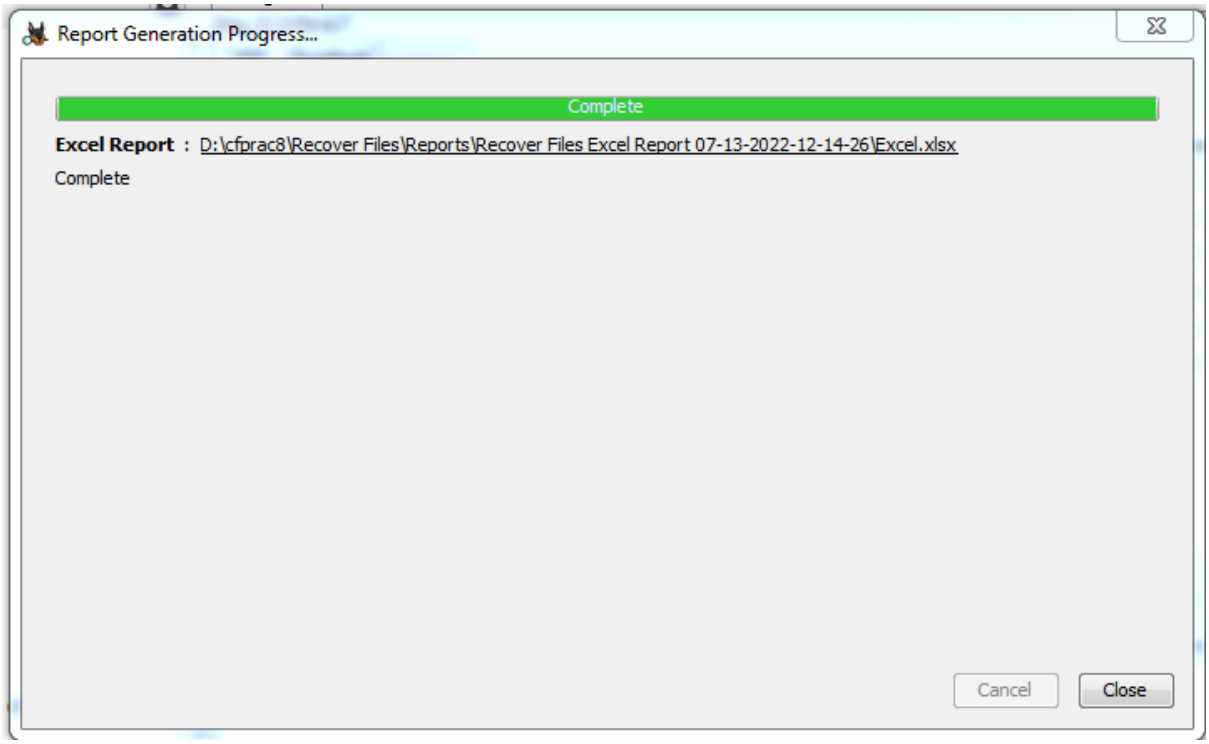

Computer
Local Disk (D:)
cfprac8
Recover Files
Export
Include in library
Share with
Burn
New folder
Name
Date modified
Type
Size
1472-cfprac7
13-07-2022 12:11
File folder
Arduino
New folder

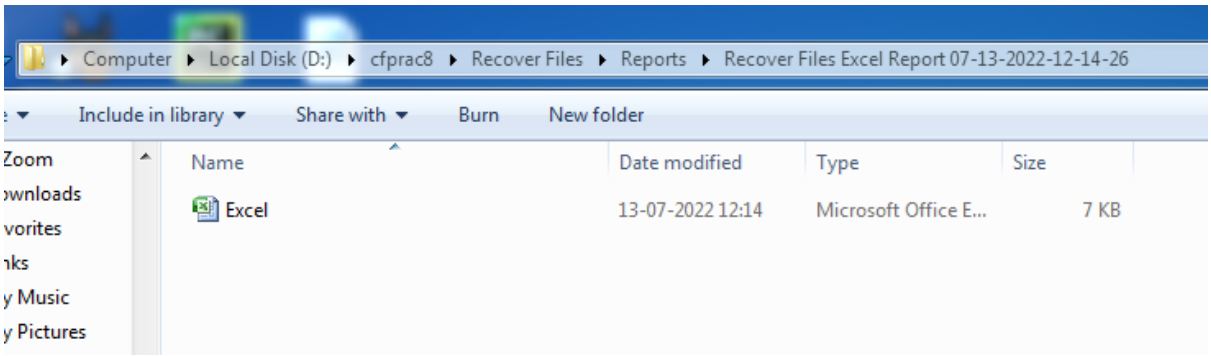

Computer ▸ Local Disk (D:) ▸ cfprac8 ▸ Recover Files ▸ Export ▸ 1472-cfprac7
Include in library
Share with
Burn
New folder
Arduino
NetBeansProje
New folder
Zoom
Name
Date modified
Type
Size
network data.ad1 13-07-2022 12:11 AD1 File 392 KB
network data.ad1 13-07-2022 12:11 Text Document 1 KB
networkdata.ad1 13-07-2022 12:11 AD1 File 392 KB
networkdata.ad1 13-07-2022 12:11 Text Document 1 KB
networkdata.ad1.txt-slack 13-07-2022 12:11 TXT-SLACK File 1 KB
networkdata.ad1-slack 13-07-2022 12:11 AD1-SLACK File 1 KB

