DEAD & LIVE FORENSIC

Data acquisition in Digital forensics includes the procedures involved in gathering digital evidence such as clonning & copying Evidence from any Electronic device.

Live acquisition

It involves in capturing data from a system that is running

It Allow investigators to capture volatile info.

Note: Live Acquistion must only be performed if necessary because it can modify the system

* A live system refers to system that are up & running where info may be altered as data is continuously processed.
* lot of evidentiary value that could be found in a live system
* Switch it off may cause loss of volatile data In contrast, leaving a computer running may cause evidence to be altered or deleted

In live acquisition technique is real world live digital forensic investigation process, Eg: a common approach to live digital forensic involves an a tools into read only mode in system attaching writable media to system & using tool to start live imaging in that tool.

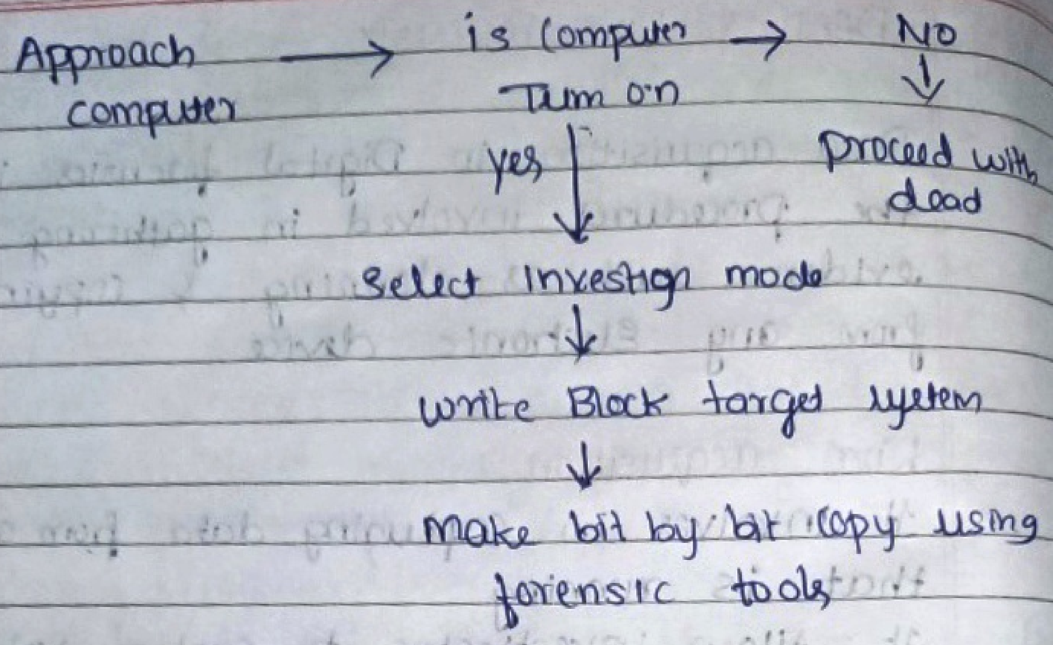


fig: Live forensic Image acquisition

Adv: * Volatile data capturing

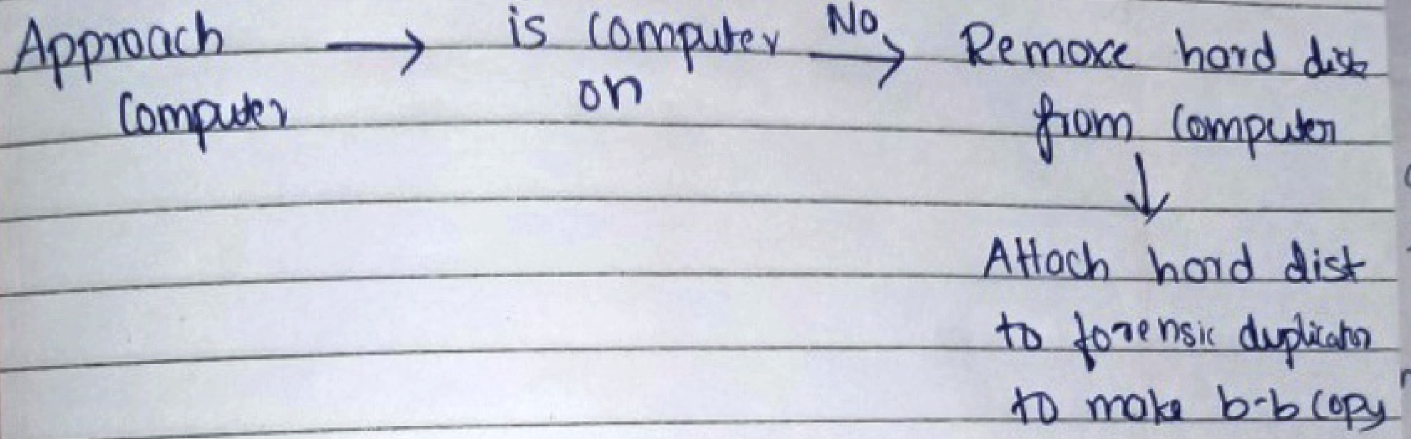
disadv
* [take more time (coz speed of creating copy depend on speed of system on processing is being carried out)
* In capturing RAM or memory

Dead acquisition

It involves in making a forensic image from computer media such as Hard drive, CDROM, removable hard drives

* It produce some information, they can't recover everything.
* By power off the system & removing the disk in order to connect it to a forensic workstation / hardware or software write blocker to creat image → refer as dead imaging

A write blocker will prevent any data from being tampered & allowing read access only. ⇒ preserve integrity of file metadata



Approach Computer → is computer on →No→ Remove hard disk from computer ↓ Attach hard disk to forensic duplicator to make b-b copy

fig: Dead forensic Image Acquisition

Adv: * need less time

Disadv: * It won't capture volatile data
* no provision in capturing RAM.