Name: Aniket Yadav
Roll no: 5734
Subject: Cyber Forensic Law
Class: Msc CS II

Practical 1

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

Code:-

Sender.java

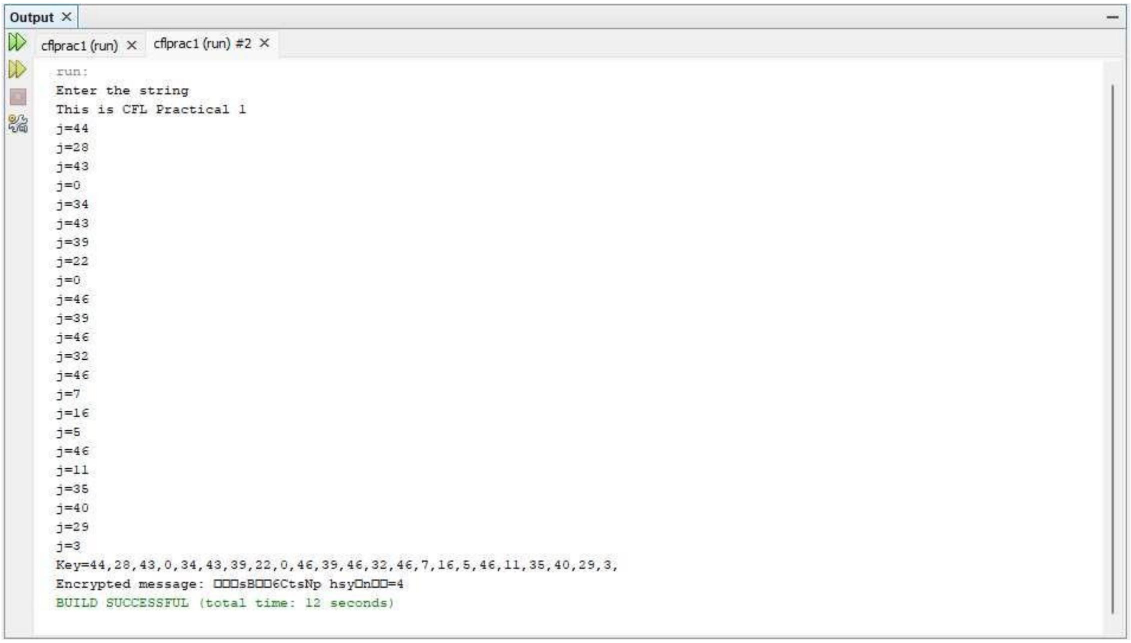
```
package cflprac1;

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++)

  {

    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");
```

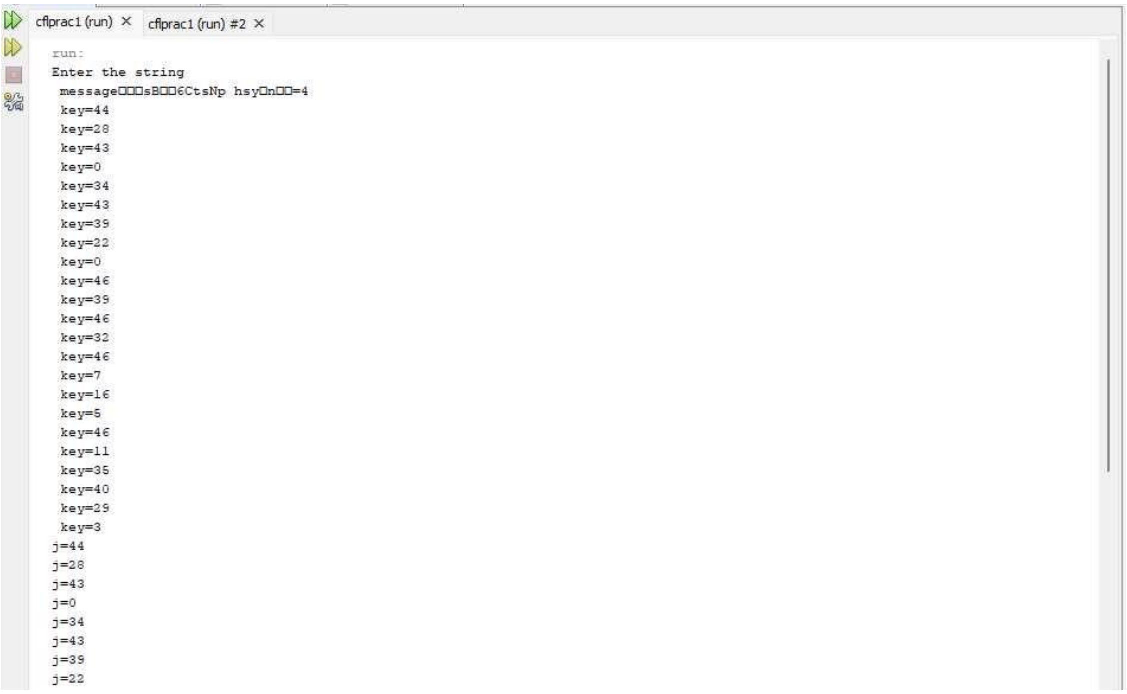
```
  BufferedReader br= new BufferedReader(new InputStreamReader(sc.getInputStream()));
  ct=br.readLine();
  String[] s=new String[ct.length()];
  s=ct.split(",");     int[]     j=new
  int[s[0].length()];
  System.out.println("
  message"+s[0]);
  for(i=0;i<s[0].length();i++)
  {
    j[i]=Integer.parseInt(s[i+1]);
    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

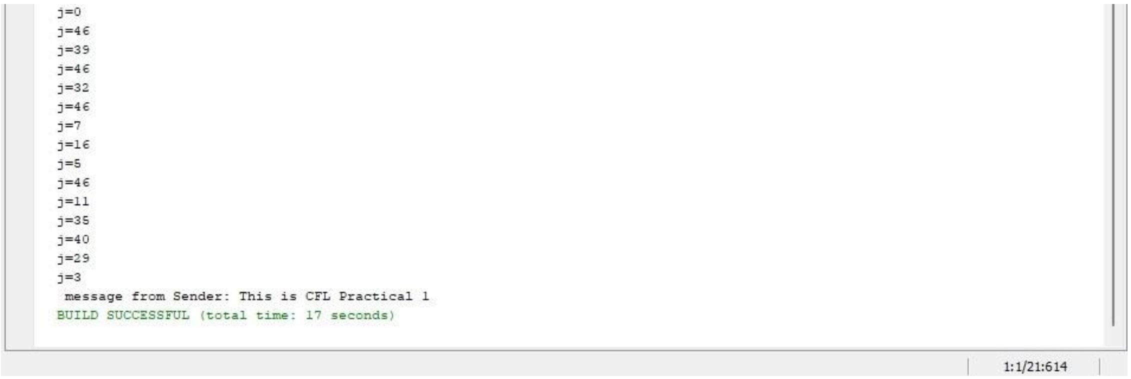


```
run:
Enter the string
This is CFL Practical 1
j=44
j=28
j=43
j=0
j=34
j=43
j=39
j=22
j=0
j=46
j=39
j=46
j=32
j=46
j=7
j=16
j=5
j=46
j=11
j=35
j=40
j=29
j=3
Key=44,28,43,0,34,43,39,22,0,46,39,46,32,46,7,16,5,46,11,35,40,29,3,
Encrypted message: □□□sB□□6CtsNp hsy□n□□=4
BUILD SUCCESSFUL (total time: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

Receiver.java



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



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

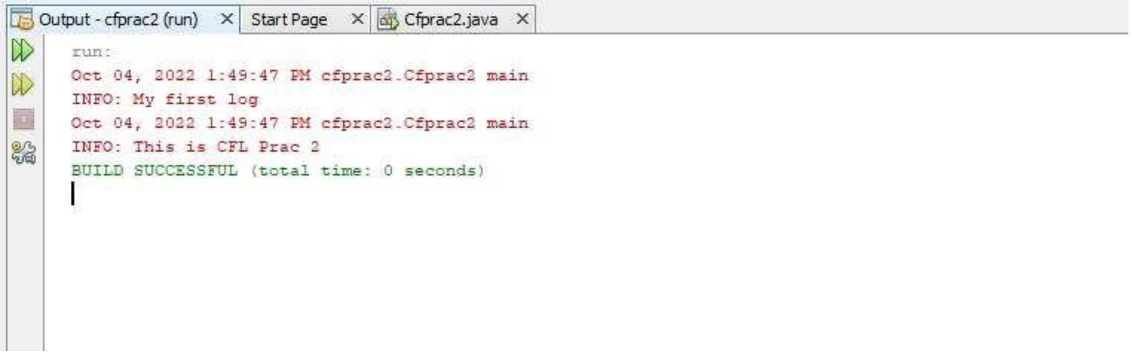
Practical 2

Aim:- Java program for creating log files.

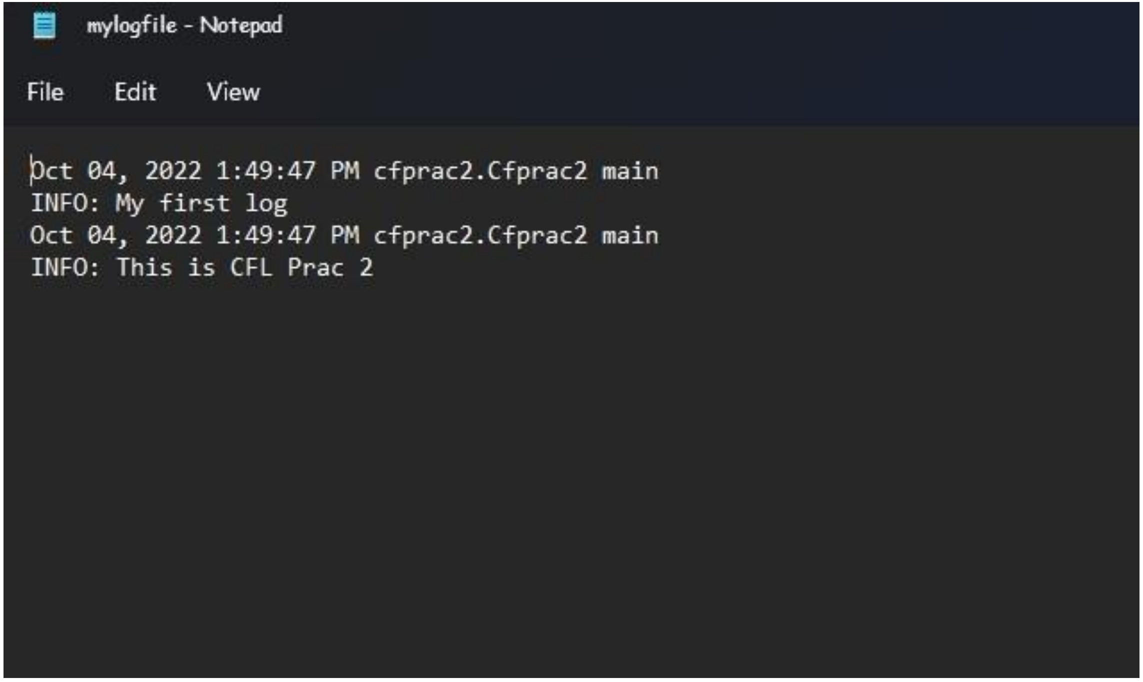
Code:-

```
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)
```



```
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
```

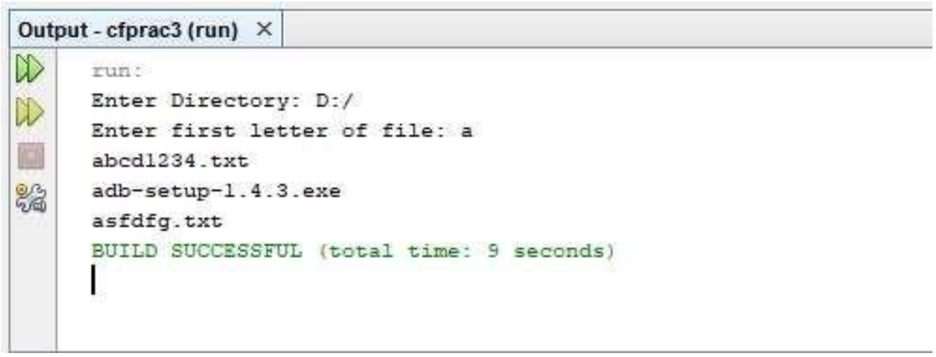
Practical 3

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);

