Practical One

Reciever

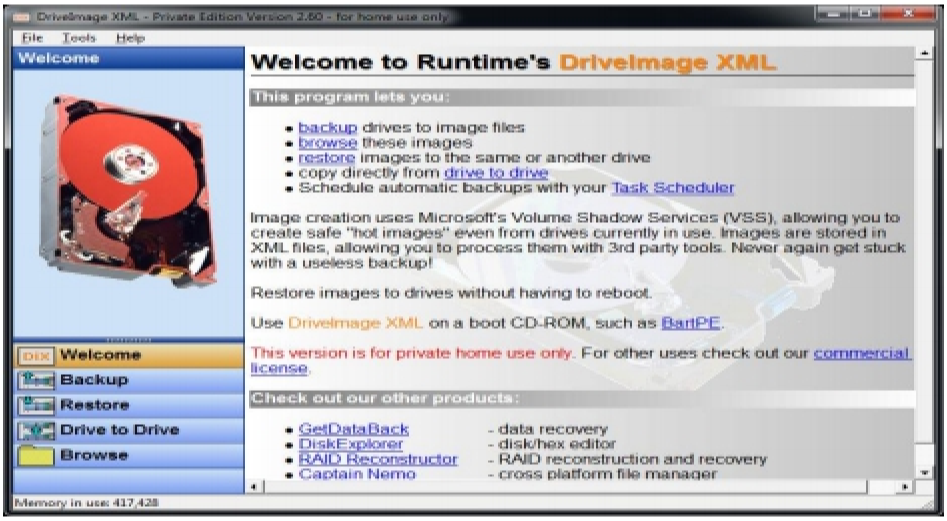
```
package practicall.one;

import java.io.*;
import java.net.*;


public class Receiver {
	public static void main(String[] args) throws Exception {
		String ct="",pt="";
		ServerSocket skt=new ServerSocket(6017);
		Socket sc=skt.accept();
		int i=0;
		System.out.println("Entered 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);
	}
}
```

Sender.java

```
package practicall.one;

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);
		System.out.println(ct);
		bw.write(ct + "," + key);
		bw.flush();
		bw.close();
	}

}
```

Practical Four

Aim: Use DriveImageXML 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!

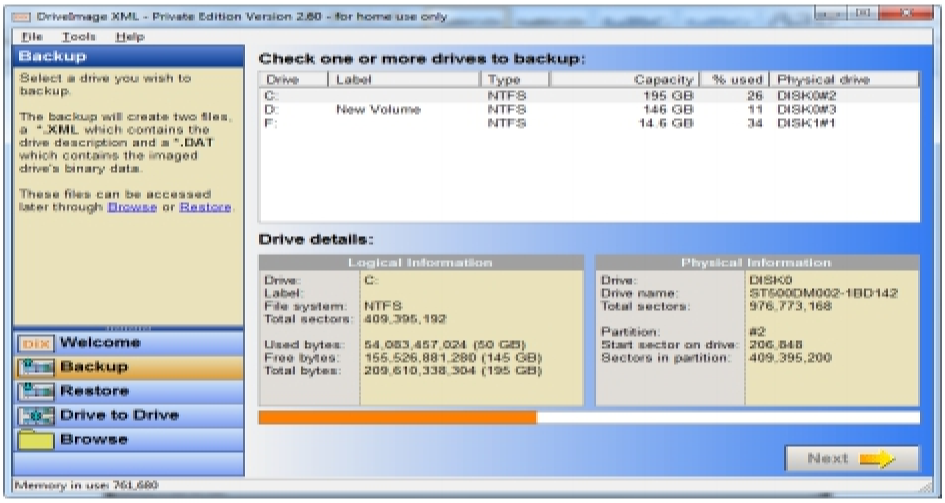
Restore images to drives without having to reboot.

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.

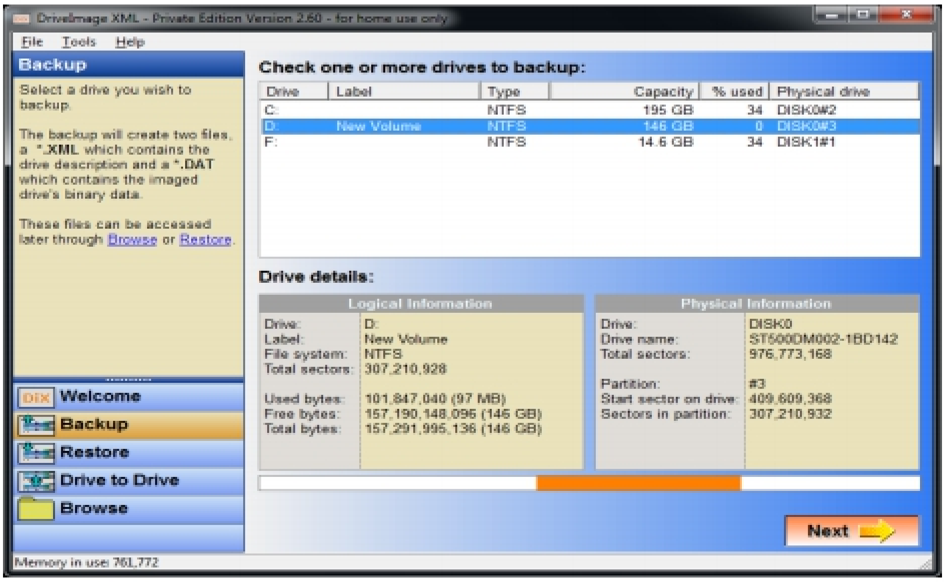
Check one or more drives to backup:

Drive	Label	Type	Capacity	% used	Physical drive
C:		NTFS	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


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.

Welcome
Backup
Restore
Drive to Drive
Browse

Check one or more drives to backup:

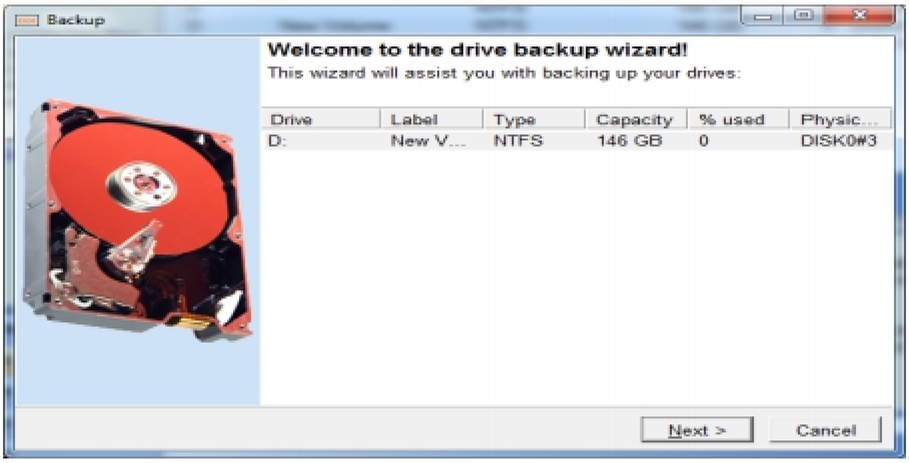
Drive	Label	Type	Capacity	% used	Physical drive
C:		NTFS	195 GB	34	DISK0#2
D:	New Volume	NTFS	146 GB	0	DISK0#3
F:		NTFS	14.6 GB	34	DISK1#1

