Nulltack
Purple team bootcamp

Live Memory Acquisition

Prepared By:
Kazim Ali Obad

Supervisor:
Anmar Mohammed
Mohammed baqer

Contents

1. Why Memory Is Always Captured First

The moment an incident is detected on a Windows machine, the very first action before anything else is to acquire the RAM. This is not optional. It is rule number one in live forensics.

But why? Think about what RAM actually is: it holds temporary data. The second the machine shuts down, reboots, or loses power, everything stored in memory is completely gone. No recovery. No second chance. That data is volatile and that word should stick in your mind.

1.1 Volatility The Core Reason

Unlike a hard drive, which retains data even when the power is off, the RAM loses everything the instant the machine powers down. This is what we call volatile data. Once it is gone, it is gone permanently.

1.2 What Valuable Evidence Lives in RAM?

Here is what you would lose if you skipped the memory capture:

- Running processes every program and service active at the time of the incident.
- Malware running entirely in memory fileless malware, rootkits, and tools that never touch the disk. If it only lives in RAM and you miss it, you missed the attacker.
- Active network connections who the machine was talking to, and on which ports. This can show you a command-and-control server connection right there in real time.
- Encryption keys, passwords, and credentials these are loaded into memory whenever they are in use. If an attacker encrypted files or logged in somewhere, evidence of the keys may still be there.

- Registry hive data loaded in memory parts of the Windows registry that were actively loaded.
- Memory-only artifacts anything the attacker did using fileless techniques.

1.3 Attackers Can Manipulate Memory Too

It is not just about what evidence is there it is also about the fact that an attacker may try to destroy it. Attackers can use memory-only tools like MemCallz and similar utilities to corrupt, overwrite, or clear memory. If you wait too long, the evidence you needed may have already been wiped by the attacker or lost due to a triggered shutdown.

2. Challenges of RAM Acquisition

Capturing RAM sounds straightforward, but there are real technical challenges you need to understand before you run any tool.

2.1 Forensic Footprint (Footprint / Tool Impact)

Every tool you run on the live machine leaves a trace. When you launch a memory acquisition tool, that tool itself uses some RAM. It writes a small amount of data to memory just by running. This is called the forensic footprint or tool impact.

Think of it like walking onto a crime scene the moment you step in, you are leaving footprints. The goal is to leave as few footprints as possible. A good acquisition tool has a small, minimal footprint.

> ***IMPORTANT***
> *Choosing a tool with a small memory footprint is critical.*
> *Every tool that touches memory risks overwriting some of the evidence you are trying to preserve.*
> *This is why tool selection is not trivial it directly affects evidence integrity.*

2.2 Data Overwriting Risk

Related to footprint is the risk of overwriting. Memory works on a push/pop model data is constantly being written and replaced. When you run an acquisition tool, there is a small chance that parts of the memory you most needed may get overwritten by the tool itself, or by other active processes, before they are captured.

This is unavoidable to some extent, but you can minimize it by using fast, lightweight tools.

2.3 User Mode vs. Kernel Mode

On Windows, there are two privilege levels at which software runs:

- ***User Mode:*** This is where regular applications run. User mode tools can only see and access portions of memory that are not hidden or protected by the operating system. Some critical memory regions are simply invisible to user mode.
- ***Kernel Mode:*** This is the privileged level where the Windows kernel itself operates. Kernel mode tools have full access to all of memory, including protected and hidden regions.

Why does this matter for forensics? Because attackers often hide their malware in protected memory regions. A user mode acquisition tool will miss those regions entirely. A kernel mode tool will capture everything.

2.4 Speed of Capture

Memory is dynamic. Data in RAM changes every fraction of a second as the system runs. The longer your acquisition takes, the more the memory state changes during the process. A fast tool captures a more accurate snapshot.

This is another reason to prefer Dumpit over slower alternatives in time-critical situations it is designed to be extremely fast.