          }
      };
      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:/
Enter first letter of file: a
abcd1234.txt
adb-setup-1.4.3.exe
asfdfg.txt
BUILD SUCCESSFUL (total time: 9 seconds)
```

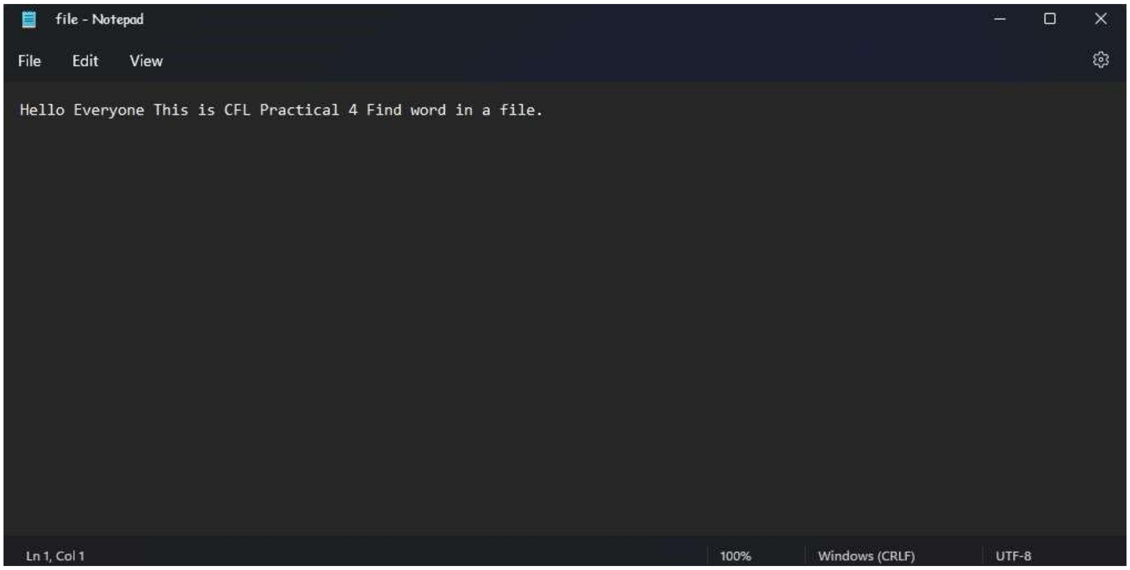
Practical 4

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

Code:-

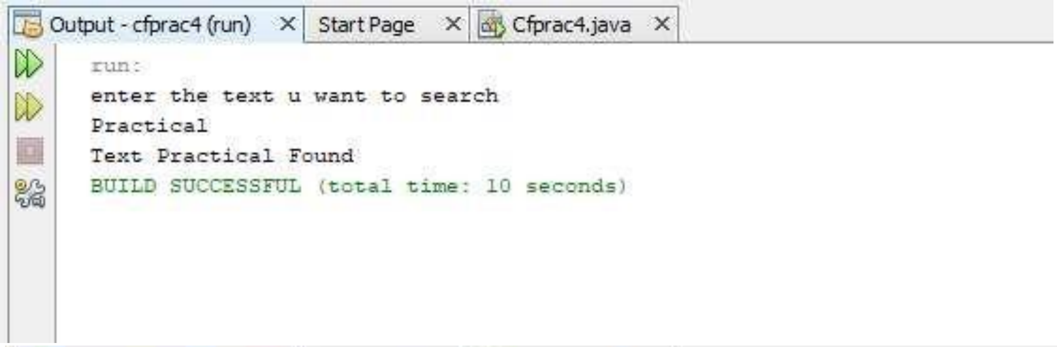
```
package      cfprac4;      import
java.io.BufferedReader;    import
java.io.FileReader;        import
java.io.InputStreamReader;
public class Cfprac4 {



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

  }

}
```

File.txt

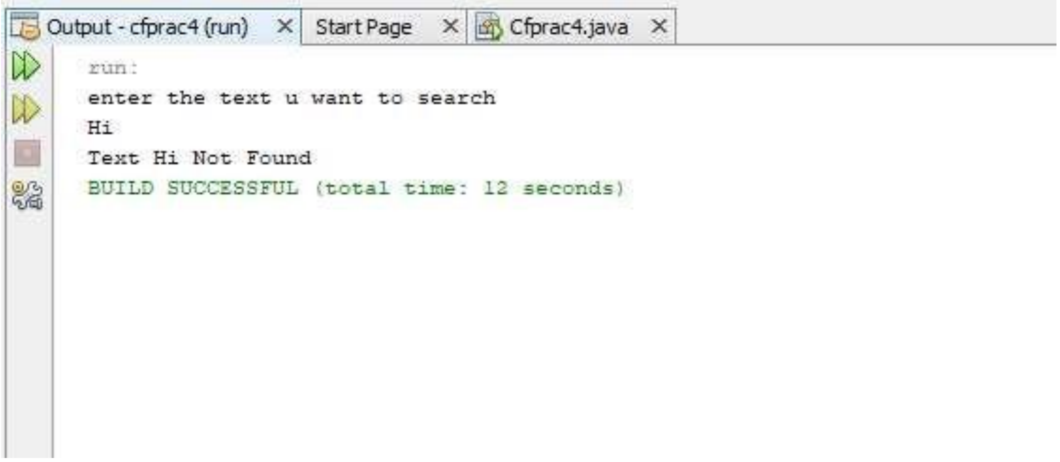


```
Hello Everyone This is CFL Practical 4 Find word in a file.
```

Output:-



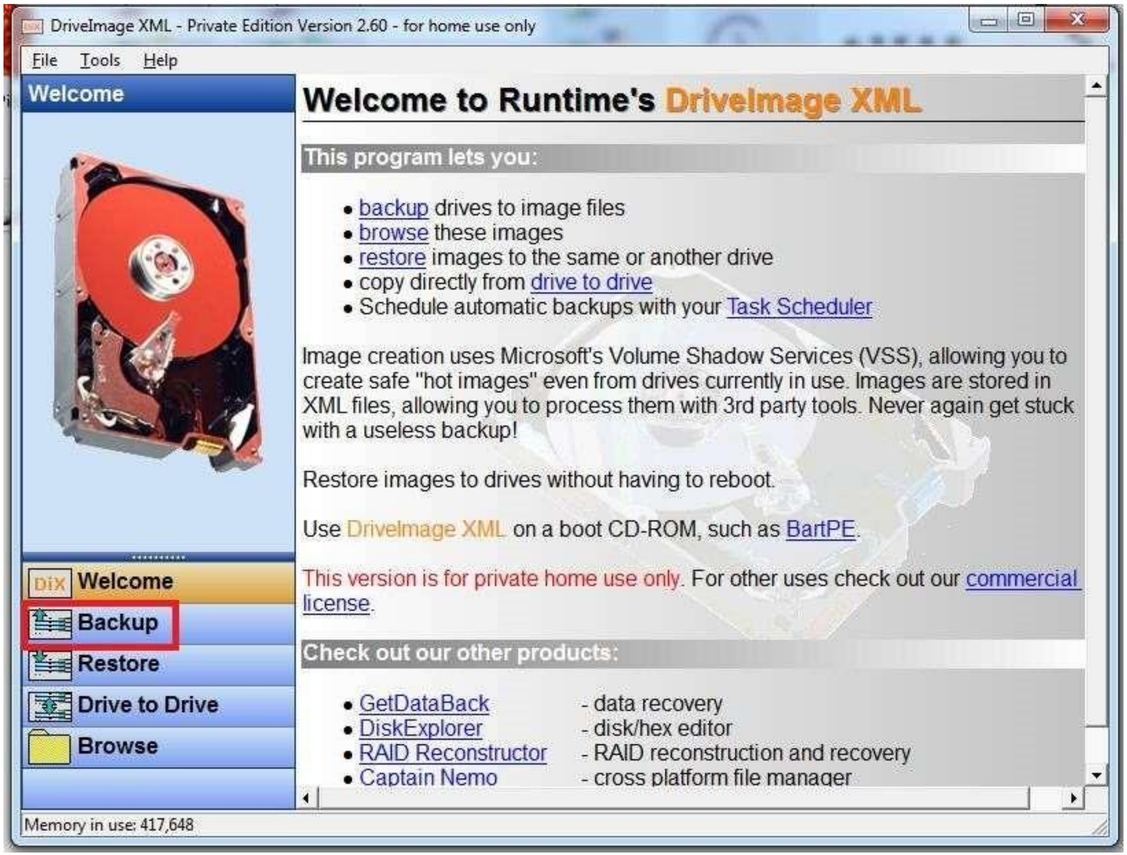
```
run:
enter the text u want to search
Practical
Text Practical Found
BUILD SUCCESSFUL (total time: 10 seconds)
```



