universidade
de aveiro

Computer Systems Forensic Analysis
AFSC

RAM Analysis

Artur Varanda

School Year 2021-2022

If evidence of compromise is never written to a hard drive, we cannot rely on disk forensics!

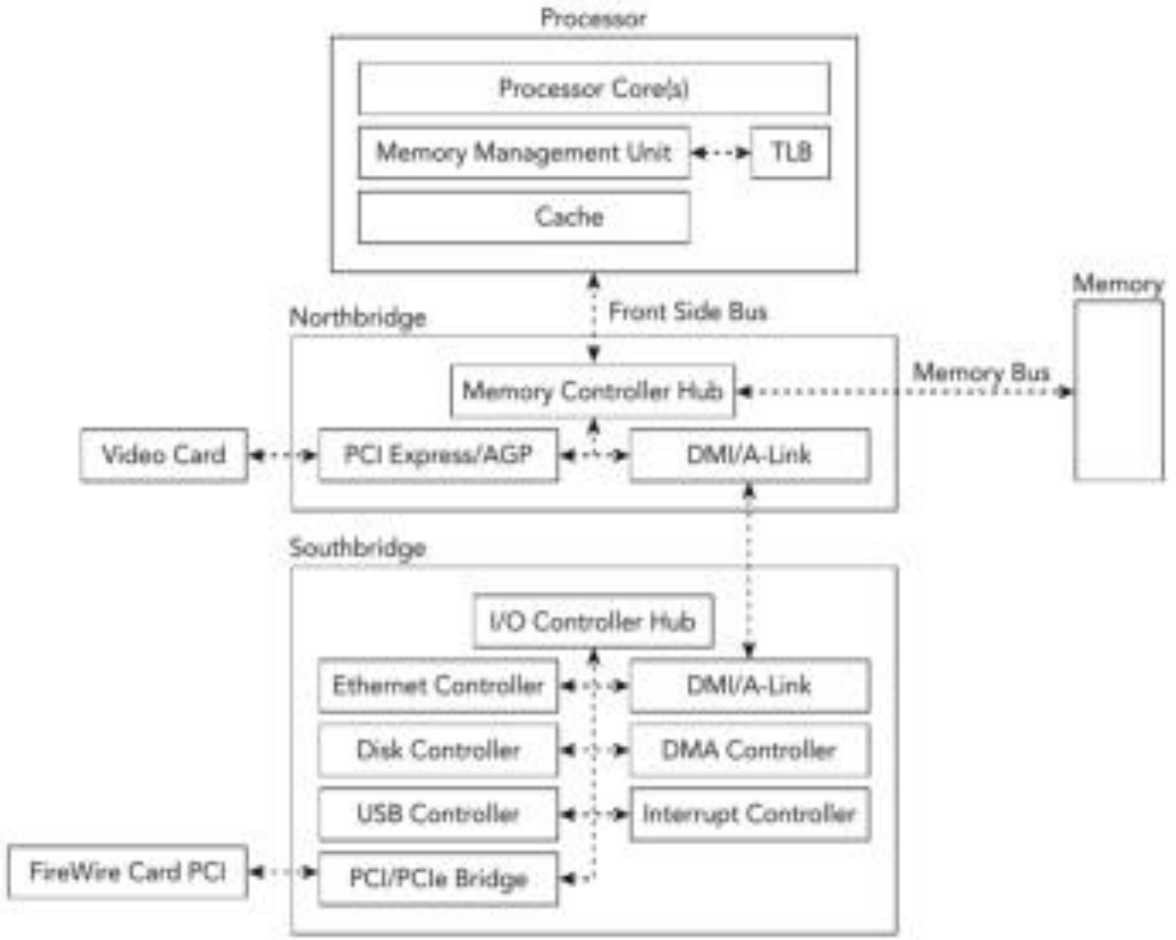
Volatile memory has a high potential to contain:

- malicious code from an infection, in whole or in part, because it must be loaded in memory to execute
- evidence that system resources were allocated by the malicious code
- encryption keys and passwords, or the plain-text contents of files before they were encrypted

Architecture

- CPU – accesses main memory to obtain its instructions and then executes them
- RAM – volatile memory that is much slower than CPU
- Cache – faster than RAM, but still slower than CPU
- MMU – Memory Management Unit to help find where the data is stored (RAM or Cache)
- TLB – Translation Lookaside Buffer is a special cache for MMU to translate memory addresses

