Protect your data, protect your life.

JOURNÉE - #CYBERSECURITY4SUCCESS

CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm *TLP:WHITE*

info@circl.lu

03. October 2016; Chambre de Commerce Luxembourg

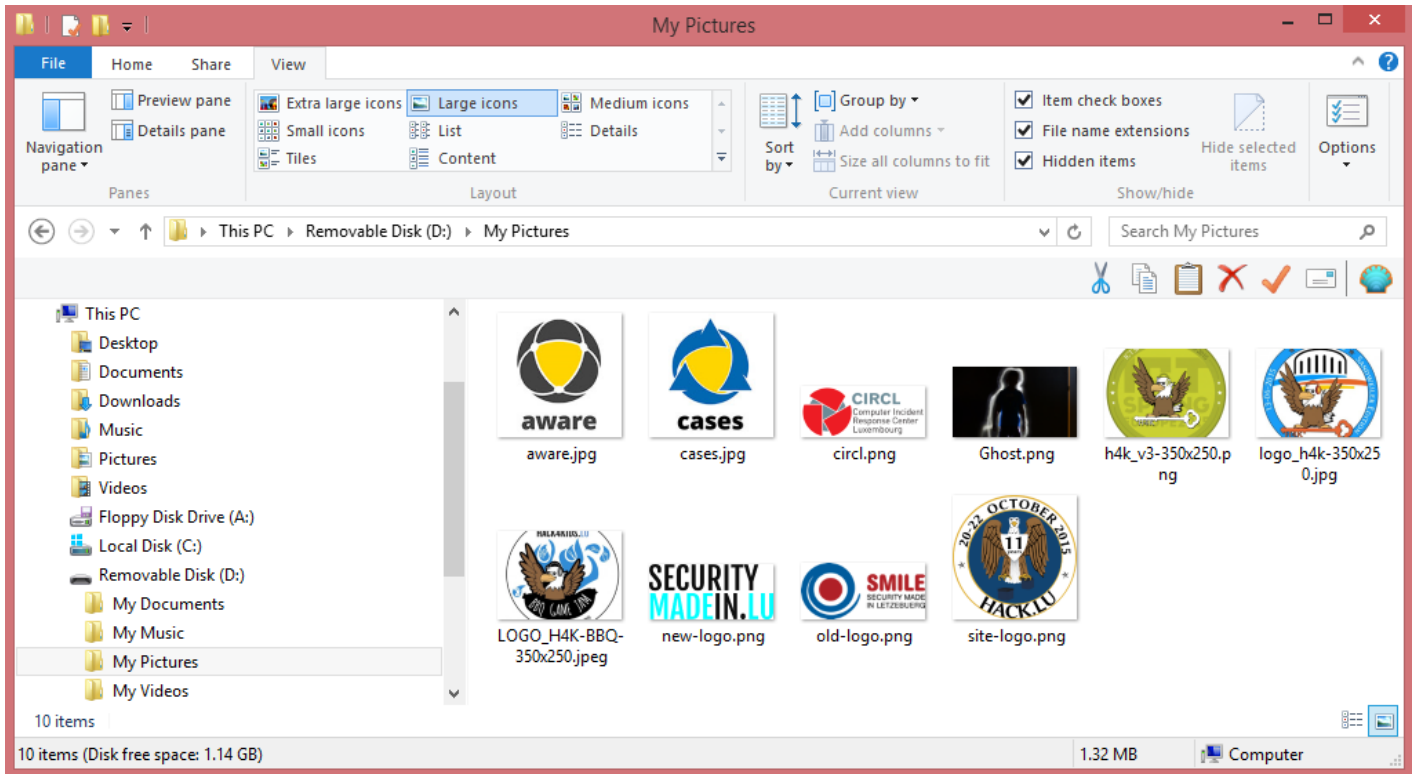
Your data is important ...

- 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 imagine!
At one point in time you may give away one of your devices.

Filesystem

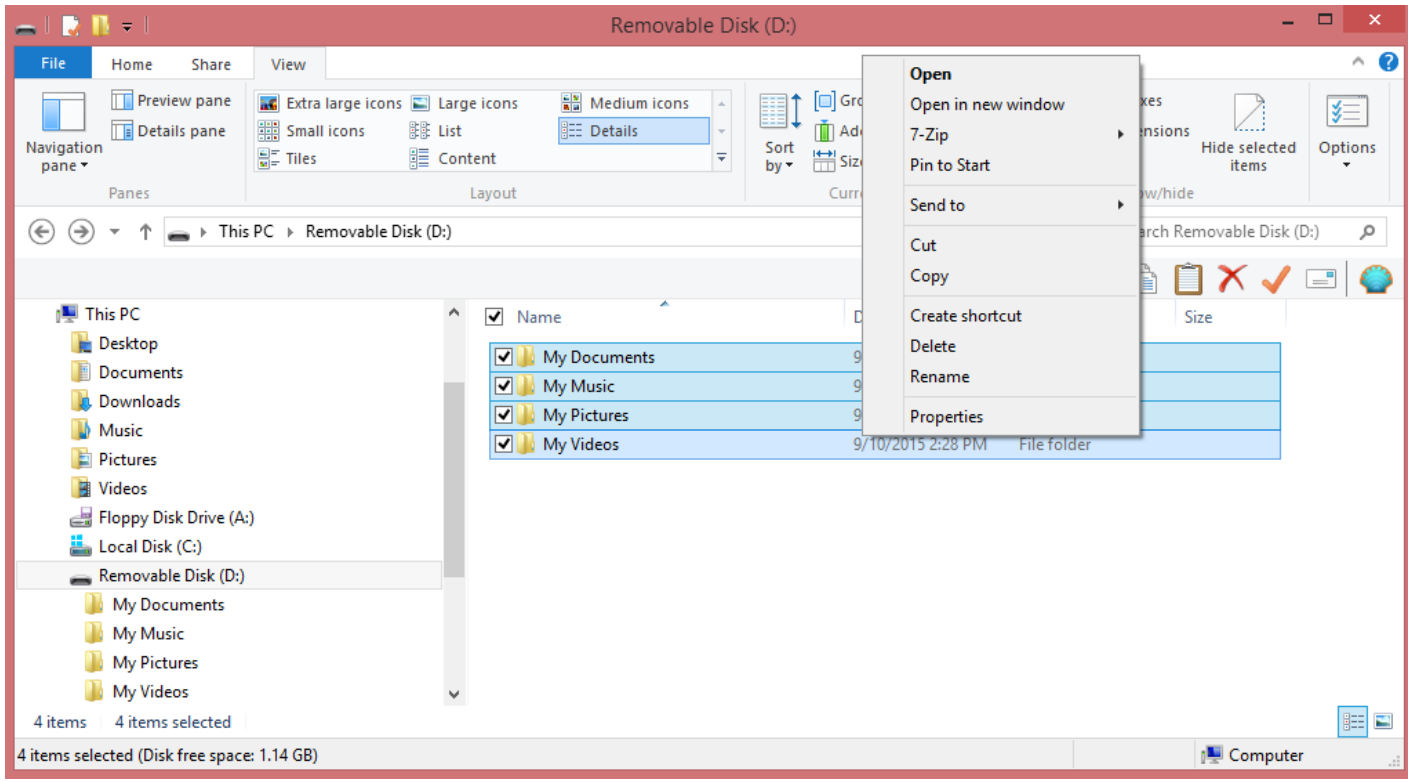
What is a filesystem?