```
run:
enter the text u want to search
Hi
Text Hi Not Found
BUILD SUCCESSFUL (total time: 12 seconds)
```

Practical 5

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



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!

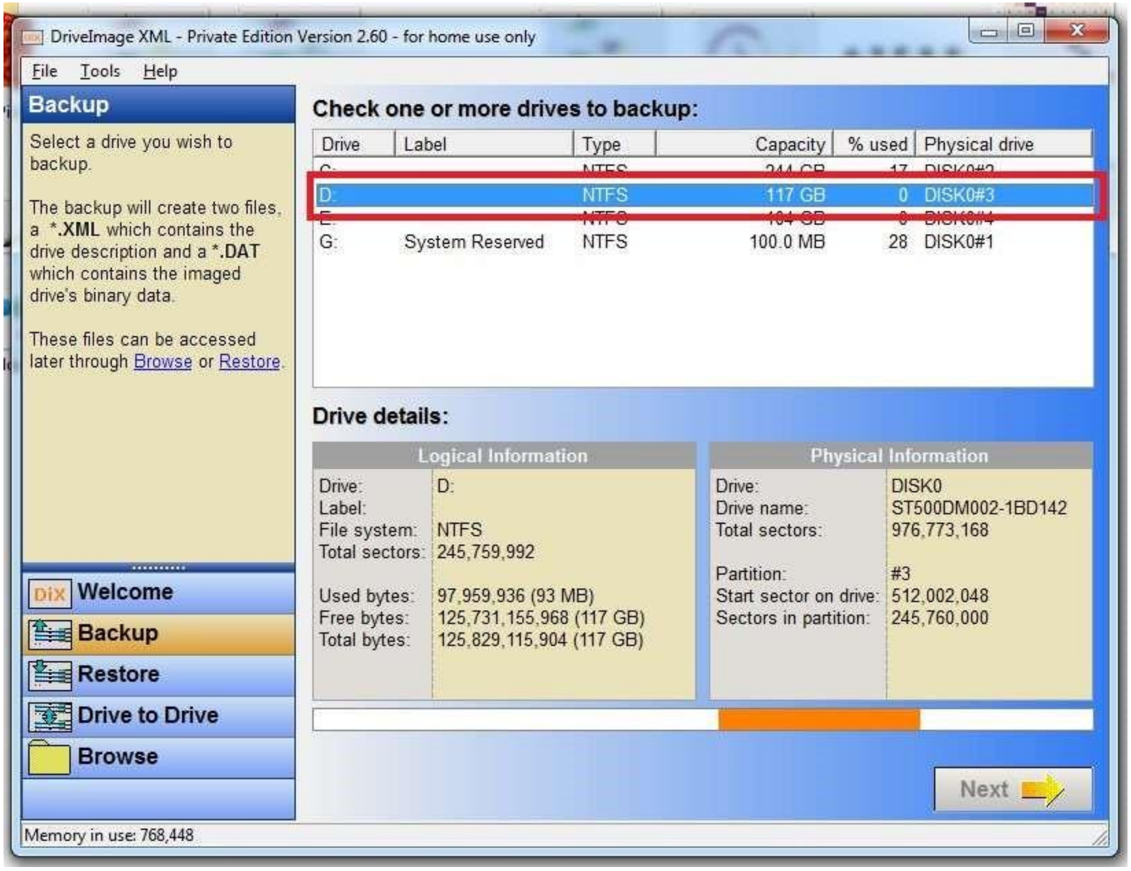
Restore images to drives without having to reboot.

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



Select a drive you wish to backup.

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

These files can be accessed later through Browse or Restore.

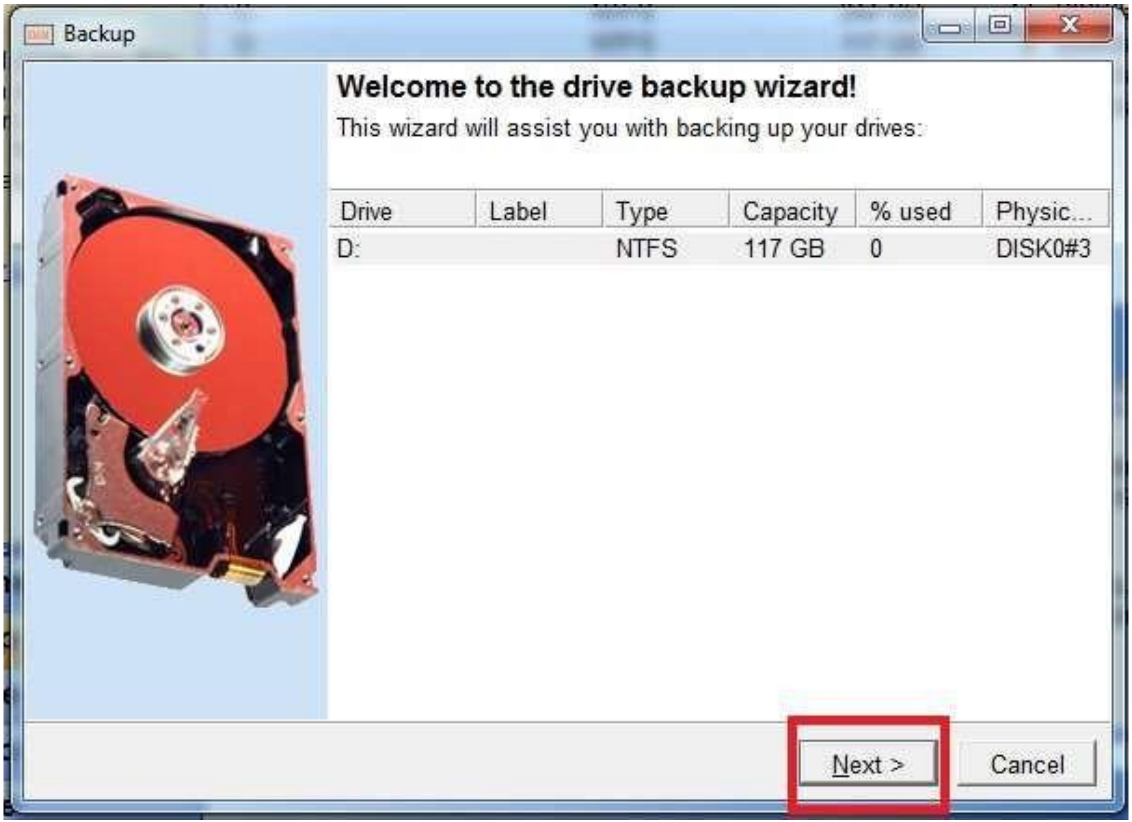
Check one or more drives to backup:

Drive	Label	Type	Capacity	% used	Physical drive
C:		NTFS	244 GB	17	DISK0#2
D:		NTFS	117 GB	0	DISK0#3
E:		NTFS	104 GB	0	DISK0#4
G:	System Reserved	NTFS	100.0 MB	28	DISK0#1

Drive details:

Logical Information	
Drive:	D:
Label:	
File system:	NTFS
Total sectors:	245,759,992
Used bytes:	97,959,936 (93 MB)
Free bytes:	125,731,155,968 (117 GB)
Total bytes:	125,829,115,904 (117 GB)

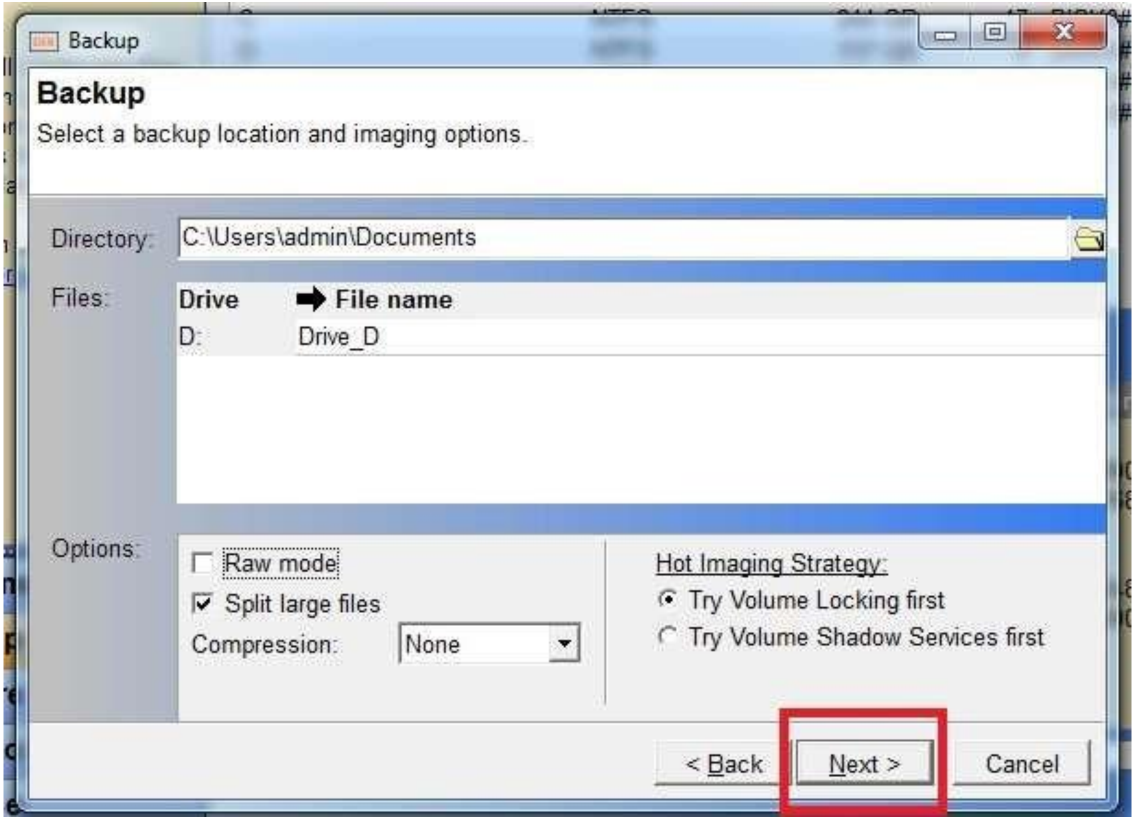
Physical Information	
Drive:	DISK0
Drive name:	ST500DM002-1BD142
Total sectors:	976,773,168
Partition:	#3
Start sector on drive:	512,002,048
Sectors in partition:	245,760,000



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



Backup

Select a backup location and imaging options.

Directory: C:\Users\admin\Documents

Files:

Drive	➡ File name
D:	Drive_D

Options:

□ Raw mode

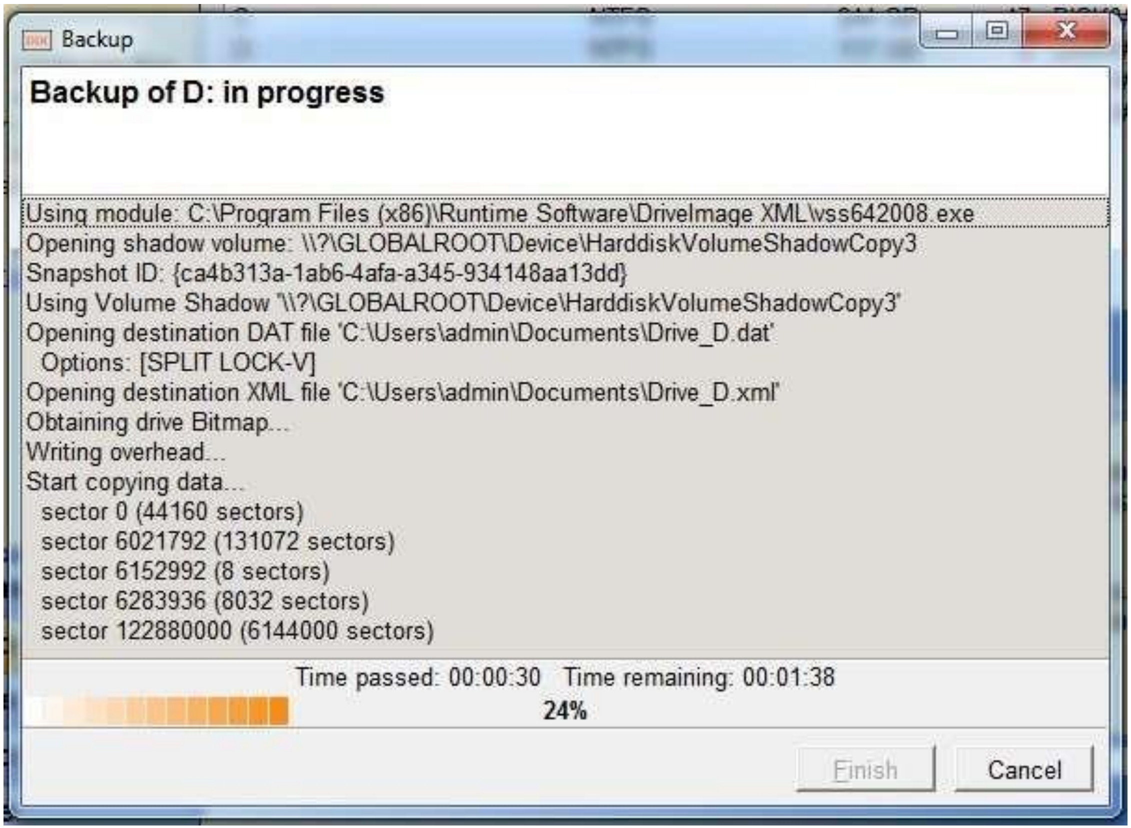
☑ Split large files

Compression: None

Hot Imaging Strategy:

● Try Volume Locking first

○ Try Volume Shadow Services first

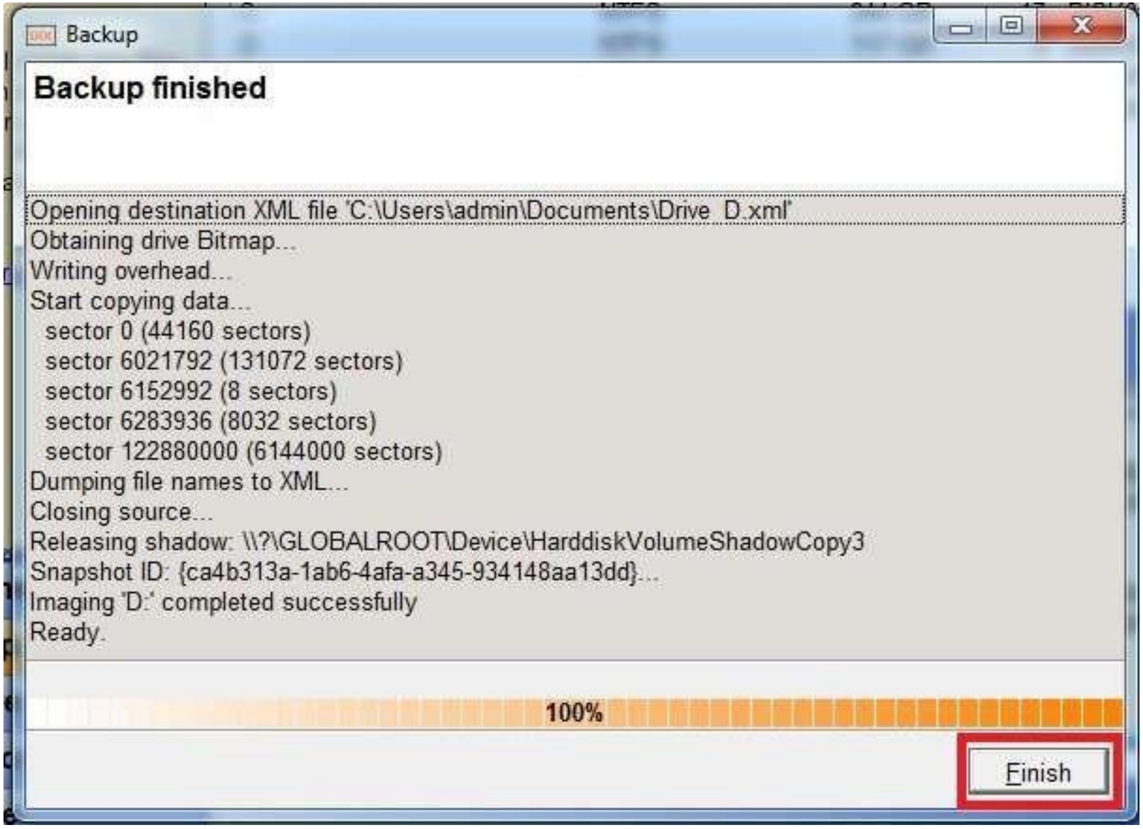


Backup of D: in progress

```
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

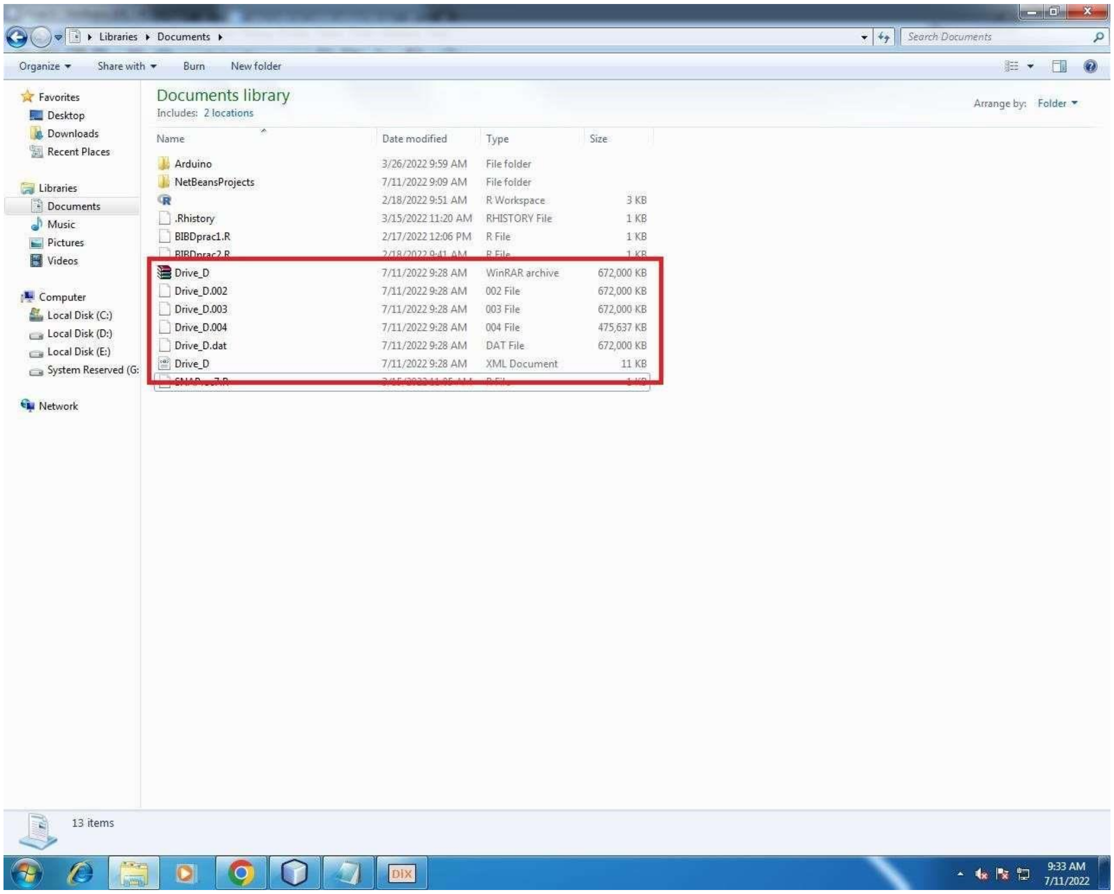
24%



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%



Documents library
Includes: 2 locations

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
BIBDprac2.R	2/18/2022 9:41 AM	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
SNAP[illegible]7.R	3/15/2022 11:05 AM	R File	1 KB

Practical 6

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

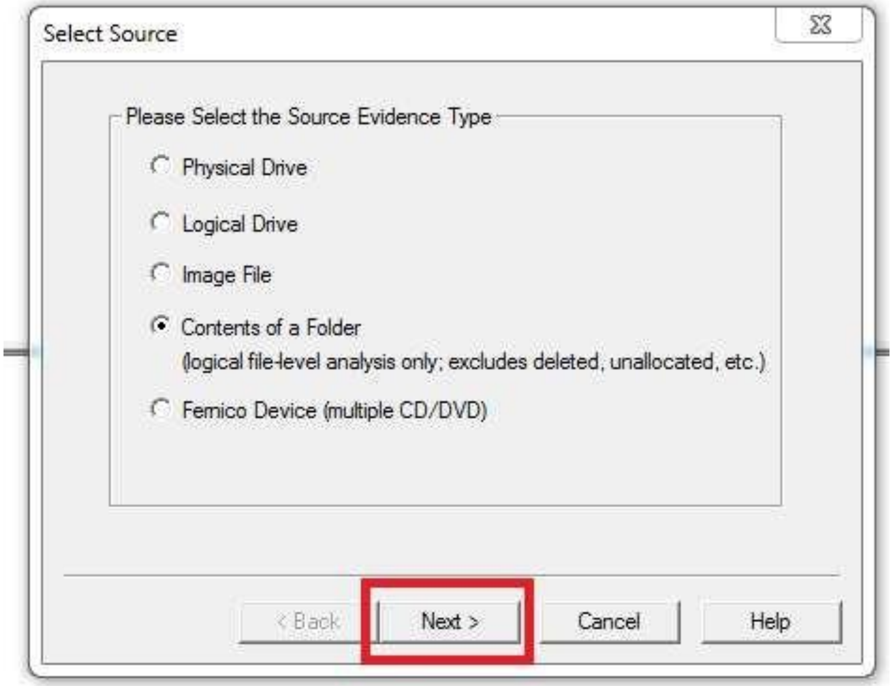
"Create forensic images of digital devices from volatile data such as memory using imager for computer system."