Figure: Physical organization of a modern system

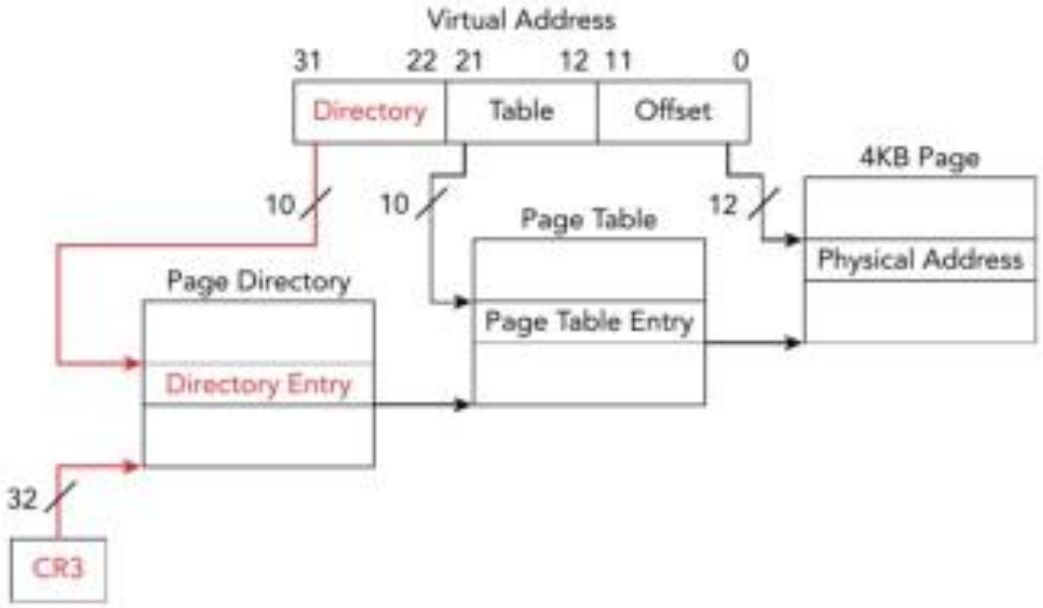


Direct Memory Access (DMA)

- provide I/O devices the capability to directly transfer data stored in system memory without processor intervention
- improves performance
- CPU initiates a data transfer and DMA controller manages the data transfer

- provides the ability to virtualize a linear address space
- creates an execution environment in which a large linear address space is simulated with a modest amount of physical memory and disk storage
- typical page size is 4 kB
- different paging structures are used for different processes
  - ✓ the OS provide each process the appearance of a single-programmed environment through a virtualized linear address space

Figure: Address translation to a 4 kB page using 32-bit paging



Impact on memory forensics

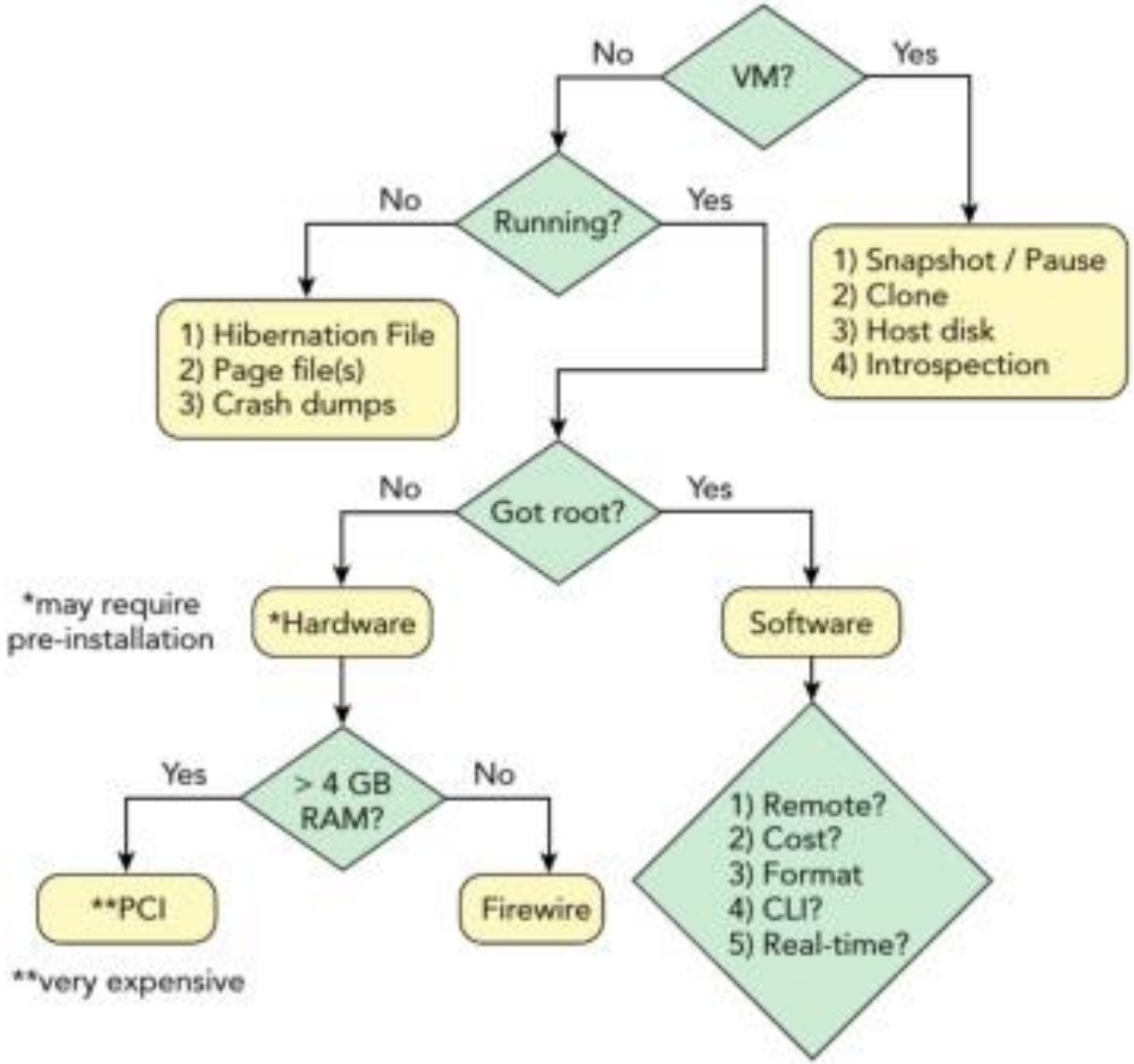
Forensics software must emulate the virtual address space and transparently handle virtual-to-physical-address translation

