Curiosities in Computer Forensics

CyberDay 2020

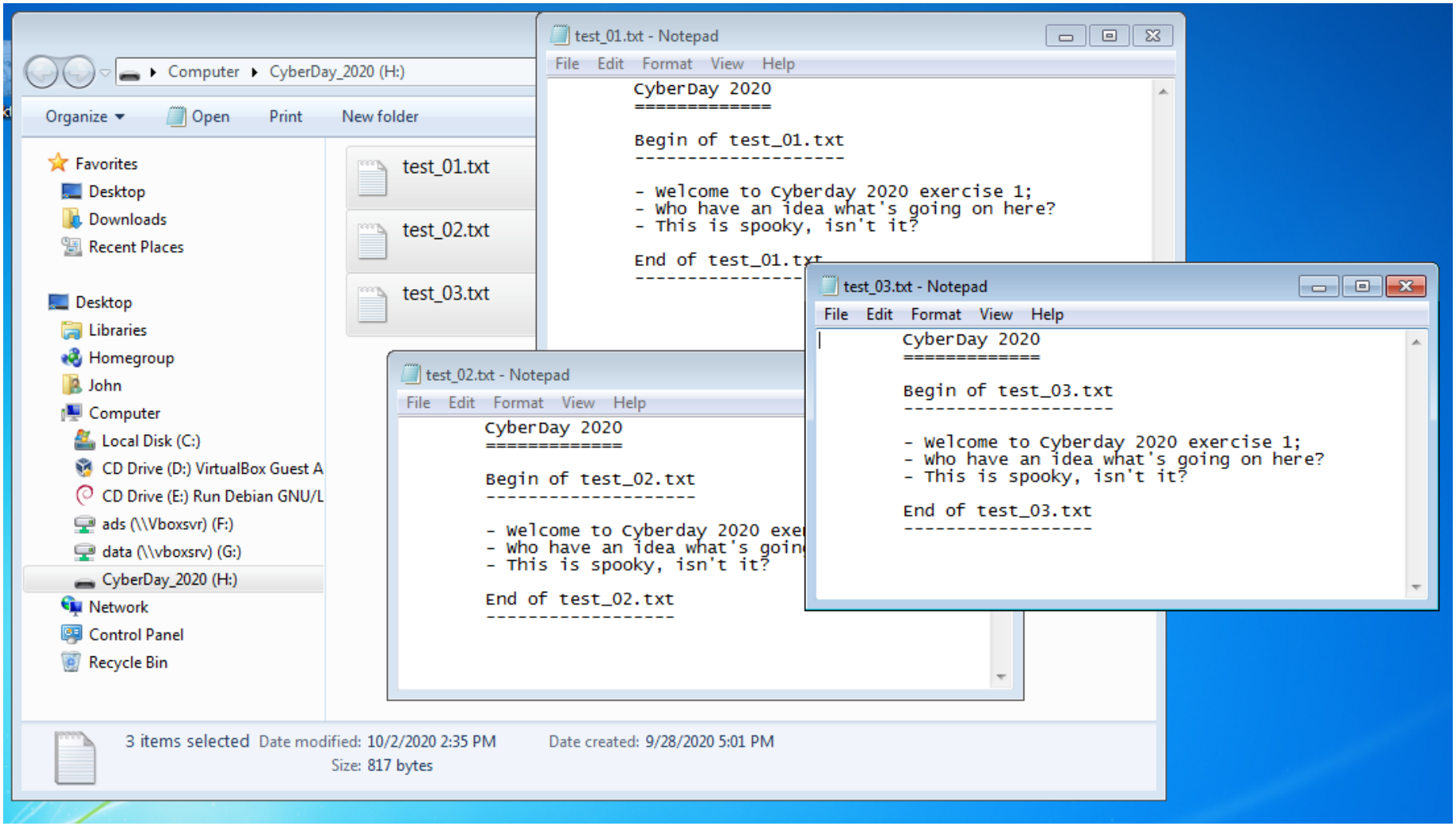
CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm - *TLP:GREEN*

