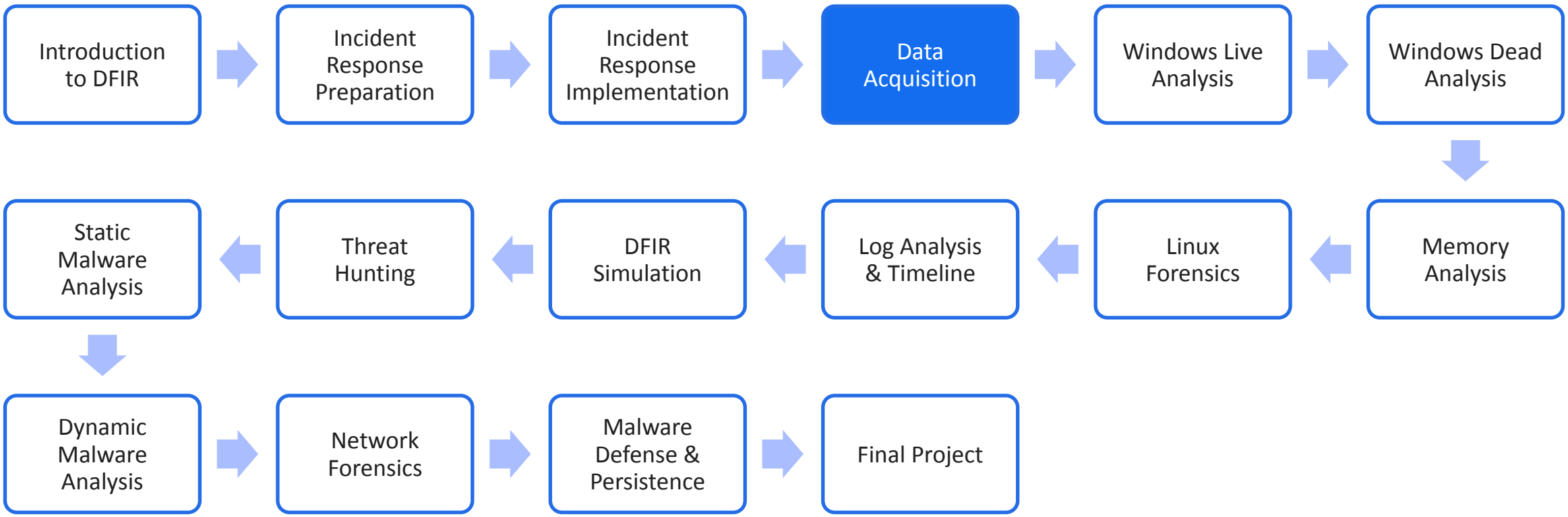
Cybersecurity Professional Program

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

Data Acquisition

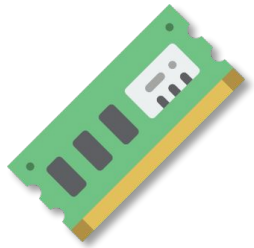
State Capture

- 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		Disadvantages
Provides an exact copy of the evidence		Sometimes, only a partial capture is possible.
Used as a backup for the evidence		Takes time to create a state capture
Artifacts can be extracted from .the capture	VS.	If the evidence was encrypted at the time of the capture, the resulting image will also be encrypted.
Allows creation of a static capture of the memory		Memory cannot be inspected for changes.
All file details can be viewed .in tables		Not the typical way to inspect data on a computer

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

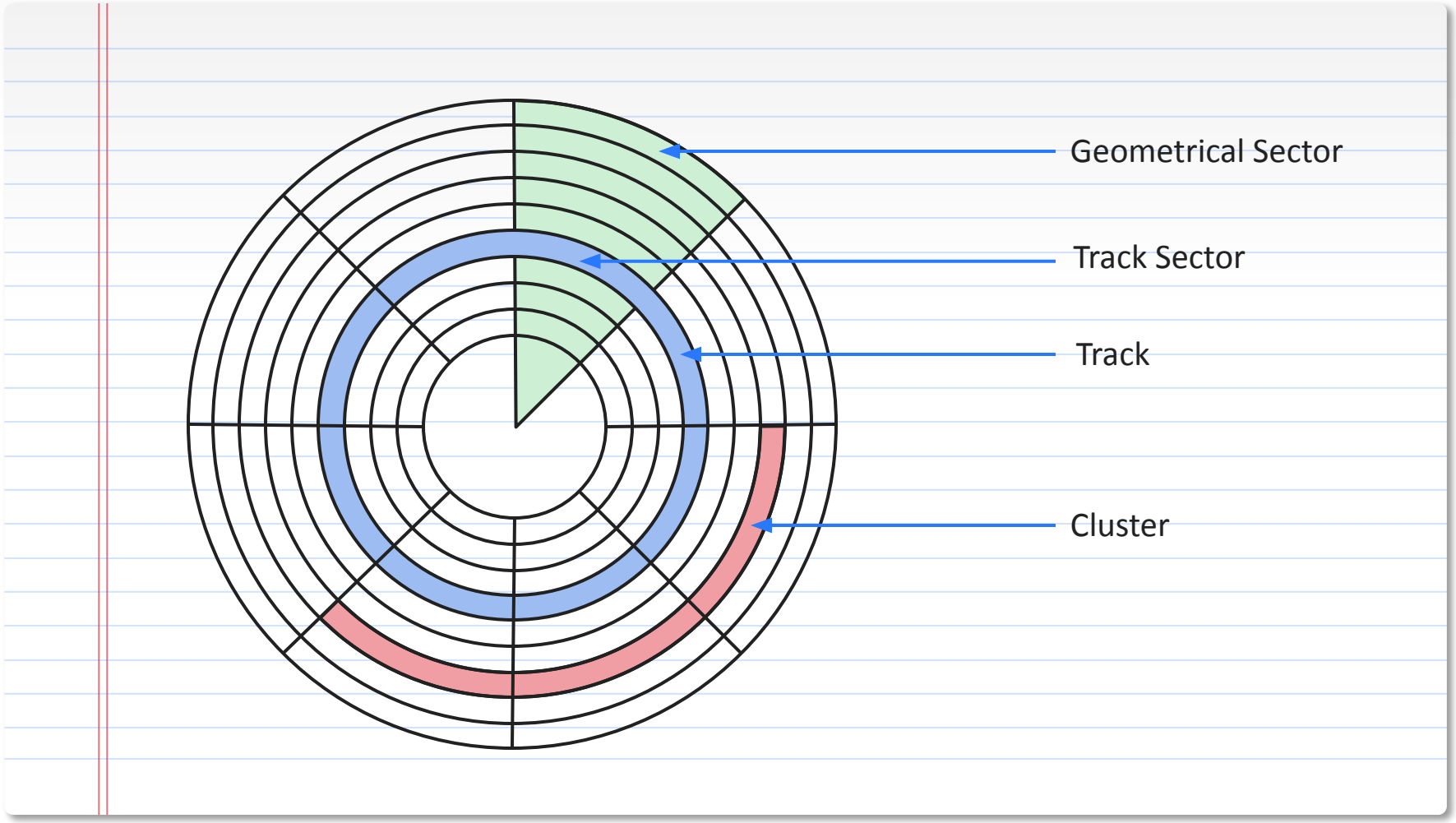
Drive Capture

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.



