CIS 8630

Business Computer Forensics and Incident Response

Lab Protocol 03: Acquisition

Purpose: Ensure every student has experienced imaging digital storage media, hashing digital media, transferring digital media and verification of hash values using forensically proper techniques.

Materials required: Lab03 usb thumbstick (a flash drive)

Deliverable: Lab notes from individual students, Evidence Custody Record and Evidence from Teams. Be sure your names and team name is on the material delivered.

Part 1 Preparation

1. Use clean notepaper, note time, date, location, who is present, instructions received (and from whom).
2. Write protect the thumbstick (move switch away from connector). Note this.
3. Prepare an Evidence Custody Record (attached)
4. Download the imaging tools from:
   http://cis.gsu.edu/rbaskerville/cis8630/labs/SimpleWinImageTools.zip
5. Unzip the files to
   C:\dayspace\tools
6. Download the HxD disk editing tools from:
   http://cis.gsu.edu/rbaskerville/cis8630/labs/HxDen.zip
7. Unzip the files to
   C:\dayspace\tools

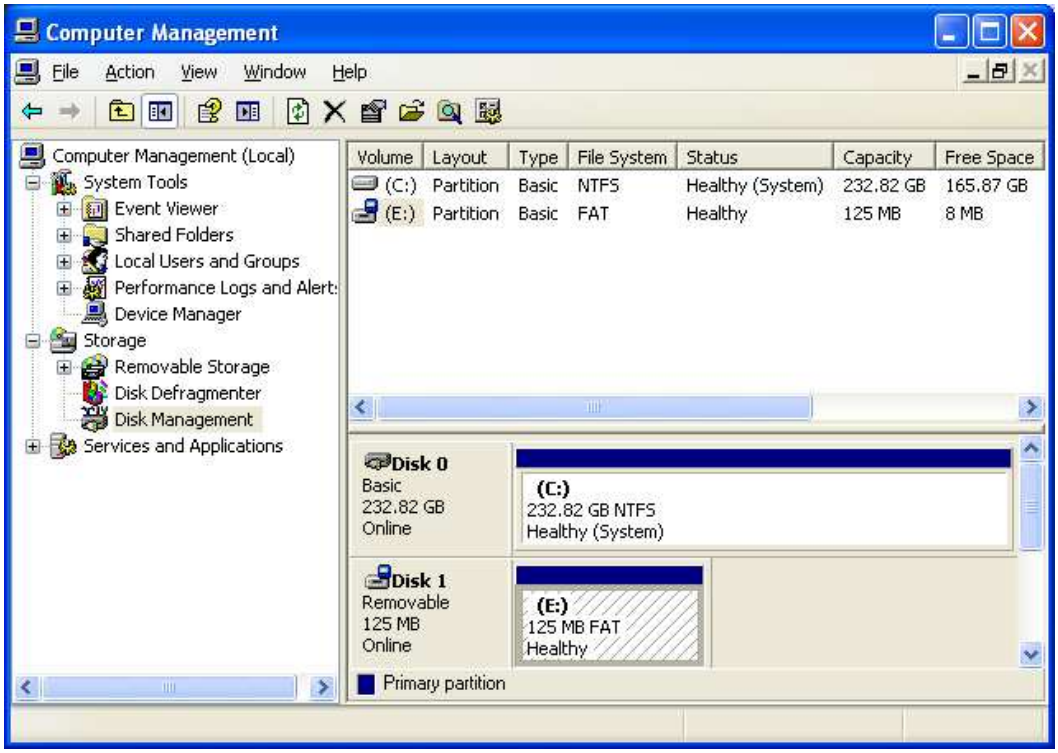
Part 2 Creating an Image and Hash Value

1. Write-protect your usb thumbstick.
2. Insert your usb thumbstick into your workstation.
3. Run HxD in the directory C:\dayspace\tools
4. If asked, click "OK" to dismiss the "First start of HxD" dialog box
5. Select "Open Disk" from the "Extras" pull-down menu.
   Choose "Removable Disk 1" under "Physical Disks"
   N.B. If you have other thumbsticks or removable disks already mounted, the removable disk number could be higher (2, 3, etc.)
6. Select "Checksums" from the "Analysis" pull-down menu.
7. Choose MD-5 and press OK. The light on the thumbstick will flicker when accessed.
8. The MD-5 hash appears in the checksum results pane at the bottom. The expected value is
   141927EA3C104EF0F25EE6053D390A82
9. Choose "Close" from the "File" pull-down menu.

