

Cybersecurity Professional Program

Data Acquisition

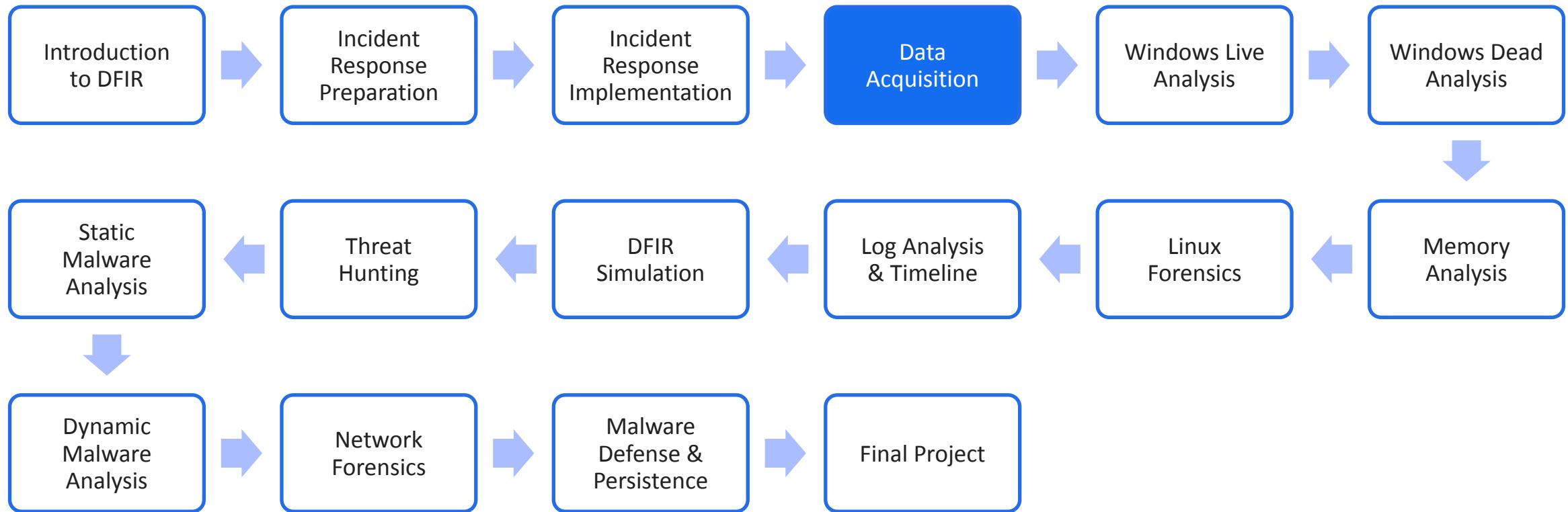
Digital Forensics &
Incident Response





Digital Forensics & Incident Response

Course Path



Objectives



The objective of this lesson is to explain how to properly acquire and preserve data for forensic investigations from both storage devices and memory.

- Data Acquisition
 - Drive Capture
 - Advanced Capture Tools
 - Evidence Inspection
- Virtual Drives
- Memory Dumping
- Virtual Memory Dumping
- Memory in Other Locations





Data Acquisition

Data Acquisition

State Capture



- To conduct a proper investigation, you must preserve the affected state.
- A capture enables understanding a threat and investigating it at the same time.
- A state capture assists in recording and preserving evidence.

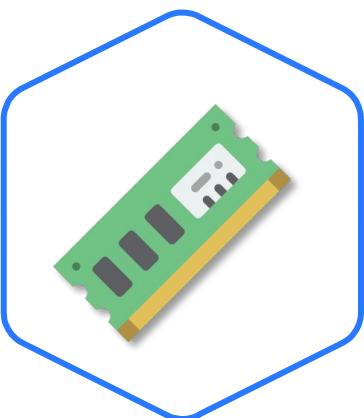


Capturable Evidence



Hard Disk Drive (HDD) or Solid-State Drive (SSD)

The hard drive may contain file and log evidence.



Memory

The memory is full of evidence of running processes.

Capturing network traffic does not constitute preservation of evidence.

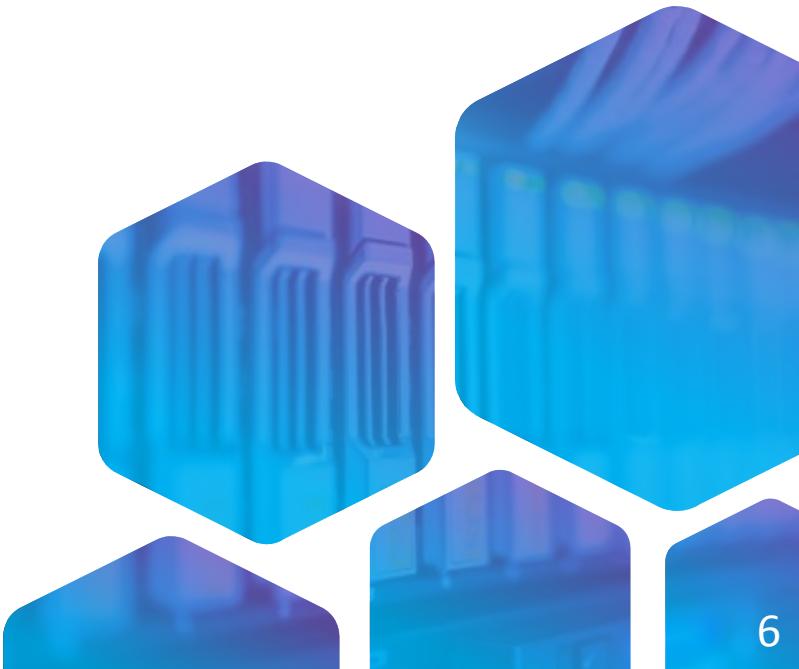




Image Capture Pros & Cons

Advantages

Provides an exact copy of the evidence

Used as a backup for the evidence

Artifacts can be extracted from .the capture

Allows creation of a static capture of the memory

All file details can be viewed .in tables

Disadvantages

Sometimes, only a partial capture is possible.

Takes time to create a state capture



If the evidence was encrypted at the time of the capture, the resulting image will also be encrypted.

Memory cannot be inspected for changes.

Not the typical way to inspect data on a computer



Data Acquisition

Acquisition Recommendations

- 1 Memory captures are better if the user is logged on.
- 2 Use sterilized media for acquisition.
- 3 Complete memory acquisition before drive acquisition.
- 4 System interaction should be minimal.
- 5 Choose the right capture format.
- 6 Some capture tools are more efficient than others.
- 7 Always capture to an external source.
- 8 Document the capture properly.



Data Acquisition

Drive Capture

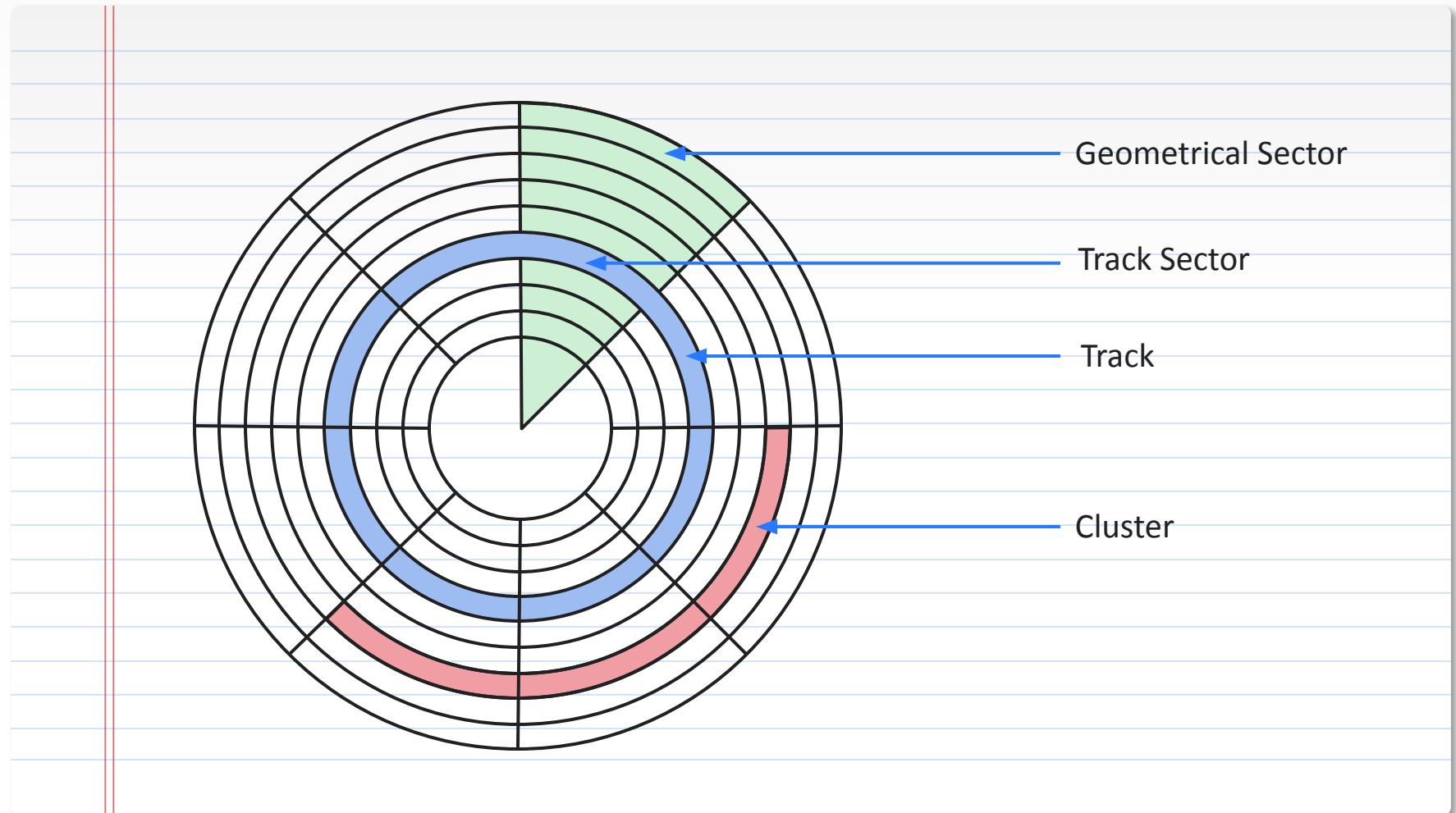
Drive Sectors & Partitions



Each drive is divided into sectors.

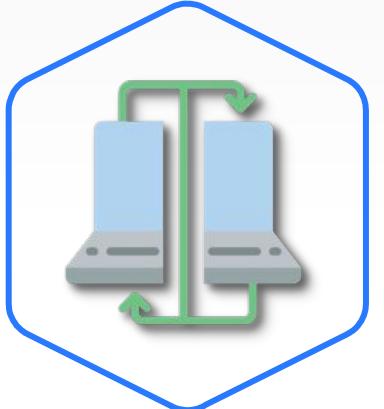
Although some sectors may not be allocated, they can still include data.