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

Falcon

Capture Formats

RAW

ISO

EWF

dd

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

Drive Capture

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

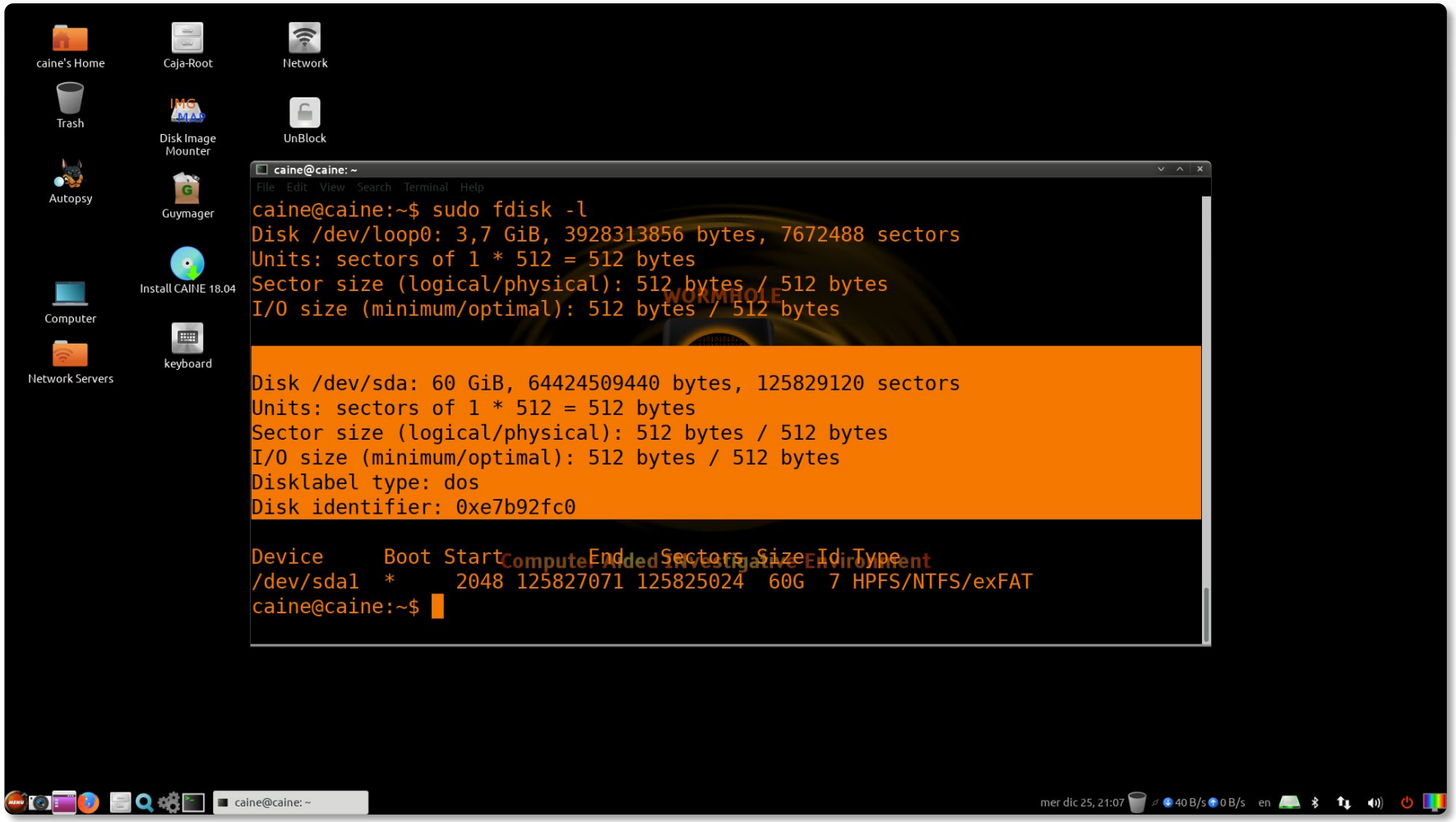
if: the source disk

of: the target disk where the piped data is written

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

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.



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

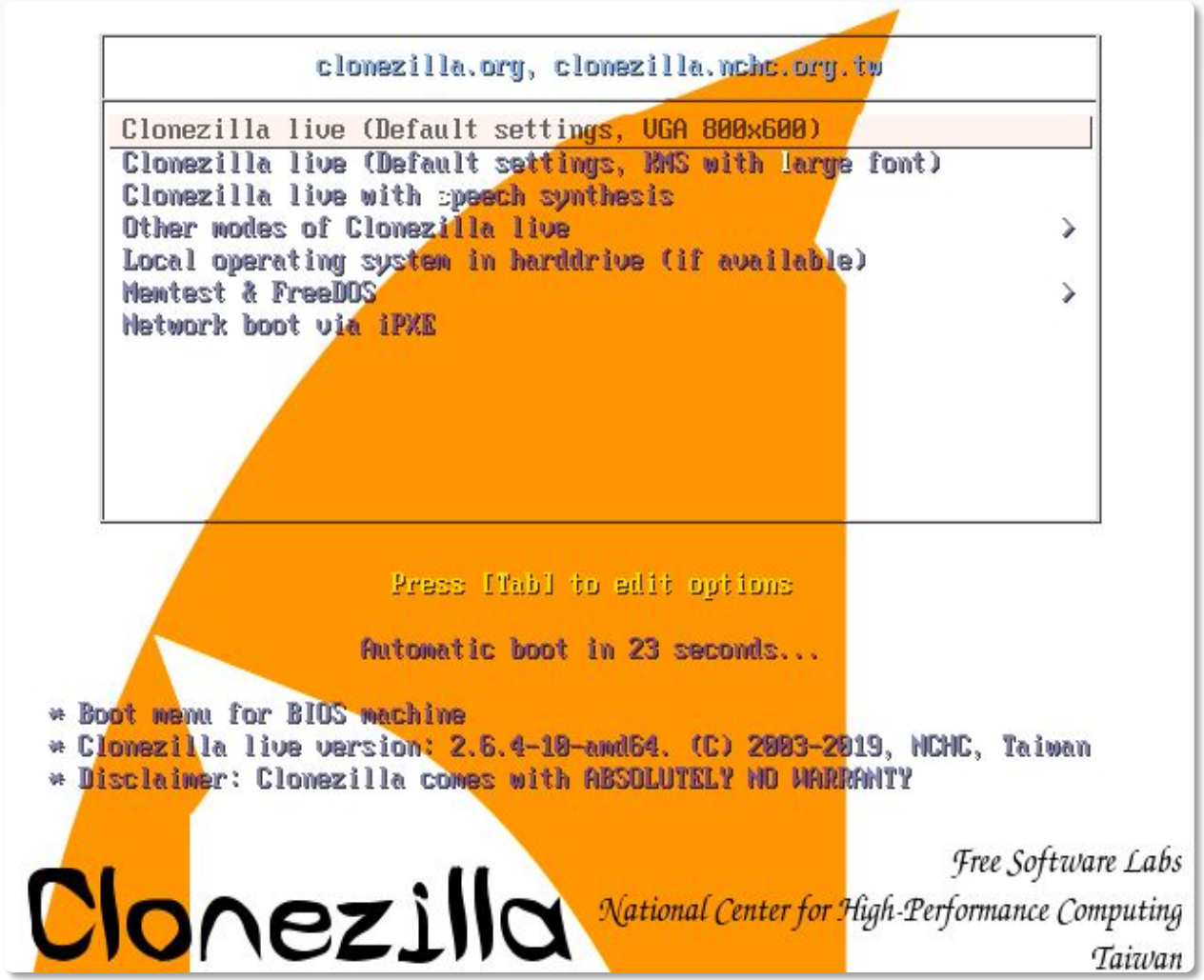
- Lab document
- ***CAINE.iso***

Data Acquisition

Advanced Capture Tools

Advanced Capture Tools

Clonezilla

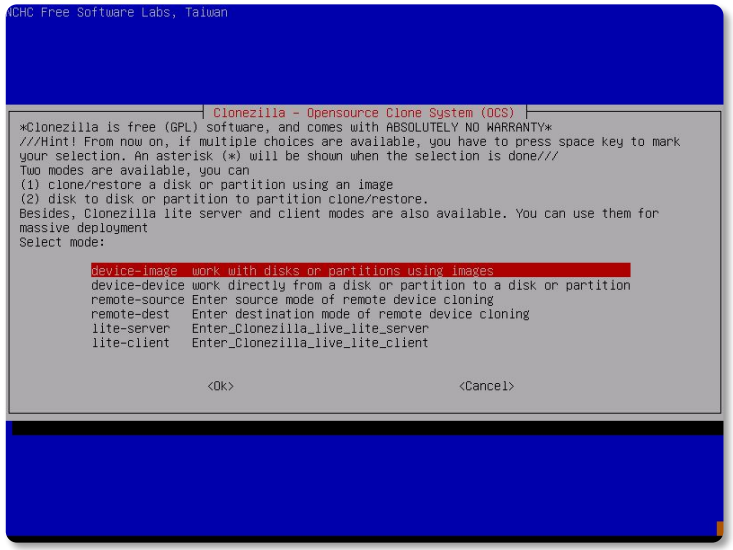


Clonezilla is a live Linux distribution dedicated to cloning drives.

Clonezilla uses its own format to save images.

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

Clonezilla Capture Modes



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

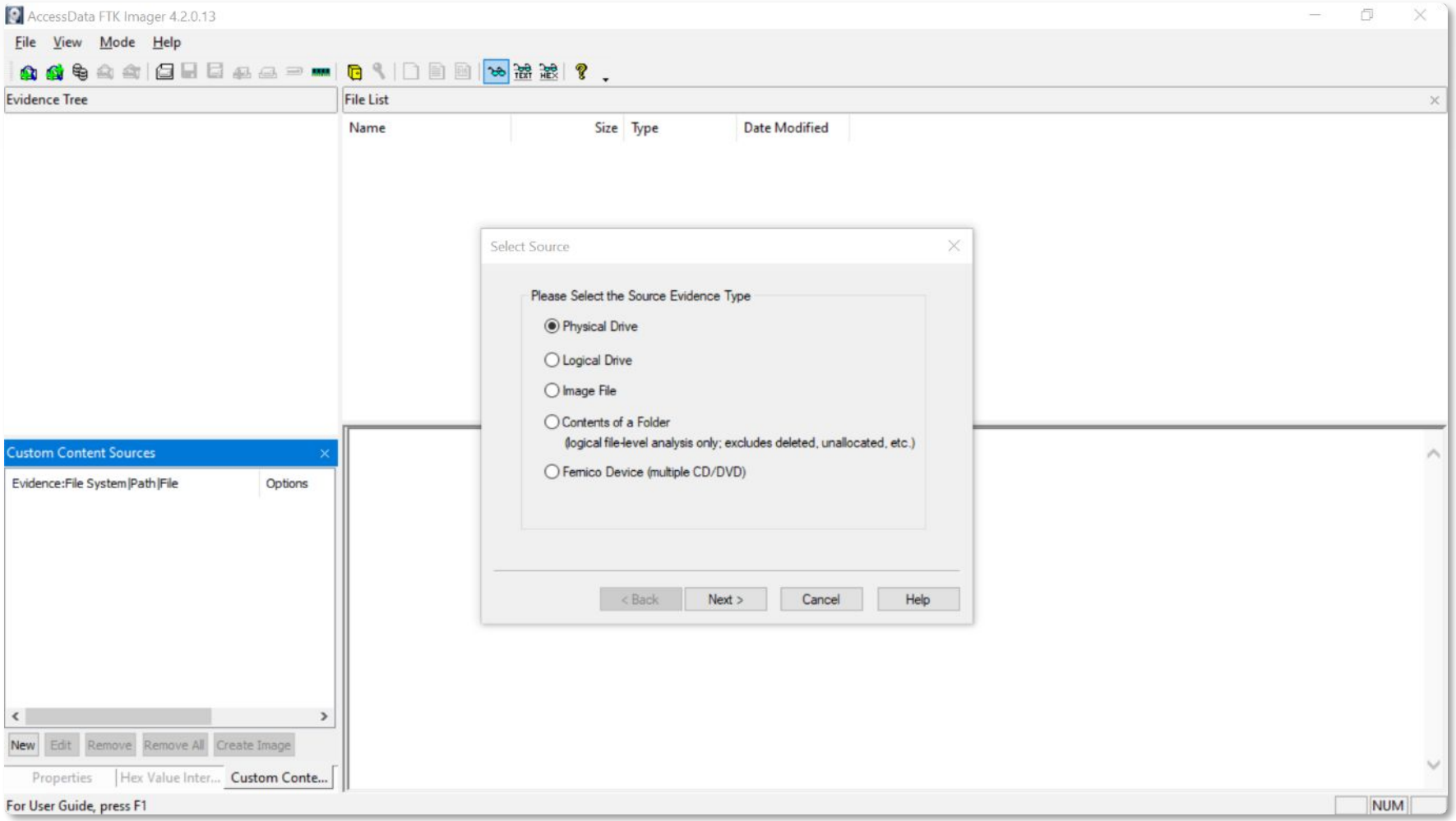
Device-device: This option clones an entire drive or partition to another drive or partition.

