Module 04: Data Acquisition and Duplication

Lab Scenario

Electronic evidence is fragile by nature and it can be very easily modified, destroyed, or damaged. Even the boot process can delete temporary files, modify stamps, or alter other data to writing data, and then create new files to the drive using the boot process.

Lab Objectives

The objective of this lab is to help students learn to monitor a system remotely and to extract hidden text strings and other tasks that include:

- Creating a dd image file
- Converting image file to a bootable virtual machine
- Memory acquisition (RAM) on Windows workstation
- Extracting the hidden content from hard drives

Overview of Data Acquisition and Duplication

Data acquisition is the process of gathering evidence or information. This can be done by using established methods to acquire data from a suspected storage media in order to get access to information about the crime or other incident and potentially using that data as evidence to convict a suspect.

Data duplication is a critical process in any computer forensic investigation. Many duplication tools are available that can duplicate or create a copy of data. To start an investigation, a person who wants to examine data on a suspect machine needs to create an image of the disk.

Lab Tasks

Recommended labs to assist you in data acquisition and duplication:

- Creating a dd image of a system drive
- Converting acquired image file to a bootable virtual machine
- Acquiring RAM from Windows workstation
- Viewing contents of forensic image file

Lab 1: Creating a dd Image of a System Drive

Lab Scenario

Jason, a forensics investigator, is appointed to examine a suspect's computer. Examining suspect's machine directly would result in loss of data and hence it is necessary to generate a forensic copy/image of the suspect machine's hard disk. The investigator needs to perform forensic examination on the acquired evidence file and retrieve potential artifacts that could be useful for investigation.

As a forensics investigator, you need to know how to create a dd image of any system drive.

Lab Objectives

A dd image is a disk image file that is a bit-by-bit copy of hard disk or a partition of a disk that includes all the files/folders, deleted files, files left in slack space and unallocated space, file system information, etc.

The objective of this lab is to help you understand how to create a dd image of system drive using dd tool in Windows OS.

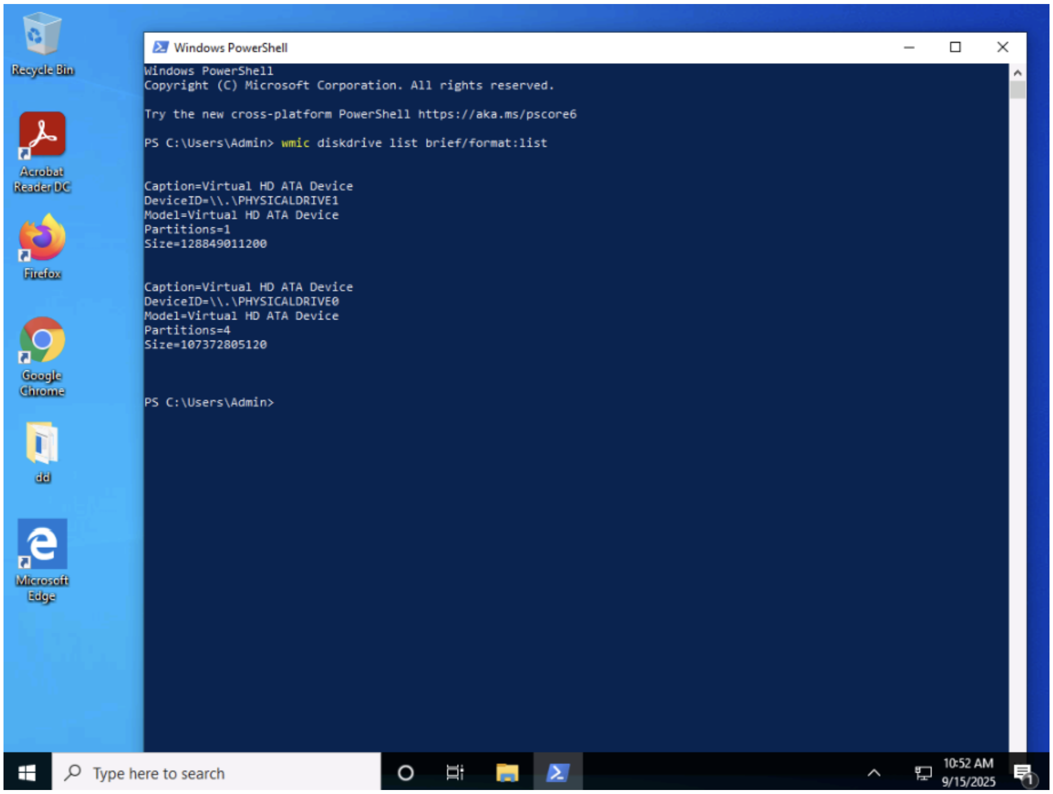
Overview of the Lab

This lab familiarizes you with physical acquisition of a system drive/disk using the dd command.

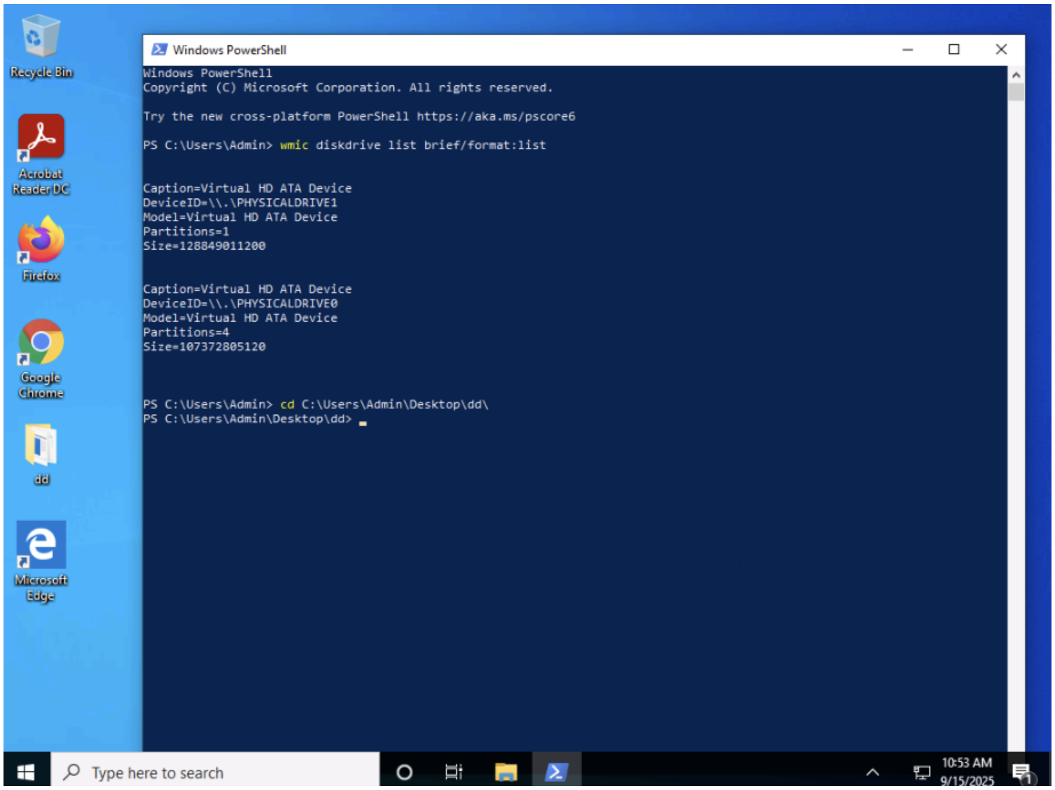
Physical acquisition of the suspect disk/drive usually requires an external data storage medium, such as a hard disk or a pen drive, to collect the image generated during physical acquisition process.

Physical acquisition of the suspect disk/drive usually requires an external data storage medium, such as a hard disk or a pen drive, to collect the image generated during physical acquisition process.