A partition is a logical, not physical, entity containing multiple sectors.



Drive Capture

Partial & Full Clone



Full Clone

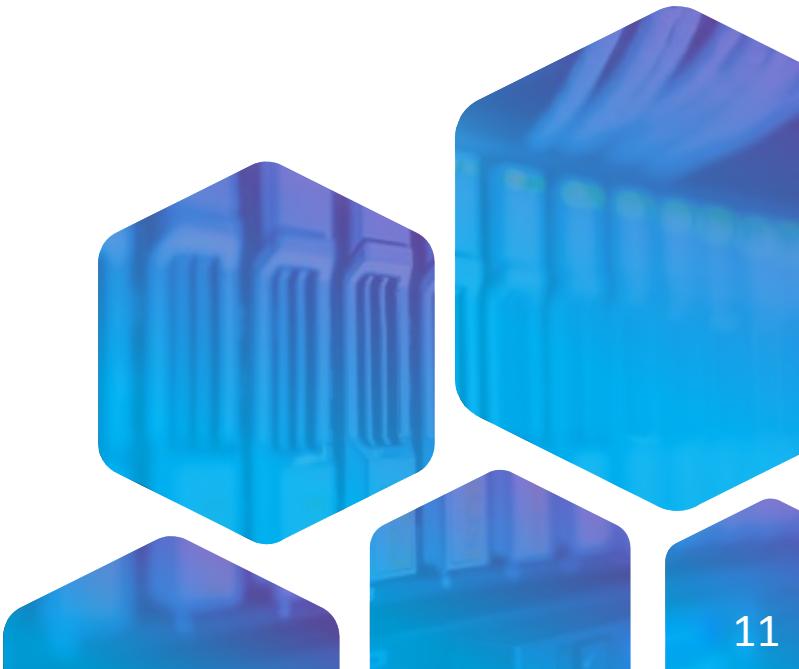
A full clone is the closest option to having the actual drive, but only some of the data on a drive is useful for forensics.



Logical Image

A logical image narrows the search field. Some evidence may be spread across multiple partitions.

Capturing the state of an HDD or SSD is known as cloning.



Drive Capture

Capture Tools



dd



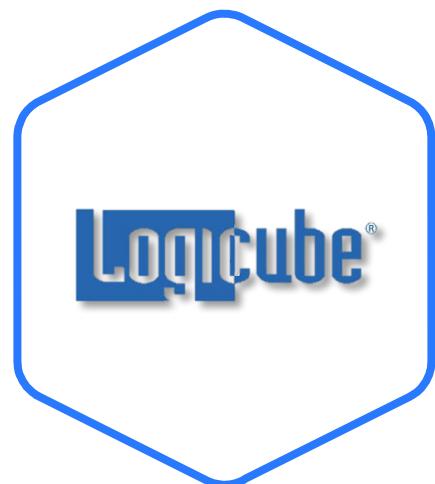
Clonezilla



FTK Imager



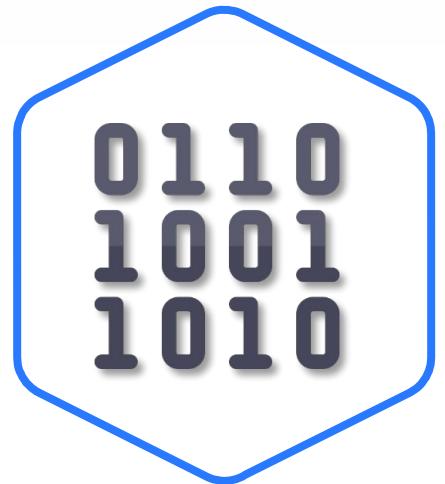
Acronis



Logicube

Drive Capture

Capture Formats



RAW



ISO



EWF



dd

The capture format is based on the media from which it is captured.

The dd Tool



- A Linux CLI tool used to fully clone drives and partitions
- Typically used via a live media drive





Drive Capture

The *dd* Command

```
root@kali:~# dd if=/dev/sda of=/dev/sdb  
root@kali:~# dd if=/dev/sda of=/dev/sdb bs=4096 conv=sync,noerror
```

***dd*:** data duplicator

***if*:** the source disk

***of*:** the target disk where the piped data is written

| ***bs*** and ***conv*** determine how data is copied.



Drive Capture

Capture from Live Media

Cloning is typically done through external media.

This prevents accidental changes to the drive.

It is also important to save the clone to an external drive.

The screenshot shows the CAINE Linux desktop environment. On the left is a dock with icons for Home, Caja-Root, Network, Trash, Disk Image Mounter, Unblock, Autopsy, Guymager, Install CAINE 18.04, Computer, and Network Servers. The main window is a terminal window titled 'caine@caine: ~'. It displays the following output from the 'fdisk -l' command:

```
caine@caine:~$ sudo fdisk -l
Disk /dev/loop0: 3,7 GiB, 3928313856 bytes, 7672488 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
WORKHOLE

Disk /dev/sda: 60 GiB, 64424509440 bytes, 125829120 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe7b92fc0

Device      Boot Start End Sectors Size Id Type
/dev/sdal    *   2048 125827071 125825024  60G  7 HPFS/NTFS/exFAT
caine@caine:~$
```

The terminal window has a dark background with orange highlights for the disk information. The bottom of the screen shows the CAINE desktop interface with various application icons.

Lab DFIR-04-L1

Drive Capture
30–40 Min.



Mission

Create a drive capture and save it in a separate mounted drive.

Steps

- Attach two additional drives to a VM.
- Reboot the VM via live media.
- Create an image capture of the drive.
- Compare the source and the capture.

Environment & Tools

- VirtualBox
- Windows 10

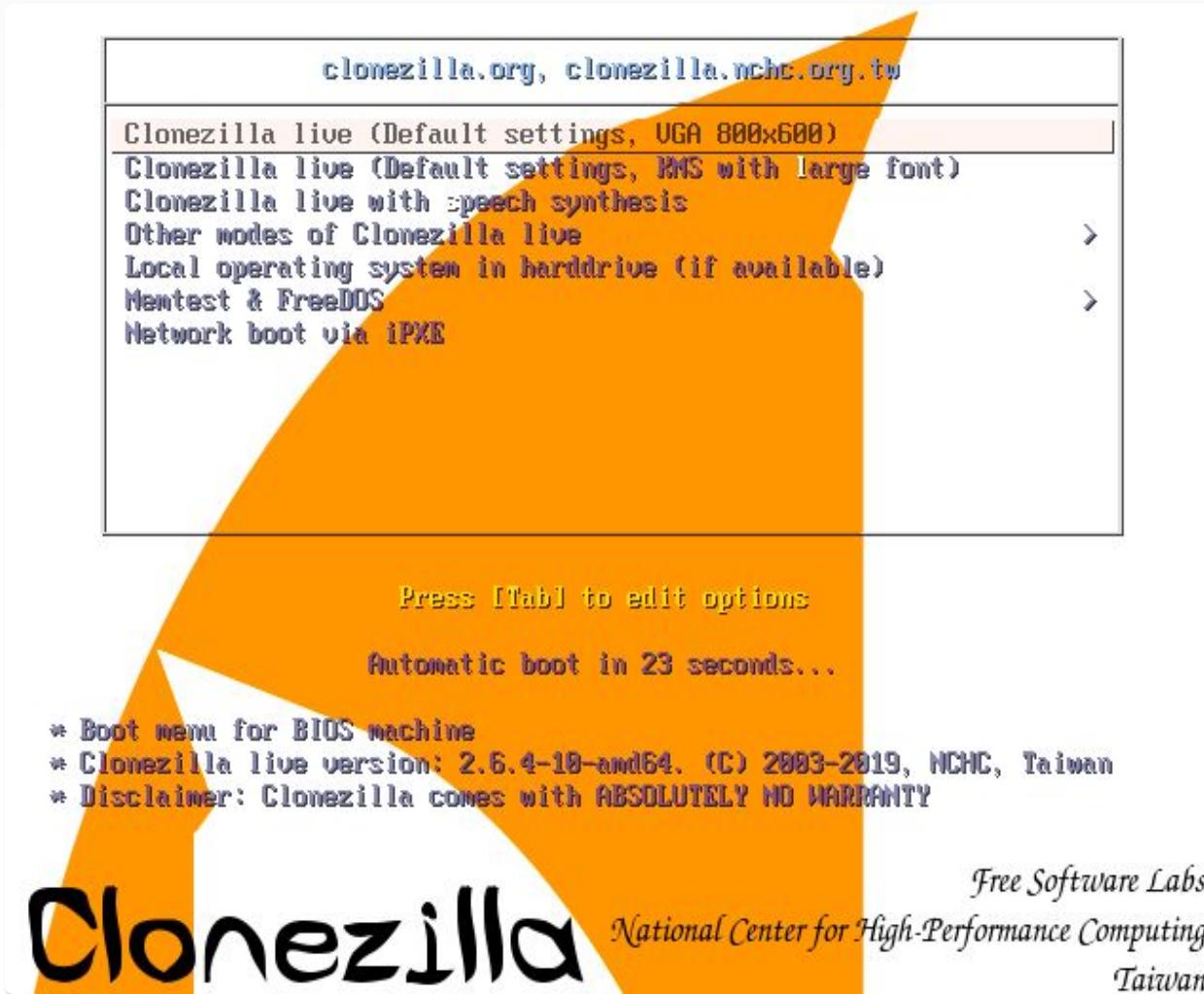
Related Files

- Lab document
- ***CAINE.iso***



Data Acquisition

Advanced Capture Tools



Clonezilla is a live Linux distribution dedicated to cloning drives.

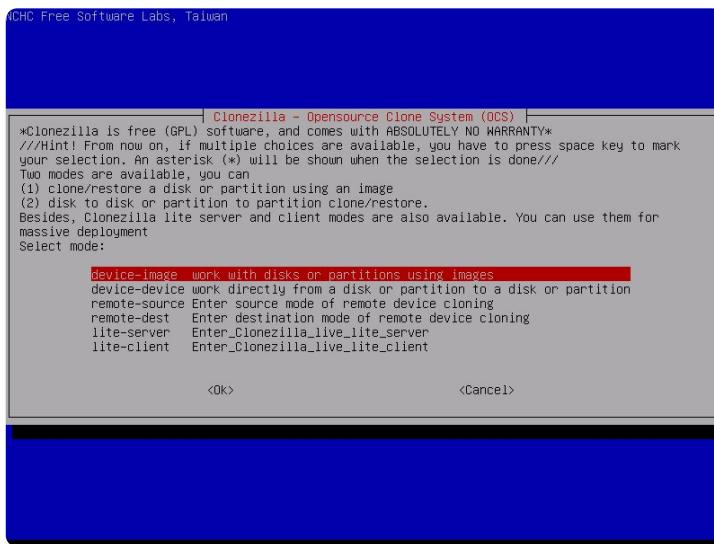
Clonezilla uses its own format to save images.

It can clone more than 40 computers at the same time.

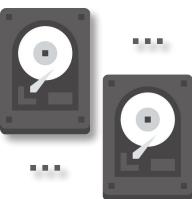


Advanced Capture Tools

Clonezilla Capture Modes



Device-image: This option creates an image capture from an actual drive.