Memory Acquisition

Memory acquisition (also know as dumping, capturing, sampling)

- copy the contents of the volatile memory to a non-volatile storage
- an important source to get a better understanding of what happened
- decision must be made about which data to collect and the best method for doing so
  - ✓ methods and tools depend on the goals of the investigation and the characteristics of the system
  - ✓ choosing a proper tool is important to avoid corrupt memory images, destroyed evidence, and limited, if any, analysis capabilities

Memory acquisition decision tree



Decisions to make:

- remote or local – do you have physical access to the target system? Is it a server with no keyboard or monitor attached?
- cost – do you have budget restrictions on the acquisition software you can buy?
- file format – does your analysis tool support the file format of the acquisition tool?
- CLI or GUI – do you prefer command-line or graphical user interface tools? A CLI tool might have a smaller footprint, besides you might not have graphical engine running acquisition or runtime
- interrogation – Do you need a full physical memory dump or just the ability to determine the running processes, network connections?

Memory acquisition risks

Before you acquire physical memory, you should always consider the risks

- most OSs do not provide a supported native mechanism for acquiring physical memory
- memory acquisition tools might leave the system instable
- poorly written malware can be unstable and may behave in an unpredictable way
- is the target a mission-critical system that can be shut down or rebooted only in extreme circumstances?

There might be circumstances in which the consequences (i.e., death, environmental damage) of destabilizing a system are never worth the risk.

