Forensics Low Level

Having fun with Linux onboard tools

CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm - *TLP:WHITE*

info@circl.lu

PTS21 2021-07-05

CIRCL
FORENSICS Training

Modify "Read Only" mounted data

Modify "Read Only" mounted data

Message from a forensic book

> *"Nothing will prevent your Linux system from modifying data on a read only mounted device"*

→ Challenge: Modify data on a read only mounted block device

- I will simulate an attack:
  - Targeted tamper of evidences
  - Only use Linux on-board tools
  - Be `root` user
  - Of course: It's a trick
- BUT I will not cheat like:
  - Remount the device in RW mode

Modify "Read Only" mounted data

Play Script:

Preparation:

1. Identify how the device is connected
2. Review mount options
3. Re-mount the device in "Read Only" mode
4. Review mount options
5. Open file, modify data and try to safe

Attack:

1. Use `strings` to find the data
2. Calculate sector number
3. `dd` sector on to local disk
4. Modify local stored sector with a hexeditor
5. `dd` sector back on RO mounted block device

Validate results

Modify "Read Only" mounted data

Preparation command line interaction

```
# dmesg -T
     [So Jun  6 00:45:37 2021] sd 1:0:0:0: [sdb] Write Protect is off
     [So Jun  6 00:45:37 2021] sd 1:0:0:0: [sdb] No Caching mode page found
     [So Jun  6 00:45:37 2021]  sdb: sdb1


# mount
     /dev/sdb1 on /media/michael/CIRCL-DFIR type vfat (rw,nosuid,.....


# mount -o remount,ro /dev/sdb1


# mount
     /dev/sdb1 on /media/michael/CIRCL-DFIR type vfat (ro,nosuid,.....


# md5sum /dev/sdb1
     bf99ef758076cf7b9eecc0aaf38c738b  /dev/sdb1
```

-

Modify "Read Only" mounted data

Attack command line interaction

```
# strings -td /dev/sdb1 | grep Hello
     298897 Hello World!
     299106 Hello World!

# echo $(( 299106 / 512 ))
     584

# dd if=/dev/sdb1 bs=512 skip=584 count=1 of=584.raw
     1+0 records in
     1+0 records out
     512 bytes copied, 0,000255244 s, 2,0 MB/s

# ls -l 584.raw
     -rw-r--r-- 1 root root 512 Jun 11 10:15 584.raw

# hexer 2051.raw

# dd if=584.raw bs=512 seek=584 count=1 of=/dev/sdb1
     1+0 records in
     1+0 records out
     512 bytes copied, 0,000254733 s, 2,0 MB/s

# md5sum /dev/sdb1
     b208f533ee935bcf6b4d3475214ac52f  /dev/sdb1
```

Modify "Read Only" mounted data

Countermeasures:

- Try on board methods:
  - `hdparm -r1 /dev/sdb`
  - `blockdev --setro /dev/sdb`
  - `udev` rules
    → Attack on block device still possible

