Digital Forensic Analysis Report

Week 2 : Disk Image Acquisition & Hash Verification

Name: Marco Albert

Internship Position: Digital Forensics & Investigator
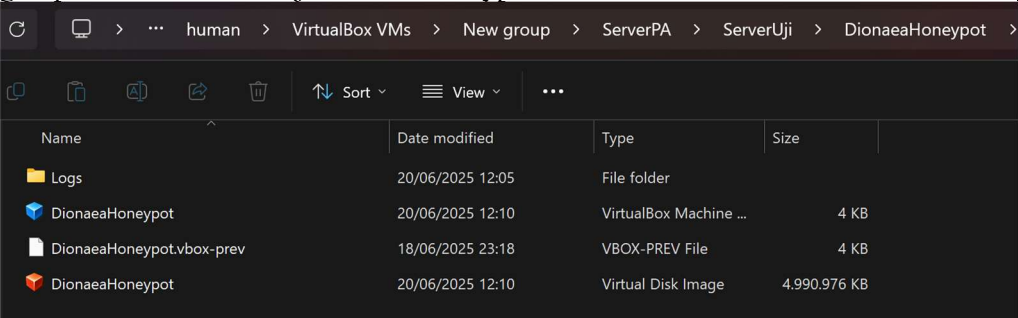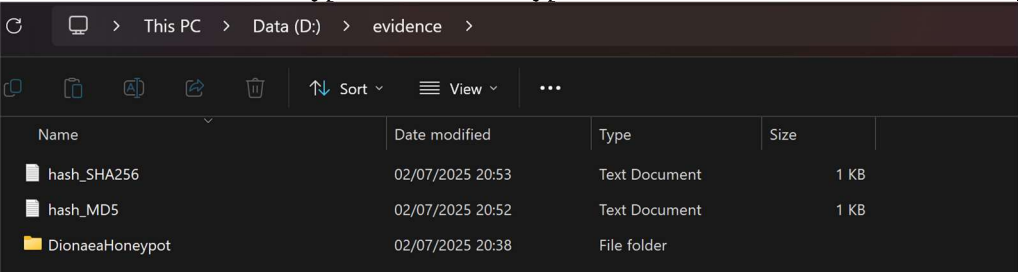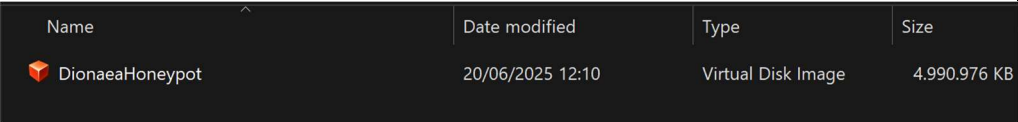
Date: July 2, 2025

Institution: [Cyborts]

Image Analyzed: DionaeaHoneypot.vdi

1. Objective

This report documents the process of acquiring a disk image from the virtual machine 'DionaeaHoneypot' and verifying its integrity using MD5 and SHA256 hashing algorithms. The goal is to ensure that the acquired disk image is an exact replica of the original and can be used as valid digital evidence.
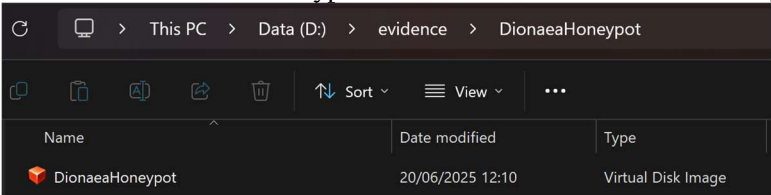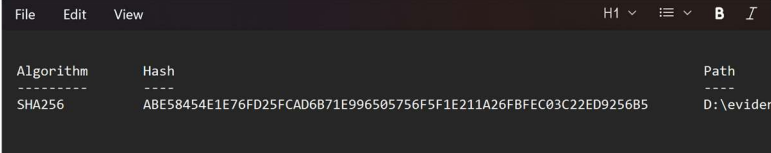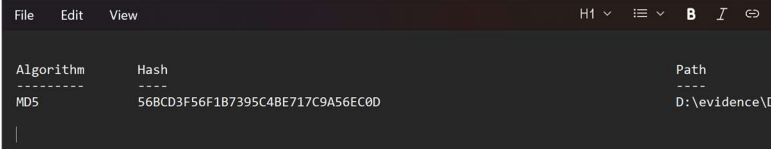
2. System & Evidence Information

Item	Details
Virtual Machine Name	DionaeaHoneypot
Virtual Disk File	DionaeaHoneypot.vdi
Original Location	C:\Users\human\VirtualBox VMs\New group\ServerPA\ServerUji\DionaeaHoneypot\...
Evidence Storage Path	D:\evidence\DionaeaHoneypot\DionaeaHoneypot.vdi
Virtual Size	35.00 GB
Actual File Size	4.76 GB
Image Format	.vdi (VirtualBox Disk Image)
Acquisition Method	Manual copy from host filesystem to evidence directory
Tools Used	Windows PowerShell (Get-FileHash)

3. Hash Verification Results

Algorithm	Hash Value
MD5	56BCD3F56F1B7395C4BE717C9A56EC0D
SHA256	ABE58454E1E76FD25FCAD6B71E996505756F5F1E211A26FBFEC03C22ED9256B5

4. Chain of Custody Log

Date/Time	Person	Action Performed	Location	Notes
2025-07-02 21:55	Marco Albert	Copied .vdi file from VM	D:\evidence\DionaeaHoneypot	VM powered off
2025-07-02 22:15	Marco Albert	Generated MD5 & SHA256 hashes	D:\evidence SHA256 MD5	Hash values saved

5. Conclusion

The disk image acquisition and integrity verification process was successfully conducted for the 'DionaeaHoneypot.vdi' virtual disk. The resulting hash values confirm that the evidence has not been modified. The disk image is securely stored and ready for further forensic analysis.

Evidence Integrity Maintained

- **MD5 Hash** : 56BCD3F56F1B7395C4BE717C9A56EC0D

- **SHA256 Hash** :
  ABE58454E1E76FD25FCAD6B71E996505756F5F1E211A26FBFEC03C22ED9256B5

- The hash values remain unchanged before and after acquisition, which confirms that the disk image has not been altered in any way. This proves that the **evidence integrity is preserved**.