Filesystem

Physical disk, partition, filesystem

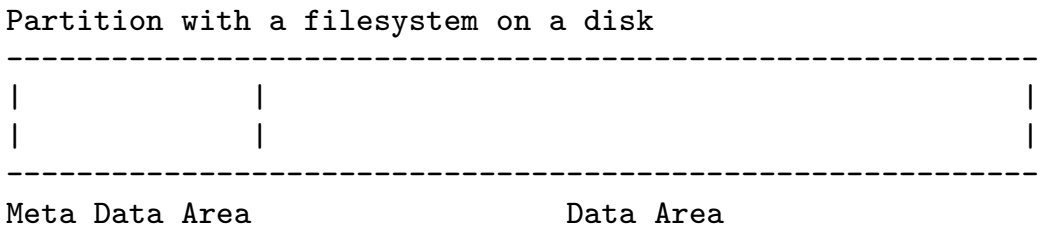
Examples: FAT32, VFAT, NTFS, EXTx...



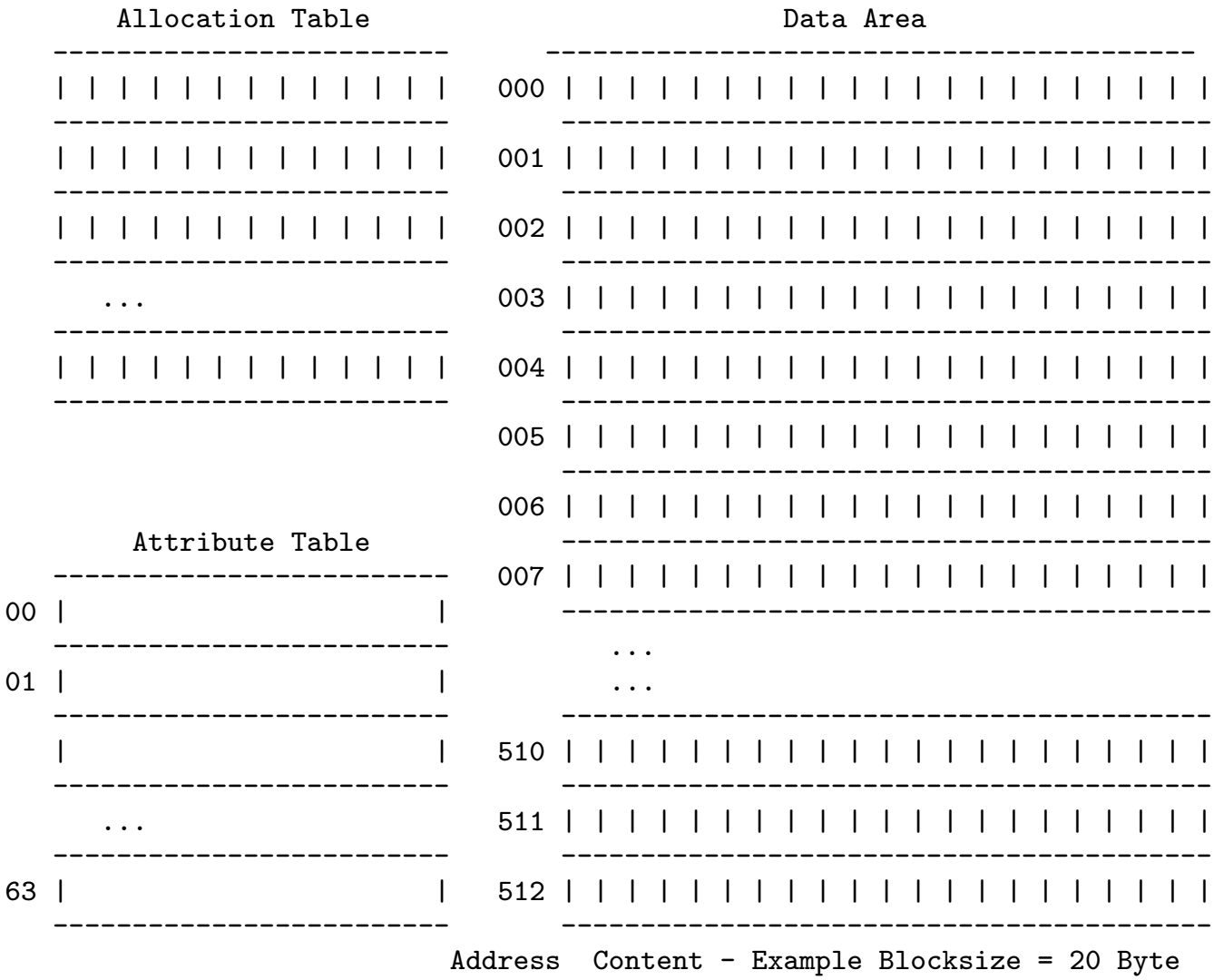
Filesystem

How it works in general?

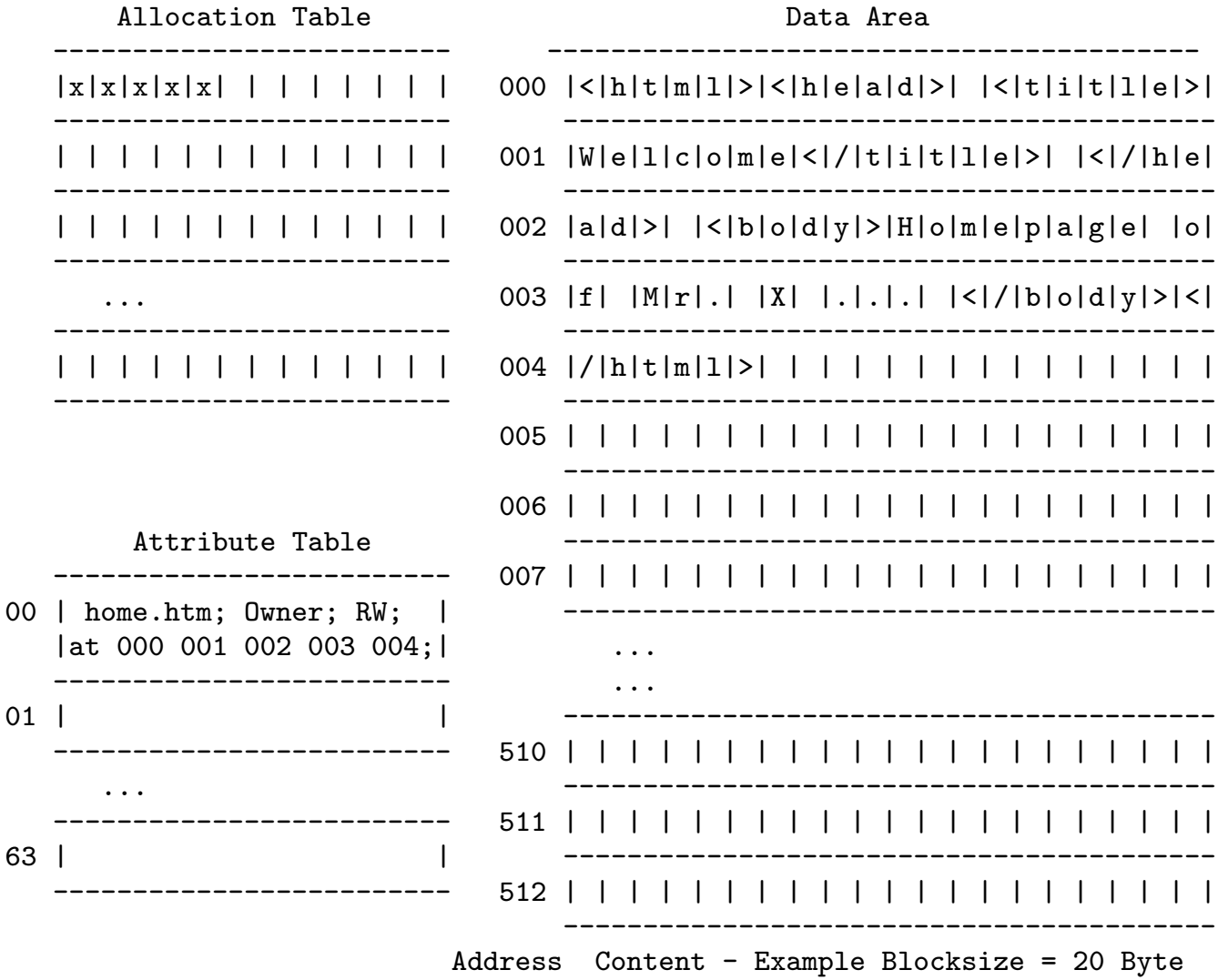
An extremly simplyfied model.