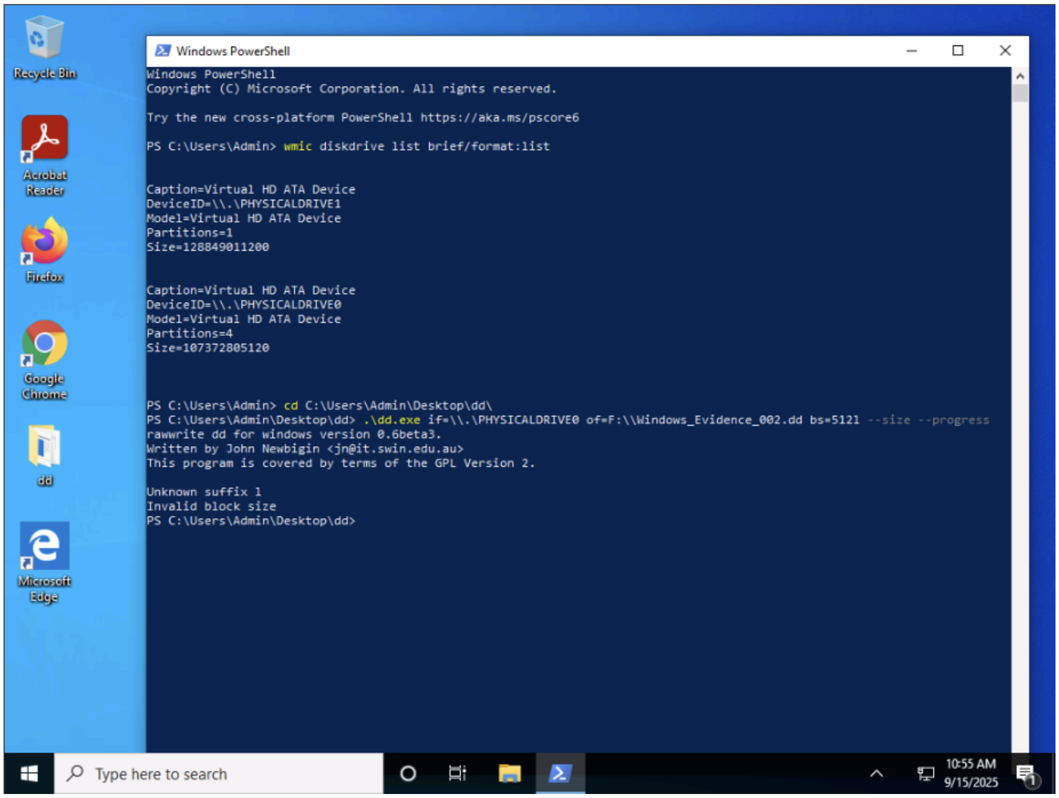
In this lab, we will be performing physical acquisition of the primary disk/internal disk (**PHYSICALDRIVE0**) of the Windows 10 virtual machine using **dd** command. Acquisition usually requires an external data storage device for storing the image. However, since this is a lab environment, we are using a secondary physical disk (**PHYSICALDRIVE1**, created during the lab setup) assuming it as an external storage device to store the image. Therefore, we will be treating this disk as an external disk for this lab.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Admin> wmic diskdrive list brief/format:list


Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE1
Model=Virtual HD ATA Device
Partitions=1
Size=128849011200


Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE0
Model=Virtual HD ATA Device
Partitions=4
Size=107372805120



PS C:\Users\Admin>
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Admin> wmic diskdrive list brief/format:list


Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE1
Model=Virtual HD ATA Device
Partitions=1
Size=128849011200


Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE0
Model=Virtual HD ATA Device
Partitions=4
Size=107372805120



PS C:\Users\Admin> cd C:\Users\Admin\Desktop\dd\
PS C:\Users\Admin\Desktop\dd> _
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Admin> wmic diskdrive list brief/format:list


Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE1
Model=Virtual HD ATA Device
Partitions=1
Size=128849011200


Caption=Virtual HD ATA Device
DeviceID=\\.\PHYSICALDRIVE0
Model=Virtual HD ATA Device
Partitions=4
Size=107372805120



PS C:\Users\Admin> cd C:\Users\Admin\Desktop\dd\
PS C:\Users\Admin\Desktop\dd> .\dd.exe if=\\.\PHYSICALDRIVE0 of=F:\\Windows_Evidence_002.dd bs=5121 --size --progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

Unknown suffix 1
Invalid block size
PS C:\Users\Admin\Desktop\dd>
```

The dd.exe command was used to create a physical image of PHYSICALDRIVE0. The tool processed the disk, but some sectors could not be read, resulting in an error for those sectors. The image was still created and can be used for further forensic analysis.

Lab 2: Converting Acquired Image File to a Bootable Virtual Machine

Lab Scenario

During an investigation, the investigator needs to perform data acquisition on the suspect's machine in a forensically sound manner. In some cases, the investigator might need to create a live environment of the machine and boot the forensically acquired image file into the virtual machine so that the investigator can extract additional artifacts that may not have been discovered in the static analysis. These additional artifacts might serve as an evidence and help the investigator solve the case.

As a forensic investigator, you should know how to convert an acquired image file to a bootable virtual machine.

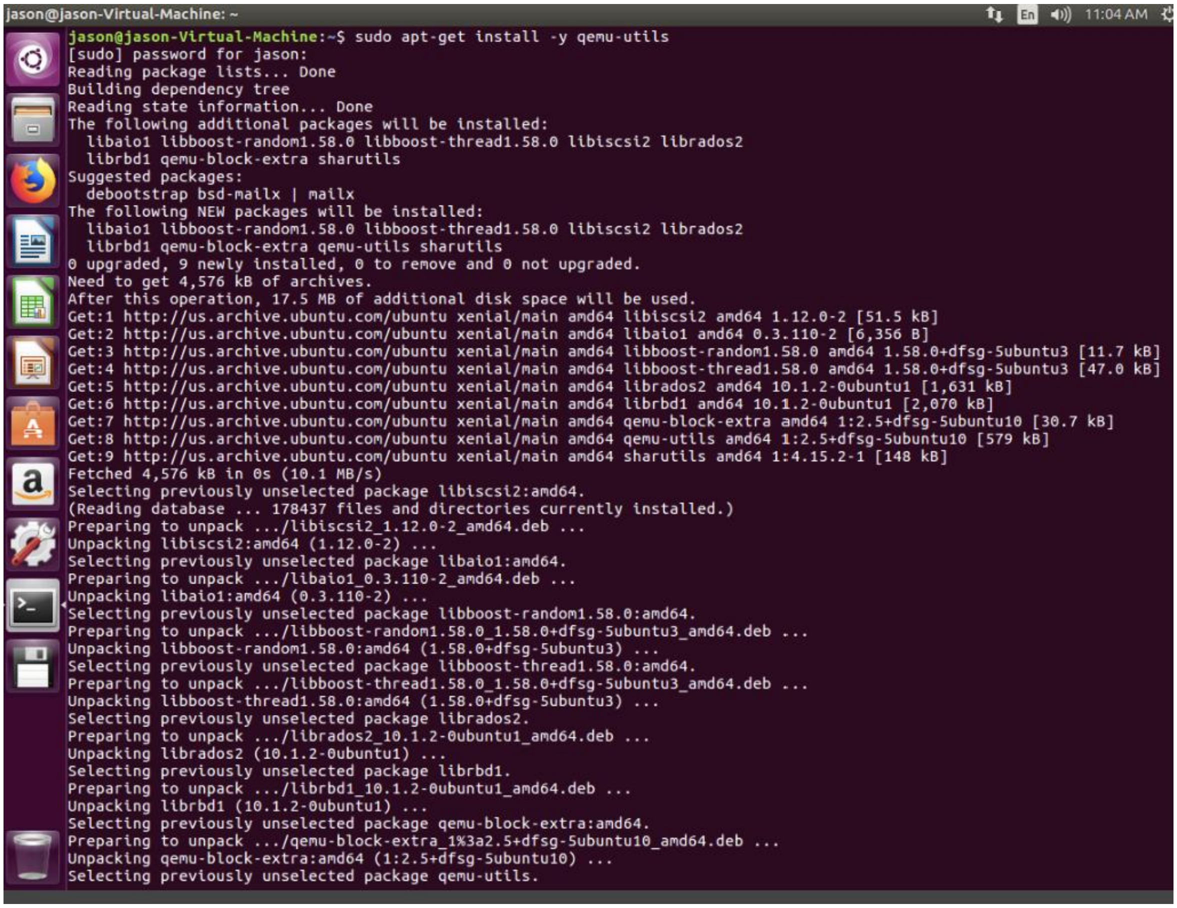
Lab Objectives

A virtual machine runs a dedicated OS on shared physical hardware resources and provides the same functionality as an actual computer.

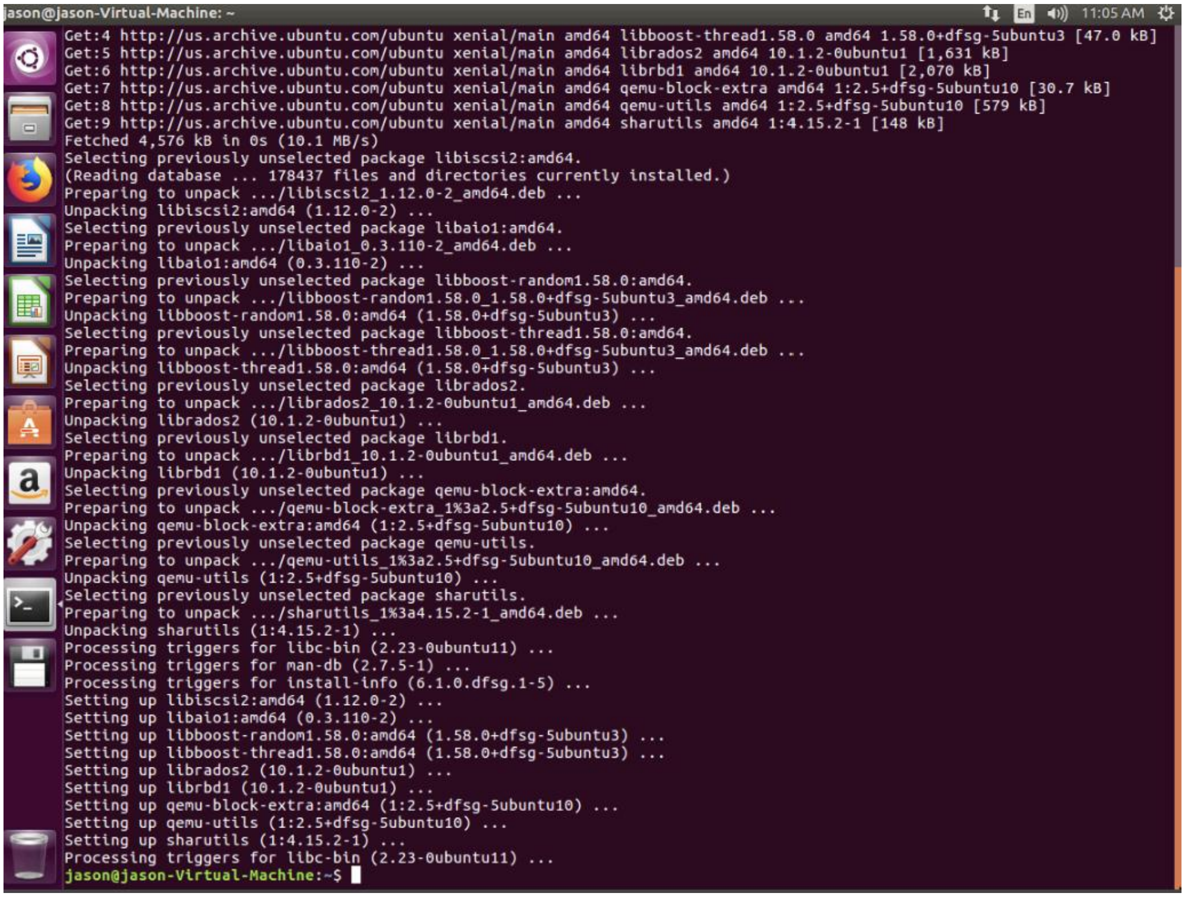
The objective of this lab is to help you understand how to convert an acquired image file to a bootable virtual machine.

Overview of the Lab

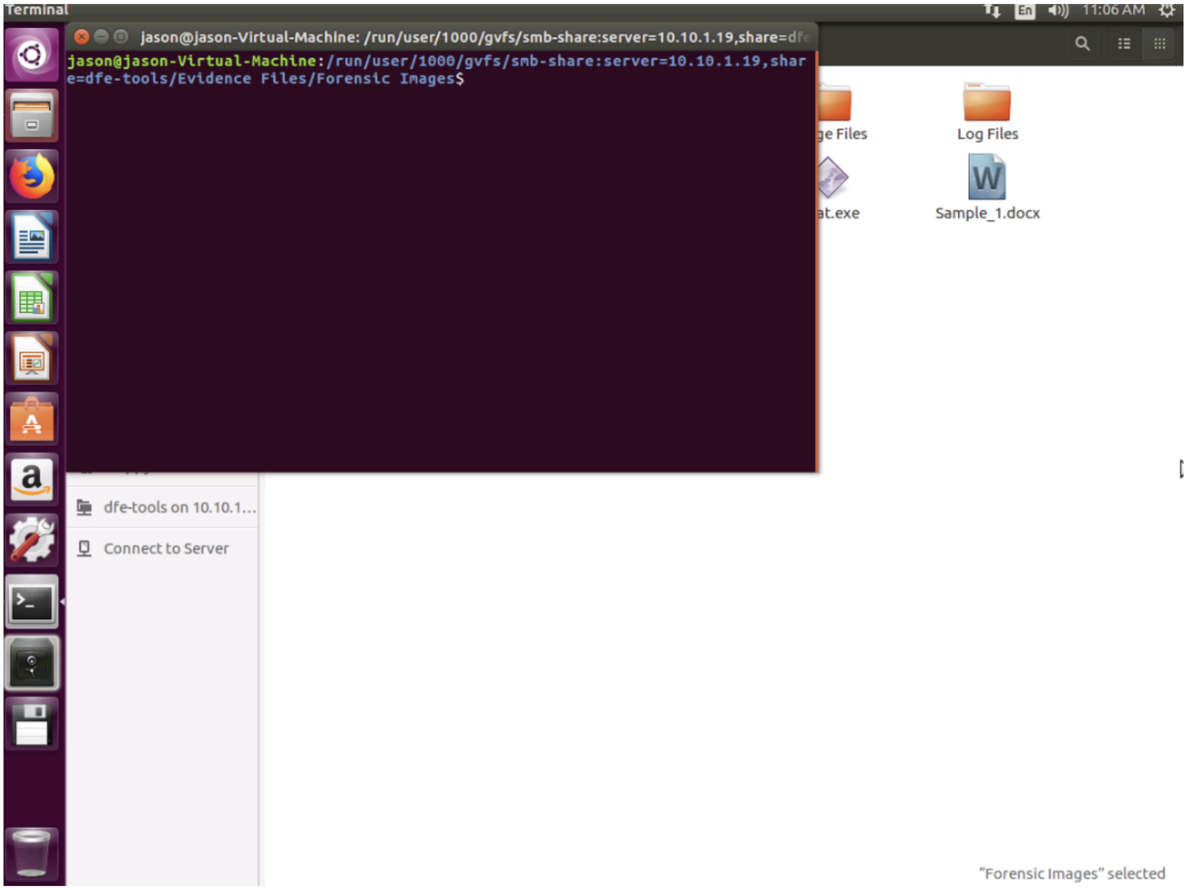
In the lab **Creating a dd Image of a System Drive**, we saw how to create a dd image of an entire disk. In this lab, we shall demonstrate how to convert that disk into a bootable virtual machine in order to launch the virtual machine and examine artifacts.