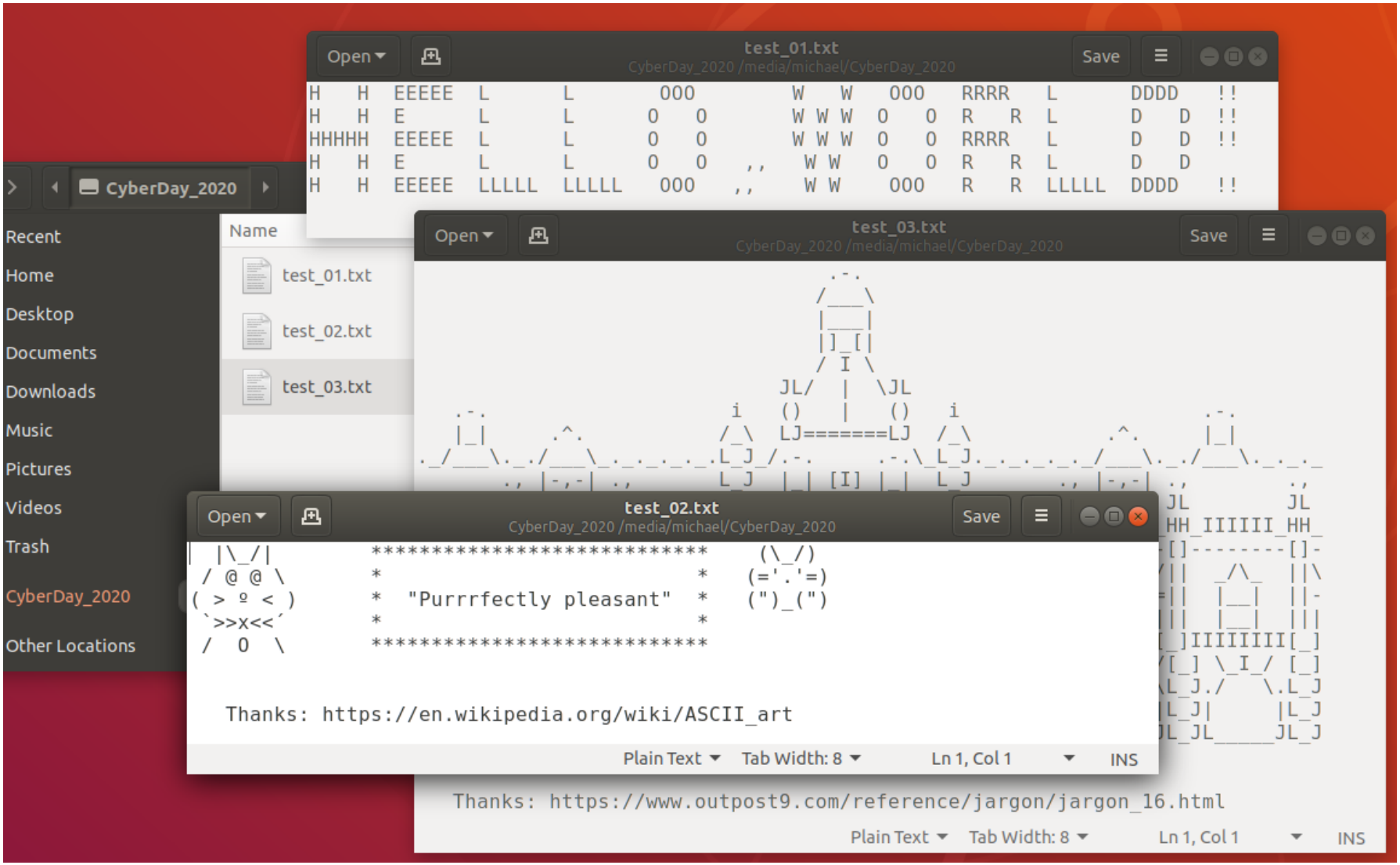
info@circl.lu

2020-10-06

My name is Legion: Demo



My name is Legion: Demo



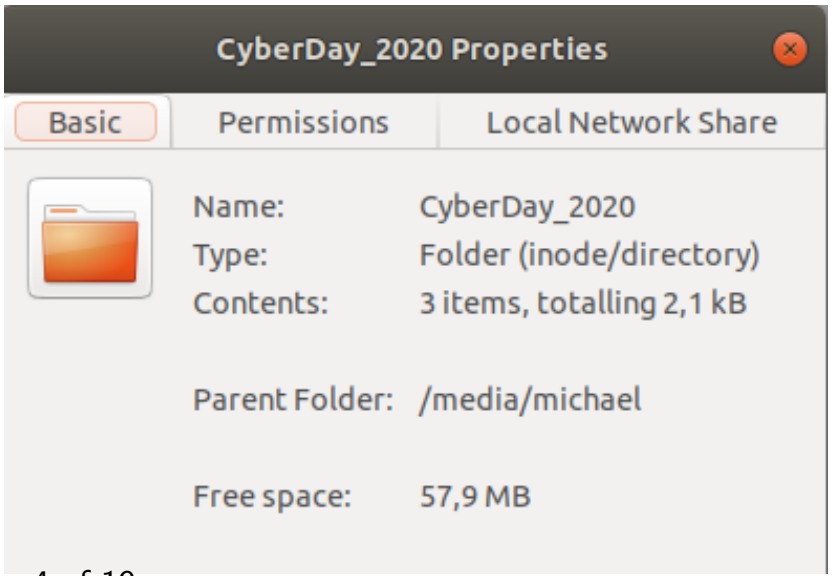
My name is Legion: Demo

```
# dmesg -T
      [Fr Okt  2 03:46:28 2020] sd 1:0:0:0: [sdb] 15974400 blocks: (8.18 GB/7.62 GiB)
      [Fr Okt  2 03:46:28 2020] sd 1:0:0:0: [sdb] Write Protect is off

# mount
      /dev/sdb1 on /media/michael/CyberDay_2020

# mmls /dev/sdb
      Cannot determine partition type

# fdisk -l /dev/sdb
      Device     Boot  Start    End Sectors  Size Id Type
      /dev/sdb1        144000 262143  118144 57,7M  7 HPFS/NTFS/exFAT
```