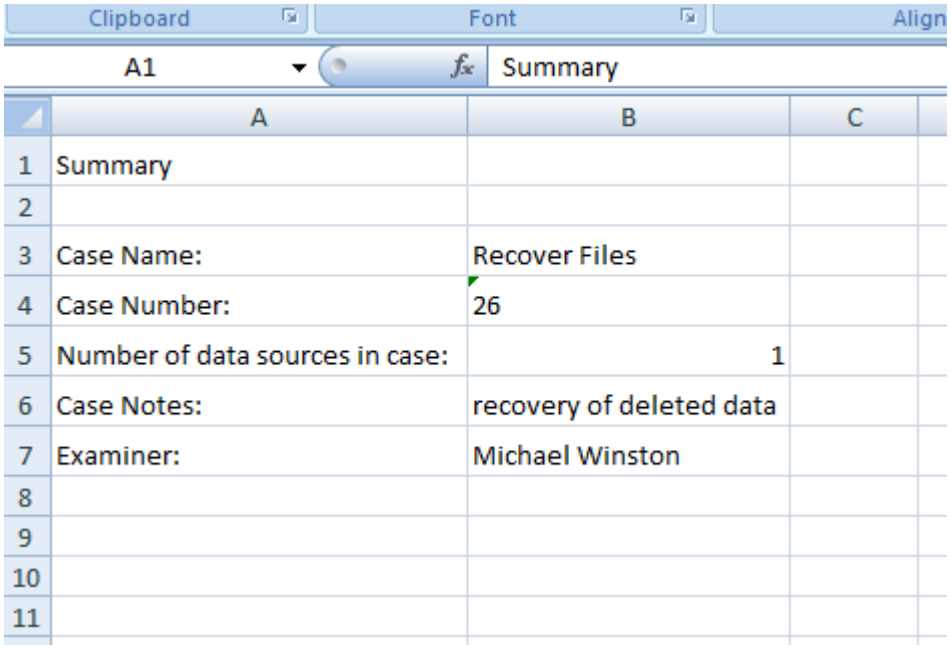

Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back
Next >
Finish
Cancel
Help


Generate Report
Select which data source(s) to include
D:
Uncheck All
Check All
< Back
Next
Finish
Cancel
Help


Generate Report
Configure Report
Select which data to report on:
All Results
All Tagged Results
Specific Tagged Results
Select All
Deselect All
Choose Result Types...
< Back
Next >
Finish
Cancel
Help







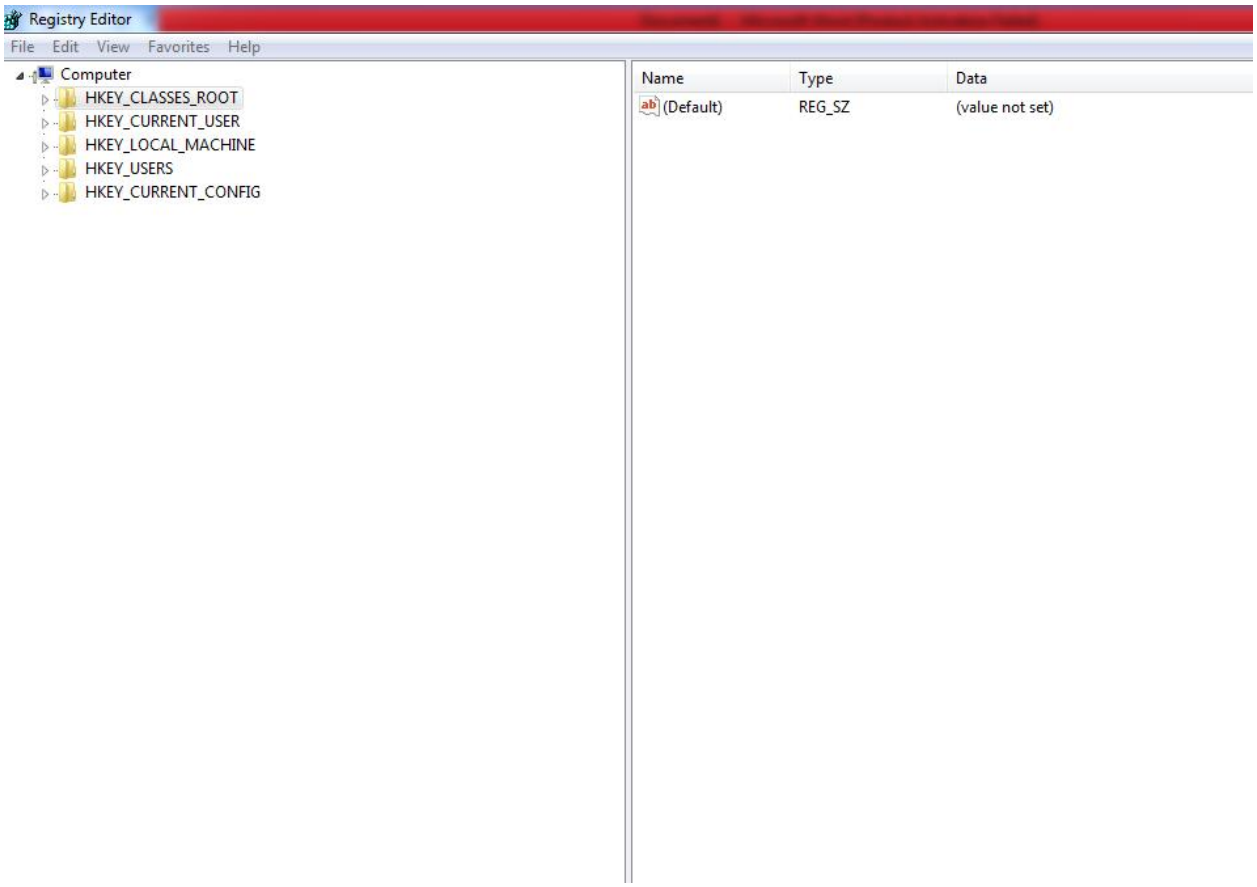
	A	B	C
1	Summary		
2			
3	Case Name:	Recover Files	
4	Case Number:	26	
5	Number of data sources in case:	1	
6	Case Notes:	recovery of deleted data	
7	Examiner:	Michael Winston	
8			
9			
10			
11			

Practical 8

Aim:- Access relevant information from Windows registry for investigation process using registry view.

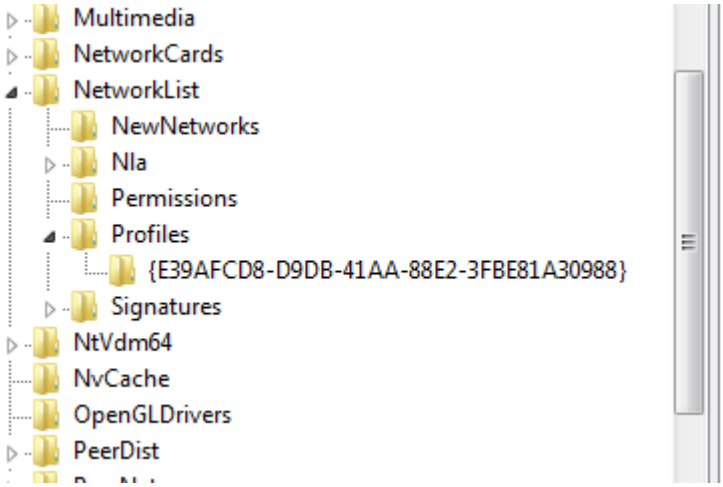
Accessing the registry.

Go to start menu and search **"regedit".**



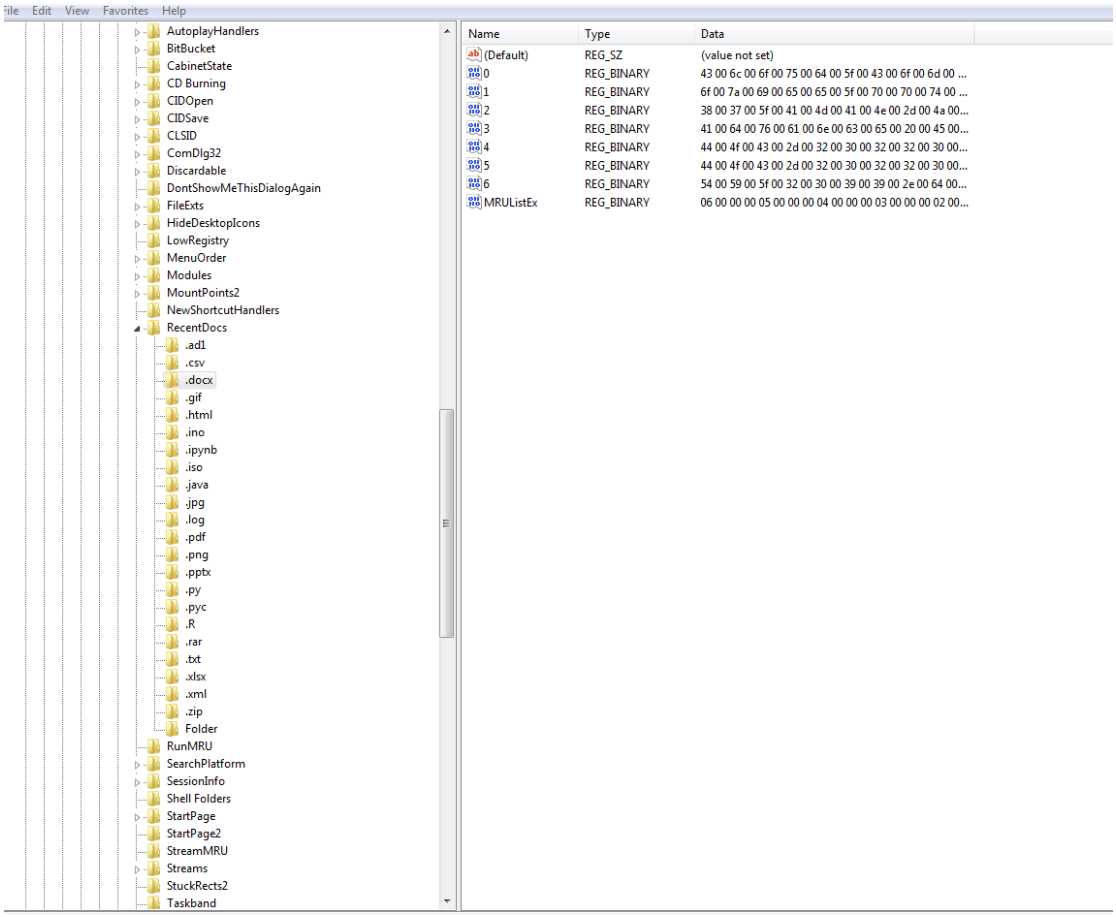
Wireless evidence in the registry.

HKEY_LOCAL_MACHIME/SOFTWARE/Microsoft/Windows NT/CurrentVersion/NetworkList/Profiles



