Memory Forensics Tool Usage Guide

## 1. Overview

Memory forensics is a critical component in incident response, enabling analysts to investigate volatile system artifacts like running processes, network connections, loaded drivers, and potential malware in RAM. This document provides instructions on how to use Magnet RAM Capture to acquire memory and Hex Workshop to analyze it manually.

## 2. Magnet RAM Capture

### Purpose

Magnet RAM Capture is a free, lightweight tool developed by Magnet Forensics to acquire physical memory (RAM) from Windows systems.

### Usage Instructions

**Step 1:** **Download & Prepare**

* Download from: <https://www.magnetforensics.com/resources/magnet-ram-capture/>
* Place it on an external drive or separate directory.

**Step 2:** **Execute with Admin Rights**

* Right-click and select 'Run as Administrator'.

**Step 3: Select Output Directory**

* Choose a safe destination (preferably not on the system drive).

**Step 4: Capture RAM**

* Click 'Capture'.  
  Wait for the progress bar to complete. The result is a .raw memory image.

**Step 5: Validate (Optional)**

* Use hashing tools (e.g., md5sum, sha256sum) to validate image integrity.

## 3. Hex Workshop

### Purpose

Hex Workshop is a powerful hex editor that allows for low-level inspection of memory dumps, offering features like searching, bookmarking, and structure decoding.

### Usage Instructions

**Step 1: Download & Install**

* Download from: <http://www.hexworkshop.com/>
* Install the application.

**Step 2: Open Memory Dump**

* Go to File → Open, then select the .raw file from Magnet RAM Capture.

**Step 3: Analyze Contents**

* Use Ctrl+F or Search → Find to locate:  
  - Strings like cmd.exe, powershell, http, or suspicious domains.  
  - Hex patterns or opcodes indicating shellcode.

**Step 4: Navigate & Bookmark**

* Use Ctrl+G to go to specific offsets.
* Right-click to add bookmarks and notes for suspicious regions.

**Step 5: Structure Viewer**

* View structured data using the built-in or custom structure templates (e.g., PE headers).
* Helps in identifying injected modules or executable artifacts.

## 4. Example Workflow

1. Incident Detected: Suspect system compromise.
2. RAM Acquisition: Use Magnet RAM Capture to generate a .raw memory image.
3. Initial Review: Open the image in Hex Workshop to:  
    - Search for malicious strings or known C2 indicators.  
    - Bookmark regions containing suspicious binaries or process traces.

## 5. References

* Magnet RAM Capture: https://www.magnetforensics.com/resources/magnet-ram-capture/
* Hex Workshop: http://www.hexworkshop.com