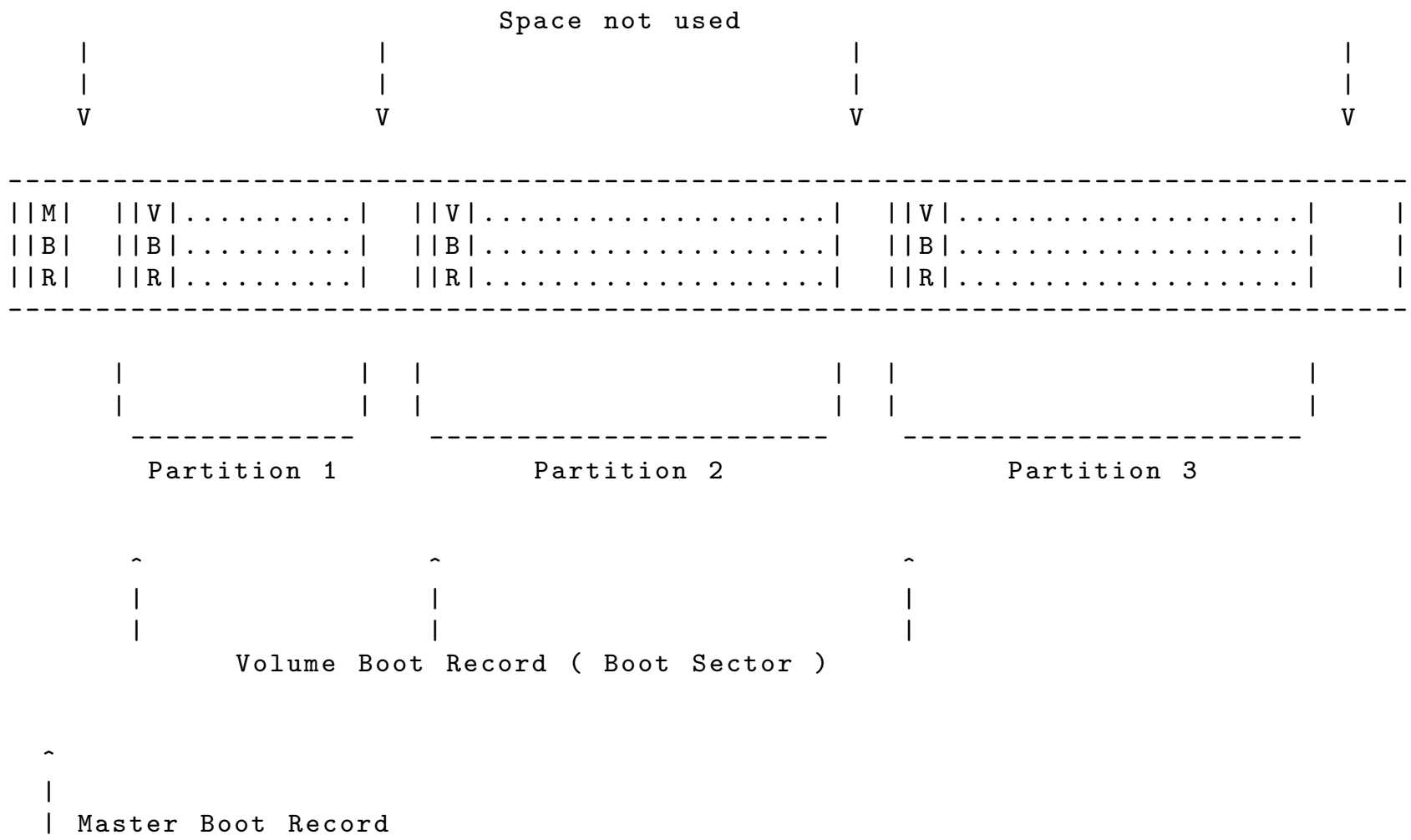
My name is Legion: Boot Sector

My name is Legion: Boot Sector

```
00000000: eb52 904e 5446 5320 2020 2000 0208 0000  .R.NTFS    .....
00000010: 0000 0000 00f8 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 8000 8000 ffff 0300 0000 0000  ................
00000030: 0400 0000 0000 0000 ff3f 0000 0000 0000  .........?......
00000040: f600 0000 0100 0000 3c91 9a52 e282 f91a  ........<..R....
00000050: 0000 0000 0e1f be71 7cac 22c0 740b 56b4  .......q|.".t.V.
00000060: 0ebb 0700 cd10 5eeb f032 e4cd 16cd 19eb  ......^..2......
00000070: fe54 6869 7320 6973 206e 6f74 2061 2062  .This is not a b
00000080: 6f6f 7461 626c 6520 6469 736b 2e20 506c  ootable disk. Pl
00000090: 6561 7365 2069 6e73 6572 7420 6120 626f  ease insert a bo
000000a0: 6f74 6162 6c65 2066 6c6f 7070 7920 616e  otable floppy an
000000b0: 640d 0a70 7265 7373 2061 6e79 206b 6579  d..press any key
000000c0: 2074 6f20 7472 7920 6167 6169 6e20 2e2e   to try again ..
000000d0: 2e20 0d0a 0000 0000 0000 0000 0000 0000  . ..............
...
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

