Digital Forensics - Lab FAT

Class No :	**CH2021221000516**	Slot :	**L49 + L50**
Course Code :	**CSE4004**	Faculty Name :	**Nagaraj SV**

Aadhitya Swarnesh

- 9 December 2021

Question 1 :

Analyse the following email header using a tool and determine the source, destination, path taken etc.

Email has become one of the important means of communication in today's world. However, emails can be faked. Analysis of email headers provides useful leads for investigators. There are number of online tools that are useful for email header analysis.

For example : https://dnschecker.org/email-header-analyzer.php

In this lab, we will use the forensic tools available to study emails, especially the headers to gain more information and details about the emails. We can gain knowledge about the sender, the recipient, their email addresses, the time in which the mail was sent, and even the network information of the people involved. These details can prove to be vital to any forensic investigations in this current age of technological advancement.

We have been provided with a email header information in the question which we will be using to figure out more information on the people involved. We will be using the

website mentioned above which helps us to decode the header data and give more overall presentable data in a format which is easily understandable.

The following image shows the email header which has been provided to us for analysis :

```
From: Media Temple user (mt.kb.user@gmail.com)
Subject: article: How to Trace a Email
Date: January 25, 2011 3:30:58 PM PDT
To: user@example.com
Return-Path: <mt.kb.user@gmail.com>
Envelope-To: user@example.com
Delivery-Date: Tue, 25 Jan 2011 15:31:01 -0700
Received: from po-out-1718.google.com ([72.14.252.155]:54907) by cl35.gs01.gridserver.com with esmtp (Exim 4.63) (envelope-from <mt.kb.user@gmail.com>) id 1KDoNH-0000f0-RL for user@example.com; Tue, 25 Jan 2011 15:31:01 -0700
Received: by po-out-1718.google.com with SMTP id y22so795146pof.4 for <user@example.com>; Tue, 25 Jan 2011 15:30:58 -0700 (PDT)
```

We will now proceed to the aforementioned online tool and insert this header into the space available as shown below :

On clicking the analyst button available there, the tool parses the header for data and then presents them in precise readable format as follows :

Email Source Ip Info	
Source IP Address	72.14.252.155
Source IP Hostname	72.14.252.155
Country	Canada
State	Quebec
City	Montreal
Zip Code	H4X
Latitude	45.5017
Longitude	-73.5673
ISP	Google LLC
Organization	Google LLC
Threat Level	low

By this table, we can figure out the key information about the email header which is the IP address of the sender, by which we can approximately track the location from which this mail was sent.

This tool also provides more useful data which is based on the IP address which was extracted from the header. These as shown below :

WHOIS Lookup Info

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#


NetRange:       72.14.192.0 - 72.14.255.255
CIDR:           72.14.192.0/18
NetName:        GOOGLE
NetHandle:      NET-72-14-192-0-1
Parent:         NET72 (NET-72-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2004-11-10
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/72.14.192.0
```

