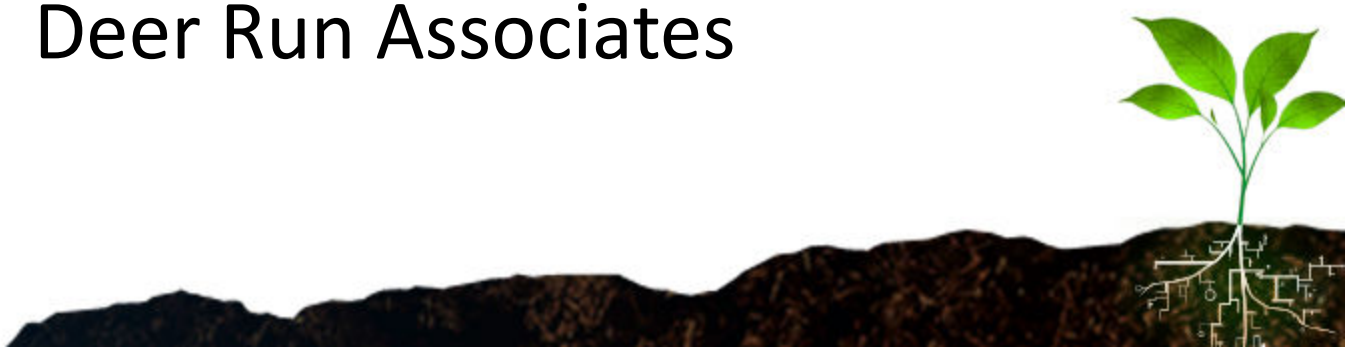
CEIC® 2011

Images and dm-crypt and LVM2… Oh mount!