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

Advanced Capture Tools

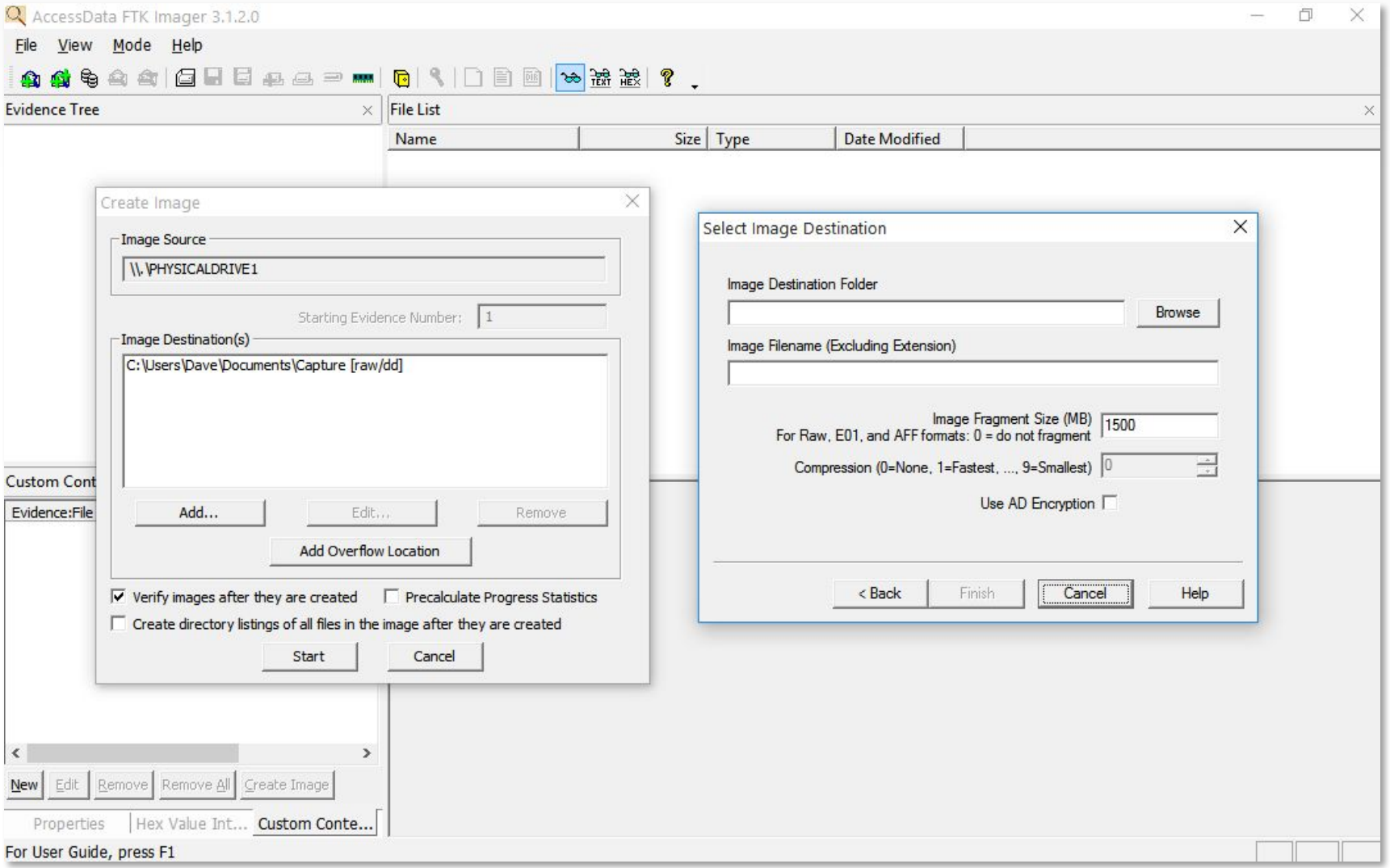
FTK Imager

- 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.



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

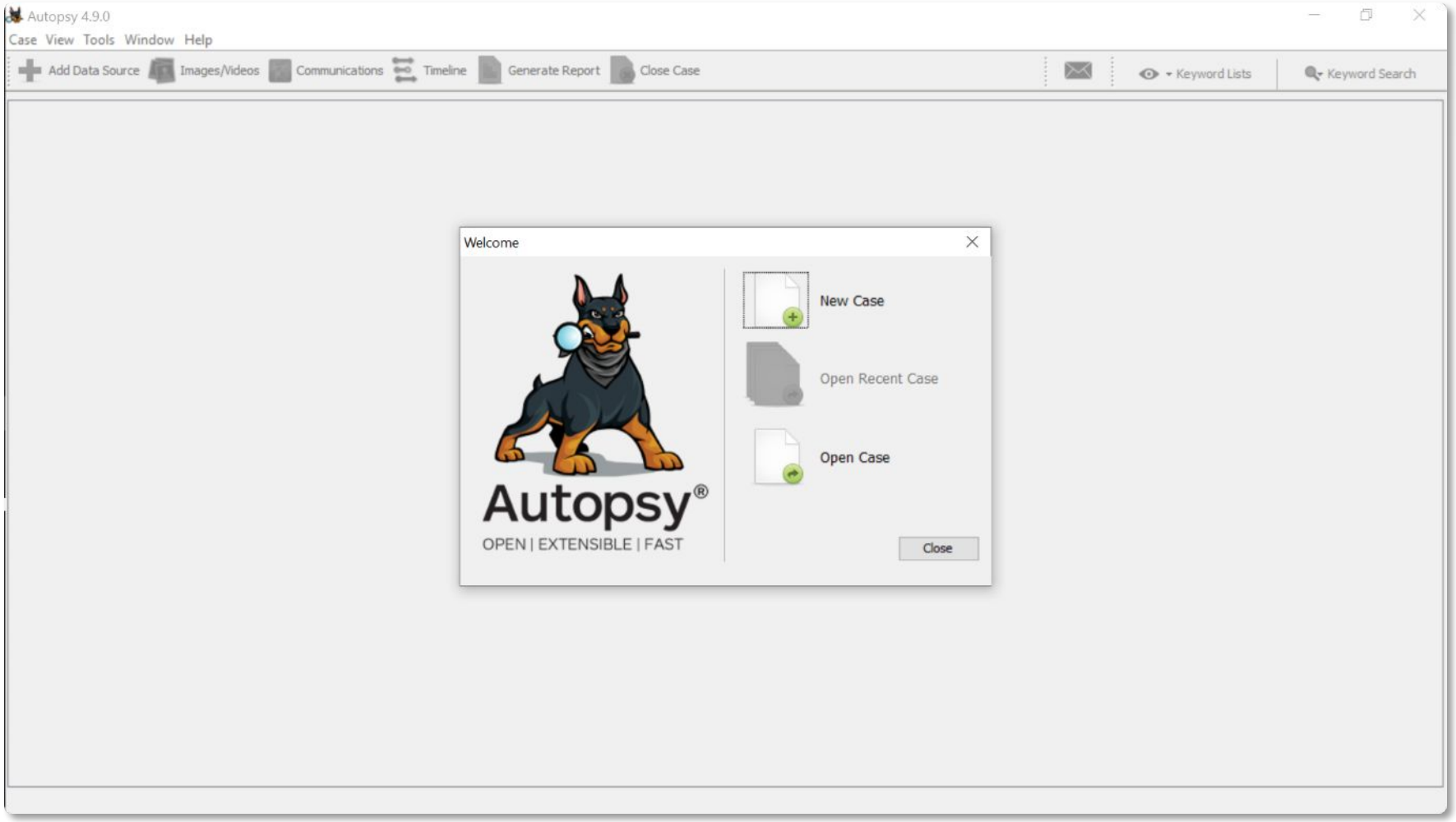
- The traditional way to investigate an image is to open it in a dedicated software tool.
- An alternative method is to create a VM based on the image.

> 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.