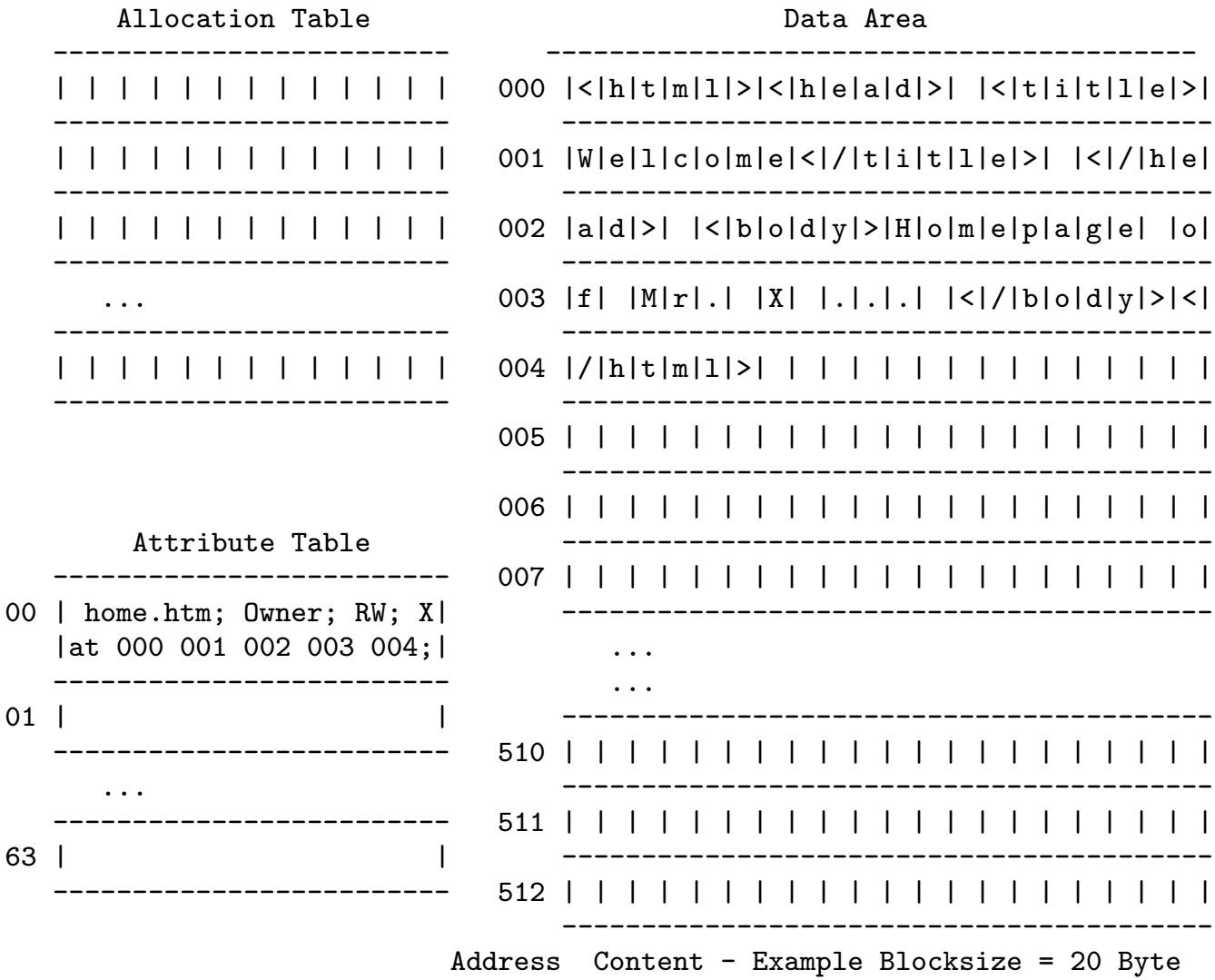
Filesystem


Allocation Table
Data Area
Attribute Table
00
01
63
000
001
002
003
004
005
006
007
510
511
512
Address Content - Example Blocksize = 20 Byte

