

# Information and Technology Services

## Windows Forensic Acquisition Procedure

### **Overview and Scope**

- This procedure has been developed to ensure that any forensic acquisition of questionable computers is performed following a tested process that results in a consistent set of data. This procedure is to be used whenever the investigation of an information security incident leads the investigator to believe that acquiring an image of a computer is necessary.

### **Procedure**

- **Live System Acquisition**

If the system is online when you arrive on the scene then you should attempt to gather some volatile data from the computer before it is shut down. These procedures carry some risk of changing the contents of the source drive, such as date and time stamps on the files that you access. This is an acceptable risk, however, because the volatile data that will be lost when the computer is powered down may contain extremely valuable data.

- **Running a Trusted Command Prompt**

Insert the Helix Live CD into the Windows machine. Accept the warning when the disk is first inserted. From the Menu bar select Quick Launch, and then command prompt. This will open a command prompt from the CD which will reduce the likelihood that another running process is affecting the output that you receive from your commands.

- **Acquiring Physical Memory**

Run the following command in the trusted command prompt:

```
dd.exe if=\\.\PhysicalMemory conv=noerror | nc <listening ip> <listening port>
```

You can also use the GUI interface on the Helix CD to acquire physical memory and send it to a listening computer.

- **Basic Commands**

Run the following commands in the trusted command prompt to gather basic information about the computer, running processes, mapped drives, and network connections.

```
date /t
time /t
uptime
net use
net session
net file
net share
net view
net user
net accounts
net localgroups
net start
nbtstat -c
nbtstat -an
arp -a
netstat -a
```

- **Gather additional information**

The following commands can be used from the Helix Live CD to gather running processes, and the ports that these processes are using

```
psinfo /accepteula
pslist /accepteula
fport
```

- **Acquiring Hard Drive Image**

The preferable method for gathering a hard drive image is to power down the machine after the live acquisition and gather the hard drive data from another operating system. The suspect hard drive must be connected to a machine that will not mount the drive. A machine booted to the Helix forensic CD is one option. Another option is to connect the suspect hard drive to a hardware write blocker.

Before acquiring the hard drive image, the suspect hard drive must be checked for a host protected area (HPA). Use the command `disk_stat` (from the Sleuthkit tools) to check for the presence of an HPA. If an HPA is detected, run the command `disk_sreset` to remove the HPA.

Where possible, the program `dcfldd` is used to acquire the hard drive, split it into chunks, and run both the md5 and the sha256 hash algorithms against each chunk. This technique is preferable to others because if there is a problem with the acquisition you can reacquire and pick up where you left off while maintaining forensic integrity. This also gives the investigator the opportunity to work on pieces of the drive before the imaging process is complete.

```
dcfldd if=/dev/sourcedirve hash=md5,sha256 hashwindow=10G md5log=md5.txt
sha256log=sha256.txt hashconv=after bs=512 conv=noerror,sync split=10G
splitformat=aa of=driveimage.dd
```

`dcfldd` = name of program

`if` = input file

`hash` = comma separated list of hash functions to use

`hashwindow` = how big of a chunk to hash each time (recommend same size as split)

`md5log` = where to keep the md5 hashes

`sha256log` = where to keep the sha256 hashes

`hashconv` = decides whether to hash the chunks before or after the corrections done by conv

`bs` = byte size. 512 is the default sector size on a hard drive

`conv` = `noerror,sync` will write zeros if it can't read a sector, and `sync` will make sure that the good data lines up on both drives if there are errors

`split` = how big of a chunk to write before splitting to another file

`splitformat` = the naming convention of the files.

## **Exceptions**

- This procedure can be changed by the principle investigator at the time of the acquisition if these procedures will not work properly due to the circumstances of the investigation.
- Any deviation from this procedure must be recorded in detail in the case notes of the investigation.

## **Effective and Review Data**

- This procedure takes effect July 1, 2008

- This procedure will be reviewed on July 1, 2009 and every year after that.

**See Also**

<http://www.networksecurityarchive.org/html/Computer-Forensics/2005-05/msg00004.html>

<http://osdir.com/ml/security.forensics/2006-02/msg00029.html>