Equipment

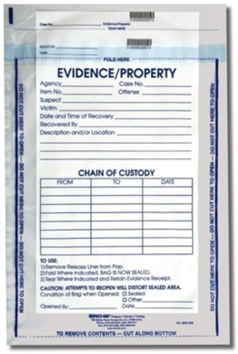
Collecting evidence in digital forensics investigations is something that takes careful planning and preparation and if the investigator doesn't have the proper toolkit, then the evidence may become compromised. Many law enforcement departments around the globe have dedicated forensic laboratories where they can analyze evidence in a manner that will prevent it from being tampered with. As an investigator, you will need to have the same kind of tools at your disposal, comparable to what you would find in a laboratory.

EQUIPMENT

Forensic Laptop or Workstation

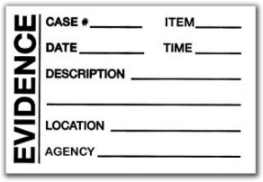
Bringing a laptop specifically designated for digital evidence can be essential when gathering the evidence at the scene or capturing evidence that may be in memory. Popular Linux distributions such as CAINE or DEFT can often be found on these laptops, as well as commercialized systems for law enforcement.

Electro-Static Evidence Bags with Tamper-proof Stickers



Electro-Static Evidence Bags will help protect any sensitive digital components from Electro-Static Discharge (ESD) during the transport of the evidence from its initial location, to a secure lab environment. Labeling is often applied to these bags to let investigators know what is contained inside of them. Having bags or stickers that are sealed, and the seal must be physically broken to gain access to the evidence within is critical to ensure the chain of custody is maintained, and that evidence is not tampered with whilst in storage or transit.

Labels



EVIDENCE

CASE # ________ ITEM ________
DATE ________ TIME ________
DESCRIPTION ________________
____
LOCATION ________________
AGENCY ________________

Labeling is essential when conducting any kind of evidence collection. Knowing what piece of hardware is, helps yourself and other people in the chain of custody determine what the evidence is, without having to go inside of it.

Photographs

Photographs, like in any kind of crime scene, can be helpful to show the investigator the bigger picture. This could include how the equipment was set-up at the crime scene, as well as providing clues later on, that might be helpful to the investigation.

Grounding Bracelets

Similar to Electro-Static Bags, grounding bracelets are important for investigators to use, to ensure that when handling evidence, they do not inadvertently compromise or damage the evidence.

Hardware Write-Blockers

Hardware Write Blockers can be an essential piece of equipment that will ensure that your evidence has not been tampered with. It can either be software on your forensic laptop, or a hardware device that permits read-only access to data storage devices without compromising the integrity of any data that may be contained on them.

Blank Hard Drives

In the event that you need to copy data on-site, having blank hard disks are an essential piece of hardware to have in your toolkit. These can be used in conjunction with write-blockers to copy the disk to another one without making any writeable changes to the media. Drives used for forensic work need to be extremely high capacity, especially if bit-by-bit copies of suspect hard drives are being copied. The size of the receiving drive must always be higher than that of the original drive.

SPECIALIST EQUIPMENT

In some cases, specialized equipment/software is used on the scene to assess the digital evidence that was found. This can include:

- **Wireless Stronghold/Faraday Boxes –** to block any wireless signals from reaching the evidence, preventing remote access or wiping.
- **Specialized Write-Blockers –** write-blockers that could also be used on cell phones, GPS devices, IoT devices, and other non-standard hard-drives.
- **Phone Jammers –** acting the same as a faraday box or wireless stronghold.
- **Dedicated Flash Drives –** containing tools like Encase, FTK, CSILinux and MacQuisiton.

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson