Protect your data, protect your life.

Data Destruction Day

CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm - *TLP:GREEN*

info@circl.lu

19. September 2015; Windhof

Your data is important ...

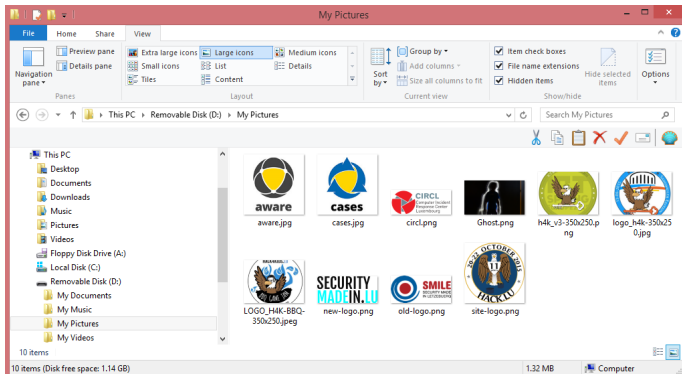- Pictures / Movies $\rightarrow$ it's your life
- Private and business emails $\rightarrow$ it's your job
- Documents $\rightarrow$ it's your information
- Passwords and credentials $\rightarrow$ it's your security
- Online Banking $\rightarrow$ it's your money

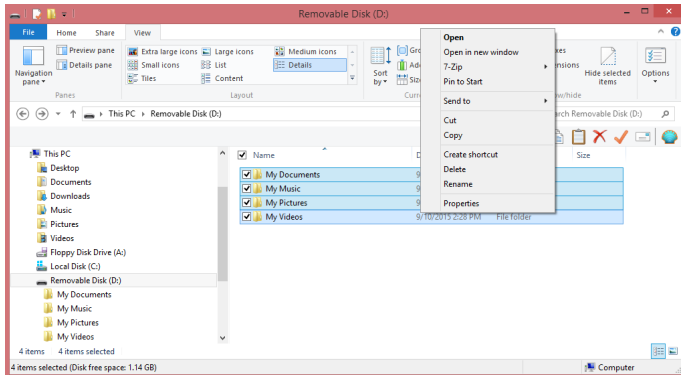$\rightarrow$ ... more important than you may imagin!
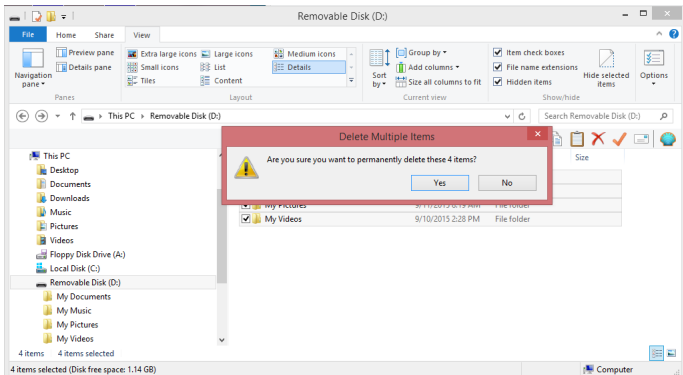
Delete all files

- 1. Connect drive

Delete all files
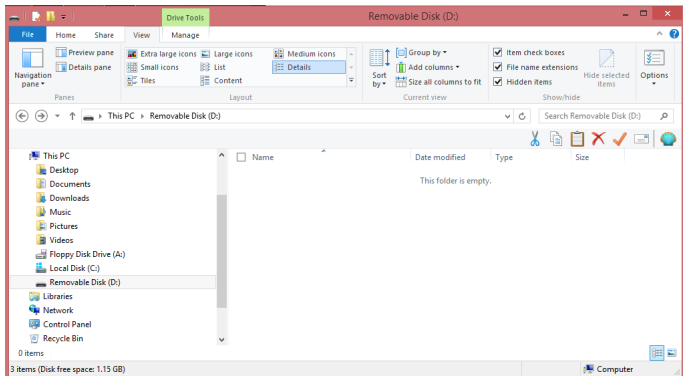
- 2. Select all files to delete