Device-device: This option clones an entire drive or partition to another drive or partition.



Remote-source: One of Clonezilla's most important features is that it can clone over the network.



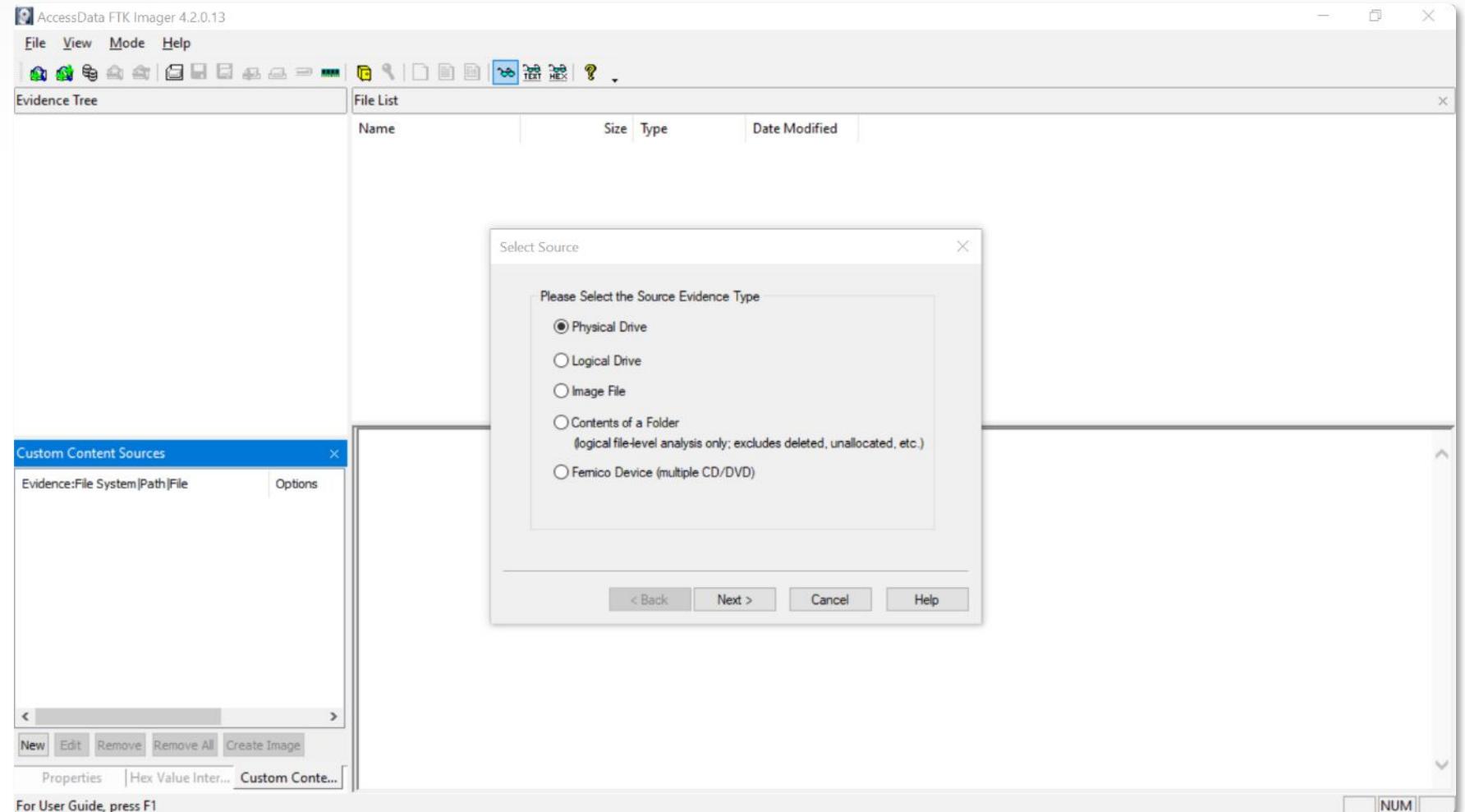
Advanced Capture Tools

FTK Imager

FTK Imager is part of the Forensic Toolkit suite of tools.

The tool can be installed on the OS or executed from live media.

Although FTK is commercial, the imaging software is free.





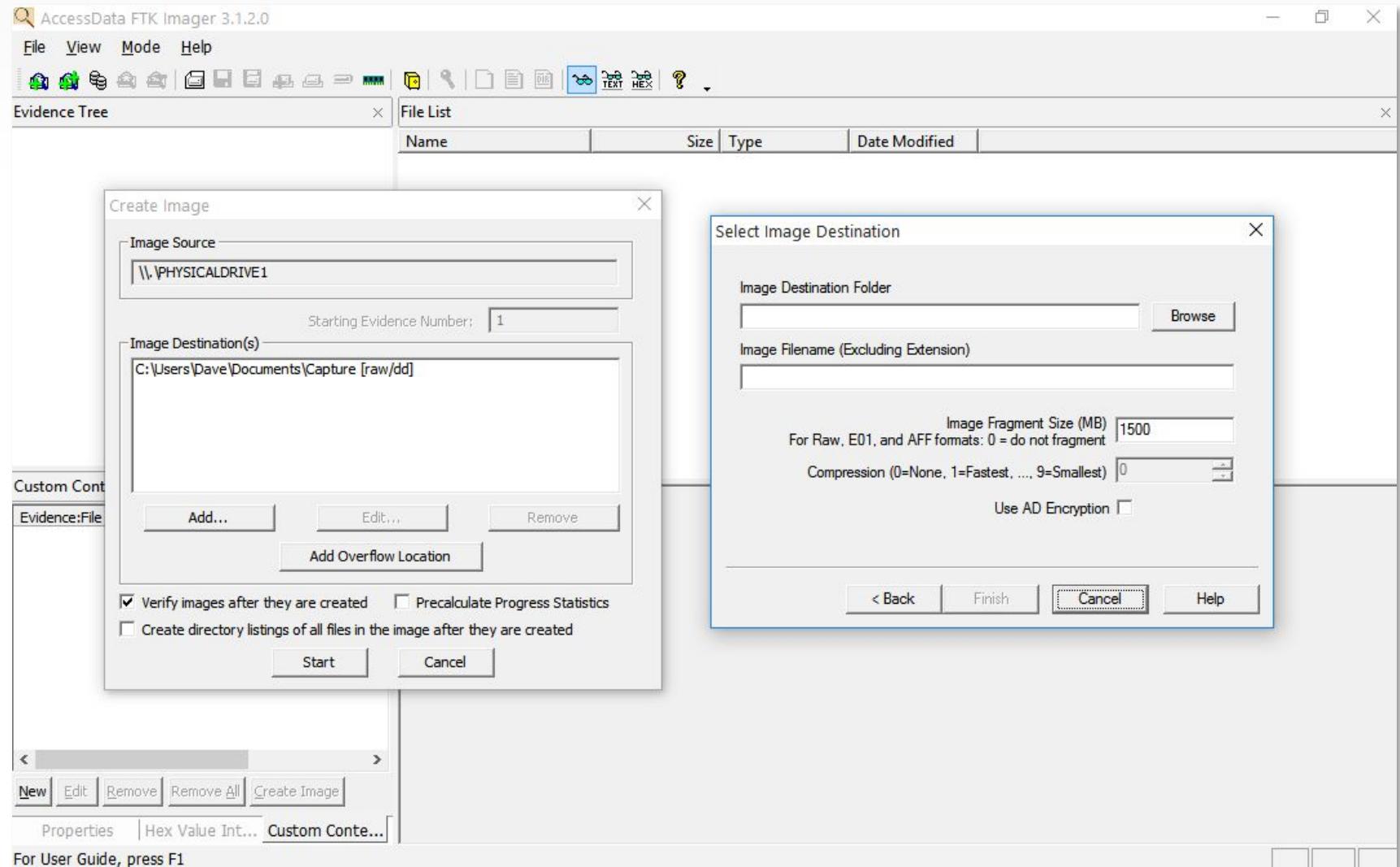
Advanced Capture Tools

Cloning a Drive with FTK

In FTK Imager, the capture is done through an interactive wizard.

The wizard prompts the user to choose the drive or partition to clone and the format.

Typically, the raw (dd) format is used, and the image is fragmented.



Forensic Image Formats



E01

Provides compression per file checksum and password protection



AFF

Stores the imaged disk as compressed segments for better saving and metadata of the image

Unlike non-forensic images, forensic images provide additional features that do not alter content on the drive.

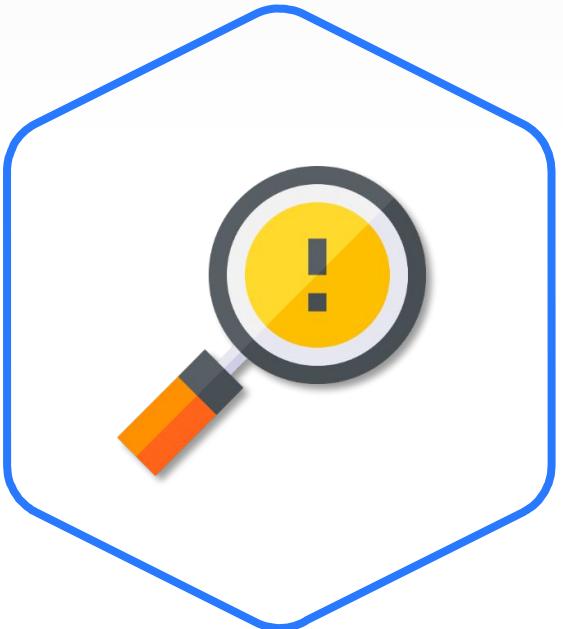




Data Acquisition

Evidence Inspection

Image Investigation



- The traditional way to investigate an image is to open it in a dedicated software tool.
- An alternative method is to create a VM based on the image.

If a drive is encrypted, the preferred method of investigation is to create a VM based on the image.