1. Create forensic images: In digital forensics, creating a forensic image means making an exact, bit-for-bit copy of data from a digital device. This process ensures that the original data remains unchanged while allowing forensic experts to analyze the copied data for investigation purposes.
2. Of digital devices: This refers to any electronic device that stores data, such as computers, smartphones, tablets, etc.
3. From volatile data: Volatile data refers to information that is lost when the power is turned off or the device is rebooted. In digital forensics, volatile data typically means the data held in a device's

RAM (Random Access Memory) because it gets erased when the device loses power.

4. Such as memory: Here, “memory” specifically refers to RAM. When investigating a computer system, capturing the contents of RAM is crucial because it can contain valuable information like running processes, open files, network connections, and other data that is lost once the computer is shut down or restarted.
5. Using imager for computer system: An imager is a specialized tool or software used to create a forensic image of a digital device. In the context of volatile data, the imager is used to capture and save the contents of the device’s memory (RAM) before it is lost.

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



Select Source

Please Select the Source Evidence Type

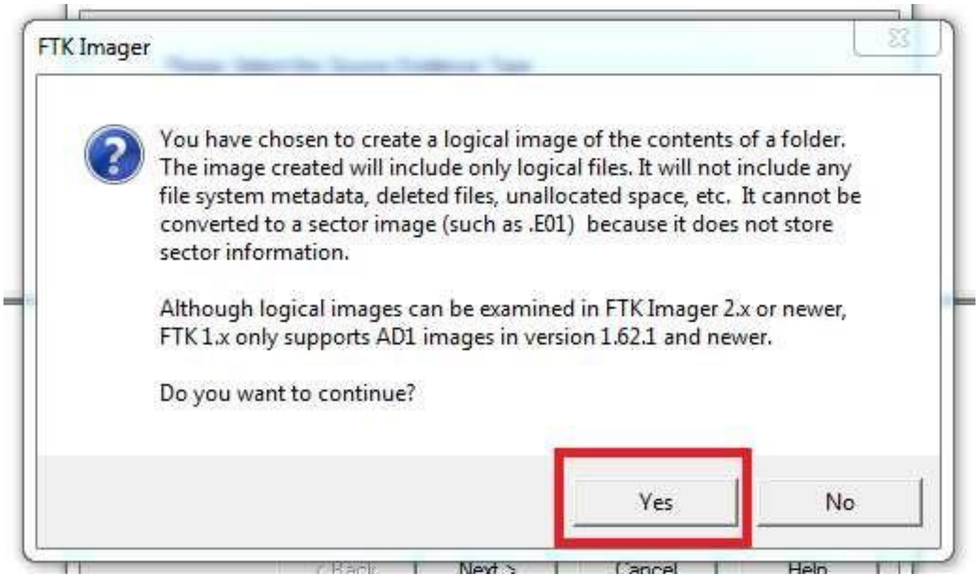
○ Physical Drive

○ Logical Drive

○ Image File

● Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ Fernico Device (multiple CD/DVD)

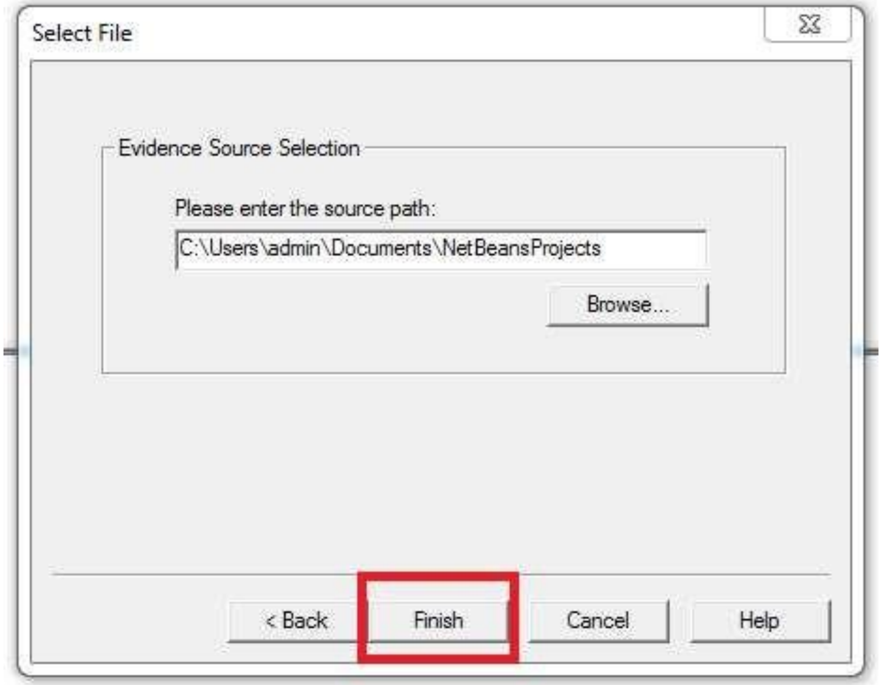


FTK Imager

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

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

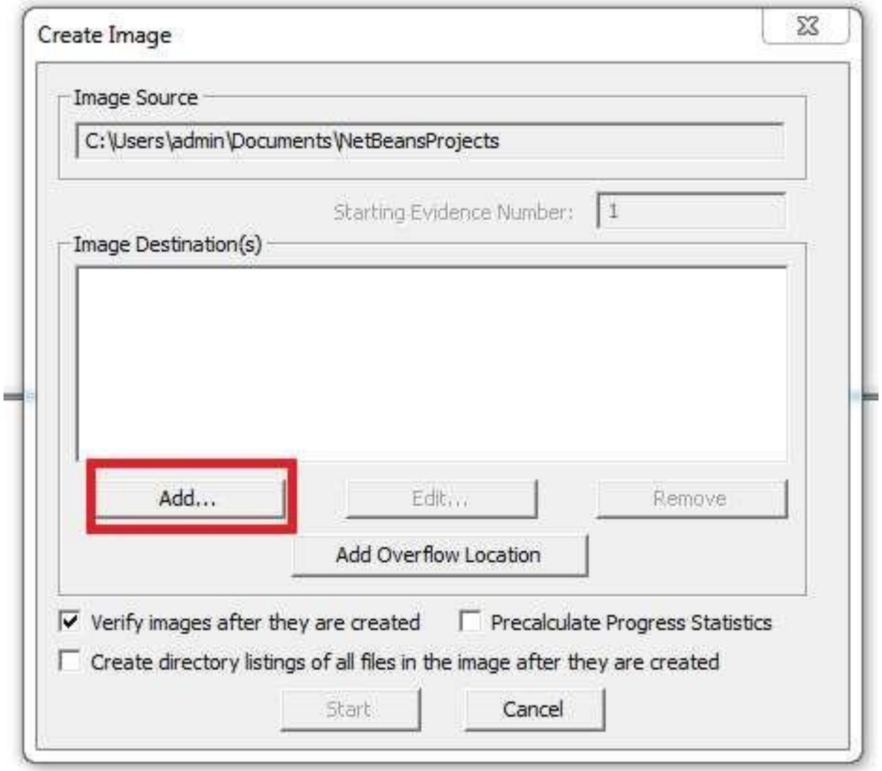
Do you want to continue?



Select File

Evidence Source Selection

Please enter the source path: C:\Users\admin\Documents\NetBeansProjects



Create Image

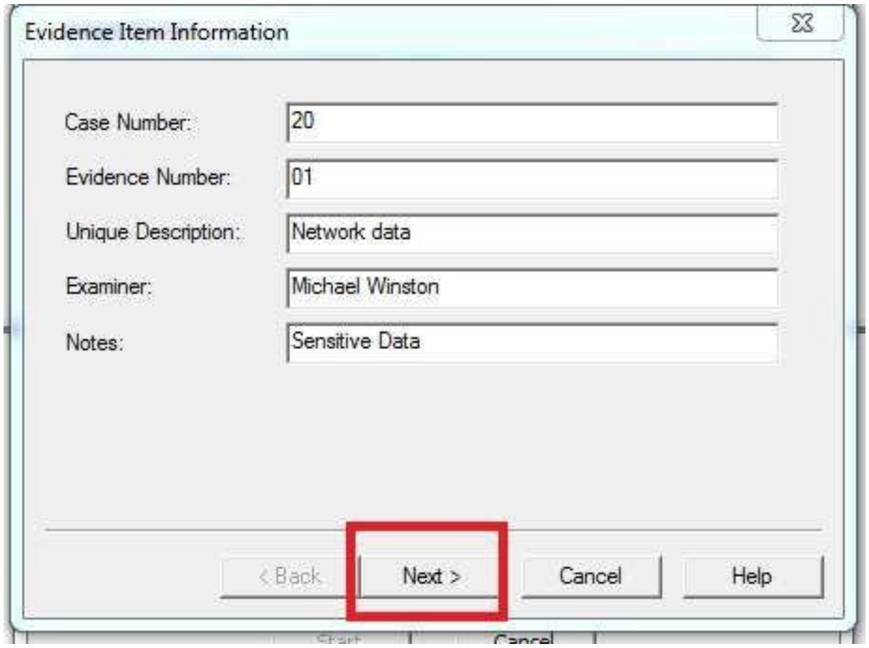
Image Source: C:\Users\admin\Documents\NetBeansProjects

Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created


Evidence Item Information

Case Number: 20

Evidence Number: 01

Unique Description: Network data

Examiner: Michael Winston

Notes: Sensitive Data

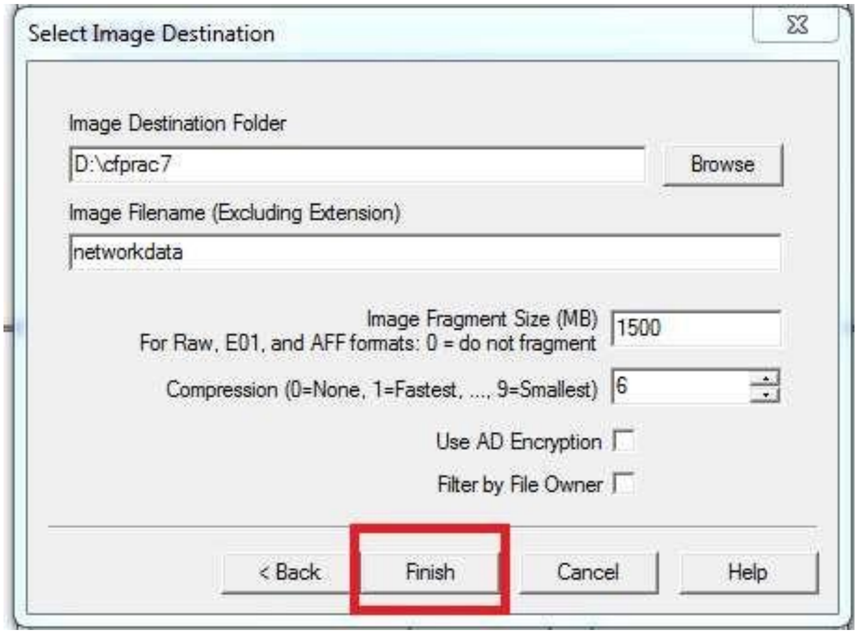

Select Image Destination

Image Destination Folder: D:\cfprac7

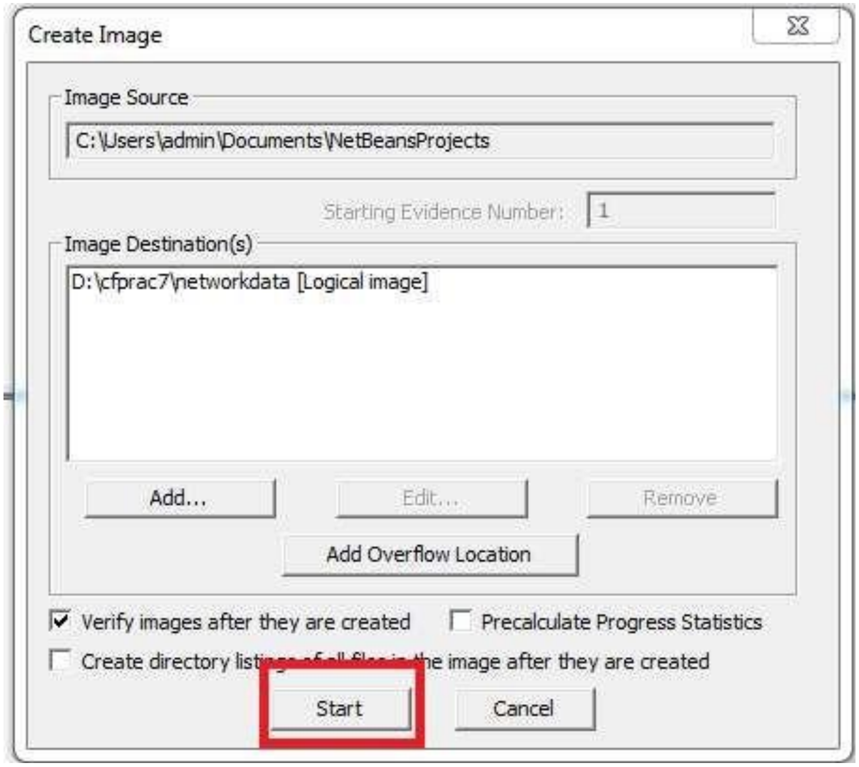
Image Filename (Excluding Extension): networkdata

