As We Are Many

The spooky USB stick

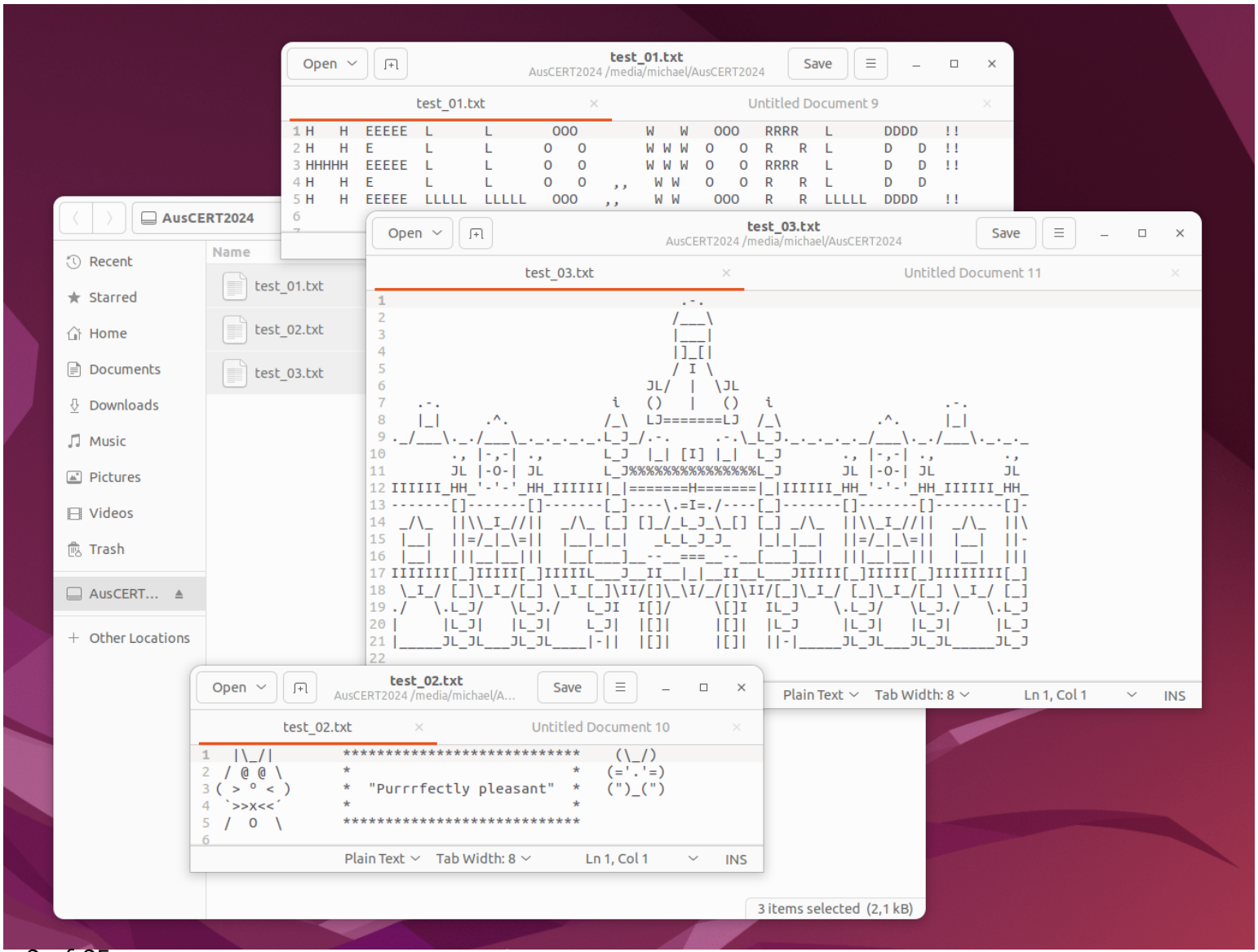
CIRCL
Computer Incident
Response Center
Luxembourg