Delete all files

- 3. Confirm to delete all files

Delete all files

- 4. All files are now deleted

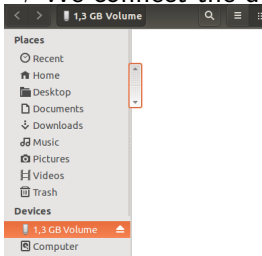**CIRCL**
Computer Incident
Response Center
Luxembourg

- Live exercise: Deleted files
  - → Can we restore some files?
  - → We connect the device with the deleted files:

  - → Looks empty!

Live exercise: Deleted files

```
$ dmesg
...
...
[88758.591351]  sdb: sdb1
[88758.592677] sd 18:0:0:0: [sdb] No Caching mode page found
[88758.592680] sd 18:0:0:0: [sdb] Assuming drive cache: write through
[88758.592681] sd 18:0:0:0: [sdb] Attached SCSI removable disk


$ sudo fls -m / -r /dev/sdb1 > body.txt
$ mactime -b body.txt | less
...
...
Fri Sep 11 2015 10:13:31  980502 m.cb  48  70-128-2 /My Pictures/Ghost.png (deleted)
Fri Sep 11 2015 10:13:56   36047 m.cb  48  71-128-2 /My Pictures/logo_h4k-350x250.jpg (deleted)
Fri Sep 11 2015 10:14:10   32286 m.cb  48  72-128-2 /My Pictures/LOGO_H4K-BBQ-350x250.jpeg (deleted)
...
...
Fri Sep 11 2015 10:16:56   12071 m.cb  48  75-128-2 /My Pictures/circl.png (deleted)
Fri Sep 11 2015 10:18:34    5948 m.cb  48  76-128-2 /My Pictures/cases.jpg (deleted)
Fri Sep 11 2015 10:18:47    5314 m.cb  48  77-128-2 /My Pictures/aware.jpg (deleted)
...
...
```
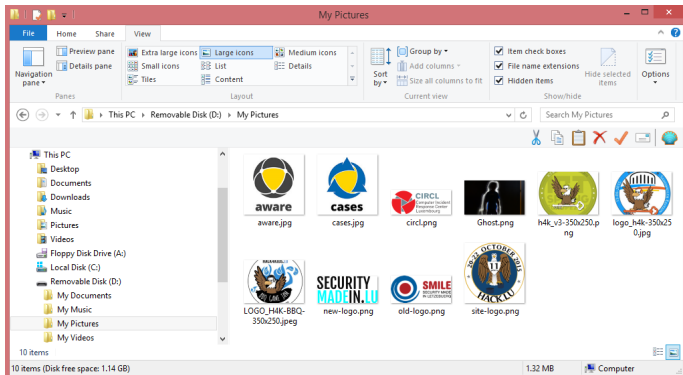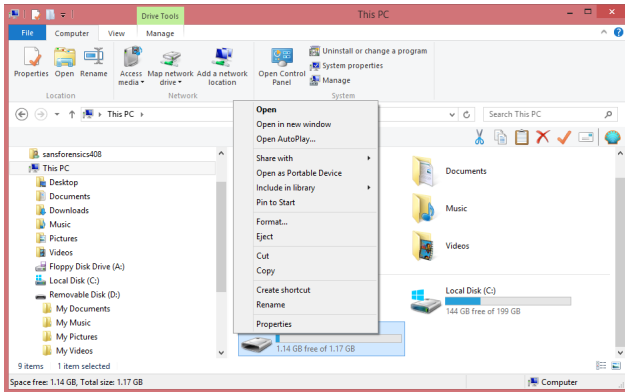
Format hard drive