Filesystem - Storing a file - home.htm

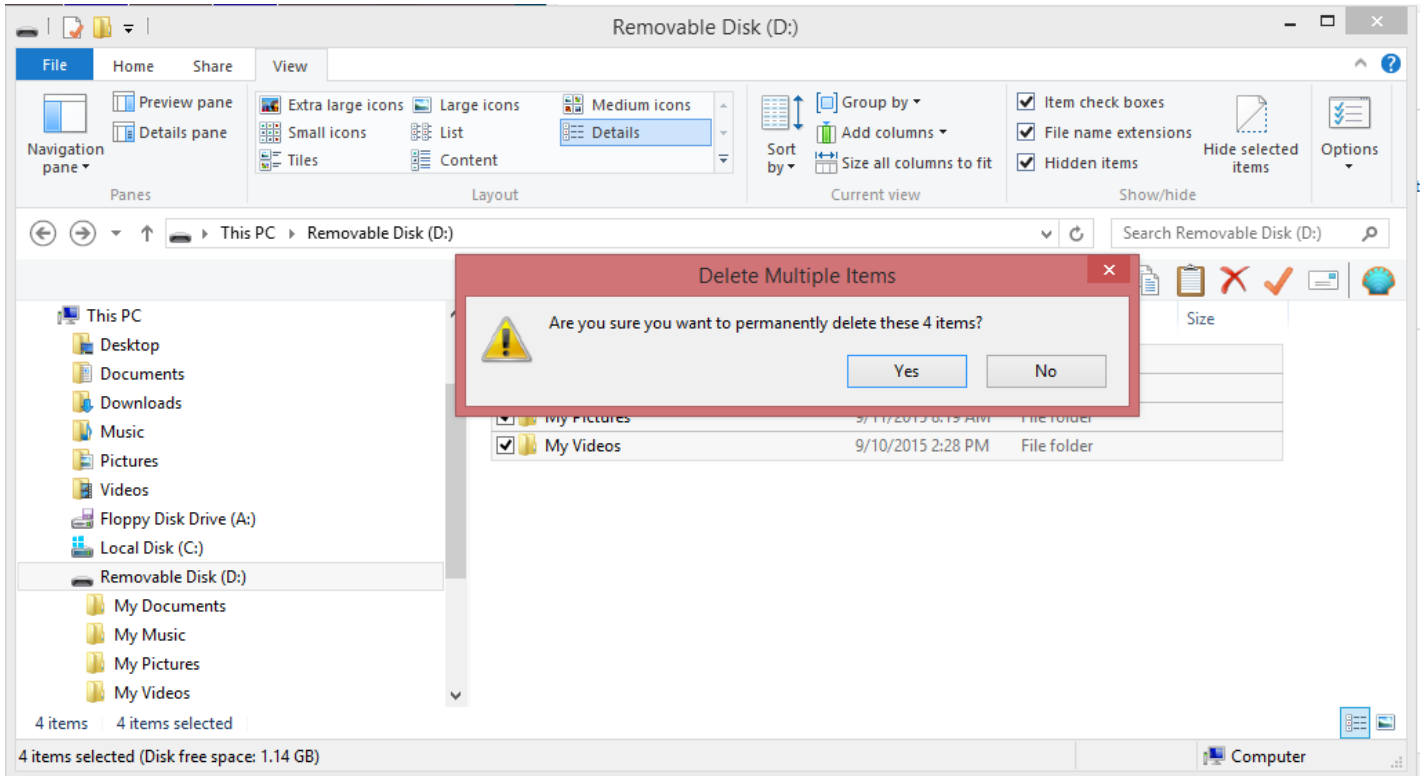


Filesystem - Deleting a file - home.htm



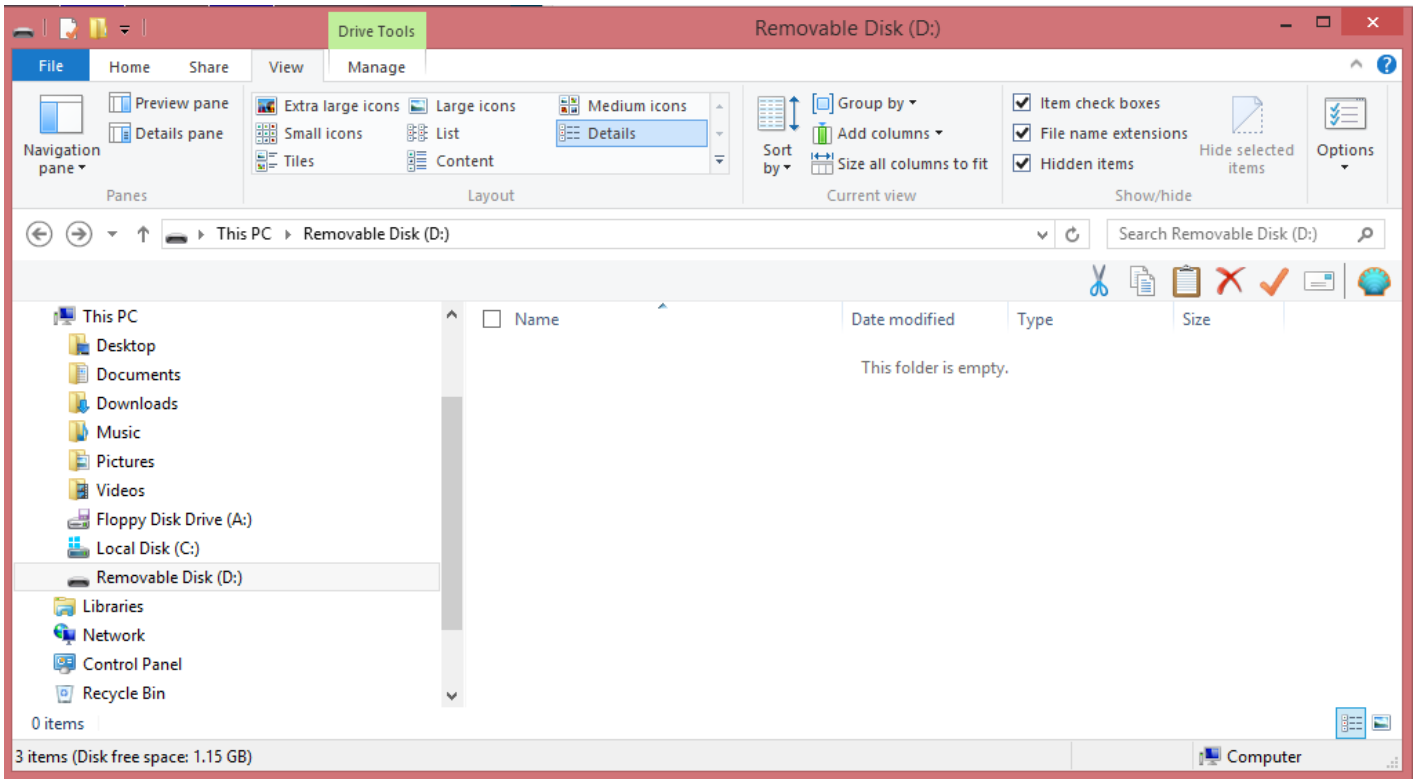
Exercise: Deleting files

Confirm to delete all files



Exercise: Deleting files

Files deleted



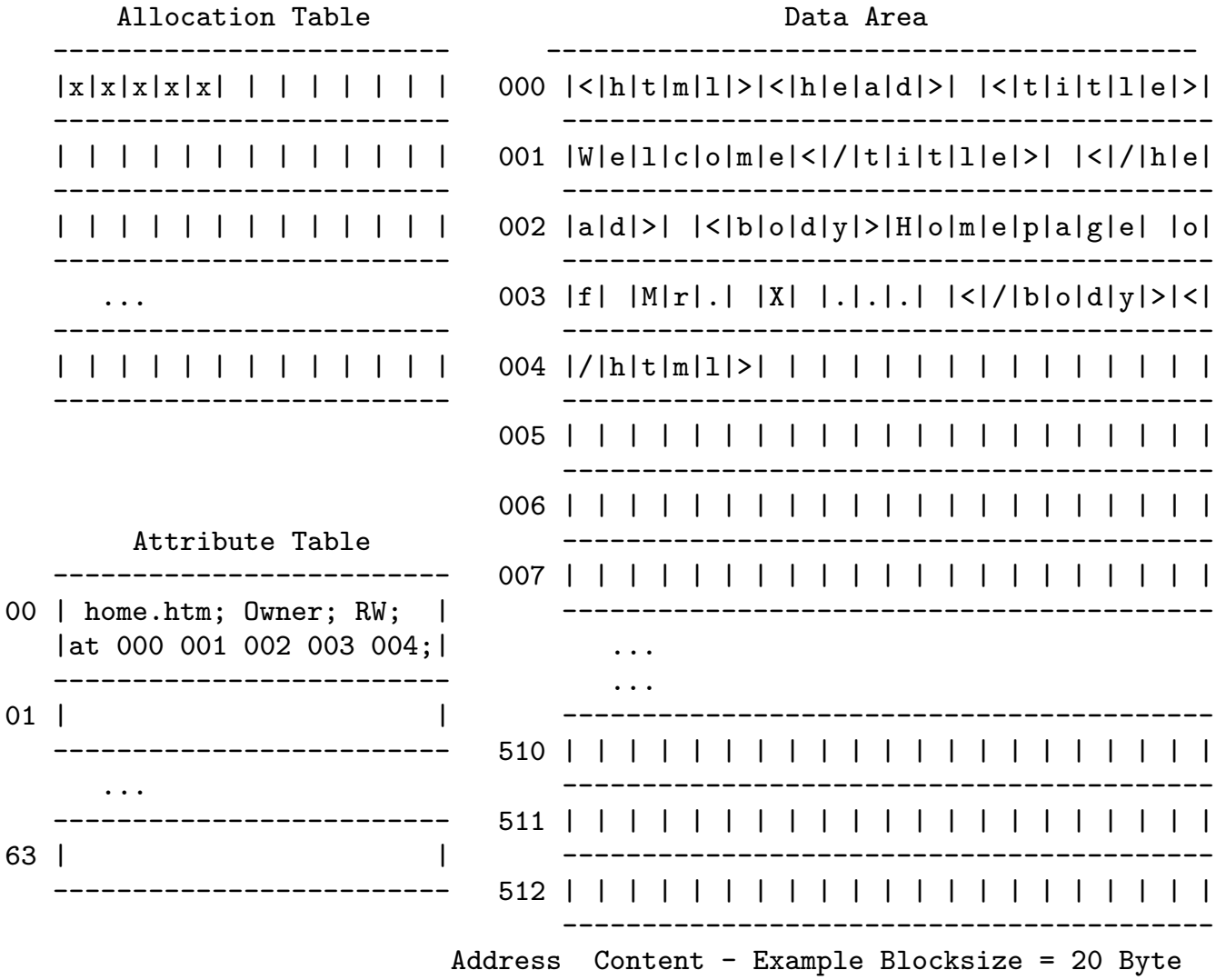
CIRCL
Computer Incident
Response Center
Luxembourg