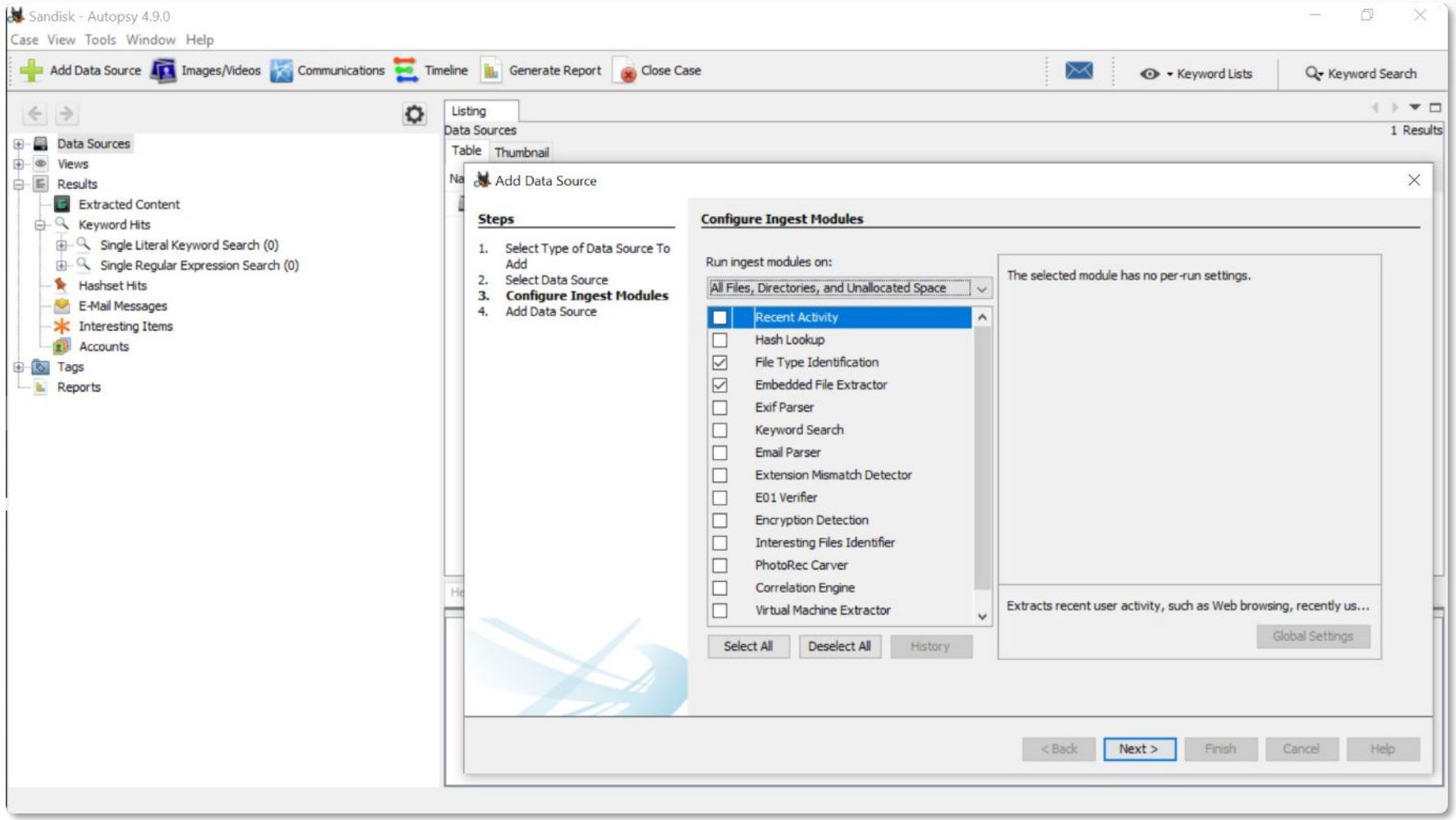


Autopsy Features

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.



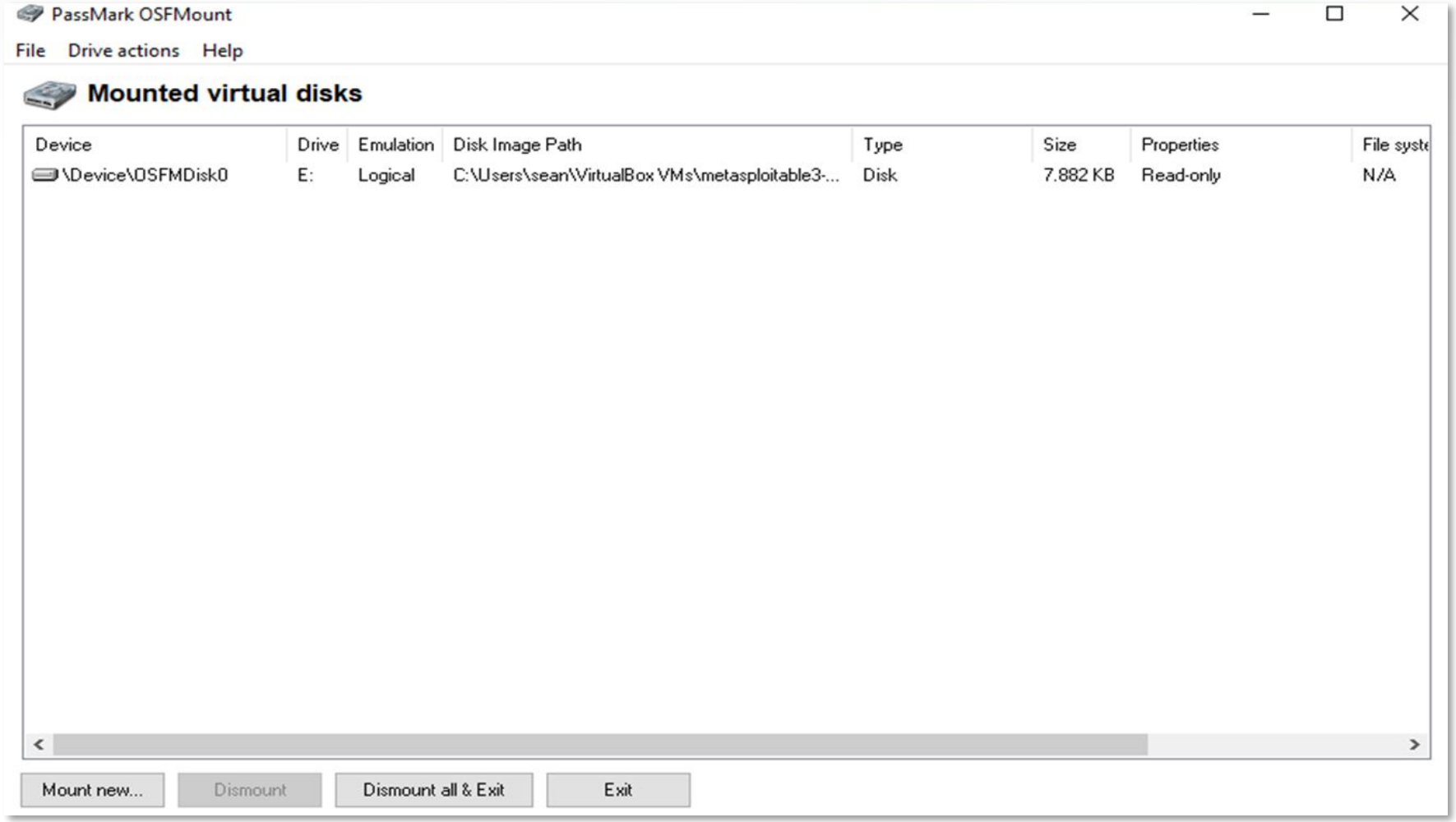
Evidence Inspection

OSFMount

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

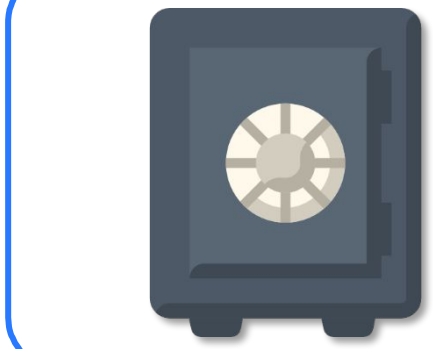
It reads the disk partition bit for bit. By default, image files are mounted as read-only.

OSFMount supports disks that are mounted in RAM.



Evidence Inspection

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

- 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.

Evidence Inspection

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.