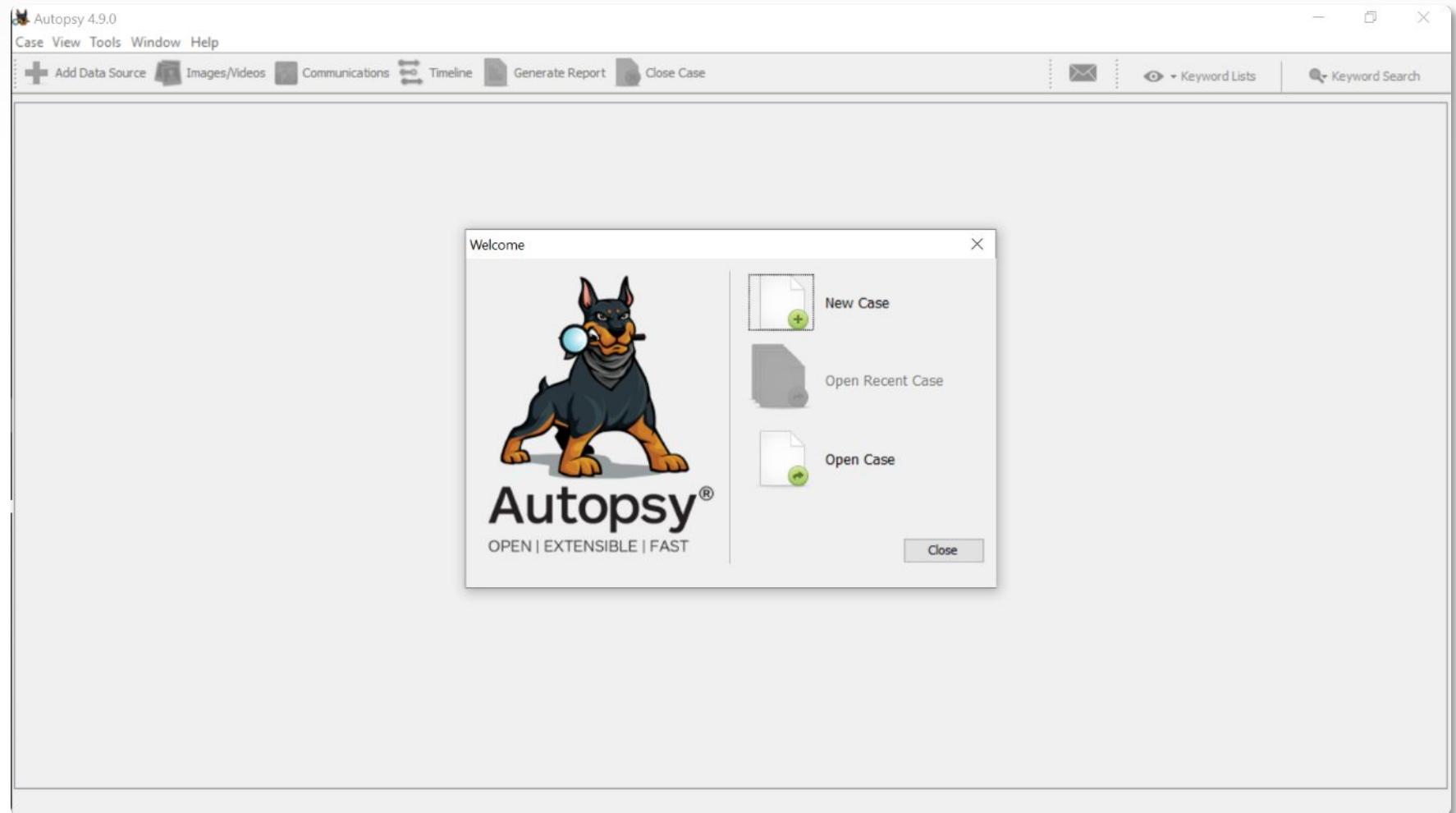
Evidence Inspection

Autopsy

Autopsy uses forensic tools from The Sleuth Kit.

Each case to be examined in Autopsy is created separately.

A case can include multiple captures.





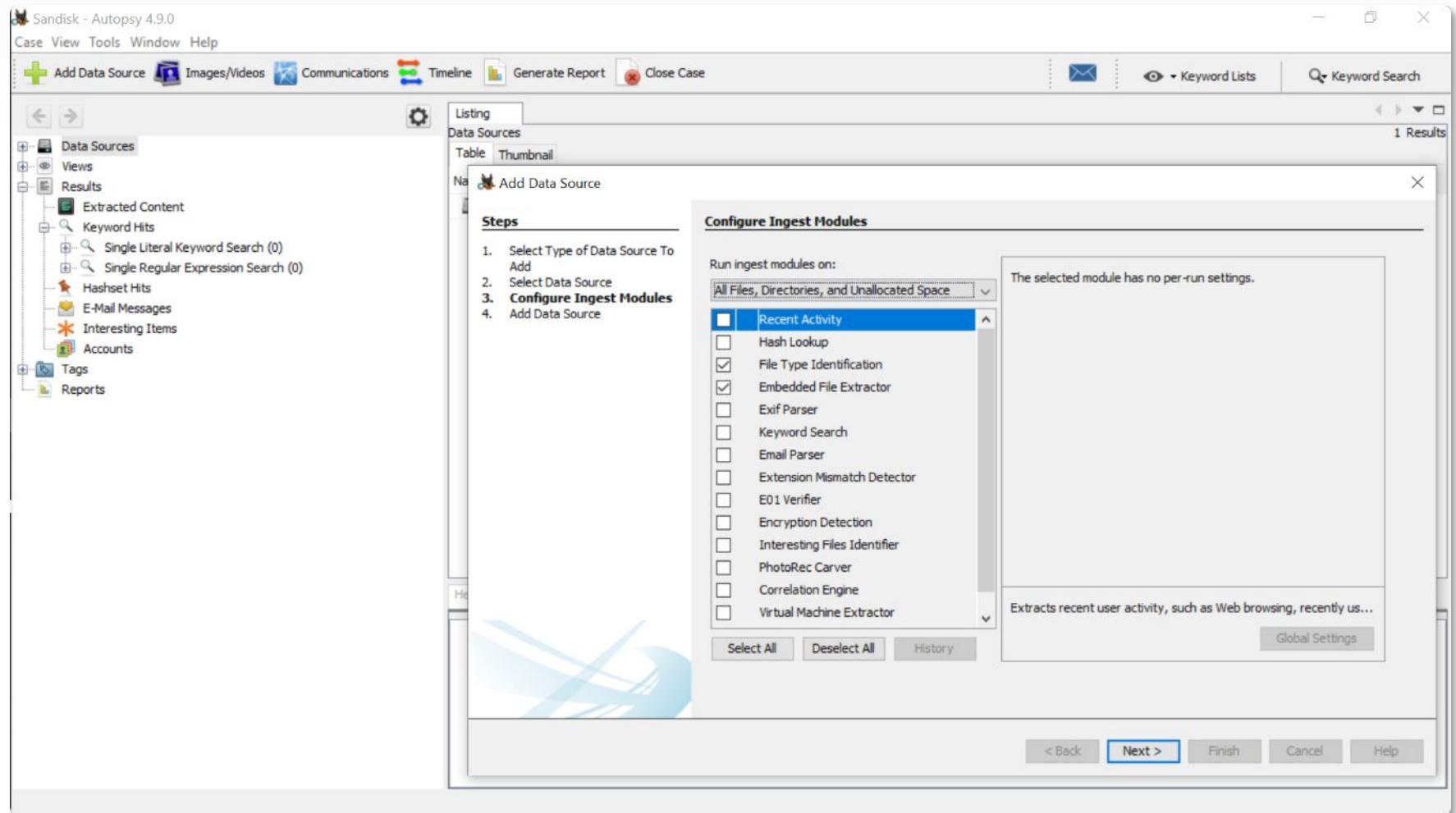
Evidence Inspection

Autopsy Features

Autopsy includes many tools to enhance the analysis of captured images.

These tools include hash lookup, file carving, metadata extraction, and others.

The tools can extract important data and index data for faster queries.





OSFMount allows you to mount local dd image files in Windows.

It reads the disk partition bit for bit. By default, image files are mounted as read-only.

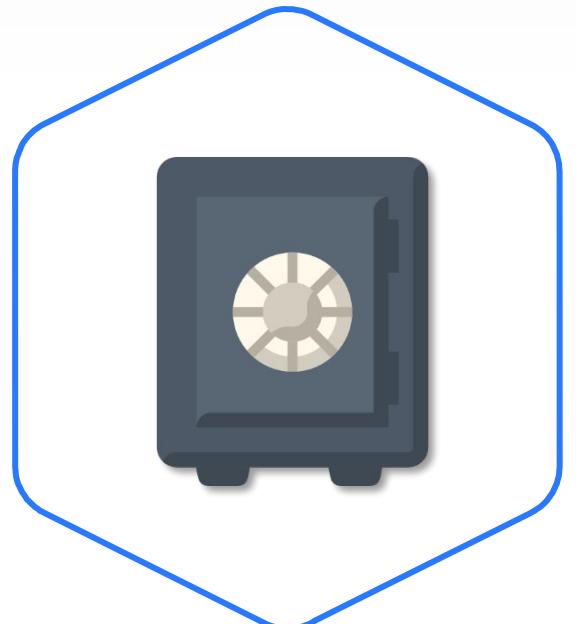
OSFMount supports disks that are mounted in RAM.

The screenshot shows the PassMark OSFMount application interface. The title bar reads "PassMark OSFMount". The menu bar includes "File", "Drive actions", and "Help". The main window is titled "Mounted virtual disks". A table lists the following information:

Device	Drive	Emulation	Disk Image Path	Type	Size	Properties	File system
\Device\OSFMDisk0	E:	Logical	C:\Users\sean\VirtualBox VMs\metasploitable3...	Disk	7.882 KB	Read-only	N/A

At the bottom of the window are buttons for "Mount new...", "Dismount", "Dismount all & Exit", and "Exit".

Preservation



- A critical part of any cyber investigation is the isolation and preservation of digital evidence in its original state.
- Preservation of evidence helps both the investigation and the legal process that may follow.





- Hashing can verify file integrity.
- Hashing both the capture source and the captured image can prove a file's authenticity.

In a criminal investigation, hashes can be used in a court of law to provide evidence of integrity.



Lab DFIR-04-L2

FTK Drive Capture
20–30 Min.



Mission

Create a disk image with FTK Imager and mount it using OSFMount.

Steps

- Install FTK Imager.
- Create a disk image.
- Install OSFMount.
- Mount the created image.