Hal Pomeranz

Deer Run Associates

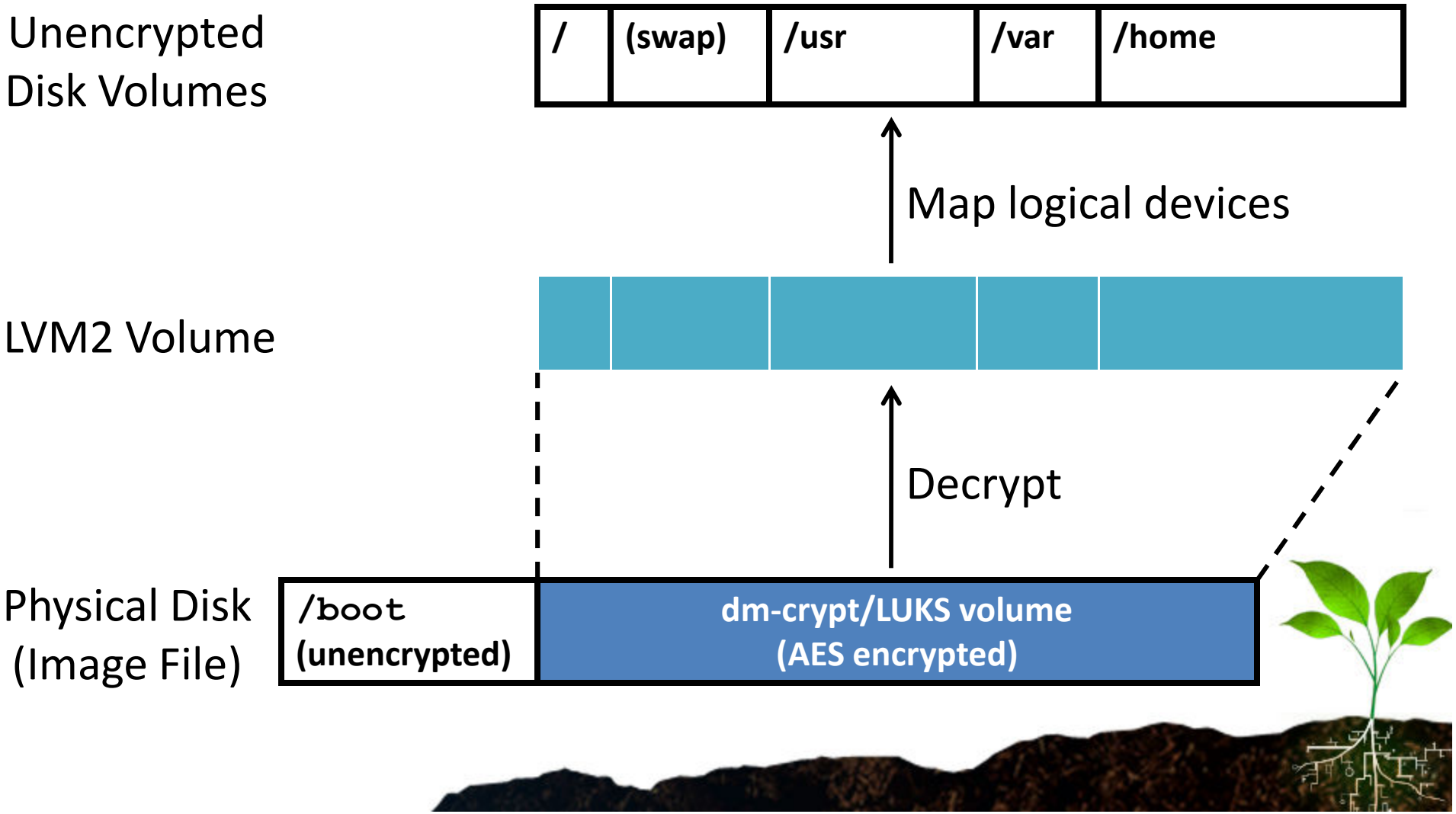


Not Your Grandma's Linux! CEIC 2011

- Default installs create complex disk geometries
- Layers of configuration to penetrate
  - Encrypted volumes
  - Logical volume management

Layers of Complication

CEIC 2011



What's On the Drive?

CEIC 2011

```
# mmls -t dos sda.raw
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

     Slot    Start        End          Length       Description
00:  Meta    0000000000   0000000000   0000000001   Primary Table
01:  -----   0000000000   0000002047   0000002048   Unallocated
02:  00:00   0000002048   0000499711   0000497664   Linux (0x83)
03:  00:01   0000499712   0041940991   0041441280   Linux (0x83)
04:  -----   0041940992   0041943039   0000002048   Unallocated
```

- No swap area?
- Looks like small `/boot` + encrypted volume

Further Details

CEIC 2011

```
# fsstat -o 2048 sda.raw
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: 2c71dce497ca7d83694ea172de905590

Last Written at: Mon Oct 11 08:05:12 2010
Last Checked at: Tue Oct  5 10:04:19 2010

Last Mounted at: Wed Oct  6 08:01:26 2010
Unmounted properly
Last mounted on: /boot
[…]

# fsstat -o 499712 sda.raw
Cannot determine file system type
```

Offset values from **`mmls`** output

Seems to support encryption theory

Further Info on Partition 2

CEIC 2011

- Will be easier to have loopback device
- But losetup wants byte offset, not sector offset

Calculate byte offset from sector offset

```
# expr 499712 \* 512
255852544
# losetup -r -o 255852544 /dev/loop0 sda.raw
# file -s /dev/loop0
/dev/loop0: LUKS encrypted file, ver 1 [aes, cbc-essiv:sha256, sha1]…
```

"-r" for "read-only"

Decryption

CEIC 2011

```
# cryptsetup luksDump /dev/loop0
LUKS header information for /dev/loop0

Version:                1
Cipher name:            aes
Cipher mode:            cbc-essiv:sha256
Hash spec:              sha1
[…]
Key Slot 0: ENABLED
Key Slot 1: DISABLED
Key Slot 2: DISABLED
[…]
# cryptsetup luksOpen /dev/loop0 encrypted
Enter passphrase for /dev/loop0:
Key slot 0 unlocked.
# file -s /dev/mapper/encrypted
/dev/mapper/encrypted: LVM2 (Linux Logical Volume Manager)…
```

No shortcuts here!
Suspect must reveal passphrase…

Find and Activate Volumes

CEIC 2011

```
# pvdisplay /dev/mapper/encrypted
  --- Physical volume ---
  PV Name               /dev/mapper/encrypted
  VG Name               VG000
  PV Size               19.76 GiB / not usable 2.00 MiB
  […]

# vgscan
  Reading all physical volumes.  This may take a while...
  Found volume group "VG000" using metadata type lvm2
  Found volume group "RD" using metadata type lvm2
# vgchange -a y VG000
  5 logical volume(s) in volume group "VG000" now active
```

