The Challenge of SSD Forensics

Paul Pelzl

Guidance Software

Guidance Software

- 15 year old company
- Started in computer forensics; expanded to services, eDiscovery, and cyber security
- Best known for the EnCase suite of analysis software
- Also manufactures embedded devices for use in the forensics industry

What is Computer Forensics?

- Encompasses the recovery and investigation of material found in digital devices
- Targets include networks, databases, mobile devices, and individual PCs (SSDs!)
- Usually related to criminal activity which involves computers
- Forensic practitioners found in law enforcement, intelligence agencies, corporate IT security, law offices, etc.

What is Computer Forensics?

Try to answer questions like:

- Was an individual in possession of confidential or restricted material?
- Who was an individual in contact with?
- What is the timeline of recent activities carried out on a PC?
- What is the extent of the damage due to a network intrusion?

The Golden Age of Hard Drive Forensics

Rotational magnetic media has well-understood behavior:

- Deleted files or old data are still accessible until overwritten
- Essentially all the physical media is accessible (minus a tiny spare-block store)
- Bad blocks happen
- Aside from bad-block remapping, logical sectors are associated with predictable (consistent) regions of physical media

The Golden Age of Hard Drive Forensics

Forensic best-practice for hard-drive analysis:

- Full-disk imaging (raw sector data, not just filesystem content)
- Unlock hidden partitions (HPA/DCO) to retrieve the full media contents
- Full-disk cryptographic hashes are legally accepted for verifying integrity of evidence images

SSDs Breed Forensic Uncertainty

- Garbage collection
  - Will deleted data be available? For how long?
  - What data is returned when reading a garbage-collected block?
  - If I hash a disk at two different times, is there any chance of getting a consistent result?
- Over-provisioning
  - How do I know that relevant data is not hiding in the (potentially large) reserved block store?

SSDs Breed Forensic Uncertainty

- Block mapping weirdness
  - What data is returned when reading a block which was never written?

- Of course, the answers to these questions vary by manufacturer and model…
- *Uncertainty and nondeterministic behavior are very undesirable for people making statements in a court of law!*

What do Forensic Analysts Want?

- Preserve data whenever possible (disable background garbage collection)
- Read consistent data
- Access the full physical media (reserved block store)
  - Block mapping information would be a nice bonus…
- Guidance is willing to work with manufacturers under NDA

Conclusion

- Inconsistent behavior of SSDs is problematic for low-level analysis (including forensics)
- Some relatively modest behavioral changes would help a lot