3. RAM Acquisition Tools Comparison

There are multiple tools available for live Windows memory acquisition. In this lecture, we focus on two: Dumpit and Belkasoft RAM Capturer. Here is how they compare side by side:

Feature	Dumpit	Belkasoft RAM Capturer
Footprint	0.66 MB extremely small. Leaves minimal trace in memory.	2.1 MB more than double Dumpit's footprint.
Ease of Use	Very easy simple command-line execution.	Very easy simple GUI.
Operating Mode	Kernel Mode full access to all memory regions, including protected and hidden areas.	User Mode cannot see kernel-protected memory regions.
Speed	Very fast designed for rapid acquisition.	Slower takes up to 12 minutes for large RAM.
Output Format	Generates a single image file.	Generates a single image file.
Pause / Resume	Supported you can pause and resume acquisition.	Not supported.
Best Use Case	Preferred for live forensics: fast, minimal footprint, full kernel access, and pause/resume support.	Acceptable when Dumpit is unavailable and machine has no kernel-level threats.

3.1 The FTK Manager Option (User Mode Alternative)

There is a third option: using the FTK Manager in user mode. This is slower and has a larger footprint than Dumpit, but it has one niche use it allows you to use a specific function called WinPmem. FTK in this mode works if you need a user mode fallback and already have it in your toolkit.

The recommendation remains: if you want the best speed and smallest footprint, use Dumpit. If you need to bypass complex protections or want full kernel access, Dumpit in kernel mode is also the answer for that.

4. Before You Begin Critical Storage Rule

Before you even launch an acquisition tool, you need to set up your storage correctly. There is one hard rule:

MANDATORY RULE

- ***NEVER save the memory image to the local hard drive of the machine you are investigating.***
- ***ALWAYS save to an external USB drive.***
- ***The USB drive must have MORE available space than the total RAM of the target machine.***
- ***Example: if the machine has 8 GB of RAM, your USB must have at least 16 GB free.***

4.1 Why External Storage?

There are two reasons for this rule:

1. First: the machine you are investigating is potentially compromised. Writing an evidence file onto a compromised machine contaminates both the machine and the image. The attacker's tools could potentially tamper with the image.
2. Second: this is a live acquisition. You are capturing the machine's current state so you can analyze it elsewhere, off the compromised machine. The whole point is to take the evidence away with you and analyze it on a clean, controlled system.

4.2 Why the USB Must Be Larger Than RAM

The RAM image file will be approximately the same size as the total RAM installed in the machine. If the machine has 8 GB of RAM, the image will be roughly 8 GB. Your USB needs enough headroom to hold the full image plus any other acquisition files or tools you are carrying.

5. Live Memory Acquisition with Dumpit Step by Step

Here is exactly how to perform a live RAM acquisition on a Windows machine using Dumpit. Every step matters.

5.1 Requirements Before You Start

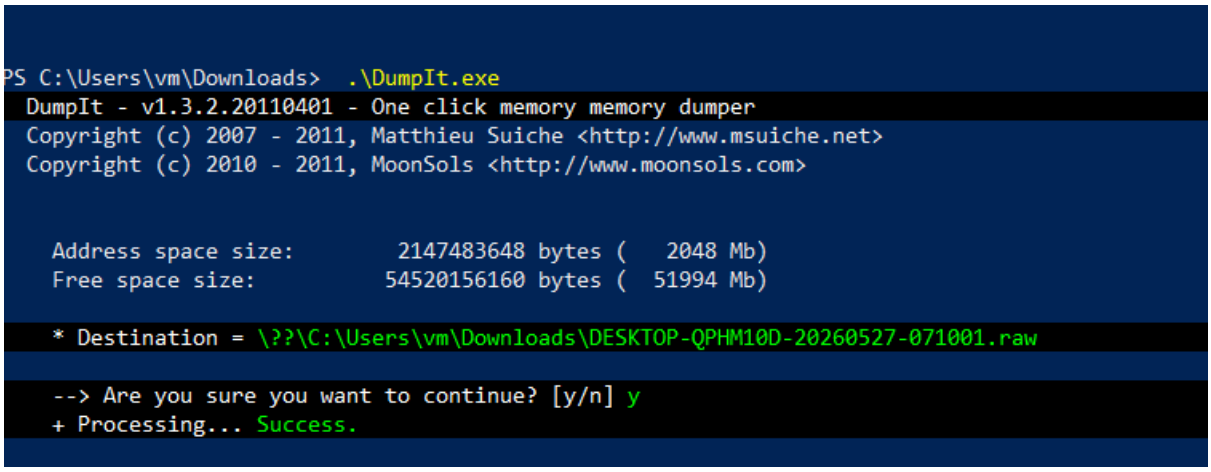
- Dumpit executable (downloaded and placed on your USB drive).
- A USB drive with free space greater than the target machine's RAM.
- Administrator privileges on the target machine.