- 1. Connect drive

Format hard drive

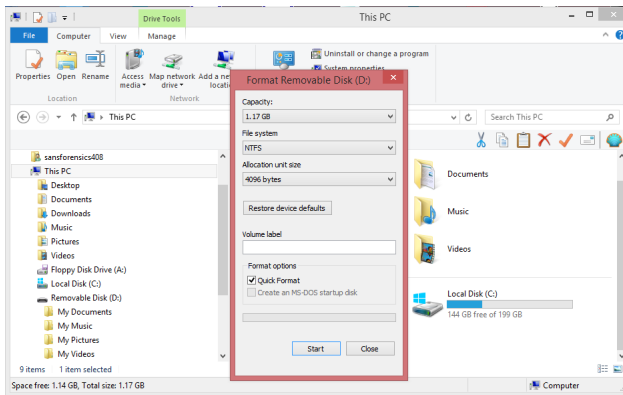- 2. Select drive to be formatted

Format hard drive
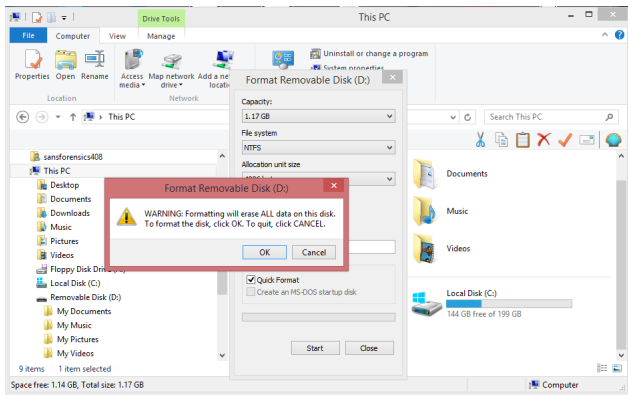
- 3. Format drive

Format hard drive

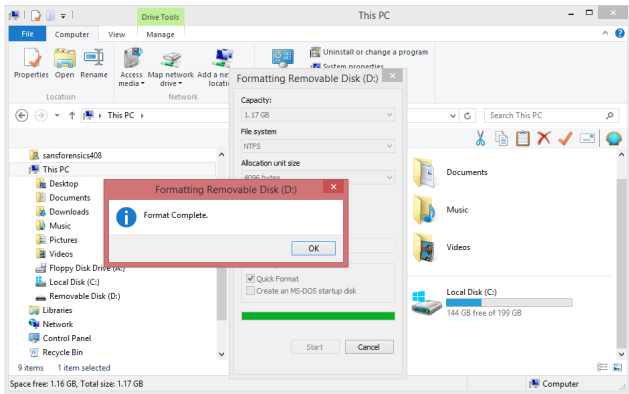- 4. WARNING

Format hard drive

- 5. Format Completed
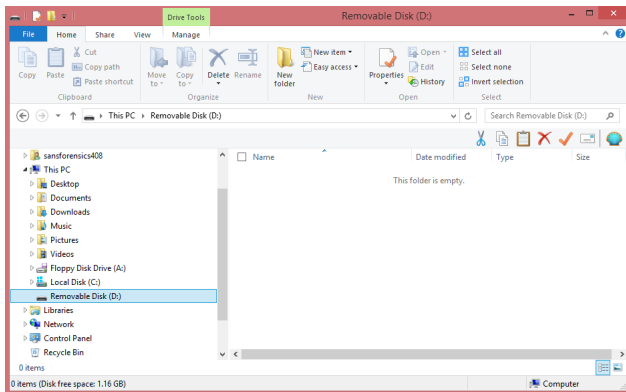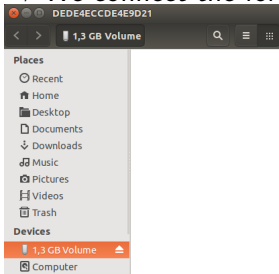
Format hard drive

- 6. We have a fresh formatted drive

- Live exercise: Formated device
  - → Can we restore some files?
  - → We connect the formated device:

  - → Looks empty!