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 □



Create Image

Image Source: C:\Users\admin\Documents\NetBeansProjects

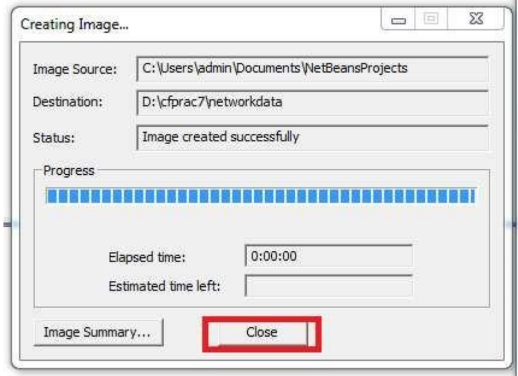
Starting Evidence Number: 1

Image Destination(s): D:\cfprac7\networkdata [Logical image]

☑ Verify images after they are created

☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created



Creating Image...

Image Source: C:\Users\admin\Documents\NetBeansProjects

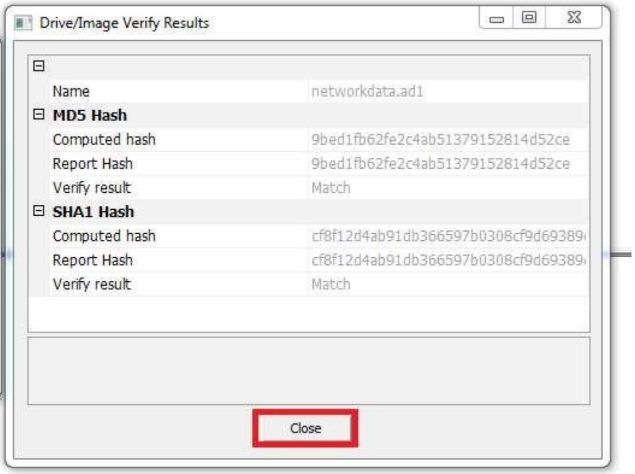
Destination: D:\cfprac7\networkdata

Status: Image created successfully

Progress

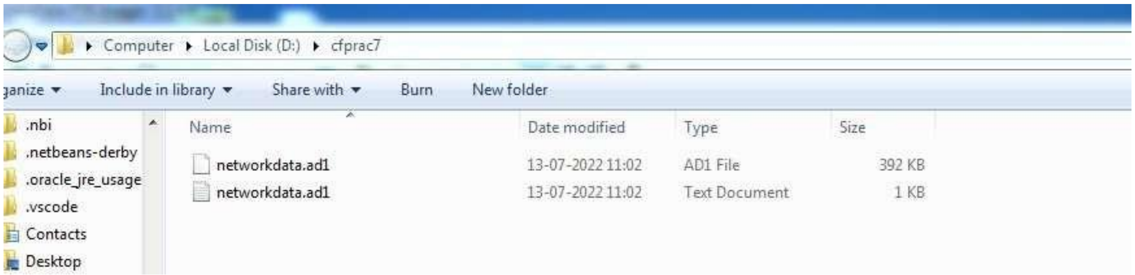
Elapsed time: 0:00:00

Estimated time left:



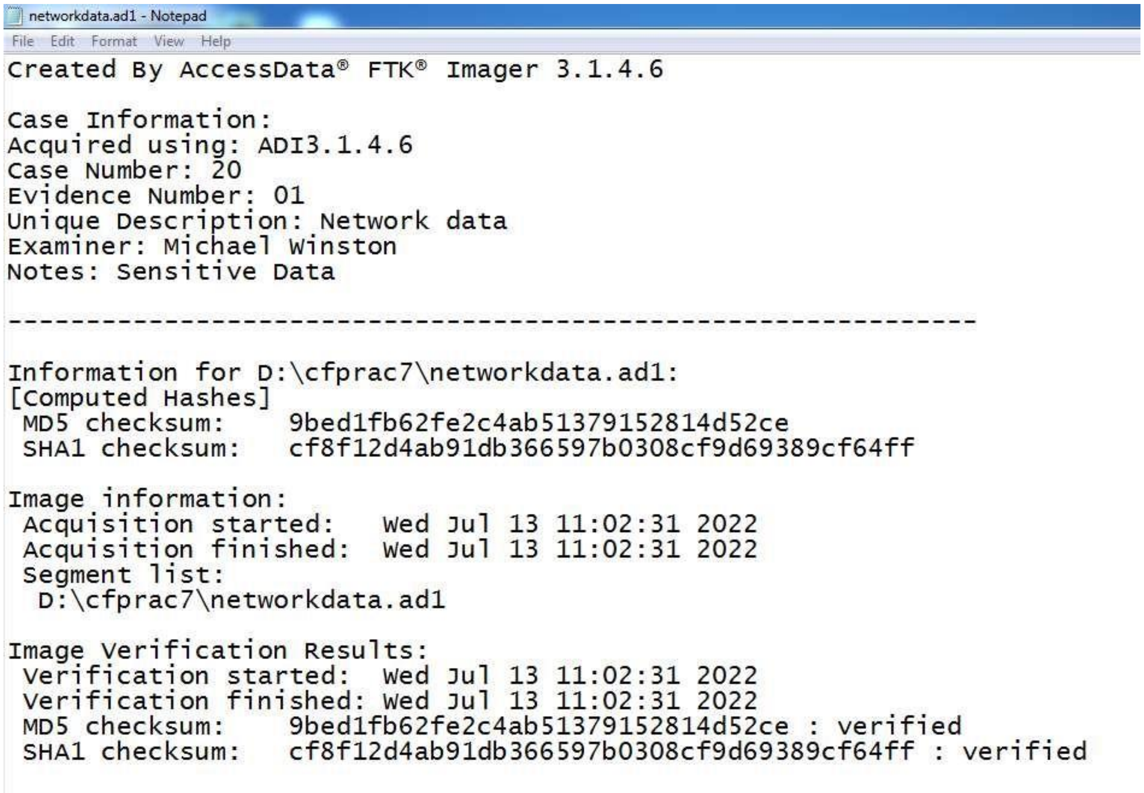
Drive/Image Verify Results

Name	networkdata.ad1
MD5 Hash	
Computed hash	9bed1fb62fe2c4ab51379152814d52ce
Report Hash	9bed1fb62fe2c4ab51379152814d52ce
Verify result	Match
SHA1 Hash	
Computed hash	cf8f12d4ab91db366597b0308cf9d69389
Report Hash	cf8f12d4ab91db366597b0308cf9d69389
Verify result	Match



Computer ▸ Local Disk (D:) ▸ cfprac7

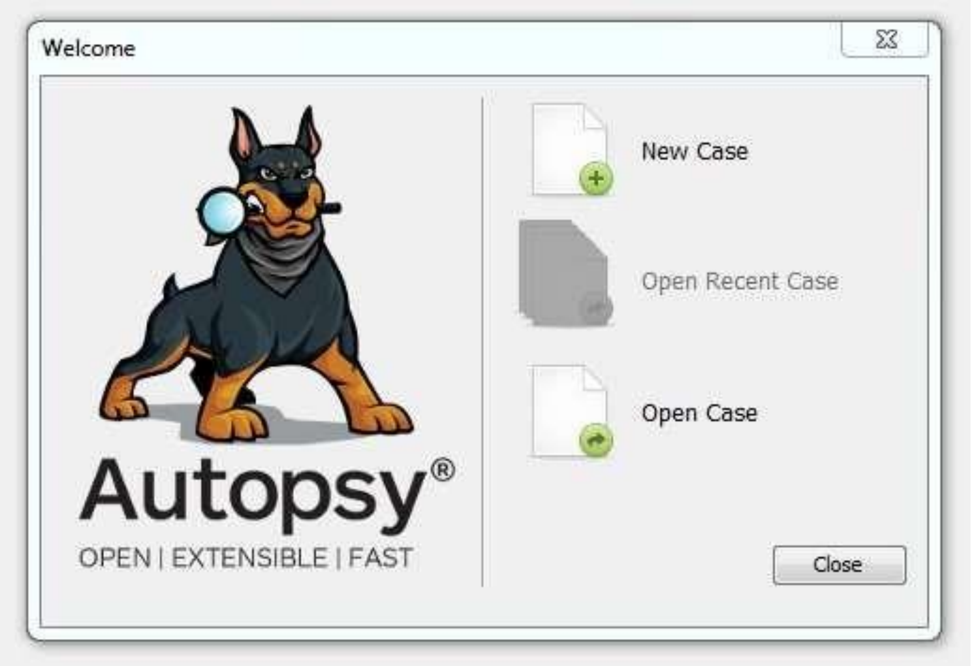
Name	Date modified	Type	Size
networkdata.ad1	13-07-2022 11:02	AD1 File	392 KB
networkdata.ad1	13-07-2022 11:02	Text Document	1 KB