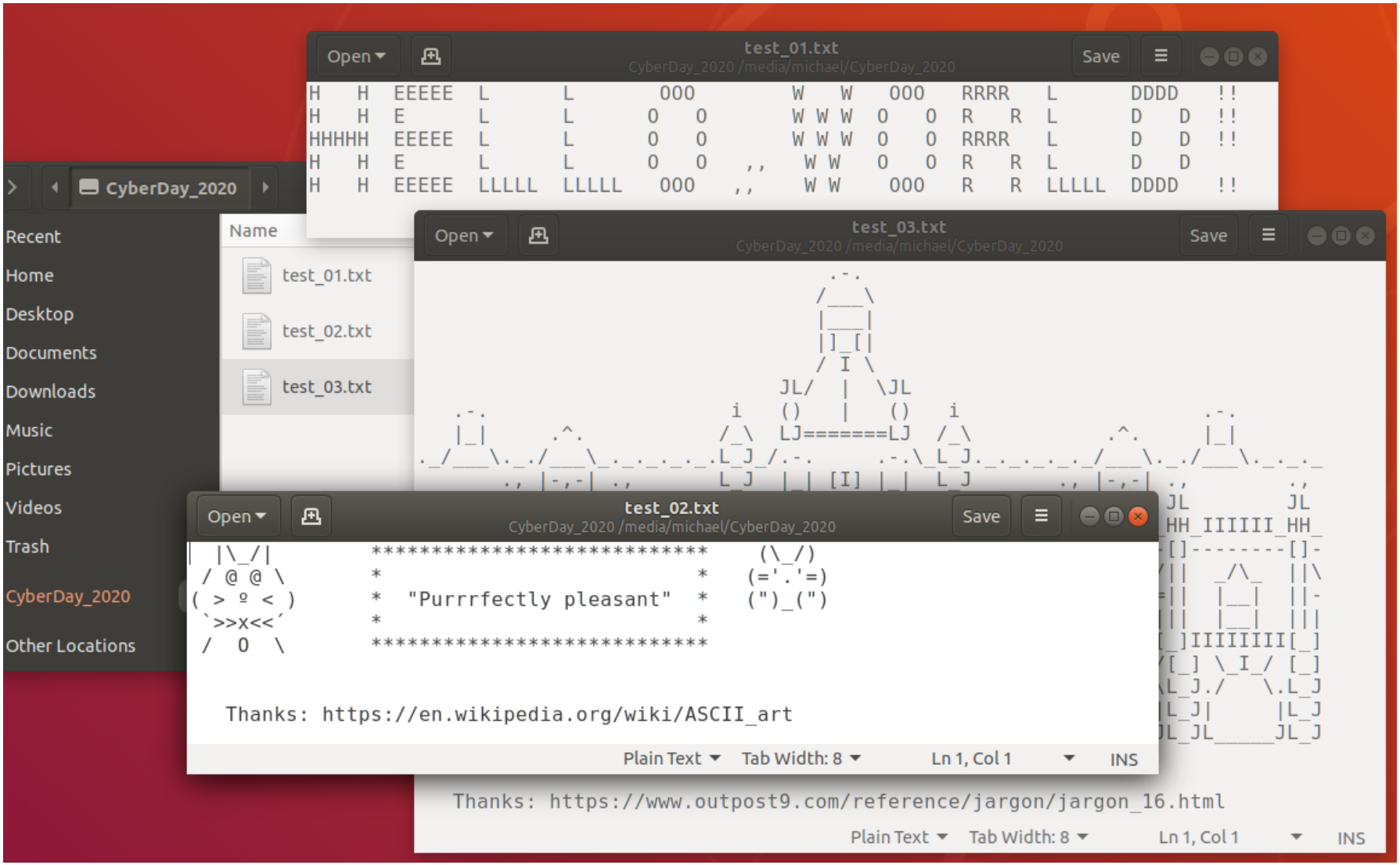
- Try Forensics Linux Distributions:
  - Live Kali in forensic mode
  - SANS SIFT Workstation
  - DEFT DFIR Toolkit
    → Some distributions do not auto mount
    → Attack on block device still possible

→ Use Hardware Write Blocker!

