Cool Careers for Girls in CyberSecurity
Law Enforcement

Duration: Each student session last for 20 minutes. Students will need a five minutes to travel to their next session.

Session Overview: Each group of students will use FBI fingerprinting tools to lift fingerprints from common objects.

Objectives:

Practice the evidence collection process
Connect physical evidence collection process to the digital evidence collection process

Materials/Supplies :

Fingerprinting kit
Paper

Introduction:

Law enforcement officers collect fingerprints (also hand and bare footprints)at crime scenes. These prints can place a suspect at the scene of a crime. This is only one type of evidence that can be collected from a crime scene. Ask the students to think of the different types of physical evidence.

Blood and other types of Liquids and Stains
Hair
Fibers and Threads
Glass
Paint
Flammable Liquids
Firearms Evidence
Tool Marks
Controlled Substances and Medicinal Preparations
Documents
Fingerprints

The evidence collection process is also documented with cameras.

Lesson:

Assist the students in collecting fingerprint evidence.

Final Thoughts:

Collecting and analyzing digital evidence also requires a process to be sure that no one can say that the collection and analysis process process destroyed or changed the evidence. Sans lists these procedures for collecting evidence from a home computer:

1. Photograph the computer and scene
2. If the computer is off do not turn it on
3. If the computer is on photograph the screen
4. Collect live data – start with RAM image (Live Response locally or remotely via F-Response) and then collect other live data "as required" such as network connection state, logged on users, currently executing processes etc.
5. If hard disk encryption detected (using a tool like Zero-View) such as full disk encryption i.e. PGP Disk — collect "logical image" of hard disk using dd.exe, Helix – locally or remotely via F-Response
6. Unplug the power cord from the back of the tower – If the computer is a laptop and does not shut down when the cord is removed then remove the battery
7. Diagram and label all cords
8. Document all device model numbers and serial numbers
9. Disconnect all cords and devices
10. Check for HPA then image hard drives using a write blocker, Helix or a hardware imager
11. Package all components (using anti-static evidence bags)
12. Seize all additional storage media (create respective images and place original devices in anti-static evidence bags)
13. Keep all media away from magnets, radio transmitters and other potentially damaging elements

    Collect instruction manuals, documentation and notes
14. Document all steps used in the seizure

http://computer-forensics.sans.org/blog/2009/09/12/best-practices-in-digital-evidence-collection/

Once the evidence has been collected it is important to create an exact copy of the digital information. There are tools that help law enforcement make these exact copies which will also duplicate any deleted or hidden files. A good message to reinforce to students is that deleted information can be recovered. They should consider all digital information permanent – this includes cell phones.