Live exercise: Formated device

```
$ dmesg
...
...
[91701.937115]  sdb: sdb1
[91701.938433] sd 19:0:0:0: [sdb] No Caching mode page found
[91701.938436] sd 19:0:0:0: [sdb] Assuming drive cache: write through
[91701.938437] sd 19:0:0:0: [sdb] Attached SCSI removable disk


$ sudo fls -m / -r /dev/sdb1 > body.txt
$ mactime -b body.txt | less
...
...
Fri Sep 11 2015 14:28:01    262144 macb  0   0-128-6  /$MFT
                              4096 macb  0   1-128-1  /$MFTMirr
                            131072 macb  0   10-128-1 /$UpCase
                                32 macb  0   10-128-4 /$UpCase:$Info
                               448 macb  0   11-144-4 /$Extend
                           5259264 macb  0   2-128-1  /$LogFile
                                 0 macb  0   3-128-3  /$Volume
                              2560 macb  48  4-128-4  /$AttrDef
                             38496 macb  0   6-128-4  /$Bitmap
                              8192 macb  48  7-128-1  /$Boot
...
...
```

Live exercise: Formated device

```
$ sudo photorec /d /output
```



```
PhotoRec 6.14, Data Recovery Utility, July 2013
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/sdb - 8103 MB / 7728 MiB (RO) - USB Flash DISK
     Partition              Start        End   Size in sectors
 1 P HPFS - NTFS            0  33  3   159  20 53   2463745


Pass 1 - Reading sector    2097554/2463745, 32 files found
Elapsed time 0h00m50s - Estimated time to completion 0h00m08
txt: 18 recovered
png: 6 recovered
jpg: 4 recovered
mp3: 2 recovered
pdf: 2 recovered
```
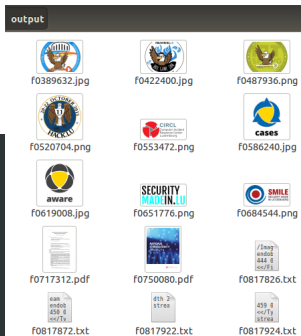
How does this work?

```
file1.txt = "123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ"
file2.txt = "1111111111222222222233333333334444444444555555555"

    Content              Metadata            Filename table
-----------------    -----------------      -----------------
.. | ............ |  .. |               |    | file1.txt = 6 |
50 | 45555555555.. |  2 |               |    | file2.txt = 8 |
51 | ............ |   3 |               |    |               |
52 | 123456789ABCD |  4 |               |    |               |
53 | EFGHIJKLMNOPQ |  5 |               |    |               |
54 | RSTUVWXYZ.... |  6 | Timestamps,   |    |               |
55 | ............ |     | Owner, Rights |    |               |
56 | 3333444444444 |    | 52,53,54      |    |               |
.. | ............ |   7 |               |    |               |
.. | ............ |   8 | Timestamps,   |    |               |
84 | 1111111111222 |    | Owner, Rights |    |               |
85 | 2222222333333 |    | 84,85,56,50   |    |               |
.. | ............ |  .. |               |    |               |
-----------------    -----------------      -----------------
```

How does this work?

- Delete all files
  - Filename table: Filename is tagged as deleted
  - Meta data: Data units are tagged as not allocated
  - Data units: Data on disk are not deleted
    Data units: At some point in time they may get overwritten
  - Recovery: Meta data and Data units could be recovered

- Format hard drive
  - Filename table: Filename table is renewed
  - Meta data: Meta data structure is renewed
  - Data units: Data on disk are not deleted
    Data units: At some point in time they may get overwritten
  - Recovery: Data units could be recovered

Protect your data, protect your life

- Encrypt sensitive data / Full disk encryption
  (TrueCrypt, PGP, Safeboot, Bitlocker)
- Hardware encrypted drive
- Wipe out files / Wipe out drives
- Educate yourself
  https://www.privacysalon.lu/
- Physically destroy your drive