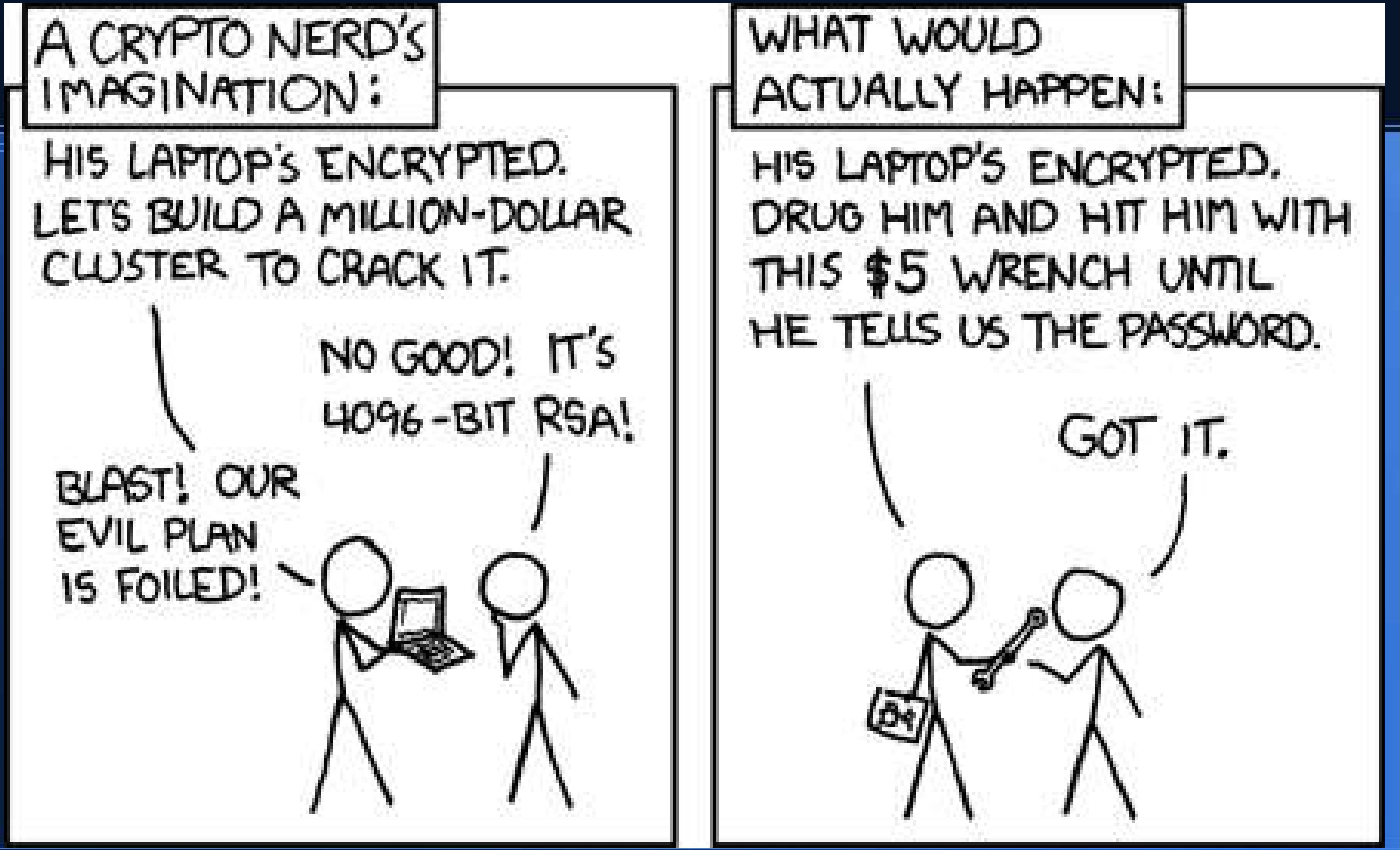
Future challenges in deniable encryption

