

Protect your data, protect your life.  
JOURNÉE - #CYBERSECURITY4SUCCESS



**CIRCL**  
Computer Incident  
Response Center  
Luxembourg

Michael Hamm *TLP:WHITE*

[info@circl.lu](mailto:info@circl.lu)

03. October 2016; Chambre de  
Commerce Luxembourg

## Your data is important ...

---

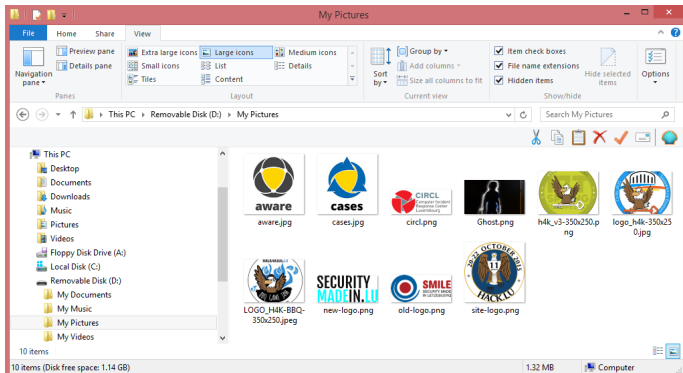
- Pictures / Movies → it's your life
- Private and business emails → it's your job
- Documents → it's your information
- Passwords and credentials → it's your security
- Online Banking → it's your money

→ ... more important than you may imagine!

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

# Filesystem

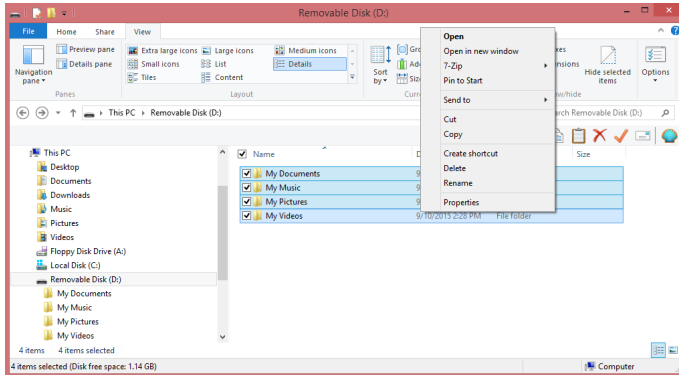
What is a filesystem?



# Filesystem

Physical disk, partition, filesystem

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



# Filesystem

---

How it works in general?

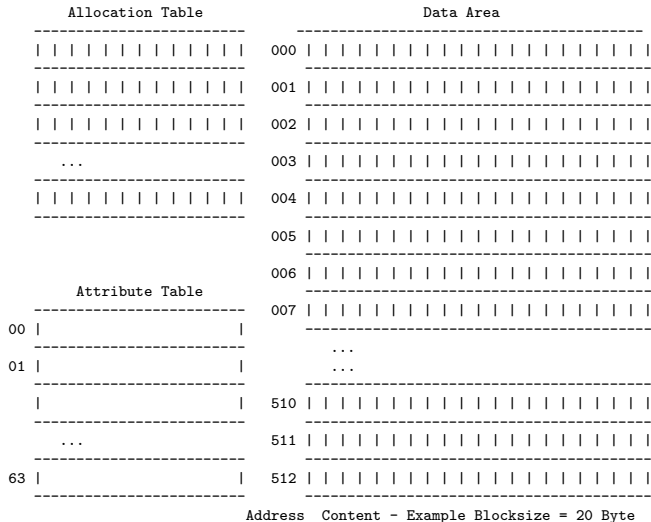
An extremely simplified model.

Partition with a filesystem on a disk



# Filesystem

---



# Filesystem - Storing a file - home.htm

Allocation Table		Data Area	
-----	x x x x x	000	< h t m l > < h e a d >   < t i t l e >
-----		001	W e l l c o m e < / t i t l e >   < / h e
-----		002	a d >   < b o d y > H o m e p l a g e   o
-----	...	003	f   M r .  X   . . .  < / b o d y > <
-----		004	/ h t m l >
-----		005	
-----		006	
-----		007	
-----		...	...
-----		...	...
-----		510	
-----		511	
-----		512	
-----			

Attribute Table	
00	home.htm; Owner; RW;    at 000 001 002 003 004;
01	
...	
63	

Address Content - Example Blocksize = 20 Byte

# Filesystem - Deleting a file - home.htm

Allocation Table		Data Area	
	-----	000	< h t m l > < h e a d >   < t i t l e >
	-----	001	W e l l c o m e < / t i t l e >   < / h e
	-----	002	a d >   < b o d y > H o m e p a g e   o
...	-----	003	f   M r .  X   . . .  < / b o d y > <
	-----	004	/ h t m l >
	-----	005	
	-----	006	
	-----	007	
	-----	...	...
	-----	...	...
Attribute Table			
00   home.htm; Owner; RW; X	-----		
at 000 001 002 003 004;	-----		
01	-----	510	
...	-----	511	
63	-----	512	