Michael Hamm,
Christian Studer

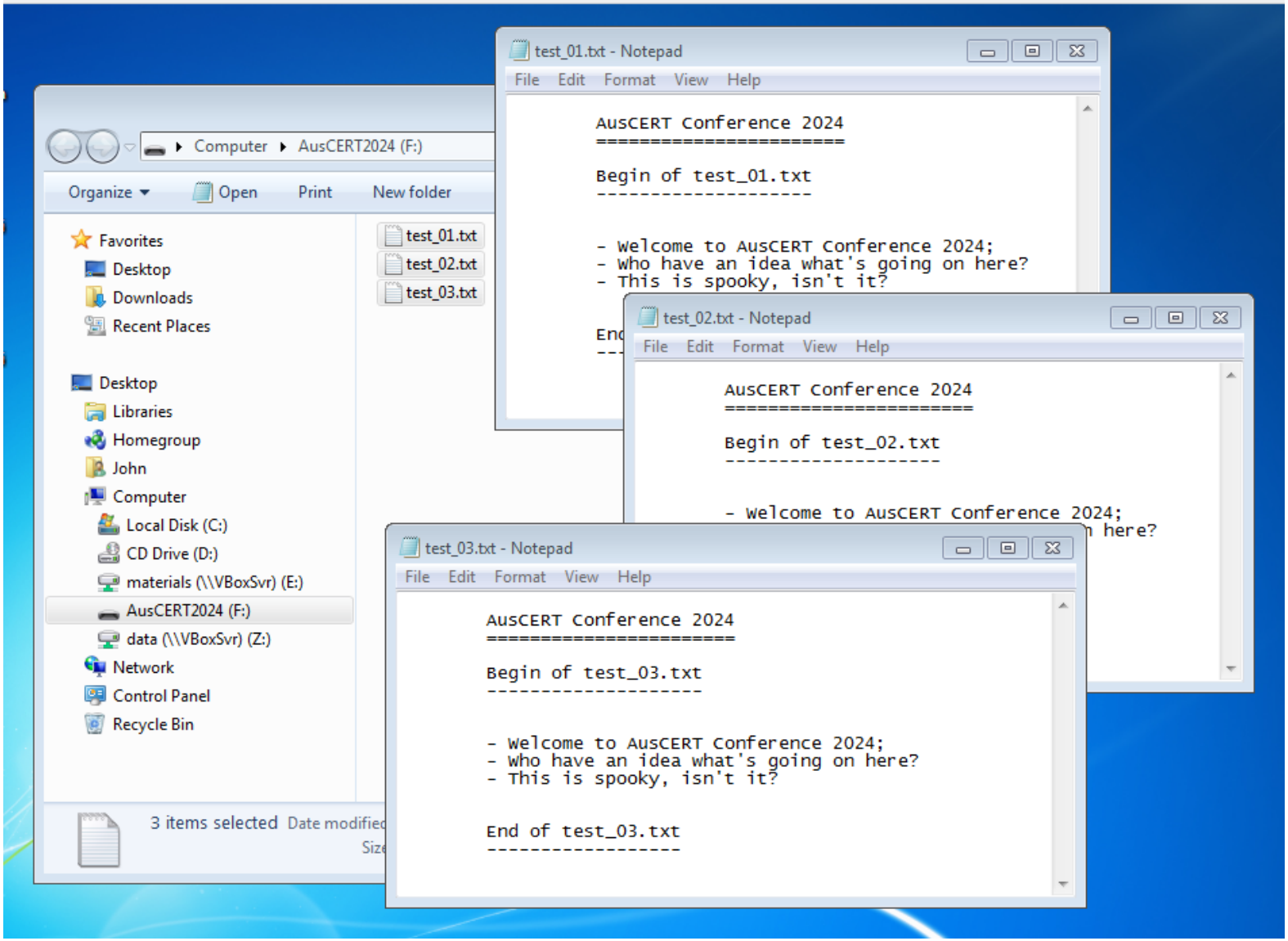
TLP:CLEAR

AUSCERT 2024

Live Demo


test_01.txt
AusCERT2024 /media/michael/AusCERT2024
Open
Save
test_01.txt
Untitled Document 9
H H EEEEE L L OOO W W OOO RRRR L DDDD !!
H H E L L O O W W W O O R R L D D !!
HHHHH EEEEE L L O O W W W O O RRRR L D D !!
H H E L L O O ,, W W O O R R L D D
H H EEEEE LLLLL LLLLL OOO ,, W W OOO R R LLLLL DDDD !!
AusCERT2024
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
AusCERT...
Other Locations
Name
test_01.txt
test_02.txt
test_03.txt
test_03.txt
Untitled Document 11
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
test_02.txt
Untitled Document 10
|_/|
/ @ @ \
(> º <)
`>>x<<´
/ O \
"Purrrfectly pleasant"
(_/)
(='.'=)
(")_(")
3 items selected (2,1 kB)

Live Demo


test_01.txt - Notepad
File Edit Format View Help
AusCERT Conference 2024
Begin of test_01.txt
- Welcome to AusCERT Conference 2024;
- Who have an idea what's going on here?
- This is spooky, isn't it?
test_02.txt - Notepad
File Edit Format View Help
AusCERT Conference 2024
Begin of test_02.txt
- Welcome to AusCERT Conference 2024;
test_03.txt - Notepad
File Edit Format View Help
AusCERT Conference 2024
Begin of test_03.txt
- Welcome to AusCERT Conference 2024;
- Who have an idea what's going on here?
- This is spooky, isn't it?
End of test_03.txt
Computer ▸ AusCERT2024 (F:)
Organize Open Print New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Homegroup
John
Computer
Local Disk (C:)
CD Drive (D:)
materials (\\VBoxSvr) (E:)
AusCERT2024 (F:)
data (\\VBoxSvr) (Z:)
Network
Control Panel
Recycle Bin
test_01.txt
test_02.txt
test_03.txt
3 items selected