Logical Volume Info

CEIC 2011

```
# lvscan | grep VG000
  ACTIVE            '/dev/VG000/root' [976.00 MiB] inherit
  ACTIVE            '/dev/VG000/usr' [7.45 GiB] inherit
  ACTIVE            '/dev/VG000/var' [3.72 GiB] inherit
  ACTIVE            '/dev/VG000/swap' [1.86 GiB] inherit
  ACTIVE            '/dev/VG000/home' [5.77 GiB] inherit
# fsstat /dev/VG000/home
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext3
Volume Name:
Volume ID: c1bd1e504c99a5a6514b6b54c1c51749
[…]
Last Mounted at: Wed Oct  6 08:01:29 2010
Unmounted properly
Last mounted on: /home
[…]
```

Accessing Logical Volumes

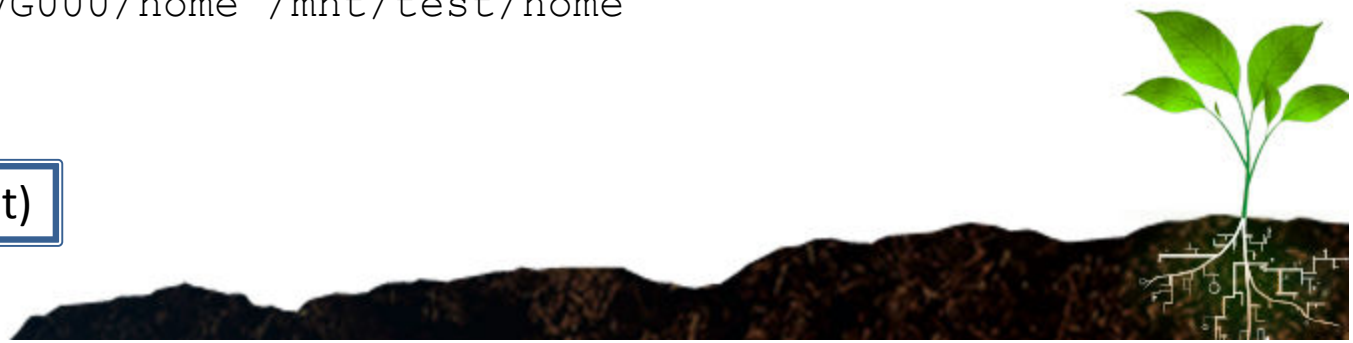
CEIC 2011

```
# dd if=/dev/VG000/home of=home.img
12107776+0 records in
12107776+0 records out
6199181312 bytes (6.2 GB) copied, 92.6313 s, 66.9 MB/s
# dd if=/dev/VG000/swap of=swap.img
3899392+0 records in
3899392+0 records out
1996488704 bytes (2.0 GB) copied, 27.4054 s, 72.9 MB/s
#
#
#
# mount -o ro /dev/VG000/root /mnt/test
# mount -o ro /dev/VG000/usr /mnt/test/usr
# mount -o ro /dev/VG000/var /mnt/test/var
# mount -o ro /dev/VG000/home /mnt/test/home
```

Raw images for your preferred forensic tool

Browse files as local file system

"read-only" (redundant)