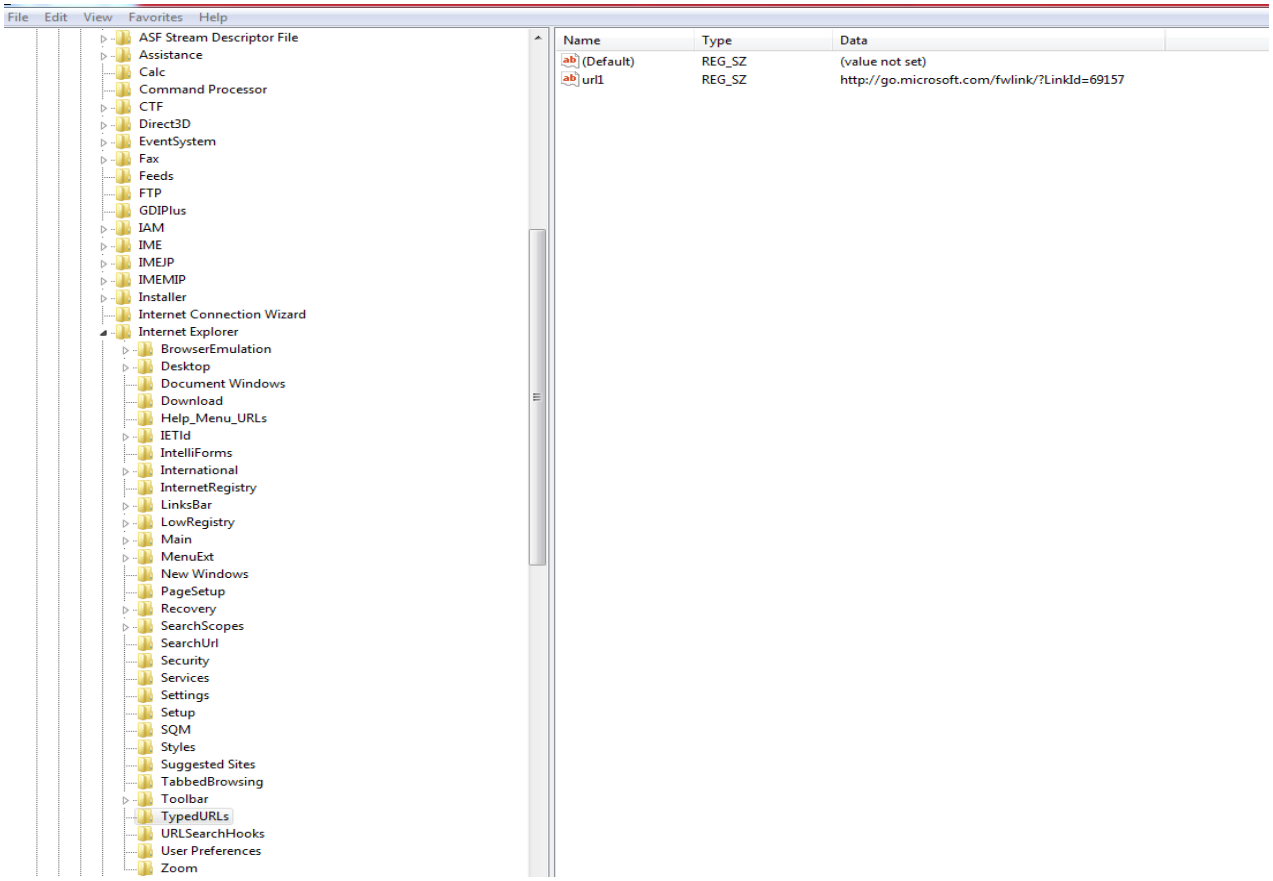
RecentDocs key

HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer /RecentDocs/.docx



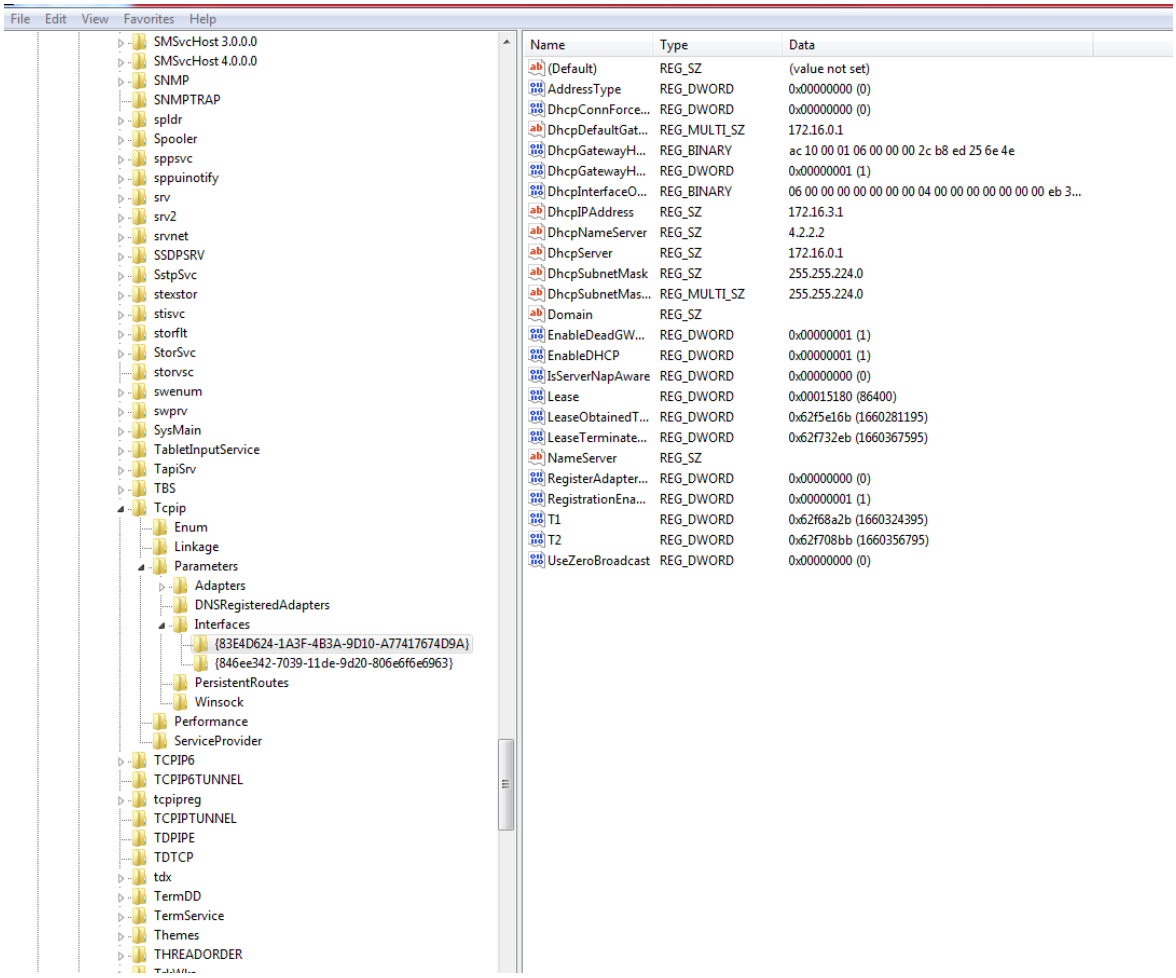
TypedURLs key

HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs



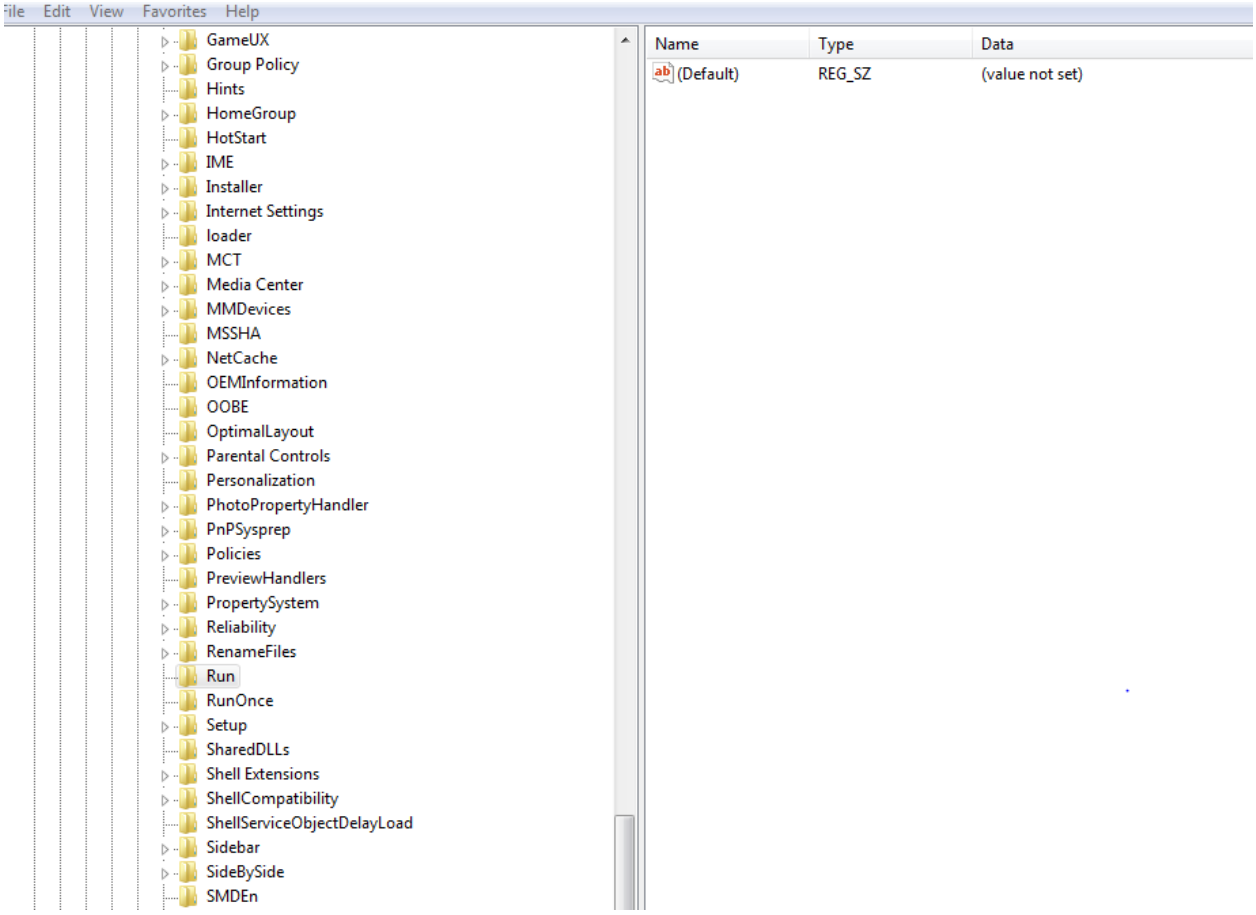
IP Address

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services/Tcpip/Parameters /Interfaces