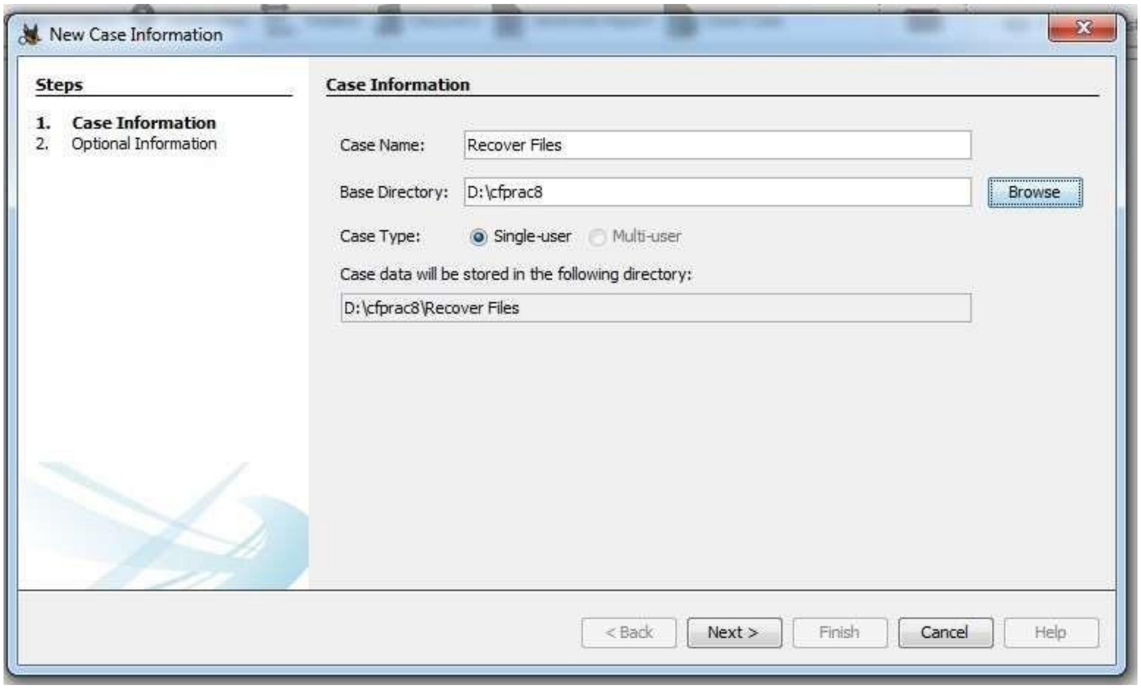


```
Created By AccessData® FTK® Imager 3.1.4.6

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

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

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

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

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

Practical 7

Aim:- Recovering and inspecting deleted files.





New Case Information

Steps

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

Case Information

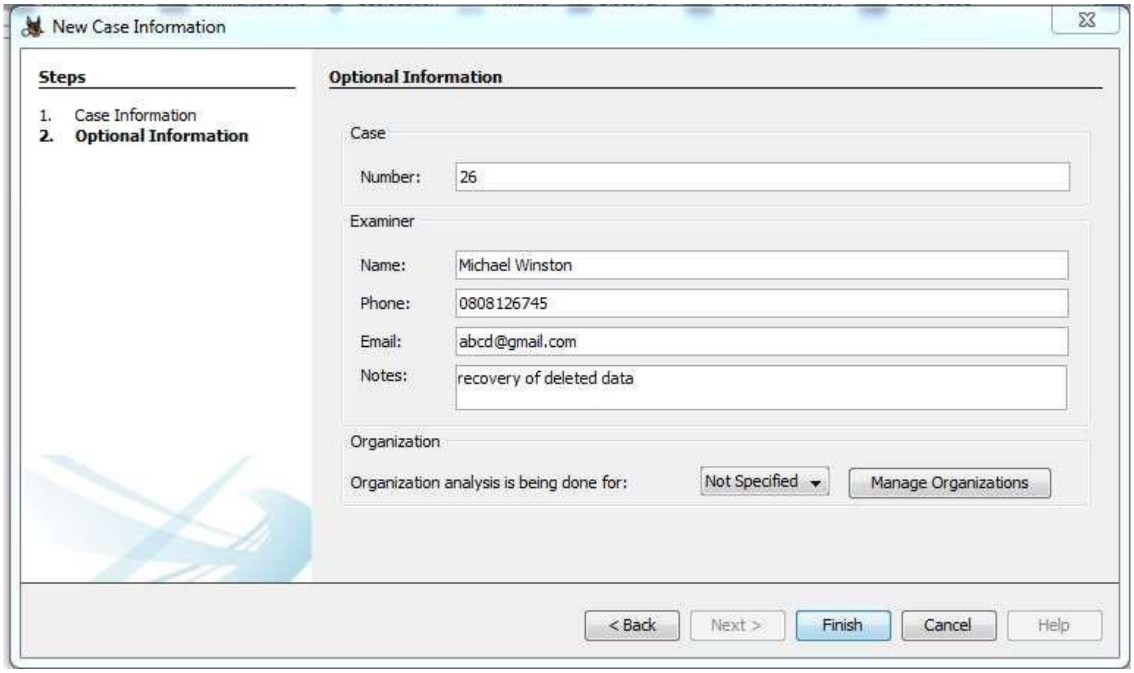
Case Name: Recover Files

Base Directory: D:\cfprac8

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

D:\cfprac8\Recover Files



New Case Information

Steps

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

Optional Information

Case

Number: 26

Examiner

Name: Michael Winston

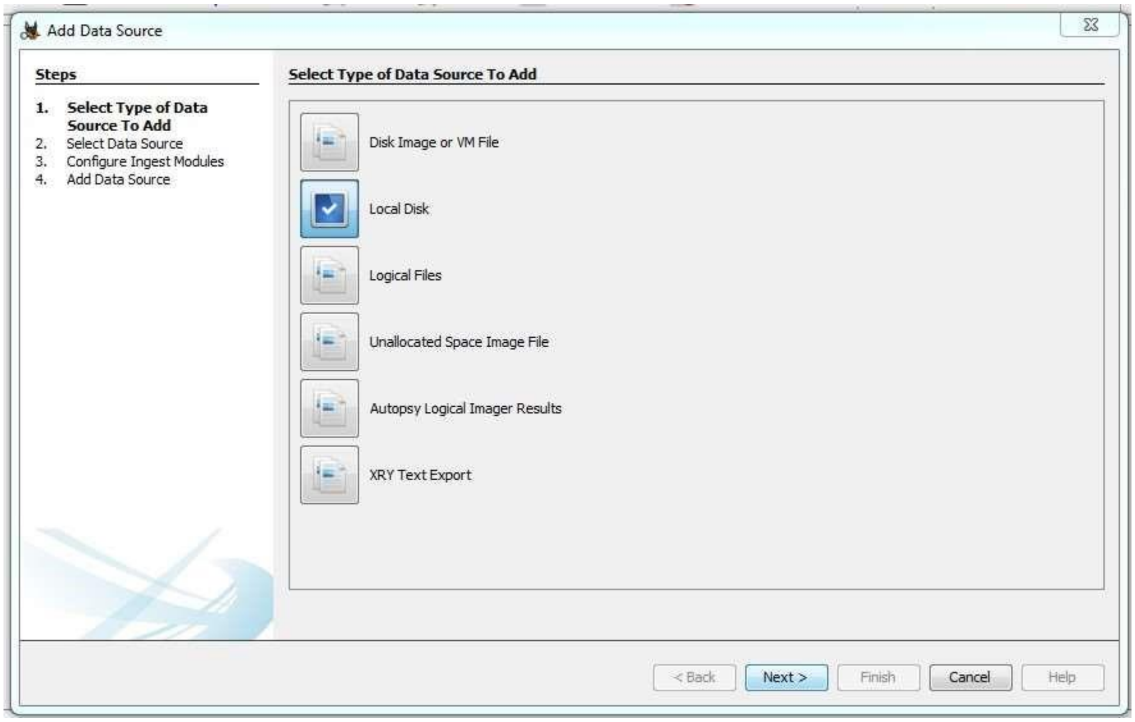
Phone: 0808126745

Email: abcd@gmail.com

Notes: recovery of deleted data

Organization

Organization analysis is being done for: Not Specified



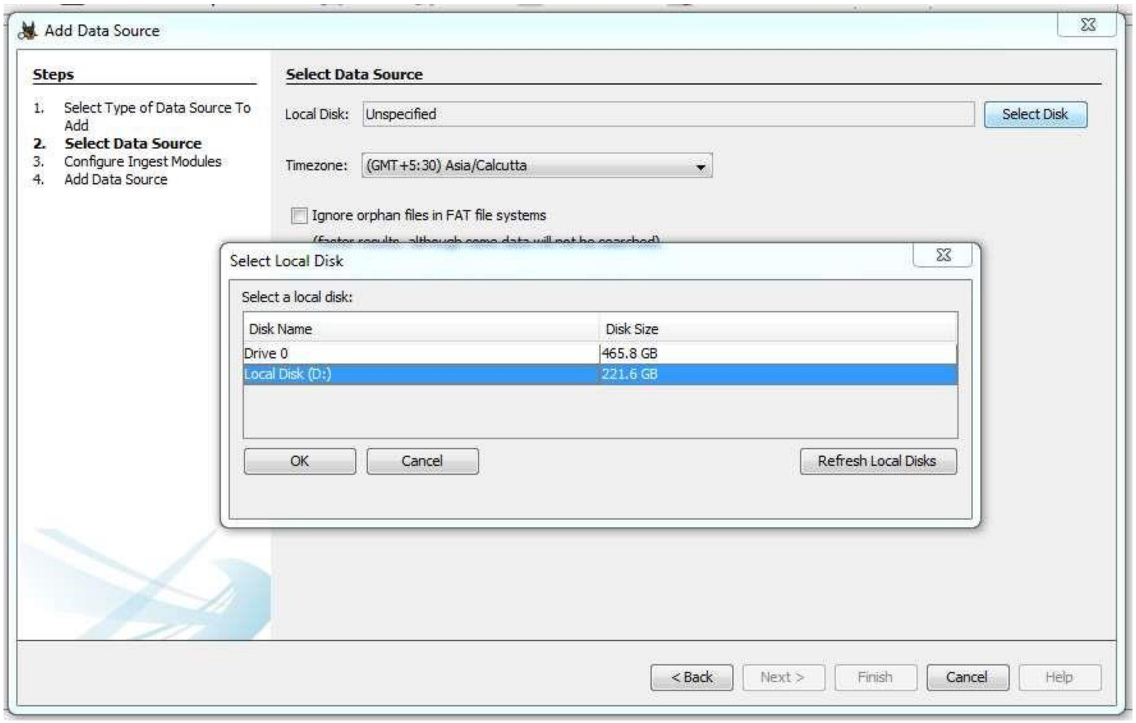
Add Data Source

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



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

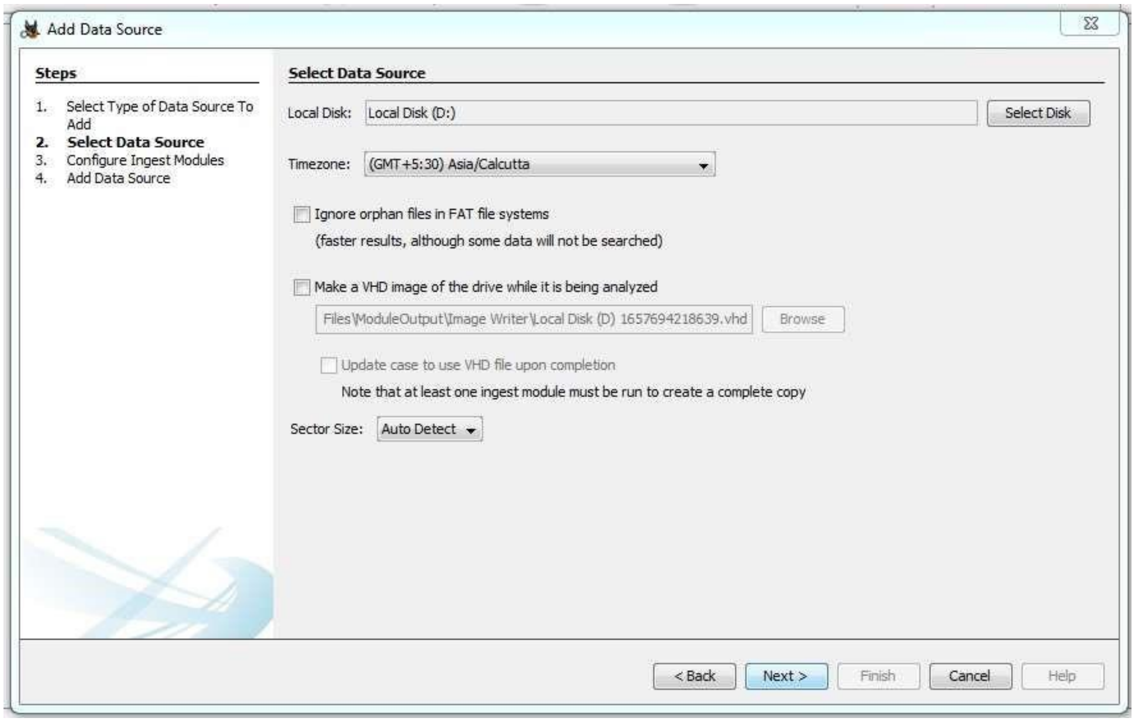
Timezone: (GMT+5:30) Asia/Calcutta

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

Select Local Disk

Select a local disk:

Disk Name	Disk Size
Drive 0	465.8 GB
Local Disk (D:)	221.6 GB



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:)

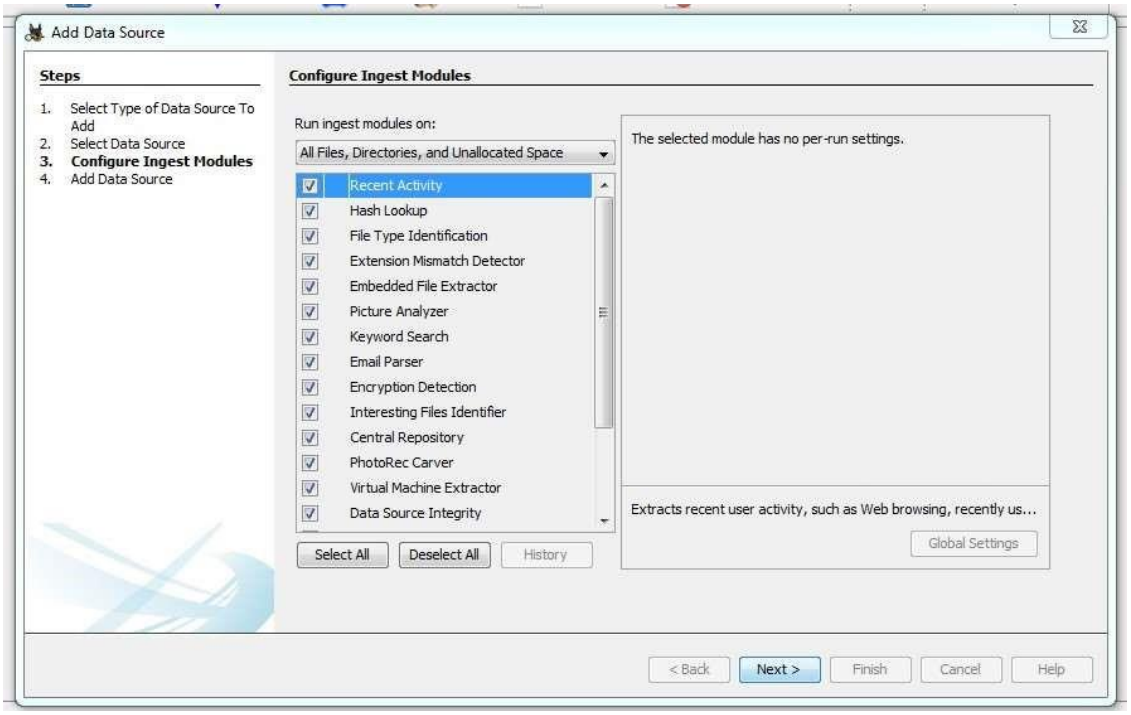
Timezone: (GMT+5:30) Asia/Calcutta

□ 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

□ 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



Add Data Source

Steps

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