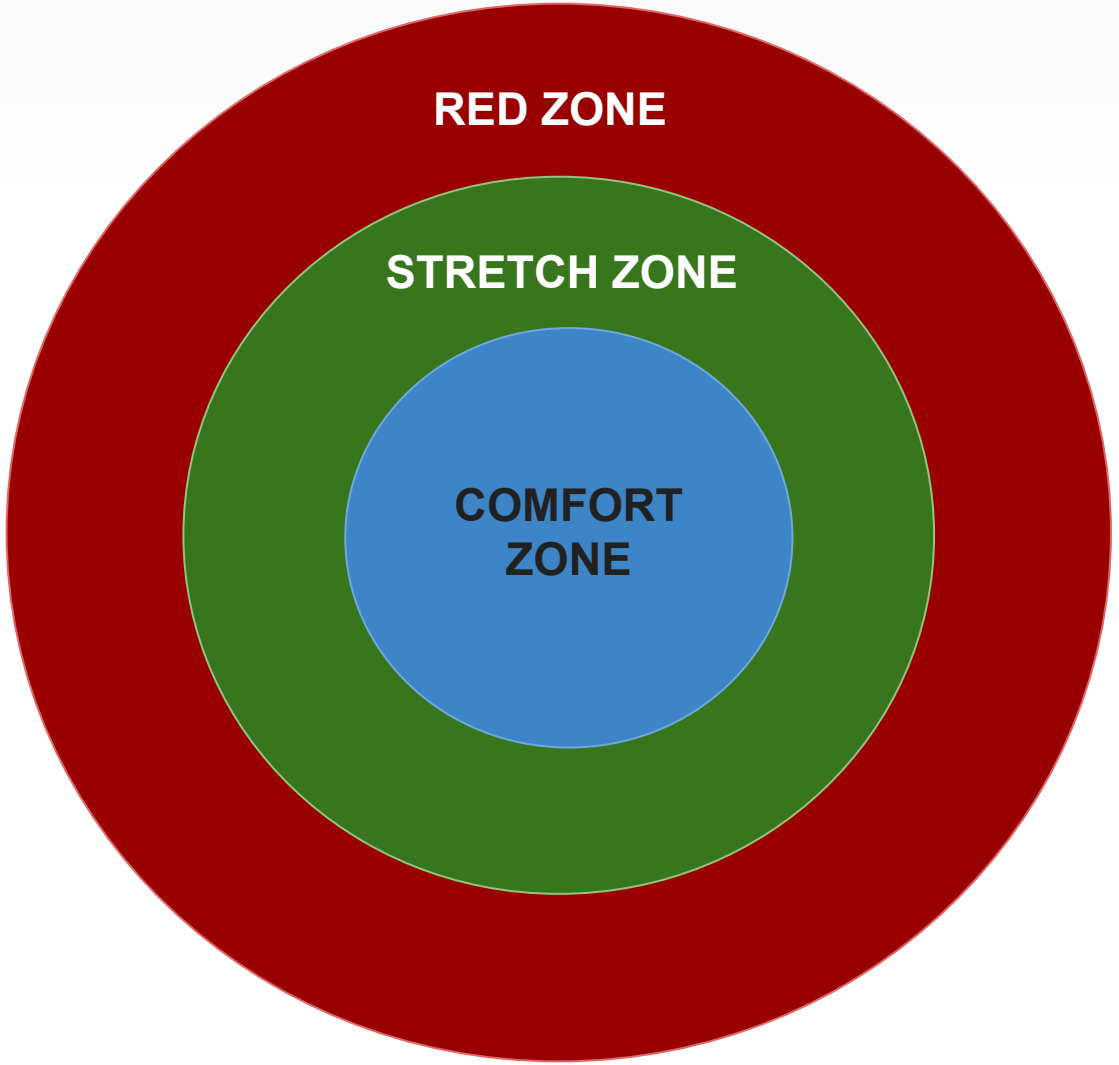
Environment & Tools

- VirtualBox
- Windows 10

Related Files

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

Pulse Check



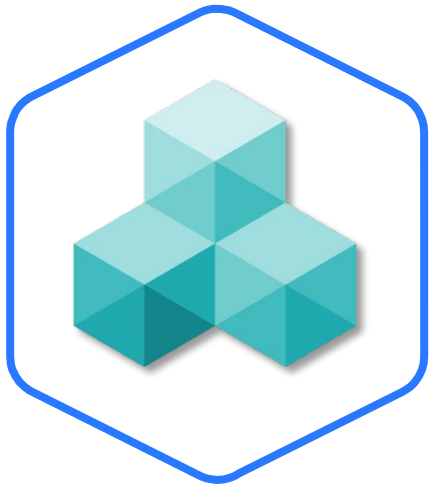
Data Acquisition

Virtual Drives

Physical vs. Virtual Drives

Physical		Virtual
Contains RAW data		Contains RAW + VM data
No format, only bytes		Different formats for different vendors
.The drive has a constant size	VS.	Space can be dynamically allocated.
A single unit of data		Can be split across files
A device with mechanical components		A file within the file system

Virtual Drive Formats



VHD

VMDK

VDI

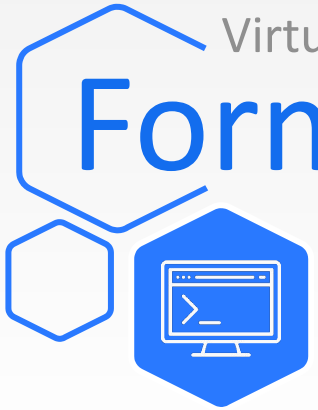
VHDX

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.