Memory acquisition risks

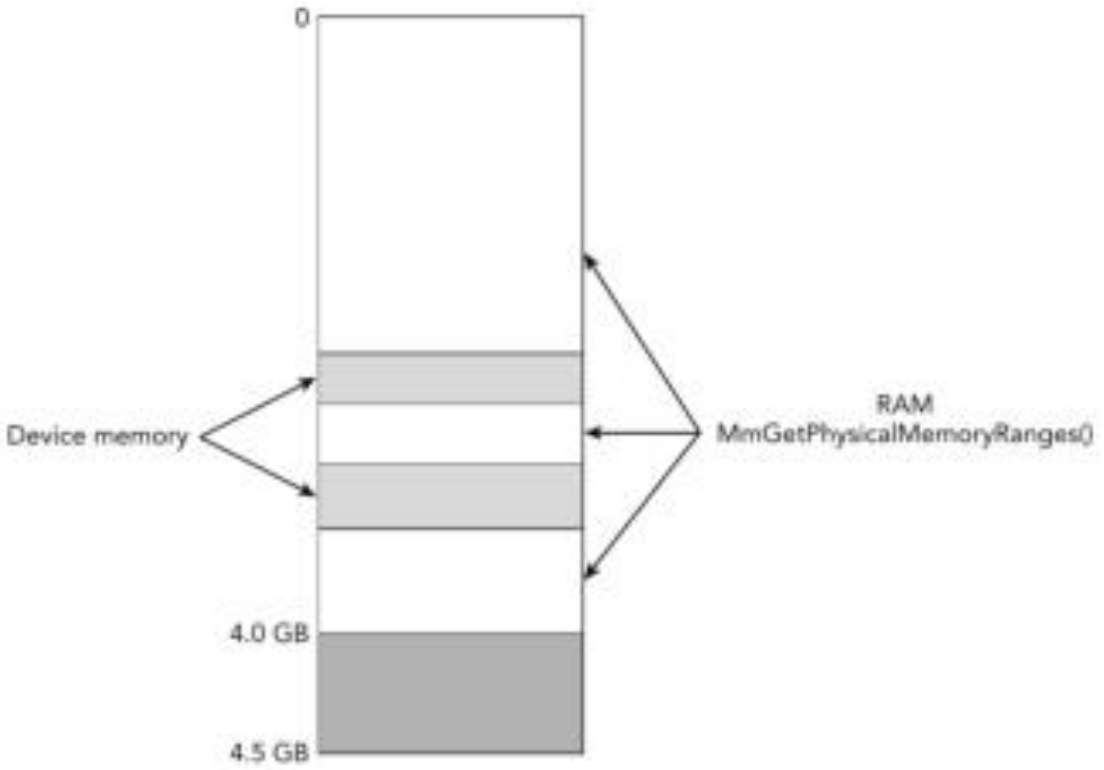
Why memory acquisition can lead to system instabilities and evidence corruption?

- atomicity – memory acquisition is not an atomic operation and the contents of RAM are constantly changing. During acquisition, other processes are writing memory, the kernel is adding/removing linked-list elements, network connections are being initiated or torn down, and so on
- cache coherency – processors were not designed to accommodate the simultaneous mapping of the same physical address with multiple cache attributes (non-cached, cached, write-combined). A poorly written acquisition tool can easily invalidate the very memory being acquired.

Memory acquisition risks

- device memory – there are physical memory regions reserved for use by the firmware, by the ISA or PCI busses, or by various motherboard devices. Reading from one of these regions may alter the state of the device you are accessing.
  - ✓ few tools are able to acquire these regions with reliability and accuracy

Figure: Physical memory layout



When to acquire memory

Choosing the proper time to depends on a number of factors.

List of suggestions:

- plan the acquisition when the suspect is online (or at least logged in), which can give you access to:
  - ✓ the suspect's logon session, information about cloud services or remote storage
  - ✓ and any encrypted documents that the suspect might have been viewing
- avoid the most active periods:
  - ✓ so that the suspect doesn't detect your activity
  - ✓ to minimize the number of anomalies you encounter when you analyze the evidence

How to acquire memory

Local acquisition to removable media:

- never dump memory to the target system's local drives, such as the C: partition
- dumping memory to an external USB, ESATA, or Firewire drive
- the file system of the external drive must support file sizes equal to the amount of RAM (FAT32 has a limit of 4 GB)
- advices:
  - ✓ removable media should be used only on one computer to avoid spreading malware
  - ✓ wipe removable media before using (or re-using) it to acquire evidence
  - ✓ do not plug possibly infected removable media directly into your forensic workstation, inspect it on another computer, then copy the evidence over an isolated network

Runtime interrogation:

- use automated tools that log all the preformed steps

Remote acquisition

- typically, the acquisition tool is pushed over the network to the target system
- the tool can run through a scheduled task or service
- the dump can be stored on a network share (last resort) or via a stream with netcat, but this method has some risks
  - ✓ administrator credentials and the contents of the target system's RAM may be exposed
  - ✓ create a temporary admin account and use an encrypted channel with a tool that supports TLS
  - ✓ configure the firewall to limit the traffic between the target and the remote acquisition system
- the use of compression is recommended

Acquisition tools

Software acquisition tools

All software-based acquisition tools follow a similar method:

- load a kernel module that maps the desired physical addresses into the virtual address space of a process
- access the data from the virtual address space
- write the contents to the requested non-volatile storage
- most tools avoid acquiring device memory regions
  - ✓ the acquisition process is more stable
  - ✓ but might miss important evidence, such as sophisticated rootkits

There are many tools, just to name a few:

- Windows
  - ✓ AccessData FTK Imager (free)
  - ✓ EnCase (comercial)
  - ✓ Winpmem (open source)
- Mac
  - ✓ OSXPmem (open source)
- Linux
  - ✓ LiME - Linux Memory Extractor (open source)
  - ✓ AVML - Acquire Volatile Memory for Linux (free)