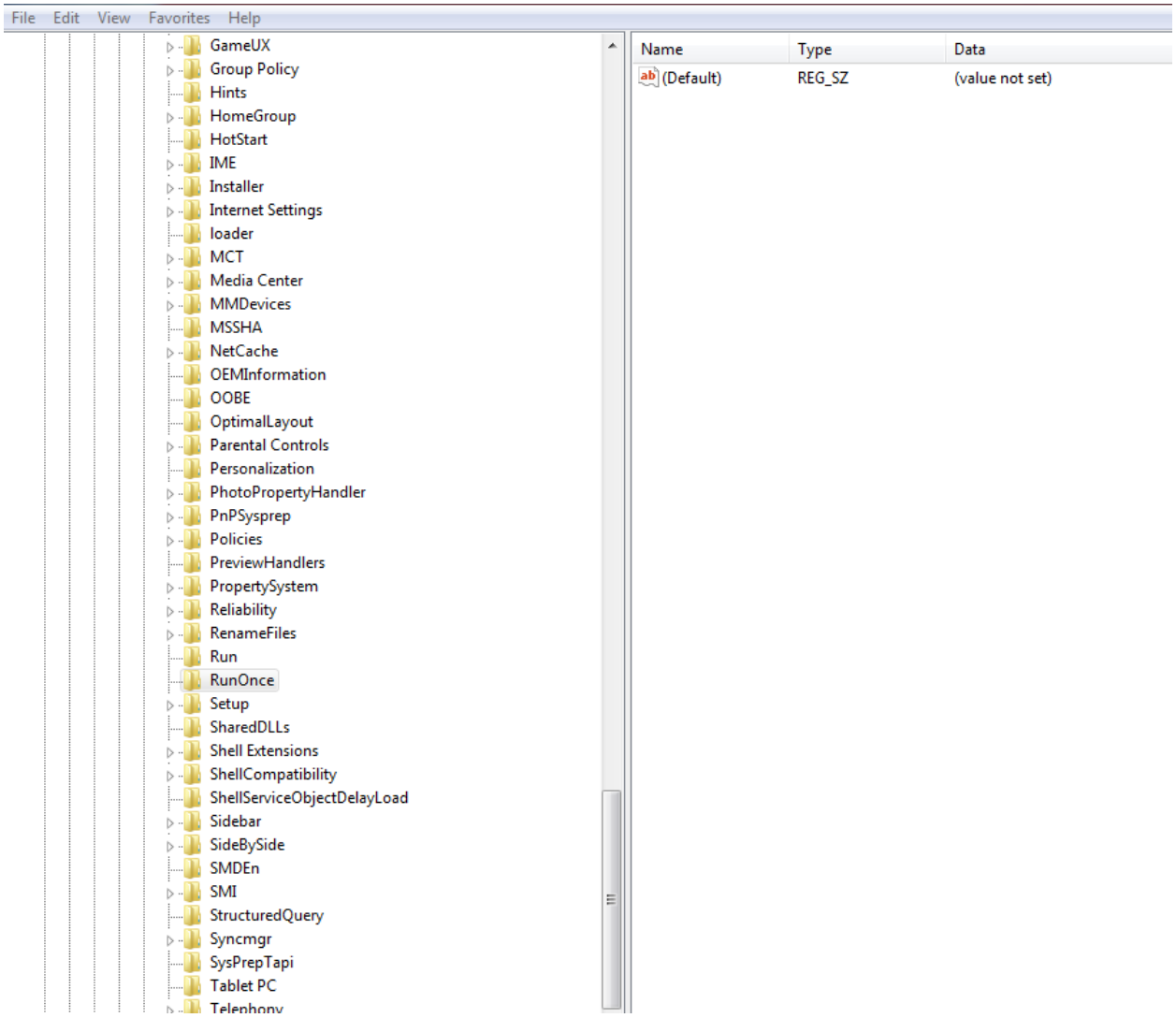
Startup location in the registry

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/CurrentVersion/Run



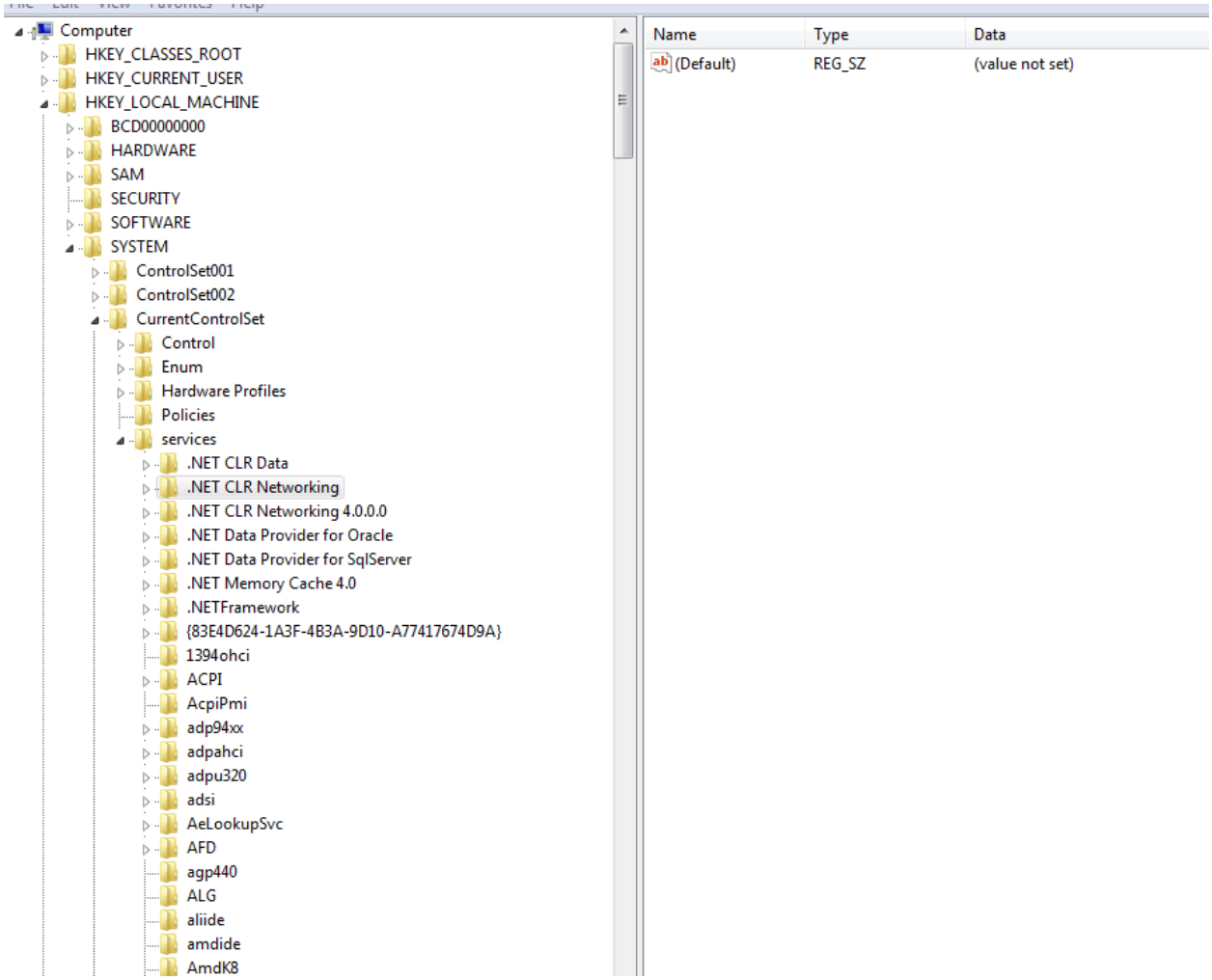
RunOnce Startup

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/CurrentVersion /RunOnce