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

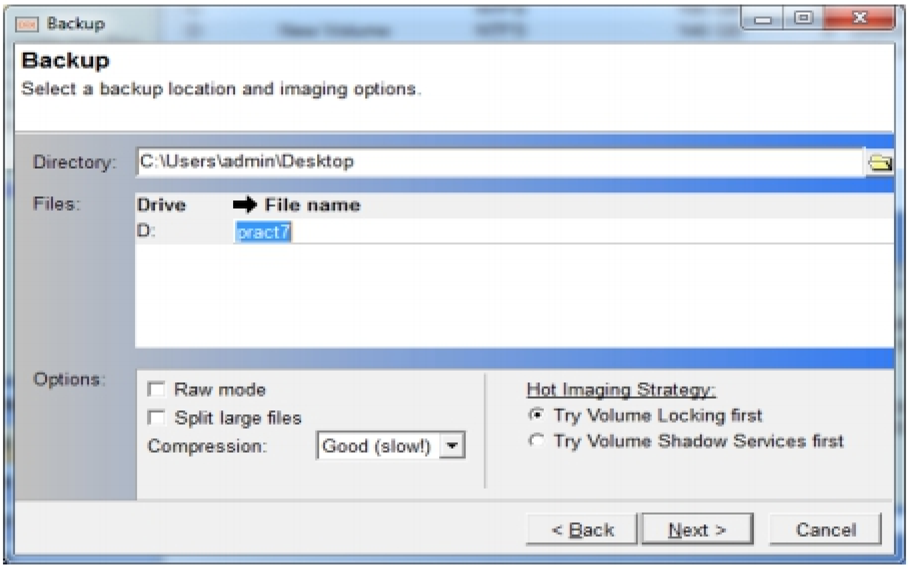
Memory in use: 761,772



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

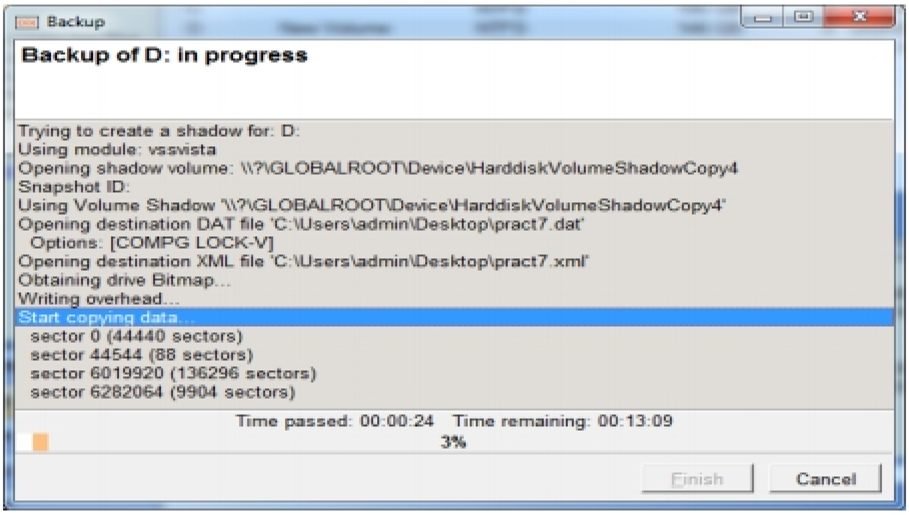
□ Split large files

Compression: Good (slow!)

Hot Imaging Strategy:

● Try Volume Locking first

○ Try Volume Shadow Services first

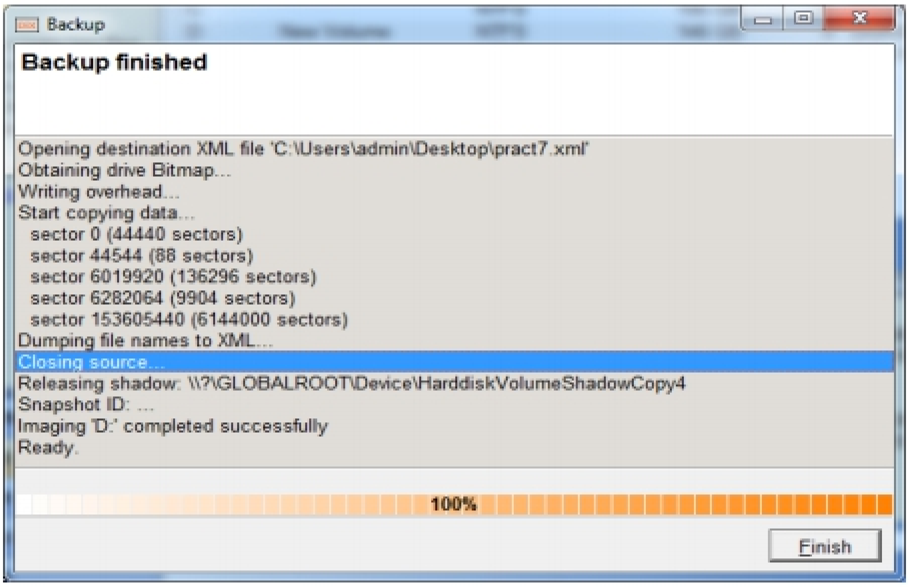


Backup of D: in progress

```
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

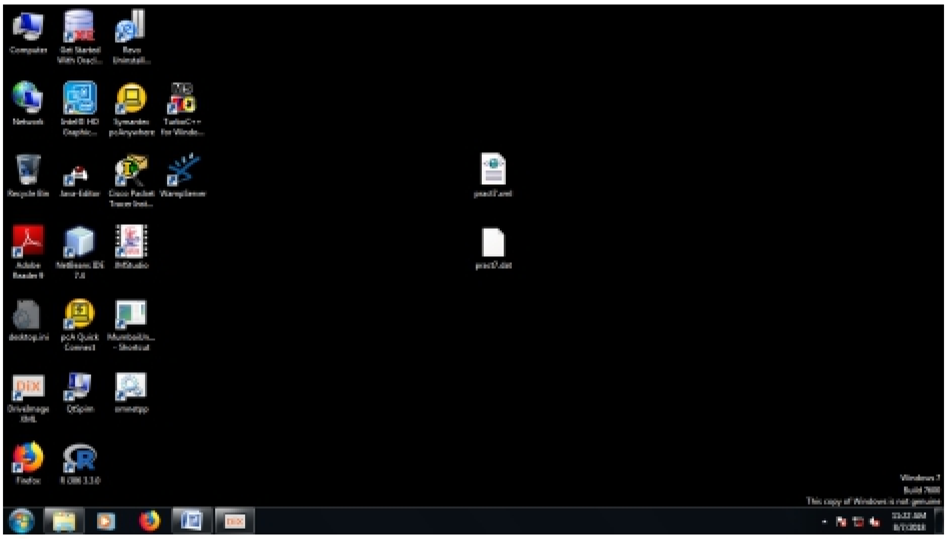
3%



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.
```

100%



Practical Five

Logger.java

```
package practical.five;

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

public class mylogger {

	public static void main(String[] args) throws IOException {

Logger l=Logger.getLogger(mylogger.class.getName());
FileHandler fh;
try
{
fh=new FileHandler("c:/users/ankur/desktop/mylogfile.log",true);
l.addHandler(fh);
l.setLevel(Level.ALL);
SimpleFormatter sf=new SimpleFormatter();
fh.setFormatter(sf);
l.info("My first log");
}
catch(IOException e)
{
e.printStackTrace();
}

l.info("Hi How r u?");
}

}
```

Practical Six

File Search

```
package practical.six;

import java.io.*;


public class FileSearch {
public static void main(String[] args) throws IOException {
String d="";
final String f;
BufferedReader br=new BufferedReader(new InputStreamReader(System.in));
System.out.println("Enter the directory ");
d=br.readLine();
System.out.println("Enter the filter");
f=br.readLine();
File dir=new File(d);
FilenameFilter filter=new FilenameFilter(){
@Override
public boolean accept(File dir,String name){
return name.startsWith(f);
}
};
String[] children=dir.list(filter);
if(children==null){
System.out.println("Not found");
}else{
for(int i=0;i<children.length;i++){
String filename=children[i];
System.out.println(filename);
 }
 }
 }

}
```