```
jason@jason-Virtual-Machine:~$ sudo apt-get install -y qemu-utils
[sudo] password for jason:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libaio1 libboost-random1.58.0 libboost-thread1.58.0 libiscsi2 librados2
  librbd1 qemu-block-extra sharutils
Suggested packages:
  debootstrap bsd-mailx | mailx
The following NEW packages will be installed:
  libaio1 libboost-random1.58.0 libboost-thread1.58.0 libiscsi2 librados2
  librbd1 qemu-block-extra qemu-utils sharutils
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,576 kB of archives.
After this operation, 17.5 MB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libiscsi2 amd64 1.12.0-2 [51.5 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libaio1 amd64 0.3.110-2 [6,356 B]
Get:3 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libboost-random1.58.0 amd64 1.58.0+dfsg-5ubuntu3 [11.7 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libboost-thread1.58.0 amd64 1.58.0+dfsg-5ubuntu3 [47.0 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 librados2 amd64 10.1.2-0ubuntu1 [1,631 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 librbd1 amd64 10.1.2-0ubuntu1 [2,070 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 qemu-block-extra amd64 1:2.5+dfsg-5ubuntu10 [30.7 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 qemu-utils amd64 1:2.5+dfsg-5ubuntu10 [579 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 sharutils amd64 1:4.15.2-1 [148 kB]
Fetched 4,576 kB in 0s (10.1 MB/s)
Selecting previously unselected package libiscsi2:amd64.
(Reading database ... 178437 files and directories currently installed.)
Preparing to unpack .../libiscsi2_1.12.0-2_amd64.deb ...
Unpacking libiscsi2:amd64 (1.12.0-2) ...
Selecting previously unselected package libaio1:amd64.
Preparing to unpack .../libaio1_0.3.110-2_amd64.deb ...
Unpacking libaio1:amd64 (0.3.110-2) ...
Selecting previously unselected package libboost-random1.58.0:amd64.
Preparing to unpack .../libboost-random1.58.0_1.58.0+dfsg-5ubuntu3_amd64.deb ...
Unpacking libboost-random1.58.0:amd64 (1.58.0+dfsg-5ubuntu3) ...
Selecting previously unselected package libboost-thread1.58.0:amd64.
Preparing to unpack .../libboost-thread1.58.0_1.58.0+dfsg-5ubuntu3_amd64.deb ...
Unpacking libboost-thread1.58.0:amd64 (1.58.0+dfsg-5ubuntu3) ...
Selecting previously unselected package librados2.
Preparing to unpack .../librados2_10.1.2-0ubuntu1_amd64.deb ...
Unpacking librados2 (10.1.2-0ubuntu1) ...
Selecting previously unselected package librbd1.
Preparing to unpack .../librbd1_10.1.2-0ubuntu1_amd64.deb ...
Unpacking librbd1 (10.1.2-0ubuntu1) ...
Selecting previously unselected package qemu-block-extra:amd64.
Preparing to unpack .../qemu-block-extra_1%3a2.5+dfsg-5ubuntu10_amd64.deb ...
Unpacking qemu-block-extra:amd64 (1:2.5+dfsg-5ubuntu10) ...
Selecting previously unselected package qemu-utils.
```

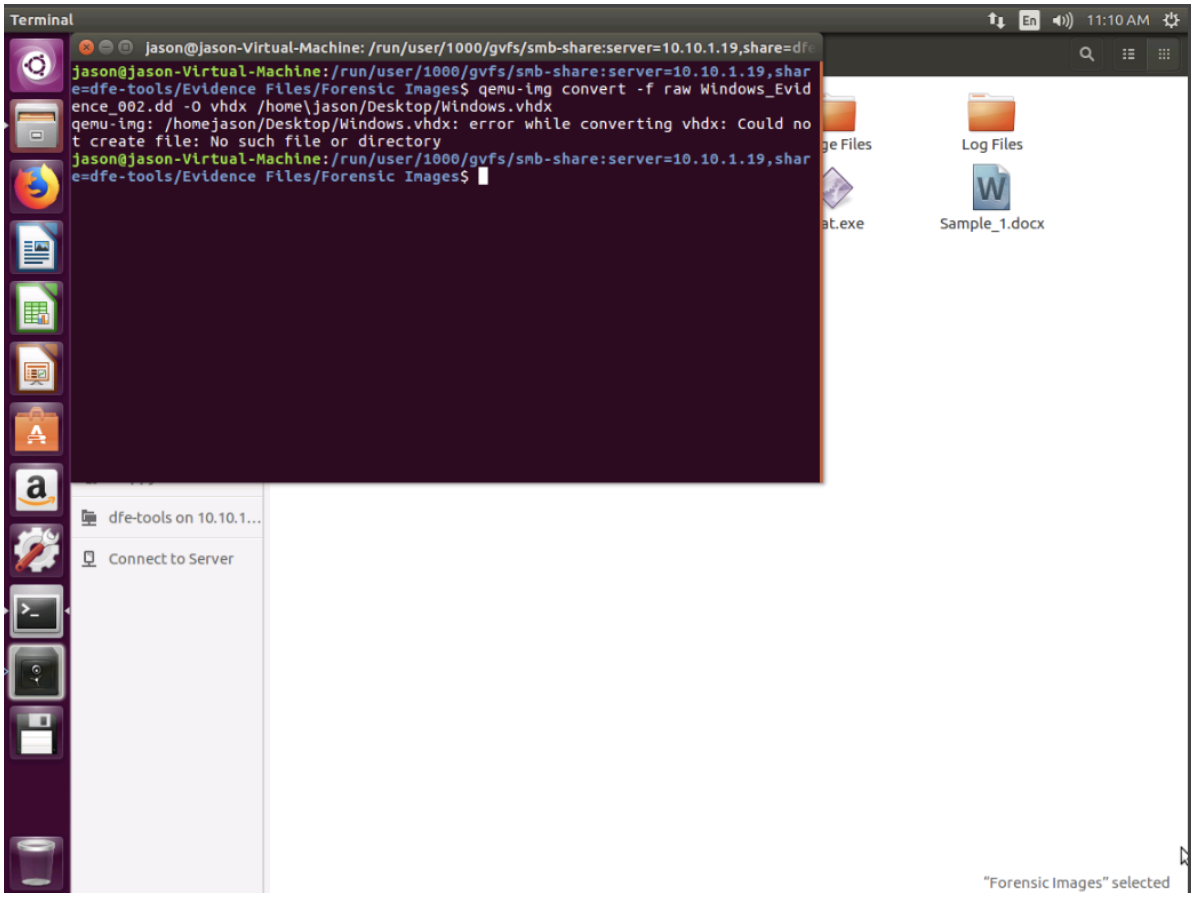