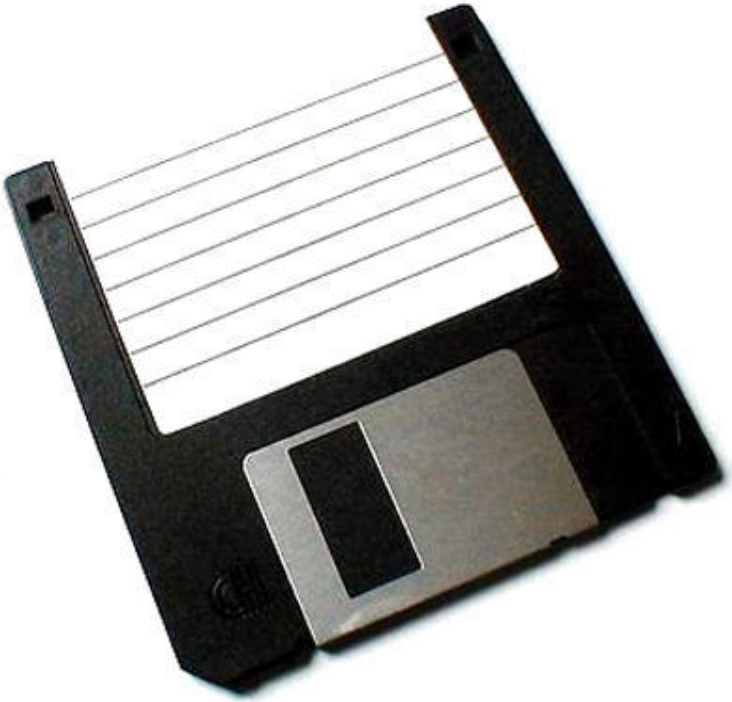
Investigation

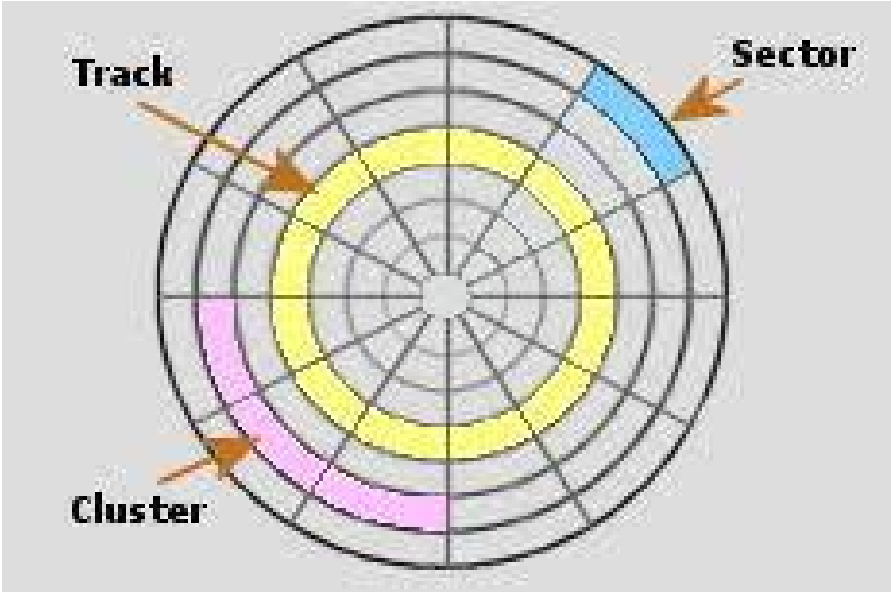
```
$ sudo dmesg -T -W
      usb 3-9: new high-speed USB device number 8 using xhci_hcd
      usb 3-9: Product: USB Flash Disk
      usb-storage 3-9:1.0: USB Mass Storage device detected
      sd 0:0:0:0: [sda] 15722496 512-byte logical blocks: (8.05 GB/7.50 GiB)
      sda: sda1


$ sudo fdisk -l /dev/sda
      Device     Boot  Start    End Sectors  Size Id Type
      /dev/sda1        144000 262143  118144 57,7M  7 HPFS/NTFS/exFAT


$ sudo mmls /dev/sda



$ mount | grep sda
      /dev/sda1 on /media/michael/AusCERT2024 type ntfs3 (rw,nosuid, .....


$ sudo fsstat /dev/sda1
      File System Type: NTFS
      Volume Serial Number: 7B702E352BD29E15
      OEM Name: NTFS
      Volume Name: AusCERT2024
      Version: Windows XP
```

CIRCL
FORENSICS Training

As We Are Many: Whats going on?

Volume Boot Record - Boot Sector






```
-------------------------------------------------------------------------------
||V|  test_01.txt                                                            |
||B|           test_02.txt                                                   |
||R|                    test_03.txt                                          |
-------------------------------------------------------------------------------
  ^
  | Boot Sector
```