```
OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL


OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN
```

```
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN

RTechHandle: ZG39-ARIN
RTechName:   Google LLC
RTechPhone:  +1-650-253-0000
RTechEmail:  arin-contact@google.com
RTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#
```

If we try to analyse this further with another website, we can gain more information on the path taken by this mail from reaching the receiver from the sender :

MessageId	c8f49cec0807011530k11196ad4p7cb4b9420f2ae752@mail.gmail.com
Created at:	1/25/2011, 9:00:58 AM GMT+5:30 (Delivered after **19 hours**)
From:	Media Temple user (mt.kb.user@gmail.com)
To:	user@example.com
Subject:	article: How to Trace a Email

#	Delay	From *			To *	Protocol	Time received	
0	19 hours		→		10.140.188.3	Web	1/26/2011, 4:00:58 AM GMT+5:30	
1			→	[Google]	10.141.116.17	SMTP	1/26/2011, 4:00:58 AM GMT+5:30	*Originated at Gmail*
2			→	[Google]	po-out-1718.google.com	SMTP	1/26/2011, 4:00:58 AM GMT+5:30	
3	3 sec	po-out-1718.google.com	→		cl35.gs01.gridserver.com		1/26/2011, 4:01:01 AM GMT+5:30	

Thus, we have analyzed the header of this email, and have gotten to the roots of its origination. In this manner this online tool can easily be used to analyze the header of such emails. We have also gotten to know the sender's address, their service providers, and also their geological coordinates for the email's origination.

Key Takeaways :

Source : 72.14.252.155 (Canada)

Destination : cl35.gs01.gridserver.com

Path taken : Pings through multiple servers (3) before reaching the destination as shown in the above image.