```
0 - 2           Size:  3    Jump to bootstrap code
3 - 10          Size:  8    OEM-ID: NTFS
11 - 12         Size:  2    Bytes per sector: 0x0002 -> 0x0200 (little endian)-> 512
13              Size:  1    Sectors per cluster: 0x08 -> 4096 bytes per cluster
...
0x5a                        Bootstrap code
0x1fe           Size:  2    Signature: 0x55AA
```

My name is Legion: Partitions & MBR

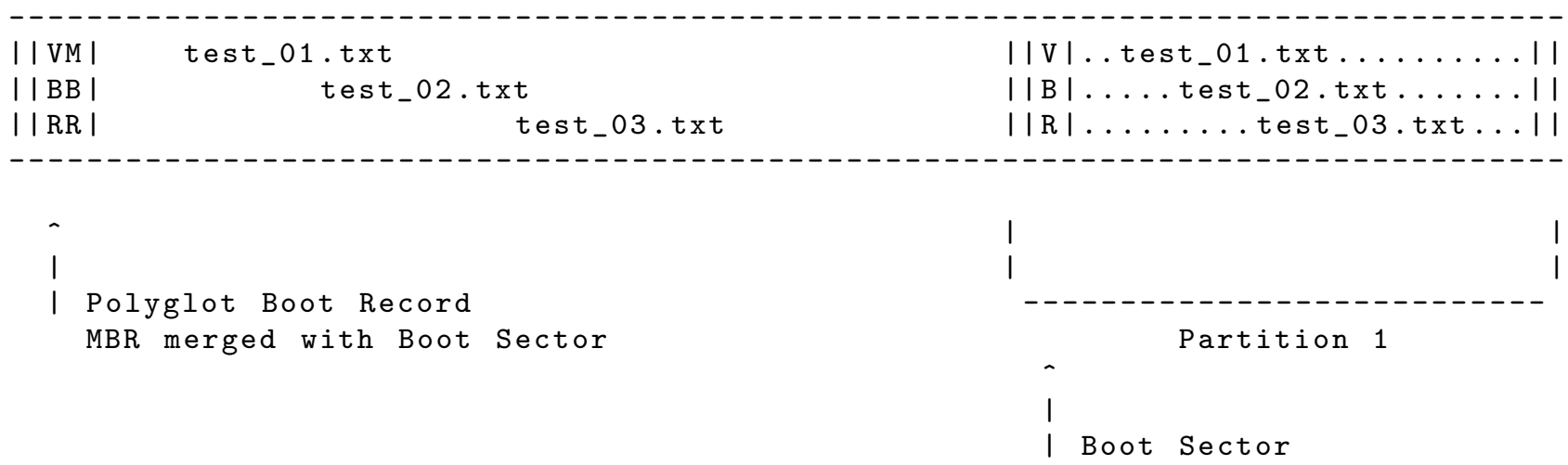


My name is Legion: Partitions & MBR

```
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
...
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 0000 0000 e4e5 c24e 0000 00f5  ...........N....
000001c0: 2e08 0751 0110 8032 0200 80cd 0100 0000  ...Q...2........
000001d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

```
000             Size: 439       Boot code
440             Size:   4       Disc signature
444             Size:   2       Reserved
446             Size   16       Partitiontable entry 1
462             Size   16       Partitiontable entry 2
478             Size   16       Partitiontable entry 3
494             Size   16       Partitiontable entry 4
510 - 511       0x1FE - 0x1FF   0x55AA
```

My name is Legion: Polyglot Boot Record




```
00000000: eb52 904e 5446 5320 2020 2000 0208 0000  .R.NTFS    .....
00000010: 0000 0000 00f8 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 8000 8000 ffff 0300 0000 0000  ................
00000030: 0400 0000 0000 0000 ff3f 0000 0000 0000  .........?......
...
000001b0: 0000 0000 0000 0000 e4e5 c24e 0000 00f5  ...........N....
000001c0: 2e08 0751 0110 8032 0200 80cd 0100 0000  ...Q...2........
000001d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001e0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001f0: 0000 0000 0000 0000 0000 0000 0000 55aa  ..............U.
```