jenda@hrach.eu

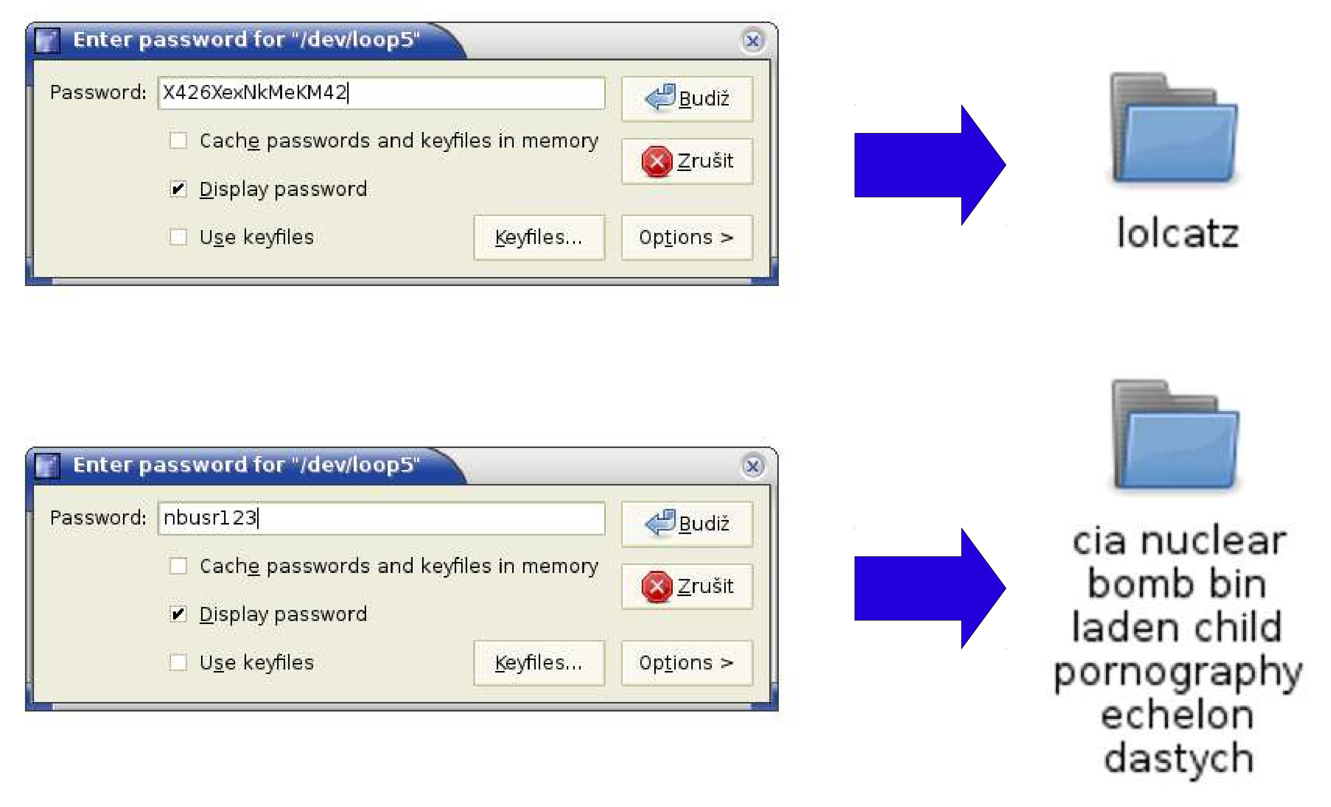
Hard drive encryption

- /dev/sda2: sticky LUKS encrypted file, ver 1 [aes, xts-plain, sha1] UUID: d747bbfe-816f-4010-b49c-2d04a54cd897
- https://en.wikipedia.org/wiki/Key_disclosure_law
- Britain: 2/5 years
- France: 3/5 years/€45k
- US: court in progress, border searches
- CZ: we will see…


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LETS BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Deniable encryption

- Multiple passwords, multiple outputs
- Given N passwords, it's impossible to prove than N+1 passwords exist



Enter password for "/dev/loop5"

Password: X426XexNkMeKM42

☐ Cache passwords and keyfiles in memory

☑ Display password

☐ Use keyfiles

Enter password for "/dev/loop5"

Password: nbusr123

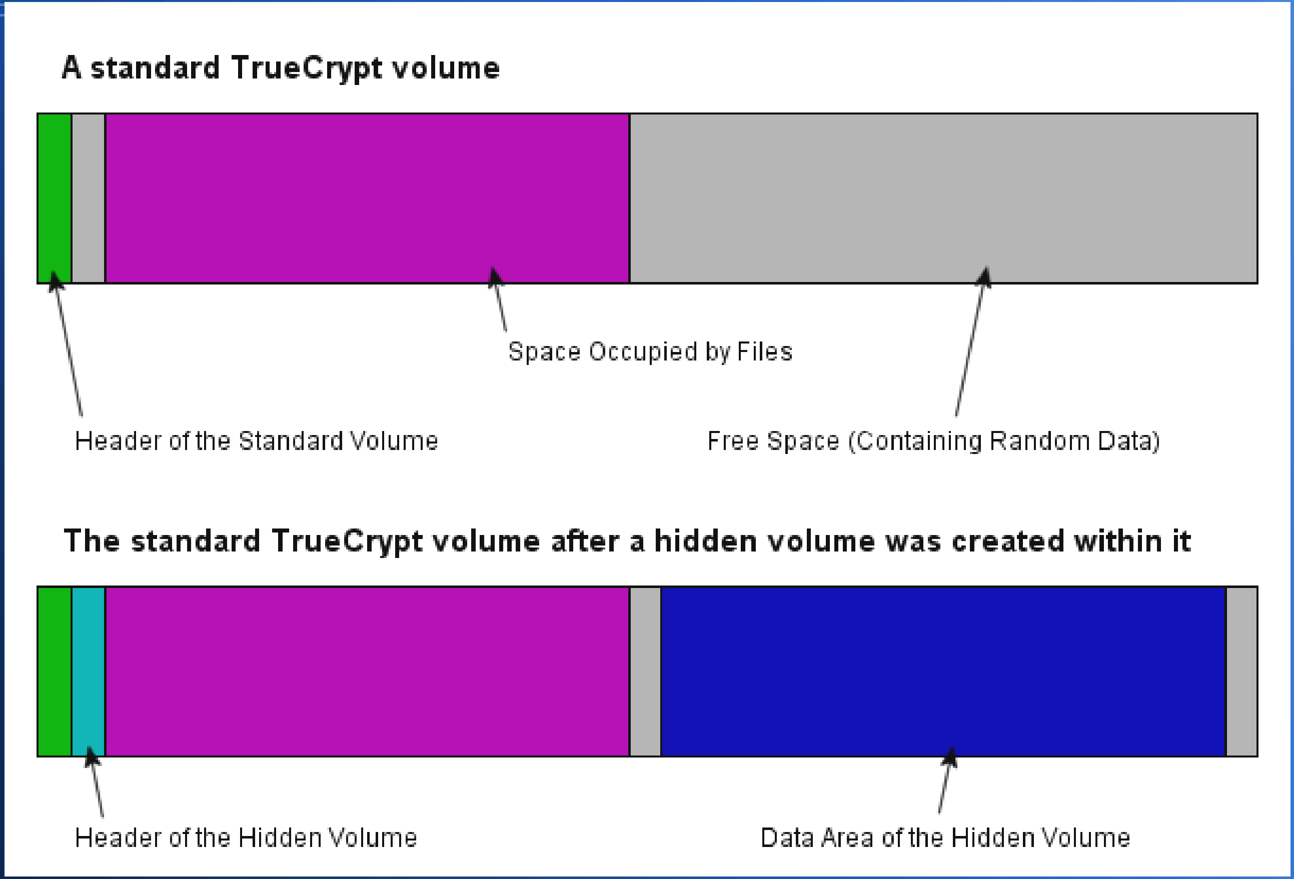
☐ Cache passwords and keyfiles in memory