Question 2 :

Perform file carving. Download the file from the link

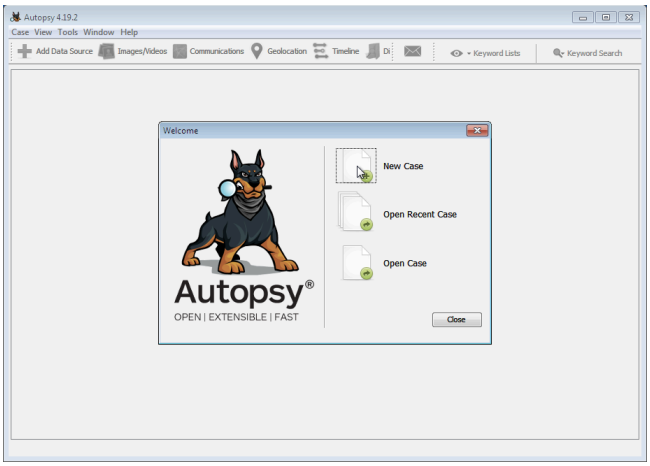
https://cfreds-archive.nist.gov/FileCarving/Images/L1_Documents.dd.bz2

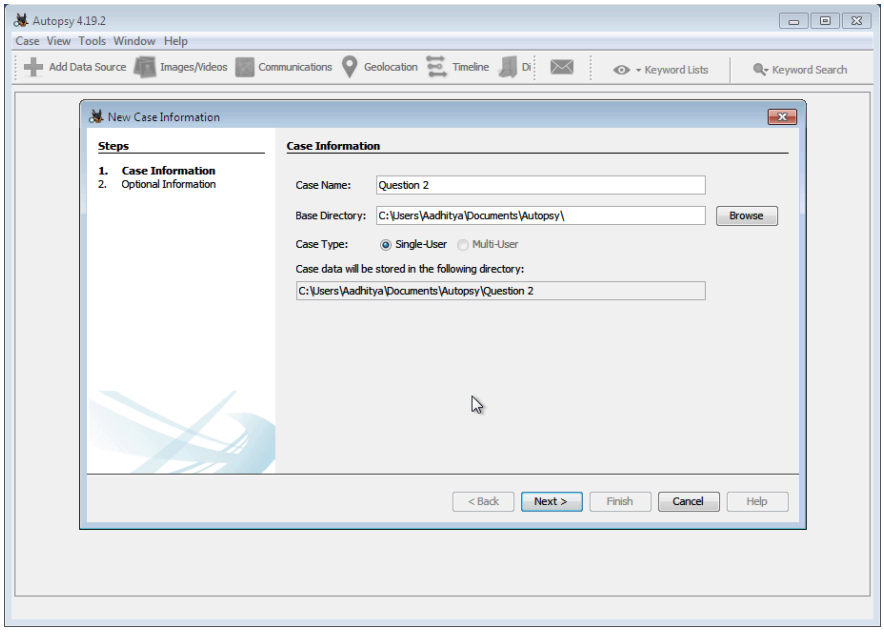
Use bunzip2 or other utilities such as 7Zip to uncompress the file and get the file L1_Documents.dd This file contains document files of any or all of the following types — DOC, XLS, PPT, PDF.

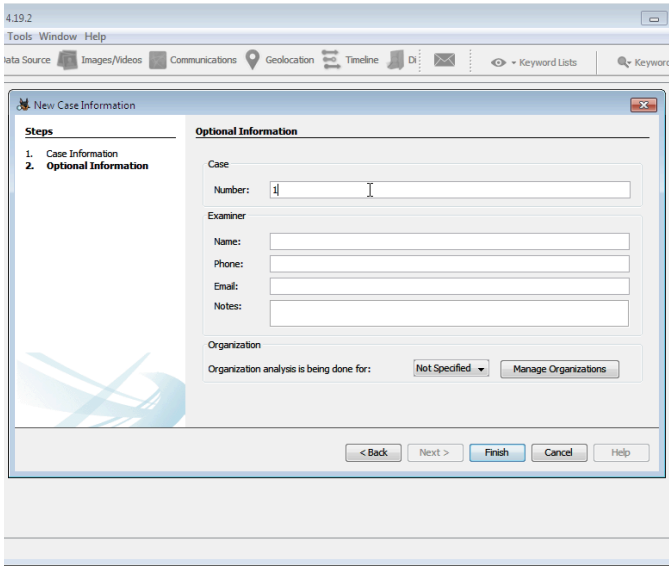
Use an appropriate file recovery tool to recover files from the image file.

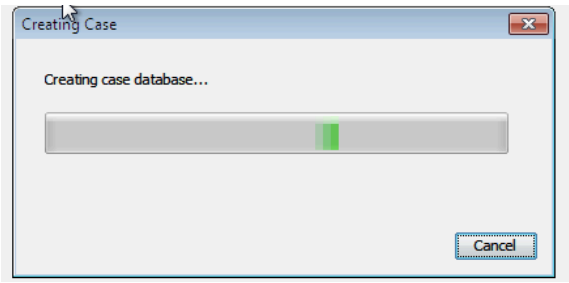
We will be using the Autopsy tool to perform the File Carving process here. We will download and extract the given file using 7zip, and then open it in autopsy to carve the files.

The below steps are for opening autopsy and creating a new case for this lab question.

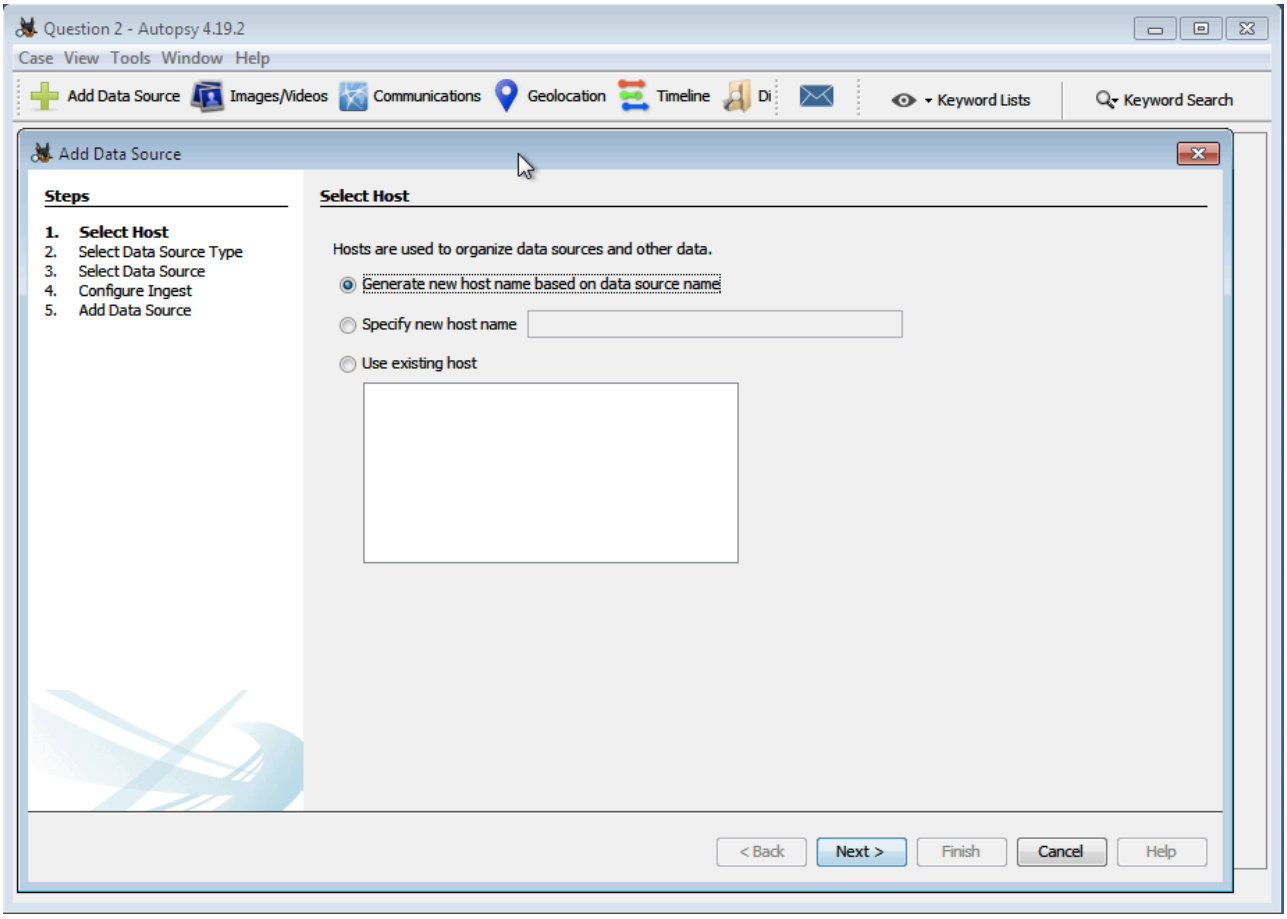


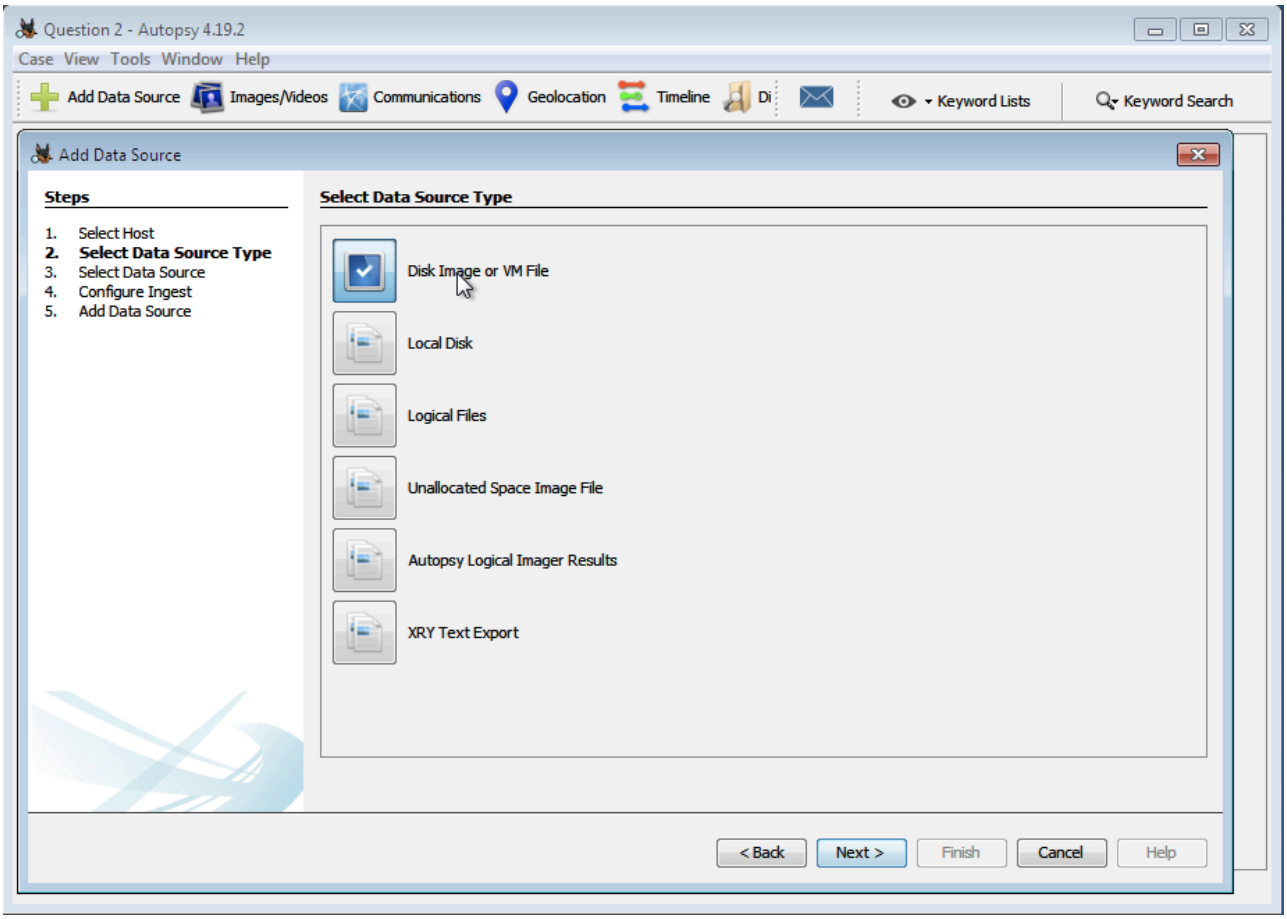


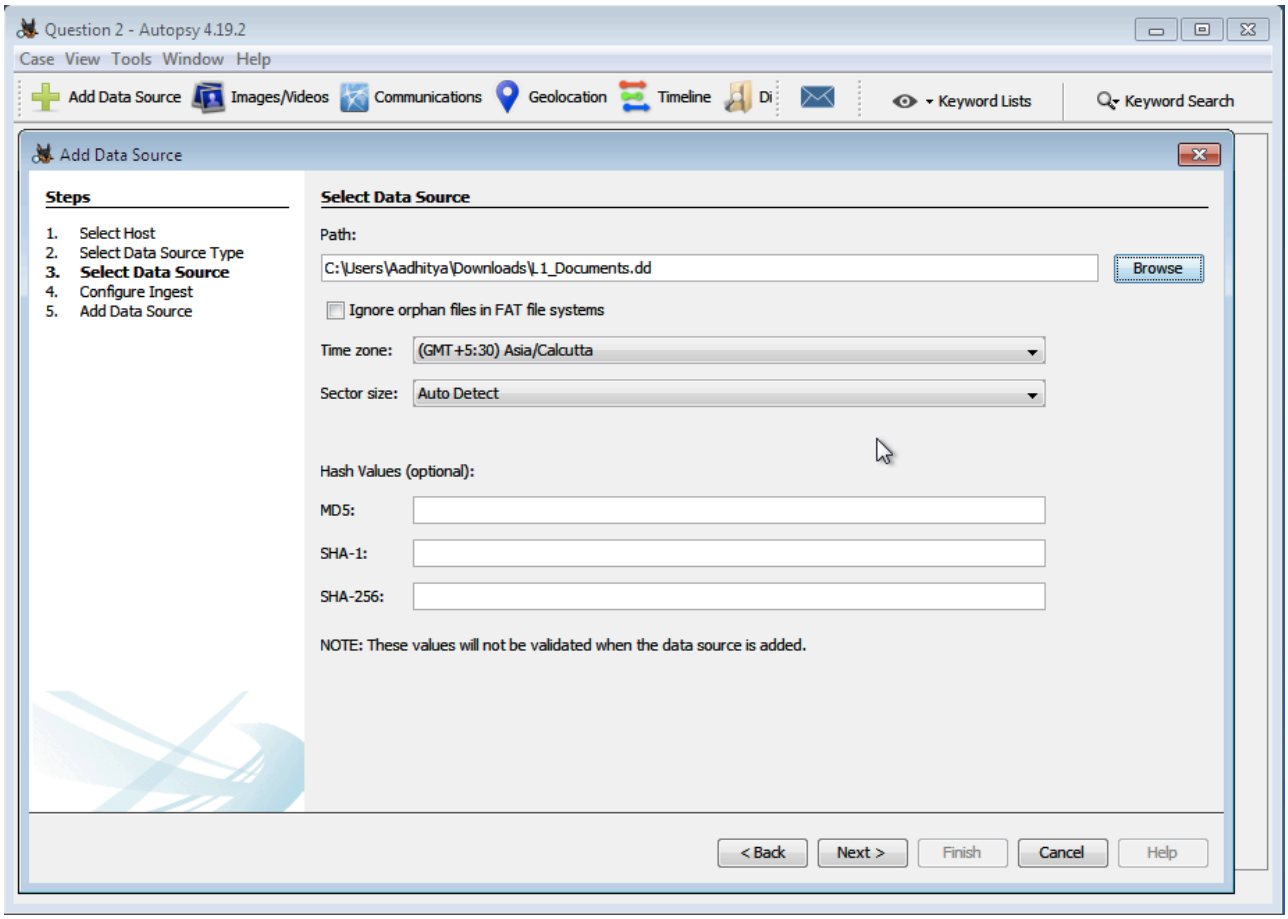


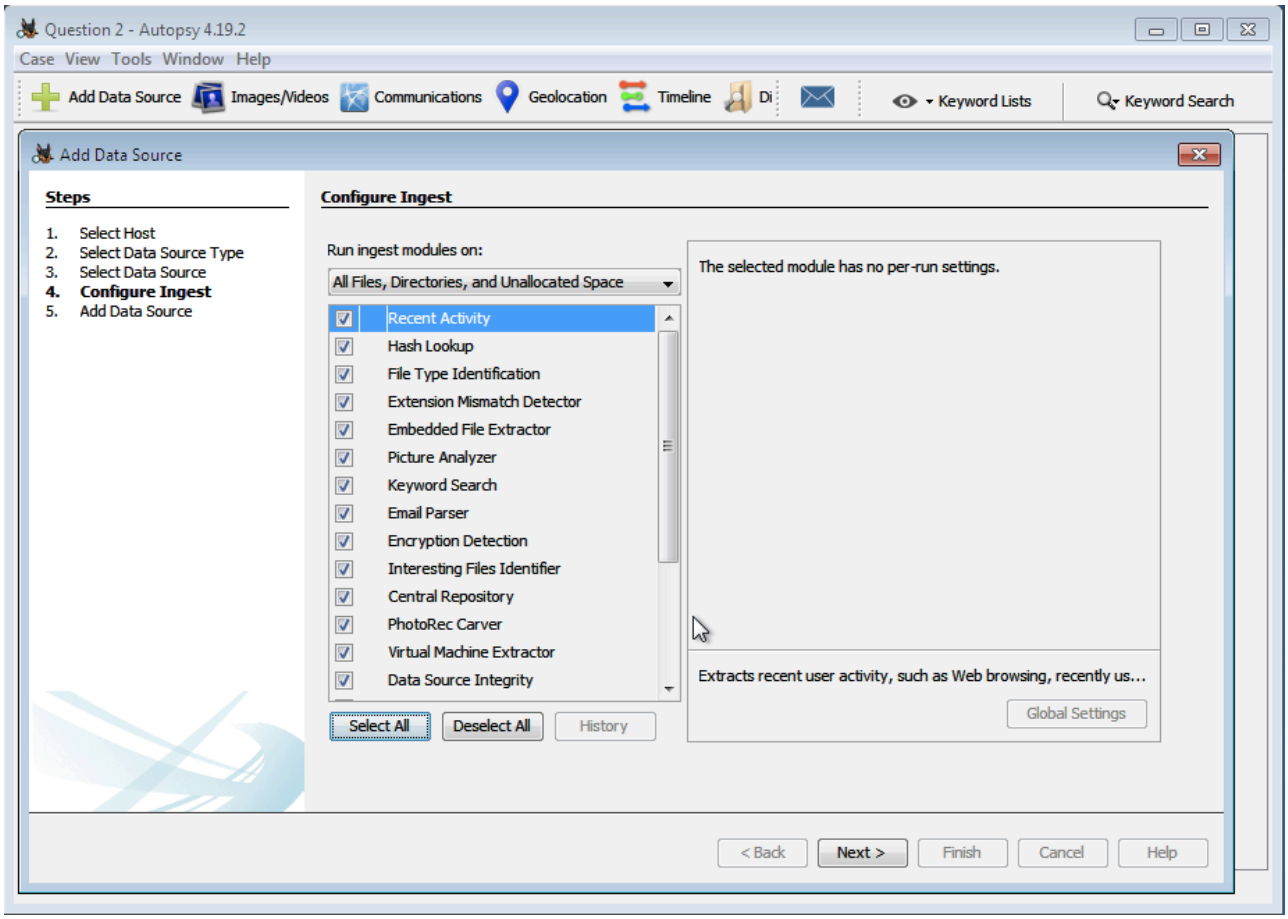


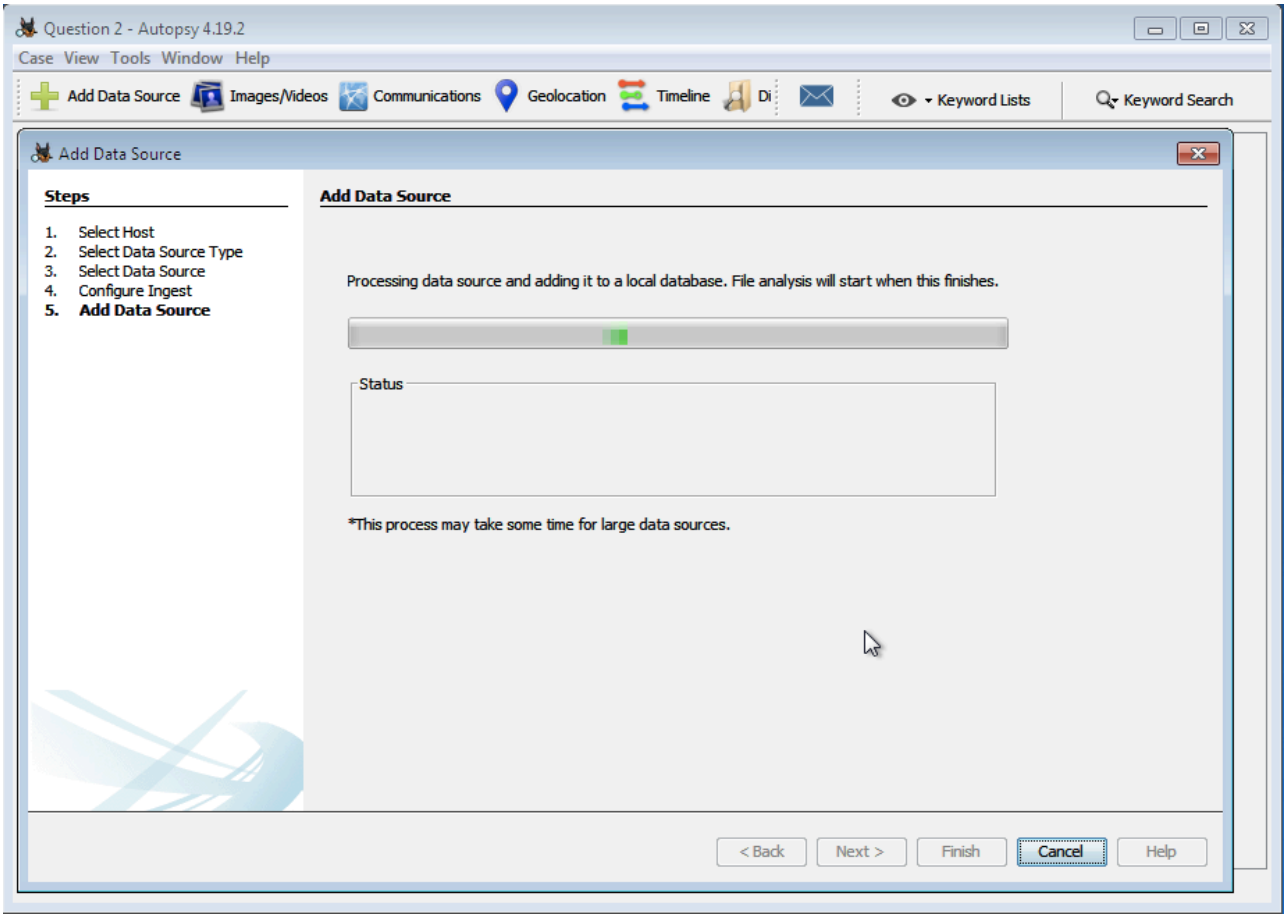
We will now add a new data source, the steps to do this is as follows :
Here, we add the image file that we had downloaded and extracted earlier.




Question 2 - Autopsy 4.19.2
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source Type
Disk Image or VM File
Local Disk
Logical Files
Unallocated Space Image File
Autopsy Logical Imager Results
XRY Text Export
< Back
Next >
Finish
Cancel
Help

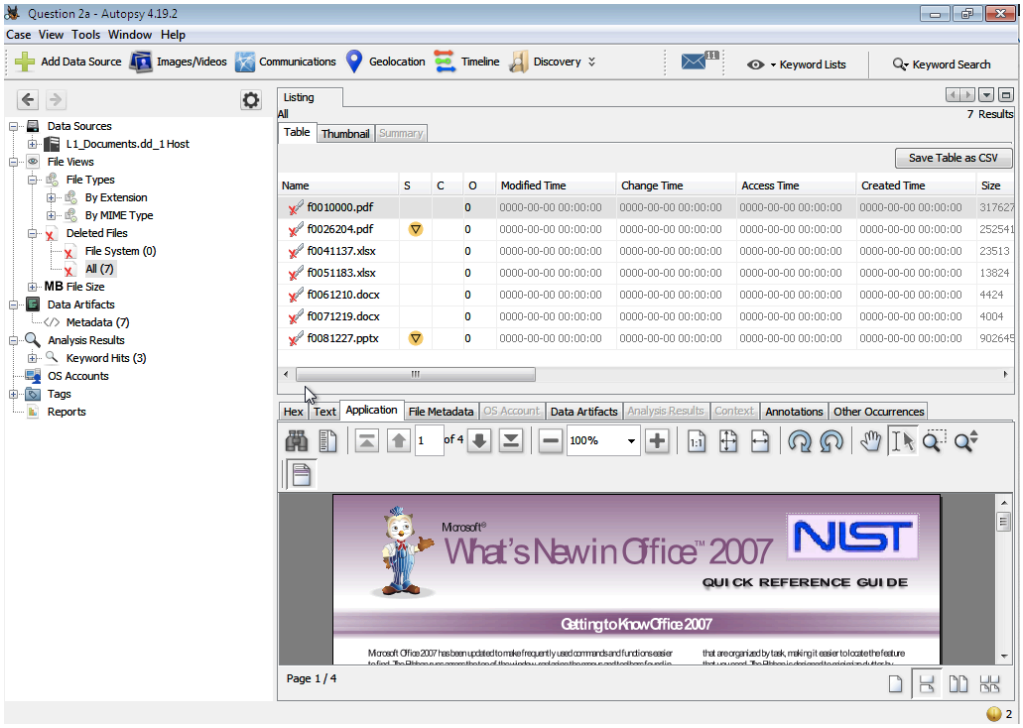

Question 2 - Autopsy 4.19.2
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Select Data Source