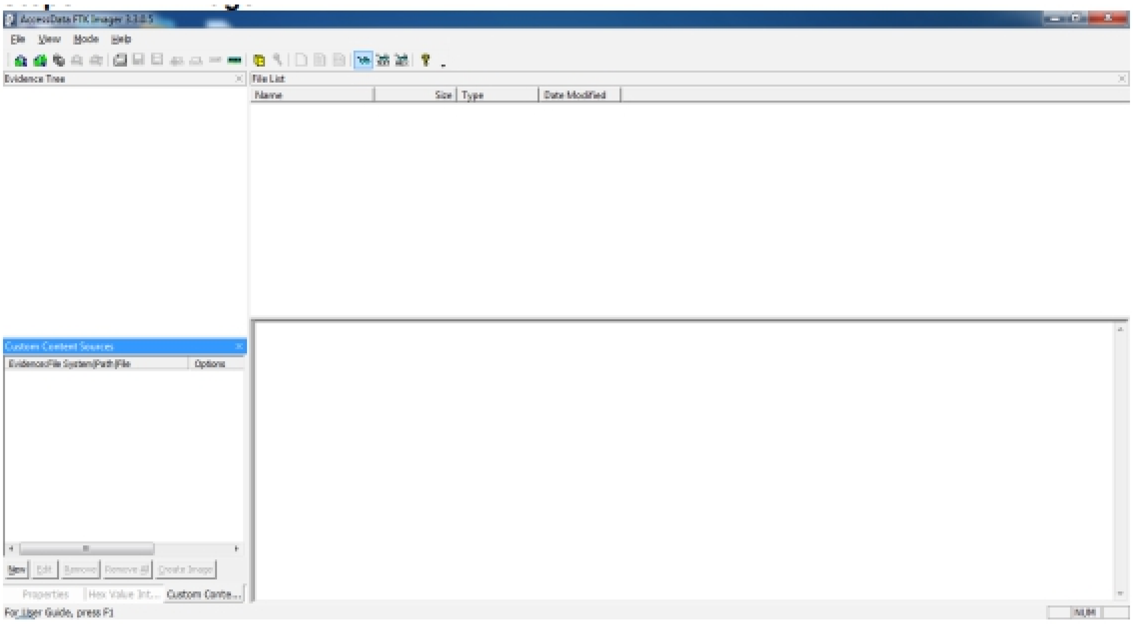
Practical Seven

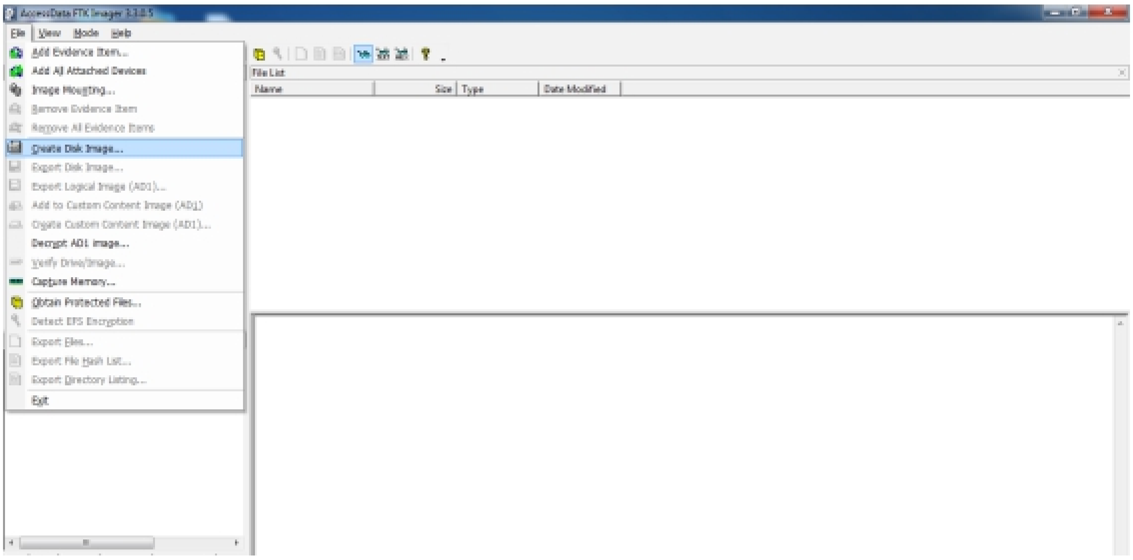
Search Word

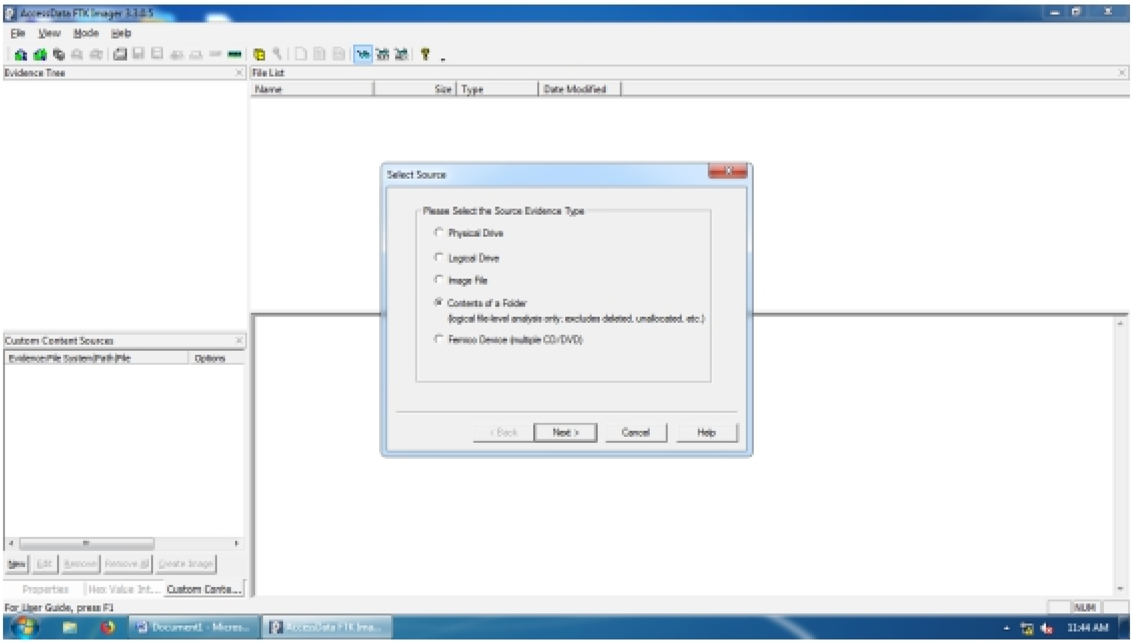
```
package practical.seven;

import java.io.BufferedReader;
import java.io.FileReader;
import java.io.InputStreamReader;

public class SearchWord {
public static void main(String[] args) {

  try
  {
  String str="";
  String ser="";
int flag=0;
BufferedReader br=new BufferedReader(new FileReader("C:\\Users\\ankur\\Desktop\\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);
  }
  }
}
```

Practical Eight

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







Select Source

Please Select the Source Evidence Type

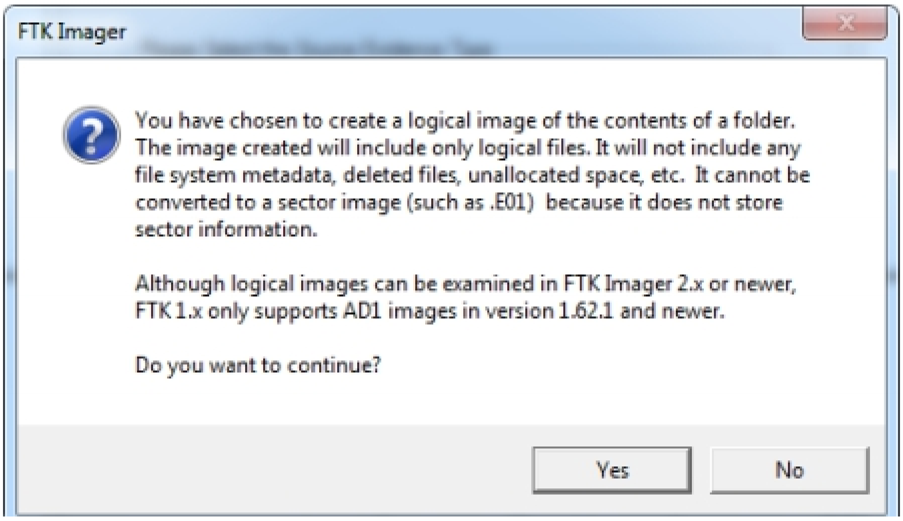
○ Physical Drive

○ Logical Drive

○ Image File

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

○ Fernico Device (multiple CD/DVD)

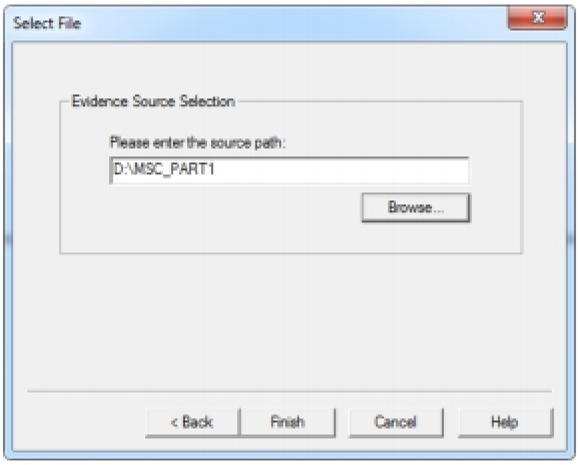


FTK Imager

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?