Volume Boot Record - 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 - 0A         Size:  8    OEM-ID: NTFS
1B - 1C         Size:  2    Bytes per sector: 0x0002 -> 0x0200 (little endian)-> 512
1D              Size:  1    Sectors per cluster: 0x08 -> 4096 bytes per cluster
...
54                          Bootstrap code
1FE             Size:  2    Signature: 0x55AA
```

Master Boot Record & Partitioned Disk

Track, Head, Cylinder, Sector, Block, Cluster

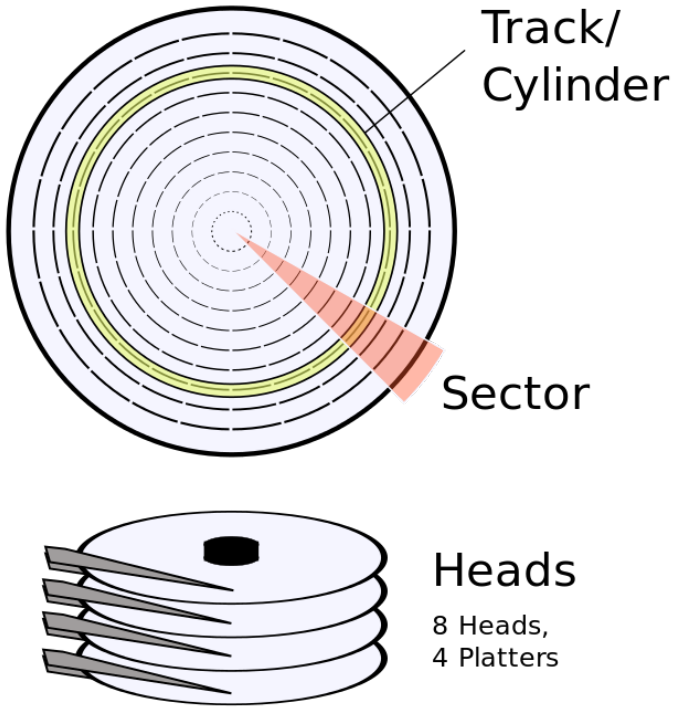


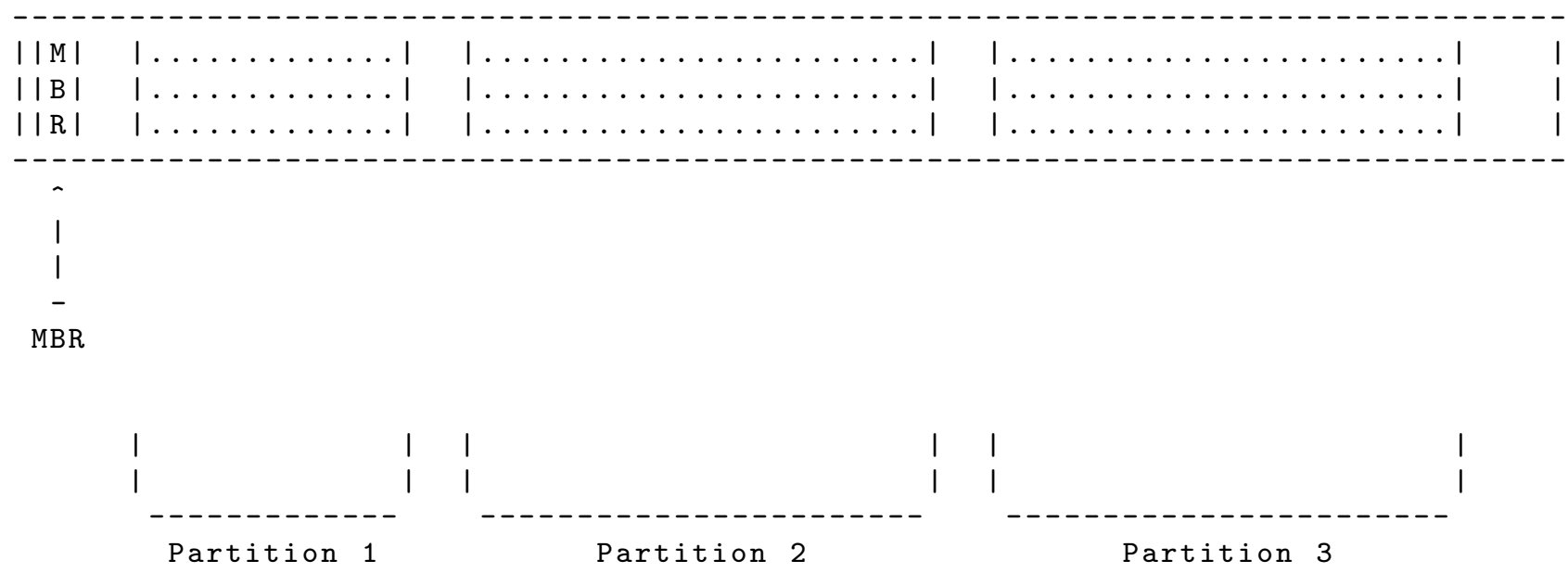
Image (c) wikipedia.org - Image used solely for illustration purposes

Master Boot Record & Partitioned Disk

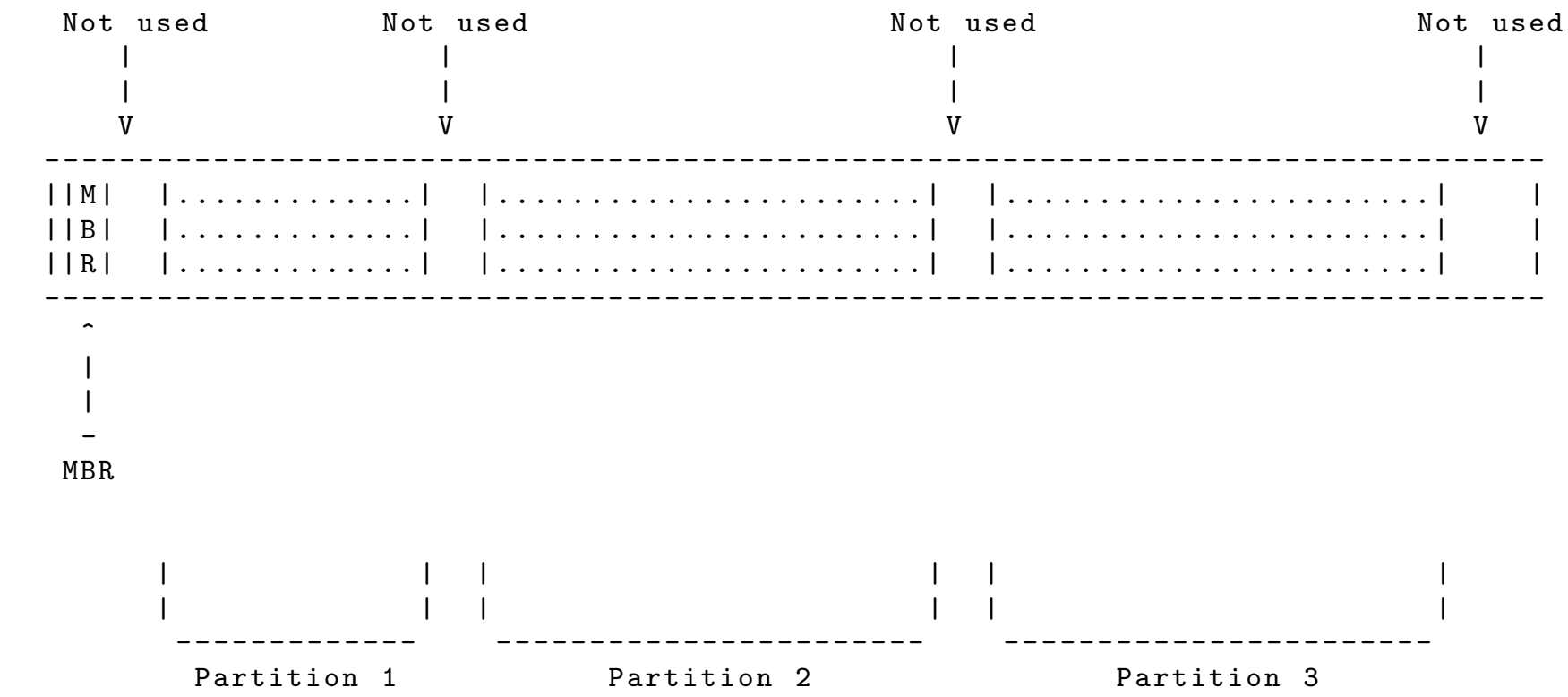
-

Master Boot Record & Partitioned Disk

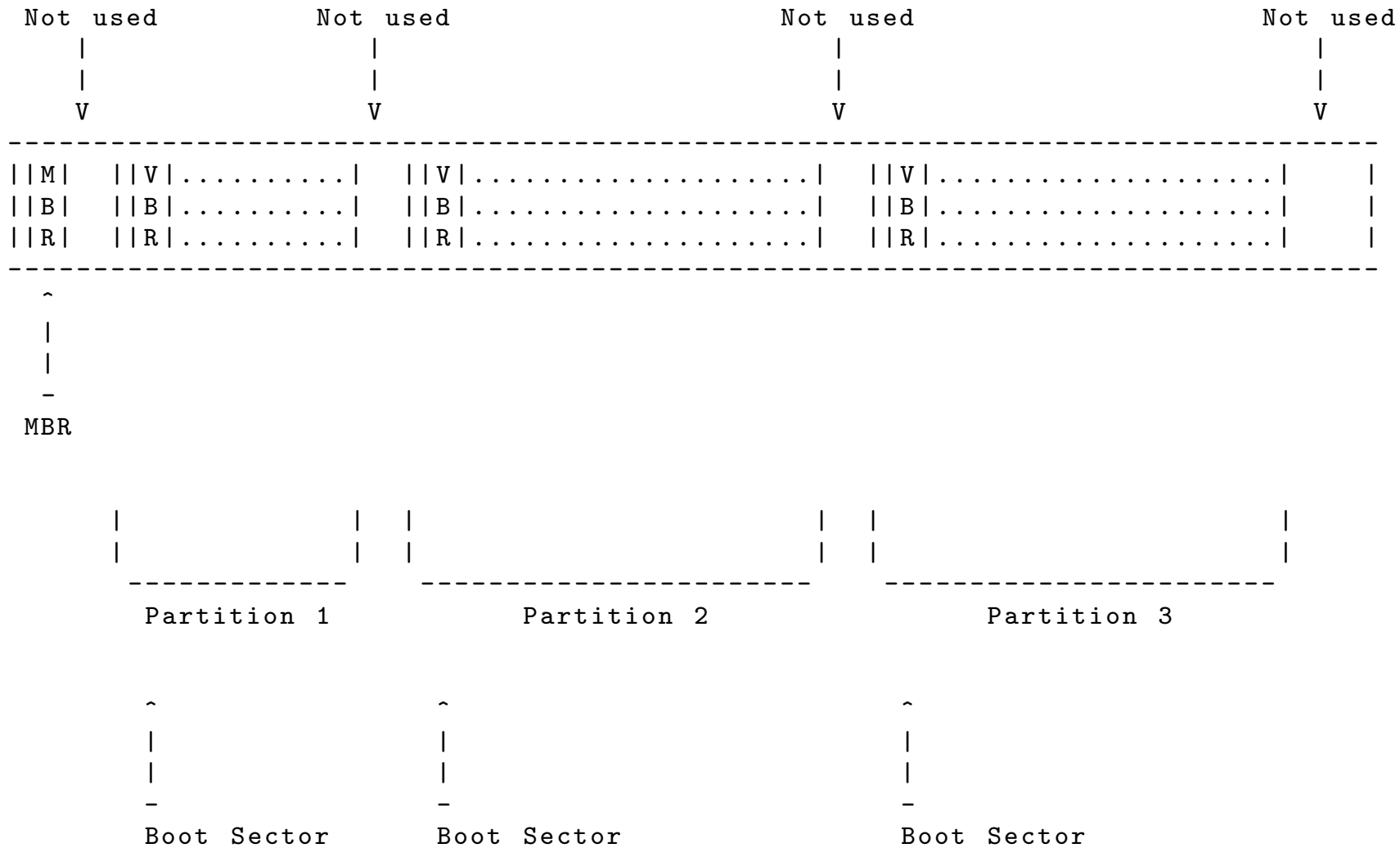
Master Boot Record & Partitioned Disk



Master Boot Record & Partitioned Disk



Master Boot Record & Partitioned Disk