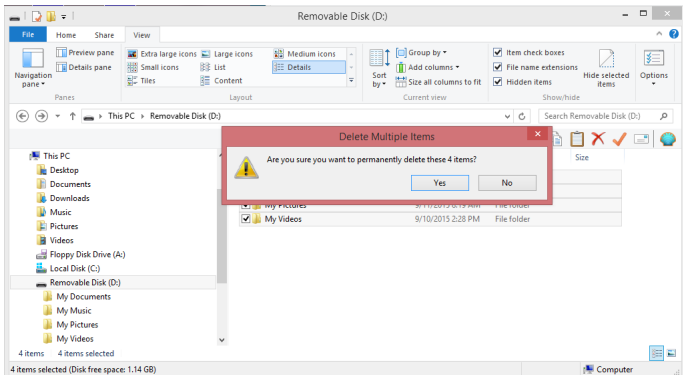
Address Content - Example Blocksize = 20 Byte



# Exercise: Deleting files

---

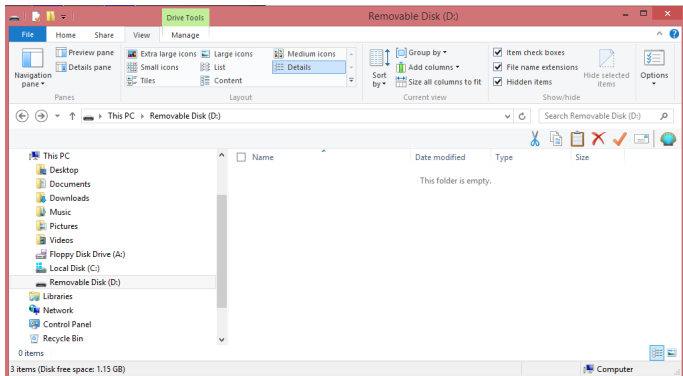
Confirm to delete all files



# 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
```

```
12 of 25# icat /dev/sdc1 73 > circl.png
```

# Filesystem - Storing a file - home.htm

Allocation Table		Data Area	
-----	x x x x x	000	< h t m l > < h e a d >   < t i t l e >
-----		001	W e l l c o m e < / t i t l e >   < / h e
-----		002	a d >   < b o d y > H o m e p a g e   o
-----	...	003	f   M r .  X   . . .  < / b o d y > <
-----		004	/ h t m l >
-----		005	
-----		006	
-----		007	
-----		...	...
-----		...	...
-----		510	
-----		511	
-----		512	
-----			

Attribute Table	
00	home.htm; Owner; RW;    at 000 001 002 003 004;
01	
...	
63	

Address Content - Example Blocksize = 20 Byte

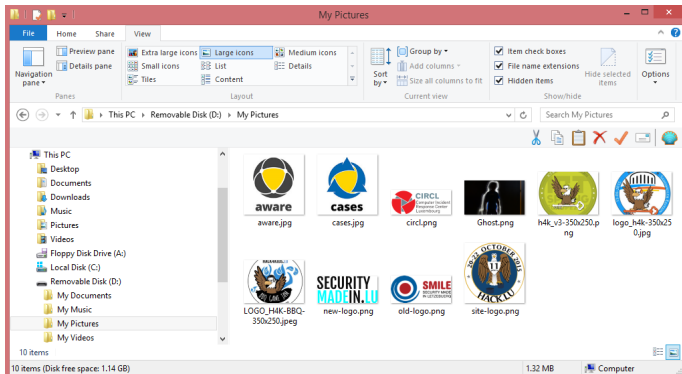
# Filesystem - Formating a partition

Allocation Table		Data Area	
		000	< h t m l > < h e a d >   < t i t l e >
		001	W e l l c o m e < / t i t l e >   < / h e
		002	a d >   < b o d y > H o m e p a g e   o
...		003	f   M r .  X   . . .  < / b o d y > <
		004	/ h t m l >
		005	
		006	
		007	