There are a few tools, but only some are open source:

- volatility – available for Windows, Mac and Linux
- rekall – fork from volatility

Volatility examples

```
volatility -f memdump.raw imageinfo

volatility -f memdump.raw --profile=WinXPSP3x86 pslist

volatility -f memdump.raw --profile=WinXPSP3x86 consoles

volatility -f memdump.raw --profile=WinXPSP3x86 -p 1564 memdump -D .

volatility -f memdump.raw --profile=WinXPSP3x86 sockets

volatility -f memdump.raw --profile=WinXPSP3x86 connections

# hiberfil.sys is a dump made by the OS in compressed format

# it is necessary to decompress to improve the analysis:

volatility -f hiberfil.sys --profile=WinXPSP3x86 imagecopy -O hiberfil.raw
```

Volatility Command Reference

Windows

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference

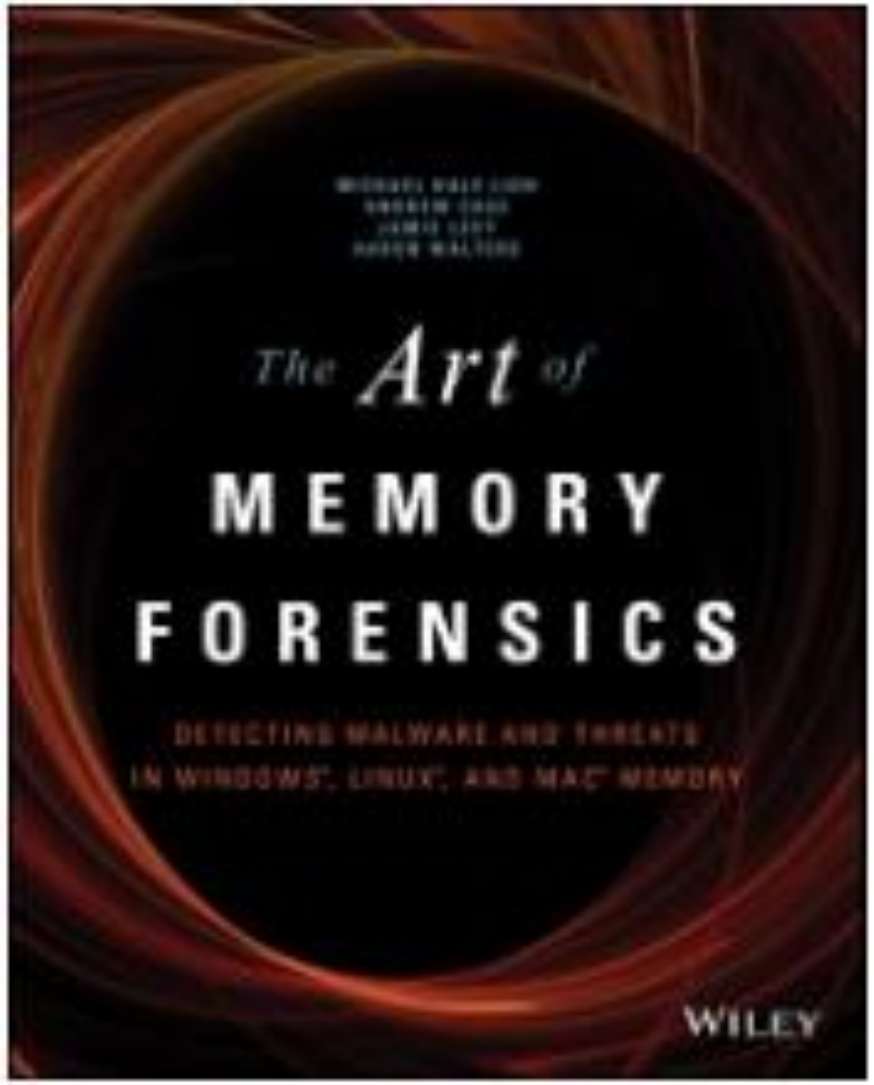
Linux:

https://github.com/volatilityfoundation/volatility/wiki/Linux-Command-Reference

Bibliography

Book

- Title: The Art of Memory Forensics: detecting malware and threats in windows, linux, and Mac memory
- Authors: Ligh, M. H., Case, A., Levy, J., & Walters, A.
- Publisher: John Wiley & Sons
- Date: July 28, 2014
- ISBN: 978-1118825099
- https://www.amazon.com/exec/obidos/ASIN/0321268172/



08-Lab01 – Analysis of a memory dump with Volatility v2.6

QUESTIONS?