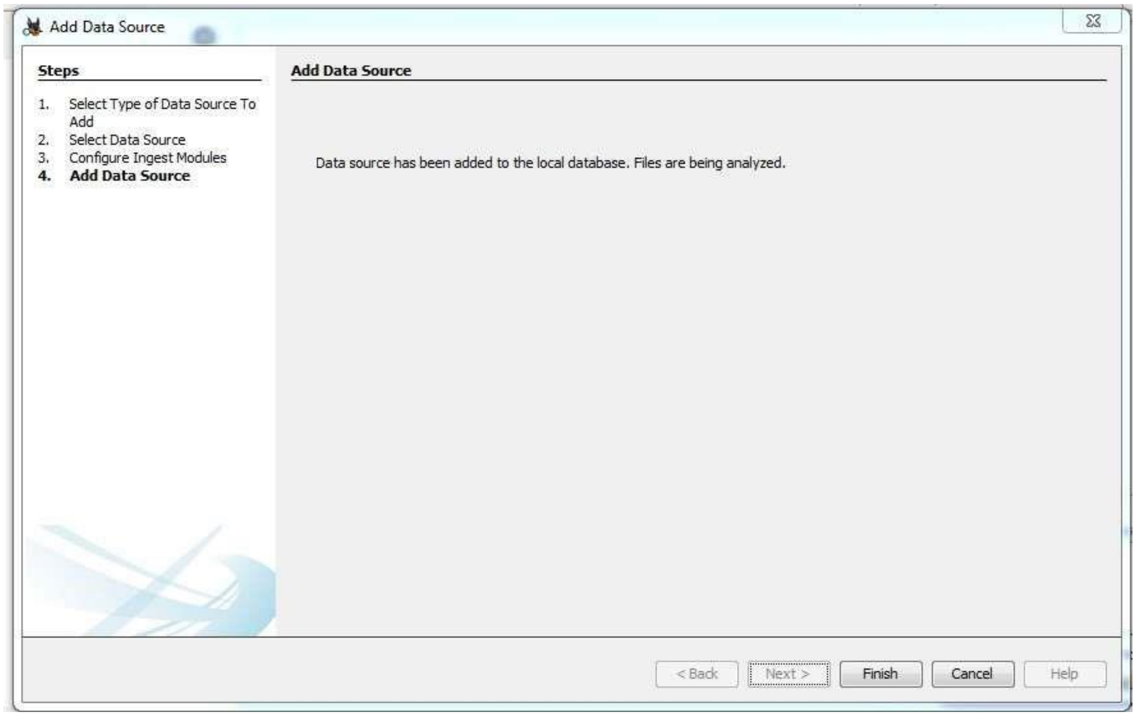
Configure Ingest Modules

Run ingest modules on: All Files, Directories, and Unallocated Space

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

The selected module has no per-run settings.

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

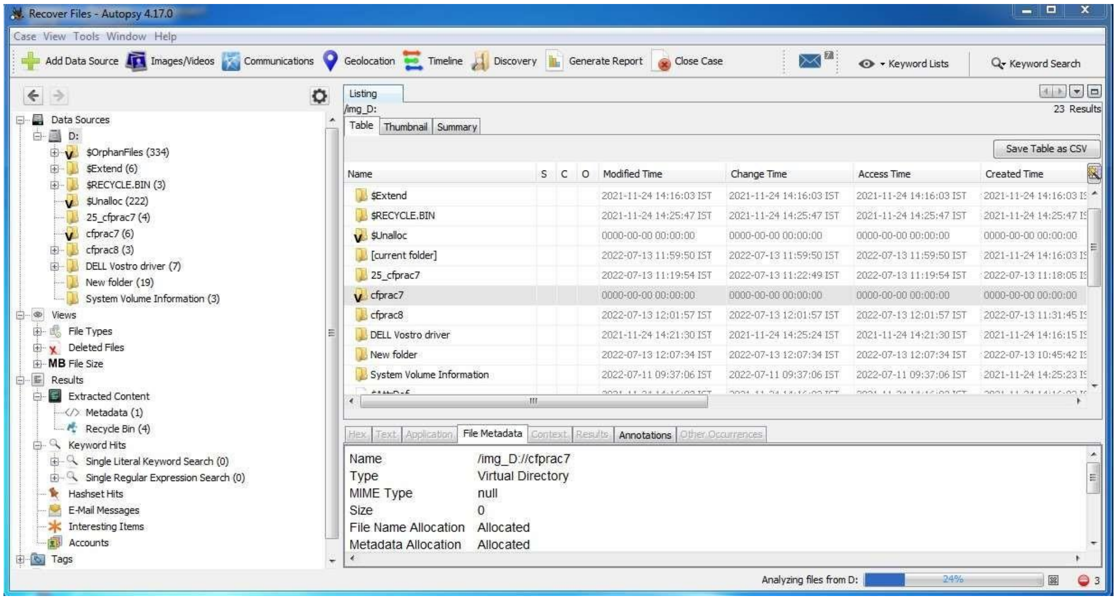


Steps

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.



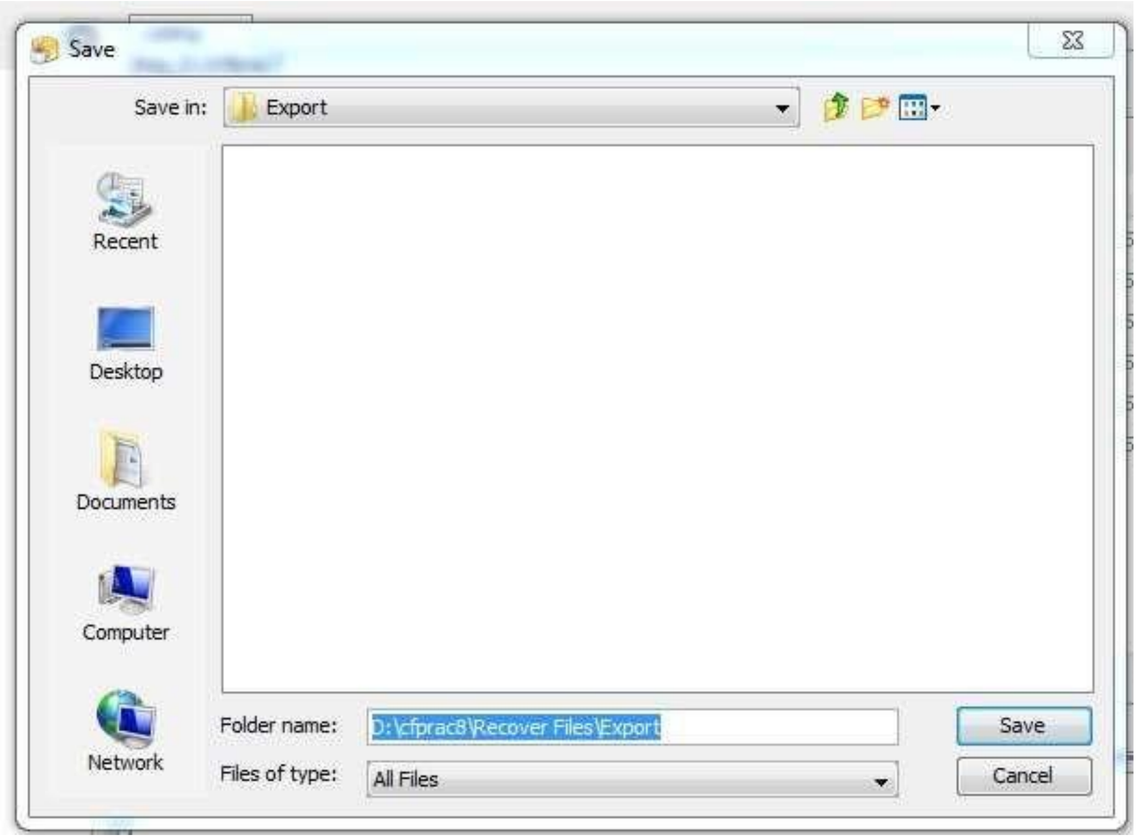
/img_D:

23 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
$Extend				2021-11-24 14:16:03 IST	2021-11-24 14:16:03 IST	2021-11-24 14:16:03 IST	2021-11-24 14:16:03 IS
$RECYCLE.BIN				2021-11-24 14:25:47 IST	2021-11-24 14:25:47 IST	2021-11-24 14:25:47 IST	2021-11-24 14:25:47 IS
$Unalloc				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
[current folder]				2022-07-13 11:59:50 IST	2022-07-13 11:59:50 IST	2022-07-13 11:59:50 IST	2021-11-24 14:16:03 IS
25_cfprac7				2022-07-13 11:19:54 IST	2022-07-13 11:22:49 IST	2022-07-13 11:19:54 IST	2022-07-13 11:18:05 IS
cfprac7				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
cfprac8				2022-07-13 12:01:57 IST	2022-07-13 12:01:57 IST	2022-07-13 12:01:57 IST	2022-07-13 11:31:45 IS
DELL Vostro driver				2021-11-24 14:21:30 IST	2021-11-24 14:25:24 IST	2021-11-24 14:21:30 IST	2021-11-24 14:16:15 IS
New folder				2022-07-13 12:07:34 IST	2022-07-13 12:07:34 IST	2022-07-13 12:07:34 IST	2022-07-13 10:45:42 IS
System Volume Information				2022-07-11 09:37:06 IST	2022-07-11 09:37:06 IST	2022-07-11 09:37:06 IST	2021-11-24 14:25:23 IS

Name	/img_D://cfprac7
Type	Virtual Directory
MIME Type	null
Size	0
File Name Allocation	Allocated
Metadata Allocation	Allocated

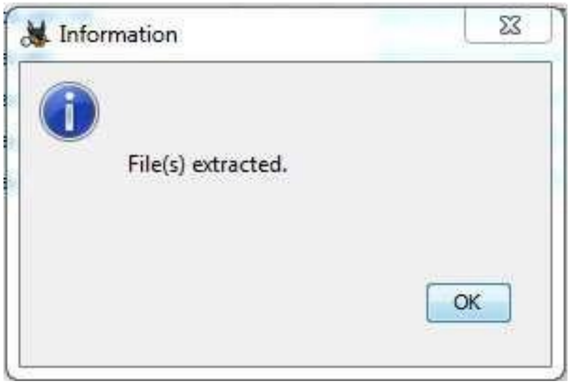
Analyzing files from D: 24%



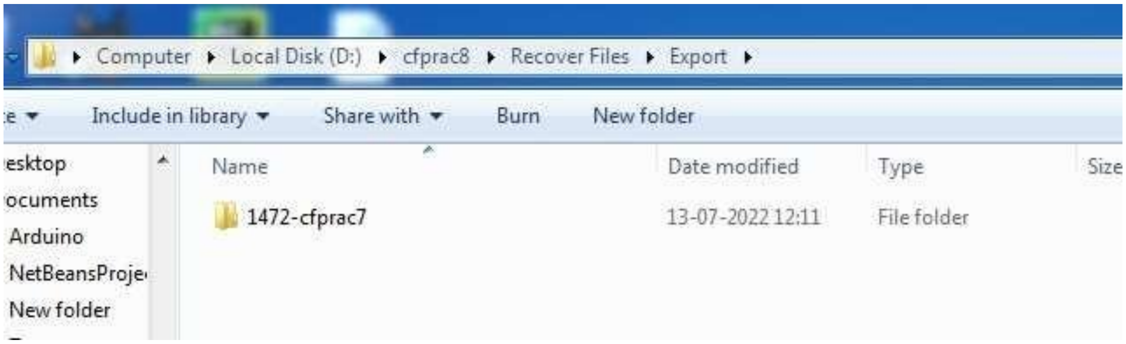