Please enter the source path: D:\MSC_PART1

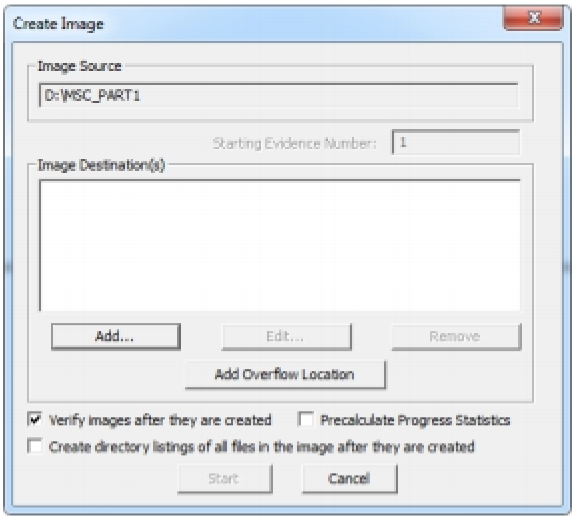


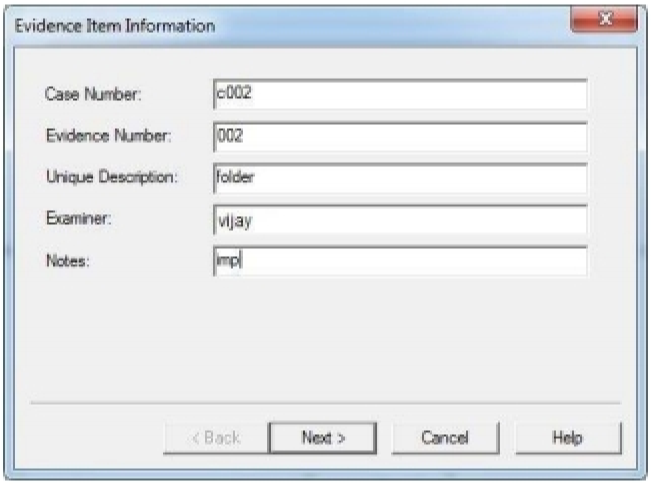
Image Source: D:\MSC_PART1

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


Evidence Item Information

Case Number: c002

Evidence Number: 002

Unique Description: folder

Examiner: vijay

Notes: imp

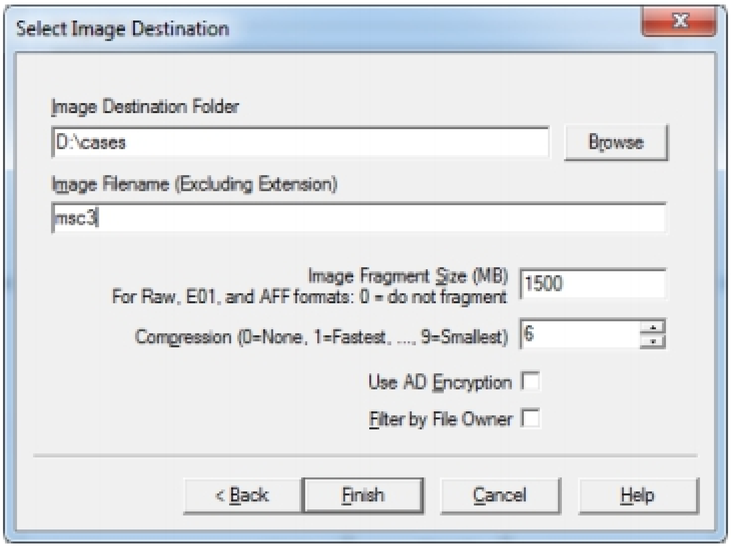

Select Image Destination

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 □

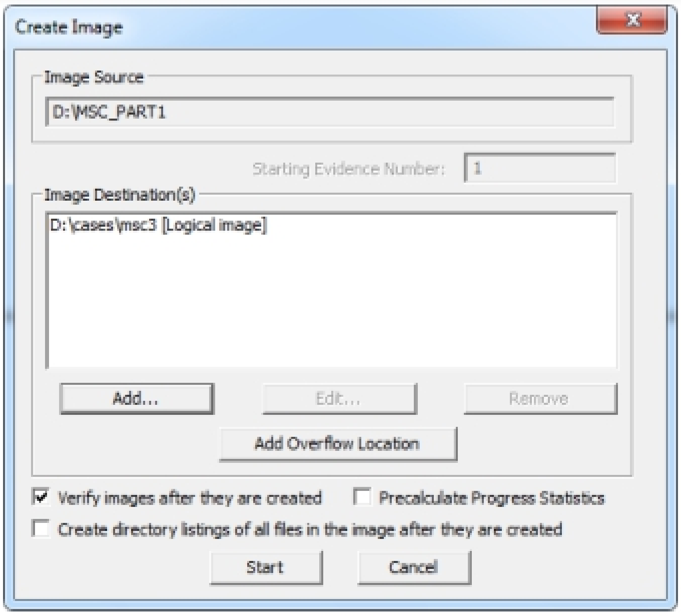


Image Source

D:\MSC_PART1

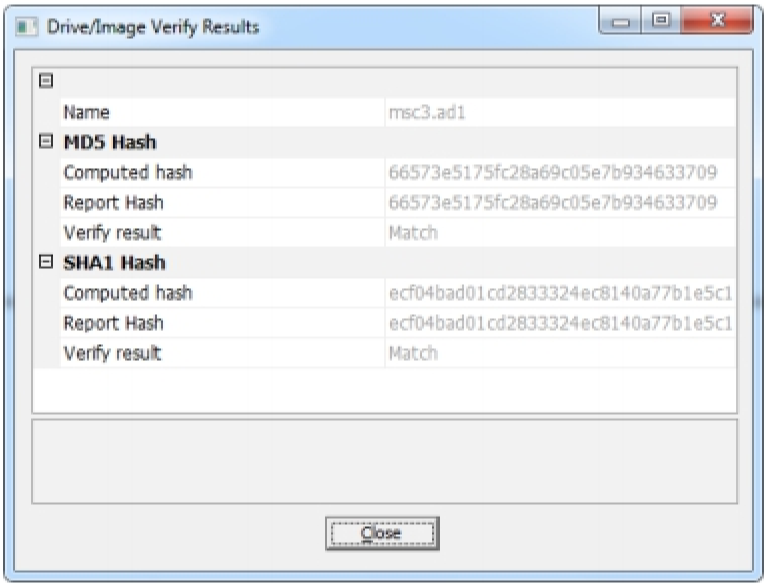
Starting Evidence Number: 1

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



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

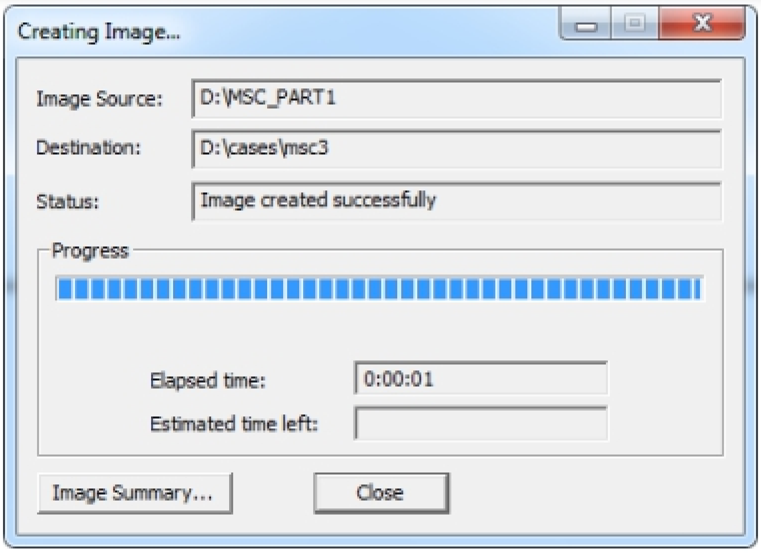


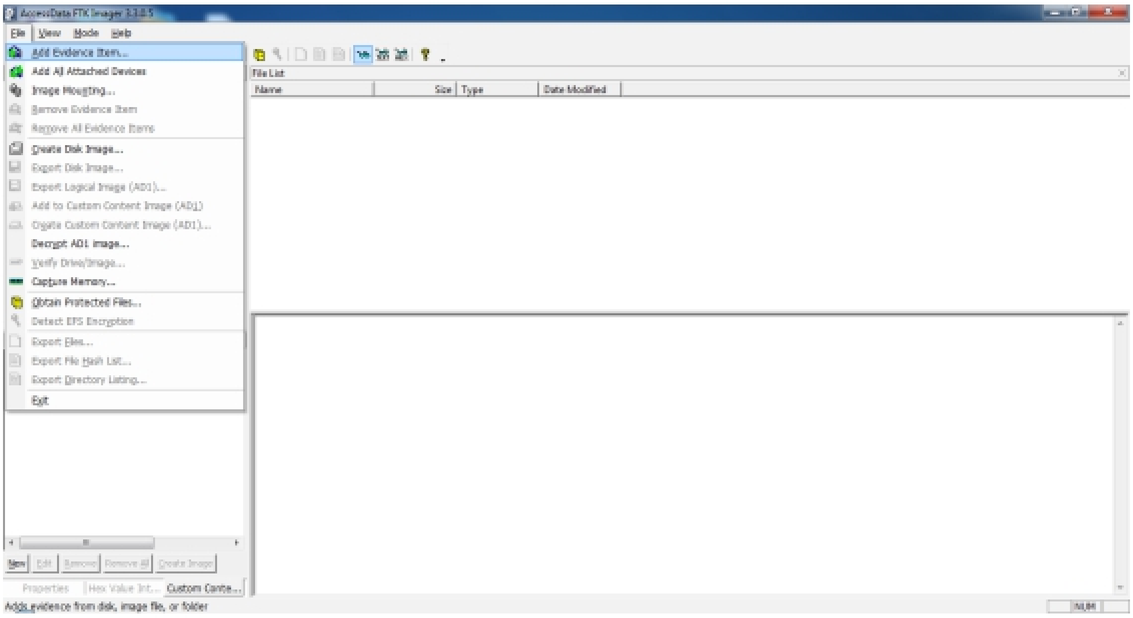
Image Source: D:\MSC_PART1