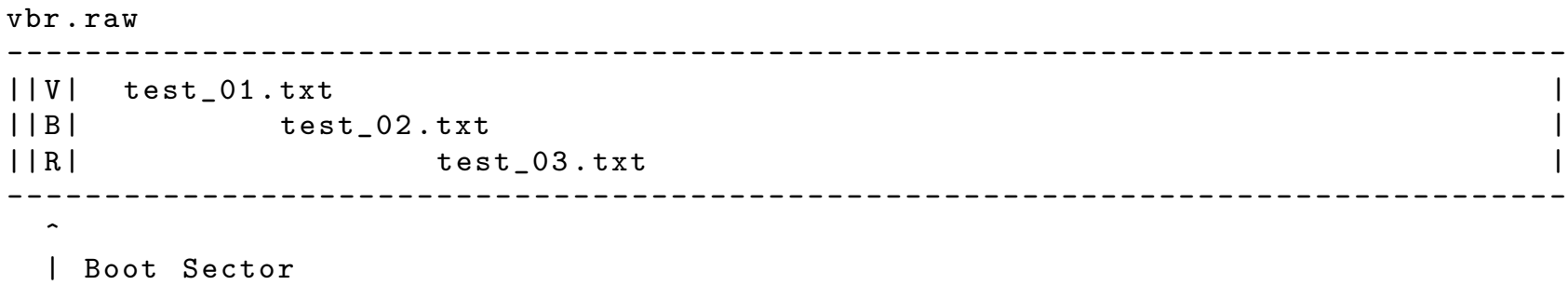


Master Boot Record & Partitioned Disk

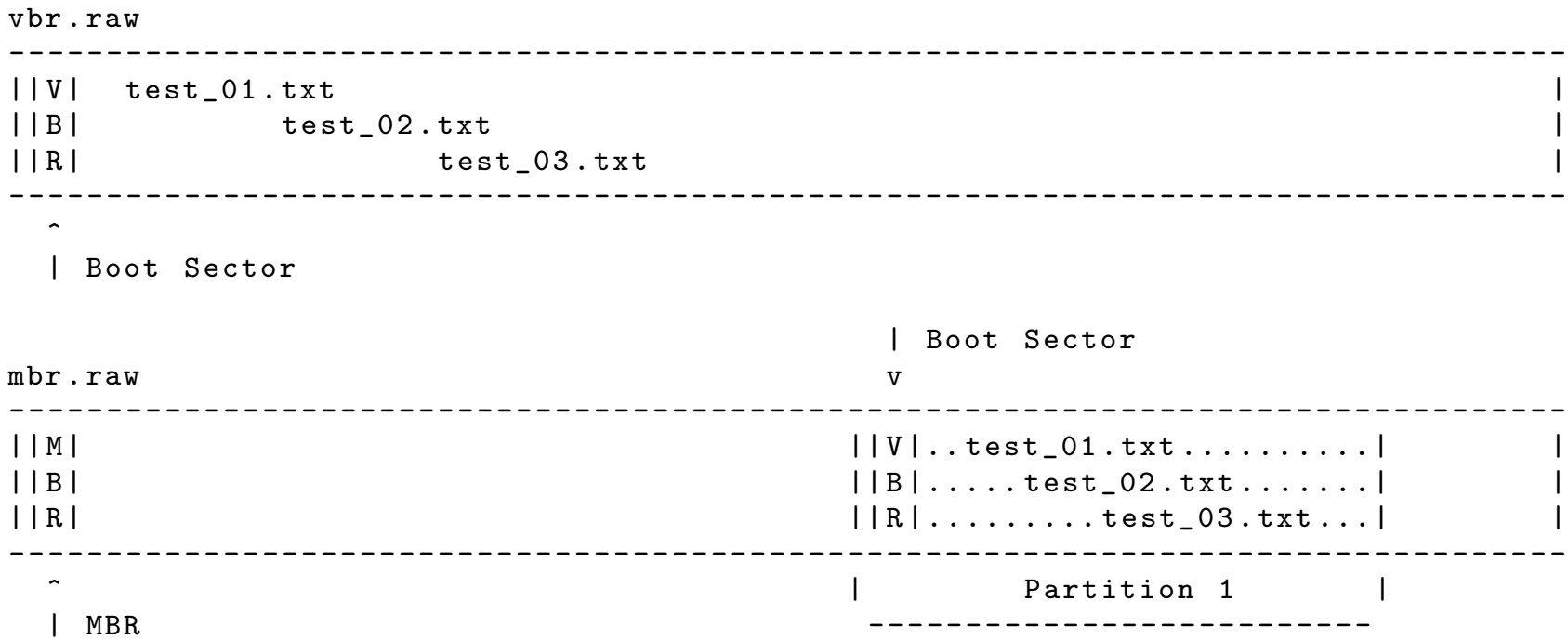
```
00000000: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000010: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
...
000001a0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000001b0: 0000 0000 0000 0000 ce69 d7db 0000 00f5  .........i......
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