Note : *You MUST run Dumpit as Administrator. Without administrator (elevated) privileges, Dumpit* ***cannot access kernel memory*** *and the acquisition will fail or be incomplete. Right-click and select 'Run as Administrator', or open an elevated Command Prompt.*

5.2 Running Dumpit

Open an elevated Command Prompt and navigate to the location of Dumpit on your USB drive. Then run:

```
PS C:\Users\vm\Downloads>  .\DumpIt.exe
```



When prompted, type y and press Enter to confirm and begin acquisition.

5.3 Understanding the Dumpit Output

Before the acquisition begins, Dumpit shows you several important pieces of information:

- Address space size the total RAM installed on the machine. This tells you how large your image file will be.
- Free space size the available space in the current directory (your USB). Verify this is larger than your RAM.
- Destination filename the name Dumpit will give the image file. It uses a format based on the machine's hostname and the current date and time. This is your evidence file.

Once you confirm, Dumpit begins the acquisition. The time this takes depends on the amount of RAM. With Dumpit's kernel mode speed, it completes faster than alternatives.

5.4 After Acquisition Always Verify the Image

This step is non-negotiable. After every single acquisition, before you do anything else, verify the integrity of the image you just captured.

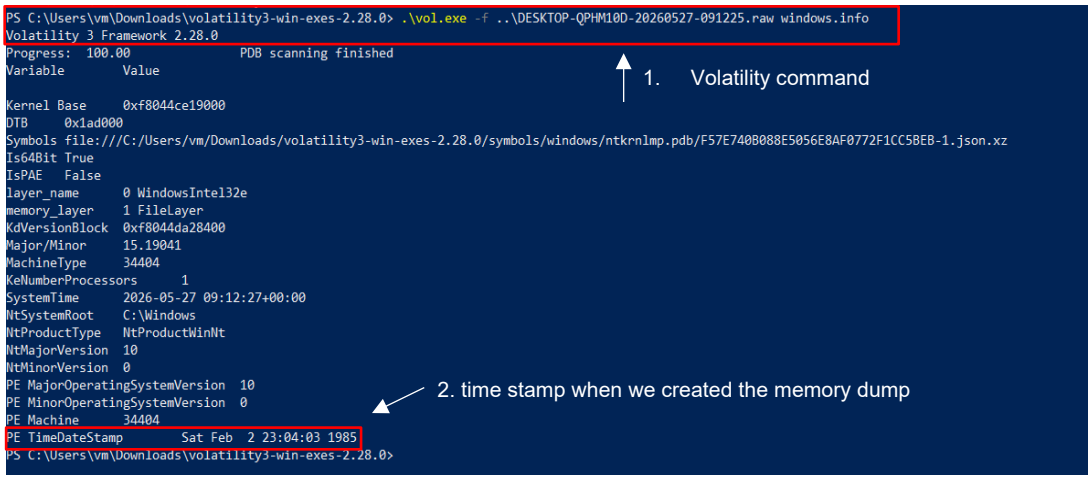
Volatility (the analysis framework) has a built-in command for this called imageinfo. Run it against your captured image:

```
.\vol.exe -f ..\DESKTOP-QPHM10D-20260527-091225.raw windows.info
ERROR   : volatility.debug    : Please specify a location (-l) or filename (-f)
PS C:\Users\vm\Downloads> .\volatility_2.6_win64_standalone.exe -f .\DESKTOP-QPHM10D-20260527-071001.raw imagein
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
```

If the output shows you a valid operating system profile and a correct timestamp, your image is intact. If it returns errors or corruption warnings, the image has been corrupted and you need to capture again.

VERIFICATION RULE

1. A valid image will return: OS profile, architecture, and timestamp matching the acquisition time.
2. If the image is corrupted: re-acquire. Do not attempt analysis on a corrupted image.
3. Record the image hash (MD5 or SHA256) for chain-of-custody documentation.