Path:
C:\Users\Aadhitya\Downloads\L1_Documents.dd
Browse
Ignore orphan files in FAT file systems
Time zone:
(GMT+5:30) Asia/Calcutta
Sector size:
Auto Detect
Hash Values (optional):
MD5:
SHA-1:
SHA-256:
NOTE: These values will not be validated when the data source is added.
< Back
Next >
Finish
Cancel
Help

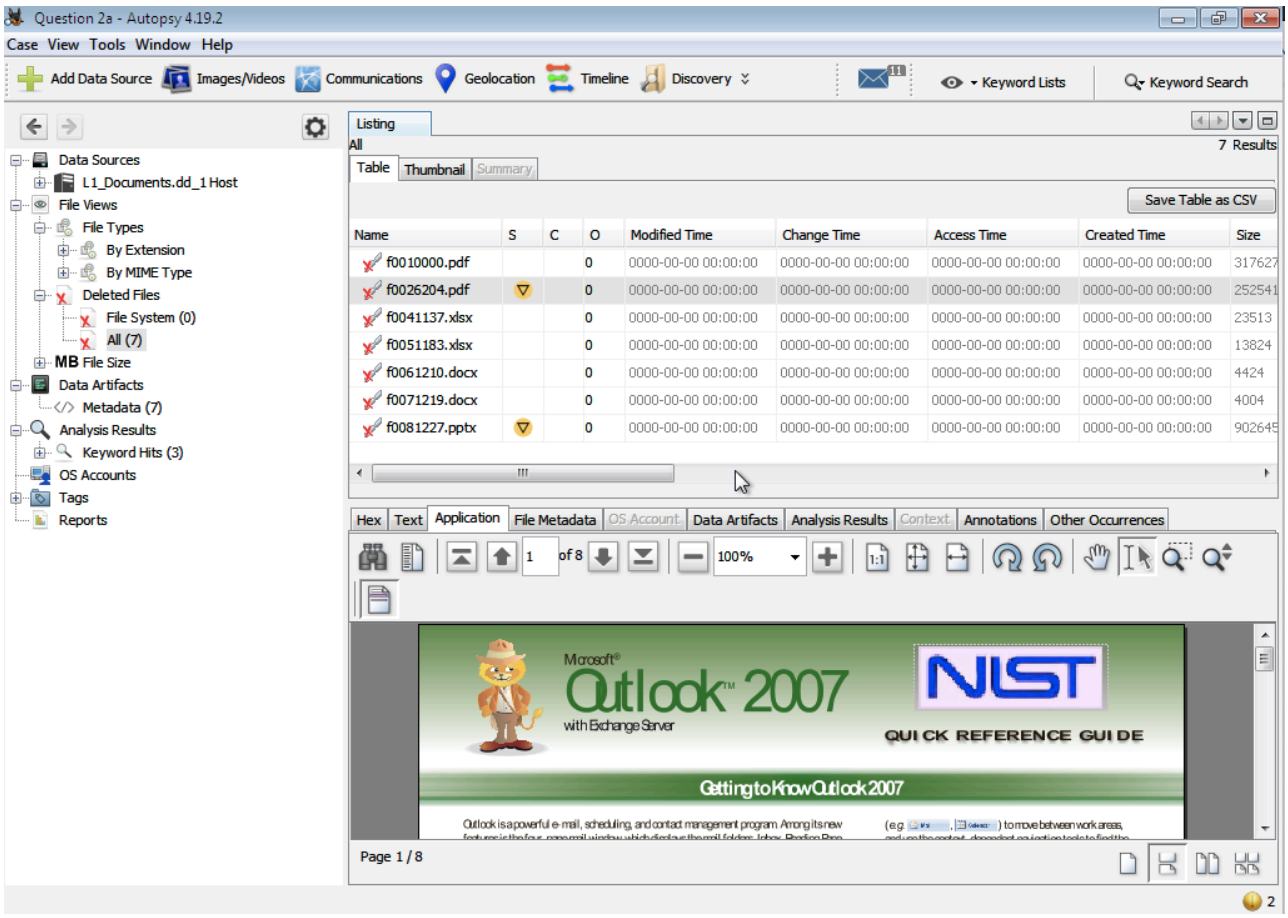

Question 2 - Autopsy 4.19.2
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Configure Ingest
Run ingest modules on:
All Files, Directories, and Unallocated Space
Recent Activity
Hash Lookup
File Type Identification
Extension Mismatch Detector
Embedded File Extractor
Picture Analyzer
Keyword Search
Email Parser
Encryption Detection
Interesting Files Identifier
Central Repository
PhotoRec Carver
Virtual Machine Extractor
Data Source Integrity
Select All
Deselect All
History
The selected module has no per-run settings.
Extracts recent user activity, such as Web browsing, recently us...
Global Settings
< Back
Next >
Finish
Cancel
Help

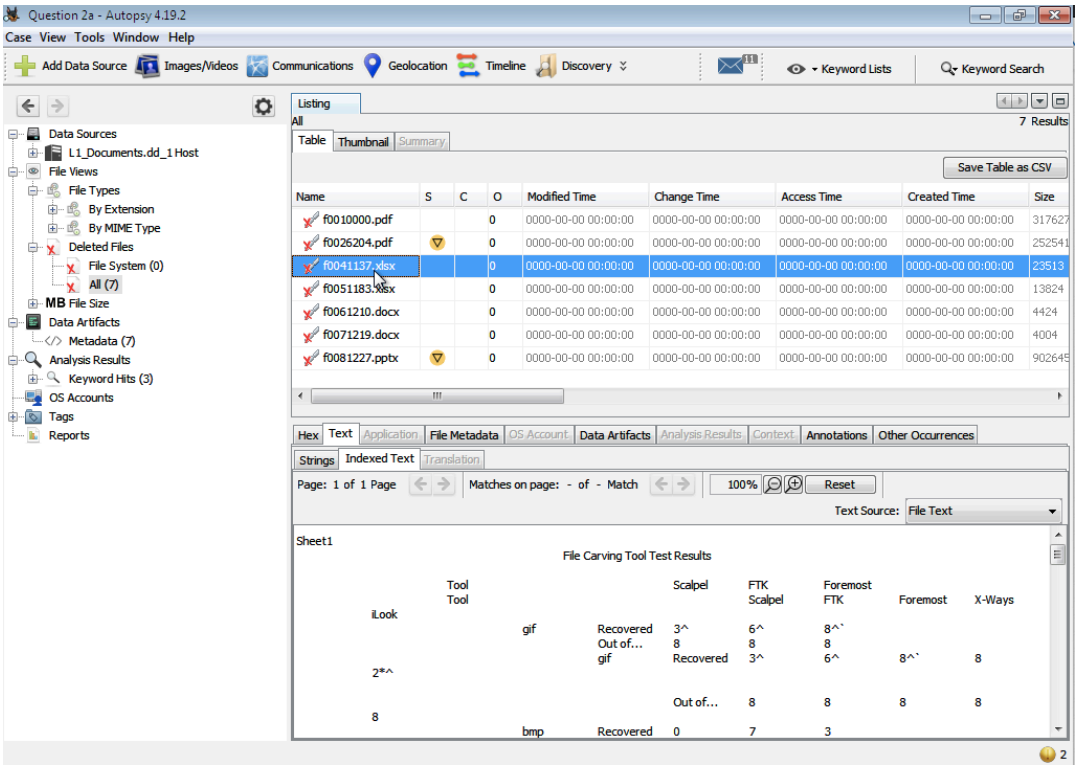

Question 2 - Autopsy 4.19.2
Case View Tools Window Help
Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Keyword Lists
Keyword Search
Add Data Source
Steps
1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. Add Data Source
Add Data Source
Processing data source and adding it to a local database. File analysis will start when this finishes.
Status
*This process may take some time for large data sources.
< Back
Next >
Finish
Cancel
Help

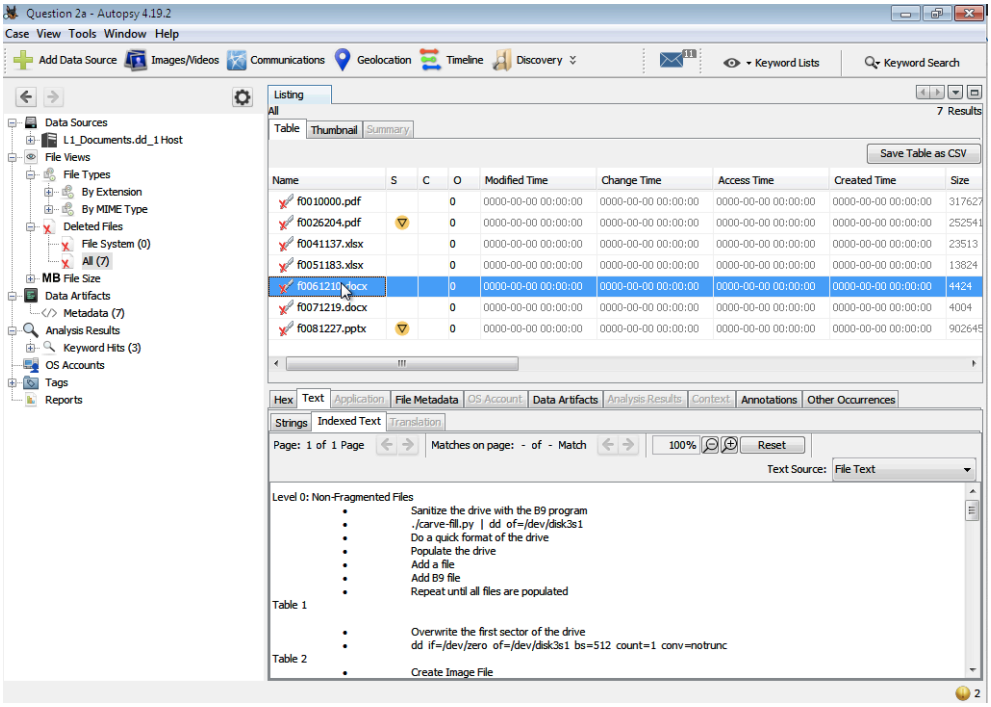