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
```

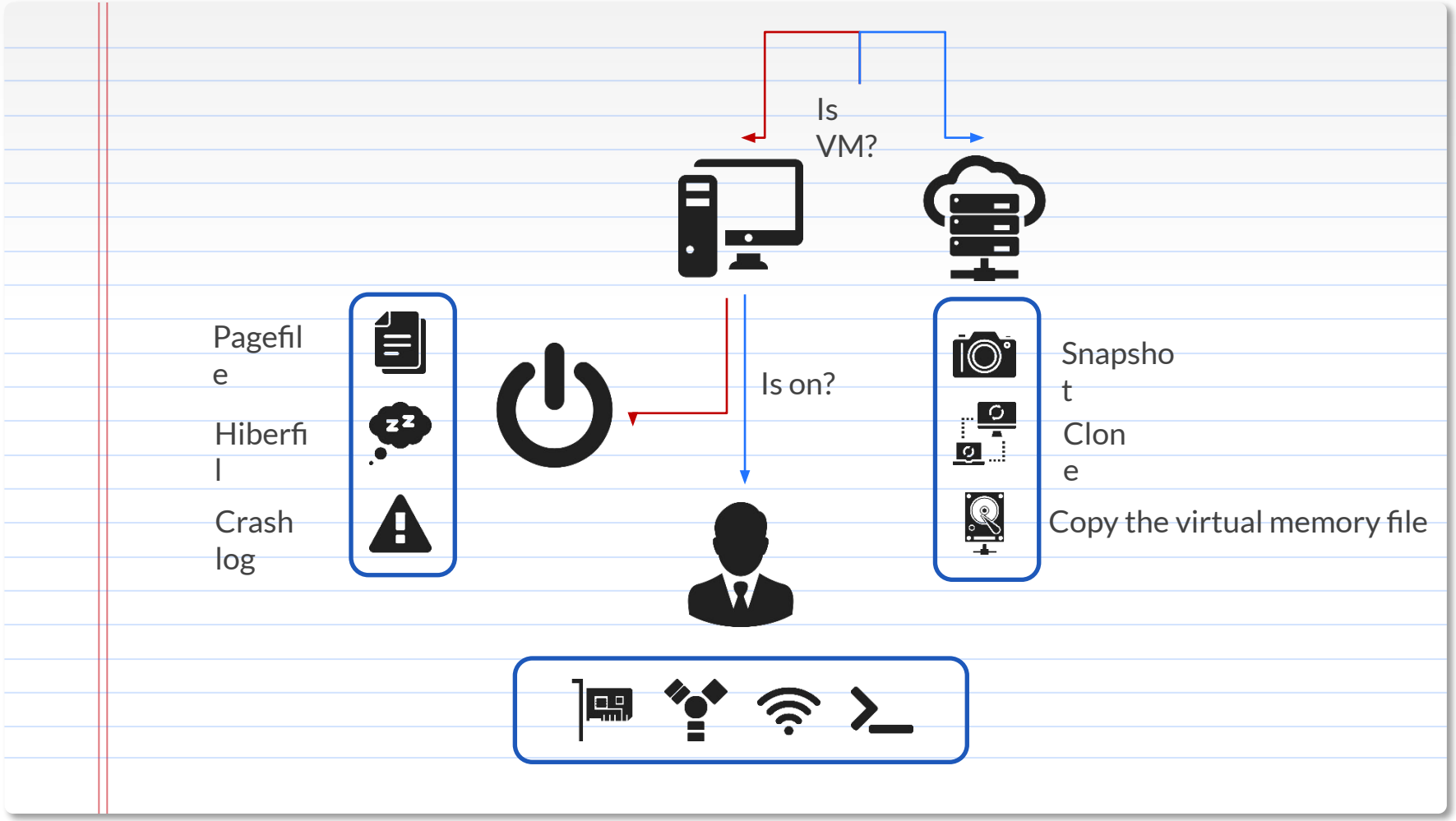
Data Acquisition

Memory Dumping

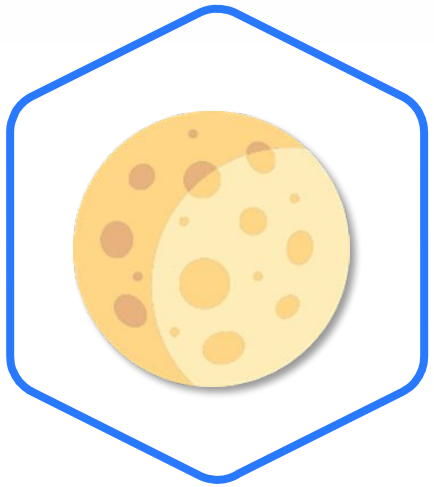
Memory Dumping

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 Tools



MWMT

FastDump

FTK Imager

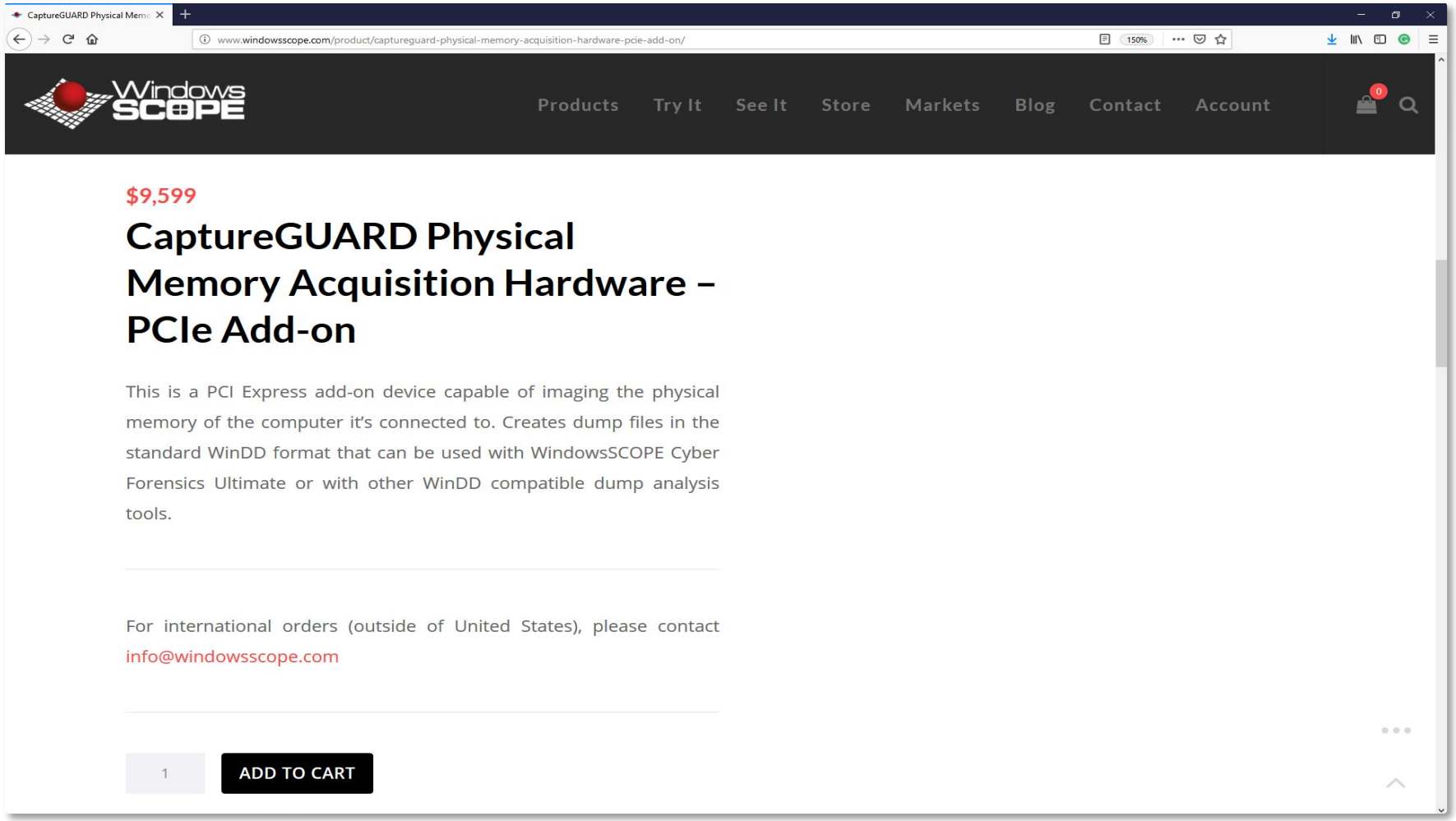
WinPmem

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

Memory Dumping

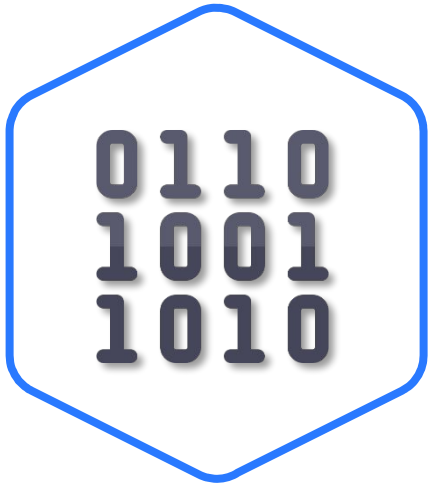
Commercial Tools

- 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.



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

Memory Dump Formats

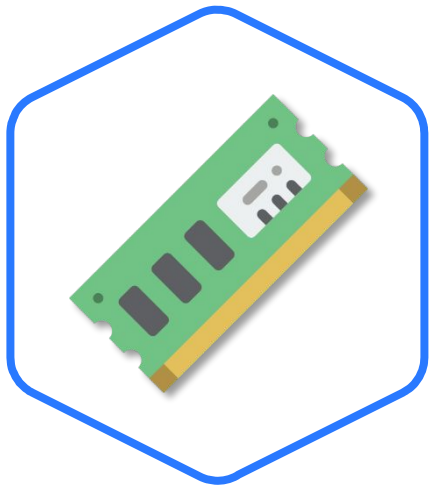


RAW

Crash Dump

Hibernation

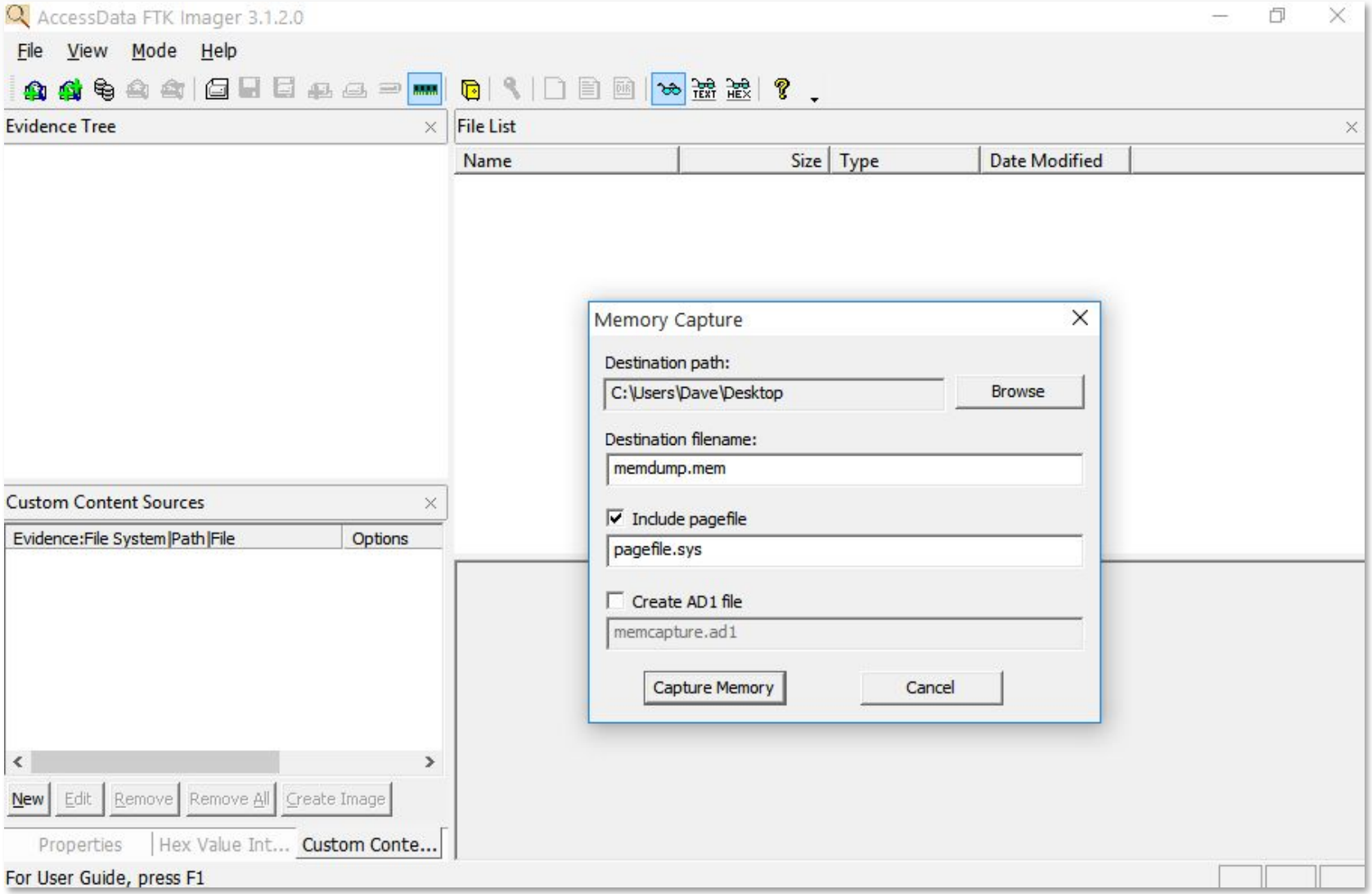
EWF



AFF4

Dumping Memory in FTK Imager

- Use tools like FTK Imager and DumpIt 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.



