4.5

Wednesday, September 27, 2023 6:09 PM

acquire OS-level info from Windows

- check sys/sec logs
- reboot and analyze memory dump files

  Windows writes mem contents to dump file on kernel error

- sleep mode and anal hibernation file

  creates at root of boot volume

establishing provenance of evidence

- record acquisition process on video
- timestamps of acquisition process
- collect evidence in order of

volatility

writing down time is not admissable

NTFS uses UTC

Legal hold - info that may be relevant to investigation

eDiscovery - filtering relevant evidence produced from all the data gathered in forensic exam

investigation

- ensure non-repudiation
- no evidence is missed
- establish provenance of evidence

notify consumers of breach immediate

GDPR - 72 hrs

HIPPA - > 500 people

timeline - preservation of evidence remain credible

disk image - digital file accurately representing contents and config of a disk volume or whole data unit

bootloader + OS

Use write blocker when forensic exam