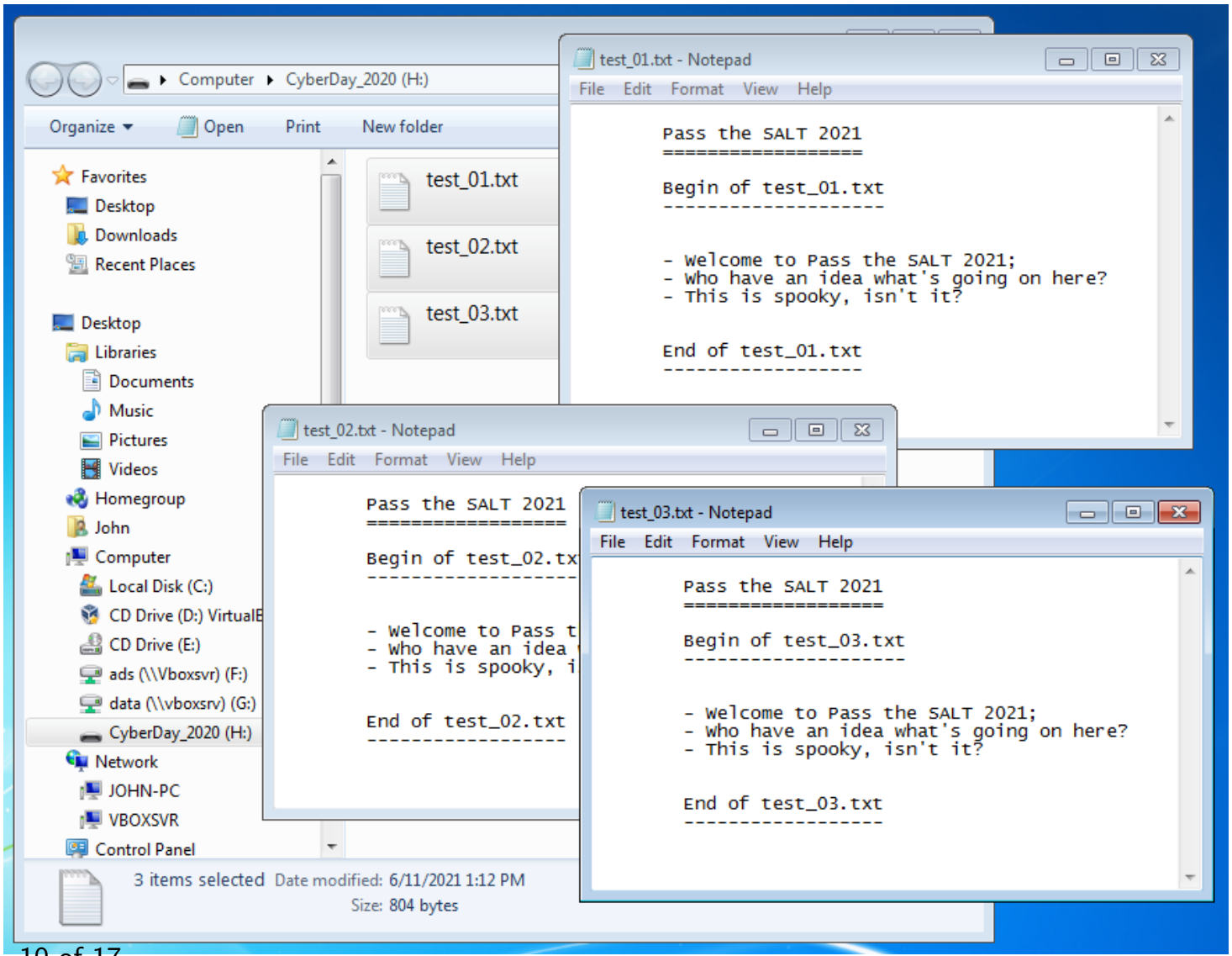
CIRCL
FORENSICS Training

My name is Legion

My name is Legion: Demo

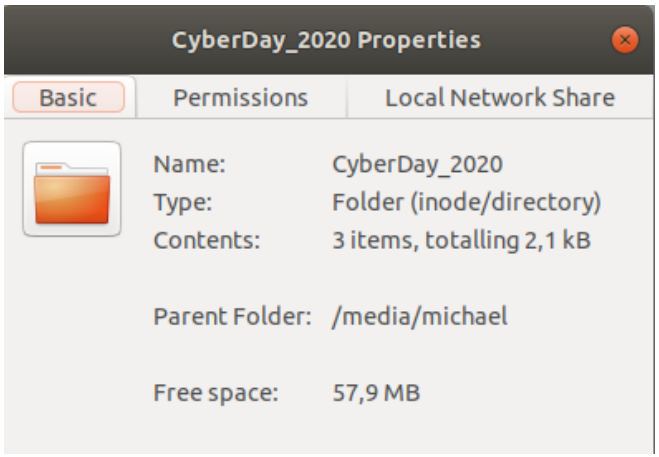


My name is Legion: Demo



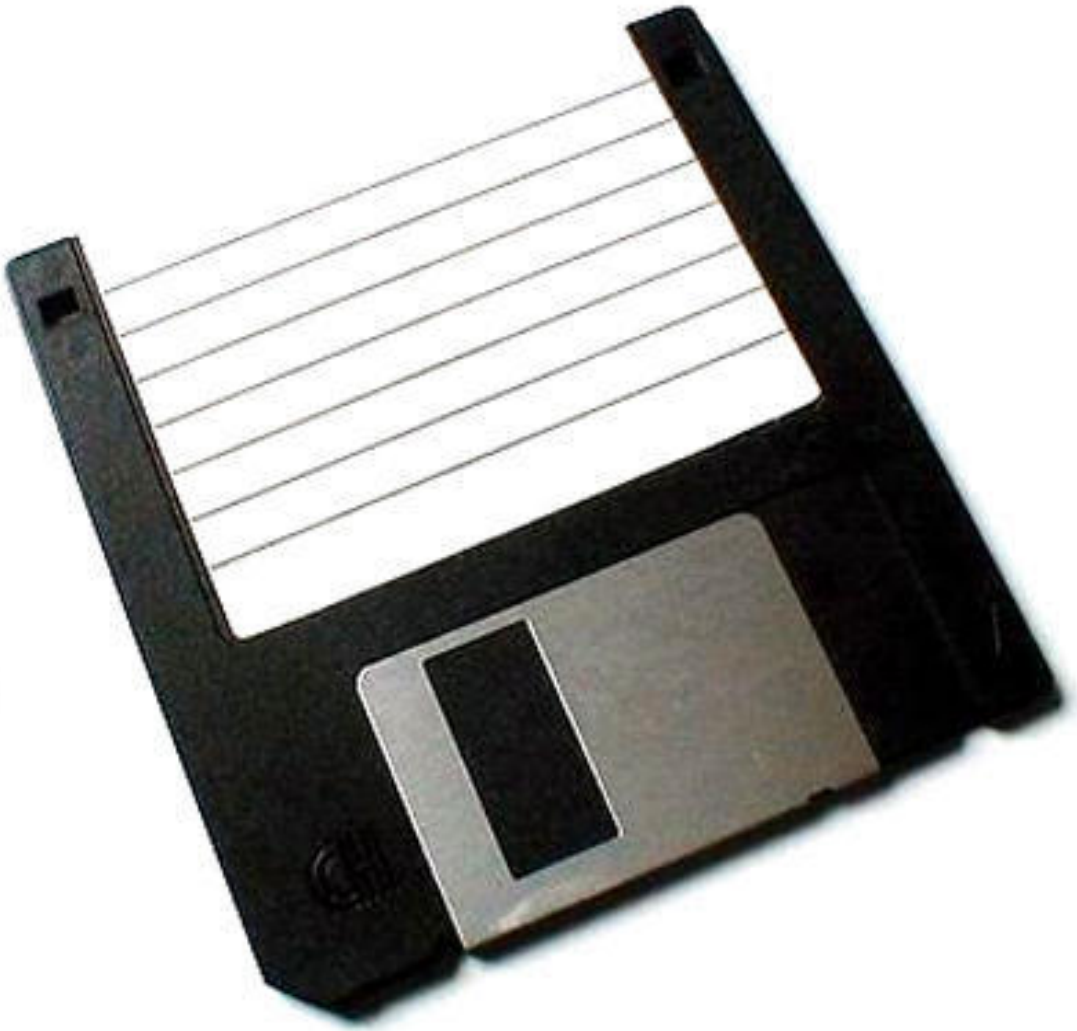
My name is Legion: Demo

```
# dmesg
      sd 1:0:0:0: [sdb] 15826944 512-byte logical blocks: (8.10 GB/7.55 GiB)
      sd 1:0:0:0: [sdb] Write Protect is off
      sdb: sdb1

# mount
      /dev/sdb1 on /media/michael/CyberDay_2020 type fuseblk (rw,nosuid,.....

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