Memory Dumping

Volatility

- 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.

Memory Dumping

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 vs. Physical Memory

Physical		Virtual
Contains RAW data		Contains RAW and VM data
No format, only bytes		Different formats for different vendors
.The memory has a constant size	VS.	The memory can be dynamically allocated.
Requires tools for capture		Can be captured by a hypervisor
A device with mechanical components		An allocated area within the memory

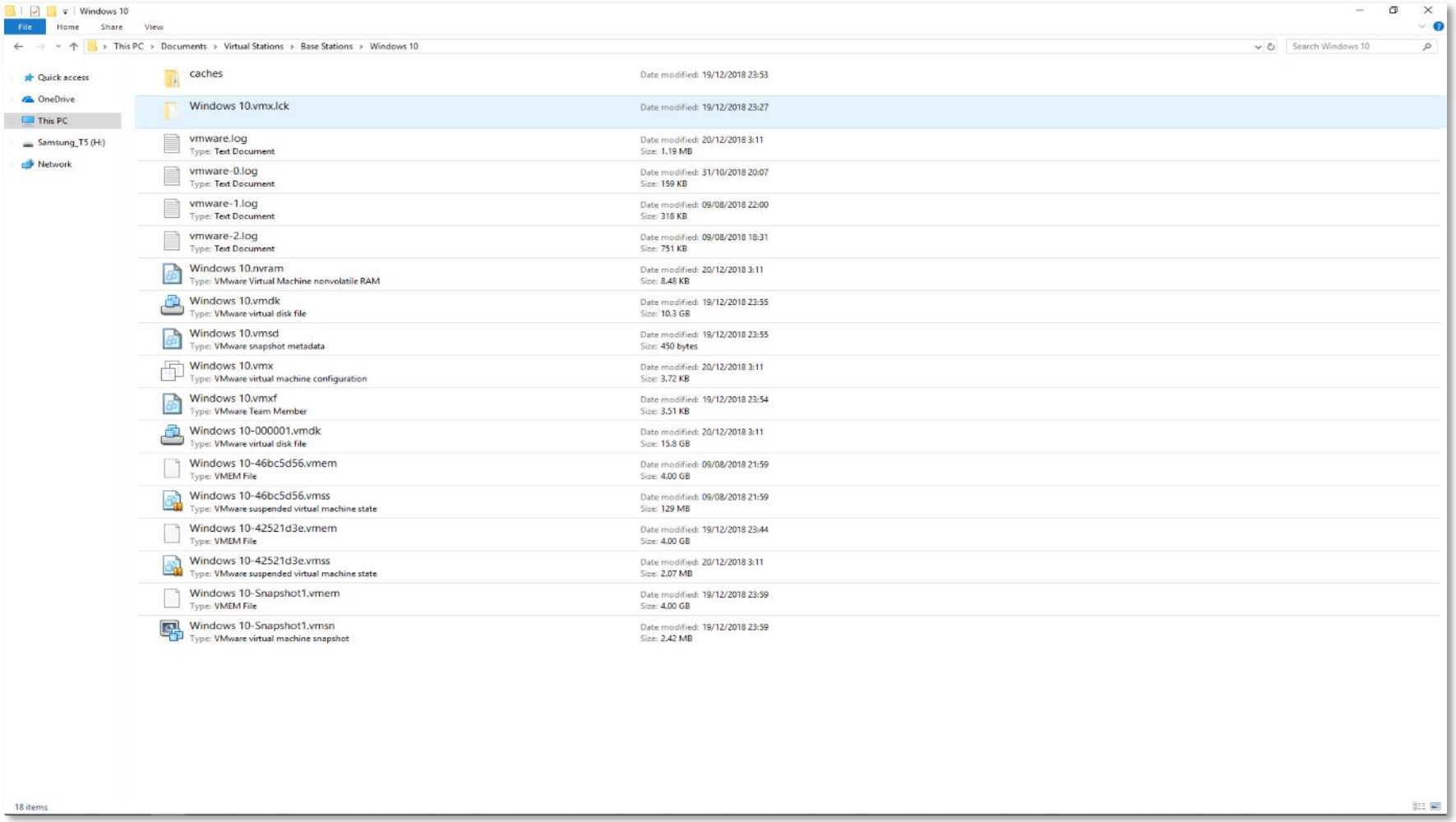
Virtual Memory Dumping

VMware Memory

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

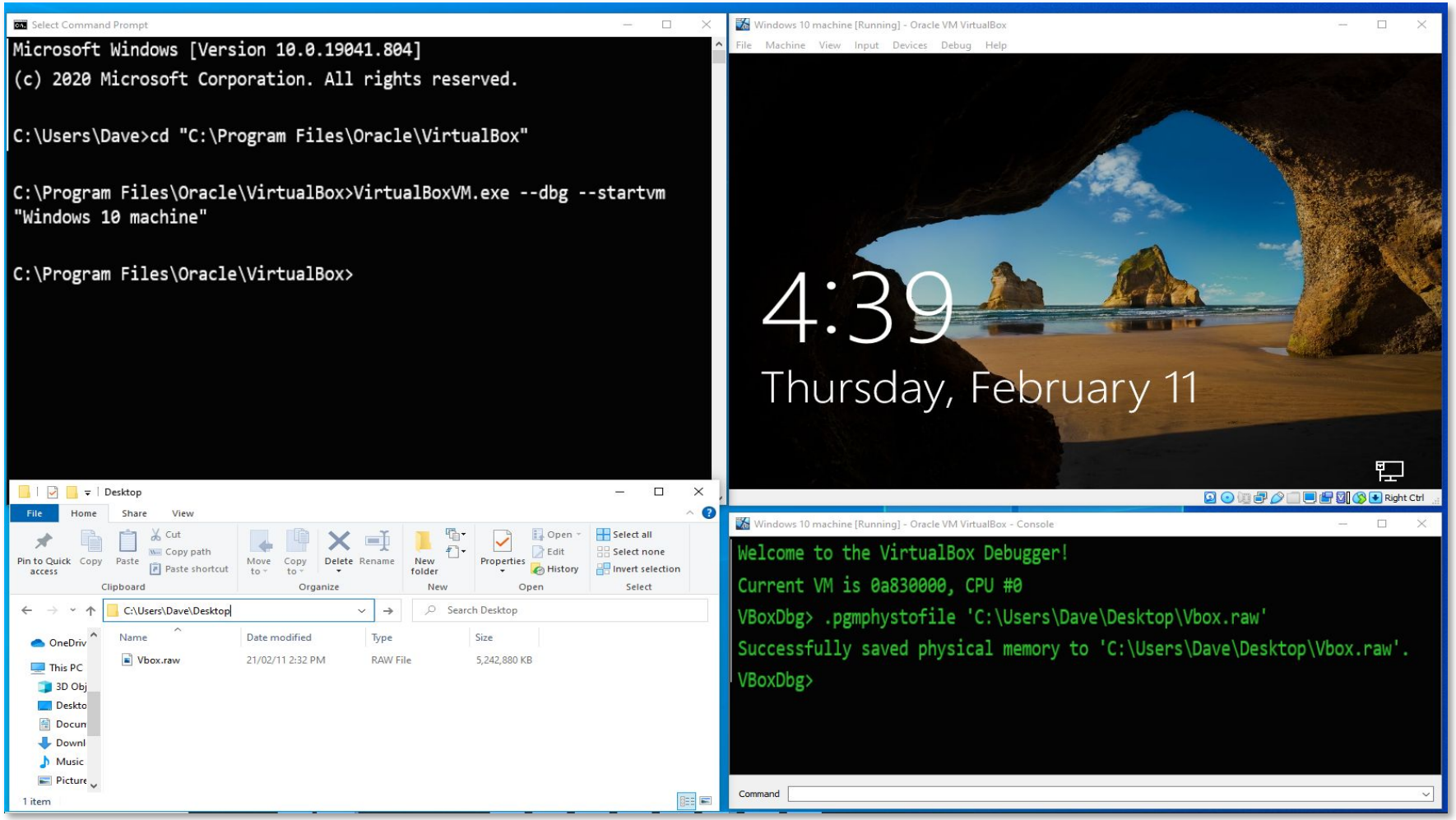
Memory files typically will be in ***.vmem***, ***.vmsn***, and ***.vmss*** formats.