- Live exercise: Recover deleted files

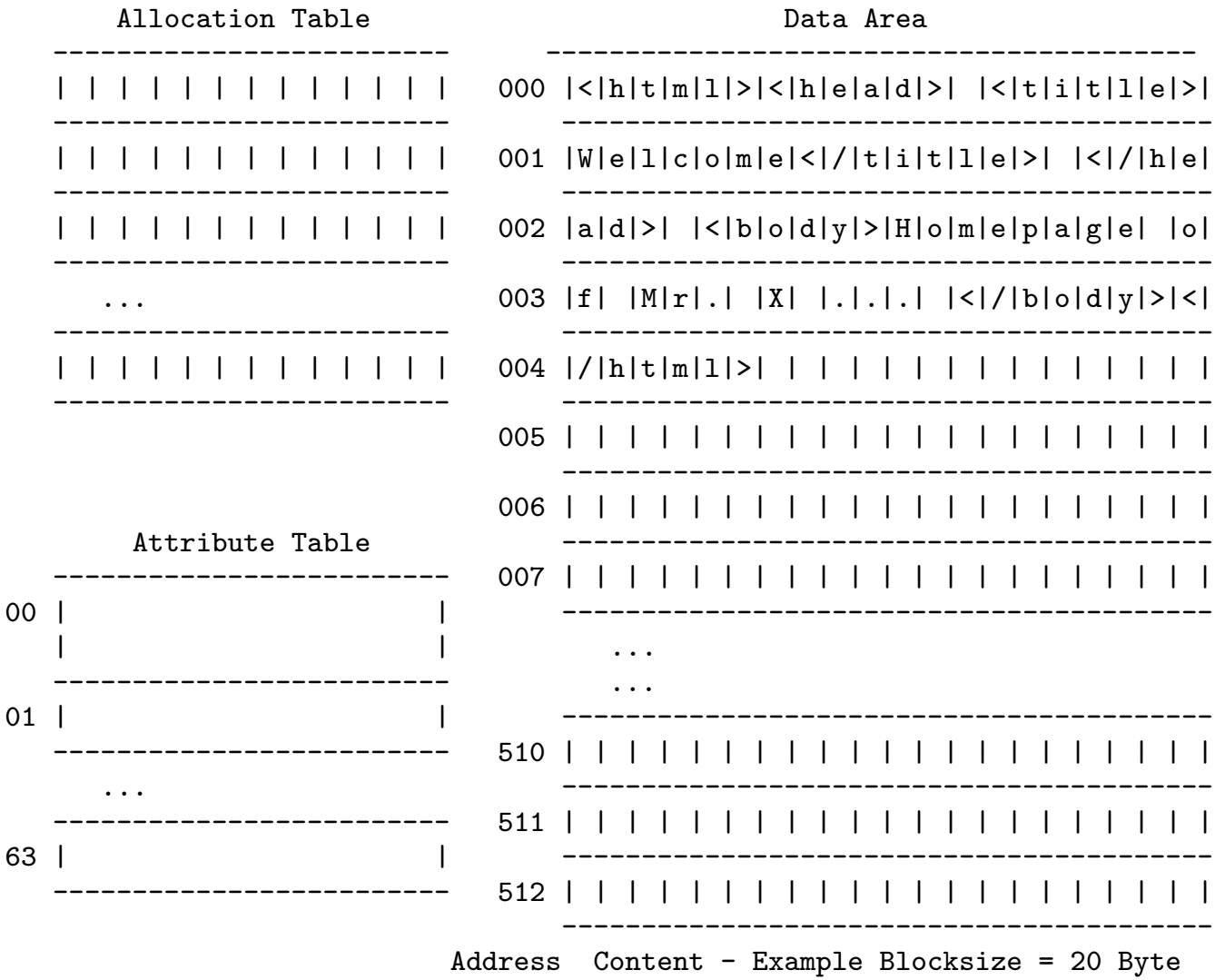
Live exercise: Recover deleted files

```
# dmesg
...
[28095.196673]  sdc: sdc1
[28095.197992] sd 20:0:0:0: [sdc] No Caching mode page found


# fls -m / -r /dev/sdc1 > body.txt
# mactime -b body.txt | less
...
Tue Oct 04 2016 11:41:10     48 ...b   64-144-2 /My Documents (deleted)
                            476 macb   67-128-2 /My Documents/H4K.txt (deleted)
                         501741 macb   68-128-2 /My Documents/LU_NCSS_2_EN_booklet.pdf (deleted)
                             48 macb   69-144-2 /My Music (deleted)
                             48 ...b   70-144-2 /My Pictures (deleted)
                           5314 macb   71-128-2 /My Pictures/aware.jpg (deleted)
                           5948 macb   72-128-2 /My Pictures/cases.jpg (deleted)
                          12071 macb   73-128-2 /My Pictures/circl.png (deleted)
                          ...

# istat /dev/sdc1 73
                  MFT Entry Header Values:
                  Entry: 73        Sequence: 2
                  ...
                  Attributes:
                  ...
                  Type: $DATA (128-2)   Name: N/A   Non-Resident   size: 12071  init_size: 12071
                  3838 3839 3840 3841 3842 3843

# icat /dev/sdc1 73 > circl.png
```