		...	...
		...	...
		510	
		511	
		512	
Attribute Table			
00			
01			
...			
63			

Address Content - Example Blocksize = 20 Byte

# Exercise: Formatting a partition

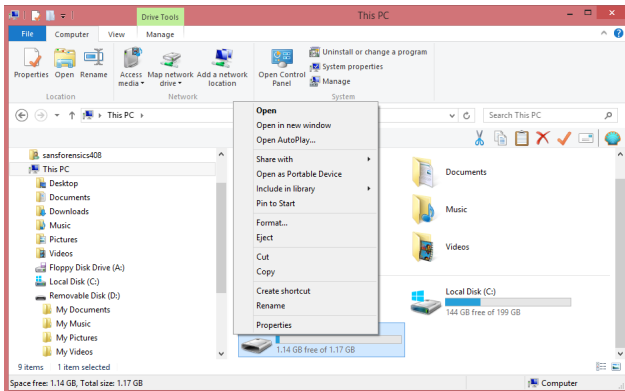
Connect drive.



# Exercise: Formatting a partition

---

Select the partition to be formatted.

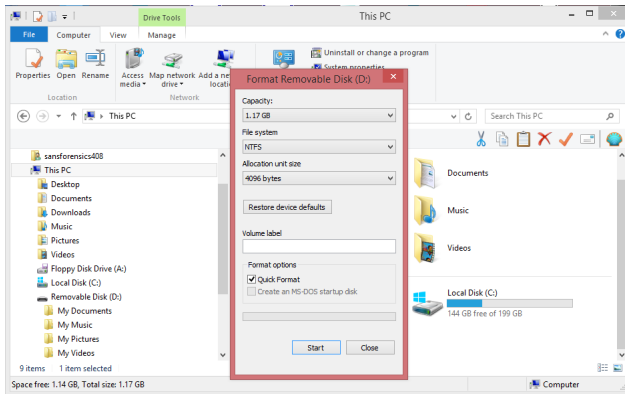




# Exercise: Formatting a partition

---

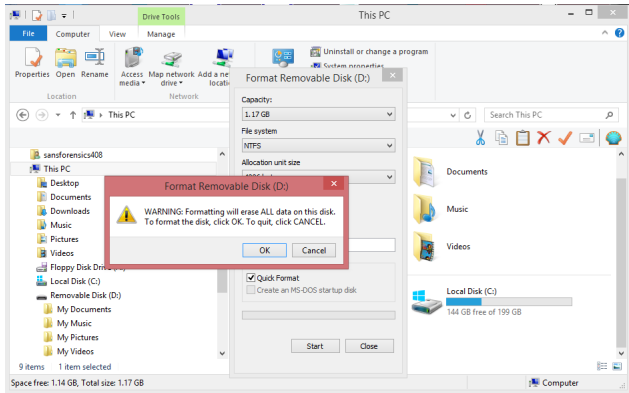
Formatting...



# Exercise: Formatting a partition

---

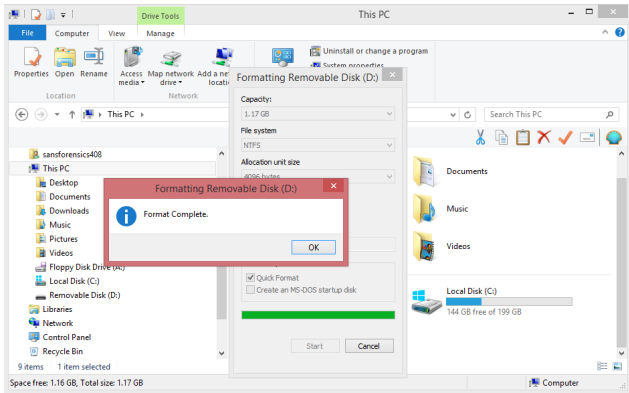
Uuuhhhhhh a "WARNING"



# Exercise: Formatting a partition

---

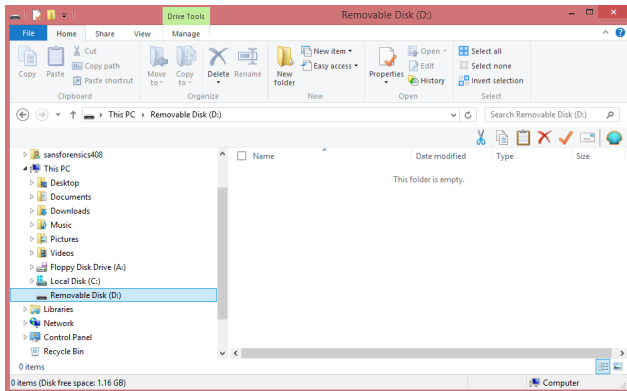
Format Complete.



# Exercise: Formatting 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
```

output



f0389632.jpg



f0422400.jpg



f0487936.png



f0520704.png



f0553472.png



f0586240.jpg



f0619008.jpg



f0651776.png



f0684544.png



f0717312.pdf



f0750080.pdf



f0817826.txt



f0817872.txt



f0817922.txt



f0817924.txt

# 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;
- Formatting 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 fresh formatted 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