Once these series of steps are over, the autopsy tool carves the files of the formats and then displays them as shown the following images. Note that the names of these files are different than the ones in original disk, but the content are the same.

We will now open a few of those just to show the process to open and recover these files :









We were thus able to use the autopsy software and carve the files as shown in the images above. This is an important part of a forensic investigator, and we were able to recover these files successfully as stated in the question, and the recovered files have been saved successfully.

Question 3 :

This exercise makes use of a compressed dd image used to test metadata based deleted file recovery forensic tools. Metadata based deleted file recovery uses residual metadata left behind after a file is deleted to attempt to reconstruct the file. These images are not for testing file carving tools (tools that scan unallocated blocks to find file headers and trailers and then reconstructing deleted files).

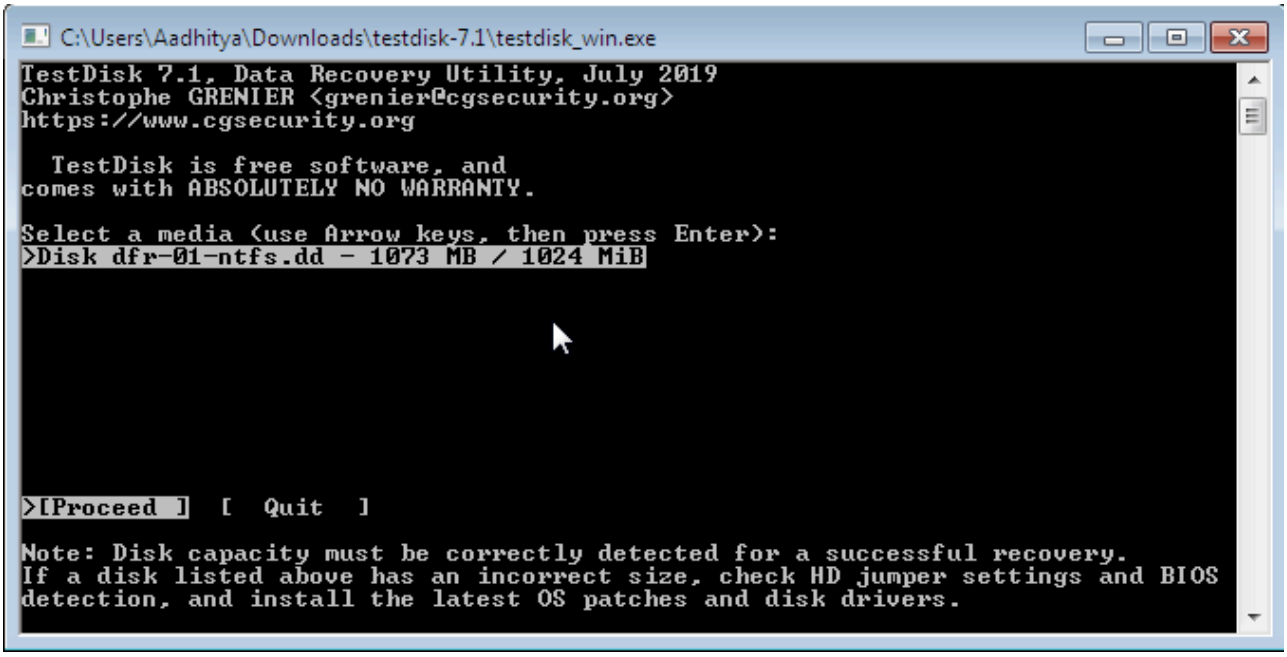
Recover one non-fragmented file from the following NTFS image.

https://cfreds-archive.nist.gov/dfr-images/dfr-01-ntfs.dd.bz2

Use bunzip2 or other utilities to get the dd file.

We will be using test disk tool for this experiment. We will first open test disk on this image file after downloading the zip file given and extracting it with 7zip.

The following images show the process of recovering these files from the image provided :

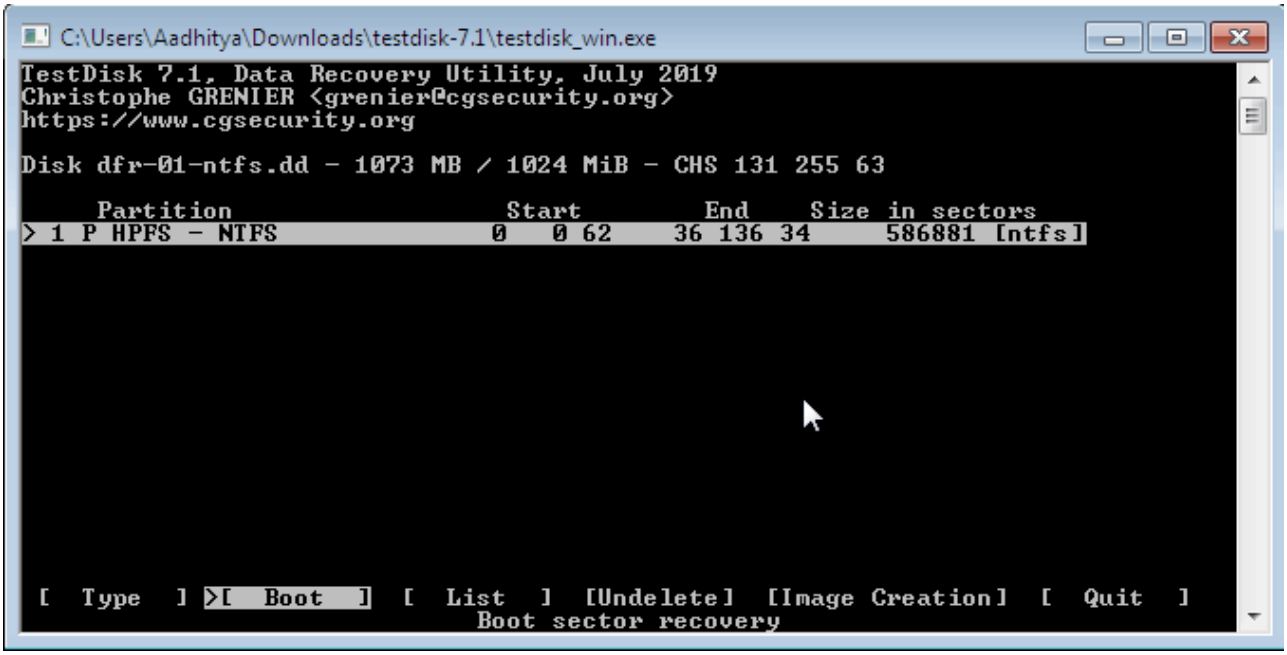


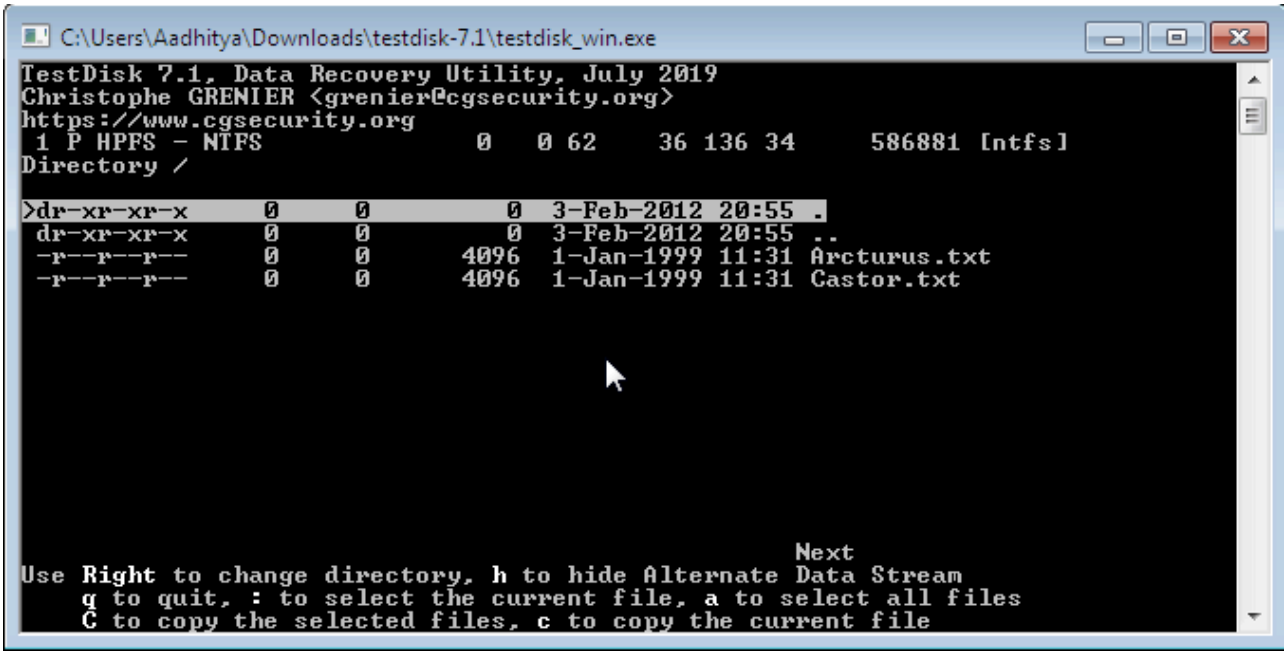
We select the type of partition, here it is intel as it has recognized the same.

