CIS/ECE 387 Fall 2018 Lab2

Assigned: 9/24/2018
Due: **10/3/2018**

ACTIVITY 1: USING DD TO COPY AND COMPARE FILES

SOFTWARE

If you are not using a Linux machine, you'll need to download SIFT Workstation 3 for this exercise.

USB DRIVE

For this activity, you will need a USB drive with at least three files of any format on it. You can use any size drive, but using one that is one GB or less will keep the imaging process from being too long.

GOAL

After capturing volatile system information, the next step is to acquire nonvolatile data on the suspect machine. In this activity, we will use the Linux dd utility and several of its options to copy a file, image a drive, and also use hashes to check the integrity of the copies.

INSTRUCTIONS

1. Launch SIFT Workstation 3 and open a terminal.
2. Use the command *dd* to copy an existing file on your computer. Name the new file *copy.dd*.
3. Using *md5sum*, create MD5 hashes of the original file and the copy.
4. Compare the hash of the copy to the hash of the original file; confirm that the hashes are the same.
5. Repeat Steps 3 and 4 using *shasum* to generate SHA1 hashes.
6. Use dd to copy one block of zero from */dev/zero* to a file called *zero.dd*.
   (Hint: use the dd option count).
7. Insert the USB drive and connect your USB to SIFT Workstation 3. The USB drive should auto-mount. (NOTE: In a real investigation, you should use a write blocker to prevent the SIFT Workstation from modifying the USB drive.)
8. Run the command *mount* to find the USB device file name. You will use the device file name in command dd to make a full image of your USB.
   For example, my USB's device file is */dev/sdb*; it is mounted on */media/sansforensics/DISK_IMG*.
   (Hint: using "lsblk" or "sudo fdisk -l" command to find it out)

9. Use dd to make a full image of your USB flash drive. Name the image *usb.dd*.
   (Hint: *dd if=/dev/sdb of=usb.dd*)

10. Create both MD5 and SHA1 hashes of the USB flash.
    (Hint: *md5sum /dev/sdb; shasum /dev/sdb*)

11. Create both MD5 and SHA1 hashes of the USB image.
    (Hint: *md5sum usb.dd; shasum usb.dd*)

12. Make sure that:
    The md5 hash of the USB flash matches with the md5 hash of the USB image
    The sha1 hash of the USB flash matches with the sha1 hash of the USB image.

ACTIVITY 2: IMAGING WITH NETCAT OVER A NETWORK

GOAL

In this activity, we will explore how netcat (nc) can be used for receiving data over a network.

Sometimes, investigators will capture data from a suspect machine and send data to another networked computer (a forensic machine). In this activity, you will mimic this process by sending the capture data from one terminal to another terminal on the same machine.

INSTRUCTIONS

1. Launch SIFT Workstation 3.

2. Open two terminals on SIFT Workstation 3. One terminal represents a forensic machine; the other represents the suspect machine.

3. On the forensic machine terminal, use *nc –l* to listen on port 8888 for the incoming data. Save the received data as ncData.dd.
   (Hint: *nc –l 8888 > ncData.dd*)

4. On the suspect machine terminal, use dd to copy an existing file and pipe (|) to netcat (nc), sending the copy of the file to the forensic machine terminal.
   Since we are sending data to the same machine, we use local host's IP address 127.0.0.1. If you send data to a networked machine, replace 127.0.0.1 with the receiving machine's IP address.
   (Hint: In our case, we run *dd if=the-original-file | nc 127.0.0.1 8888*)

5. Generate MD5 and SHA1 hashes of *ncData.dd* and compare them with the original file's MD5 and SHA1 hashes.

Report

Your report should include the activity log (the main steps you take or the commands you run) with some screenshots and/or outputs and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab2” assignment folder. Each group just submits one report.