```
Get:4 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libboost-thread1.58.0 amd64 1.58.0+dfsg-5ubuntu3 [47.0 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 librados2 amd64 10.1.2-0ubuntu1 [1,631 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 librbd1 amd64 10.1.2-0ubuntu1 [2,070 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 qemu-block-extra amd64 1:2.5+dfsg-5ubuntu10 [30.7 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 qemu-utils amd64 1:2.5+dfsg-5ubuntu10 [579 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 sharutils amd64 1:4.15.2-1 [148 kB]
Fetched 4,576 kB in 0s (10.1 MB/s)
Selecting previously unselected package libiscsi2:amd64.
(Reading database ... 178437 files and directories currently installed.)
Preparing to unpack .../libiscsi2_1.12.0-2_amd64.deb ...
Unpacking libiscsi2:amd64 (1.12.0-2) ...
Selecting previously unselected package libaio1:amd64.
Preparing to unpack .../libaio1_0.3.110-2_amd64.deb ...
Unpacking libaio1:amd64 (0.3.110-2) ...
Selecting previously unselected package libboost-random1.58.0:amd64.
Preparing to unpack .../libboost-random1.58.0_1.58.0+dfsg-5ubuntu3_amd64.deb ...
Unpacking libboost-random1.58.0:amd64 (1.58.0+dfsg-5ubuntu3) ...
Selecting previously unselected package libboost-thread1.58.0:amd64.
Preparing to unpack .../libboost-thread1.58.0_1.58.0+dfsg-5ubuntu3_amd64.deb ...
Unpacking libboost-thread1.58.0:amd64 (1.58.0+dfsg-5ubuntu3) ...
Selecting previously unselected package librados2.
Preparing to unpack .../librados2_10.1.2-0ubuntu1_amd64.deb ...
Unpacking librados2 (10.1.2-0ubuntu1) ...
Selecting previously unselected package librbd1.
Preparing to unpack .../librbd1_10.1.2-0ubuntu1_amd64.deb ...
Unpacking librbd1 (10.1.2-0ubuntu1) ...
Selecting previously unselected package qemu-block-extra:amd64.
Preparing to unpack .../qemu-block-extra_1%3a2.5+dfsg-5ubuntu10_amd64.deb ...
Unpacking qemu-block-extra:amd64 (1:2.5+dfsg-5ubuntu10) ...
Selecting previously unselected package qemu-utils.
Preparing to unpack .../qemu-utils_1%3a2.5+dfsg-5ubuntu10_amd64.deb ...
Unpacking qemu-utils (1:2.5+dfsg-5ubuntu10) ...
Selecting previously unselected package sharutils.
Preparing to unpack .../sharutils_1%3a4.15.2-1_amd64.deb ...
Unpacking sharutils (1:4.15.2-1) ...
Processing triggers for libc-bin (2.23-0ubuntu11) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for install-info (6.1.0.dfsg.1-5) ...
Setting up libiscsi2:amd64 (1.12.0-2) ...
Setting up libaio1:amd64 (0.3.110-2) ...
Setting up libboost-random1.58.0:amd64 (1.58.0+dfsg-5ubuntu3) ...
Setting up libboost-thread1.58.0:amd64 (1.58.0+dfsg-5ubuntu3) ...
Setting up librados2 (10.1.2-0ubuntu1) ...
Setting up librbd1 (10.1.2-0ubuntu1) ...
Setting up qemu-block-extra:amd64 (1:2.5+dfsg-5ubuntu10) ...
Setting up qemu-utils (1:2.5+dfsg-5ubuntu10) ...
Setting up sharutils (1:4.15.2-1) ...
Processing triggers for libc-bin (2.23-0ubuntu11) ...
jason@jason-Virtual-Machine:~$
```



Terminal
En
11:06 AM
jason@jason-Virtual-Machine: /run/user/1000/gvfs/smb-share:server=10.10.1.19,share=dfe
ge Files
Log Files
at.exe
Sample_1.docx
dfe-tools on 10.10.1…
Connect to Server
"Forensic Images" selected

```
jason@jason-Virtual-Machine:/run/user/1000/gvfs/smb-share:server=10.10.1.19,shar
e=dfe-tools/Evidence Files/Forensic Images$
```


Terminal
11:10 AM
jason@jason-Virtual-Machine: /run/user/1000/gvfs/smb-share:server=10.10.1.19,share=dfe
ge Files
Log Files
at.exe
Sample_1.docx
dfe-tools on 10.10.1...
Connect to Server
"Forensic Images" selected