```
C:\Users\Aadhitya\Downloads\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk dfr-01-ntfs.dd - 1073 MB / 1024 MiB

Please select the partition table type, press Enter when done.
>[Intel  ] Intel/PC partition
 [EFI GPT] EFI GPT partition map (Mac i386, some x86_64...)
 [Humax  ] Humax partition table
 [Mac    ] Apple partition map (legacy)
 [None   ] Non partitioned media
 [Sun    ] Sun Solaris partition
 [XBox   ] XBox partition
 [Return ] Return to disk selection_

Hint: Intel partition table type has been detected.
Note: Do NOT select 'None' for media with only a single partition. It's very
rare for a disk to be 'Non-partitioned'.
```

```
C:\Users\Aadhitya\Downloads\testdisk-7.1\testdisk_win.exe
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

Disk dfr-01-ntfs.dd - 1073 MB / 1024 MiB
     CHS 131 255 63 - sector size=512

>[ Analyse  ] Analyse current partition structure and search for lost partitions
 [ Advanced ] Filesystem Utils
 [ Geometry ] Change disk geometry
 [ Options  ] Modify options
 [ MBR Code ] Write TestDisk MBR code to first sector
 [ Delete   ] Delete all data in the partition table
 [ Quit     ] Return to disk selection
_

Note: Correct disk geometry is required for a successful recovery. 'Analyse'
process may give some warnings if it thinks the logical geometry is mismatched.
```

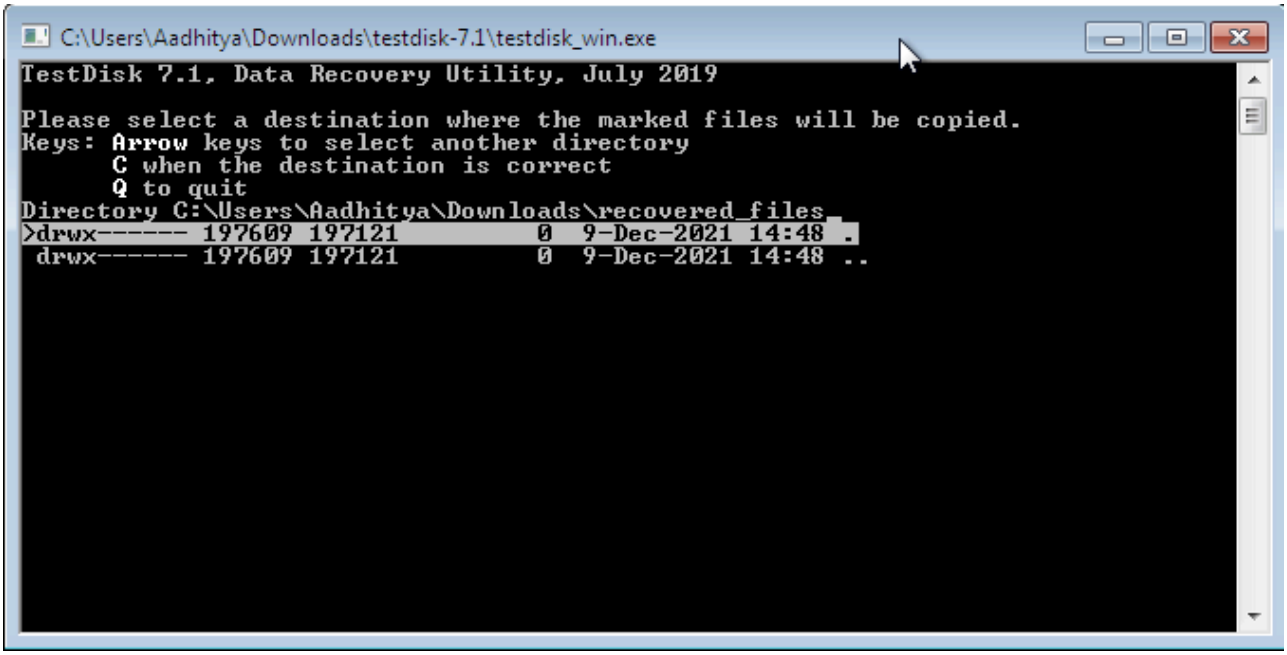
From the below image, we go to the list files, where the files are listed as shown in the further images :

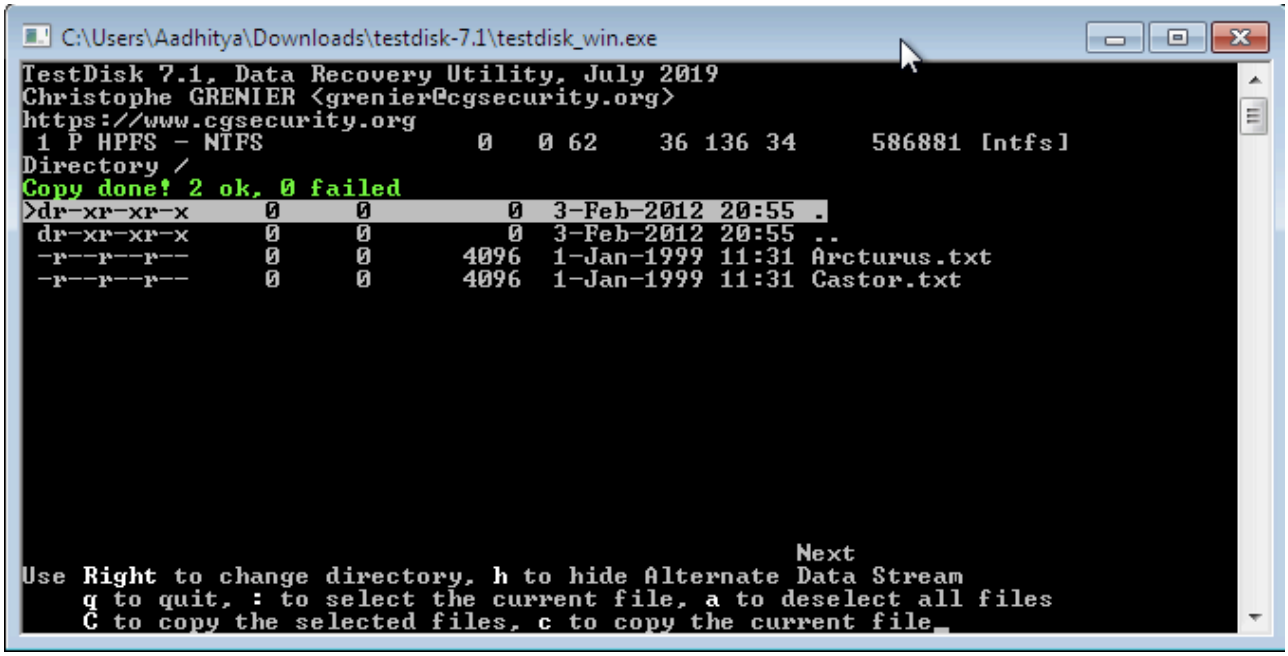




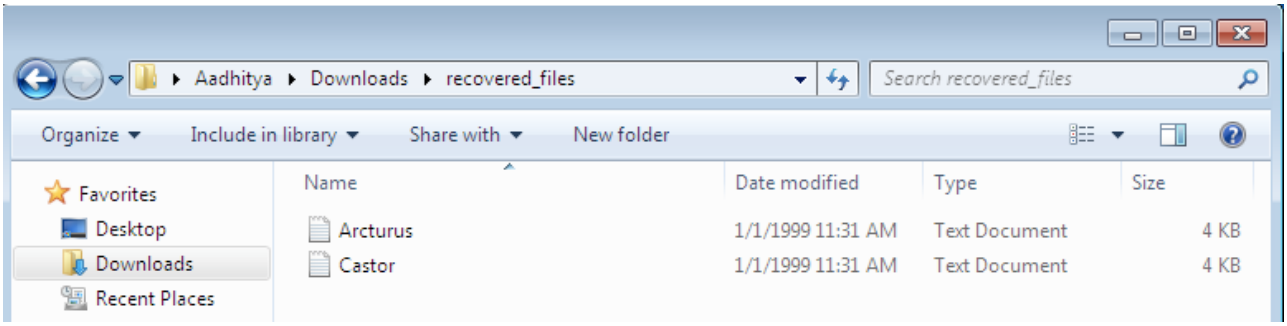
We then copy these both files and then paste them in a separate folder, as created, the copy process is shown above and the pasting is shown below :

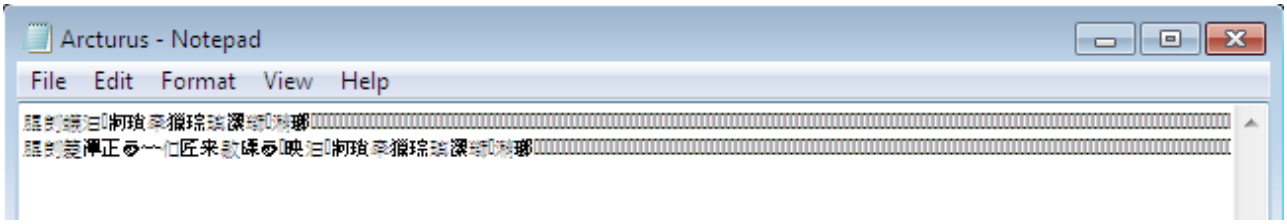
After this is done, we get a count of the number of files successfully copied, we can notice here that both have been copied successfully.

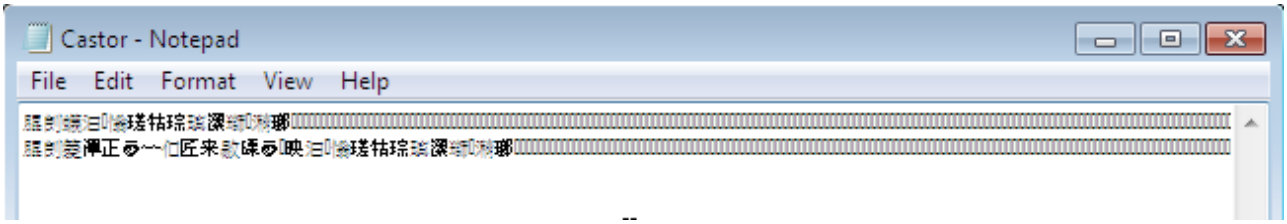




Now we can see these two files in the windows explorer, and when opened we can view these files as well. All this is shown in the images below :



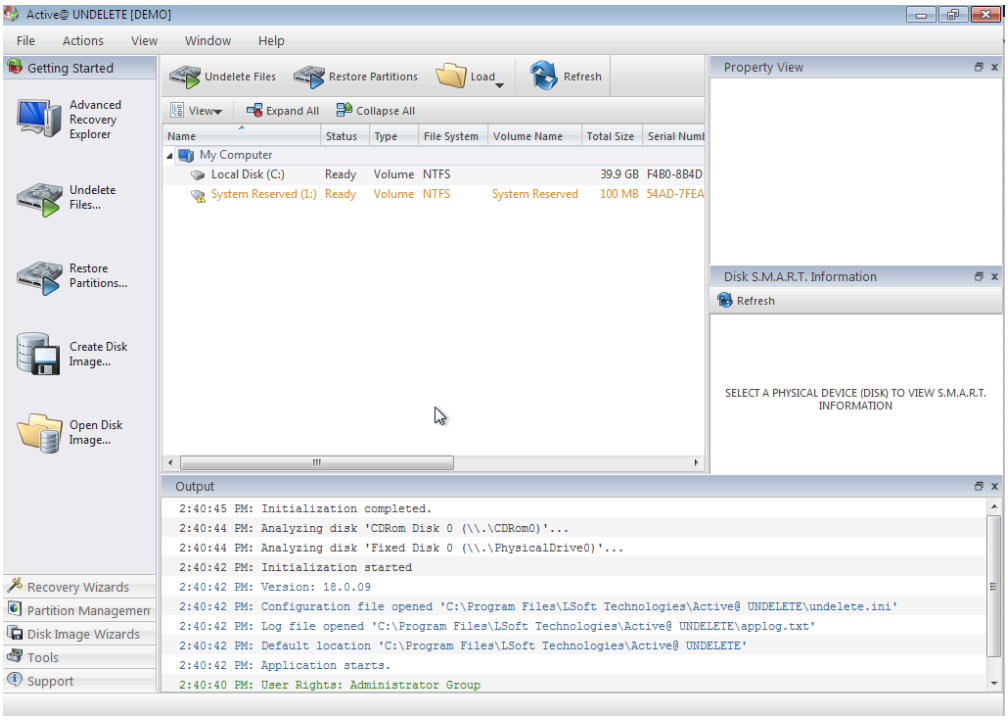


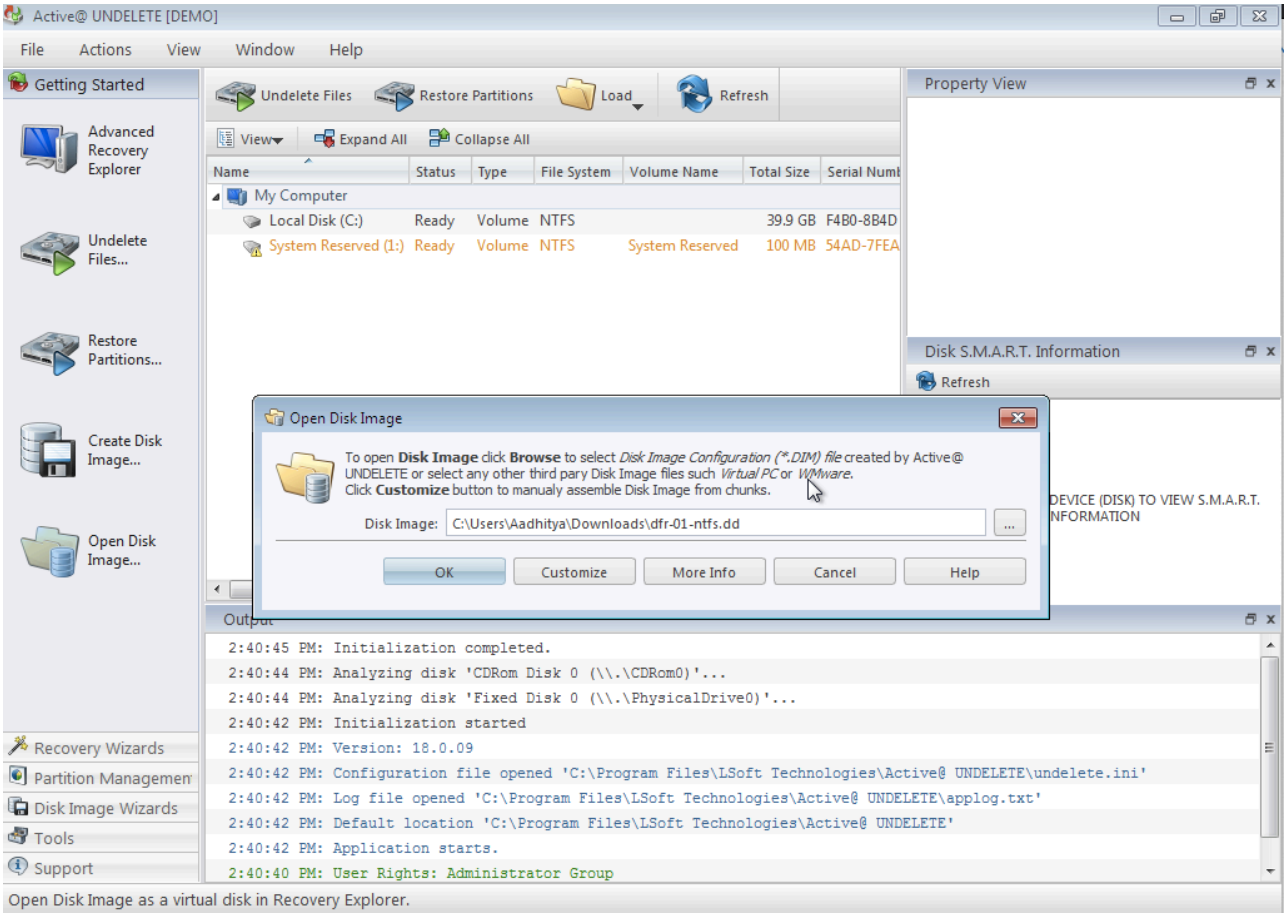


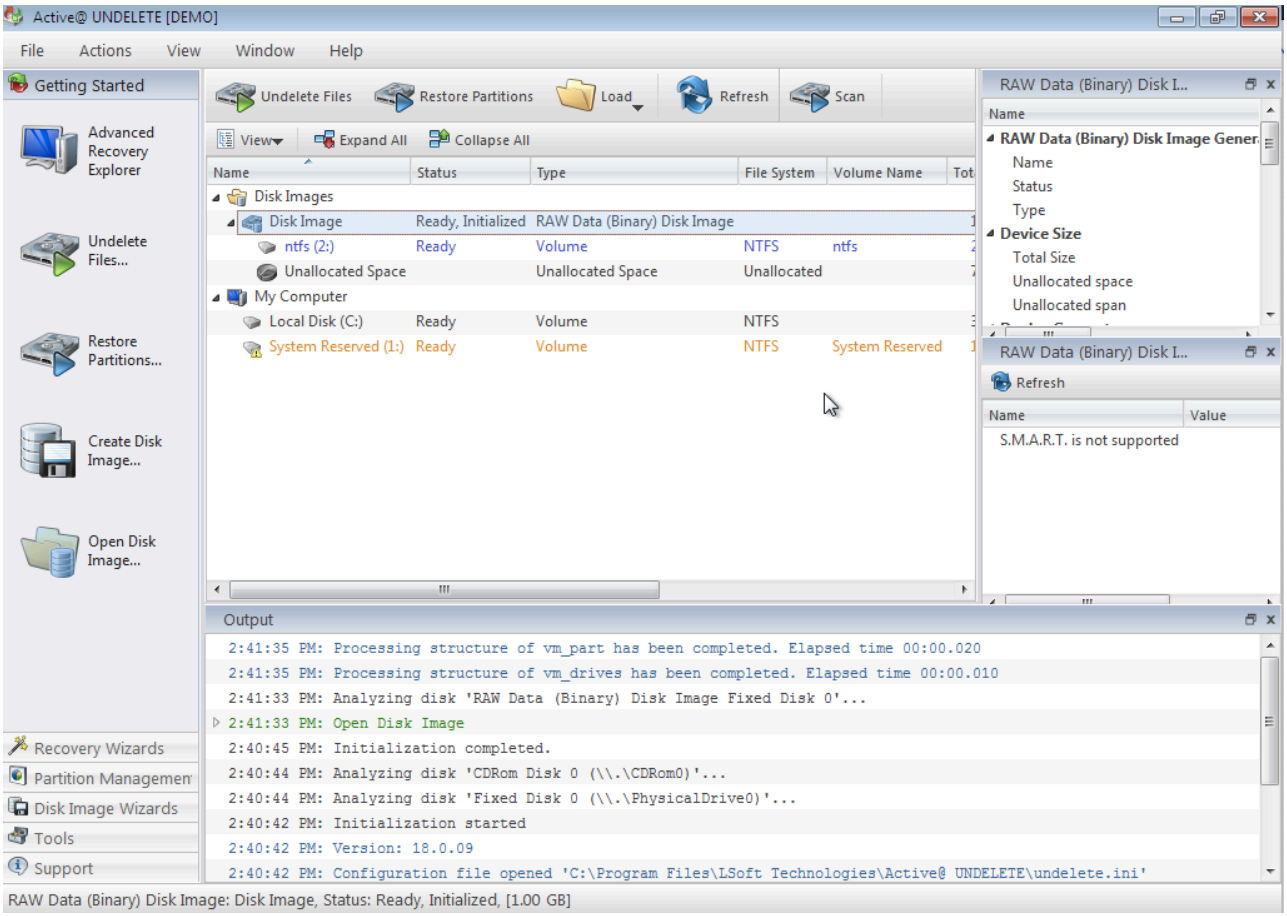
--

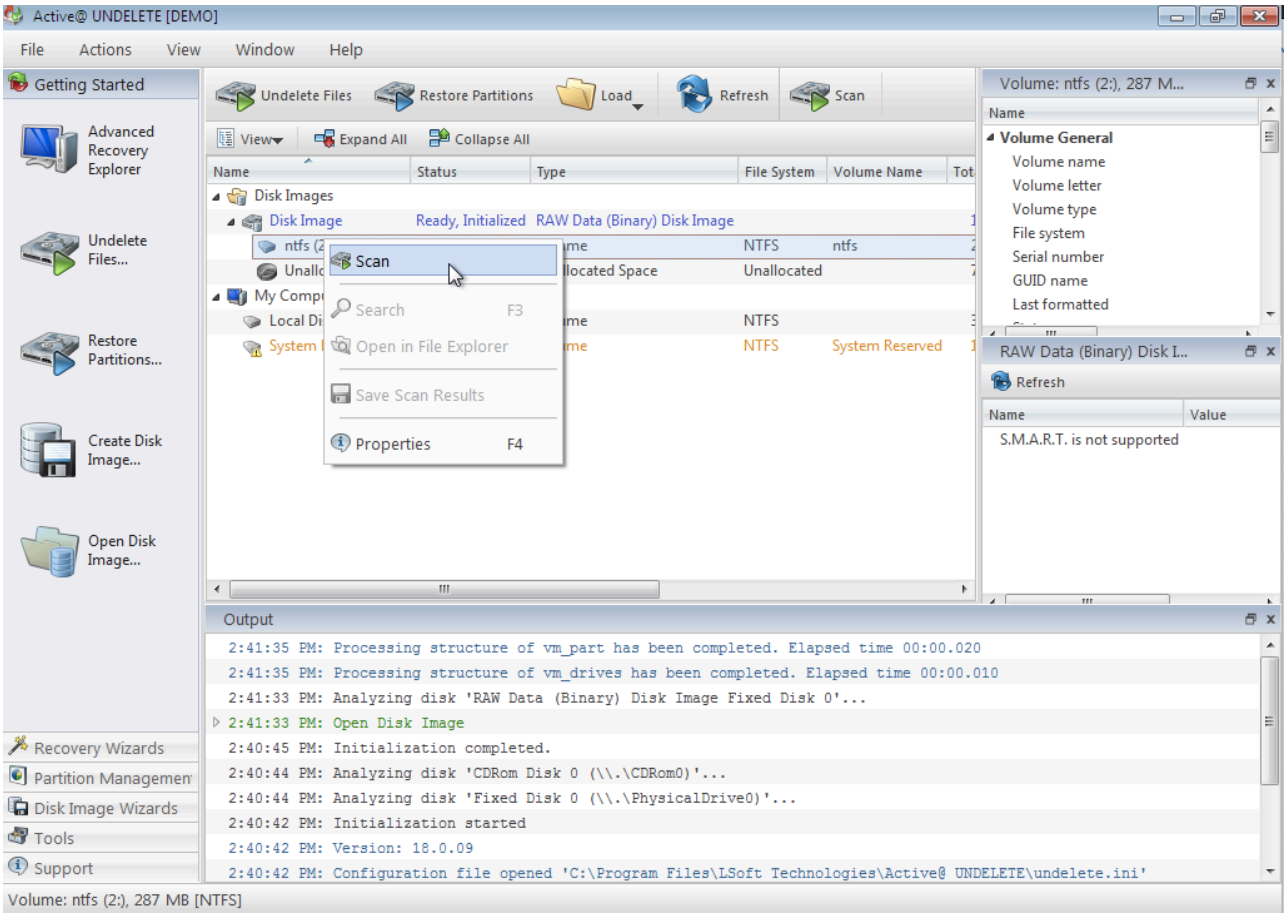
Thus, we were able to use test disk to perform a metadata based file recovery on the image provided to us. Thus the process has been done successfully.

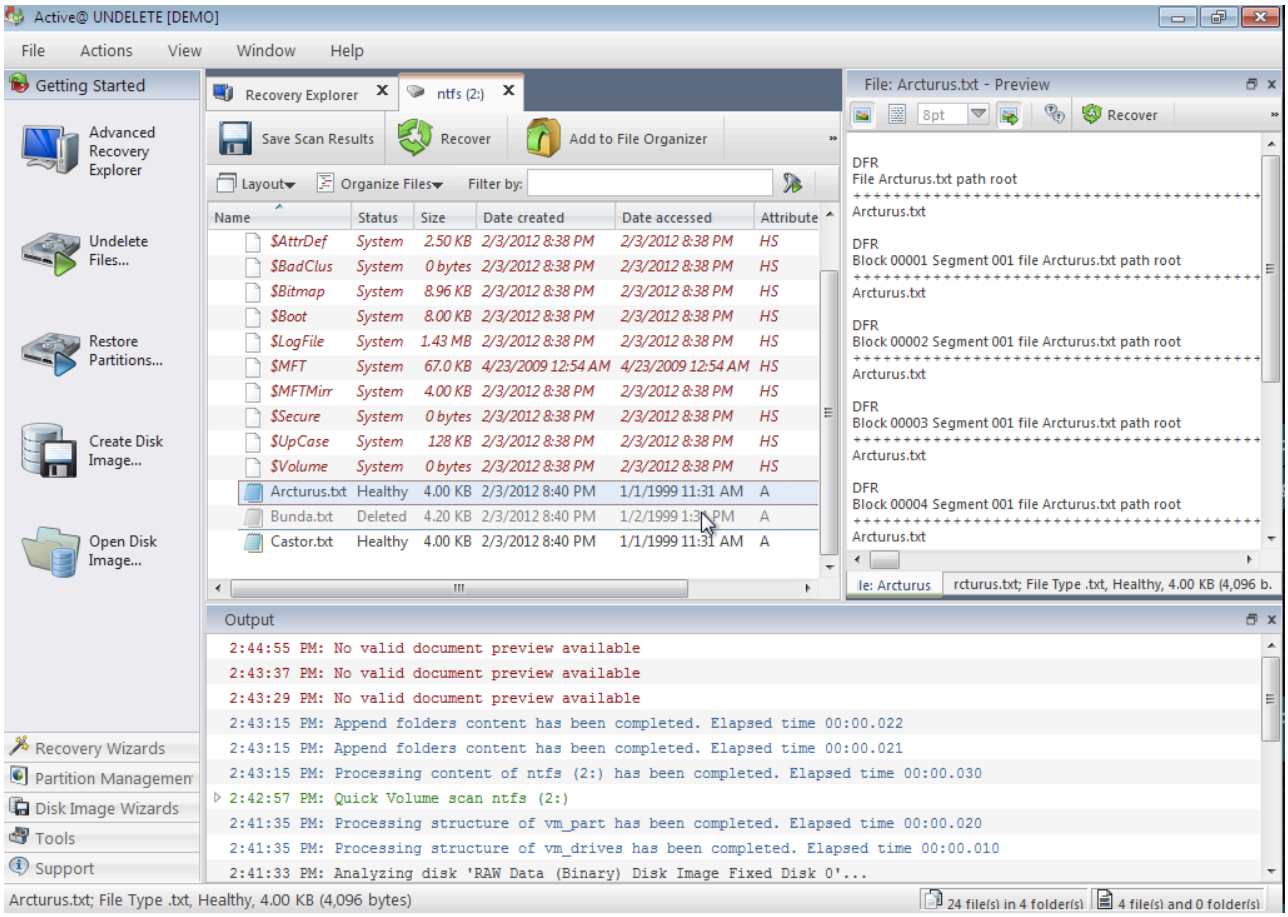
Additionally, we have also tried to solve this question using the Active Undelete tool, and the following images show the same :

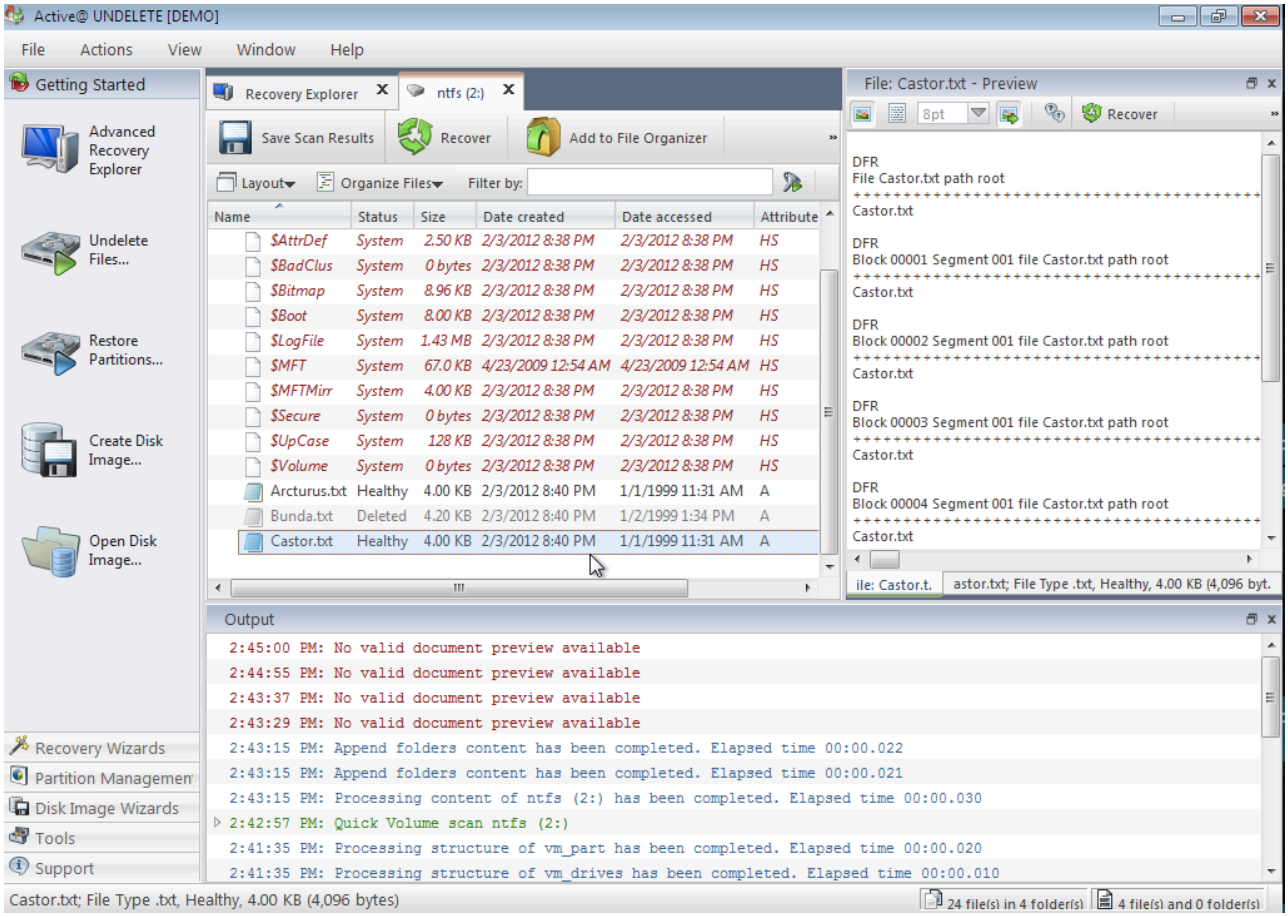





Active@ UNDELETE [DEMO]
File Actions View Window Help
Getting Started
Advanced Recovery Explorer
Undelete Files...
Restore Partitions...
Create Disk Image...
Open Disk Image...
Recovery Wizards
Partition Managemen
Disk Image Wizards
Tools
Support
Undelete Files
Restore Partitions
Load
Refresh
Scan
View
Expand All
Collapse All
Name Status Type File System Volume Name
Disk Images
Disk Image Ready, Initialized RAW Data (Binary) Disk Image
ntfs (2:) Ready Volume NTFS ntfs
Unallocated Space Unallocated Space Unallocated
My Computer
Local Disk (C:) Ready Volume NTFS
System Reserved (1:) Ready Volume NTFS System Reserved
RAW Data (Binary) Disk I...
Name
RAW Data (Binary) Disk Image Gener
Name
Status
Type
Device Size
Total Size
Unallocated space
Unallocated span
RAW Data (Binary) Disk I...
Refresh
Name Value
S.M.A.R.T. is not supported
Output
2:41:35 PM: Processing structure of vm_part has been completed. Elapsed time 00:00.020
2:41:35 PM: Processing structure of vm_drives has been completed. Elapsed time 00:00.010