Lost in Hyperspace: Demo

USB key before manipulation:

```
# dmesg -T
     [Do Jan 23 21:40:07 2020] sd 1:0:0:0: [sdb] 250068992 512-byte logical blocks:
     [Do Jan 23 21:40:07 2020] sd 1:0:0:0: [sdb] Write Protect is off
     [Do Jan 23 21:40:07 2020]  sdb: sdb1 < sdb5 sdb6 sdb7 >

# mount
     /dev/sdb7 on /media/michael/DFIR
     /dev/sdb6 on /media/michael/CIRCL
     /dev/sdb5 on /media/michael/test

# fdisk -l /dev/sdb
     Device     Boot  Start    End Sectors  Size Id Type
     /dev/sdb1         2048 264191  262144  128M  5 Extended
     /dev/sdb5         4096  20479   16384    8M  7 HPFS/NTFS/exFAT
     /dev/sdb6        22528 120831   98304   48M  7 HPFS/NTFS/exFAT
     /dev/sdb7       122880 253951  131072   64M  7 HPFS/NTFS/exFAT

# df -ha | grep sdb
     /dev/sdb7             64M  2,5M   62M   4% /media/michael/DFIR
     /dev/sdb6             48M  2,5M   46M   6% /media/michael/CIRCL
     /dev/sdb5            8,0M  2,5M  5,6M  31% /media/michael/test
```

Lost in Hyperspace: Demo

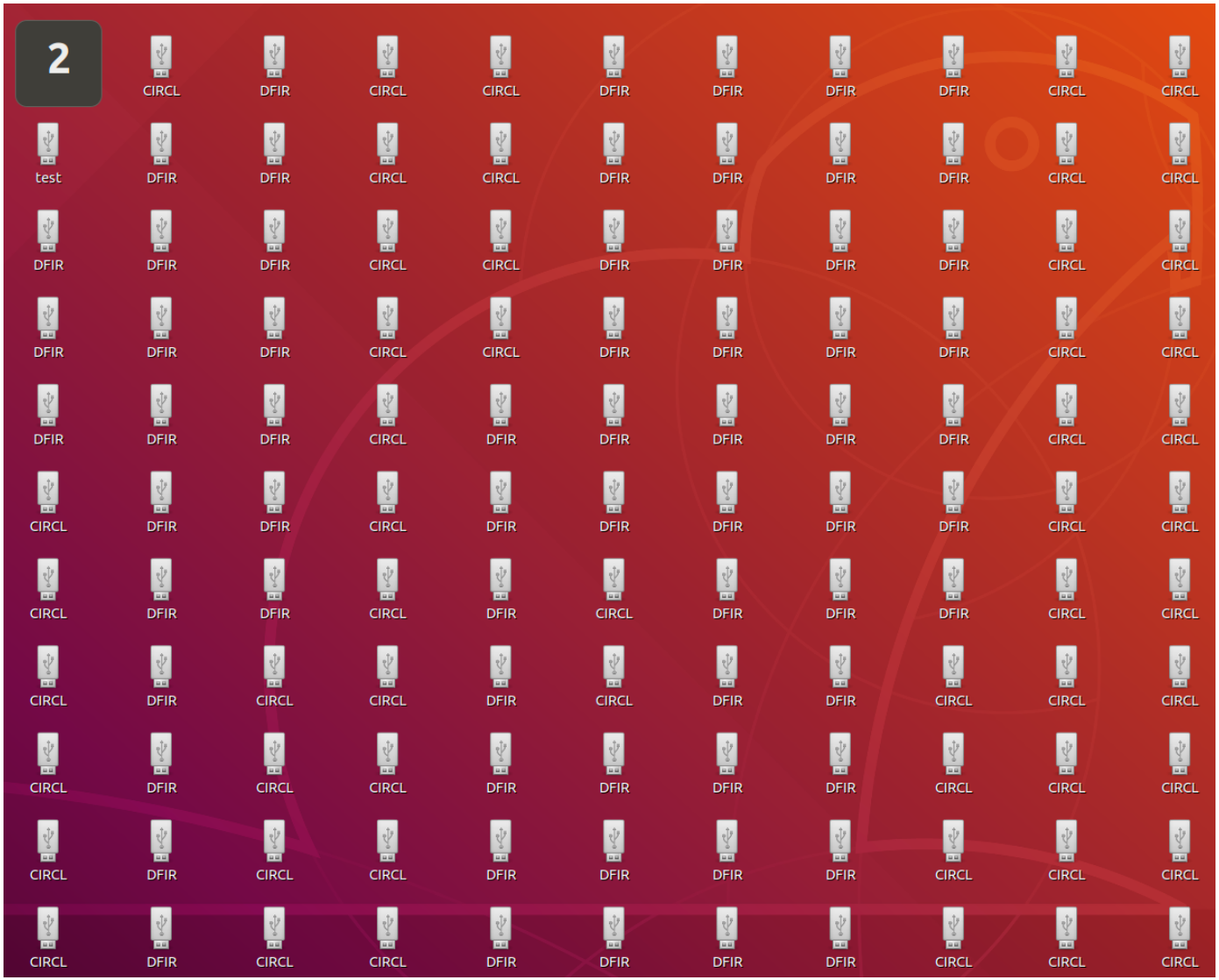
USB key during manipulation:

```
# hexedit /dev/sdb
     .....
     03B001B0   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 06  ................
     03B001C0   41 0B 07 03  82 28 00 08  00 00 00 00  02 00 00 00  A....(..........
     03B001D0   00 00 05 00  00 00 00 48  00 00 00 88  01 00 00 00  .......H........
```