```
jason@jason-Virtual-Machine:/run/user/1000/gvfs/smb-share:server=10.10.1.19,shar
e=dfe-tools/Evidence Files/Forensic Images$ qemu-img convert -f raw Windows_Evid
ence_002.dd -O vhdx /home\jason/Desktop/Windows.vhdx
qemu-img: /homejason/Desktop/Windows.vhdx: error while converting vhdx: Could no
t create file: No such file or directory
jason@jason-Virtual-Machine:/run/user/1000/gvfs/smb-share:server=10.10.1.19,shar
e=dfe-tools/Evidence Files/Forensic Images$ 
```

Attempted to convert the physical disk image `Windows_Evidence_002.dd` to VHDX format using `qemu-img`. The conversion failed because the specified directory did not exist. This illustrates the steps for preparing images for Hyper-V virtualization.

Lab 3: Acquiring RAM from Windows Workstations

Lab Scenario

James, a forensic investigator, is performing live analysis on a suspect's computer. In this process, the investigator needs to primarily capture the RAM dump of the machine as RAM contains volatile data that is lost when the machine loses power. In this scenario, the investigator performs RAM acquisition on Windows workstation.

To be an expert forensic investigator, one must understand how to acquire a RAM dump from Windows and Linux OSes.

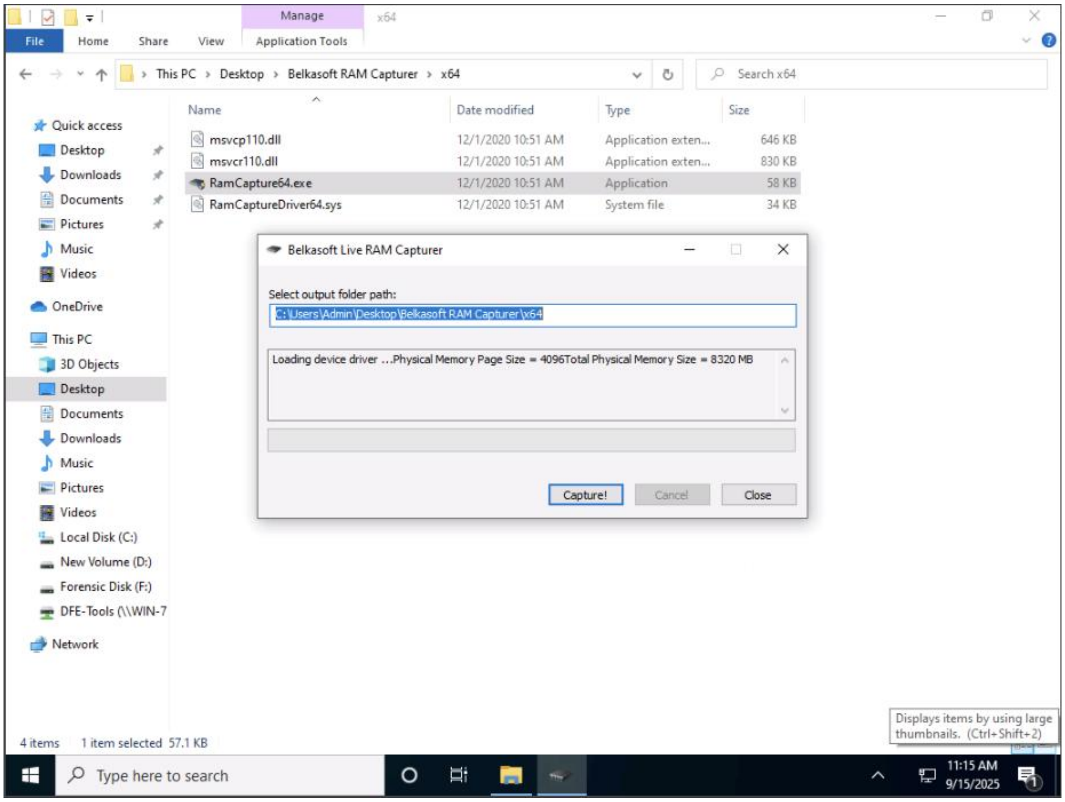
Lab Objectives

RAM (Random Access Memory) is a volatile-memory storage found in computing devices that temporarily holds the data your device needs to access.

The objective of this lab is to help students learn how to perform RAM acquisition on Windows workstation.

Overview of the Lab

This lab familiarizes you with the **Belkasoft RAM Capturer** tool, which helps perform RAM acquisition on Windows systems.



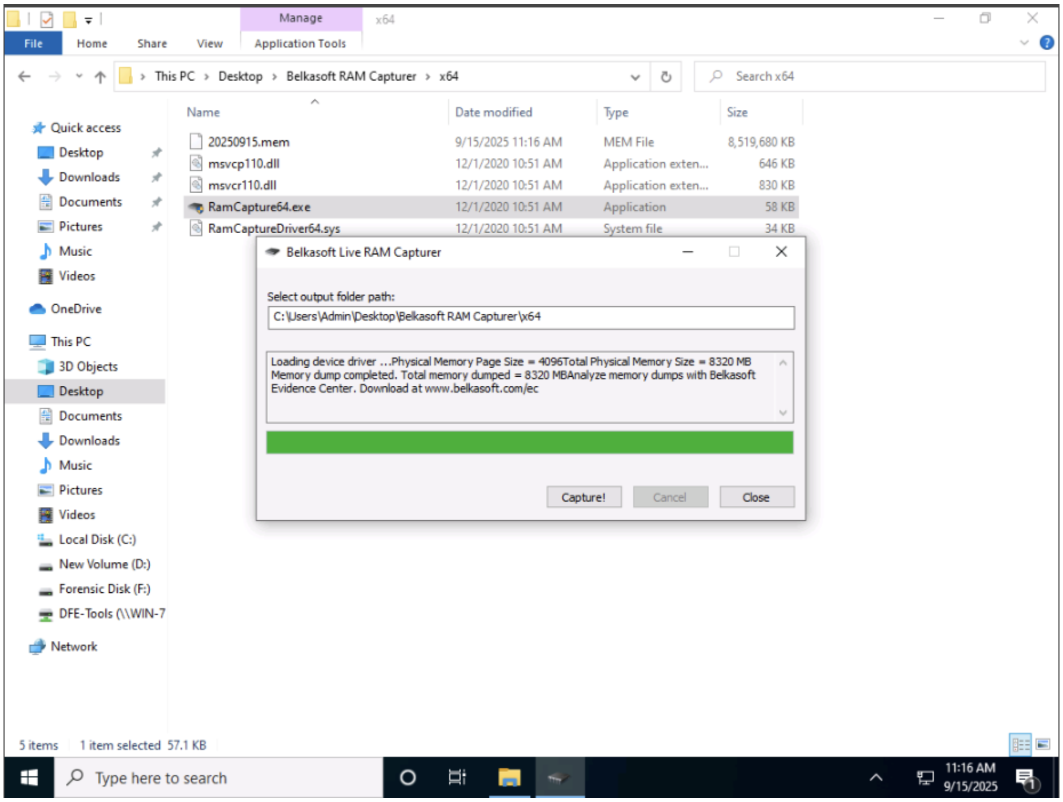
Name	Date modified	Type	Size
msvcp110.dll	12/1/2020 10:51 AM	Application exten...	646 KB
msvcr110.dll	12/1/2020 10:51 AM	Application exten...	830 KB
RamCapture64.exe	12/1/2020 10:51 AM	Application	58 KB
RamCaptureDriver64.sys	12/1/2020 10:51 AM	System file	34 KB

Belkasoft Live RAM Capturer

Select output folder path: C:\Users\Admin\Desktop\Belkasoft RAM Capturer\x64

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 8320 MB
```

Capture!
Cancel
Close
Displays items by using large thumbnails. (Ctrl+Shift+2)
4 items 1 item selected 57.1 KB
Type here to search
11:15 AM
9/15/2025

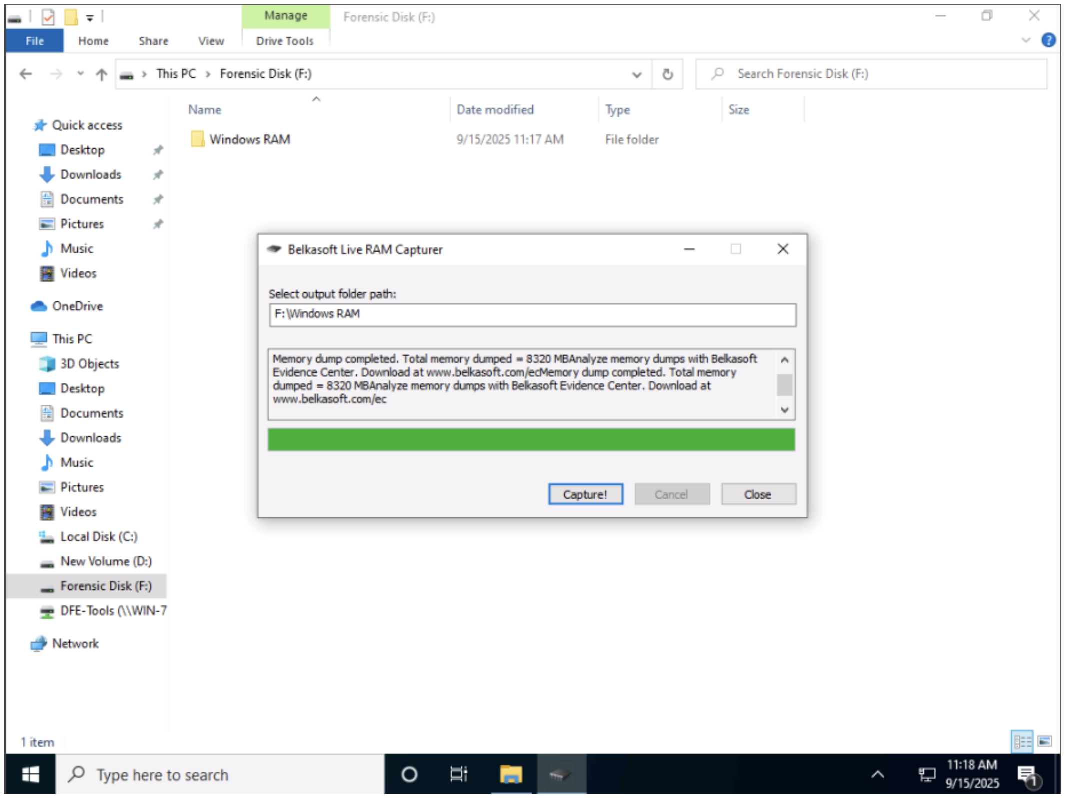


Name	Date modified	Type	Size
20250915.mem	9/15/2025 11:16 AM	MEM File	8,519,680 KB
msvcp110.dll	12/1/2020 10:51 AM	Application exten...	646 KB
msvcr110.dll	12/1/2020 10:51 AM	Application exten...	830 KB
RamCapture64.exe	12/1/2020 10:51 AM	Application	58 KB
RamCaptureDriver64.sys	12/1/2020 10:51 AM	System file	34 KB

