Information Security and Assurance

Digital Forensics

For each task with an asterisk (\*) add a screenshot (full screen, do not crop). If it’s on a command take the screenshot after pressing enter.

Revert your previous systems (DC1, PC1, LX1, MS1) back to their original state by right-clicking each and choosing Revert…

As the Incident Response Engineer for your organization, you have been given a disk to investigate.

Open HyperV in your VM

Attach the incident.vhdx disk to your Kali VM.

From within your Sandbox VM, login to Canvas

Download file onto your Sandbox VM

Go to settings of Kali VM – SCSI Controller – Hard Drive – Add – Browse – choose the .vhdx file

Start the Kali VM (root/Pa$$w0rd)

\*Open a terminal window and type

fdisk -l /dev/sdb

How big is the disk? How many partitions does it have? How big is each partition?

\*Create md5 hashes for the disk and partition by typing

md5sum /dev/sdb

md5sum /dev/sdb1

Create an image of the disk by typing

dd if=/dev/sdb of=/disk.dd

Create an image of the partition by typing

dd if=/dev/sdb1 of=/partition.dd

Why did we create these images?

\*Create md5 hashes for the images by typing

md5sum /disk.dd

md5sum /partition.dd

Did these produce the same values as the disk and partition? Why? Why would we do this?

Create a working directory by typing

mkdir /working

Make copies of the images by typing

cp /disk.dd /working/disk.dd

cp /partition.dd /working/partition.dd

\*Create md5 hashes for the copies by typing

md5sum /working/disk.dd

md5sum /working/partition.dd

Create the directory /working/partition by typing

mkdir /working/partition

\*Mount the working partition image to the filesystem by typing

mount -o ro,norecovery /working/partition.dd /working/partition

Why did we use the ro option? What additional step should we have taken if this were a real disk/investigation to assure this?

Investigate the drive by clicking Places – Computer – working

How many files did you find? Take screenshots of where you found them.

Perform a strings command against the disk partition by typing

\* strings /working/disk.dd >> /working/disk-st.txt

Open the strings output by typing

gedit /working/disk-st.txt

\*Search the file for any reference to “secret”

What is the secret?

Anything else interesting in the strings output? Why did we perform strings on the disk instead of the partition?

Why did we do our work from the copied images in the /working directory rather than the original ones created?