



The Chain Of Custody: A Big Misconception

By

Tobias Eggendorfer

Presented At

The Digital Forensic Research Conference

DFRWS 2015 USA Philadelphia, PA (Aug 9th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<http://dfrws.org>

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

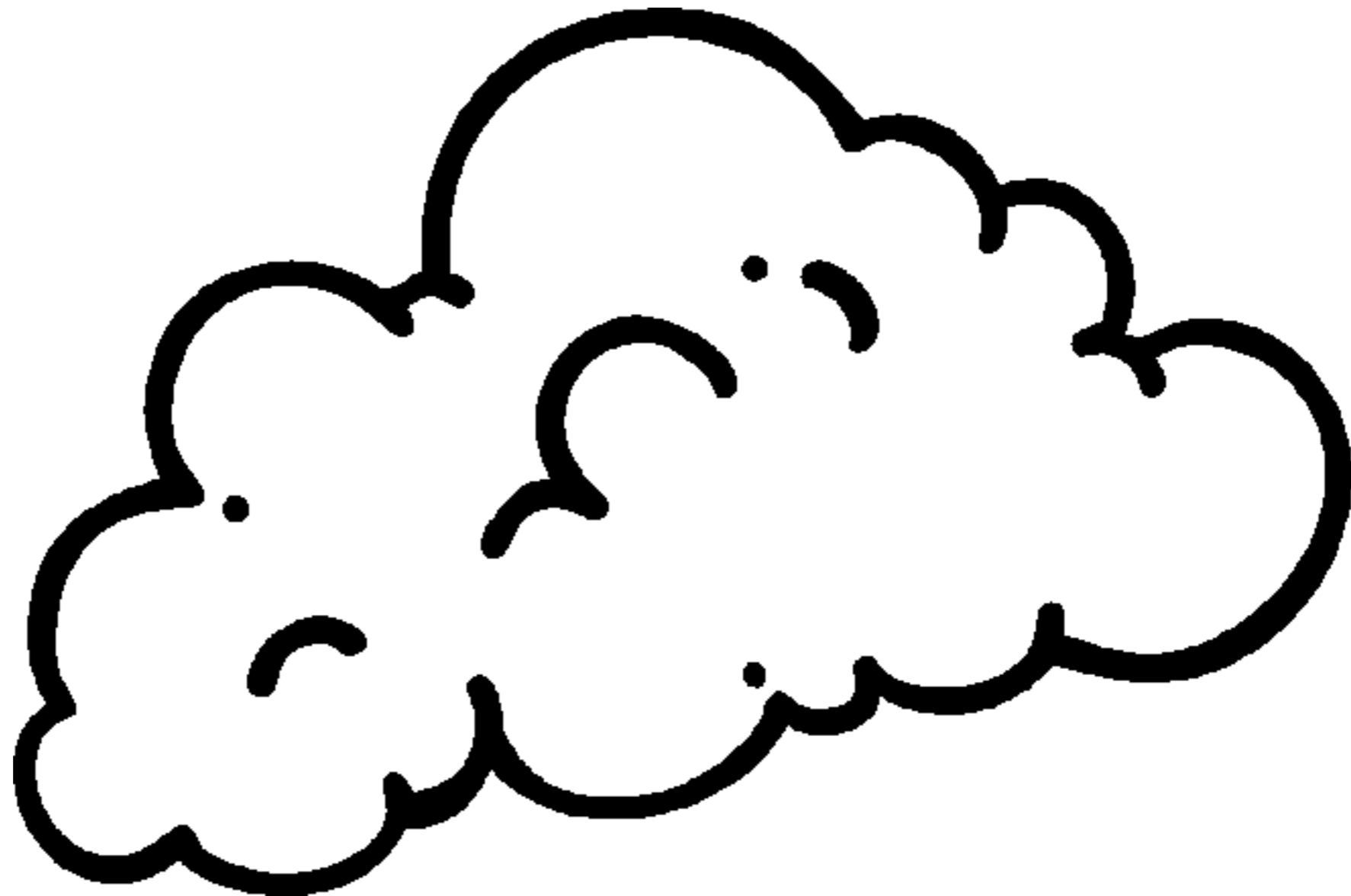
Nothing wrong, when examining this:



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 be 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