Belkasoft Live RAM Capturer

Select output folder path: C:\Users\Admin\Desktop\Belkasoft RAM Capturer\x64

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 8320 MB
Memory dump completed. Total memory dumped = 8320 MBAnalyze memory dumps with Belkasoft
Evidence Center. Download at www.belkasoft.com/ec
```

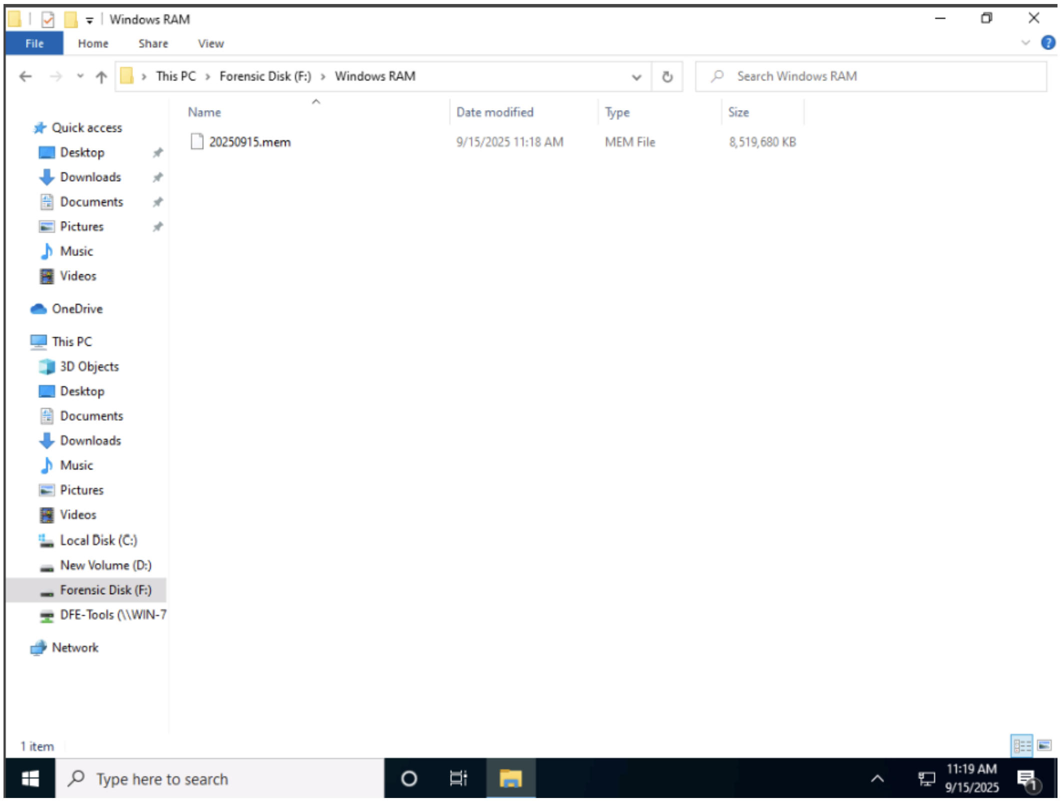


Name	Date modified	Type	Size
Windows RAM	9/15/2025 11:17 AM	File folder	

Belkasoft Live RAM Capturer

Select output folder path: F:\Windows RAM

```
Memory dump completed. Total memory dumped = 8320 MBAnalyze memory dumps with Belkasoft
Evidence Center. Download at www.belkasoft.com/ecMemory dump completed. Total memory
dumped = 8320 MBAnalyze memory dumps with Belkasoft Evidence Center. Download at
www.belkasoft.com/ec
```



Name	Date modified	Type	Size
20250915.mem	9/15/2025 11:18 AM	MEM File	8,519,680 KB

Lab 4: Viewing Contents of Forensic Image File

Lab Scenario

As part of investigation in an information theft case, senior investigator Alex has concluded scanning all the systems using the AccessData FTK Imager tool to know if the deleted files on the systems contain any information of evidentiary value. The tool saves the investigator's time as it eliminates the hectic process of recovering every deleted file from the system.

To be an expert forensic investigator, you must understand how to assess forensic images and collect the evidentiary data from those images.

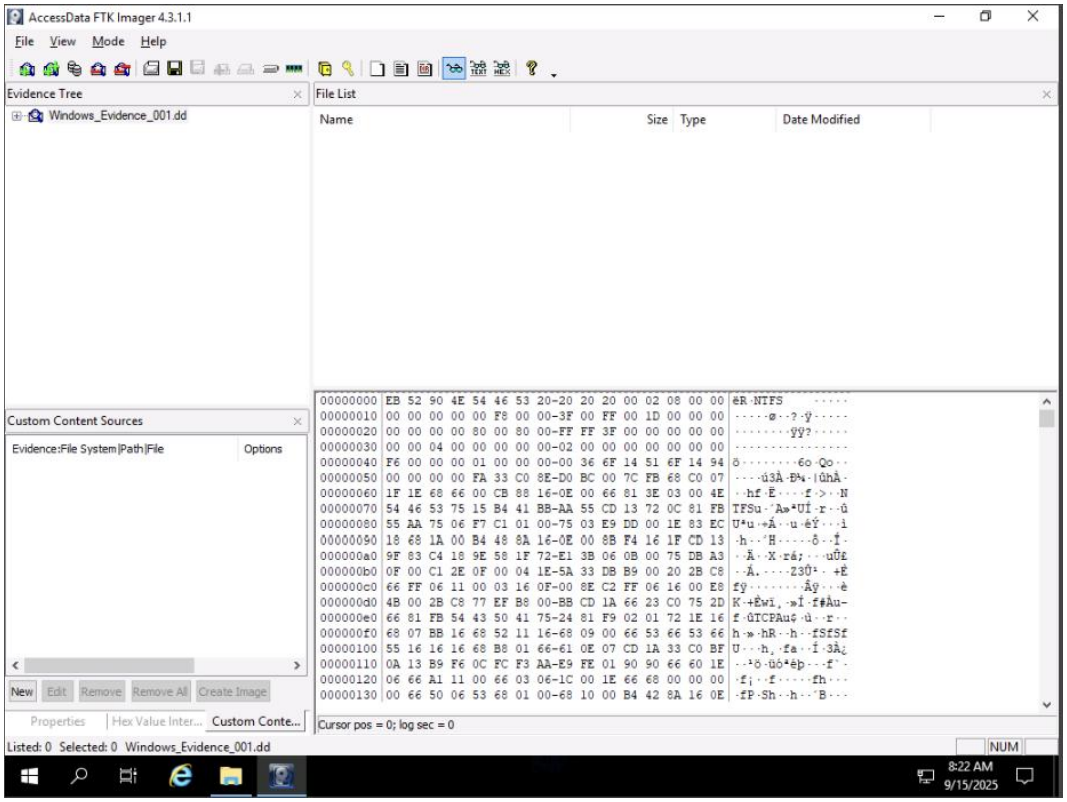
Lab Objectives

After acquiring the forensic image of the hard disk, the forensic investigator needs to preview the contents of the image file to see if it contains any evidence useful for investigation or any additional analysis is required.

The objective of this lab is to help students learn how to use **AccessData FTK Imager** for viewing forensics images.

Overview of the Lab

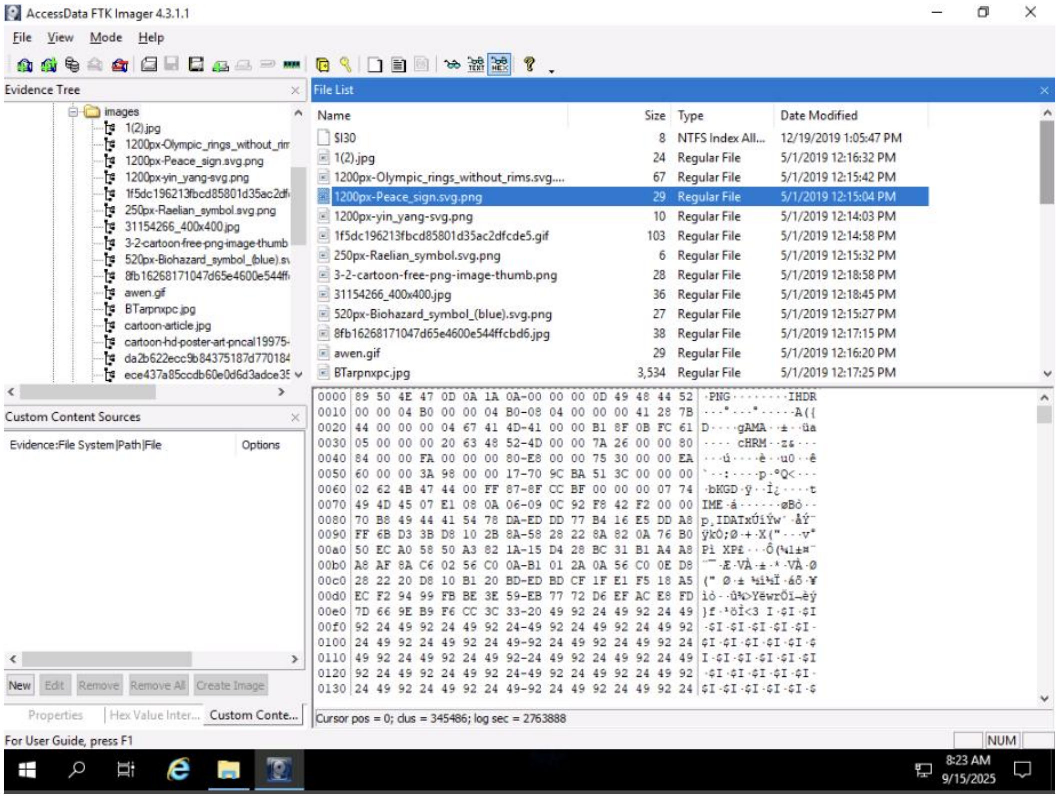
This lab familiarizes you with the **AccessData FTK Imager** tool and helps you learn how to investigate forensic images of computer data without subjecting the original evidence to modification. It also helps you understand how to assess electronic evidence to determine whether further analysis of the evidence with a forensic tool is necessary.



