Lessons in Forensics - II

What could go wrong?

CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm - *TLP:GREEN*

info@circl.lu

2020-01-29 15:31:27 UTC+1

Feedback: Lessons in Forensics - I

- Modify data on "Read Only" mounted device
- Hiding data in HPA

  cert.at: → SWAP: NSA Exploit of the Day
  →`https://www.schneier.com/blog/archives/2014/02/swap_nsa_exploi.html`
  →`https://en.wikipedia.org/wiki/Host_protected_area`

- Block device I/O Error

  David Byers and Nahid Shahmehri.
  Contagious errors:
  Understanding and avoiding issues with imaging drives containing faulty sectors.
  The International Journal of Digital Forensics and Incident Response,
  ISSN 1742-2876, E-ISSN 1873-202X, Vol. 5, no 1, p. 29-33

  → ATA commands like *WRITELONG*
  → Overwrite ECC → error on read
  → READ call → Kernel page cache
  → 4096 Bytes - 8 Sectors
  → Direct I/O mode → *iflag* = *direct*

Forensics Challenge Workshop

FIRST | The Conference | Venue | Program | Registration | Sponsorship | News | 31ST ANNUAL EDINBURGH FIRST CONFERENCE JUNE 16-21 2019

Forensics Challenge Workshop (Full-Day)

Michael Hamm

Michael Hamm (CIRCL, LU)

> *Michael Hamm has worked for more than 10 years as Ingenieur-Security in the field of classical Computer and Network Security (Firewall, VPN, AntiVirus) at the research center "Henry Tudor" in Luxembourg. Since 2010, Michael has worked as an operator and analyst at CIRCL – Computer Incident Response Center Luxembourg where he is working on forensic examinations and incident response.*

Course Level: Beginner - Intermediate

Intended Audience: Security/SOC analysts, CSIRT/CERT team members, forensics investigators.

Pre-requisites: Forensic Workstation: Linux (Kali, DEFT, SANS SIFT).

Hardware Requirements: Standard Laptop, Virtual Machine sufficient. The participant should show up with any kind of (Virtual) Forensics Workstation they usually prefer to work with. If the participant is quite new in forensics but knows Linux, either 'Kali Linux' or 'SANS SIFT Workstation' as virtual PC is a good choice.

Abstract: In this course you will solve some small size challenges to train your skills in forensics with open source tools.

Topics:

- Forensics Challenges
- Linux
- Open Source
- Data recovery
- dd
- Hexeditor
- Data ex-filtration
- Alternate Data Streams

Forensics Challenge Workshop

Simulation based on a real case

1. Small company
2. Ransomware outbreak
3. All data encrypted
4. File name extension `.rans` added
5. Backups on external disk
   - 5.1 Daily full backup of all data
   - 5.2 All data stored in individual ZIP archives
   - 5.3 Available backups:

```
    50832 Jun 14 10:53 backup_2019-02-08.zip.rans*
  2175110 Jun 14 10:57 backup_2019-02-12.zip.rans*
 11896585 Jun 14 11:01 backup_2019-02-13.zip.rans*
 11896763 Jun 14 11:10 backup_2019-02-14.zip.rans*

file *                 backup_2019-02-08.zip.rans: data
                       backup_2019-02-12.zip.rans: data
                       backup_2019-02-13.zip.rans: data
                       backup_2019-02-14.zip.rans: data
```

→ Goal: Data recovery

Forensics Challenge Workshop

Investigate backup files

```
ent backup_2019-02-08.zip.rans      ---> Entropy = 7.925631 bits per byte.
ent backup_2019-02-12.zip.rans      ---> Entropy = 7.998791 bits per byte.
ent backup_2019-02-13.zip.rans      ---> Entropy = 7.998055 bits per byte.
ent backup_2019-02-14.zip.rans      ---> Entropy = 7.998011 bits per byte.
```