6. What If the Machine Is Already Off? Special Windows Memory Files

Live acquisition requires the machine to be powered on. But what if you arrive after the machine has already been shut down? All is not lost. Windows keeps special files on disk that contain copies of, or data derived from, RAM. These are not as complete as a live RAM image but they can still yield valuable forensic evidence.

There are three special files to know:

6.1 hiberfil.sys The Hibernation File

Location: C:\hiberfil.sys What it is: When Windows enters hibernation mode (a deep sleep state), it saves the entire contents of RAM to this file on disk. This is so the machine can resume exactly where it left off when powered back on.

Why it matters forensically: This file is essentially a RAM dump from the last hibernation event. If the machine was hibernated during or after the incident, hiberfil.sys may contain a snapshot of memory from that moment including running processes, open connections, and loaded code.

Note *hiberfil.sys = a frozen snapshot of RAM from the last time the system hibernated. Always check if this file exists and copy it to your USB as part of evidence collection. It can be parsed by the same forensic tools (like Volatility) used for live memory images.*

6.2 pagefile.sys The Page File

Location: C:\pagefile.sys

What it is: When the RAM fills up, Windows moves data it does not immediately need from RAM to the pagefile on disk. Think of it as an overflow area for RAM. Data is constantly being swapped between RAM and the pagefile.

Why it matters forensically: The pagefile can contain fragments of data that were in RAM at some point including parts of running programs, loaded DLLs, web browsing data, and more. It may contain pieces of malware code or attacker tools that were paged out.

6.3 memory.dmp / minidump The Crash Dump File

Location: C:\Windows\memory.dmp

Alternate location: C:\Windows\Minidump*.dmp

What it is: When Windows crashes (the infamous Blue Screen of Death, or BSOD), the operating system automatically writes a dump of memory to disk. This is called a memory dump or minidump, depending on the configuration.

When is it created: Only when a BSOD occurs. If the system crashed during or because of the attack, this file may capture exactly what was happening in memory at the moment of the crash.

```
Primary location:  C:\Windows\memory.dmp
Minidump folder:   C:\Windows\Minidump\
```

Note : *memory.dmp is only created when the system BSODs (Blue Screen of Death).If there was no crash, this file will not exist.*

If it does exist after an incident, it may be extremely valuable especially if the attacker's action caused the crash.

6.4 Summary Off-Machine Evidence Collection

If the machine is already off when you arrive, the action plan is:

- Step 1: Go to C:\ and look for hiberfil.sys. Copy it to your USB.
- Step 2: Look for pagefile.sys in C:\. Copy it to your USB.
- Step 3: Check C:\Windows\memory.dmp. If it exists, copy it to your USB.
- Step 4: Check C:\Windows\Minidump\ for any .dmp files. Copy them to your USB.
- Step 5: Bring all copies back to your analysis machine and analyze with Volatility.

Note : *None of these files are as complete as a live RAM capture.*

They are fallback evidence for when live acquisition was not possible.

A live RAM image is always the priority these three files are your backup plan.

8. Summary Key Takeaways

Let us review the most important points from this lecture:

Topic	Key Point
Why RAM first?	Volatile data lost on shutdown. Contains running processes, network connections, passwords, and malware that leaves no disk trace.
Tool of choice	Dumpit kernel mode, smallest footprint (0.66 MB), fastest speed, supports pause/resume.
Storage rule	Always use external USB. USB must have more space than the machine's total RAM.
Privilege required	Administrator / elevated privileges are mandatory for any memory acquisition tool.
Always verify	Run Volatility imageinfo immediately after capture to confirm image integrity.
Machine is off?	Collect hiberfil.sys, pagefile.sys, and memory.dmp as fallback evidence.
Kernel vs User Mode	Kernel mode tools see everything. User mode tools miss protected and hidden memory regions.

INCIDENT RESPONSE MEMORY CHECKLIST

[ ] Incident confirmed do NOT reboot or shut down the machine.

[ ] Plug in USB with Dumpit and sufficient free space.

[ ] Open Command Prompt as Administrator.

[ ] Run Dumpit.exe from the USB drive.

[ ] Confirm acquisition when prompted (y).

[ ] Note the output filename and acquisition timestamp.

[ ] Run Volatility imageinfo to verify image integrity.

[ ] Copy verified image to safe storage for analysis.

[ ] If machine was already off: collect hiberfil.sys, pagefile.sys, memory.dmp.