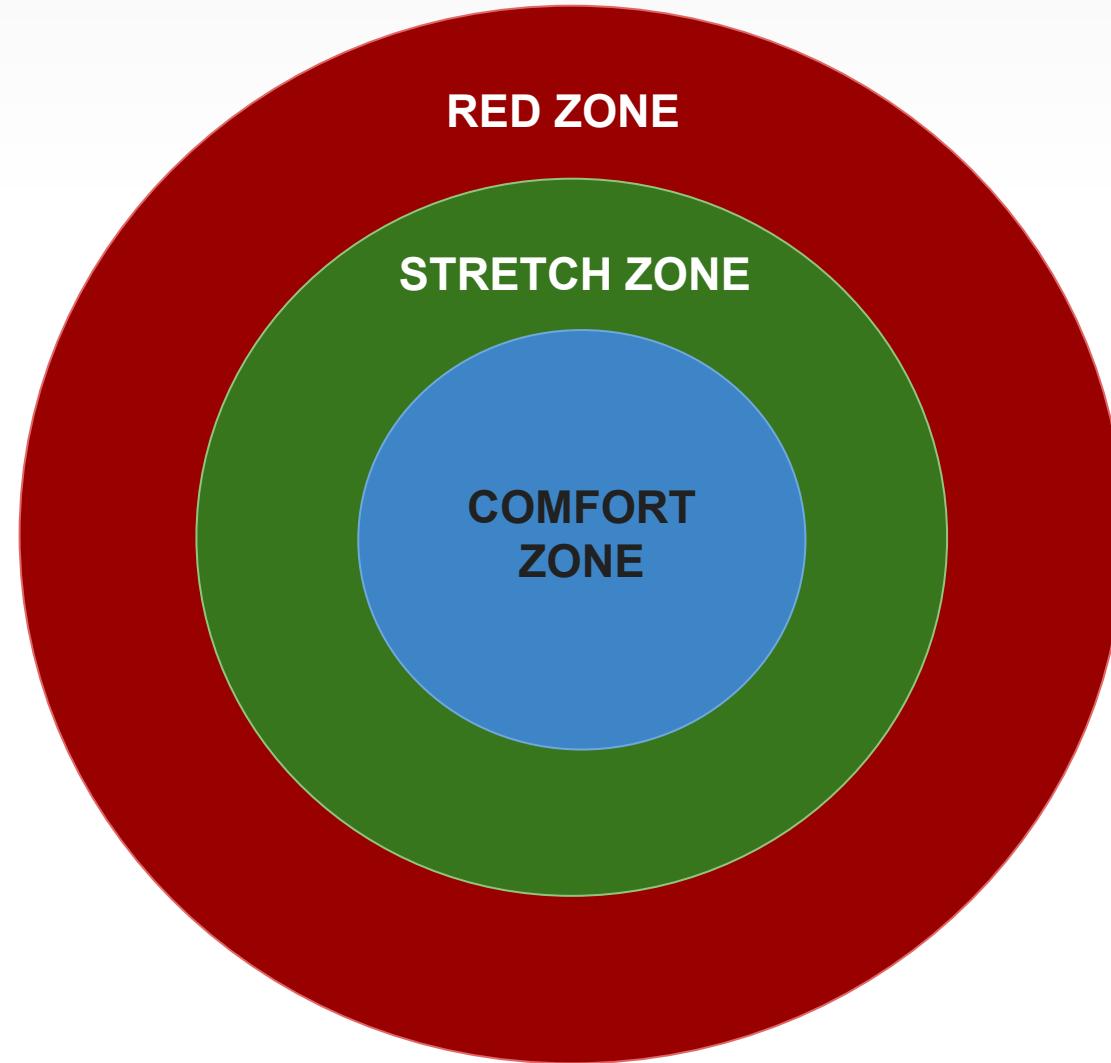
Environment & Tools

- VirtualBox
- Windows 10

Related Files

- Lab document
- *Osfmount.exe*
- *AccessData FTK Imager.exe*
- *Window.png*

Pulse Check





Data Acquisition

Virtual Drives



Virtual Drives

Physical vs. Virtual Drives

Physical

Contains RAW data

No format, only bytes

.The drive has a constant size

A single unit of data

A device with mechanical components

Virtual

Contains RAW + VM data

Different formats for different vendors

Space can be dynamically allocated.

Can be split across files

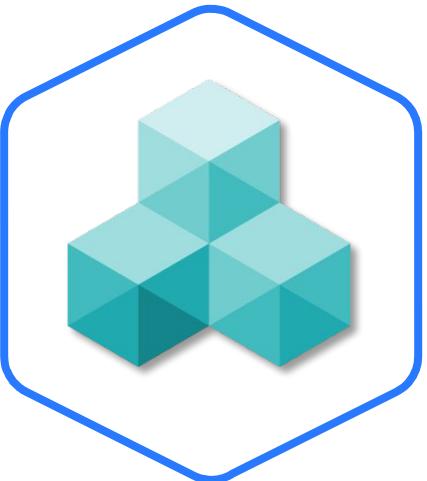
A file within the file system



Virtual Drives



Virtual Drive Formats



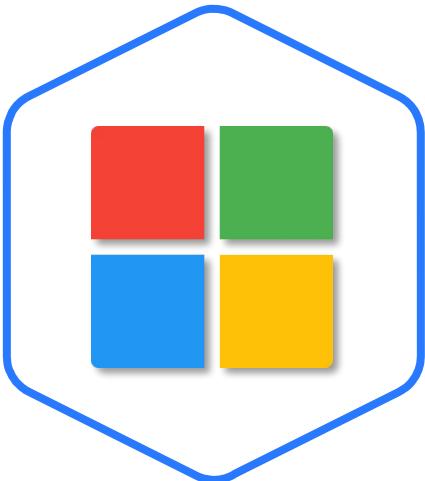
VHD



VMDK



VDI



VHDX

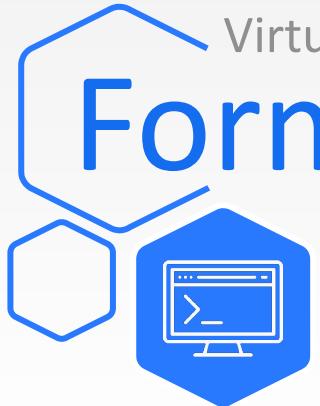
Image Splitting



- Virtualization software may split a drive into multiple files.
- To perform an investigation, you will need all the files.

Splitting is done to increase read and write speeds.





Virtual Drives

Format Conversion

You can convert virtual drives from one format to another.

qemu-img is used for this purpose.

qemu-img supports many formats and versions.

```
C:\Users\JohnD\Downloads\qemu-img-win>qemu-img.exe -h
qemu-img version 2.3.0, Copyright (c) 2004-2008 Fabrice Bellard
usage: qemu-img command [command options]
QEMU disk image utility
```

Command syntax:

```
check [-q] [-f fmt] [--output=ofmt] [-r [leaks | all]] [-T src_cache] filename
create [-q] [-f fmt] [-o options] filename [size]
commit [-q] [-f fmt] [-t cache] [-b base] [-d] [-p] filename
compare [-f fmt] [-F fmt] [-T src_cache] [-p] [-q] [-s] filename1 filename2
convert [-c] [-p] [-q] [-n] [-f fmt] [-t cache] [-T src_cache] [-O output_fmt] [-o
options]
[-s snapshot_id_or_name] [-l snapshot_param] [-S sparse_size] filename [filename2
[...]]
output_filename
info [-f fmt] [--output=ofmt] [--backing-chain] filename
map [-f fmt] [--output=ofmt] filename
snapshot [-q] [-l | -a snapshot | -c snapshot | -d snapshot] filename
rebase [-q] [-f fmt] [-t cache] [-T src_cache] [-p] [-u] -b backing_file [-F
backing_fmt]
filename
resize [-q] filename [+ | -]size
amend [-p] [-q] [-f fmt] [-t cache] -o options filename
```

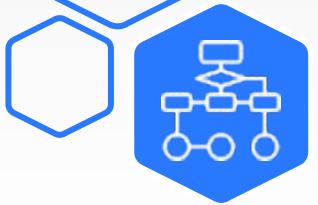


Data Acquisition

Memory Dumping

Memory Dumping

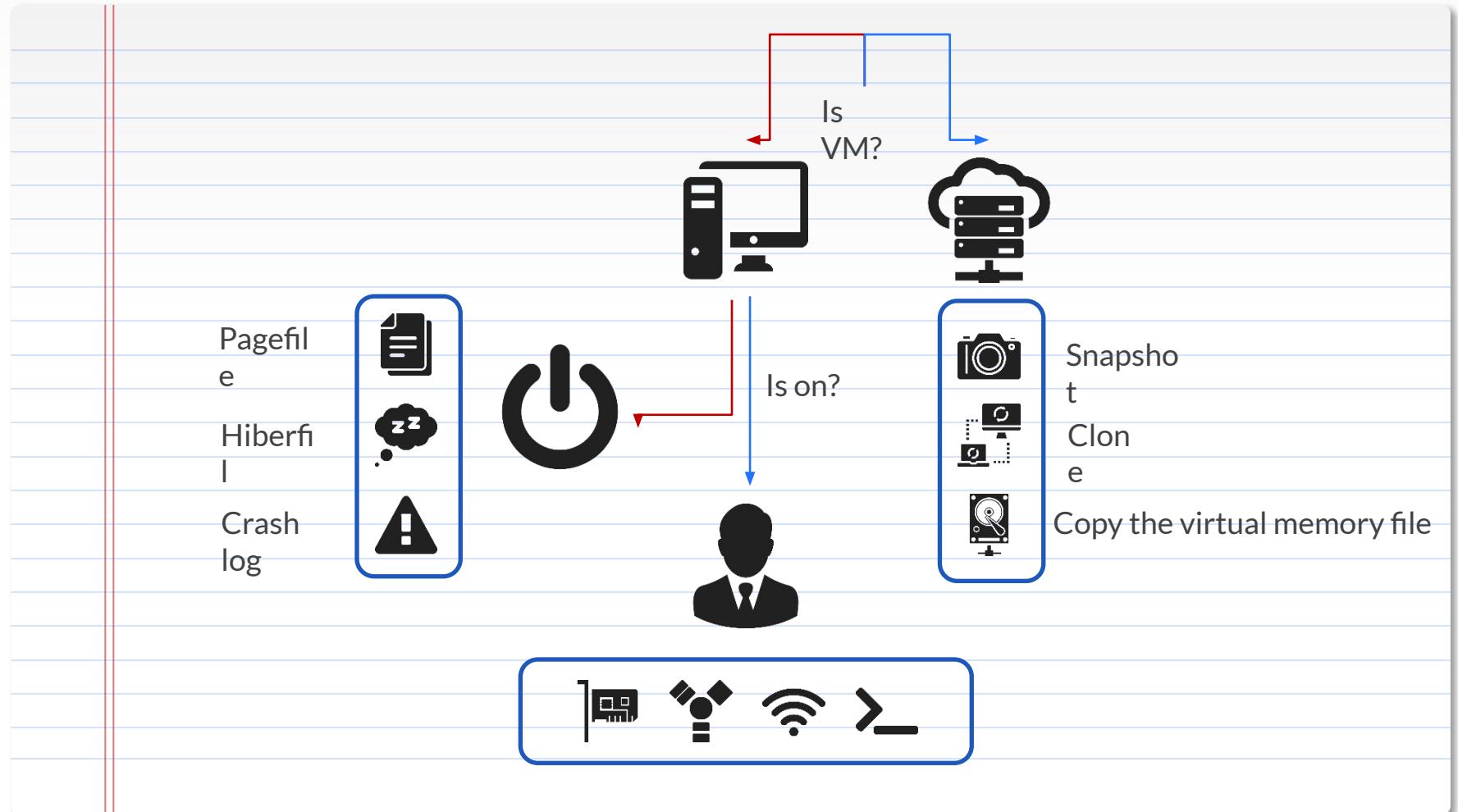
Decision Tree



Memory extraction is dependent on the system type.

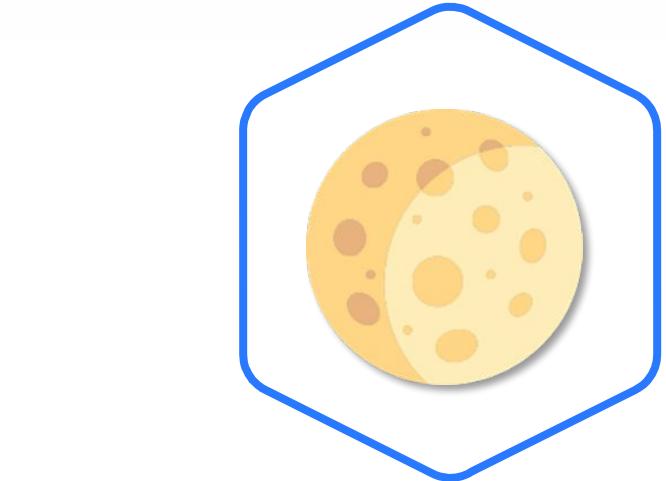
Memory dumping is different for bare-metal and virtual systems.