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



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

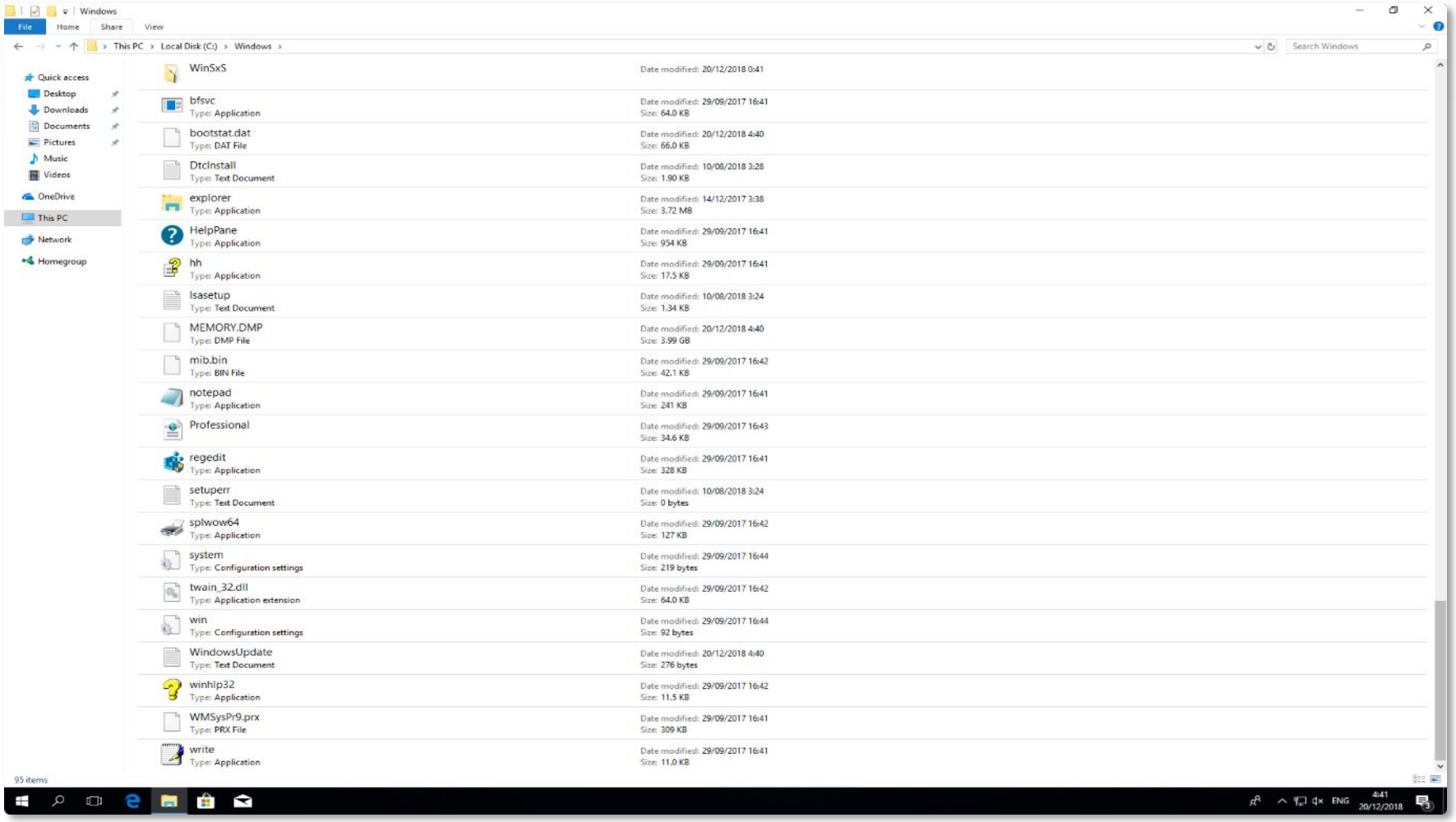
Memory in Other Locations

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.

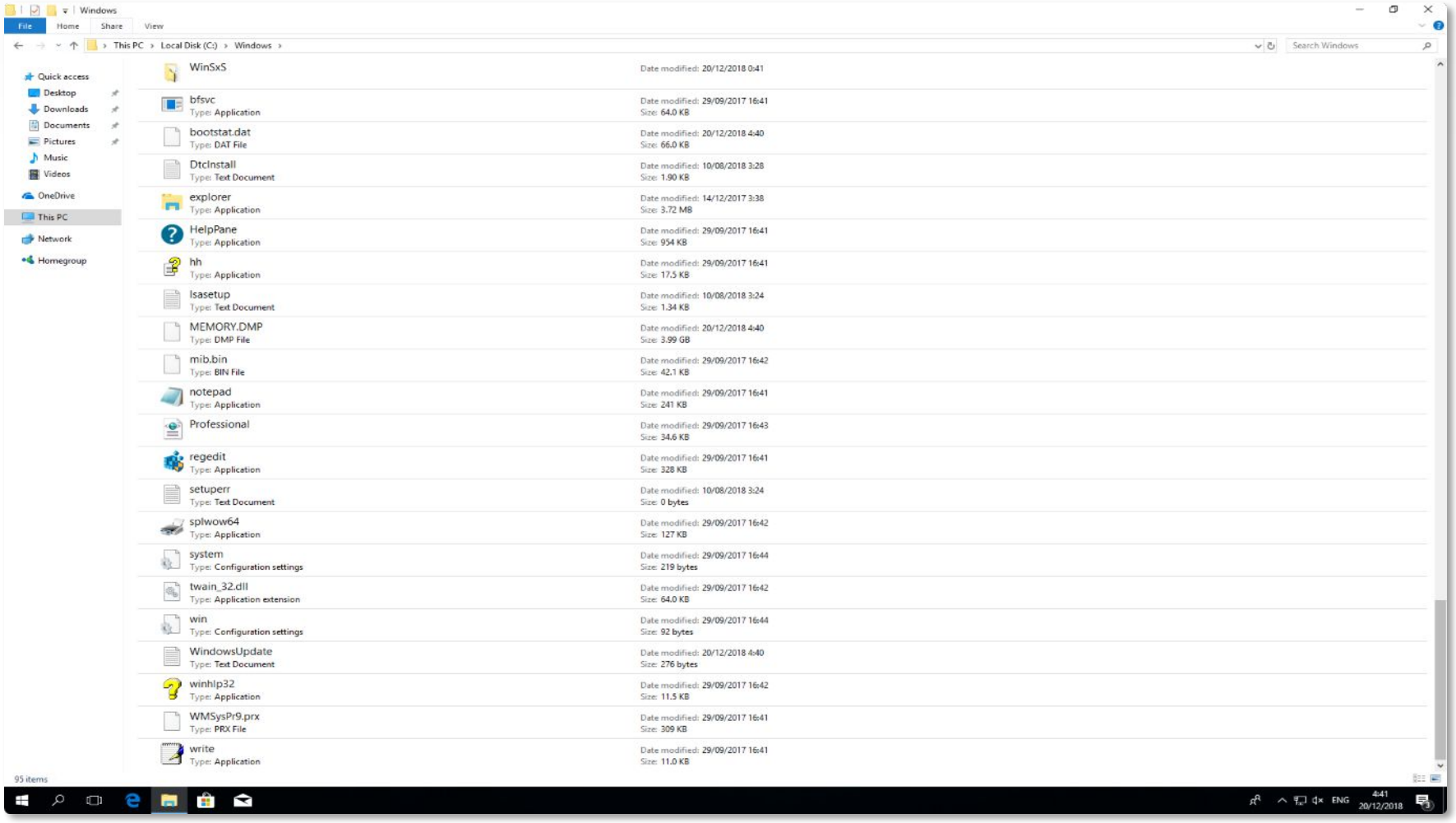
When the computer recovers, a ***memory.dmp*** file will appear in the ***%systemroot%*** directory.



Memory in Other Locations

Hibernation

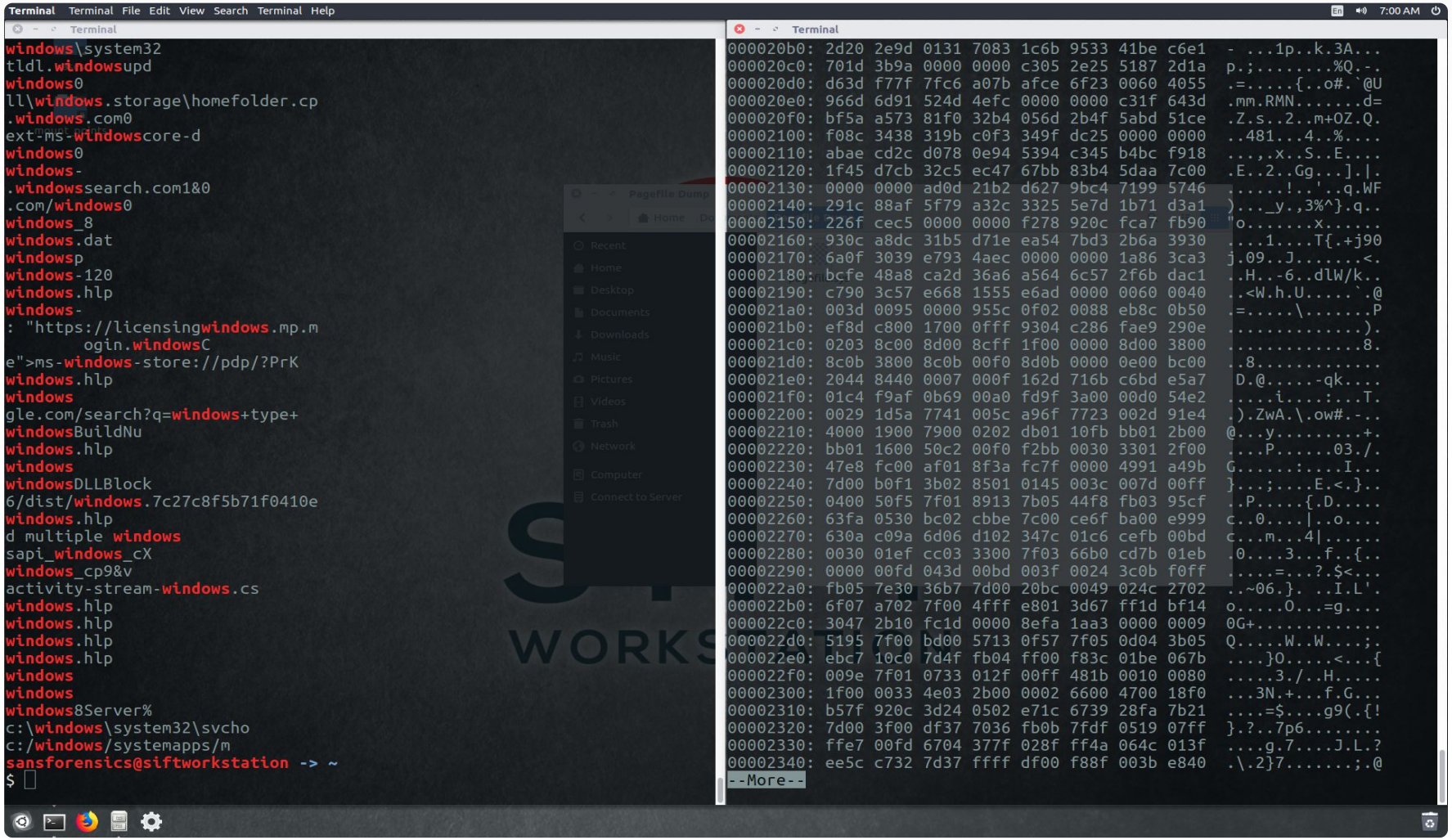
- Windows hibernation files are compressed memory files.
- Use Volatility's ***imagecopy*** tool to convert hibernation files.
- Hibernation files are classified as system files and are hidden by default.



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.



Memory in Other Locations

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?