

DIGITAL FORENSIC PROJECT



DISCLAIMER



This document does not promote or encourage any illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.



MEMORY FORENSIC & ANALYSIS

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

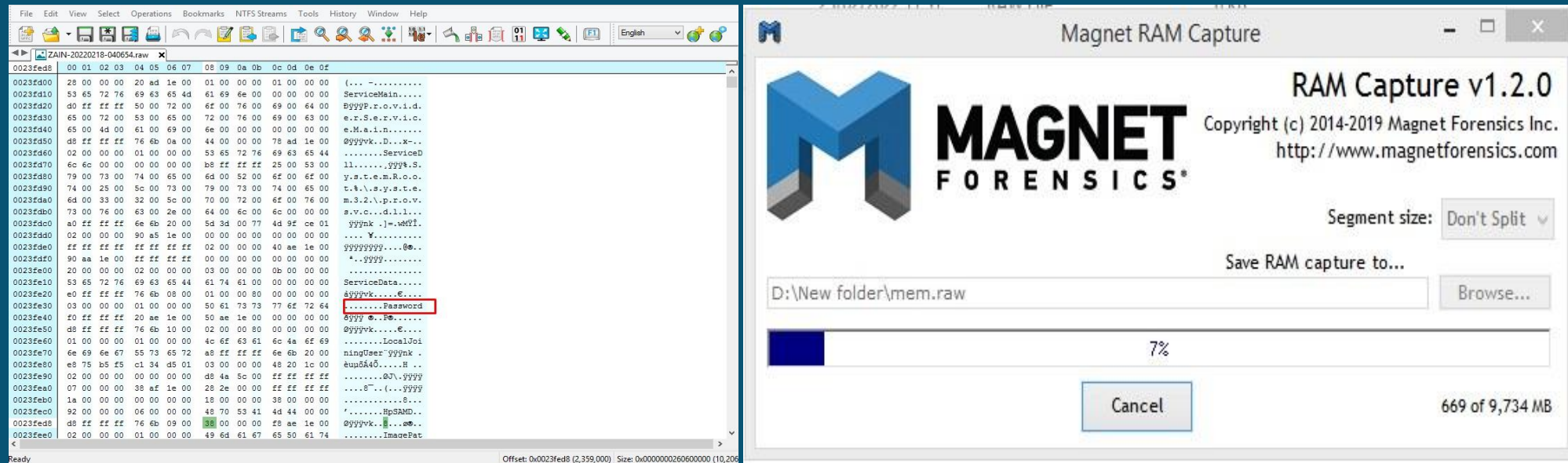


MEMORY FORENSIC & ANALYSIS

Project Name: Memory Forensic & Analysis.