Filesystem - Storing a file - home.htm

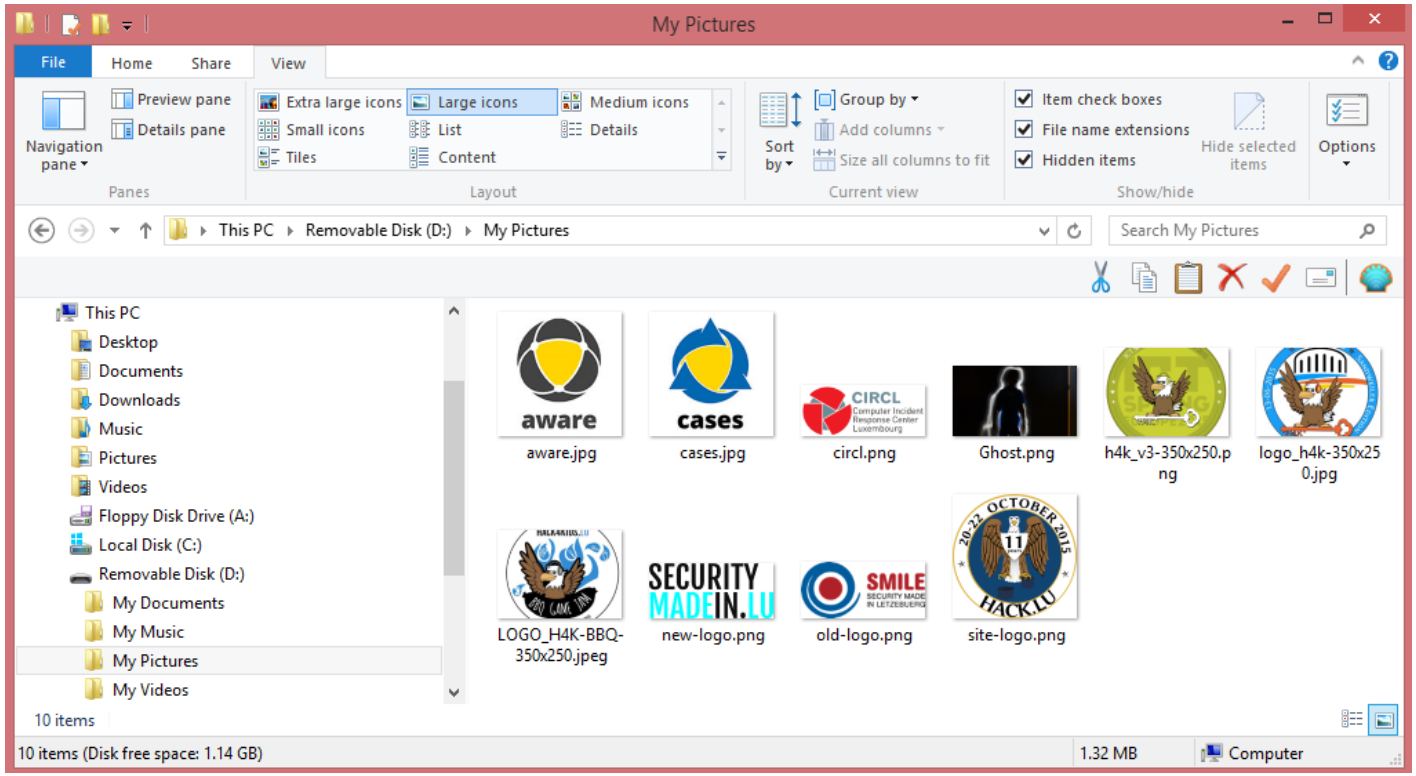


Filesystem - Formating a partition



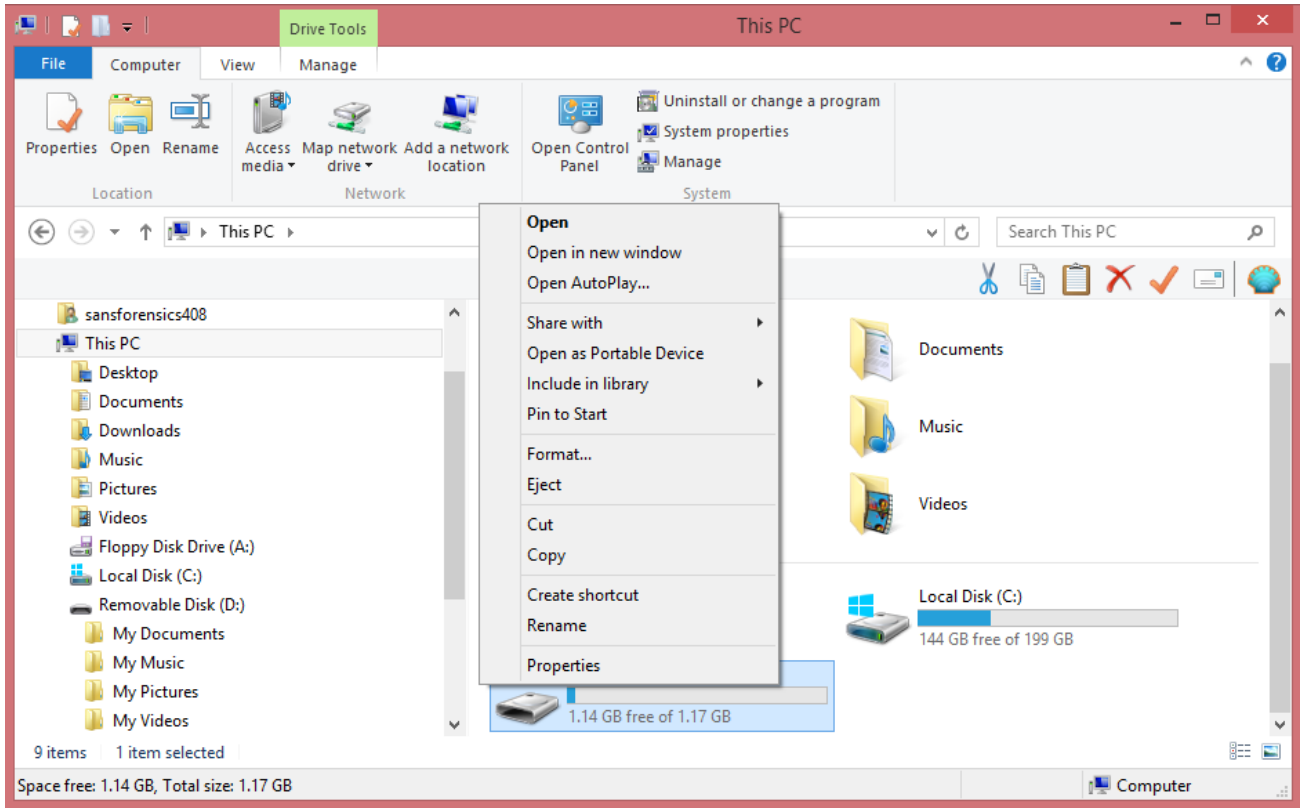
Exercise: Formating a partition

Connect drive.