Open it with a hexeditor

```
xxd backup_2019-02-08.zip.rans | less

    00000000: 504b 0304 1400 0000 0000 7b59 484e 0000  PK........{YHN..
    00000010: 0000 0000 0000 0000 0000 0900 0000 5069  ..............Pi
    00000020: 6374 7572 6573 2f00 0000 0000 0000 0000  ctures/.........
    00000030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
    .....
```

Strings?

```
strings -n 10 backup_2019-02-* | less

    $B-.jOA0|(
    Pictures/CIRCL-Logo.png
    <)&\8HVL+S
    Documents/PK
    Documents/Education_Programme_Flyer.pdf
    .....
```

Forensics Challenge Workshop

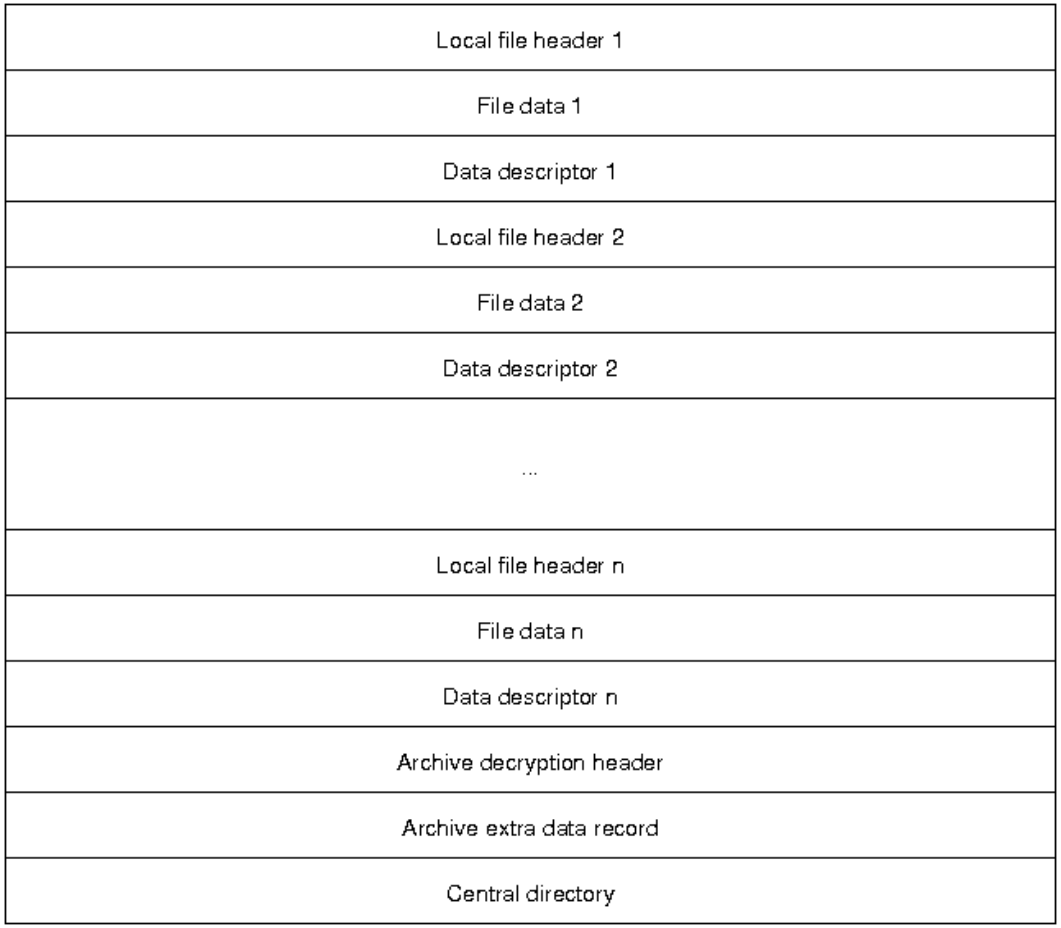


Image (c) jmu.edu - Image used solely for illustration purposes - https://users.cs.jmu.edu/buchhofp/forensics/formats/pkzip.html