Tool Used: Magnet RAM v1.2, Dump IT, Redline v2.0, Magnet AXIOM v4.10, Hexeditor

Platform: Windows



Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

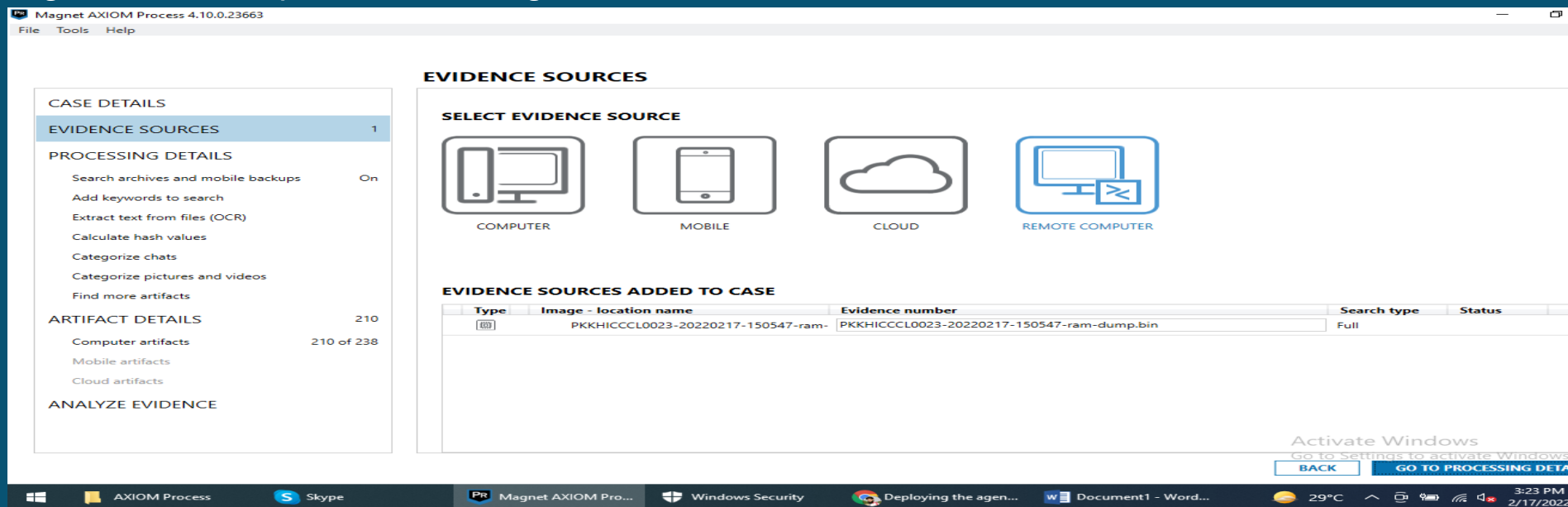


MEMORY FORENSIC & ANALYSIS

DESCRIPTION :

Memory forensics is forensic analysis of a computer's memory dump. Its primary application is investigation of advanced computer attacks which are stealthy enough to avoid leaving data on the computer's hard drive. Consequently, the memory must be analyzed for forensic information.

We follow following steps which include Acquisition of memory, Analyzing the acquired data, Recovering the evidence for which we use tools like Magnet RAM v1.2, Dump IT, Redline v2.0, Magnet AXIOM v4.10, Hexeditor.



The screenshot displays the Magnet AXIOM Process 4.10.0.23663 interface. The main window is titled "EVIDENCE SOURCES" and features a "SELECT EVIDENCE SOURCE" section with four icons: COMPUTER, MOBILE, CLOUD, and REMOTE COMPUTER. Below this, the "EVIDENCE SOURCES ADDED TO CASE" section shows a table with the following data:

Type	Image - location name	Evidence number	Search type	Status
[Icon]	PKKHICCCCL0023-20220217-150547-ram-	PKKHICCCCL0023-20220217-150547-ram-dump.bin	Full	

On the left side, the "CASE DETAILS" panel shows "EVIDENCE SOURCES" with a count of 1. The "PROCESSING DETAILS" section includes options like "Search archives and mobile backups" (On), "Add keywords to search", "Extract text from files (OCR)", "Calculate hash values", "Categorize chats", and "Categorize pictures and videos". The "ARTIFACT DETAILS" section shows a total of 210 artifacts, with "Computer artifacts" at 210 of 238. The "ANALYZE EVIDENCE" section is also visible.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.



MEMORY FORENSIC & ANALYSIS



The screenshot displays the Magnet AXIOM software interface, which is used for memory forensics. It is divided into two main panels: 'EVIDENCE SOURCES' and 'ANALYZE EVIDENCE'.

EVIDENCE SOURCES Panel:

- REMOTE COMPUTER:** Shows details for a remote computer named 'PKKHCCCL0023' with user 'Uzair' and local endpoint '192.168.8.107'. The status is 'Connected'.
- SELECT ITEMS TO DOWNLOAD:** A section with a 'STOP AND DELETE AGENT' button.
- REVIEW AND SELECT THE DATA FROM THE TARGET COMPUTER:** A section with instructions to review files and folders. It includes three icons for 'TARGETED LOCATIONS', 'FILES AND DRIVES', and 'MEMORY'.
- ITEMS TO DOWNLOAD:** A section indicating that selected items will be saved to an AFF4-L container.

ANALYZE EVIDENCE Panel:

- SOURCES TO PROCESS:** A table showing the evidence source being processed.

Type	Image - location name	Evidence number	Search type	Start time	End time
	PKKHCCCL0023-20220217-150547-ram-dump.bin	PKKHCCCL0023-20220217-150	Full	2/17/2022 3:29:03 PM	

- SEARCH IN PROGRESS:** Shows 'Time Elapsed: 1:01'.
- CURRENT SEARCH LOCATION:** Shows the current search location as 'Win10x64' with a progress indicator at 24%.
- Search Definitions:** Lists search definitions such as 'Carving memory dump file' and 'Running Volatility on memory dump file'.
- Thread Details:** A section for viewing thread details.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

