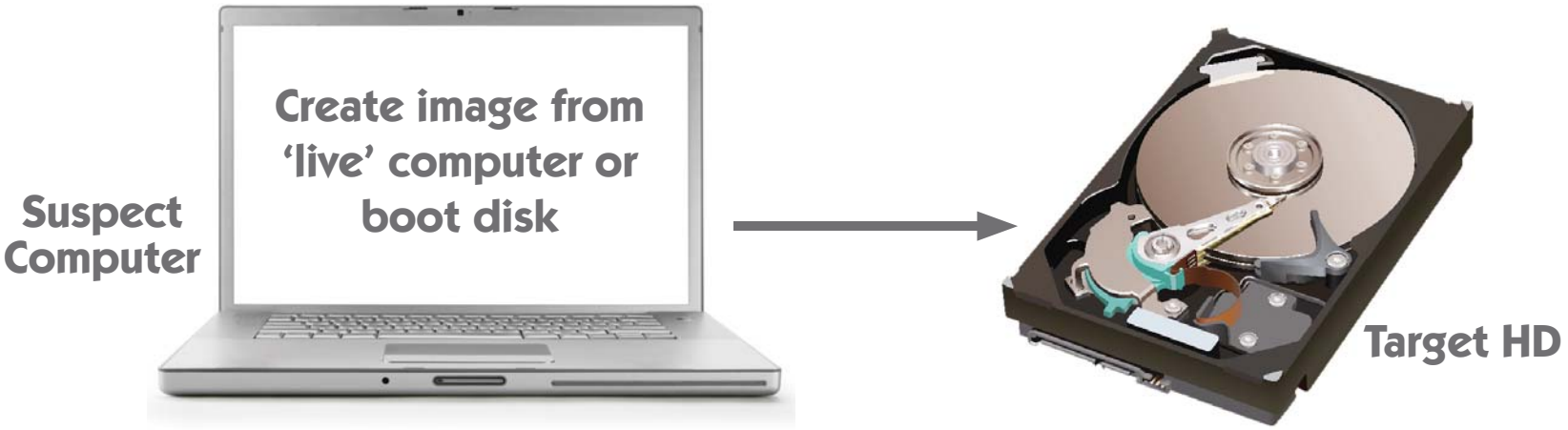
Creating a Forensic Image

Using Suspect Computer



Creating a Forensic Image

- Suspect computer is booted and controlled by forensic software which prevents modifications to the source hard drive. The forensic software creates an image (copy) of the computer's hard drive.
- Sometimes the suspect computer should not be turned off or needs to be running due to a risk of losing critical evidence or because hard drive encryption is in use. In this scenario, forensic software is ran from a CD or USB device which creates a 'live' image of the suspect's computer's hard drive and memory contents.
- Hard drive encryption 'scrambles' or hides files and prevents examiners from performing a normal analysis when the hard drive is turned off. Capturing an image or analyzing the suspect drive while powered on may be necessary.
- A verification hash or checksum is commonly used to verify the target drive (or image) is the same as the source.

PINPOINT LABORATORIES

www.pinpointlabs.com