Forensics Challenge Workshop

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	P	K	03	04	Ver		Fla		Comp		Time		Time		CRC	
10	CRC				Comp size				Ucomp size				Len		Ext	
20	File name (variable size)															
30																

```
xxd backup_2019-02-14.zip.rans | less
    00000020: 6375 6d65 6e74 732f 504b 0304 1400 0000  cuments/PK......
    00000030: 0800 1c80 4c4e 85b6 6965 7f6b 0200 ccbd  ....LN..ie.k....
    00000040: 0200 2700 0000 446f 6375 6d65 6e74 732f  ..'...Documents/
    00000050: 4564 7563 6174 696f 6e5f 5072 6f67 7261  Education_Progra
    00000060: 6d6d 655f 466c 7965 722e 7064 66dc 5a05  mme_Flyer.pdf.Z.
    00000070: 5494 cf16 ff08 1109 2905 41a4 a543 ba41  T.......).A..C.A
```

Compressed size:	7f6b 0200	⟶ 0002 6b7f	⟶ 158,591
Lenght file name:	2700	⟶ 0027	⟶ 39
Extra field:	0000	⟶ 0000	⟶ 0
Start of data:		40 + 30 + 39 + 0	⟶ 109
End of data:		109 + 158,591	⟶ 158,700
Recovery begin (head begin):		28	⟶ 40
Recover size header + data:		30 + 39 + 158,591	⟶ 158,660

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=40 count=158660 seek=40
```

Forensics Challenge Workshop

Already covered:

```
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=0 count=40 seek=0
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=158700 count=890925 seek=158700
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=40 count=158660 seek=40
```

Home work:

```
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=1049625 count=1074145 seek=104962
dd if=backup_2019-02-14.zip.rans of=rescue.zip bs=1 skip=2123770 count=77 seek=2123770

dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=2123770 count=38 seek=2123847
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=2123808 count=113286 seek=212388
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=2237094 count=4806555 seek=223717
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=7043649 count=4801146 seek=704372
dd if=backup_2019-02-13.zip.rans of=rescue.zip bs=1 skip=11844795 count=39 seek=11844872