```
00000000 EB 52 90 4E 54 46 53 20-20 20 20 00 02 08 00 00 ëR·NTFS    ·····
00000010 00 00 00 00 00 F8 00 00-3F 00 FF 00 1D 00 00 00 ·····ø··?·ÿ·····
00000020 00 00 00 00 80 00 80 00-FF FF 3F 00 00 00 00 00 ········ÿÿ?·····
00000030 00 00 04 00 00 00 00 00-02 00 00 00 00 00 00 00 ················
00000040 F6 00 00 00 01 00 00 00-00 36 6F 14 51 6F 14 94 ö········6o·Qo··
00000050 00 00 00 00 FA 33 C0 8E-D0 BC 00 7C FB 68 C0 07 ····ú3À·Ð¼·|ûhÀ·
00000060 1F 1E 68 66 00 CB 88 16-0E 00 66 81 3E 03 00 4E ··hf·Ë····f·>··N
00000070 54 46 53 75 15 B4 41 BB-AA 55 CD 13 72 0C 81 FB TFSu·´A»ªUÍ·r··û
00000080 55 AA 75 06 F7 C1 01 00-75 03 E9 DD 00 1E 83 EC Uªu·÷Á··u·éÝ···ì
00000090 18 68 1A 00 B4 48 8A 16-0E 00 8B F4 16 1F CD 13 ·h··´H·····ô··Í·
000000a0 9F 83 C4 18 9E 58 1F 72-E1 3B 06 0B 00 75 DB A3 ··Ä··X·rá;···uÛ£
000000b0 0F 00 C1 2E 0F 00 04 1E-5A 33 DB B9 00 20 2B C8 ··Á.····Z3Û¹· +È
000000c0 66 FF 06 11 00 03 16 0F-00 8E C2 FF 06 16 00 E8 fÿ········Âÿ···è
000000d0 4B 00 2B C8 77 EF B8 00-BB CD 1A 66 23 C0 75 2D K·+Èwï¸·»Í·f#Àu-
000000e0 66 81 FB 54 43 50 41 75-24 81 F9 02 01 72 1E 16 f·ûTCPAu$·ù··r··
000000f0 68 07 BB 16 68 52 11 16-68 09 00 66 53 66 53 66 h·»·hR··h··fSfSf
00000100 55 16 16 16 68 B8 01 66-61 0E 07 CD 1A 33 C0 BF U···h¸·fa··Í·3À¿
00000110 0A 13 B9 F6 0C FC F3 AA-E9 FE 01 90 90 66 60 1E ··¹ö·üóªéþ···f`·
00000120 06 66 A1 11 00 66 03 06-1C 00 1E 66 68 00 00 00 ·f¡··f·····fh···
00000130 00 66 50 06 53 68 01 00-68 10 00 B4 42 8A 16 0E ·fP·Sh··h··´B···
```

Cursor pos = 0; log sec = 0

Listed: 0 Selected: 0 Windows_Evidence_001.dd

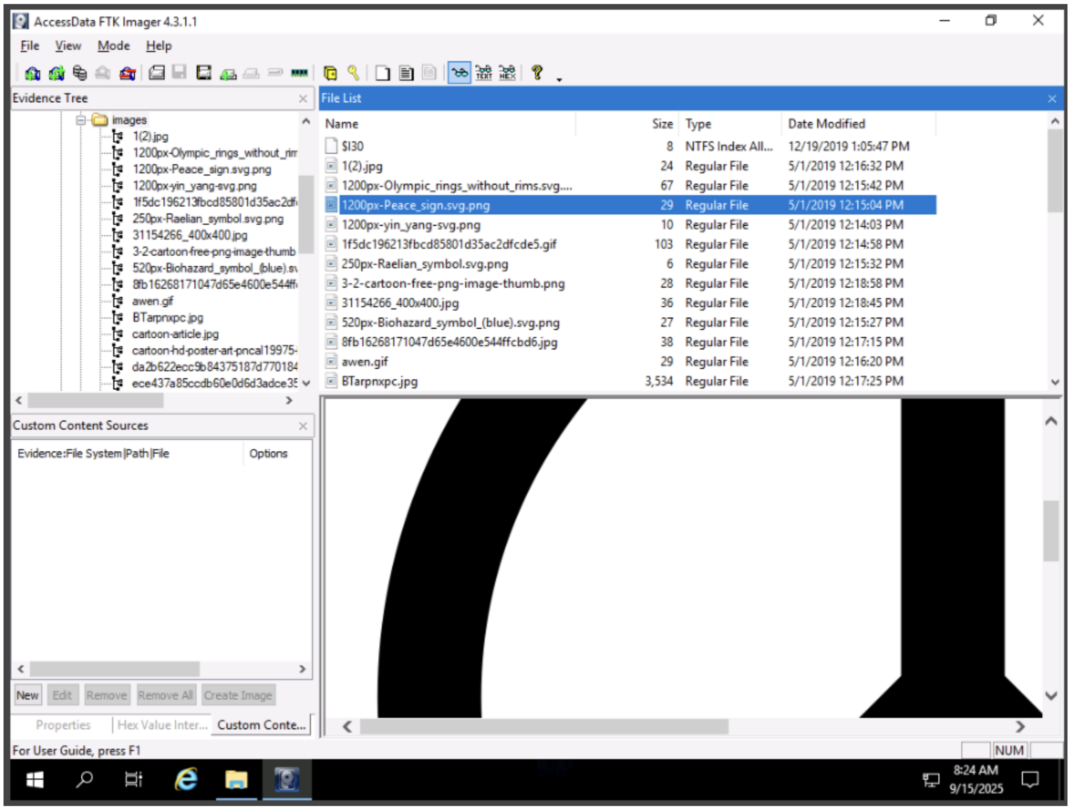


AccessData FTK Imager 4.3.1.1
File
View
Mode
Help
Evidence Tree
images
1(2).jpg
1200px-Olympic_rings_without_rim
1200px-Peace_sign.svg.png
1200px-yin_yang-svg.png
1f5dc196213fbcd85801d35ac2df
250px-Raelian_symbol.svg.png
31154266_400x400.jpg
3-2-cartoon-free-png-image-thumb
520px-Biohazard_symbol_(blue).sv
8fb16268171047d65e4600e544ff
awen.gif
BTarpnxpc.jpg
cartoon-article.jpg
cartoon-hd-poster-art-pncal19975-
da2b622ecc9b84375187d770184
ece437a85ccdb60e0d6d3adce35
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
File List
For User Guide, press F1
NUM
8:23 AM
9/15/2025

Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

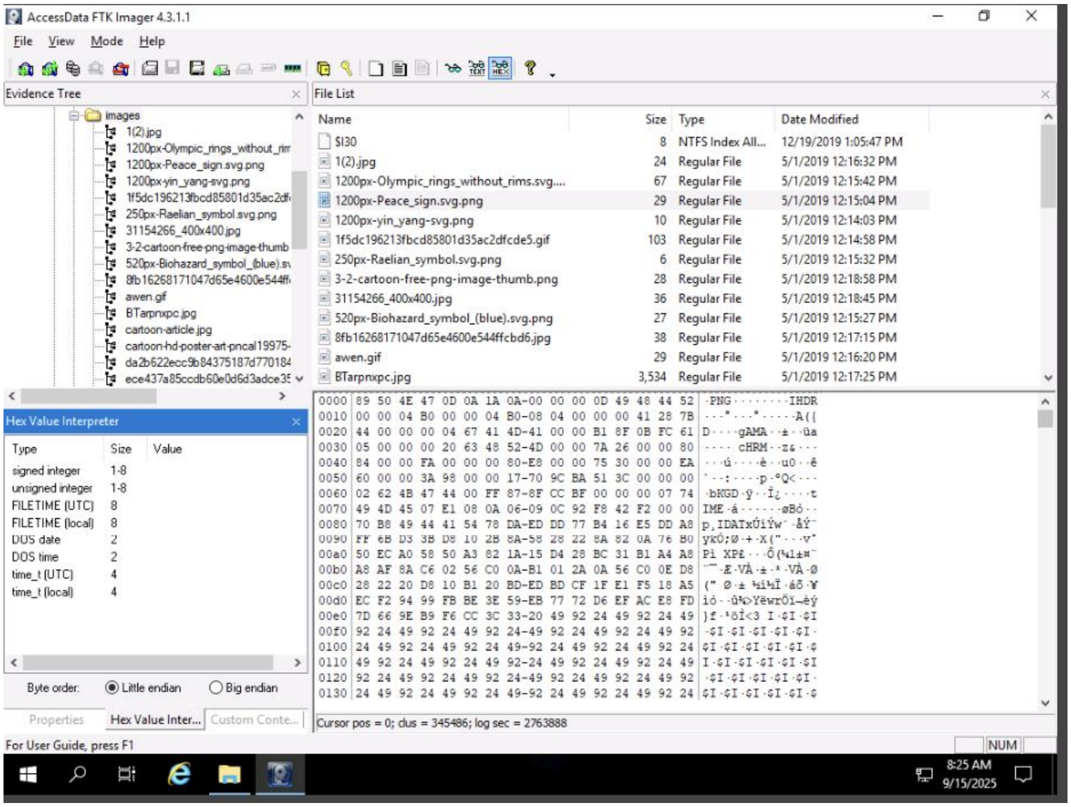
```
0000 89 50 4E 47 0D 0A 1A 0A-00 00 00 0D 49 48 44 52  ·PNG········IHDR
0010 00 00 04 B0 00 00 04 B0-08 04 00 00 00 41 28 7B  ···°···°·····A({
0020 44 00 00 00 04 67 41 4D-41 00 00 B1 8F 0B FC 61  D····gAMA··±··üa
0030 05 00 00 00 20 63 48 52-4D 00 00 7A 26 00 00 80  ···· cHRM··z&···
0040 84 00 00 FA 00 00 00 80-E8 00 00 75 30 00 00 EA  ···ú····è··u0··ê
0050 60 00 00 3A 98 00 00 17-70 9C BA 51 3C 00 00 00  `··:····p·ºQ<···
0060 02 62 4B 47 44 00 FF 87-8F CC BF 00 00 00 07 74  ·bKGD·ÿ··Ì¿····t
0070 49 4D 45 07 E1 08 0A 06-09 0C 92 F8 42 F2 00 00  IME·á······øBò··
0080 70 B8 49 44 41 54 78 DA-ED DD 77 B4 16 E5 DD A8  p¸IDATxÚíÝw´·åÝ¨
0090 FF 6B D3 3B D8 10 2B 8A-58 28 22 8A 82 0A 76 B0  ÿkÓ;Ø·+·X("···v°
00a0 50 EC A0 58 50 A3 82 1A-15 D4 28 BC 31 B1 A4 A8  Pì XP£···Ô(¼1±¤¨
00b0 A8 AF 8A C6 02 56 C0 0A-B1 01 2A 0A 56 C0 0E D8  ¨¯·Æ·VÀ·±·*·VÀ·Ø
00c0 28 22 20 D8 10 B1 20 BD-ED BD CF 1F E1 F5 18 A5  (" Ø·± ½í½Ï·áõ·¥
00d0 EC F2 94 99 FB BE 3E 59-EB 77 72 D6 EF AC E8 FD  ìò··û¾>YëwrÖï¬èý
00e0 7D 66 9E B9 F6 CC 3C 33-20 49 92 24 49 92 24 49  }f·¹öÌ<3 I·$I·$I
00f0 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0100 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
0110 49 92 24 49 92 24 49 92-24 49 92 24 49 92 24 49  I·$I·$I·$I·$I·$I
0120 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0130 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
```

Cursor pos = 0; clus = 345486; log sec = 2763888



AccessData FTK Imager 4.3.1.1
File
View
Mode
Help
Evidence Tree
images
1(2).jpg
1200px-Olympic_rings_without_rim
1200px-Peace_sign.svg.png
1200px-yin_yang-svg.png
1f5dc196213fbcd85801d35ac2df
250px-Raelian_symbol.svg.png
31154266_400x400.jpg
3-2-cartoon-free-png-image-thumb
520px-Biohazard_symbol_(blue).sv
8fb16268171047d65e4600e544ff
awen.gif
BTarpnxpc.jpg
cartoon-article.jpg
cartoon-hd-poster-art-pncal19975-
da2b622ecc9b84375187d770184
ece437a85ccdb60e0d6d3adce35
Custom Content Sources
Evidence:File System|Path|File
Options
New
Edit
Remove
Remove All
Create Image
Properties
Hex Value Inter...
Custom Conte...
File List
For User Guide, press F1
NUM
8:24 AM
9/15/2025

Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM



images
- 1(2).jpg
- 1200px-Olympic_rings_without_rim
- 1200px-Peace_sign.svg.png
- 1200px-yin_yang-svg.png
- 1f5dc196213fbcd85801d35ac2df
- 250px-Raelian_symbol.svg.png
- 31154266_400x400.jpg
- 3-2-cartoon-free-png-image-thumb
- 520px-Biohazard_symbol_(blue).sv
- 8fb16268171047d65e4600e544ff
- awen.gif
- BTarpnxpc.jpg
- cartoon-article.jpg
- cartoon-hd-poster-art-pncal19975-
- da2b622ecc9b84375187d770184
- ece437a85ccdb60e0d6d3adce35

Name	Size	Type	Date Modified
$I30	8	NTFS Index All...	12/19/2019 1:05:47 PM
1(2).jpg	24	Regular File	5/1/2019 12:16:32 PM
1200px-Olympic_rings_without_rims.svg....	67	Regular File	5/1/2019 12:15:42 PM
1200px-Peace_sign.svg.png	29	Regular File	5/1/2019 12:15:04 PM
1200px-yin_yang-svg.png	10	Regular File	5/1/2019 12:14:03 PM
1f5dc196213fbcd85801d35ac2dfcde5.gif	103	Regular File	5/1/2019 12:14:58 PM
250px-Raelian_symbol.svg.png	6	Regular File	5/1/2019 12:15:32 PM
3-2-cartoon-free-png-image-thumb.png	28	Regular File	5/1/2019 12:18:58 PM
31154266_400x400.jpg	36	Regular File	5/1/2019 12:18:45 PM
520px-Biohazard_symbol_(blue).svg.png	27	Regular File	5/1/2019 12:15:27 PM
8fb16268171047d65e4600e544ffcbd6.jpg	38	Regular File	5/1/2019 12:17:15 PM
awen.gif	29	Regular File	5/1/2019 12:16:20 PM
BTarpnxpc.jpg	3,534	Regular File	5/1/2019 12:17:25 PM