For bare-metal, the acquisition depends on whether the system is on or off.

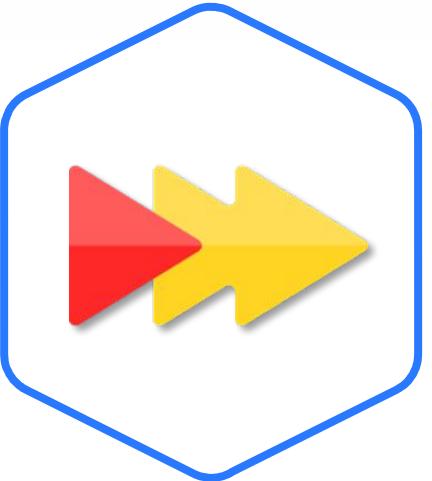


Memory Dumping

Memory Dumping Tools



MWMT



FastDump



FTK Imager



WinPmem

The primary difference among memory-capturing tools is the formats they support.



Memory Dumping

Commercial Tools

Not many memory-acquisition tools exist in the market.

You can use PCI devices, but there are not many for memory capturing, and they are expensive.

The screenshot shows a web browser displaying the WindowsSCOPE website at www.windowsscope.com/product/captureguard-physical-memory-acquisition-hardware-pcie-add-on/. The page features a black header with the WindowsSCOPE logo and navigation links for Products, Try It, See It, Store, Markets, Blog, Contact, and Account. A red price of \$9,599 is prominently displayed above the product title. The main content area describes the CaptureGUARD Physical Memory Acquisition Hardware - PCIe Add-on as a PCI Express add-on device capable of imaging physical memory. Below the description, a note for international orders and an 'ADD TO CART' button are visible.

\$9,599

**CaptureGUARD Physical
Memory Acquisition Hardware –
PCIe Add-on**

This is a PCI Express add-on device capable of imaging the physical memory of the computer it's connected to. Creates dump files in the standard WinDD format that can be used with WindowsSCOPE Cyber Forensics Ultimate or with other WinDD compatible dump analysis tools.

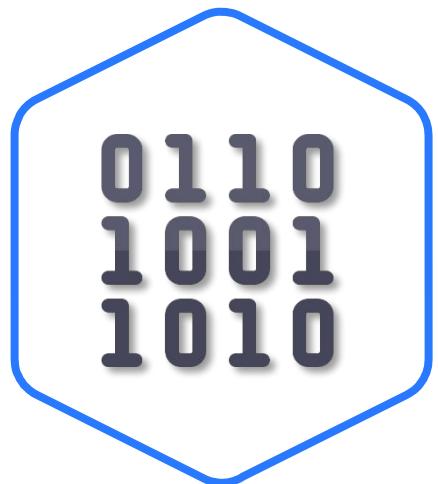
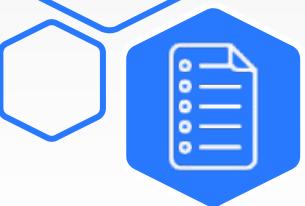
For international orders (outside of United States), please contact info@windowsscope.com

1 **ADD TO CART**

From: Windowsscope.com (accessed 07/22/21)

Memory Dumping

Memory Dump Formats



RAW



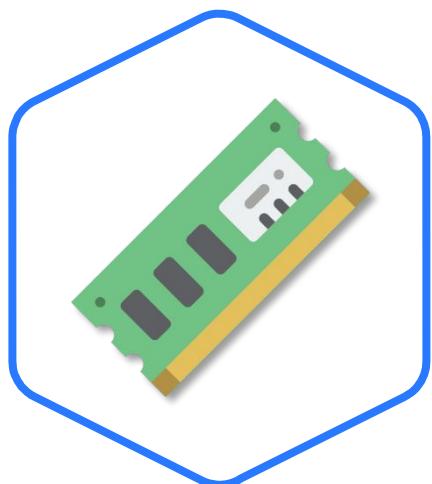
Crash Dump



Hibernation

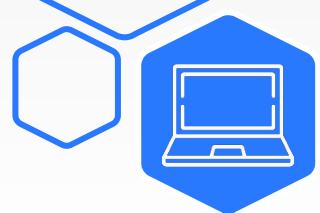


EWF



AFF4

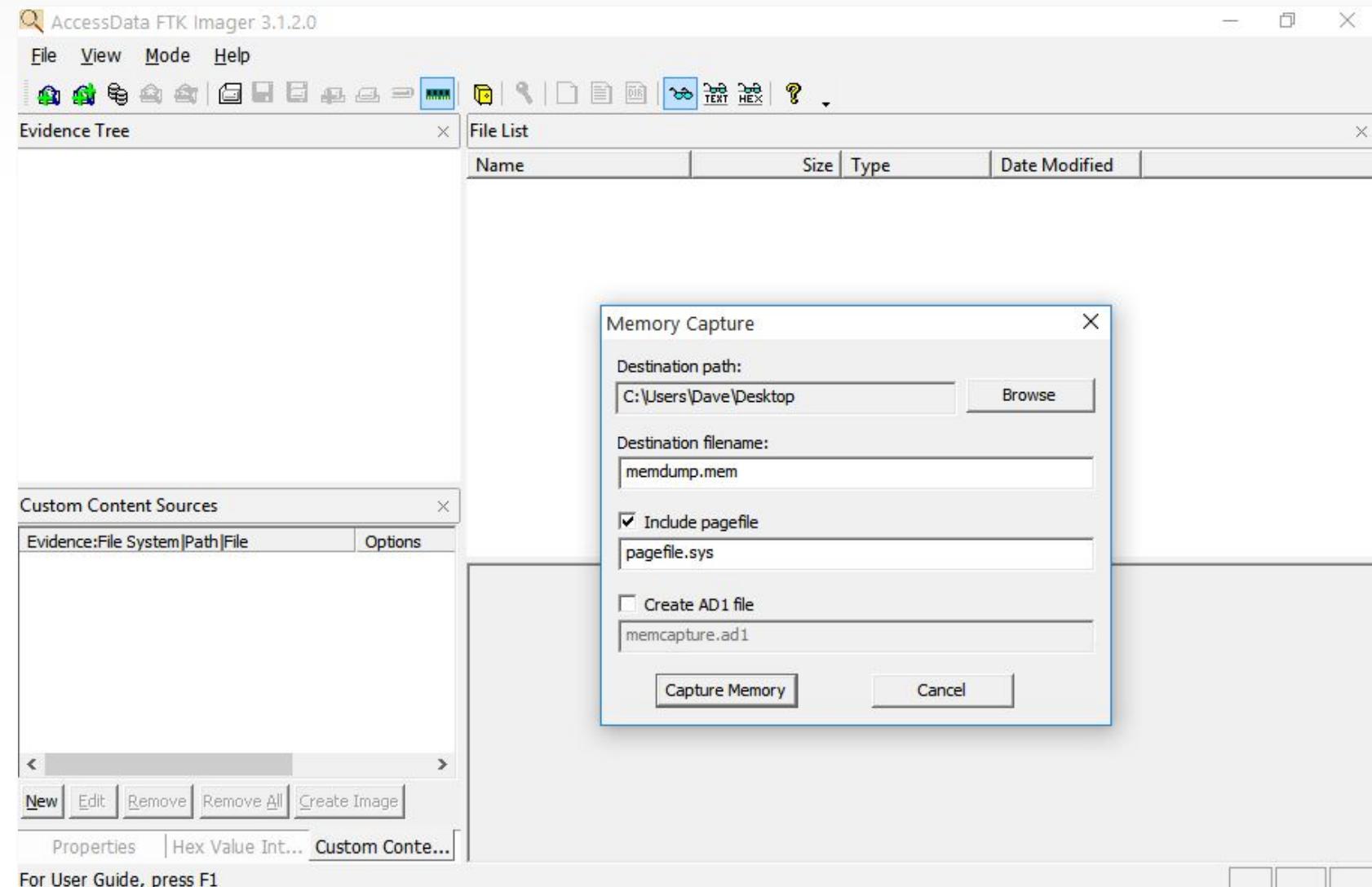
Memory Dumping



Use tools like FTK Imager and Dumpli to capture memory in a non-virtual system.

The main benefit of FTK Imager is that it can capture the page file.

Capture memory using FTK Imager via the *Memory Capture* icon in the menu at the top.





- Volatility is a popular framework used for memory analysis and investigation.
- It includes various Python-based tools for memory artifact extraction.

Google's Rekall rivals Volatility but currently is not as popular.



Lab DFIR-04-L3

Memory Capture
25–35 Min.



Mission

Use the FTK Imager tool to capture the memory of a virtual machine and acquire basic information about it with Volatility.

Steps

- Set a small memory size for the VM.
- Capture the VM's memory.
- Transfer it to SIFT.
- Examine the capture.

Environment & Tools

- VirtualBox
- Windows 10 VM
- SIFT
- FTK Imager

Related Files

- Lab document
- **SIFT-Workstation.OVA**
- **Pscp.exe**



Data Acquisition

Virtual Memory Dumping



Virtual Memory Dumping

Virtual vs. Physical Memory

Physical

- Contains RAW data
- No format, only bytes
- The memory has a constant size



Virtual

- Contains RAW and VM data
- Different formats for different vendors
- The memory can be dynamically allocated.
- Can be captured by a hypervisor
- An allocated area within the memory



