Chain of custody & Preservation of evidence: biggest misconception in IT forensics?

Prof. Dr. Tobias Eggendorfer
Hochschule Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen
IT forensics - current „teaching“

- Copy the hard disk
- Work on the copy
Nothing wrong, when examining this:
Except for the amount of data.

• That’s why
  • Jonathan Grier tried to reduce the amount
  • Bradley Schatz optimised formats to increase transfer speeds
But impossible for
However: It is attempted.

Reasons:
Evidence needs to be available.
It needs to copied so it cannot be tampered with.
But how do other forensics sciences solve this?
Can‘t keep it forever.
What if only wounded?

- Stitch it up?
- Or keep it - just in case?
Add some explosives to keep it going?
How do they do it?

- Write a report, have someone sign it
- Maybe
  - add photos or sketches
  - keep some pieces
And why?

• Their evidence can’t be copied
• It won’t last forever
We don‘t always investigate the „really nasty“ stuff.
Why aren‘t we doing this?

• We copy extensive amounts of data.
• We compromise privacy by doing so.
• We waste millions of GByte.
• We waste time.
Who said we have to do it this way?
My suggestion:

- Prefer live forensics over post-mortem
- Get rid of copying
- Reduce data (Triage)
- Keep only what‘s necessary
- Run the risk of case blowing up in court if it‘s not „a big thing“
Thank you
tobias.eggendorfer@hs-weingarten.de