USB key after manipulation:

```
# fdisk -l /dev/sdb
     /dev/sdb5          4096  20479    16384     8M  7 HPFS/NTFS/exFAT
     /dev/sdb6         22528 120831    98304    48M  7 HPFS/NTFS/exFAT
     /dev/sdb7        122880 253951   131072    64M  7 HPFS/NTFS/exFAT
     /dev/sdb8         22528 120831    98304    48M  7 HPFS/NTFS/exFAT
     /dev/sdb9        122880 253951   131072    64M  7 HPFS/NTFS/exFAT
     .....
     .....
     /dev/sdb57       122880 253951   131072    64M  7 HPFS/NTFS/exFAT
     /dev/sdb58        22528 120831    98304    48M  7 HPFS/NTFS/exFAT
     /dev/sdb59       122880 253951   131072    64M  7 HPFS/NTFS/exFAT
     /dev/sdb60        22528 120831    98304    48M  7 HPFS/NTFS/exFAT
```

Lost in Hyperspace: Demo



Lost in Hyperspace: Demo

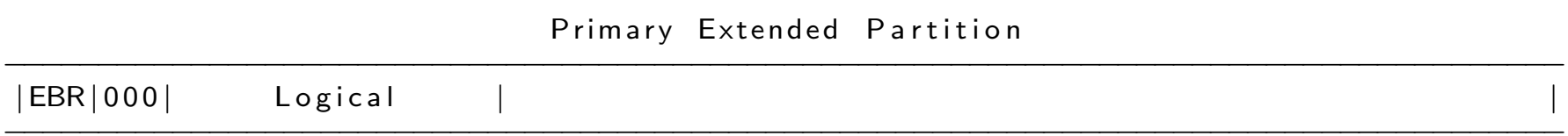
USB Key investigation:

```
# mount
      /dev/sdc62 on /media/michael/CIRCL24
      /dev/sdc85 on /media/michael/DFIR26
      /dev/sdc83 on /media/michael/DFIR25
      /dev/sdc56 on /media/michael/CIRCL21
      /dev/sdc103 on /media/michael/DFIR31
      /dev/sdc66 on /media/michael/CIRCL25
      /dev/sdc71 on /media/michael/DFIR28
      /dev/sdc74 on /media/michael/CIRCL29
      /dev/sdc54 on /media/michael/CIRCL30
      .....

# df -ha | grep sdc
      .....
      /dev/sdc95                      64M  2,5M   62M   4% /media/michael/DFIR36
      /dev/sdc101                     64M  2,5M   62M   4% /media/michael/DFIR34
      /dev/sdc107                     64M  2,5M   62M   4% /media/michael/DFIR35
      /dev/sdc115                     64M  2,5M   62M   4% /media/michael/DFIR40
      /dev/sdc99                      64M  2,5M   62M   4% /media/michael/DFIR39
      /dev/sdc110                     48M  2,5M   46M   6% /media/michael/CIRCL40
      /dev/sdc91                      64M  2,5M   62M   4% /media/michael/DFIR38
      /dev/sdc109                     64M  2,5M   62M   4% /media/michael/DFIR37

# mmls /dev/sdc
      ----> stuck
```

Lost in Hyperspace: Extended Partitions

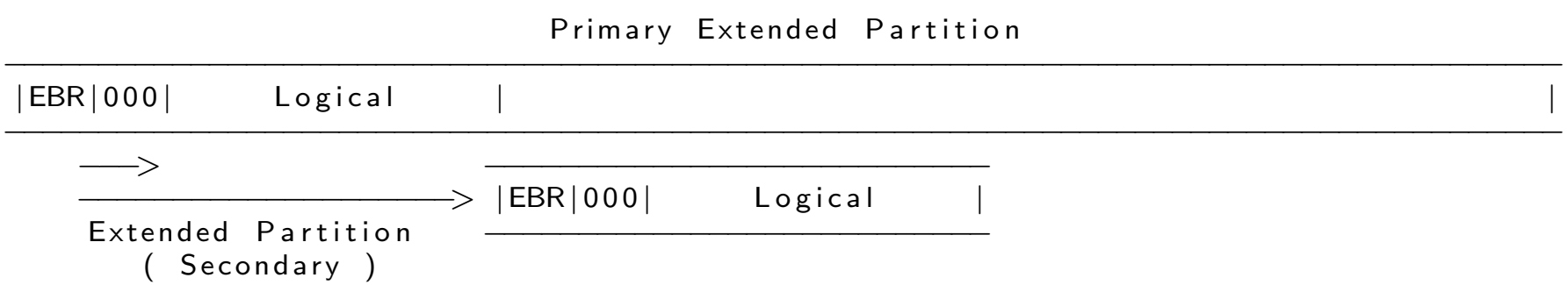


MBR:

```
000001b0: 0000 0000 0000 0000 d7b8 0cae 0000 0014
000001c0: 0904 050f 823e 0008 0000 0000 0400 0000
```

--

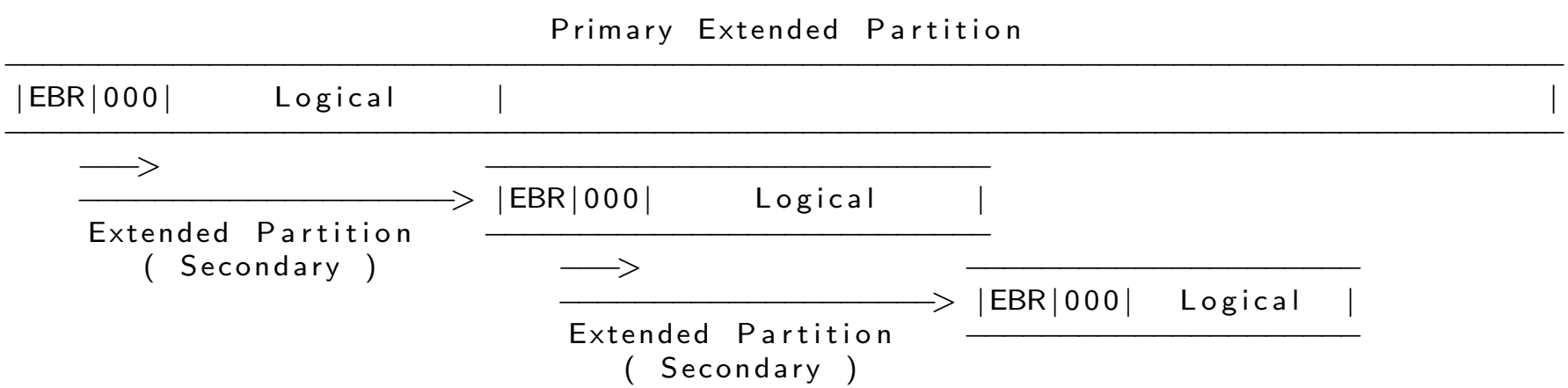
Lost in Hyperspace: Extended Partitions



MBR:
```
000001b0: 0000 0000 0000 0000 d7b8 0cae 0000 0014
000001c0: 0904 050f 823e 0008 0000 0000 0400 0000
```

EBR_01:
```
001001b0: 0000 0000 0000 0000 0000 0000 0000 0029
001001c0: 0708 0717 0a2c 0008 0000 0040 0000 0018
001001d0: 012c 051f 4206 0048 0000 0088 0100 0000
```

Lost in Hyperspace: Extended Partitions

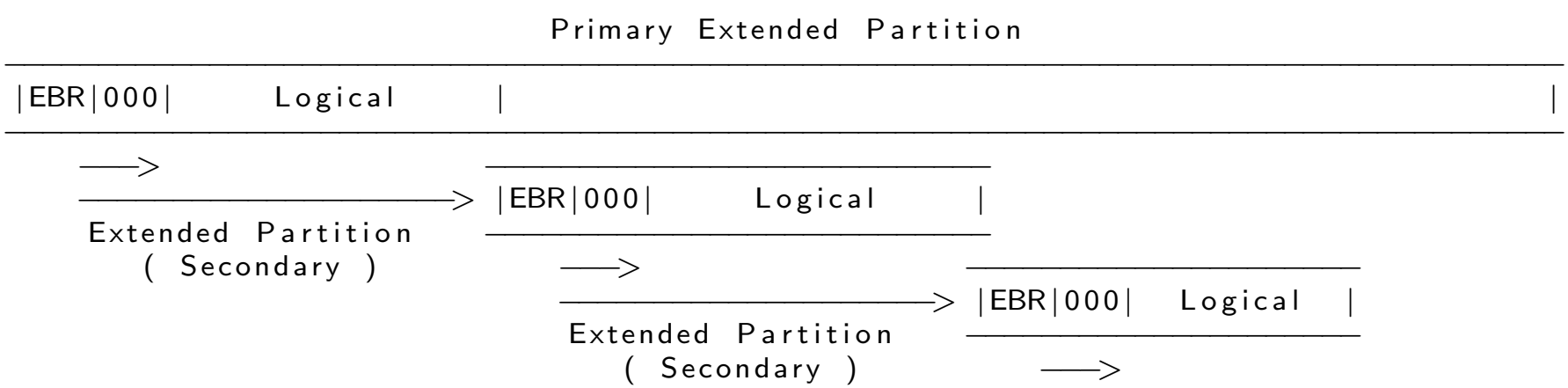



```
MBR:      000001b0: 0000 0000 0000 0000 d7b8 0cae 0000 0014
          000001c0: 0904 050f 823e 0008 0000 0000 0400 0000

          EBR_01:   001001b0: 0000 0000 0000 0000 0000 0000 0000 0029
                    001001c0: 0708 0717 0a2c 0008 0000 0040 0000 0018
                    001001d0: 012c 051f 4206 0048 0000 0088 0100 0000

          EBR_02:   00A001B0: 0000 0000 0000 0000 0000 0000 0000 002C
                    00A001C0: 0930 071F 4206 0008 0000 0080 0100 001F
                    00A001D0: 4306 0503 8228 00D0 0100 0008 0200 0000
```