2:41:33 PM: Analyzing disk 'RAW Data (Binary) Disk Image Fixed Disk 0'...
2:41:33 PM: Open Disk Image
2:40:45 PM: Initialization completed.
2:40:44 PM: Analyzing disk 'CDRom Disk 0 (\\.\CDRom0)'...
2:40:44 PM: Analyzing disk 'Fixed Disk 0 (\\.\PhysicalDrive0)'...
2:40:42 PM: Initialization started
2:40:42 PM: Version: 18.0.09
2:40:42 PM: Configuration file opened 'C:\Program Files\LSoft Technologies\Active@ UNDELETE\undelete.ini'
RAW Data (Binary) Disk Image: Disk Image, Status: Ready, Initialized, [1.00 GB]

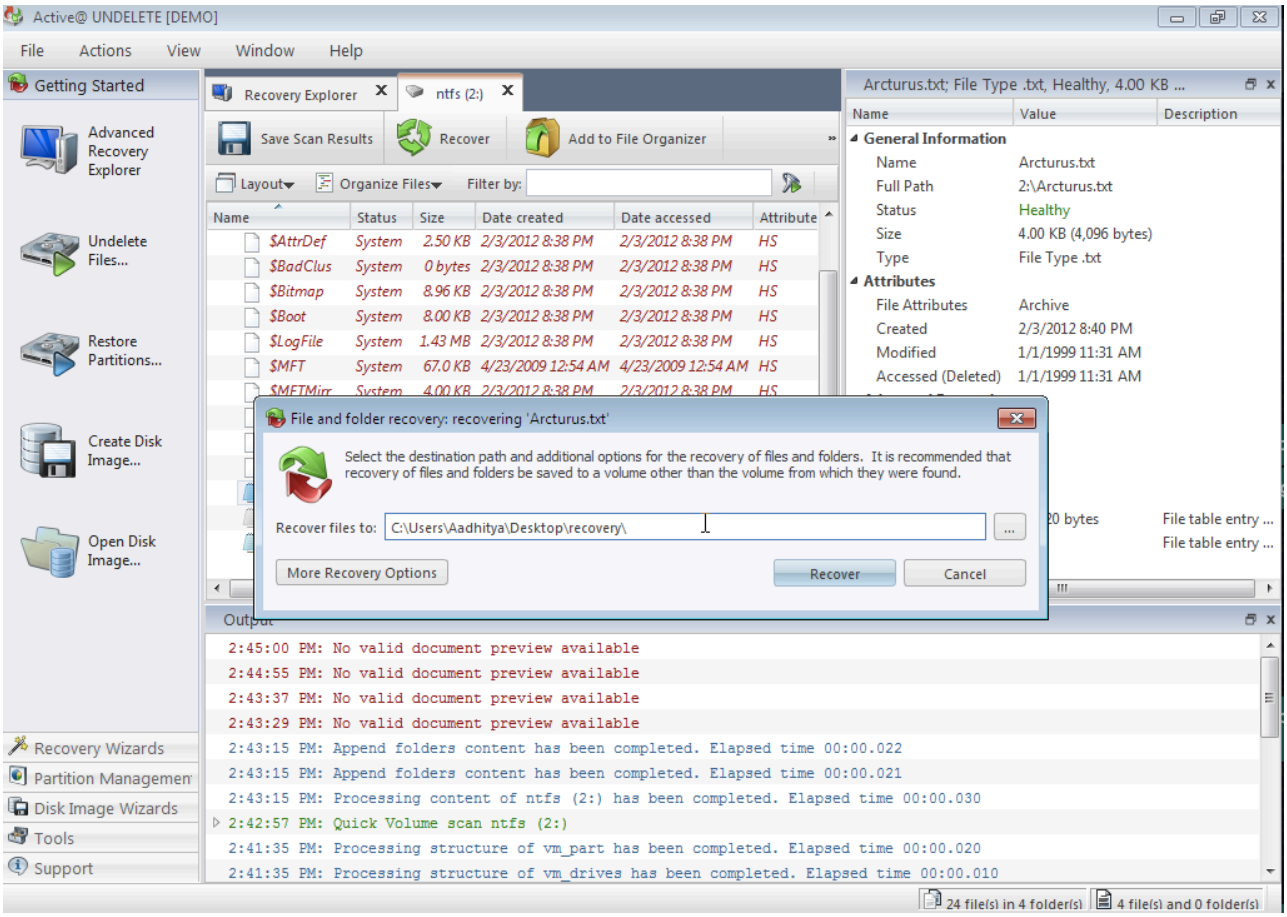

Active@ UNDELETE [DEMO]
File Actions View Window Help
Getting Started
Advanced Recovery Explorer
Undelete Files...
Restore Partitions...
Create Disk Image...
Open Disk Image...
Recovery Wizards
Partition Managemen
Disk Image Wizards
Tools
Support
Undelete Files
Restore Partitions
Load
Refresh
Scan
View
Expand All
Collapse All
Name Status Type File System Volume Name
Disk Images
Disk Image Ready, Initialized RAW Data (Binary) Disk Image
Scan
Search F3
Open in File Explorer
Save Scan Results
Properties F4
Volume: ntfs (2:), 287 M...
Name
Volume General
Volume name
Volume letter
Volume type
File system
Serial number
GUID name
Last formatted
RAW Data (Binary) Disk I...
Refresh
Name Value
S.M.A.R.T. is not supported
Output
2:41:35 PM: Processing structure of vm_part has been completed. Elapsed time 00:00.020
2:41:35 PM: Processing structure of vm_drives has been completed. Elapsed time 00:00.010
2:41:33 PM: Analyzing disk 'RAW Data (Binary) Disk Image Fixed Disk 0'...
2:41:33 PM: Open Disk Image
2:40:45 PM: Initialization completed.
2:40:44 PM: Analyzing disk 'CDRom Disk 0 (\\.\CDRom0)'...
2:40:44 PM: Analyzing disk 'Fixed Disk 0 (\\.\PhysicalDrive0)'...
2:40:42 PM: Initialization started
2:40:42 PM: Version: 18.0.09
2:40:42 PM: Configuration file opened 'C:\Program Files\LSoft Technologies\Active@ UNDELETE\undelete.ini'
Volume: ntfs (2:), 287 MB [NTFS]


Active@ UNDELETE [DEMO]
File Actions View Window Help
Getting Started
Advanced Recovery Explorer
Undelete Files...
Restore Partitions...
Create Disk Image...
Open Disk Image...
Recovery Wizards
Partition Managemen
Disk Image Wizards
Tools
Support
Recovery Explorer
ntfs (2:)
Save Scan Results
Recover
Add to File Organizer
Layout
Organize Files
Filter by:
Name Status Size Date created Date accessed Attribute
$AttrDef System 2.50 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$BadClus System 0 bytes 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Bitmap System 8.96 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Boot System 8.00 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$LogFile System 1.43 MB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$MFT System 67.0 KB 4/23/2009 12:54 AM 4/23/2009 12:54 AM HS
$MFTMirr System 4.00 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Secure System 0 bytes 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$UpCase System 128 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Volume System 0 bytes 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
Arcturus.txt Healthy 4.00 KB 2/3/2012 8:40 PM 1/1/1999 11:31 AM A
Bunda.txt Deleted 4.20 KB 2/3/2012 8:40 PM 1/2/1999 1:34 PM A
Castor.txt Healthy 4.00 KB 2/3/2012 8:40 PM 1/1/1999 11:31 AM A
File: Arcturus.txt - Preview
Recover
DFR
File Arcturus.txt path root
Arcturus.txt
DFR
Block 00001 Segment 001 file Arcturus.txt path root
Arcturus.txt
DFR
Block 00002 Segment 001 file Arcturus.txt path root
Arcturus.txt
DFR
Block 00003 Segment 001 file Arcturus.txt path root
Arcturus.txt
DFR
Block 00004 Segment 001 file Arcturus.txt path root
