Removing hard drives from computer systems for direct drive-to-drive imaging:

Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
davepet@cops.org

1. Remove screws from the case and take it off.
2. Remove screws from the hard-drive mounting bay and pull it out so that you can work with it.
3. Use a Sharpie to put dots where screws should go to remind you to insert them.
4. Using a power screwdriver, remove screws securing hard drives.
5. Mark the cables attached to the hard drives and label them so that they go back the same way they came off: 1-1, 2-2, etc. The hard drive cable normally has the red edge toward the middle of the hard drive, but mark it anyway to be sure.
6. Use the Sharpie to mark the case number, computer number, and hard drive number on top the actual hard drive.
7. Examine the hard drive to see whether it is a master or slave. There will be a li'l diagram on the back of the hard drive. You might have to move the jumpers from master to slave to cable select until your forensic processing machine recognizes the drive.
8. Tape screws together and tape them to the hard-drive mounting bay so that they are not lost.

Attaching these suspect hard drives to the forensic evidence processing computer:

SCSI

- The cord that sticks out the back of this evidence processing computer is for attaching SCSI (scuzzy) drives.
- You can recognize a SCSI drive because it has one 50-pin connector. An IDE drive has one 30-pin connector.
- Attach ribbon cable to the SCSI drive, then attach the power.

IDE

- Put the IDE drive into the removable hard drive drawer. Plug in the ribbon connector and the power.
- Slide the drawer in with the handle up, or it won't go in all the way.
- When you hear it latch, use the key to secure it and activate the power. Turn the key to the horizontal (locked) position.

Once you get these drives attached…

- Power up the evidence processing computer
- Immediately hit F1 to put the computer into the BIOS
- Make sure you can see all the drives involved at this point:
  - Primary IDE Master is our HTCU system drive
  - Primary IDE Slave is the HTCU evidence drive
  - Secondary IDE Master should be the suspect drive you attached
- If all three drives look "good-to-go," exit the BIOS setup screen
- Put the EnCase boot disk into Drive A, and let the computer reboot
- At the prompt, type EN (don't need /S, which is used in the direct parallel port connection to search for the suspect computer's slave drive)
- When the screen showing various drives involved, make sure all are reflected, and that you know which one is which:
  - The HTCU system drive is a 4-gigabyte drive, it is labeled "HTCU system"
  - The HTCU evidence processing drive, now 8 gigabytes, labeled as "evidence"
  - By process of elimination, the remaining drive is the suspect drive, and it should be labeled as a numerical drive (the only physical drive there; the other two are logical drives)
- At this point, you will probably see that all three disks are locked. In order to image the suspect drive, you will have to unlock the HTCU evidence drive, whichever one it is.
  - Enter the "locking" tab, and find the drive to unlock.
- Acquire the suspect drive
- It is a good idea that when you get to the screen "evidence file path" that you label it as the type of drive the suspect hard drive is. For example, "d:\seagate 1.2.
- You might want to note the suspect's first and last name in the "description" screen
- Once you finish these screens, the acquisition process starts. Make sure you have drive activity (the yellow light below the green power-on light winks at you).