dd if=backup_2019-02-12.zip.rans of=rescue.zip bs=1 skip=2123809 count=25464 seek=1184491
dd if=backup_2019-02-08.zip.rans of=rescue.zip bs=1 skip=25426 count=19260 seek=11870375
dd if=backup_2019-02-12.zip.rans of=rescue.zip bs=1 skip=2168533 count=5713 seek=11889635
```

Lost in Hyperspace: USB key investigation

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: USB key investigation

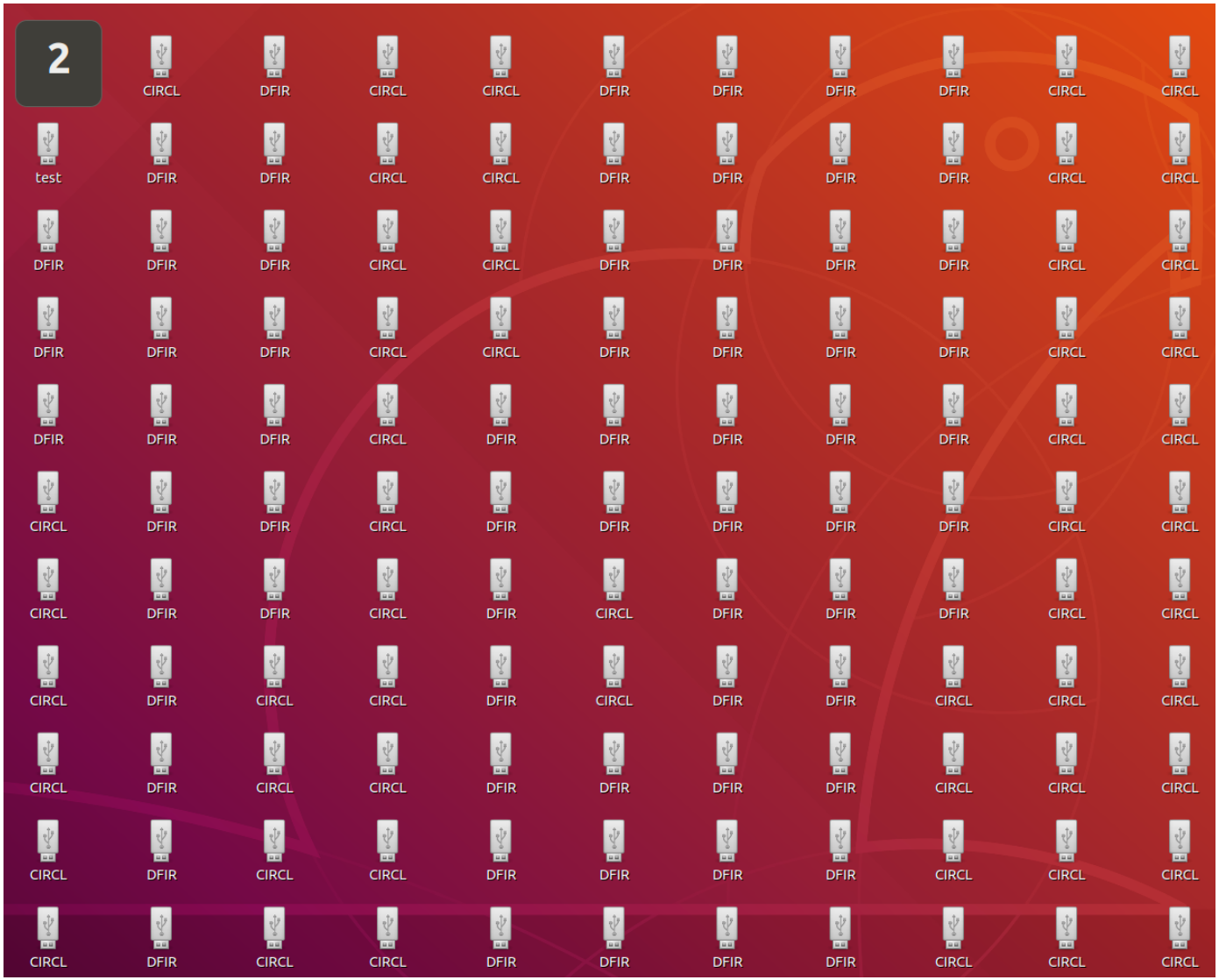
USB key during manipulation:

```
# 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: USB key investigation



Lost in Hyperspace: USB key investigation

USB Key investigation:

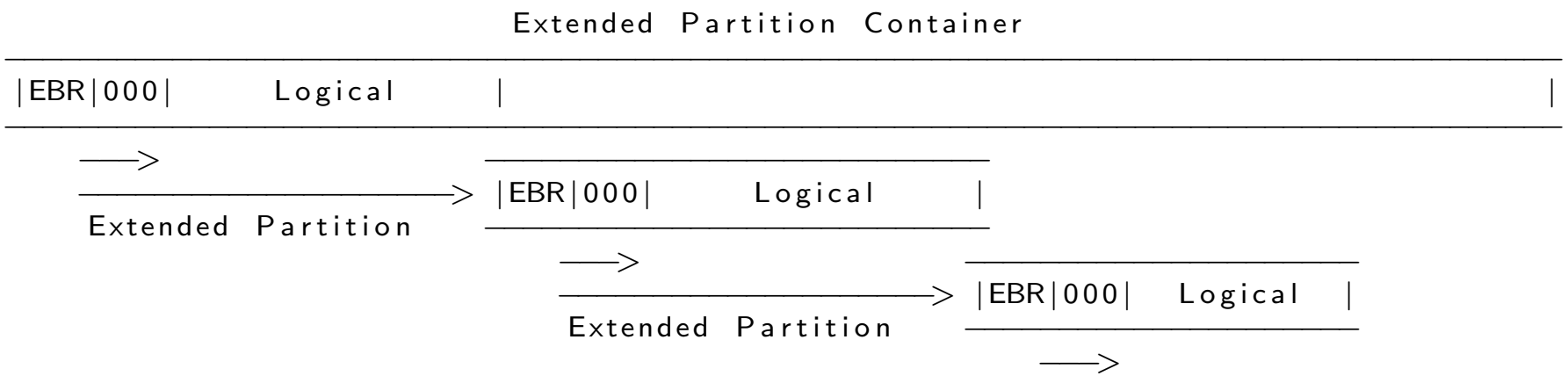
```
# mount
      /dev/sdc62 on /media/michael/CIRCL24
      /dev/sdc85 on /media/michael/DFIR26
      /dev/sdc83 on /media/michael/DFIR25
      /dev/sdc56 on /media/michael/CIRCL21
      /dev/sdc103 on /media/michael/DFIR31
      /dev/sdc66 on /media/michael/CIRCL25
      /dev/sdc71 on /media/michael/DFIR28
      /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: USB key investigation

What happened? Extended Partitions



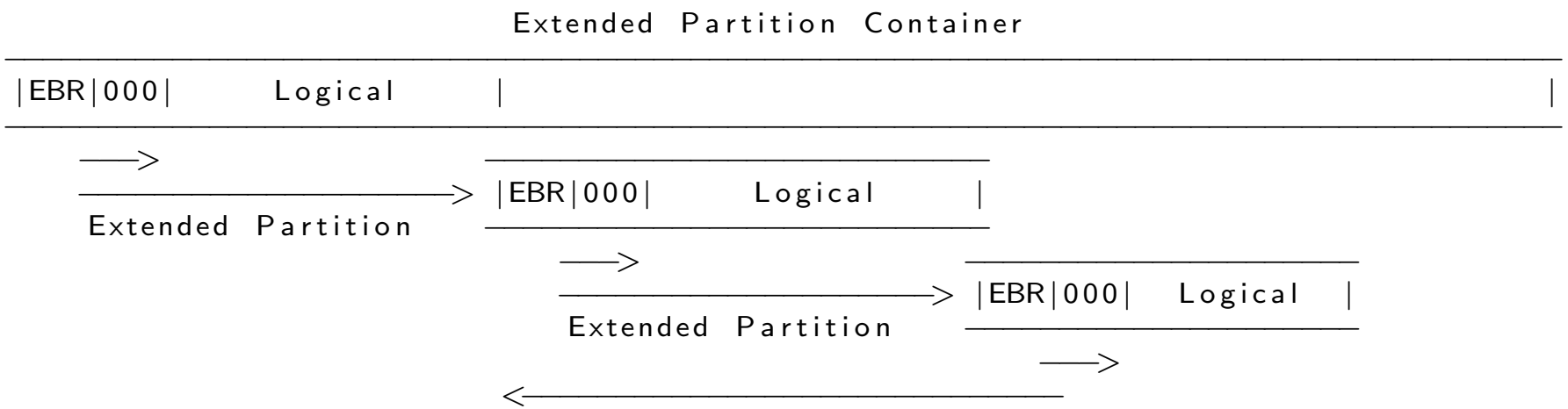

```
EBR_01:  001001b0: 0000 0000 0000 0000 0000 0000 0000 0029
         001001c0: 0708 0717 0a2c 0008 0000 0040 0000 0018
         001001d0: 012c 051f 4206 0048 0000 0088 0100 0000

         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: USB key investigation

What happened? Extended Partitions




```
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
```

Lessons in Forensics - II

- Feedback: Lessons in Forensics - I
- Forensics Challenge Workshop
- Lost in Hyperspace: USB key investigation

For Forensics Trainings contact info@circl.lu

Q & A

Thank you