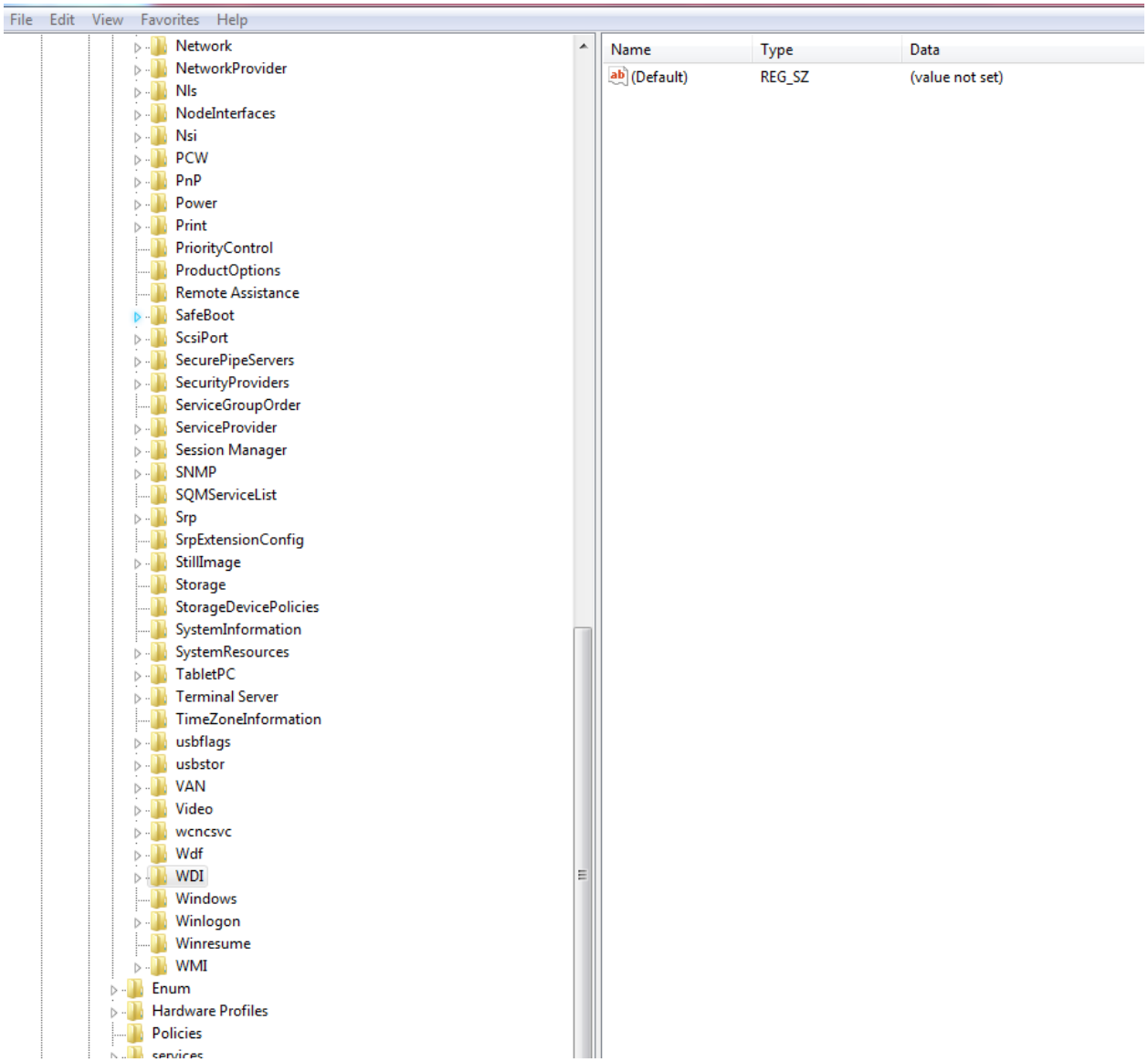
Startup Services

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services



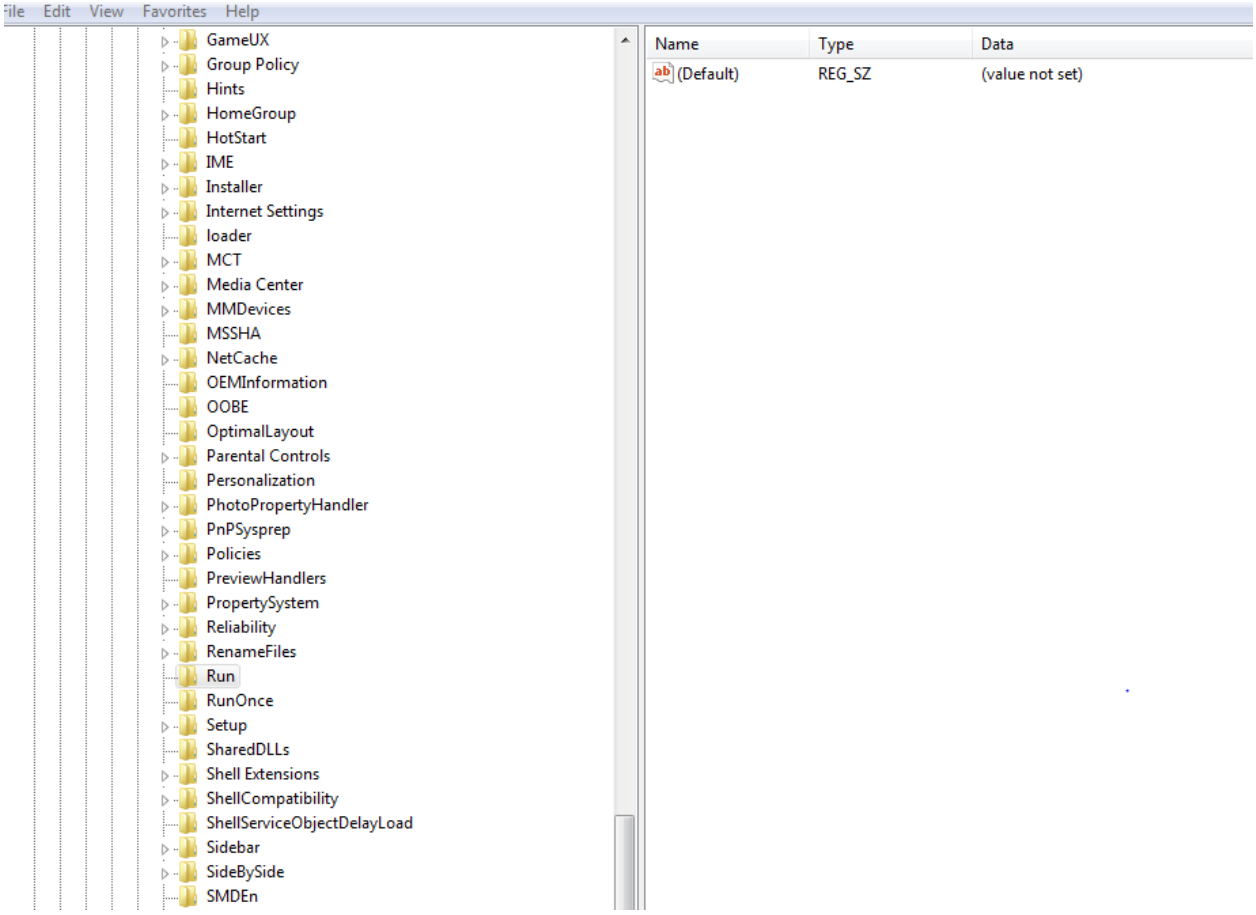
Start Legacy Application

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/WIDI