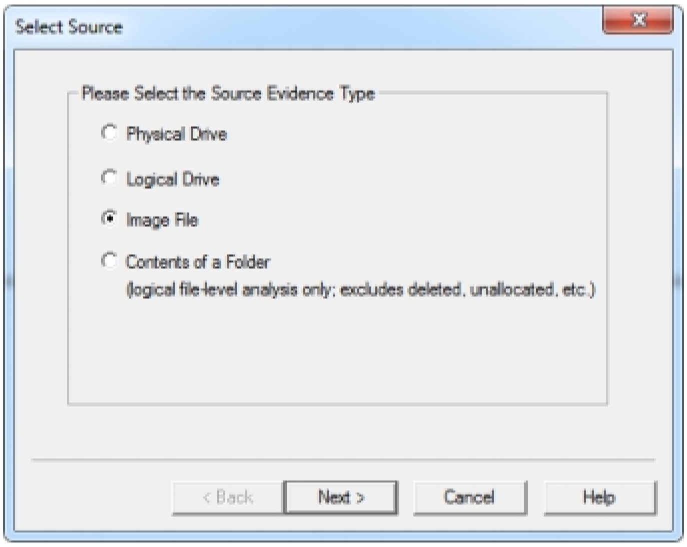
Destination: D:\cases\msc3

Status: Image created successfully

Elapsed time: 0:00:01

Estimated time left:





Select Source

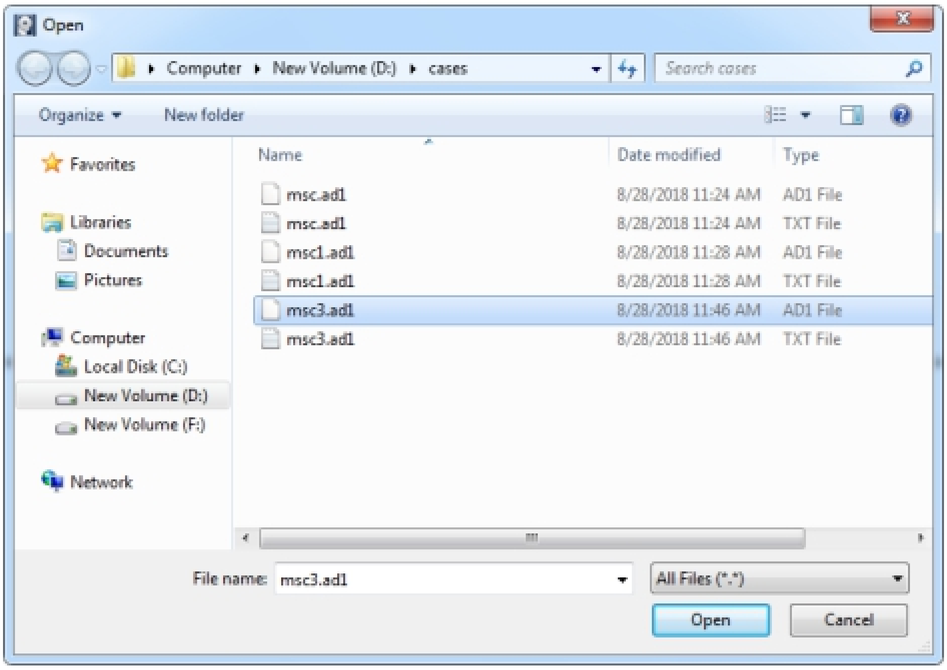
Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

● Image File

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



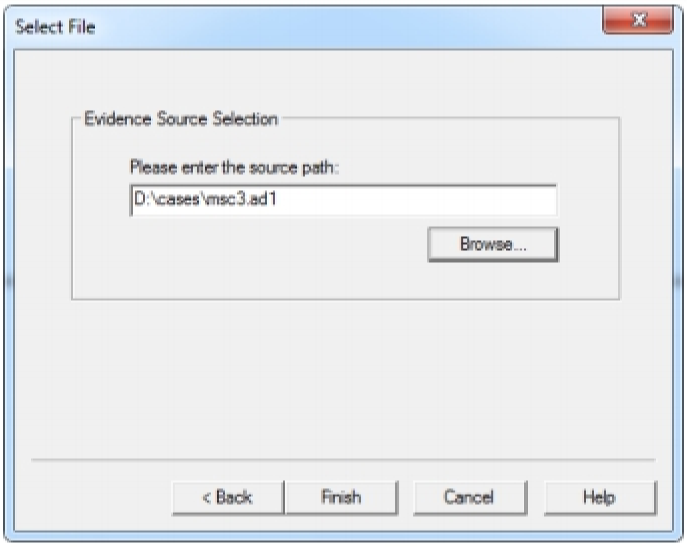
Open

Computer ▸ New Volume (D:) ▸ cases

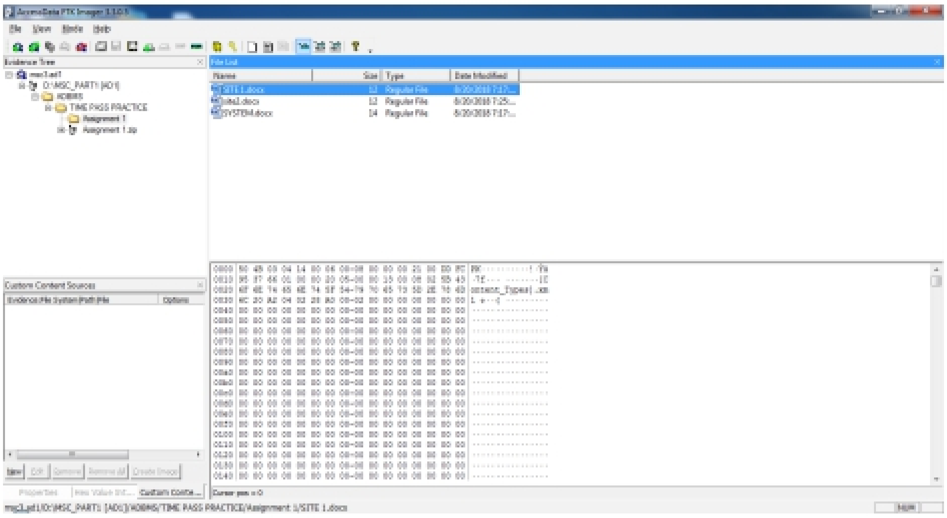
Name	Date modified	Type
msc.ad1	8/28/2018 11:24 AM	AD1 File
msc.ad1	8/28/2018 11:24 AM	TXT File
msc1.ad1	8/28/2018 11:28 AM	AD1 File
msc1.ad1	8/28/2018 11:28 AM	TXT File
msc3.ad1	8/28/2018 11:46 AM	AD1 File
msc3.ad1	8/28/2018 11:46 AM	TXT File

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:...
SYSTEM4.docx	14	Regular File	8/20/2018 7:17:...

