Steps for Secure replication

Preservation for analysis

Steps for replicating Hardware (USB, SDD, HDD SD-cards etc.)

- Was a writeblocking device or software used?
  - if so what type ? hardware or software
  - If no writeblock device was used. What were the circumstances? (live aquisition)
- What software was used to replicate data? (fx FTK imager, Magnet aquire etc.)
- Make, model and serial number of the hardware secured
- Who did perform the action.
  - What date and timeframe was this done?
- Integrity check made for ensuring integrity of data.
- Where is data replicated to?
- where are the data stored and who was this data replicated to?

Steps for replicating files (software, artifacts, logs triangulation data etc.)

Triangualtion data is data from firewall, siem, shares, antivirus, DNS etc.

- Where is it secured to?
- What types of data are we talking about and what source is it collected from
- What does the data prove?
- Who has collected the data and who has access to the data.
- How much data was secured and performed by whom?
- Data integrity check and file that contains this, toghether with a timestamp

Considertations to above

In order to share content with peers, retainer agreement or law enforcement. We need to have means for secure sharing in place.

The use of encrypted containers here, should be in place.

- Fulldisk encryption (Luks, Filevault or Bitlocker)
- Container encryption (Veracrypt, boxcryptor or similar that support AES256 encryption)

Artifacts that are of malicious content

These data are dangerous and should be treated as such.
ZIP the files with a password infected and saved as infected.zip in a seperate folder with integrity check and or a README.txt

This ensures data is kept and not accidentially activated nor deleted by antimalware protection

L A R S B L O M G A A R D - K E A X L E B @ K E A . D K