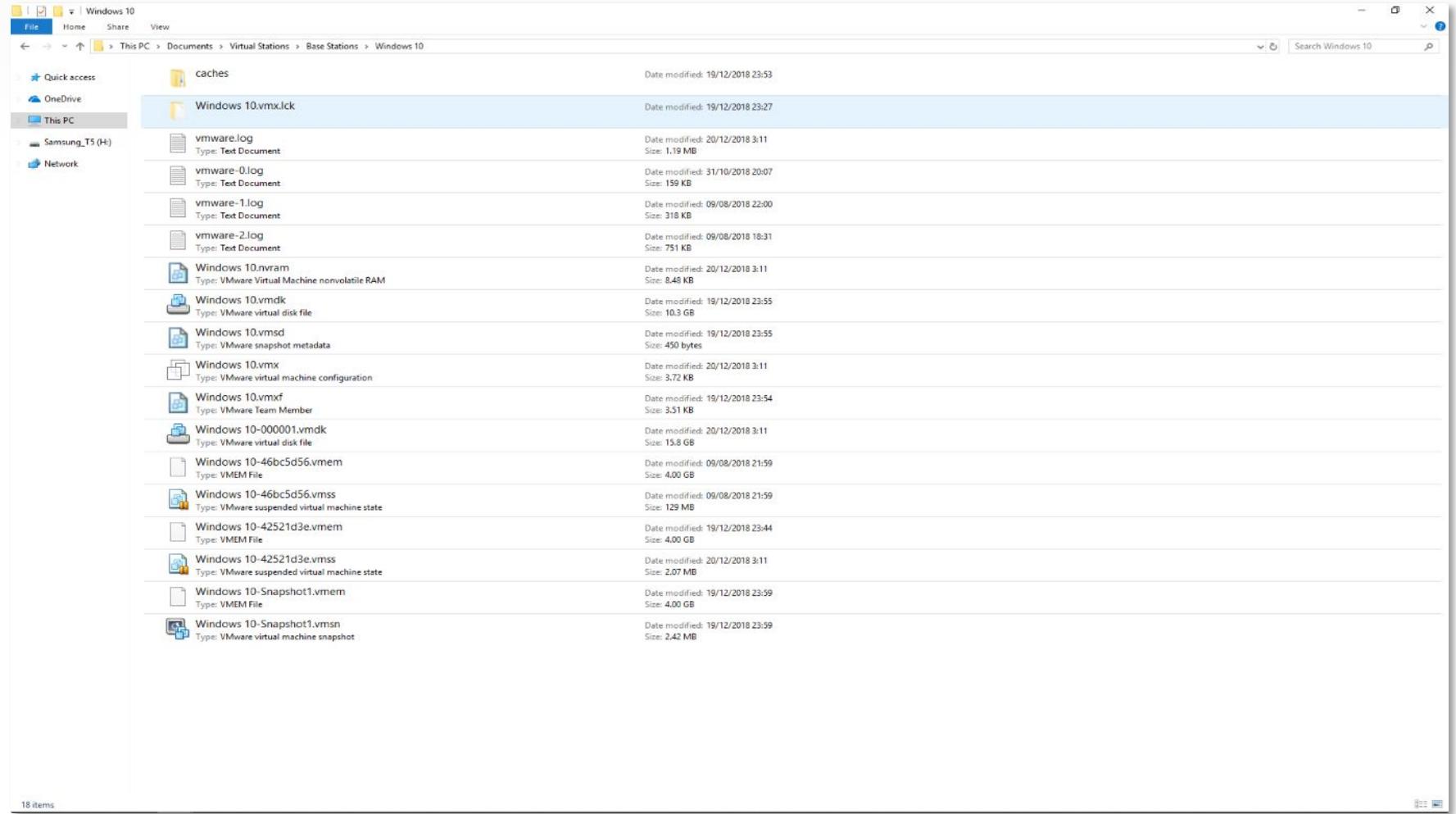
Virtual Memory Dumping

VMware Memory

VMware automatically creates a memory dump whenever a snapshot is taken.

Memory files typically will be in **.vmem**, **.vmsn**, and **.vmss** formats.

The **.vmem** files contain both the memory schema and metadata.





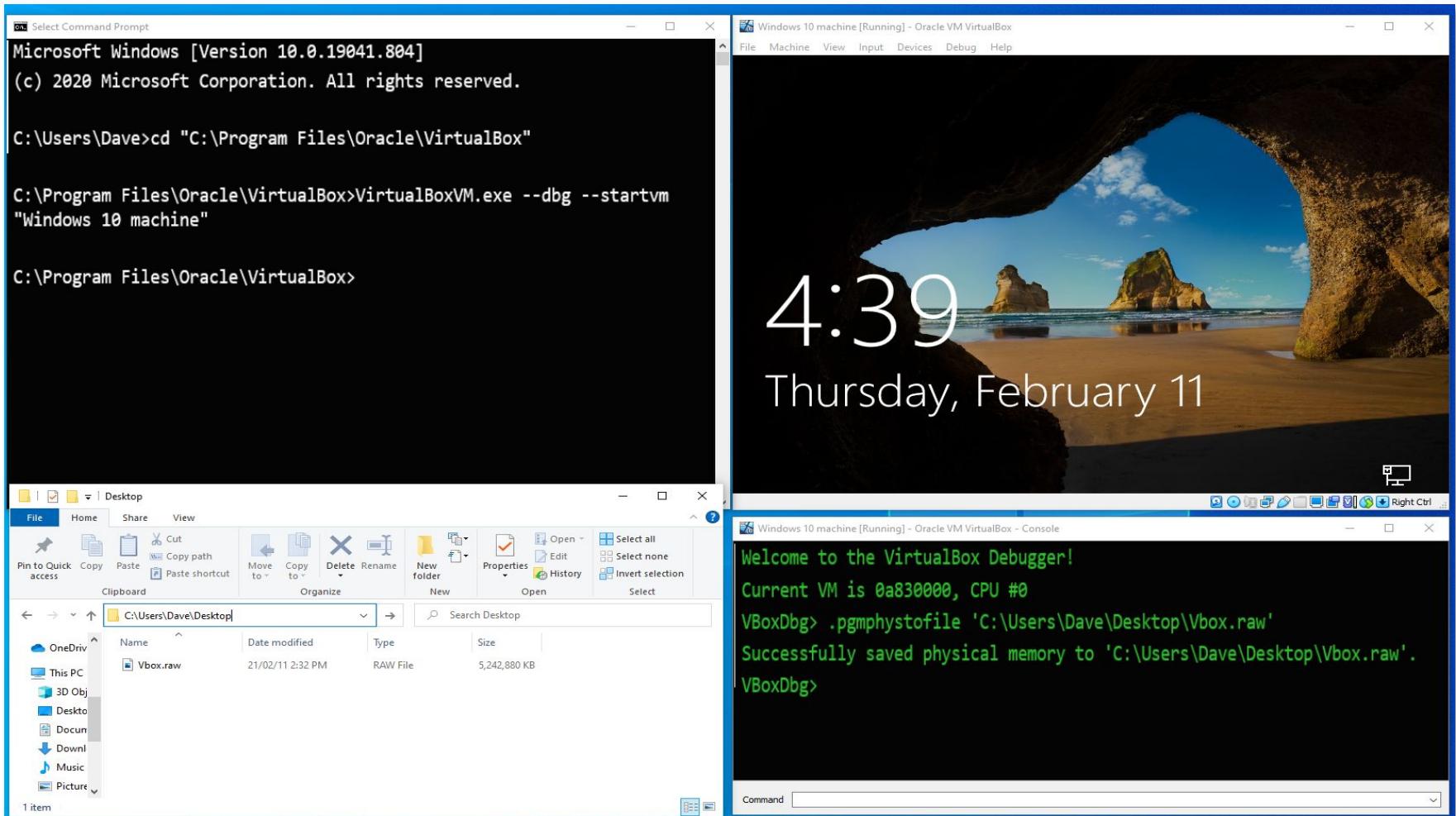
Virtual Memory Dumping

Memory Capture in VirtualBox

VirtualBox memory acquisition is more technical than other memory acquisitions.

VirtualBox starts the VM in debug mode.

The memory is captured in the debug console.





Data Acquisition

Memory in Other Locations



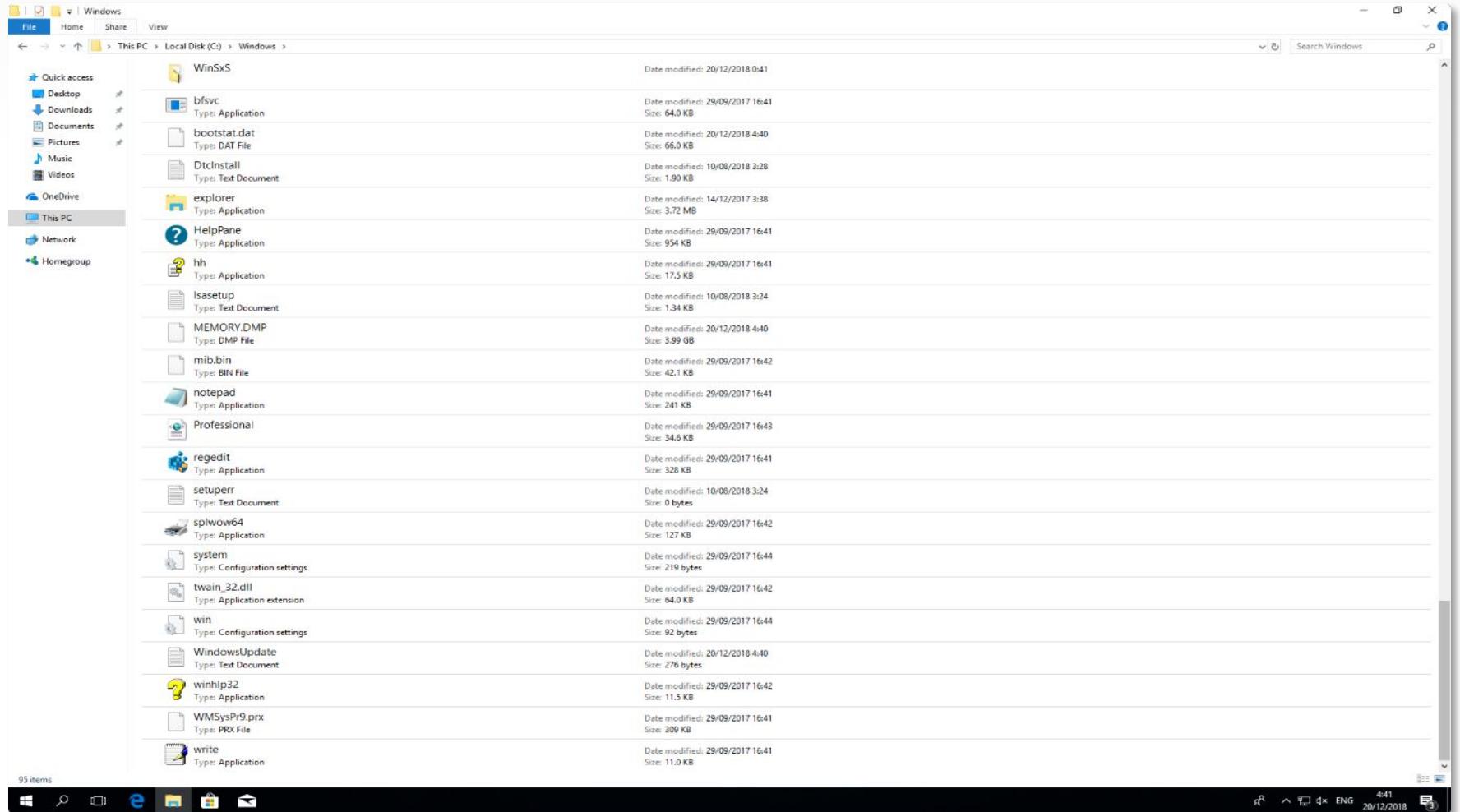
Memory in Other Locations

Crash Dumps

When the Windows operating system crashes, it creates a memory dump.

The size of the memory dump can be defined in the system settings.

When the computer recovers, a ***memory.dmp*** file will appear in the **%systemroot%** directory.





