Digital Forensic Analysis using HELIX and Autopsy

Lab

By: Randall Lewis

SCENARIO

Late yesterday evening a suspected member of organized crime was arrested for racketeering, money laundering, and potential cyber crimes. As part of the seizure, a computer tower was found in the suspect’s residence. The tower was in a powered down state. It was seized and imaged by first responders using dcfldd via Adepto on the Helix platform.

Items Provided:
1. Case Information – Request for Analysis
2. Digital Evidence – Drive Image of Suspect’s Computer Tower Hard Drive

Task: Complete a full dead-box forensic analysis of the seized suspect media.

1. Screenshot of the Device info

![Screenshot of Device info](image)

2. This is the Screenshot of the imaging in Progress

![Screenshot of imaging in progress](image)
3. This is the Screenshot of the Verification Success
4. This is the screenshot of the Chain of Custody with Hash Values

5. This is the screenshot of creating a Chain of Custody PDF.
B. Log of Forensics Analysis

- First selected a resolution of 1024 * 768
- I selected the source drive of SDA
- Device info: VMware
  Model: Virtual disk
  Size 279 MB
  Sectors: 545259
  System Bus: scsi@2:0.0:0
- Acquired the information using source device SDA
- Mount Point was /media/sda1
- Type DCFLDD: Hash MD5 Segment:1024
- I then opened up the terminal and mounted the command:
  `sudo mount -t ntfs-3g -o rw /dev/sdb1 /media/sdb1`
- Opened up destination drive in Acquire folder and I wrote in the “Mount Point”:
  `/media/sdbe`
- Clicked start and the imaging process began
- Image was acquired and verification process stated:
  “VERIFICATION SUCCESSFUL”
- Clicked and Viewed Chain of Custody and then created a PDF
- Collected on 10/3/2013 at 10:18am

Report

Client,
I have completed the lab for the forensic imaging and i will explain the steps that I took to come to the conclusion.

The first steps that was taken was to get a screenshot of the device and the type of information and data it was holding. I accomplished this by first selecting the appropriate screen resolution of 1024*768. I then clicked on the DEVICE menu tab and I selected the source drive of SDA and not SDA1. The device information was then verified to be:
Size: 279MB
Sectors: 545259
System Bus: scsi@2:0.0.0
I then took a screenshot of the device which can be viewed containing the information.

The second part of this process was to start the imaging process and get a screenshot if this in progress. This was accomplished first by opening up the Terminal and typing in a command:
sudo mount -t ntfs-3g -o rw /dev/sdb1 /media/sdb1. And this command makes the the other drive, sdb1 available. I then chose that folder and then completed the acquisition of information.
The information was as followed:
a. Source Information
i. Image Name Text Field Type: lab1_CSEC650.dd
ii. Image Notes Text Field Type: Randall
b. Options
i. Type: DCFLDD
ii. Hash: MD5
iii. Segment (MB): 1024
After clicking the START button the imaging process was then started and a screenshot was taken to show this in progress.

The third part of this imaging process was to have the imaging process and the verification of the image to be successful. This was accomplished by letting the process continue. This verification process went through and was verified by the words posted on the bottom of the box in Blue saying: "VERIFY SUCCESSFUL". This was completed on 10/3/2013 at 10:18am.

The fourth part of this imaging process was to show the Chain of Custody with the Hash Value. This was completed by clicking on the CHAIN OF CUSTODY tab in the menu. The information that was present in the tab was the:
Description: Randall
Model: Virtual Disk
Manufacturer: VMware
Date/time:10/3/2013
Created by: Lab1_csec65
Method:dcfldd
Image: Lab1_csec650.dd
Hash: Total(md5): f71625daed269ba7145a6e6b27fcb89a
Sequence: 1
We can see that all the information that was displayed and the most important is the Hash from MD5. This information will be matched against the hard drive to make sure that data
integrity is maintained. This can be seen in the screenshot that was taken of the box showing the information.

Finally a PDF of the Chain of Custody was created. This was done by simply clicking on the “Create a PDF” button and I saved it in the media file. The overall imaging process was completed successfully and the information along with the screenshots are available. I learned how to create and image file and what kind of information is processed. I learned about Helix and how important it is to Forensics. I also learned that data imaging can be done with software and with hardware.

Sincerely,
Randall Lewis