Old Wine in New Wineskins

How Remnant Data Challenges Forensics and the Law

Sebastian Hilgert, LL.M.

14th International Conference on IT Security Incident Management & IT Forensics

The Problem of Remnant Data

80% of external hard disks sold as used contained reconstructable data from their previous use (Shah et al, Applied Sciences 2022)

Reconstructable data found on drives sold as new with recycled NAND and eMMC flash memories (Schneider et al, DFRWS EU 2021)

Inadequate processing / sanitization leads to occurrence of remnant data

The Paper’s Research Questions

- How does one possess data?
- How do cases like remnant data or file fragments influence the evidentiary value of forensic findings?
- Which conclusions can be drawn for forensic professionals, as well as the legal prosecution and defense?

Establishing Possession

Unhindered Control / Power of Disposition	Knowledge of possession	Will / Intent to possess
• **Objective element** • Possibility to use, consume, destroy, alter, etc. • = Physical control	• **Subjective element** • Conscious perception of the object's existence	• **Subjective element** • Demonstrated by perpetuation of physical control

Possession of Non-Corporeal Objects

Unhindered Control / Power of Disposition	Knowledge of possession	Will / Intent to possess
• **Objective element** • Possibility to use, consume, destroy, alter, etc. • = Functional control	• **Subjective element** • Conscious perception of the data's existence	• **Subjective element** • Demonstrated by perpetuation of functional control

Ascertaining Knowledge of Possession

- Establishing timeline
  - E.g. by using MAC time stamps, corroboration with “real-world” dates
  - Novel approach: digital stratigraphy
- Evaluate data location
  - Does the user have access to data location?
    - Access permissions, hidden files, etc.
  - Would the user have perceived the files
    - After buying a new storage device, it will raise suspicion, if there are files present
    - Contrarily a user will not wade through all files present on a used smartphone’s system directory, even if access is given
    - Did the user have a concrete incentive to open a file to perceive its content?
  - > Differentiate between (typically user-specific) locations the user has access to and (typically system-related) locations they are unlikely to access

Ascertaining Will to Possess

Perpetuating functional control („save for later“)

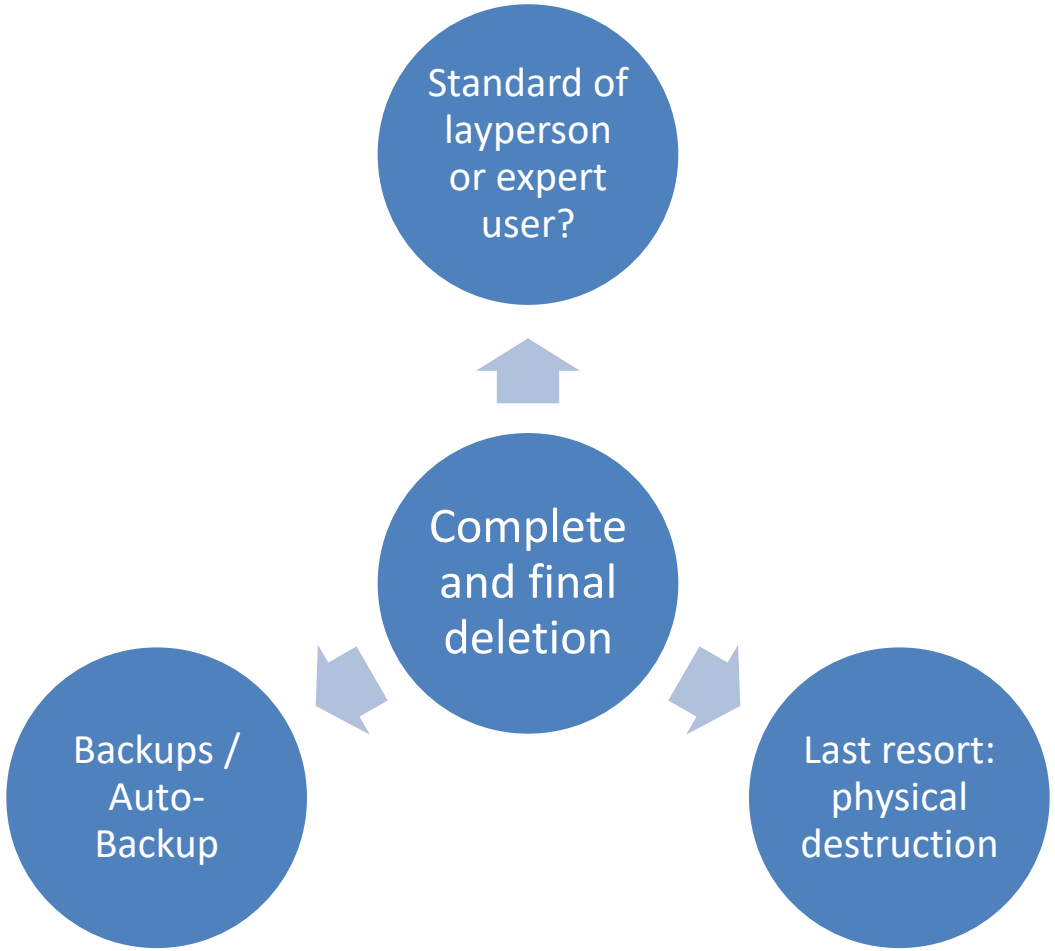
Deliberate toleration is sufficient, since purpose is irrelevant

Immediate deletion

or

Handover to competent authority

Selected Problems Regarding Deletion



Closing Remarks

Mind your scope

- What professional forensic software may be able to recover, may be outside the scope of an individual user's possibilities
- It is entirely possible to reconstruct files the user in question had no knowledge of

Remnants as a first step

- Not all devices come as a clean slate - finding remnants can therefore always only be the first step and must not be seen as definitive proof of data possession, much like it is insufficient to infer data possession from device possession

The defense's view

- Time of deletion must be assessed, if possible, in case user immediately deleted files
- When served old wine in new wineskins, or old files on new storage devices, it is paramount to rid oneself of it as soon as possible, in order not to become possessor against one's own will.