10. Open a command prompt by selecting Start and Run, type "cmd" and press "OK"
NB: If you are using a Windows 7 system you will need to open cmd in Administrator mode. Do the following:
    i. *Click Start | All Programs | Accessories*
    ii. *Hold the shift key down and right click on Command Prompt*
    iii. *Choose "Run as Administrator"*
11. Change default directories by entering the command:

    cd c:\dayspace\tools

12. To determine the disk number of your usb thumbstick perform the following:
    a. Right click on the My Computer icon and choose Manage
    b. In the left hand pane expand Storage and Disk Manager
    c. The number is displayed next to the drive entry in the right hand pane (note the Disk 1 entry for this example)



13. Image the thumbstick by keying the command:

    dd if=\\?\Device\Harddisk1\Partition0 of=c:\dayspace\lab3.img bs=512k --size --progress

    N.B. Harddisk0 is your c: drive. If you have more than one hard drive, other thumbsticks or removable disks already mounted, the removable disk number could be higher (Harddisk2, 3, etc.) as noted in step 12. The light on the thumb drive will flicker when it is being accessed (imaged).

14. Return to HxD. Select “Open Disk Image” from the “Extras” pull-down menu.
    Choose the file lab3.img
15. Select “Checksums” from the “Analysis” pull-down menu.
16. Choose MD-5 and press OK.
17. The MD-5 hash appears in the checksum results pane at the bottom. The expected value is the same
    141927EA3C104EF0F25EE6053D390A82
18. Choose “Close” from the “File” pull-down menu.
19. Prior to removing and storing the thumbstick (the physical evidence), verify that the MD-5 hash is unchanged by the imaging process. Select “Open Disk” from the “Extras” pull-down menu.
    Choose “Removable Disk 1” under “Physical Disks”
20. Select “Checksums” from the “Analysis” pull-down menu.
21. Choose MD-5 and press OK.
22. The MD-5 hash appears in the checksum results pane at the bottom. The expected value is
    141927EA3C104EF0F25EE6053D390A82
23. You can cross-verify the MD-5 Hash using a second tool if you wish. Return to the command prompt. Calculate the MD5 hash of the image by entering:

    md5deep.exe c:\dayspace\lab3.img

24. The expected value of this MD5 Hash is
    141927ea3c104ef0f25ee6053d390a82
25. Ensure your notes are accurate and include dates/times as appropriate, complete the custody form, bag the evidence, keep it secure.

Part 3 Transfer the image to your VMware workstation

1. Ensure your notes are accurate and include dates/times as appropriate, complete the custody form, bag the evidence, keep it secure.
2. Open Microsoft Remote Desktop.

   Start > Run > “mstsc” > “OK”

3. On the Remote Desktop Connection window, select “Options”
4. Click the “Local Resources” tab and select the “Disk drives” check box

5. Click “Connect” to log in.
6. Type in CIS4000-userX.cis.gsu.edu [where X is the number of your VM]
7. Enter username and password
8. Copy the image from your local workstation to the Desktop of your virtual machine (this may take a while depending on your Internet connection speed)
9. Ensure your notes are accurate and include dates/times as appropriate

Part 4 Verify the Image Hash

1. Using Parts 1 and 2 as guides, download the md5deep.exe program to your virtual machine.
2. Calculate the MD5 hash of the image on the virtual machine
3. The expected value of this MD5 Hash is **141927ea3c104ef0f25ee6053d390a82**
4. Ensure your notes are accurate and include dates/times as appropriate

Evidence Custody Record			
Case No		Unit No:	
Investigator(s)			
Name of Case			
Evidence obtained from			
Item #	Description	Vendor	Model #/Serial#
Date/Time	Processed By	Disposition	