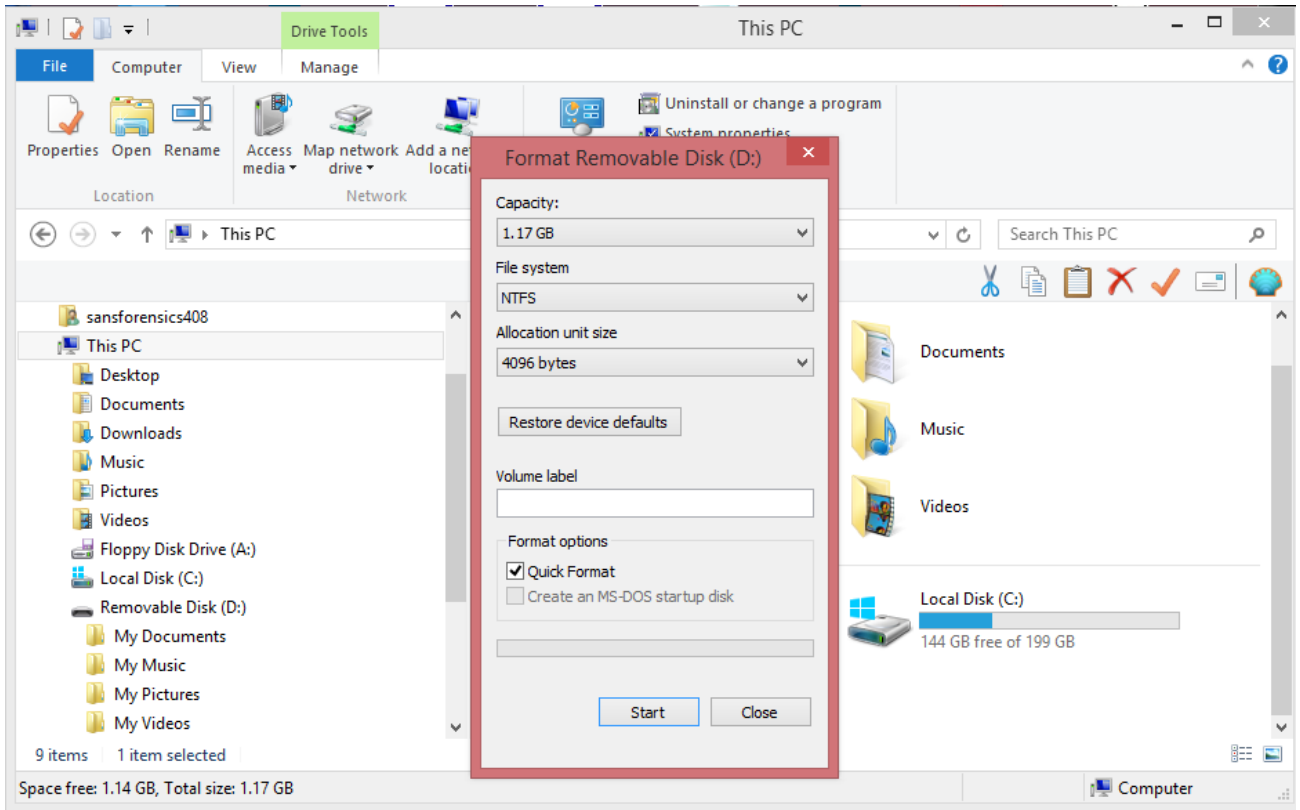
Exercise: Formating a partition

Select the partition to be formatted.



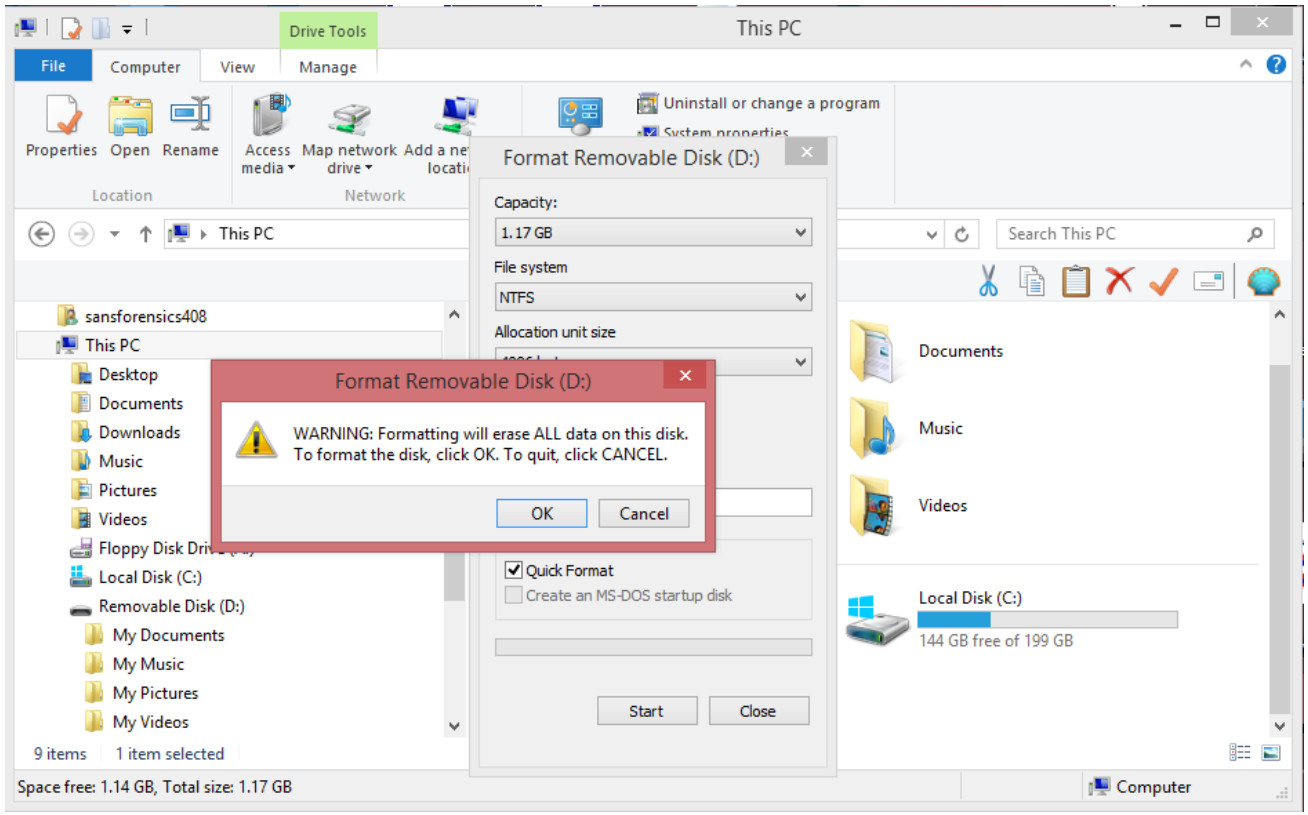
Exercise: Formating a partition

Formating...



