CET4860

Assignment 1

Creating a Forensic Duplicate and Verifying Integrity with a Cryptographic One-Way Hash

What you will need

- USB flash drive at least 1GB in size
    - You will overwrite this drive entirely so backup any content you don't want to lose
- Forensic Report Template
- Forensic Notes Template
- Linux VM

Deliverables

A zipped file, firstName.lastName.1.zip, containing:

- Your Report
    - firstName.lastName.Report.1.pdf
- Your Notes
    - FirstName.lastName.Notes.1.pdf
- Your Linux .bash_history file **after** completing the assignment
    - Hidden file located at ~/.bash_history
    - Close your terminal window then re-open it before copying the file

Getting Started

Download 4860.sp23.a1.zip. The SHA1 hash should be:

afc21003c82e4688189d8351fd43a84c0e4430bf 4860.sp23.a1.zip

If you don't receive this hash, something went wrong and you should download the file again. The 135KB zip file is a compressed 125MB disk image 35e6017ac06747d21af9c696d641838166a5ebfa 4860.sp23.a1.dd

If you do not receive that SHA1 hash, something went wrong and you should extract the file again.

Setting Up

Disable Automount in Mint

In Mint 20, start with your flash drive not inserted then:

1. Open Disks by going to Menu > Preferences > Disks
2. Insert Flash Drive
3. Your drive should appear in the list to the left
    a. If not, go to VM > Removeable Devices > Your USB > Connect (Disconnect From Host)
4. Select your USB from the left
5. If your USB has multiple volumes, just select the first, then the icon of two gears below, and then Edit Mount Options
6. You may or may not need to turn off User Session Defaults at the top before proceeding to 7
7. Turn Automatic Mount Options to Off
8. In the unlabeled box **above** Mount Point, replace everything with: nosuid,nodev,nofail,noauto
    a. "noauto" is the important bit; the rest is good housekeeping
9. Click OK

Disable USB Write Access in Windows (If you're using Windows)

In your Windows Host (not inside the VM):

1. Use Window Key + R to open the Run prompt
2. Type “gpedit.msc” without the quotation marks and hit Enter
3. You should now see the Local Group Policy Editor
4. In the left pane, under Local Computer Policy, navigate to the location the below location:
    a. Computer Configuration > Administrative Templates > System > Removable Storage Access
5. Once working in Removable Storage Access, verify the below is present in the right pane:
    a. Removable Disks: Deny Write access
6. If Removable Disks: Deny Write access is present, leave this window open for use later
7. Return to your VM

Zero Out the Media

To provide a clean slate which to put our image on, we're going to overwrite the content with zeroes

1. Verify your devices designation with sudo fdisk -l
    a. If you're unsure, run fdisk without the drive attached and then again after attaching
2. Run: sudo dd if=/dev/zero of=/dev/sdb bs=10000000 status=progress
    a. Replace /dev/sdb with the device designation of your drive
    b. You did make a snapshot of your VM just in case, right? Right!
3. Wait

4. You should see a real-time status of the amount of data which has been written
5. Keep Waiting until the amount written reaches the size of your USB drive
6. Once finished (dd will stop on its own and bring your back to the terminal prompt), remove the USB drive and reinsert
7. Run fdisk again
    a. You should see a device with no partitions now

Let's quickly breakdown that dd command

dd: Reads and writes bytes from a source to a destination

if: Input File or source from where to read

/dev/zero: the Oprah of zeroes. If you want a zero, /dev/zero has all your zero needs

of: Output File or destination for where to write

/dev/sdb: Our destination. In this case, the USB device as a whole; yours may be labelled differently

bs: Block Size which defines the size of the chunks of data to be read and wrote at a time

10000000: Really big chunks (10,000,000 bytes)

status=progress: Displays a real time update each after each block is written

Transferring the Disk Image

Now we're ready to place the assignment image on to the flash drive. We're about to overwrite 1GB worth of the destination drive, which should be zeroes, but if the wrong drive is selected, it will overwrite that just the same. You made a snapshot of your VM just in case, right? Good!

```
sudo dd if=4860.sp23.a1.dd of=/dev/sdb bs=102400
```

You may want to grab a coffee; this will take a few minutes. Once dd has finished, STOP

Do not do anything – don't even look at the USB wrong because it will know. It always knows.