☑ Display password

☐ Use keyfiles

TrueCrypt sucks

- vfat
- 2 volumes
- fragmentation
- write history


A standard TrueCrypt volume
Space Occupied by Files
Header of the Standard Volume
Free Space (Containing Random Data)
The standard TrueCrypt volume after a hidden volume was created within it
Header of the Hidden Volume
Data Area of the Hidden Volume

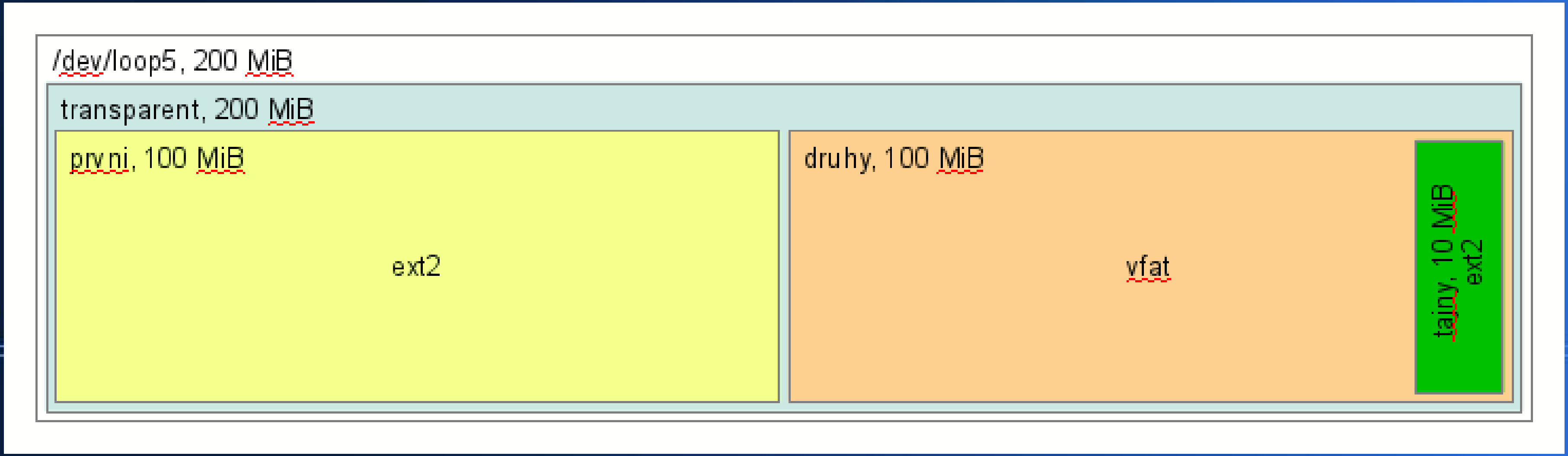
The past

- Rubberhose for Linux 2.0 and 2.2
- StegFS for Linux 2.2
- PhoneBook build 011, Jan 2004

but in Noveber 2011…

DM-Steg

- Imagine a LVM PV, where you cannot list VGs/LVs
  - and they begin to appear when you type passwords
- infinite number of containers
- shuffling
- block stealing



/dev/loop5, 200 MiB

transparent, 200 MiB

prvni, 100 MiB

ext2

druhy, 100 MiB

vfat

tajny, 10 MiB
ext2

Watch out!

- syslog
- /tmp
- recently-used
- …
- → hidden operating system

Other ways of hiding data

- Free part of encrypted LVM PV (losetup -o offset)
- Noise (least significant bit) in WAV/FLAC/RAW photos

Does it help?

No.

(lawful enforcement → maybe)