Evidence:File System\Path\File	Options

[illegible]

Cursor pos = 0

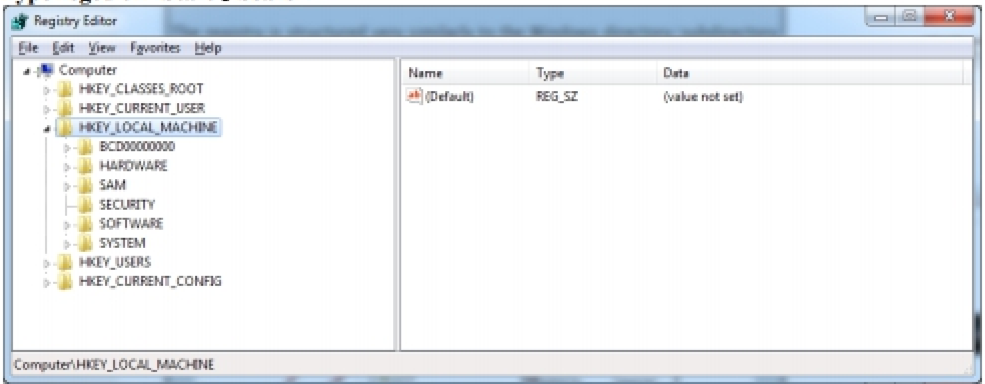
msc3.ad1/D:\MSC_PART1 [AD1]/ADBMS/TIME PASS PRACTICE/Assignment 1/SITE 1.docx

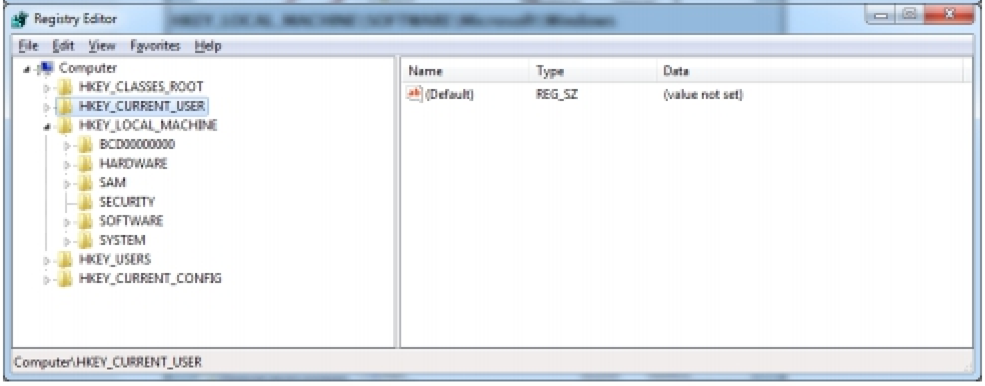
Practical Nine

Aim: Registry Editor

Accessing the Registry

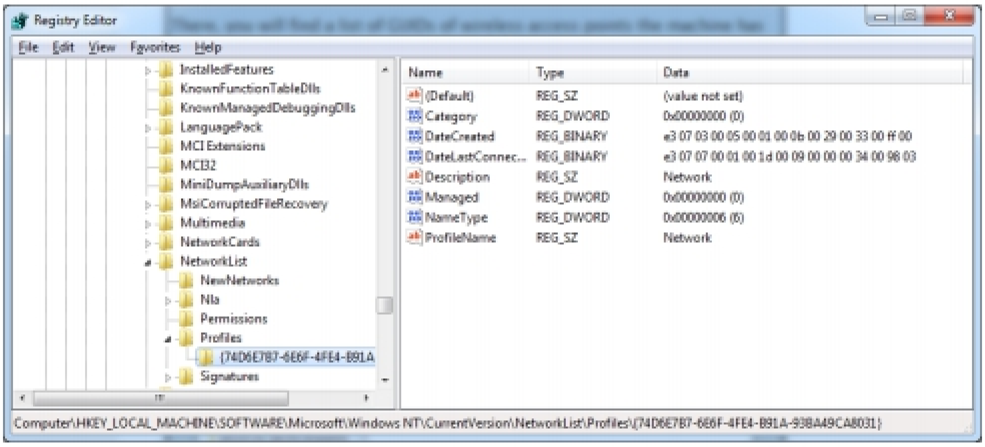
Type regedit in Start→Search





Wireless Evidence in the Registry

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

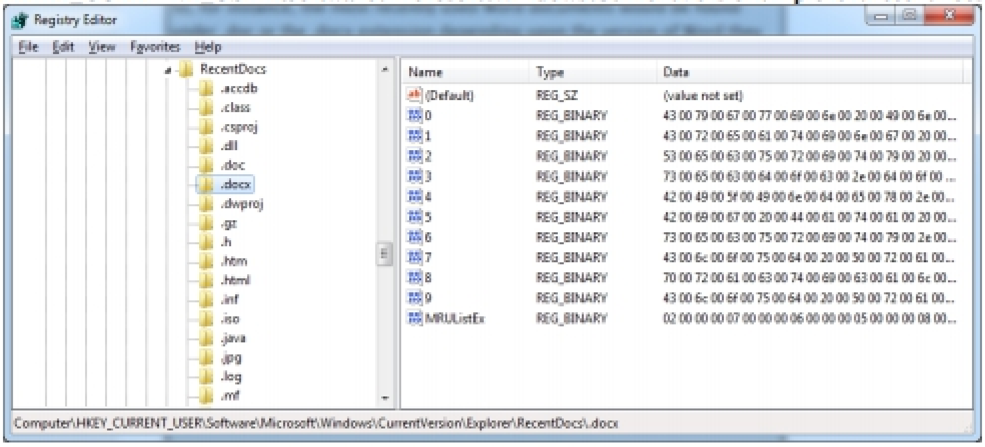


Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	e3 07 03 00 05 00 01 00 0b 00 29 00 33 00 ff 00
DateLastConnec...	REG_BINARY	e3 07 07 00 01 00 1d 00 09 00 00 00 34 00 98 03
Description	REG_SZ	Network
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD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

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{74D6E787-6E6F-4FE4-B91A-93BA49CA8031}