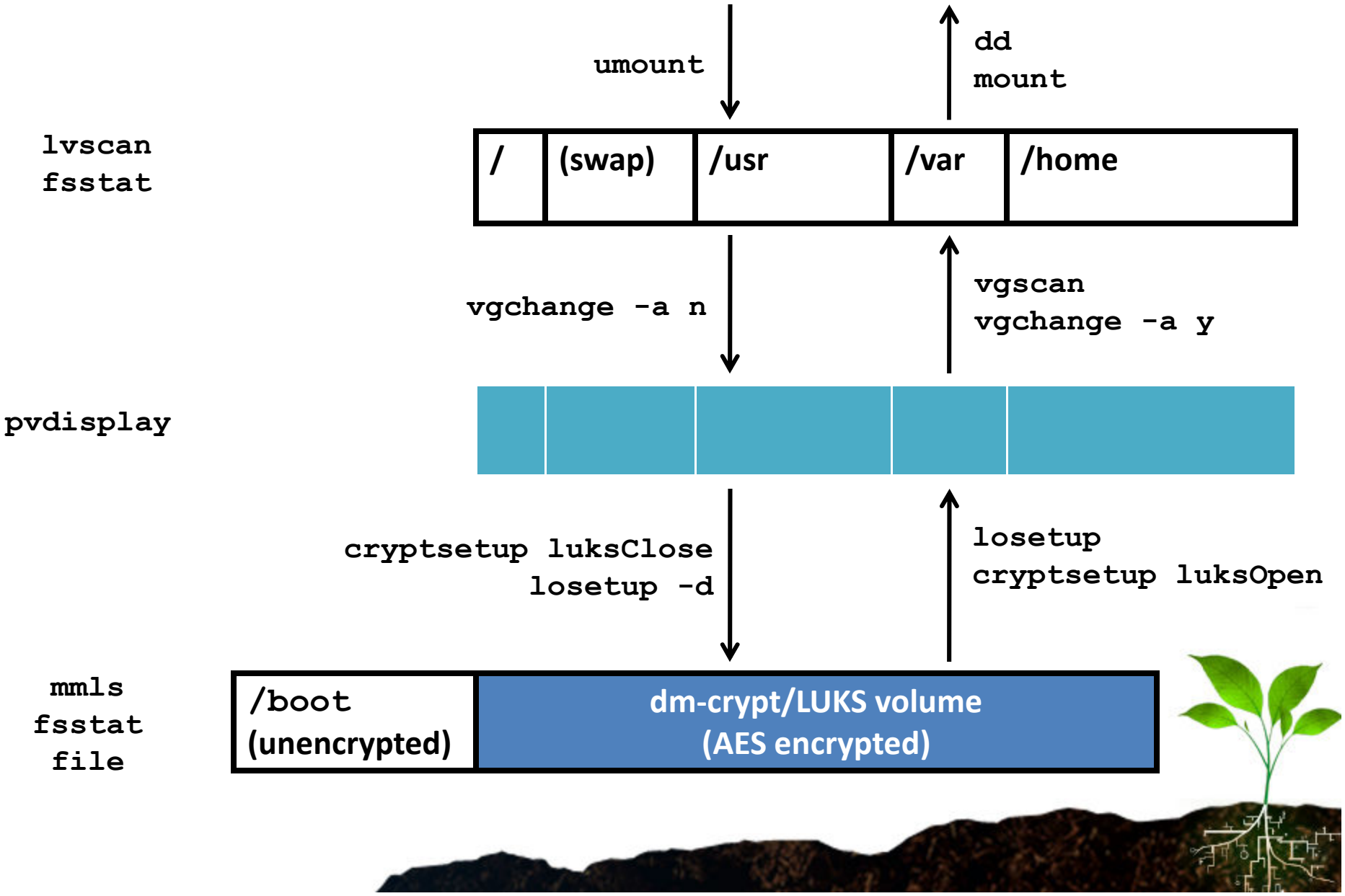
Teardown

CEIC 2011

```
# umount /mnt/test/home
# umount /mnt/test/var
# umount /mnt/test/usr
# umount /mnt/test
#
#
# vgchange -a n VG000
  0 logical volume(s) in volume group "VG000" now active
#
#
# cryptsetup luksClose /dev/mapper/encrypted
#
#
# losetup -d /dev/loop0
```

Commands by Layer

CEIC 2011



Live Response

- Commands can also be used on live systems
- Detect encryption before you “pull the plug”
- Can image logical volumes while system is live
- Saves tiresome interrogation

What Next?

CEIC 2011

- Grab an Ubuntu Alternate ISO and VMware
- Create some disk images for practice
- Practice, practice, practice

Wrapping Up

CEIC 2011

- Any final questions?
- Thanks for listening!

Hal Pomeranz hal@deer-run.com
hal@sans.org

http://www.deer-run.com/~hal/

http://computer-forensics.sans.org/blog/author/halpomeranz/

http://www.sans.org/security-training/instructors/Hal-Pomeranz

https://twitter.com/hal_pomeranz