```
# mmls /dev/sdb
      Cannot determine partition type
```

My name is Legion: Boot Sector

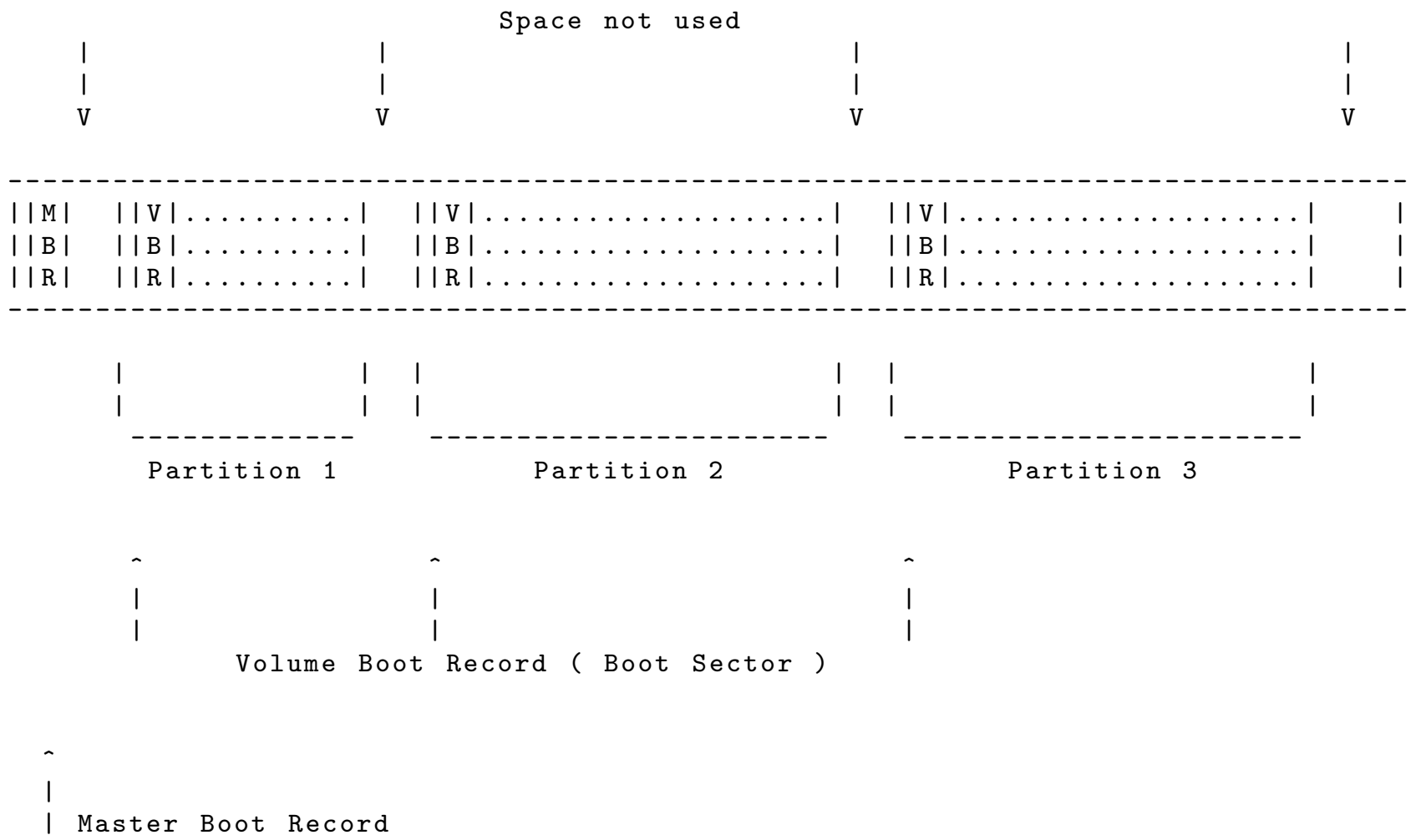


My name is Legion: Boot Sector

```
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

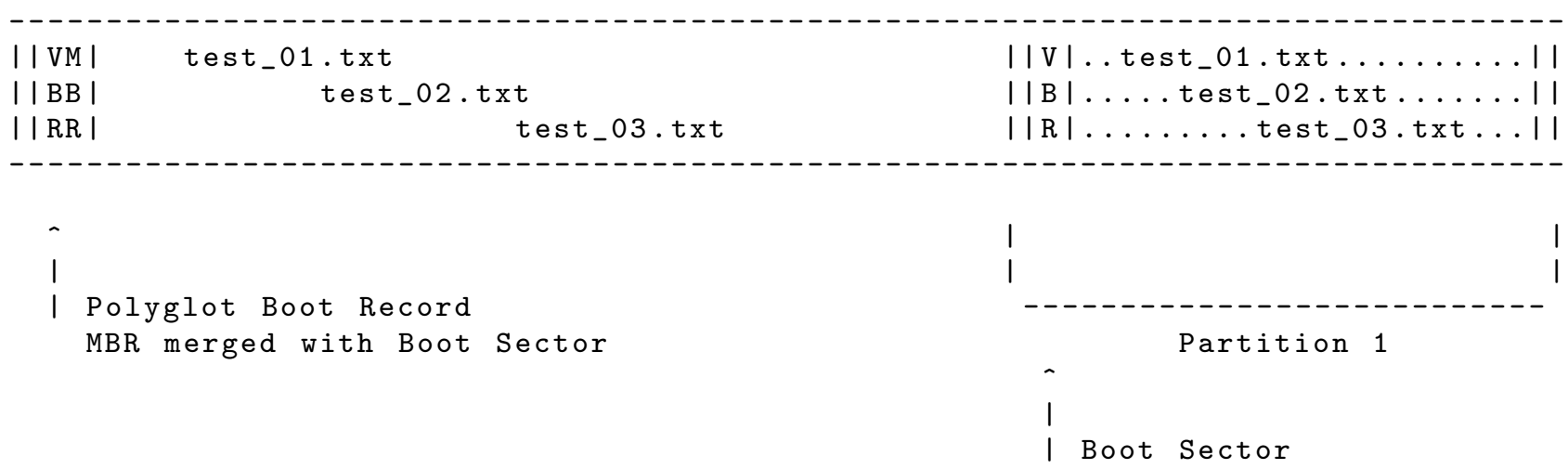


My name is Legion: Partitions & MBR

```
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.
```

CIRCL FORENSICS Training

Q & A