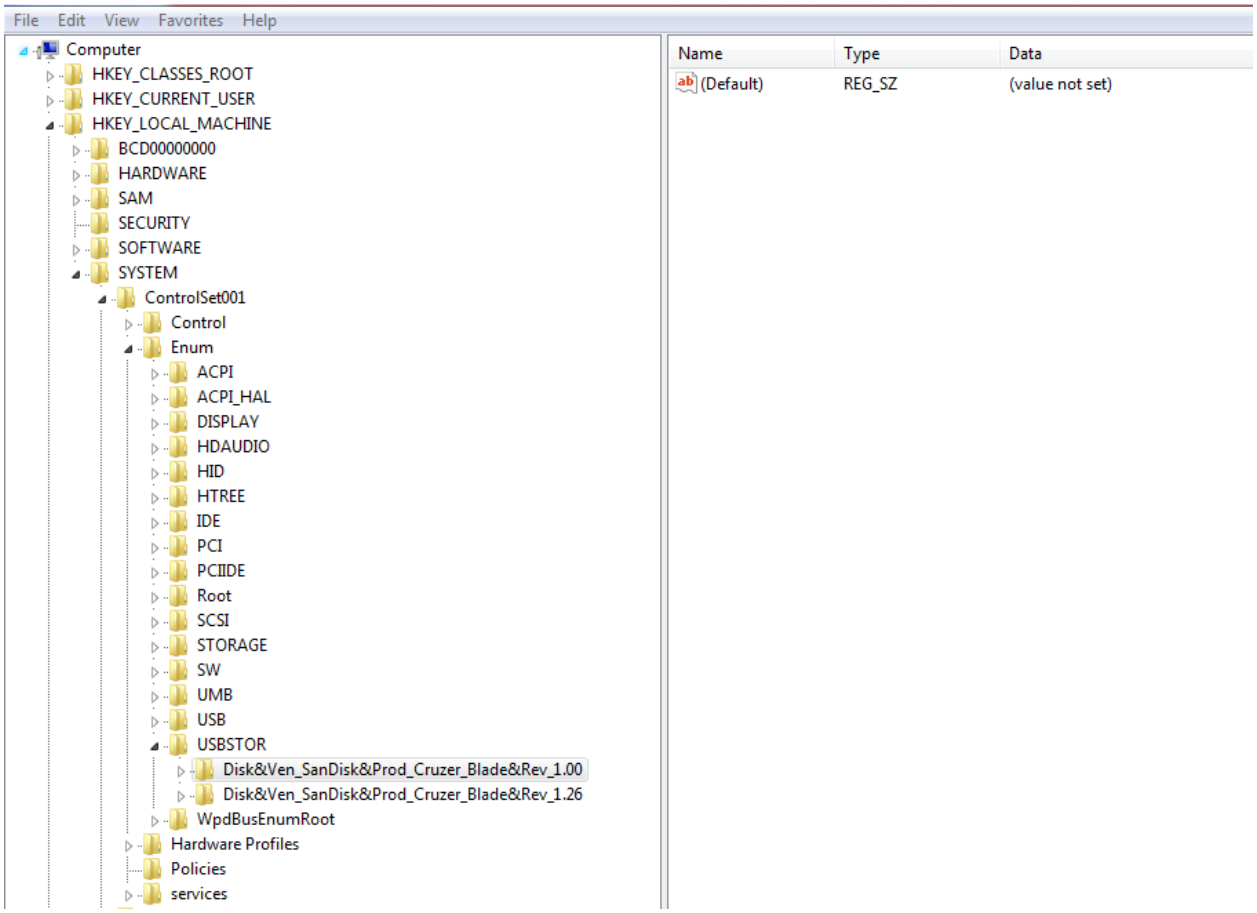
Start when a particular user logs on.

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/CurrentVersion/Run



USB Storage device

HKEY_LOCAL_MACHINE/SYSTEM/ControlSet00X/Enum/USBSTOR



MountedDevices