Save in: Export

Folder name: D:\cfprac8\Recover Files\Export

Files of type: All Files

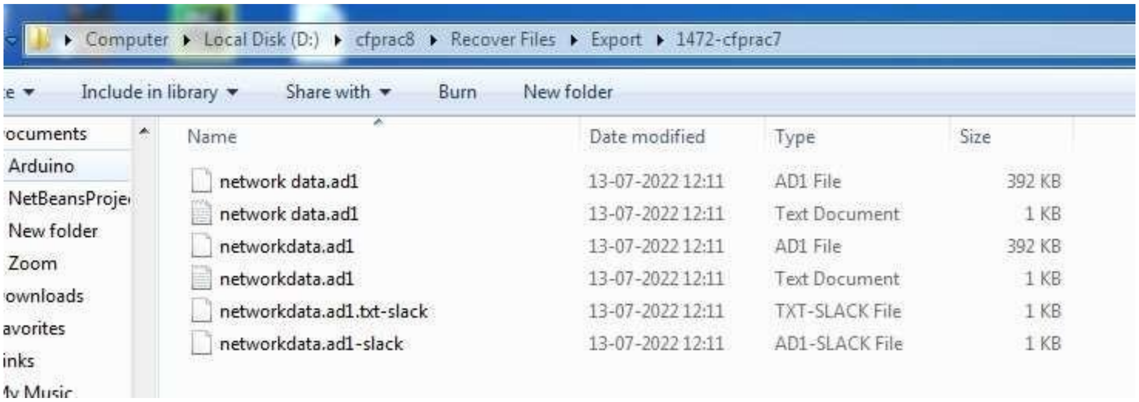


File(s) extracted.

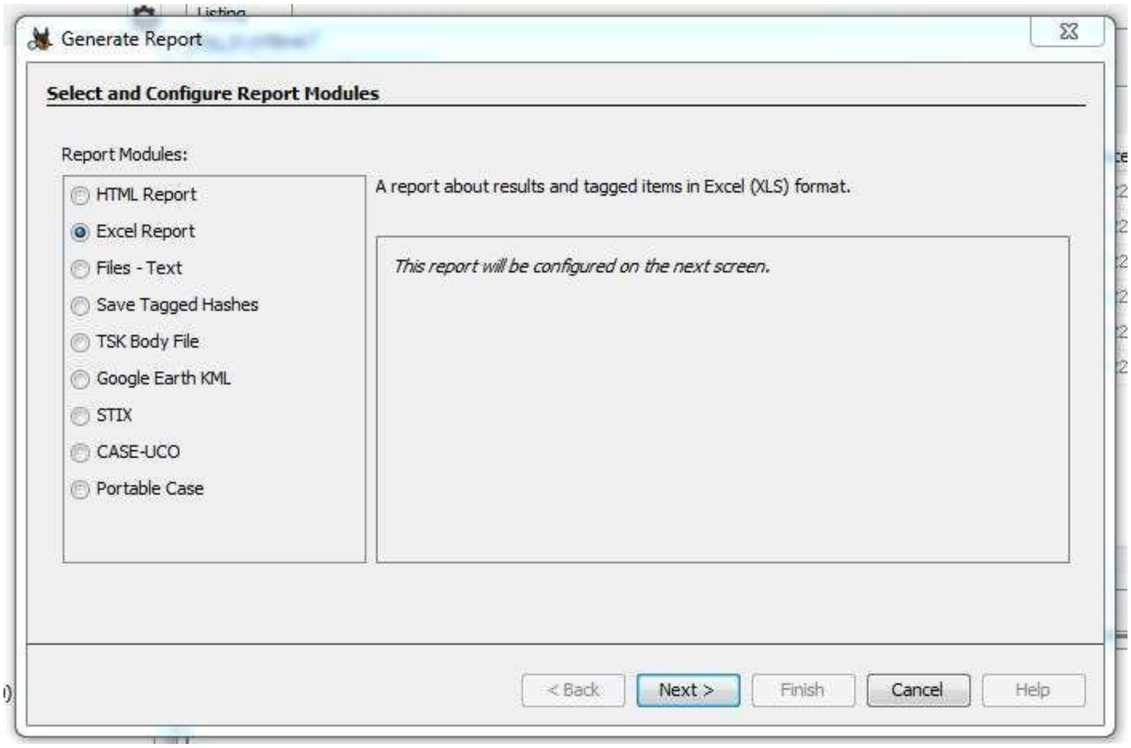


▸ Computer ▸ Local Disk (D:) ▸ cfprac8 ▸ Recover Files ▸ Export ▸

Name	Date modified	Type	Size
1472-cfprac7	13-07-2022 12:11	File folder	



Name	Date modified	Type	Size
network data.ad1	13-07-2022 12:11	AD1 File	392 KB
network data.ad1	13-07-2022 12:11	Text Document	1 KB
networkdata.ad1	13-07-2022 12:11	AD1 File	392 KB
networkdata.ad1	13-07-2022 12:11	Text Document	1 KB
networkdata.ad1.txt-slack	13-07-2022 12:11	TXT-SLACK File	1 KB
networkdata.ad1-slack	13-07-2022 12:11	AD1-SLACK File	1 KB


Generate Report

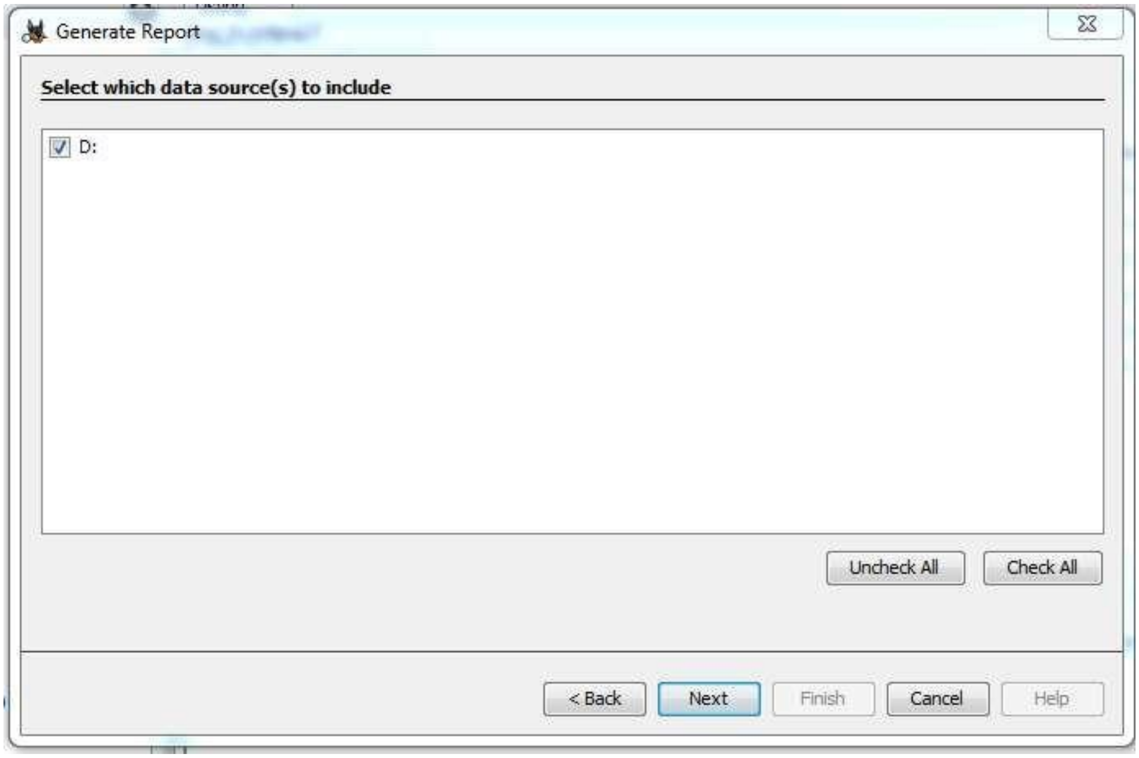
Select and Configure Report Modules

Report Modules:

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

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

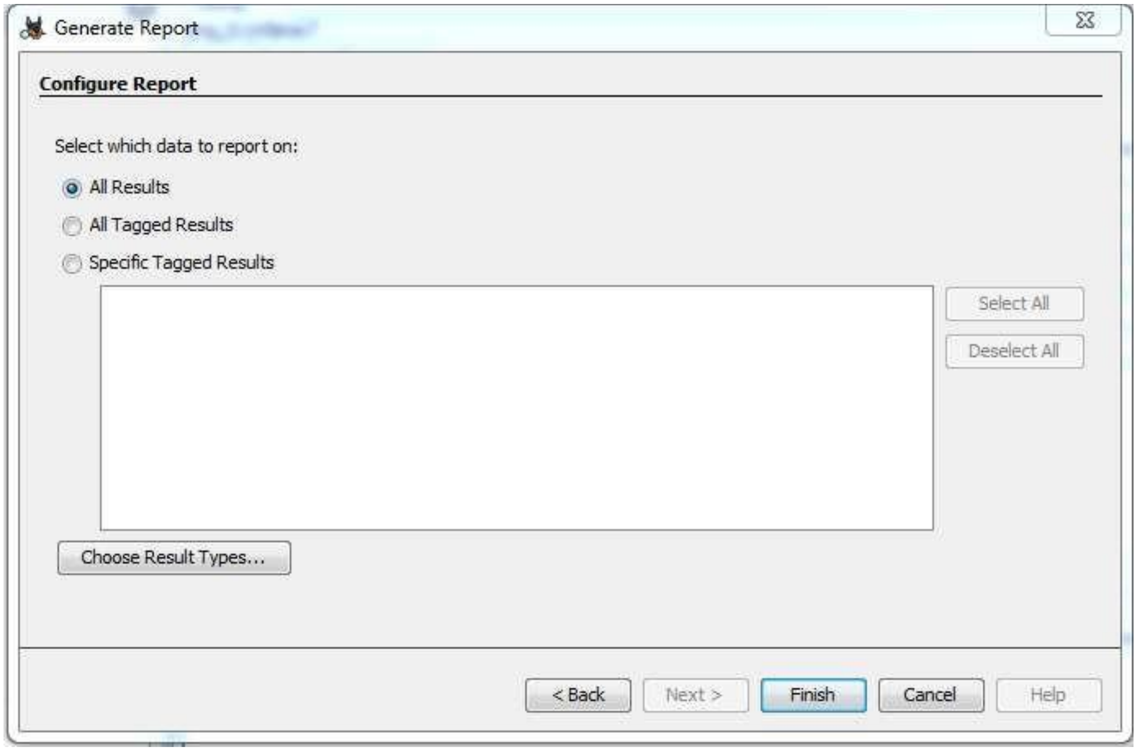
This report will be configured on the next screen.



Generate Report

Select which data source(s) to include

☑ D:



Generate Report

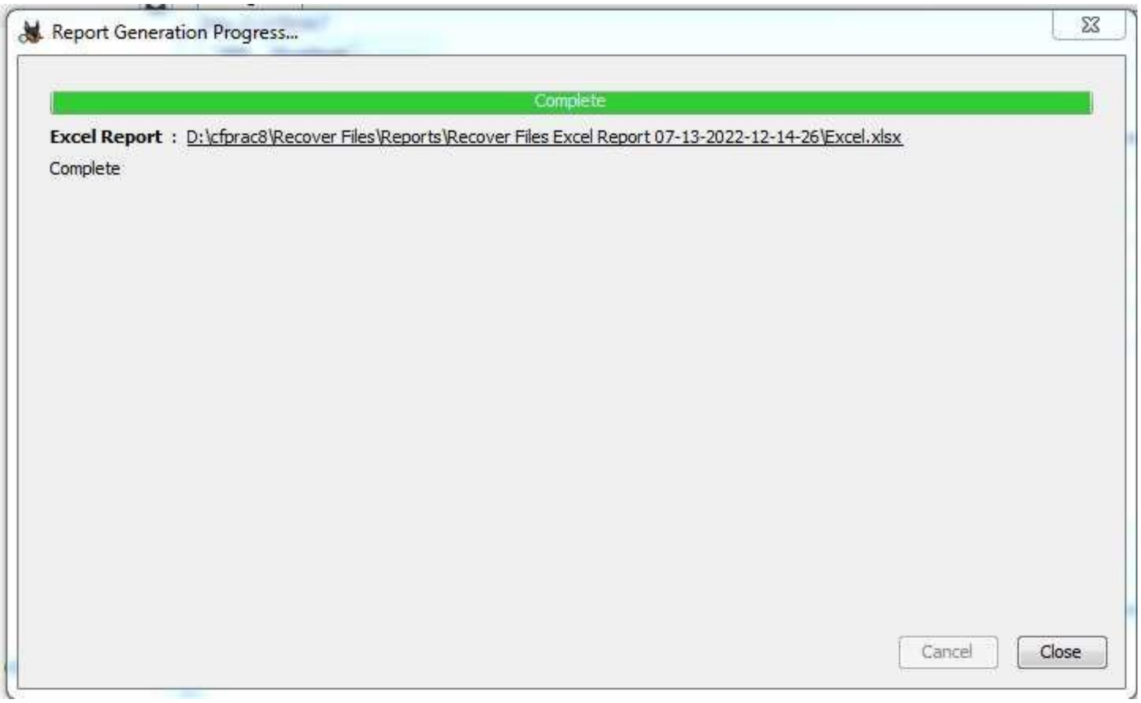
Configure Report

Select which data to report on:

● All Results

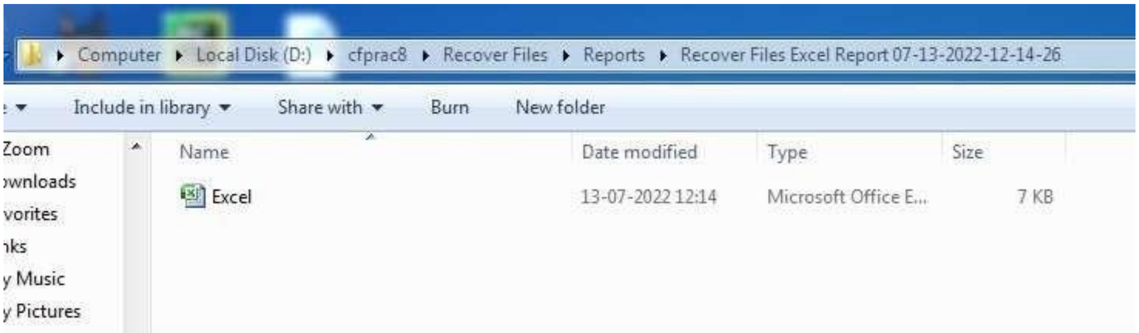
○ All Tagged Results

○ Specific Tagged Results

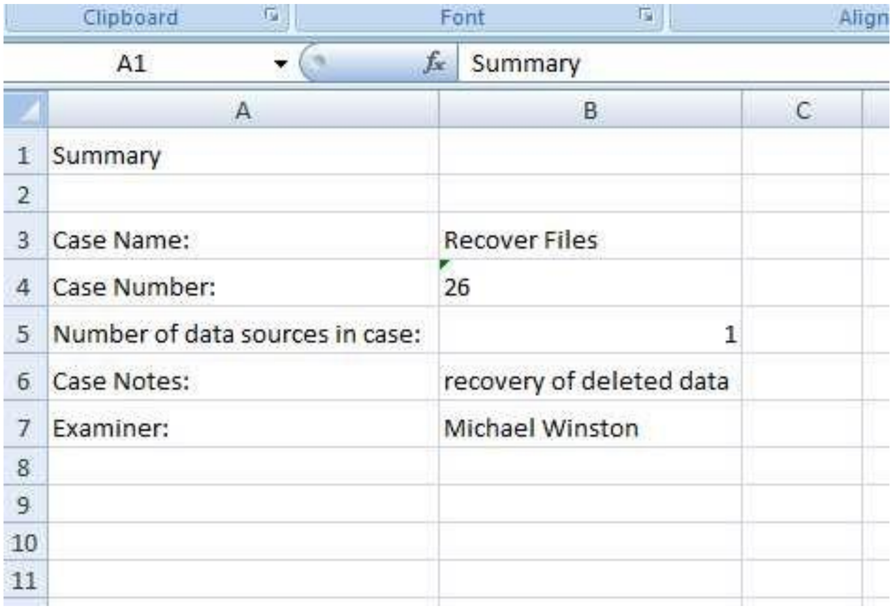


Excel Report : D:\cfprac8\Recover Files\Reports\Recover Files Excel Report 07-13-2022-12-14-26\Excel.xlsx

Complete


Computer ▸ Local Disk (D:) ▸ cfprac8 ▸ Recover Files ▸ Reports ▸ Recover Files Excel Report 07-13-2022-12-14-26
Include in library ▾
Share with ▾
Burn
New folder
Zoom
ownloads
vorites
nks
y Music
y Pictures

Name	Date modified	Type	Size
Excel	13-07-2022 12:14	Microsoft Office E...	7 KB



	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			