```
0000 89 50 4E 47 0D 0A 1A 0A-00 00 00 0D 49 48 44 52  ·PNG········IHDR
0010 00 00 04 B0 00 00 04 B0-08 04 00 00 00 41 28 7B  ···°···°·····A({
0020 44 00 00 00 04 67 41 4D-41 00 00 B1 8F 0B FC 61  D····gAMA··±··üa
0030 05 00 00 00 20 63 48 52-4D 00 00 7A 26 00 00 80  ···· cHRM··z&···
0040 84 00 00 FA 00 00 00 80-E8 00 00 75 30 00 00 EA  ···ú····è··u0··ê
0050 60 00 00 3A 98 00 00 17-70 9C BA 51 3C 00 00 00  `··:····p·ºQ<···
0060 02 62 4B 47 44 00 FF 87-8F CC BF 00 00 00 07 74  ·bKGD·ÿ··Ì¿····t
0070 49 4D 45 07 E1 08 0A 06-09 0C 92 F8 42 F2 00 00  IME·á······øBò··
0080 70 B8 49 44 41 54 78 DA-ED DD 77 B4 16 E5 DD A8  p¸IDATxÚíÝw´·åÝ¨
0090 FF 6B D3 3B D8 10 2B 8A-58 28 22 8A 82 0A 76 B0  ÿkÓ;Ø·+·X("···v°
00a0 50 EC A0 58 50 A3 82 1A-15 D4 28 BC 31 B1 A4 A8  Pì XP£···Ô(¼1±¤¨
00b0 A8 AF 8A C6 02 56 C0 0A-B1 01 2A 0A 56 C0 0E D8  ¨¯·Æ·VÀ·±·*·VÀ·Ø
00c0 28 22 20 D8 10 B1 20 BD-ED BD CF 1F E1 F5 18 A5  (" Ø·± ½í½Ï·áõ·¥
00d0 EC F2 94 99 FB BE 3E 59-EB 77 72 D6 EF AC E8 FD  ìò··û¾>YëwrÖï¬èý
00e0 7D 66 9E B9 F6 CC 3C 33-20 49 92 24 49 92 24 49  }f·¹öÌ<3 I·$I·$I
00f0 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0100 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
0110 49 92 24 49 92 24 49 92-24 49 92 24 49 92 24 49  I·$I·$I·$I·$I·$I
0120 92 24 49 92 24 49 92 24-49 92 24 49 92 24 49 92  ·$I·$I·$I·$I·$I·
0130 24 49 92 24 49 92 24 49-92 24 49 92 24 49 92 24  $I·$I·$I·$I·$I·$
```

Cursor pos = 0; clus = 345486; log sec = 2763888

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte order: ● Little endian ○ Big endian

For User Guide, press F1

Module 04: Data Acquisition and Duplication

Lab 1: Creating a dd Image of a System Drive

- Students performed a physical acquisition of a Windows system drive (PHYSICALDRIVE0) using the dd command.
- The lab demonstrated creating a bit-by-bit copy of the disk, including deleted files, slack space, and file system metadata.
- A secondary disk was used to simulate an external storage device for storing the acquired image.

Lab 2: Converting Acquired Image File to a Bootable Virtual Machine

- The acquired disk image was prepared to boot as a virtual machine.
- This allows investigators to examine the system in a live environment and extract additional artifacts.

Lab 3: Acquiring RAM from Windows Workstations

- Students learned to capture volatile memory (RAM) using the Belkasoft RAM Capturer tool.
- RAM acquisition preserves data that would be lost when the machine is powered off, such as running processes and temporary files.

Lab 4: Viewing Contents of Forensic Image File

- Students used AccessData FTK Imager to view and analyze the contents of forensic images.
- This enables investigators to examine evidence without altering the original data, and to assess whether further analysis is required.

Overall Summary:
Module 4 provided hands-on experience with data acquisition, image duplication, RAM capture, and forensic image analysis. These labs reinforce critical skills for preserving and analyzing electronic evidence in a forensically sound manner.