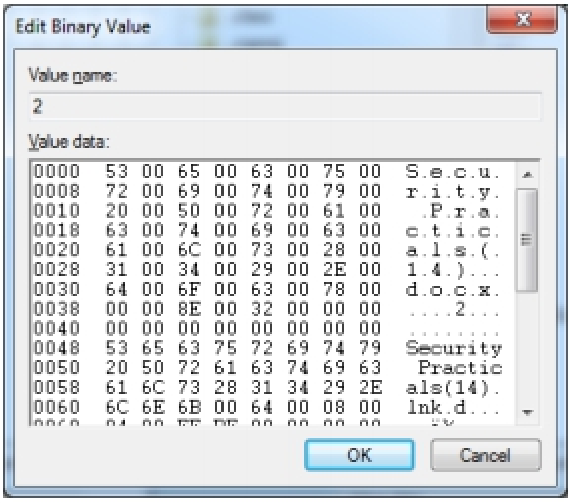
The RecentDocs Key

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

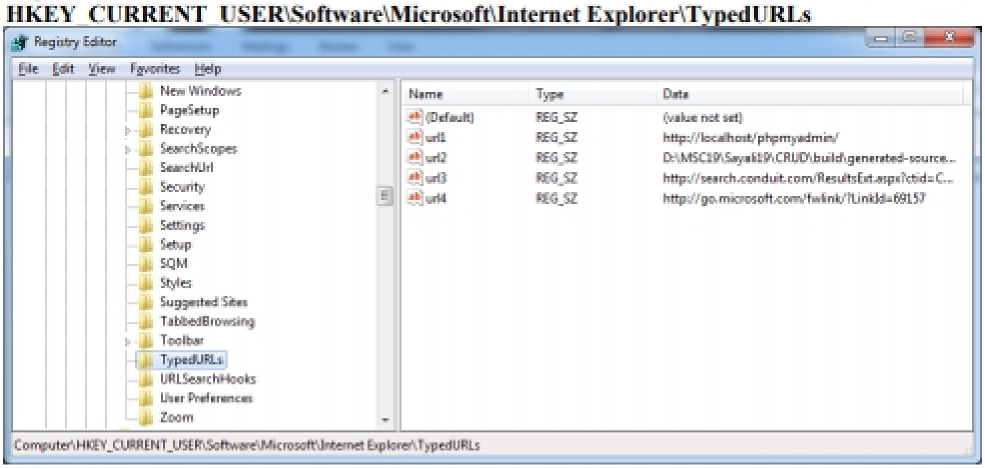


2

```
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

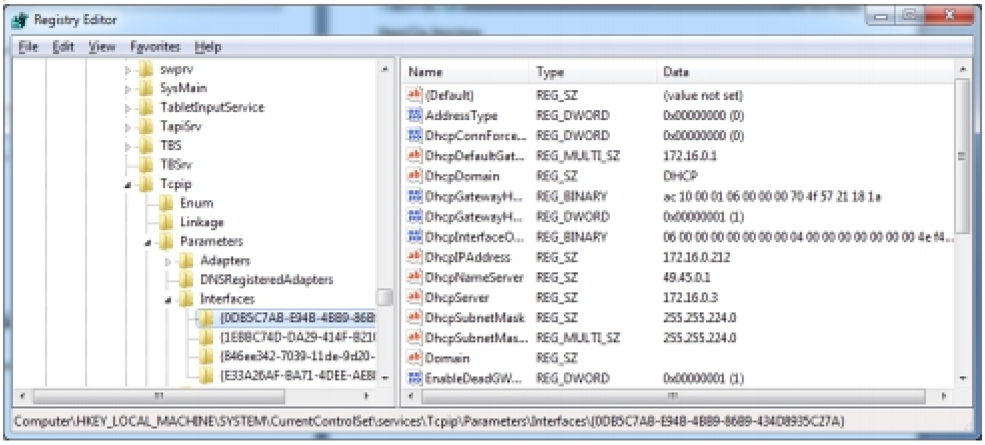


Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://localhost/phpmyadmin/
url2	REG_SZ	D:\MSC19\Sayali19\CRUD\build\generated-source...
url3	REG_SZ	http://search.conduit.com/ResultsExt.aspx?ctid=C...
url4	REG_SZ	http://go.microsoft.com/fwlink/?LinkId=69157

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

IP Addresses

HKEY_LOCAL_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interfaces

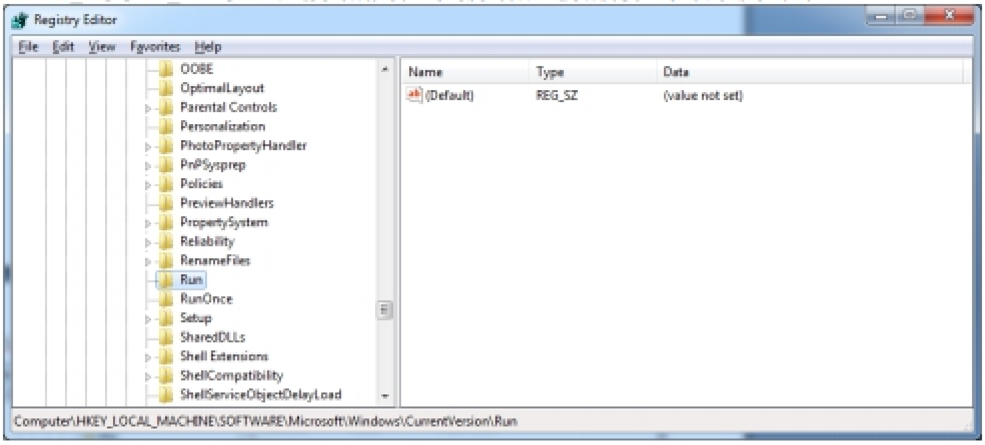


Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	172.16.0.1
DhcpDomain	REG_SZ	DHCP
DhcpGatewayH...	REG_BINARY	ac 10 00 01 06 00 00 00 70 4f 57 21 18 1a
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
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\{0DB5C7A8-E94B-4B89-86B9-434D8935C27A}

Start Up Locations in the Registry

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

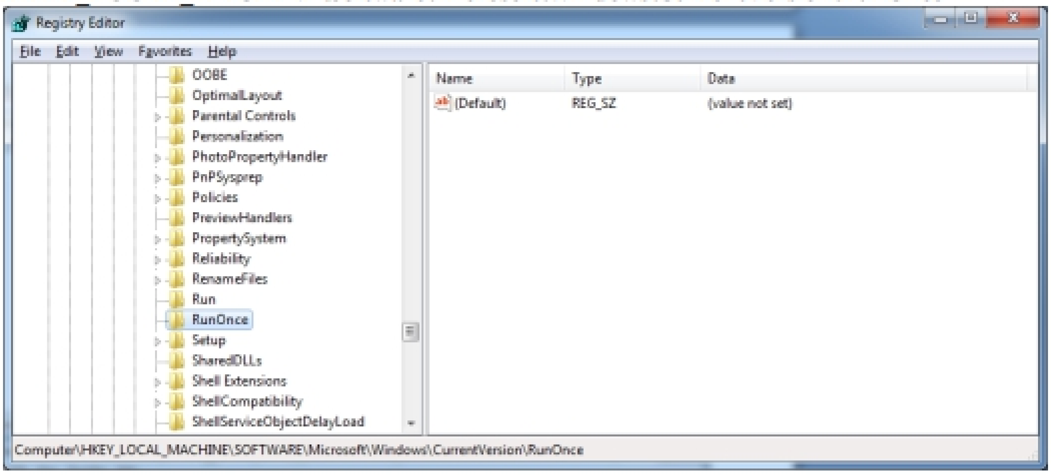


Name	Type	Data
(Default)	REG_SZ	(value not set)

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

RunOnce Startup

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

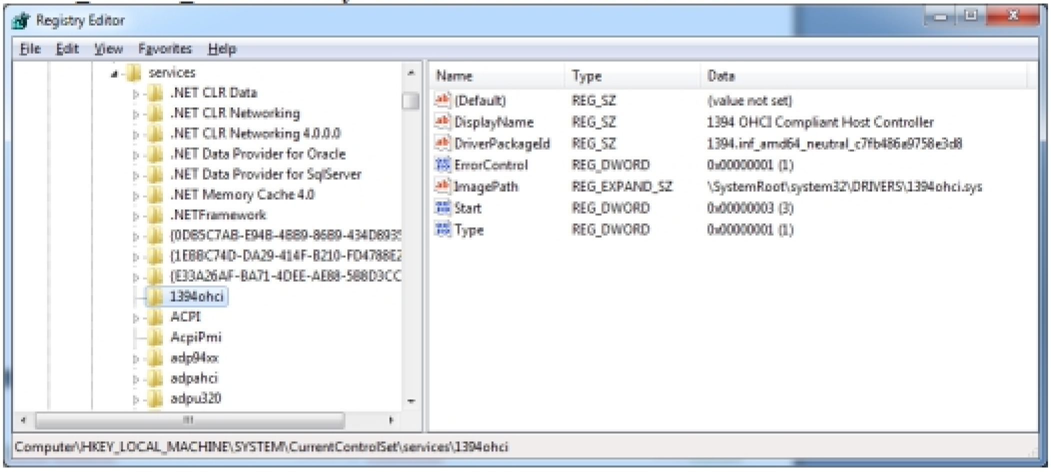


Name	Type	Data
(Default)	REG_SZ	(value not set)

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

Start Up Services

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

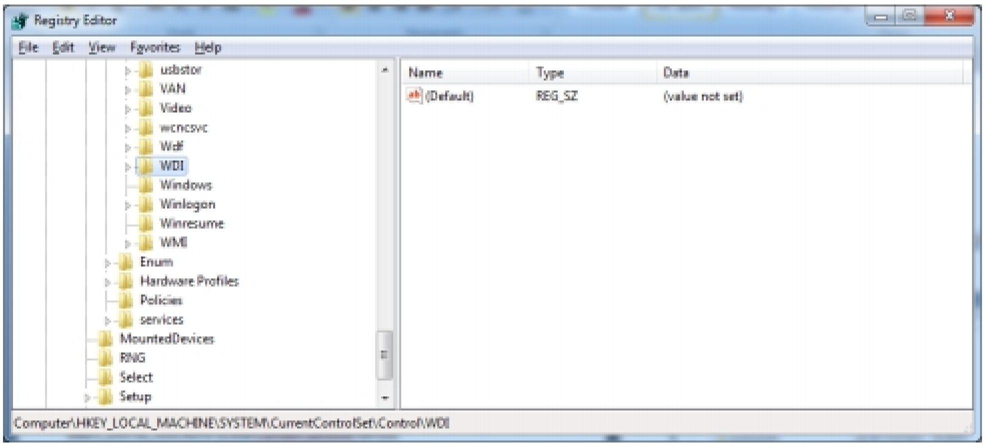