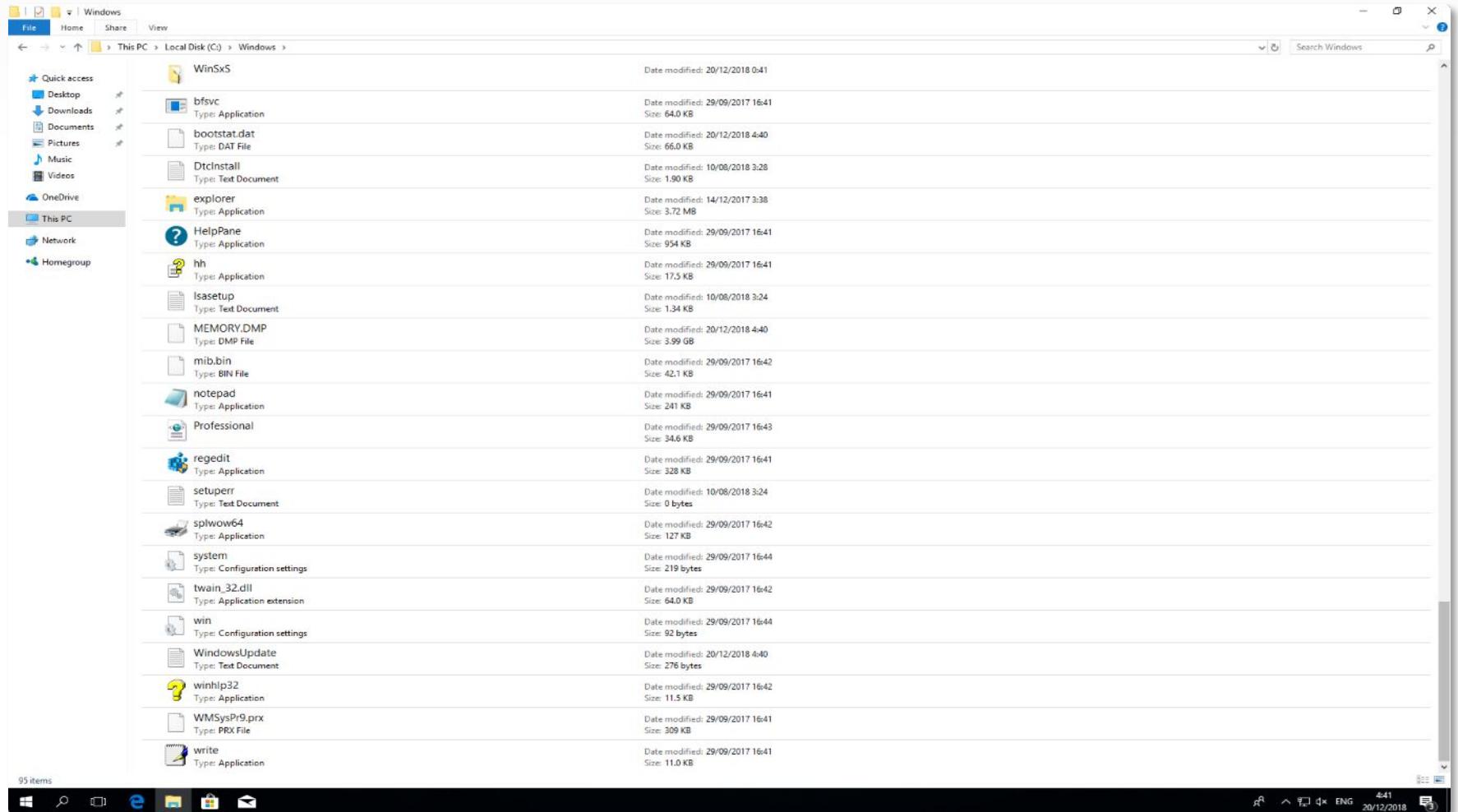
Memory in Other Locations

Hibernation

Windows hibernation files are compressed memory files.

Use Volatility's ***imagecopy*** tool to convert hibernation files.

Hibernation files are classified as system files and are hidden by default.





Memory in Other Locations

Windows Page Files

Page files store data when the RAM is low on space.

Although page files may contain useful data, they are not memory files.

A page file is often investigated by extracting strings.

```
Terminal Terminal File Edit View Search Terminal Help
windows\system32
tldl.windowsupd
windows0
ll\windows.storage\homefolder.cp
.windows.com0
ext\ms\windowscore-d
windows0
windows-
.windowssearch.com1&0
.com/windows0
windows_8
windows.dat
windowsp
windows-120
windows.hlp
windows-
: "https://licensingwindows.mp.m
    ogn.windowsC
e">ms-windows-store://pdp/?PrK
windows.hlp
windows
gle.com/search?q=windows+type+
windowsBuildNu
windows.hlp
windows
windowsDLLBlock
6/dist/windows.7c27c8f5b71f0410e
windows.hlp
d multiple windows
sapi_windows_cx
windows_cp9&v
activity-stream-windows.cs
windows.hlp
windows.hlp
windows.hlp
windows
windows
windows8Server%
c:\windows\system32\svcho
c:/windows/systemapps/m
sansforensics@stiftworkstation -> ~
$ 
```

```
000020b0: 2d20 2e9d 0131 7083 1c6b 9533 41be c6e1 - . . . 1p..k.3A...
000020c0: 701d 3b9a 0000 0000 c305 2e25 5187 2d1a p.;. . . . %Q.-.
000020d0: d63d f77f 7fc6 a07b afce 6f23 0060 4055 .=. . . . { .o#. `@U
000020e0: 966d 6d91 524d 4efc 0000 0000 c31f 643d .mm.RMN. . . . d=
000020f0: bf5a a573 81f0 32b4 056d 2b4f 5abd 51ce .Z.s..2..m+OZ.Q.
00002100: f08c 3438 319b c0f3 349f dc25 0000 0000 ..481...4.%...
00002110: abae cd2c d078 0e94 5394 c345 b4bc f918 ...,.x..S..E...
00002120: 1f45 d7cb 32c5 ec47 67bb 83b4 5daa 7c00 .E..2..Gg..].|.
00002130: 0000 0000 ad0d 21b2 d627 9bc4 7199 5746 .....!..'.q.WF
00002140: 291c 88af 5f79 a32c 3325 5e7d 1b71 d3a1 )..._y.,3%^}.q..
00002150: 226f cec5 0000 0000 f278 920c fca7 fb90 "o.....x.....
00002160: 930c a8dc 31b5 d71e ea54 7bd3 2b6a 3930 ...1..T{.+j90
00002170: 6a0f 3039 e793 4aec 0000 0000 1a86 3ca3 j.09..J.....<.
00002180: bcfe 48a8 ca2d 36a6 a564 6c57 2f6b dac1 .H..-6..dlW/k..
00002190: c790 3c57 e668 1555 e6ad 0000 0060 0040 ..<W.h.U..`@.
000021a0: 003d 0095 0000 955c 0f02 0088 eb8c 0b50 =. . . \. . . P
000021b0: ef8d c800 1700 0fff 9304 c286 fae9 290e .....
000021c0: 0203 8c00 8d00 8cff 1f00 0000 8d00 3800 ...
000021d0: 8c0b 3800 8c0b 00f0 8d0b 0000 0e00 bc00 ..8.....
000021e0: 2044 8440 0007 00ff 162d 716b c6bd e5a7 D.@....-qk...
000021f0: 01c4 f9af 0b69 0a0a fd9f 3a00 00d0 54e2 ....i.....T.
00002200: 0029 1d5a 7741 005c a96f 7723 002d 91e4 ).ZwA.\.ow#.-..
00002210: 4000 1900 7900 0202 db01 10fb bb01 2b00 @...y.....+.
00002220: bb01 1600 50c2 00f0 f2bb 0030 3301 2f00 ...P.....03/..
00002230: 47e8 fc00 af01 8f3a fc7f 0000 4991 4a9b G.....;..I...
00002240: 7d00 b0f1 3b02 8501 0145 003c 007d 00ff }....;...E.<.}.
00002250: 0400 50f5 7f01 8913 7b05 44f8 fb03 95cf ..P.....[.D...
00002260: 63fa 0530 bc02 cbbe 7c00 ce6f ba00 e999 c..0....|..o...
00002270: 630a c09a 6d06 d102 347c 01c6 cefb 00bd c..m..4|.....
00002280: 0030 01ef cc03 3300 7f03 66b0 cd7b 01eb [0....3..f.{..
00002290: 0000 00fd 043d 00bd 003f 0024 3c0b f0ff .....=....?<...
000022a0: fb05 7e30 36b7 7d00 20bc 0049 024c 2702 ..~06.}. . . I.L'.
000022b0: 6f07 a702 7f00 4fff e801 3d67 ff1d bf14 o.....0....=g...
000022c0: 3047 2b10 fc1d 0000 8efa 1aa3 0000 0009 0G+.....
000022d0: 5195 7f00 bd00 5713 0f57 7f05 0d04 3b05 Q.....W.W....;
000022e0: ebc7 10c0 7d4f fb04 ff00 f83c 01be 067b ...}0.....<.{.
000022f0: 009e 7f01 0733 012f 00ff 481b 0010 0080 .....3./..H....
00002300: 1f00 0033 4e03 2b00 0002 6600 4700 18f0 ...3N.+..f.G...
00002310: b57f 920c 3d24 0502 e71c 6739 28fa 7b21 .....=$....g9(.{!
00002320: 7d00 3f00 df37 7036 fb0b 7fdf 0519 07ff }.?.7p6.....
00002330: ffe7 00fd 6704 377f 028f ff4a 064c 013f ...g.7....J.L.?
00002340: ee5c c732 7d37 ffff df00 f88f 003b e840 .\}.2}7....;@
```

--More--

Lab DFIR-04-L4

Built-in Memory Capture

15–20 Min.



Mission

Configure Windows 10 to create a memory dump during a system crash.

Steps

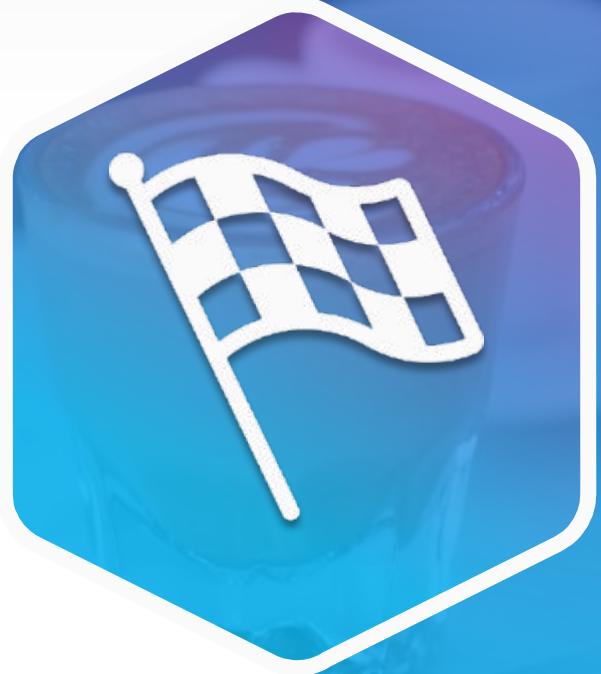
- Open the machine's system configuration settings.
- Configure the system to create a full memory dump when a crash occurs.

Environment & Tools

- VirtualBox
- Window 10

Related Files

- Lab document



Thank You

Questions?