Lost in Hyperspace: Extended Partitions



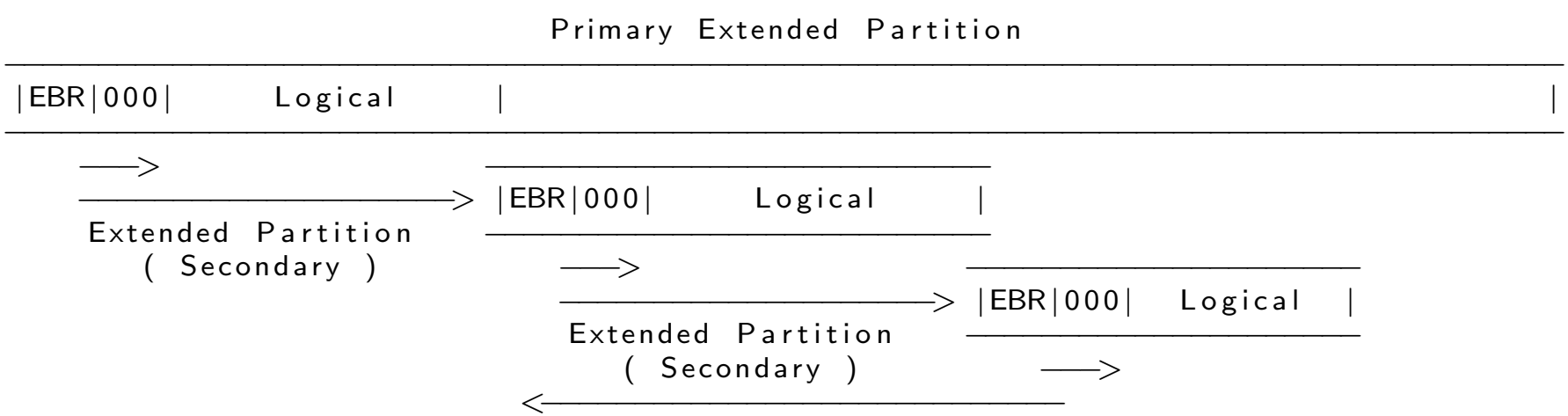
MBR:
```
000001b0: 0000 0000 0000 0000 d7b8 0cae 0000 0014
000001c0: 0904 050f 823e 0008 0000 0000 0400 0000
```

EBR_01:
```
001001b0: 0000 0000 0000 0000 0000 0000 0000 0029
001001c0: 0708 0717 0a2c 0008 0000 0040 0000 0018
001001d0: 012c 051f 4206 0048 0000 0088 0100 0000
```

EBR_02:
```
00A001B0: 0000 0000 0000 0000 0000 0000 0000 002C
00A001C0: 0930 071F 4206 0008 0000 0080 0100 001F
00A001D0: 4306 0503 8228 00D0 0100 0008 0200 0000
```

EBR_03:
```
03B001B0: 0000 0000 0000 0000 0000 0000 0000 0006
03B001C0: 410B 0703 8228 0008 0000 0000 0200 0000
03B001D0: 0000 0000 0000 0000 0000 0000 0000 0000
```

Lost in Hyperspace: Endless Loop



MBR: 000001b0: 0000 0000 0000 0000 d7b8 0cae 0000 0014
000001c0: 0904 050f 823e 0008 0000 0000 0400 0000

EBR_01: 001001b0: 0000 0000 0000 0000 0000 0000 0000 0029
001001c0: 0708 0717 0a2c 0008 0000 0040 0000 0018
001001d0: 012c 051f 4206 0048 0000 0088 0100 0000

EBR_02: 00A001B0: 0000 0000 0000 0000 0000 0000 0000 002C
00A001C0: 0930 071F 4206 0008 0000 0080 0100 001F
00A001D0: 4306 0503 8228 00D0 0100 0008 0200 0000

EBR_03: 03B001B0: 0000 0000 0000 0000 0000 0000 0000 0006
03B001C0: 410B 0703 8228 0008 0000 0000 0200 0000
03B001D0: 0000 0500 0000 0048 0000 0088 0100 0000

Curiosities in Computer Forensics

CyberDay 2020

CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm - *TLP:GREEN*

info@circl.lu

2020-10-06