Enable USB Write Protection

1. Return to the Local Group Policy Editor in Windows
2. Double-Click Removable Disks: Deny Write access
3. Select the "Enabled" radio button
4. Click the "Apply" button then the "OK" button

5. Verify the State column for Removable Disks: Deny Write access has changed to “Enabled”
6. Return to your VM

IMPORTANT: While this feature is enabled, you will not be able to write to any USB device inserted. If you need to re-run the zero out procedure on your USB, you will need to change this state to “Disabled”. Once you’re completely finished with the assignment, set the state back to “Not Configured”.

Once back inside your VM, physically remove and re-insert the USB drive, and make sure that the VM has control of the USB.

Run “fdisk -l” and verify that there is now a partition associated with your device such as an sdb1 if your device was sdb, an sdc1 if your device was labelled sdc, etc.

Verifying Integrity

Let's first make sure that the USB drive wasn't automatically mounted when it was reinserted. Just type 'mount' and hit Enter. If you don't see your device listed near the bottom, e.g., /dev/sdb1, fantastic; if you do see you device, hopefully the USB write deny has protected us, run

```
sudo umount /dev/sdb1 (Replace with your device partition if necessary)
```

Now let's verify nothing was changed in the process. Your target value is:

```
6bbbccf862c0ad5a31a919abab58dfa7a7696754  /dev/sdb1
```

Run:

```
sudo sha1sum /dev/sdb1
```

If your result matches, you're ready to go. If not, something has changed along the way. Do not pass Go and do not collect $200. Start with zeroing out the drive again and repeat the process. To do this, you will first need to return to the Local Group Policy Editor in Windows and change Removable Disks: Deny Write access to Disabled. Make sure to re-enable this at the appropriate step.

During this repeat, at the step of zeroing out your USB, use this modified command:

```
sudo dd if=/dev/zero of=/dev/sdb bs=1024000 count=30 status=progress
```

This command will zero out the partition table, created partition, and a bit of space after the partition just to be sure. Specifically, what this does is set a blocksize of 1024000 bytes (roughly 1MB) and tells dd to run for a count of 30 blocks for a total of 30MB. This will save you from needing to wait for the full drive to finish.

Repeat the procedure until you receive the expected hash for sdb1.

This is on a separate page for a reason. Make sure you read and understand everything else.

Does everything match now? Great! Remove the flash drive, set it down, and look at it. Everything up to this point was simply setup because in an online class, I cannot just simply hand you a drive which has already been preconfigured with a known hash value.

The assignment deliverables will begin from this point forward; you should proceed as if that flash drive which you've setup is the flash drive which has been delivered to you in the scenario. Almost nothing relating to the setup above should be in your report or notes and will count against your grade if included. The one caveat to this is to include the changes to disable auto-mount in Mint and denying USB write access in Windows since you are effectively setting up a software-level write blocker which we would do in the absence of a hardware write blocker.

Your Assignment

Scenario

You will be working for Special Agent Blanche Urbach attached to the Orlando field office of the Federal Bureau of Investigation. SA Urbach has brought to you a USB flash drive sealed in an antistatic evidence bag. This bag is sealed with tamper resistant tape and initialed by the Agent.

To help clear their backlog, Agent Urbach has requested of you the creation of a forensic copy of the partition contained within the provided USB flash drive along with a report and notes.

Hints

Make sure to include in your notes

- Description of the evidence as received
- Description of the flash drive
  - Make, size, serial number, color, identifying marks, etc
- Procedure to disable auto-mount
- Procedure to disable USB writing (if using Windows)
- Hash of the original partition before copying
- Hash of the forensic duplicate of the partition
- Hash of the original partition after copying
- Version of the OS including kernel and any tools you used

Your report should indicate a summary of the actions performed, results, forensic questions/answers, etc.

Forensic Questions (Include these answers as a separate page at the end of the report)

1. If you were working on a case for a law enforcement agency, which hashing algorithm would you use and why. This is a light research question – do not just say MD5 of SHA1 because that's what we use here because we're mainly concerned with speed. The answer here should also be more than a few words or a single sentence. Make sure to state your answer and fully elaborate on why that is your answer.
2. What are some possible causes for a hash of an original and a forensic duplicate to not match and possible issue which would result from the mismatch
3. What are possible issues which could result if the operating system automatically mounted the flash drive prior to creating the forensic duplicate

Name your assignment your firstName.lastName.1.pdf/doc and upload this to the Assignment 1 drop box on Florida Online by the due date.