Registry Editor
File
Edit
View
Favorites
Help
services
.NET CLR Data
.NET CLR Networking
.NET CLR Networking 4.0.0.0
.NET Data Provider for Oracle
.NET Data Provider for SqlServer
.NET Memory Cache 4.0
.NETFramework
{0D85C7AB-E94B-4BB9-86B9-434D893
{1EBBC74D-DA29-414F-B210-FD4788E2
{E33A26AF-BA71-4DEE-AE88-588D3CC
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

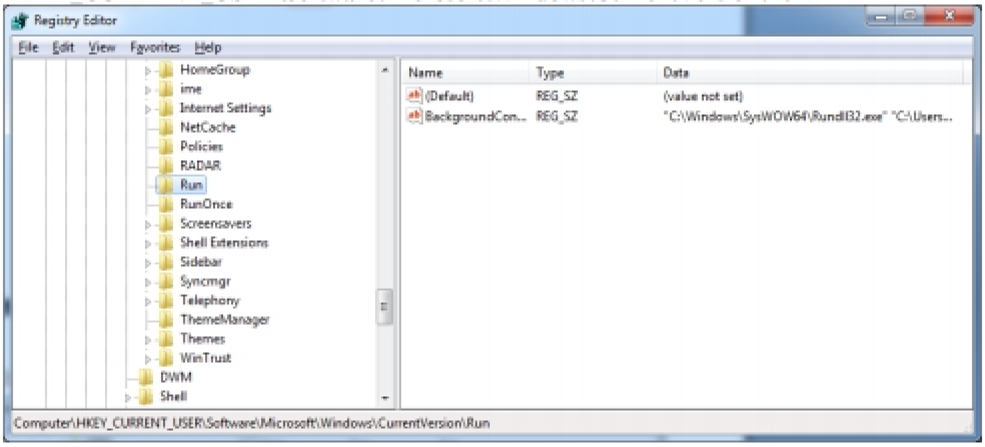


Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI

Start When a Particular User Logs On

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

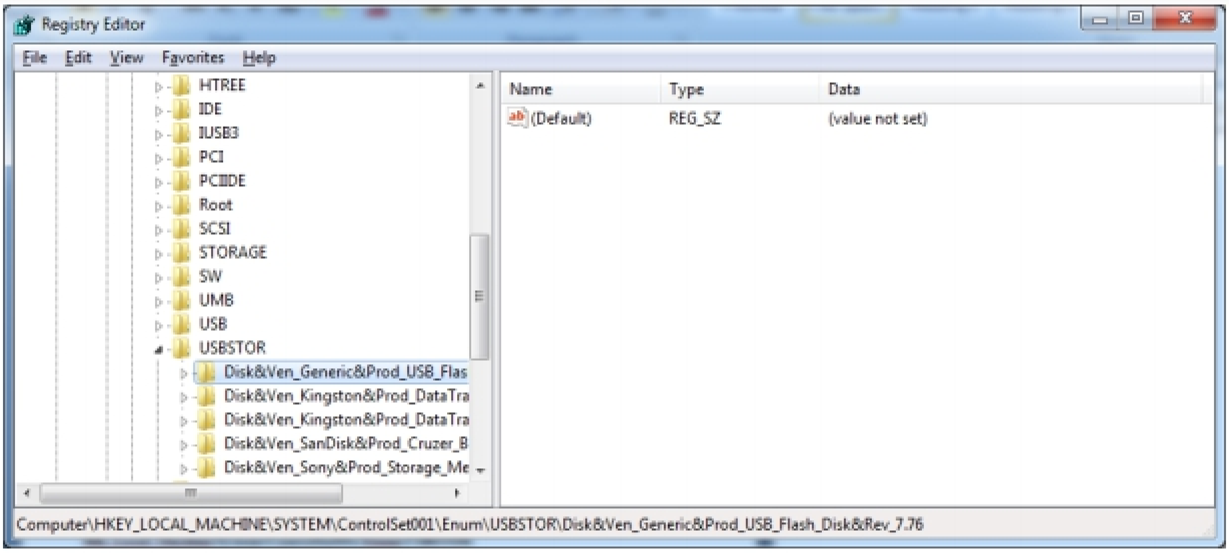


Name	Type	Data
(Default)	REG_SZ	(value not set)
BackgroundCon...	REG_SZ	"C:\Windows\SysWOW64\Rundll32.exe" "C:\Users...

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

USB Storage Devices

HK_Local_Machine\System\ControlSet00x\Enum\USBSTOR

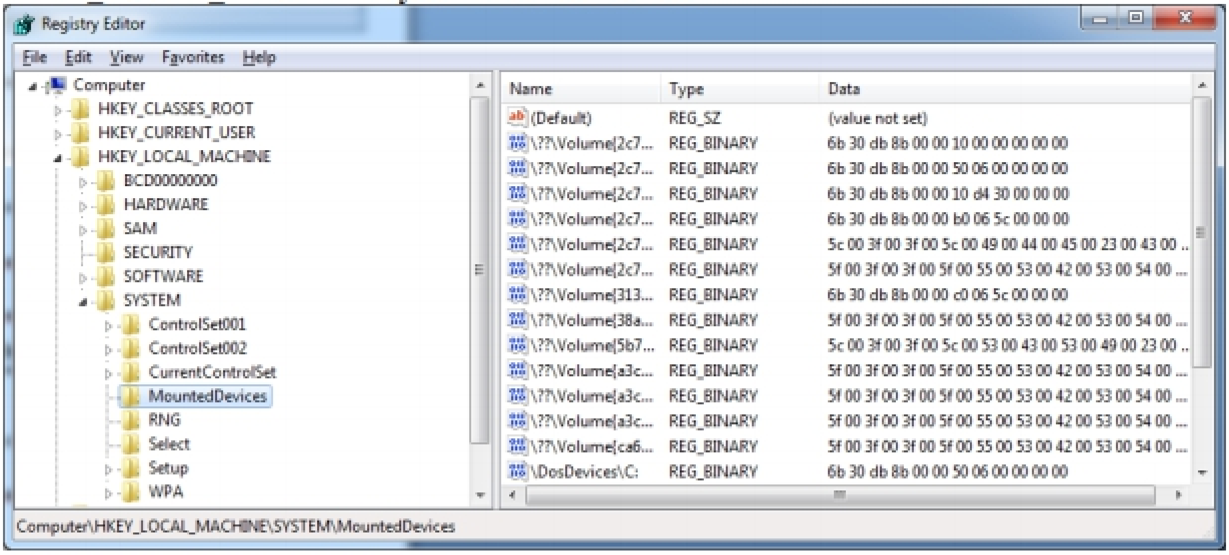

Registry Editor
File
Edit
View
Favorites
Help
HTREE
IDE
IUSB3
PCI
PCIIDE
Root
SCSI
STORAGE
SW
UMB
USB
USBSTOR
Disk&Ven_Generic&Prod_USB_Flas
Disk&Ven_Kingston&Prod_DataTra
Disk&Ven_Kingston&Prod_DataTra
Disk&Ven_SanDisk&Prod_Cruzer_B
Disk&Ven_Sony&Prod_Storage_Me

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 Ten

Virus

```
package practical.ten;

import java.io.FileWriter;
import java.io.IOException;

public class Virus {

        public static void main(String[] args) {
              try
{
FileWriter fw=new FileWriter("D:/virus.dll",true);
while(true)
{
fw.write("virus has been activated");
}
}
catch(IOException e)
{
e.printStackTrace();
}
      }

}
```