Craiger's Cyberforensic Commandline Cheatsheet (C^4)

1. Create a forensic image

```
# dd if=/dev/hda1 of=forensic.dd bs=4096 conv=noerror,notrunc,sync
```

2. Create forensic image over network

Client: `# dd if=/dev/hda1 | nc 192.168.1.100 9999 -w 3`

Client: `# cat /dev/hda1 | nc 192.168.1.100 9999 -w 3`

Server: `# nc -l -v -p 9999 > forensic.dd`

Server: `# netcat -l -v -p 9999 > forensic.dd`

3. Mount an image read-only

```
# mount -t ntfs -o ro,loop,noatime,noexec,nodev image.dd /mnt/evidence
# mount -t vfat -o ro,loop,noatime,noexec,nodev image.dd /mnt/evidence
```

4. Unmount the same image

```
# umount /mnt/evidence
```

5. Find all files that contain the word marijuana (ignore case)

```
# grep -r -i marijuana *  // -r is for recursive, -i is for case insensitive
# grep -r -i marijuana *.doc // find marijuana in all files ending with *.doc
# grep -r -i -f keywords.txt * // fgrep, keywords.txt contains multiple keywords
```

6. Find MS Word files accessed in the last five minutes

```
# find . -name '*.doc' -amin -5
```

7. Find MS Word files accessed in the last five days

```
# find . -name '*.doc' -atime -5
```

8. Find MS Excel files created more than 10 days ago

```
# find . -name '*.xls' -atime +10
```

9. Find MS PowerPoint files accessed in the last 10 minutes

```
# find . -name '*.ppt' -amin -10
```

10. Find all JPG files that were created in the last 10 days.

```
# find . -type f -ctime -10 -print0 | xargs -0 file | grep 'JFIF'
```

11. Find graphics files that are hidden

```
# find / -type f ! \( -name '*.jpg' -or -name '*.bmp' -or -name
'*.png' \) -print0 | xargs -0 file | grep -i -f graphics.keywords >
hidden.file.list
```

12.Find credit card numbers

```
# egrep "[45]###[- ]*###[- ]*###[- ]*"
# grep "####-####-####-####"
```

13.Find Window's OS version on Windows 9X/ME

```
#grep –a 'RegisteredOwner' –C 4 system.dat | strings
# grep –a 'ProductName' –C 2 /windows/system.dat | strings > file.txt
```

INCIDENT RESPONSE

From: Craiger, J.P. (2004). Computer forensics procedures and methods. In H.Bigdoli (Ed.), The Information Security Handbook. New York: John Wiley.

1. **Immediately** determine if a destructive program is running on the computer. If one is running, the investigator should pull the power plug from the ***back*** of the computer (not at the outlet). This will ensure no further evidence is lost.
   1.1. Place tape across all open disk drives so that no media is inadvertently placed in the disk drives.
2. Begin documenting the computer and its surroundings. Video tape and pictures are good supplements to handwritten notes. Things to document include:
   2.1. The computer's make, model, serial number.
   2.2. Attachments to the computer (e.g., external hard drives, speakers, cable modem, USB or network hubs, wireless network routers, and so on).
   2.3. The state of the machine, i.e., whether it was running or not.
3. If the computer is running, take a picture of the screen. Pictures demonstrate that the computer was running as well visually document what was running at the time.
4. Physically open the computer and take pictures of the inside of the computer. This will show the number of hard disks connected, as well as any peripherals connected, such as network and sound cards, that were connected.
5. Take pictures of the front, side, and back of the computer. A picture of the back of the computer will allow an investigator to recreate the computer setup should the entire computer need to be seized and taken back to the lab for further investigation. If the computer is to be seized, label connectors (network, USB, firewire, etc.).
6. Search for 'sticky notes' or any other written documentation nearby the computer (including under the keyboard, under the desk, in desk drawers, etc.). Users often write down passwords and leave them in convenient places near the computer. These passwords may be necessary if the user has used encryption to obfuscate file contents. Make sure to look at the waste basket as it may hold valuable information.
7. Execute a *bag-and-tag* of all potential evidence. Bag-and-tag is a law enforcement term that refers to the process of placing crime scene evidence (e.g., hairs, fibers, guns, knives, bloody gloves, and so on) bags, and tag with relevant information including date and time collected, name of investigator, where collect-

ed, etc. All potential evidence such as floppy disks, CDs, DVDs, papers surrounding the computer, etc., should be subjected to a bag-and-tag.

8. Some situations require the confiscation of the source computer by law enforcement (Heverly & Wright, 2002). If the computer is to be transported to an offsite forensics lab, label each computer part and place in an appropriate container for transport.
9. Take any computer manuals in case they are needed for reference back at the forensics lab.
10. If the original evidence is to be confiscated it should be stored in a secure place.