# Lab – How to Capture RAM Memory from a Windows machine

# Overview

In this lab, you will learn multiple ways to capture the RAM memory from a Windows machine for analysis. A memory dump (also known as a core dump or system dump) is a snapshot capture of computer memory data from a specific instant.

For the hacker, RAM can be treasure trove of data to include encryption keys, passwords, network connections, processes running, and much more.

Capturing RAM can allow an investigator to understand what applications were being used by a suspect or at the time of an attack. high Remote attacker would store data, and tools in RAM rather than on the system. Capturing volatile data in a computer's memory dump enables investigators to do a full memory analysis and access data including:

* browsing history
* encryption keys
* chat messages
* clipboard contents
* run-time system activity
* open network connections (often these artifacts are only found in RAM)
* recently executed commands and processes
* injected code fragments
* memory stored before shutdown or crash

Crucial information related to Malware behavior, Dark Web sessions, anti-forensics software usage, passwords, clipboard stored data and social media chat information is obtained from volatile memory acquisition.

Different situations may require the use of differ methods for acquiring a memory dump. In this lesson you will some these methods.

**The steps for acquisition are as follows:**

1. Determine the state of the machine.
2. Identify the operating system.
3. Check for authentic device access.
4. Insert acquisition media.
5. Perform Volatile Memory Dump
6. Collect SWAP, PAGEFILE.sys and system protected files.
7. Hash and verify the acquired files.
8. Create Investigator copies