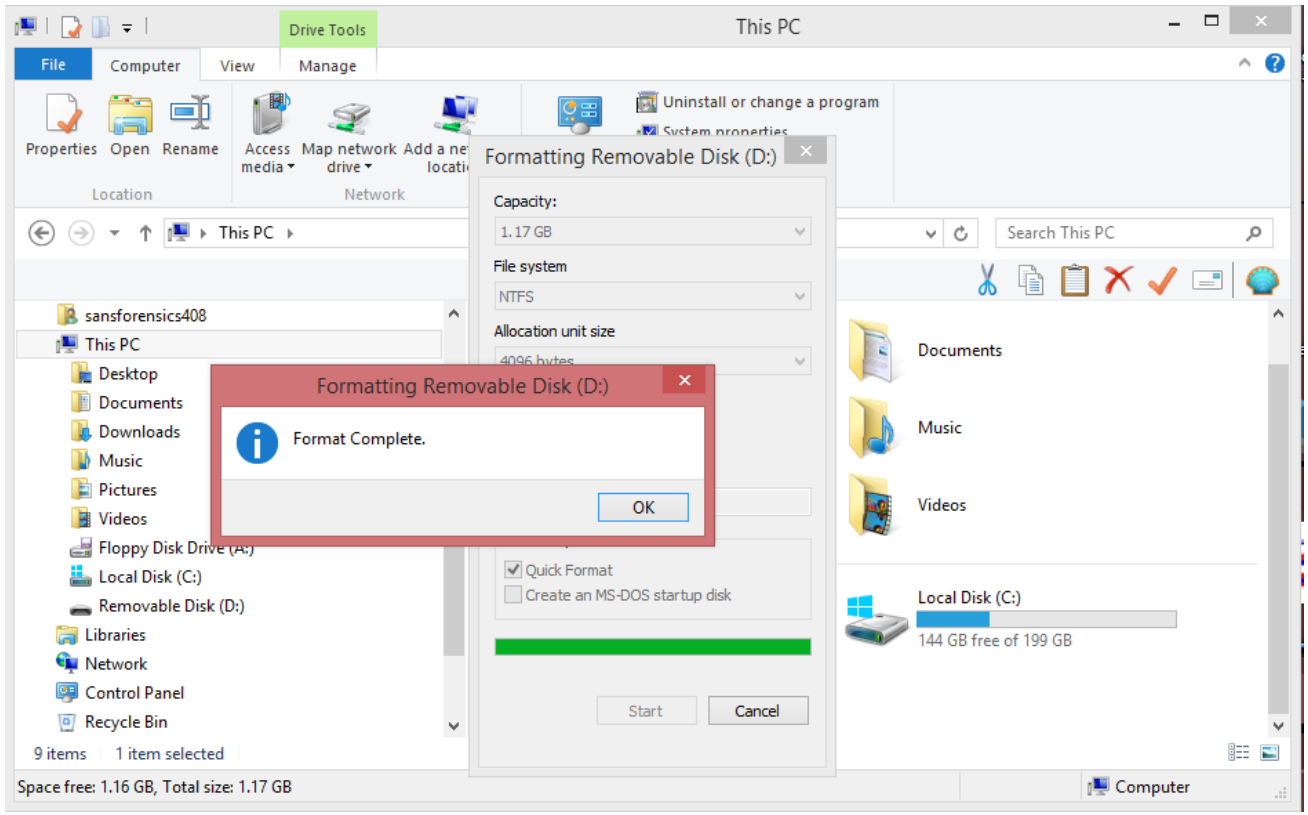
Exercise: Formating a partition

Uuuhhhhhhh a "WARNING"



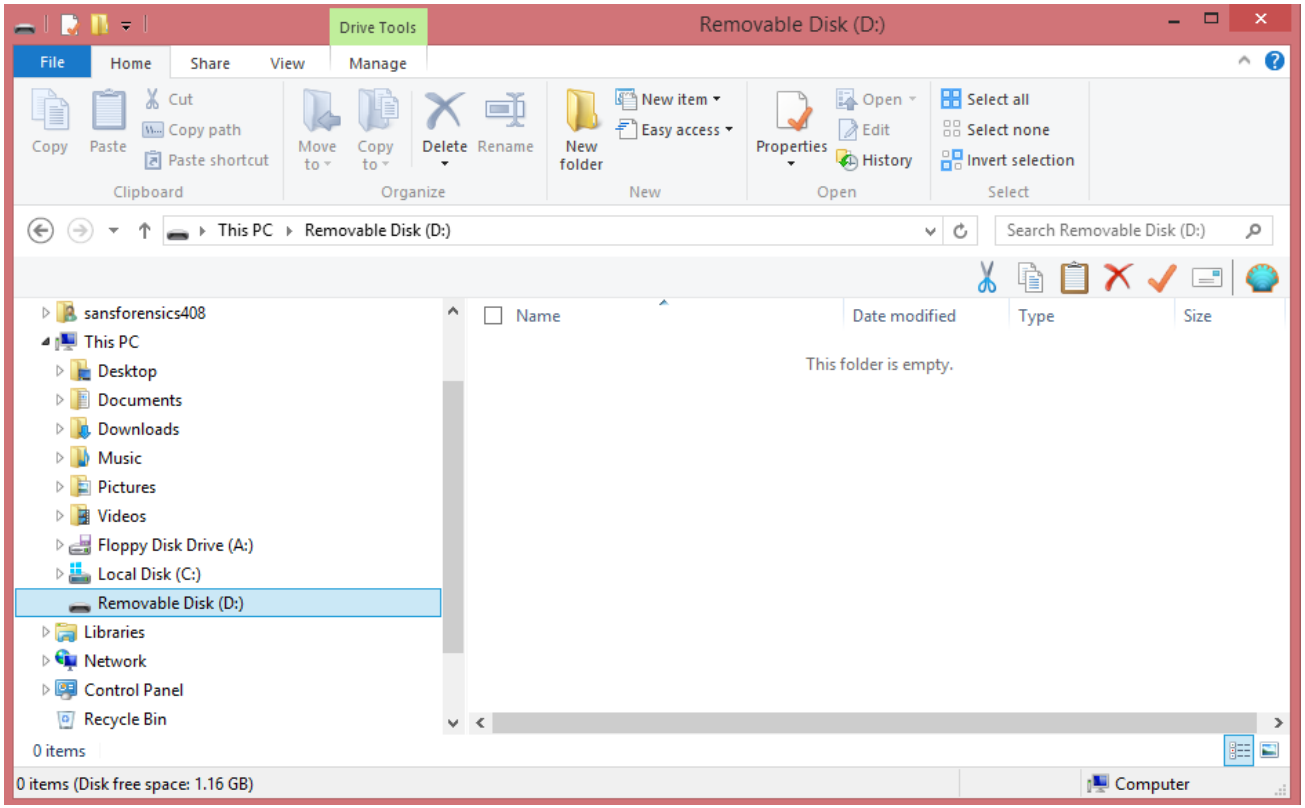
Exercise: Formating a partition

Format Complete.



Exercise: Formating a partition

We have a freshly formatted drive.



CIRCL
Computer Incident
Response Center
Luxembourg

- Live Exercise: Recover files

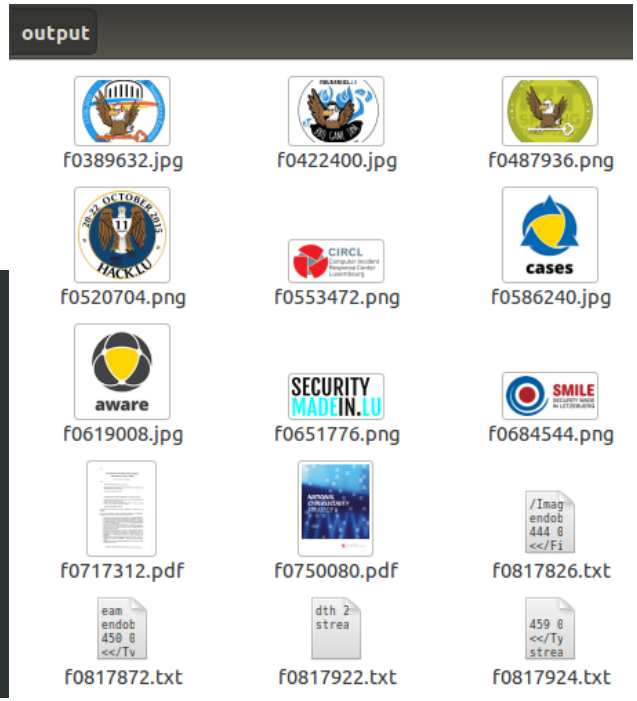
Live Exercise: Recover files

```
# dmesg
...
...
        [29032.416556]  sdc: sdc1
        [29032.417931] sd 21:0:0:0: [sdc] No Caching mode page found


# fls -m / -r /dev/sdc1 > body.txt
# mactime -b body.txt | less

        Tue Oct 04 2016 16:21:54    27648 macb    0-128-1  /$MFT
                                     4096 macb    1-128-1  /$MFTMirr
                                   131072 macb   10-128-1 /$UpCase
                                       32 macb   10-128-2 /$UpCase:$Info
                                      344 macb   11-144-2 /$Extend
                                        0 macb   16       /$OrphanFiles/OrphanFile-16 (deleted)
                                        0 macb   17       /$OrphanFiles/OrphanFile-17 (deleted)
...



        # photorec /dev/sdc1

        Carving ;-)
```

Live Exercise: Recover files

File Signatures / Magic Numbers / Magic Bytes

```
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
```



Summary

- Deleting files
  - Metadata stay on disk for a while;
  - Data stay on disk for a while;
  - Unallocated blocks get overwritten once;
  - Good chances to recover files for a while;
- Formating a partition
  - Metadata structures are renewed;
  - Data stay on disk for a while;
  - Blocks are unallocated and get overwritten once;
  - Good chances to recover files on frech formated units;

Protect your data, protect your life

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