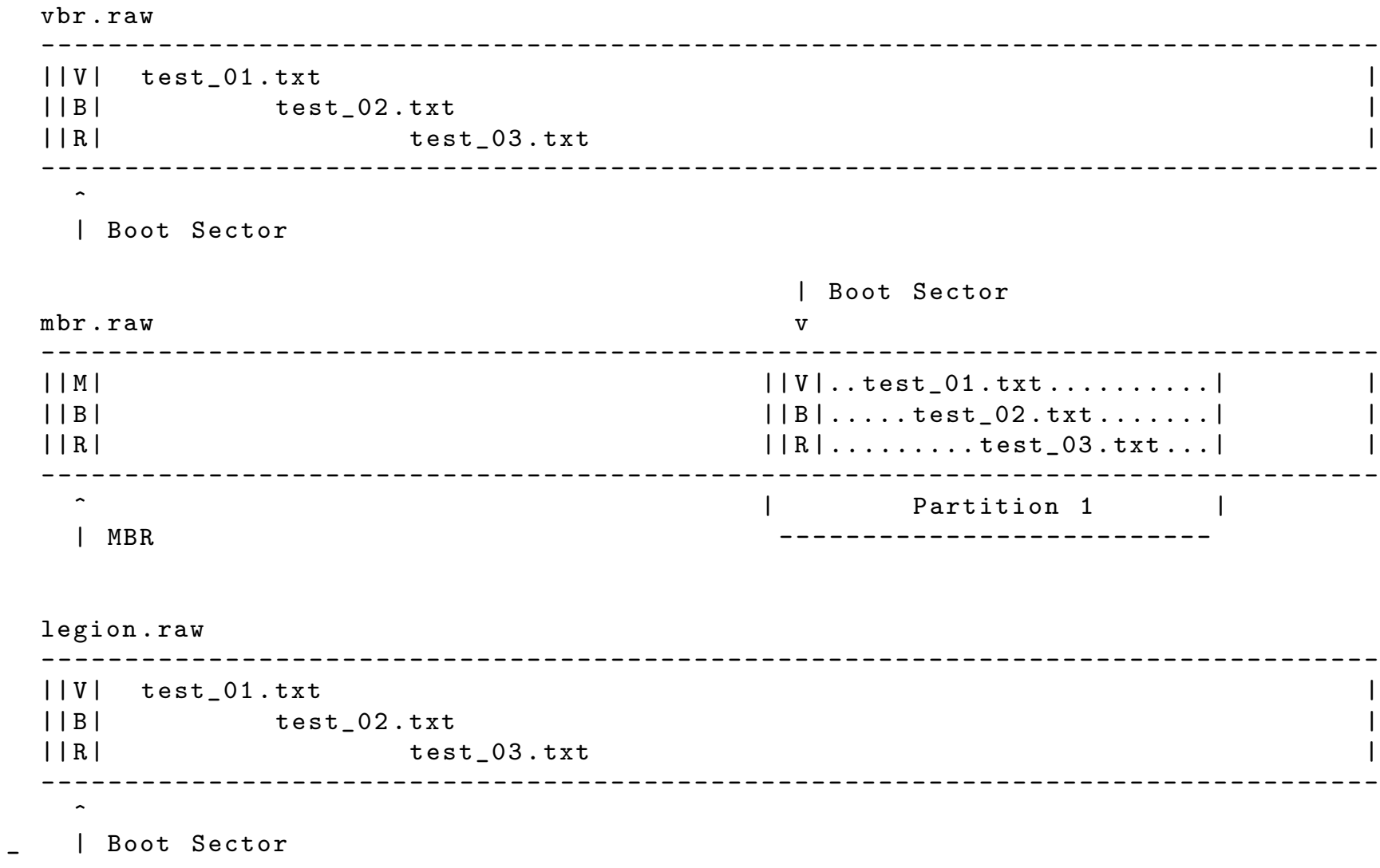
Polyglot Boot Record



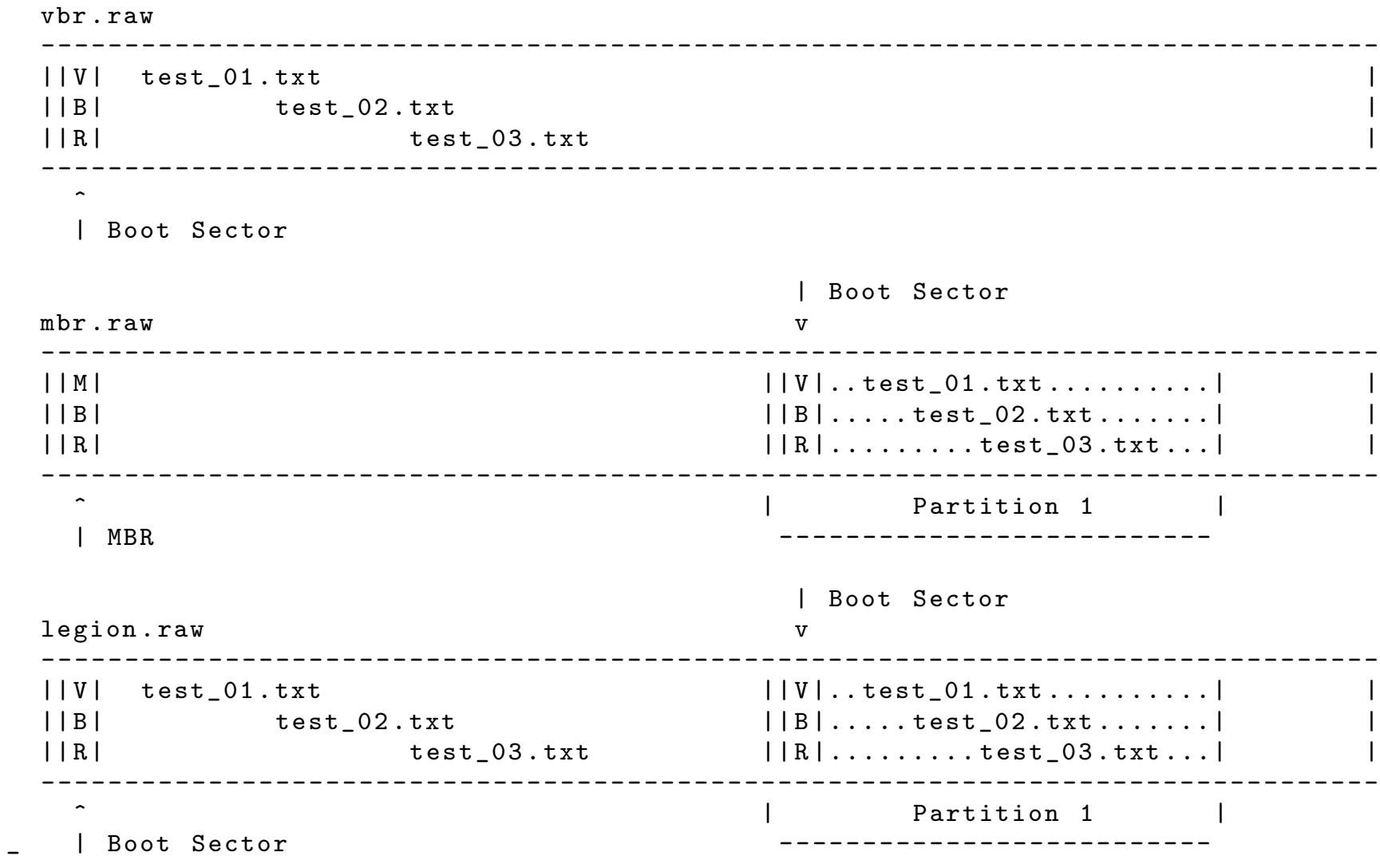
Polyglot Boot Record



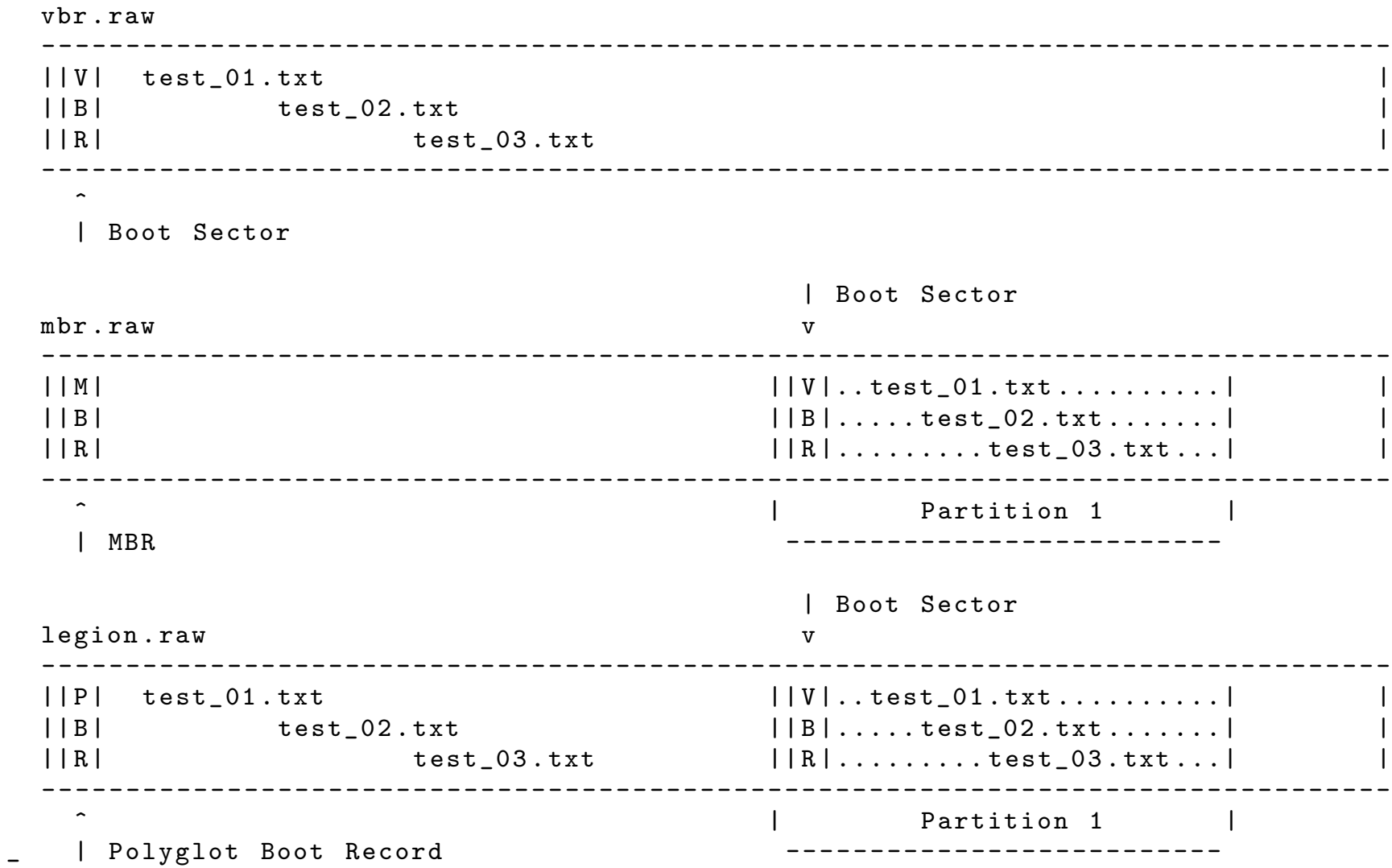
Polyglot Boot Record



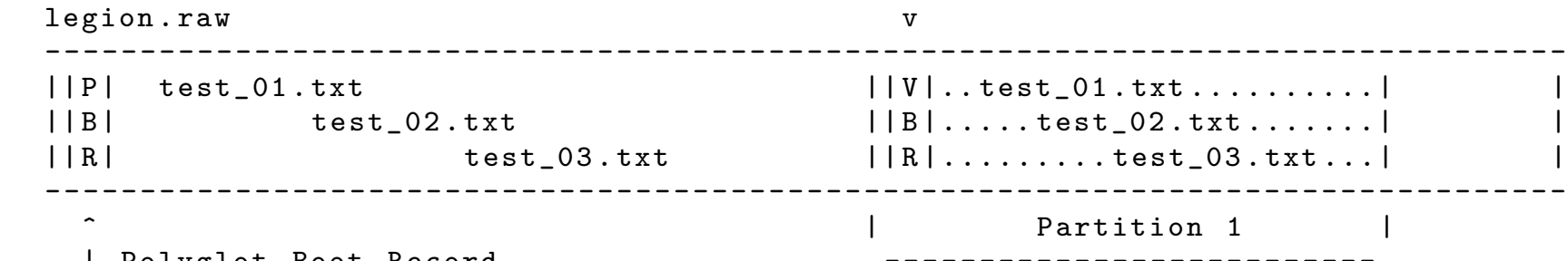
Polyglot Boot Record



Polyglot Boot Record



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  .........?......
00000040: f600 0000 0100 0000 af3c 3363 b6f7 8833  .........<3c...3
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


000001b0: 0000 0000 0000 0000 ce69 d7db 0000 00f5  .........i......
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

As We Are Many: Self Study

Disclaimer!

- use dd
- with root rights
  → Kamikaze - Do not use a production system!

As We Are Many: Self Study

```
---- files
     |-- mbr
     |   |-- test_01.txt
     |   |-- test_02.txt
     |   |-- test_03.txt
     |-- vbr
        |-- test_01.txt
        |-- test_02.txt
        |-- test_03.txt
```

```
1.    Create VBR image
----------------------
1.1   dd if=/dev/zero of=vbr.raw count=262144          # Create 128MByte file
1.2   sudo losetup -f --show vbr.raw
1.3   losetup                                         # Find loopback device
1.4   sudo mkfs.ntfs -L AusCERT2024 /dev/loopXX       # Format device <loop xyz>
1.5   sudo losetup -D                                 # Detach loopback device
```

```
2.    Add some text files
-------------------------
2.1   sudo mkdir /mnt/legion                          # Create mountpoint
2.2   sudo mount vbr.raw /mnt/legion/                 # Mount vbr image
2.3.1 cp files/vbr/test_01.txt /mnt/legion/           # Create test files
2.3.2 cp files/vbr/test_02.txt /mnt/legion/
2.3.3 cp files/vbr/test_03.txt /mnt/legion/
2.4   sudo umount /mnt/legion/
```

As We Are Many: Self Study

```
3.    Create MBR image
----------------------

3.1   dd if=/dev/zero of=mbr.raw count=262144          # Create 128MByte file
3.2   sudo losetup -f --show mbr.raw