Arcturus.txt
Output
2:44:55 PM: No valid document preview available
2:43:37 PM: No valid document preview available
2:43:29 PM: No valid document preview available
2:43:15 PM: Append folders content has been completed. Elapsed time 00:00.022
2:43:15 PM: Append folders content has been completed. Elapsed time 00:00.021
2:43:15 PM: Processing content of ntfs (2:) has been completed. Elapsed time 00:00.030
2:42:57 PM: Quick Volume scan ntfs (2:)
2:41:35 PM: Processing structure of vm_part has been completed. Elapsed time 00:00.020
2:41:35 PM: Processing structure of vm_drives has been completed. Elapsed time 00:00.010
2:41:33 PM: Analyzing disk 'RAW Data (Binary) Disk Image Fixed Disk 0'...
Arcturus.txt; File Type .txt, Healthy, 4.00 KB (4,096 bytes)
24 file(s) in 4 folder(s)
4 file(s) and 0 folder(s)


Active@ UNDELETE [DEMO]
File Actions View Window Help
Getting Started
Advanced Recovery Explorer
Undelete Files...
Restore Partitions...
Create Disk Image...
Open Disk Image...
Recovery Wizards
Partition Managemen
Disk Image Wizards
Tools
Support
Recovery Explorer
ntfs (2:)
Save Scan Results
Recover
Add to File Organizer
Layout
Organize Files
Filter by:
Name Status Size Date created Date accessed Attribute
$AttrDef System 2.50 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$BadClus System 0 bytes 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Bitmap System 8.96 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Boot System 8.00 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$LogFile System 1.43 MB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$MFT System 67.0 KB 4/23/2009 12:54 AM 4/23/2009 12:54 AM HS
$MFTMirr System 4.00 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Secure System 0 bytes 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$UpCase System 128 KB 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
$Volume System 0 bytes 2/3/2012 8:38 PM 2/3/2012 8:38 PM HS
Arcturus.txt Healthy 4.00 KB 2/3/2012 8:40 PM 1/1/1999 11:31 AM A
Bunda.txt Deleted 4.20 KB 2/3/2012 8:40 PM 1/2/1999 1:34 PM A
Castor.txt Healthy 4.00 KB 2/3/2012 8:40 PM 1/1/1999 11:31 AM A
File: Castor.txt - Preview
Recover
DFR
File Castor.txt path root
Castor.txt
DFR
Block 00001 Segment 001 file Castor.txt path root
Castor.txt
DFR
Block 00002 Segment 001 file Castor.txt path root
Castor.txt
DFR
Block 00003 Segment 001 file Castor.txt path root
Castor.txt
DFR
Block 00004 Segment 001 file Castor.txt path root
Castor.txt
Output
2:45:00 PM: No valid document preview available
2:44:55 PM: No valid document preview available
2:43:37 PM: No valid document preview available
2:43:29 PM: No valid document preview available
2:43:15 PM: Append folders content has been completed. Elapsed time 00:00.022
2:43:15 PM: Append folders content has been completed. Elapsed time 00:00.021
2:43:15 PM: Processing content of ntfs (2:) has been completed. Elapsed time 00:00.030
2:42:57 PM: Quick Volume scan ntfs (2:)
2:41:35 PM: Processing structure of vm_part has been completed. Elapsed time 00:00.020
2:41:35 PM: Processing structure of vm_drives has been completed. Elapsed time 00:00.010
Castor.txt; File Type .txt, Healthy, 4.00 KB (4,096 bytes)
24 file(s) in 4 folder(s)
4 file(s) and 0 folder(s)

We can notice here that there are three text files, the two which are same as earlier, and also one another text file called as bunda.txt.

We will now use the same tool to extract all the three files. The extraction process is shown below :



Thus, we were able to recover two files and as well as one deleted files, so we can say that we have recovered all the non fragmented files.