3.3   sudo fdisk /dev/loopXX                          # Partition device <loop xyz>
        n                                             # Create partition
        p                                             # middle to end of the disk
        1
        144000                                        # From: 144000
        262143                                        #   To: 262143
        w                                             # -> Do not kill MFT of vbr.raw
3.4   sudo losetup -d /dev/looXX
3.5   sudo losetup -f --show -P mbr.raw              # Format partition
3.6   sudo mkfs.ntfs -L AusCERT2024 /dev/loopXXp1


4.    Add some text files
-------------------------

4.1   sudo mount /dev/loopXXp1 /mnt/legion           # Mount mbr partition
4.2.1 cp files/mbr/test_01.txt /mnt/legion/          # Create test files
4.2.2 cp files/mbr/test_02.txt /mnt/legion/
4.2.3 cp files/mbr/test_03.txt /mnt/legion/
4.3   sudo umount /mnt/legion
4.4   sudo losetup -d /dev/loopXX
-
```

As We Are Many: Self Study

```
5.    Create the polyglot image
------------------------------

5.1   cp vbr.raw legion.raw                          # Take the vbr image as a base
                                                     # to create the legion image

5.2   dd if=mbr.raw of=legion.raw                    # Copy all bytes from the
            skip=144000 seek=144000                  # mbr image partition into
            count=$(( 262143-144000+1 ))             # the legion image
            conv=notrunc

5.3   dd if=mbr.raw of=legion.raw bs=16              # Copy partition table from
            skip=27 seek=27 count=2                  # the mbr image into the
            conv=notrunc                             # legion image

5.4   sudo dd if=legion.raw of=/dev/sdXX             # The legion disk image is ready
            status=progress                          # Write it to a USB stick
```

CIRCL
FORENSICS Training

Q & A