



Digital Forensics Module Part 2

Jaap van Ginkel
Silvio Oertli

July 2016



Hands-On (Acquisition)



Tools used in the Hands-on Workshop

- We will use open source tools for this part
 - DEFT 8.2 (Forensic Linux distribution)
 - Guymager (Graphical Acquisition Tool)

- Booting Computer with DEFT-CD or USB Stick
 - Depending on the Computer, you need to change Bootingdevice (F2/F6/F9/...)



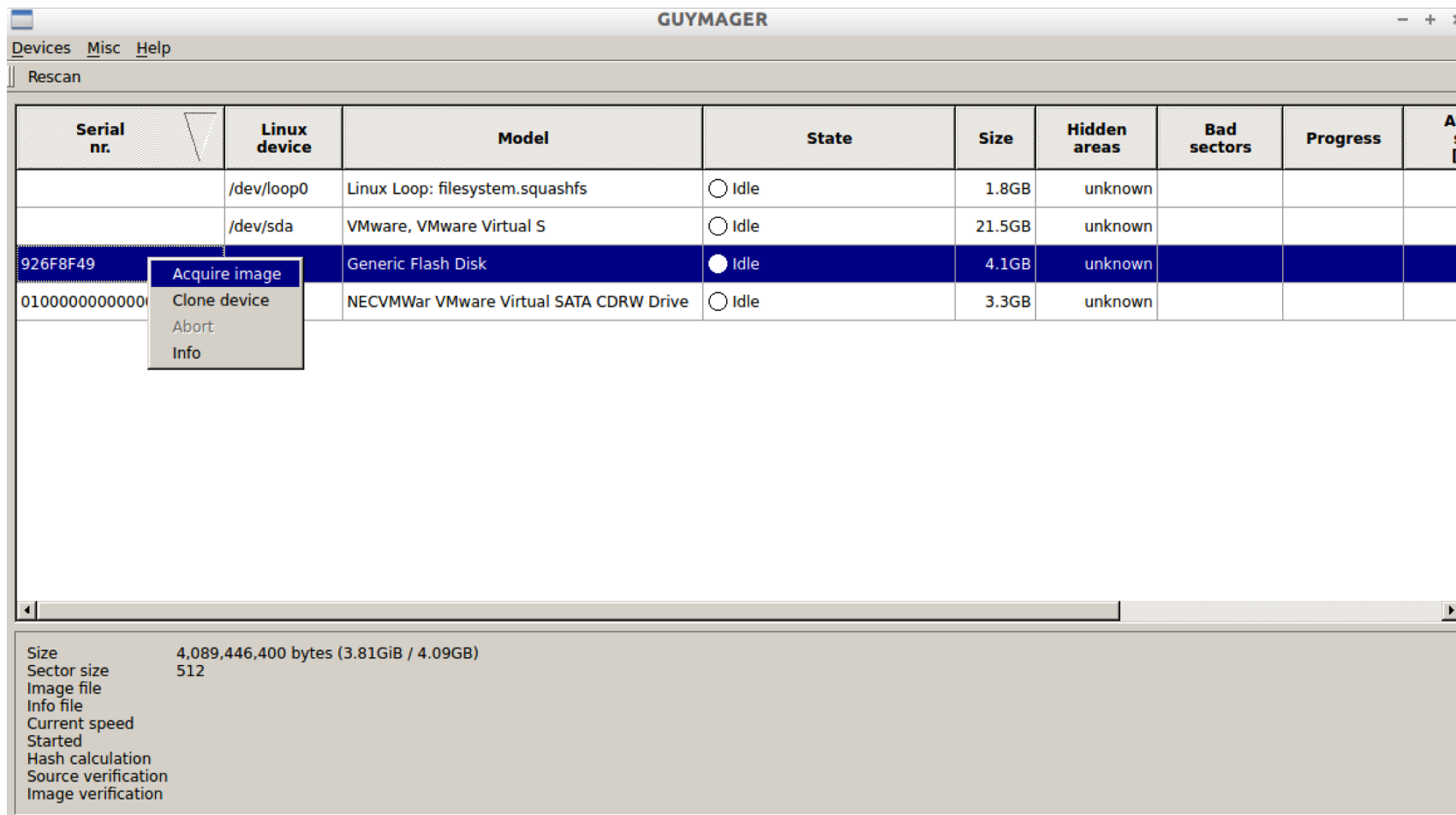
Acquisition

- When you see the Desktop, insert the evidence USB-Stick on the computer
- Doubleclick the Guymager-Icon on the left



Acquisition

- Rightclick on the USB-Stick-Entry and Choose Acquire image



The screenshot shows the GUYMAGER application window. At the top, there are menu options: Devices, Misc, Help. Below the menu is a 'Rescan' button. The main area contains a table with the following columns: Serial nr., Linux device, Model, State, Size, Hidden areas, Bad sectors, Progress, and Avs [I].

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Avs [I]
	/dev/loop0	Linux Loop: filesystem.squashfs	<input type="radio"/> Idle	1.8GB	unknown			
	/dev/sda	VMware, VMware Virtual S	<input type="radio"/> Idle	21.5GB	unknown			
926F8F49		Generic Flash Disk	<input checked="" type="radio"/> Idle	4.1GB	unknown			
01000000000000		NECVMWar VMware Virtual SATA CDRW Drive	<input type="radio"/> Idle	3.3GB	unknown			

A context menu is open over the 'Generic Flash Disk' row, showing the following options: Acquire image, Clone device, Abort, and Info.

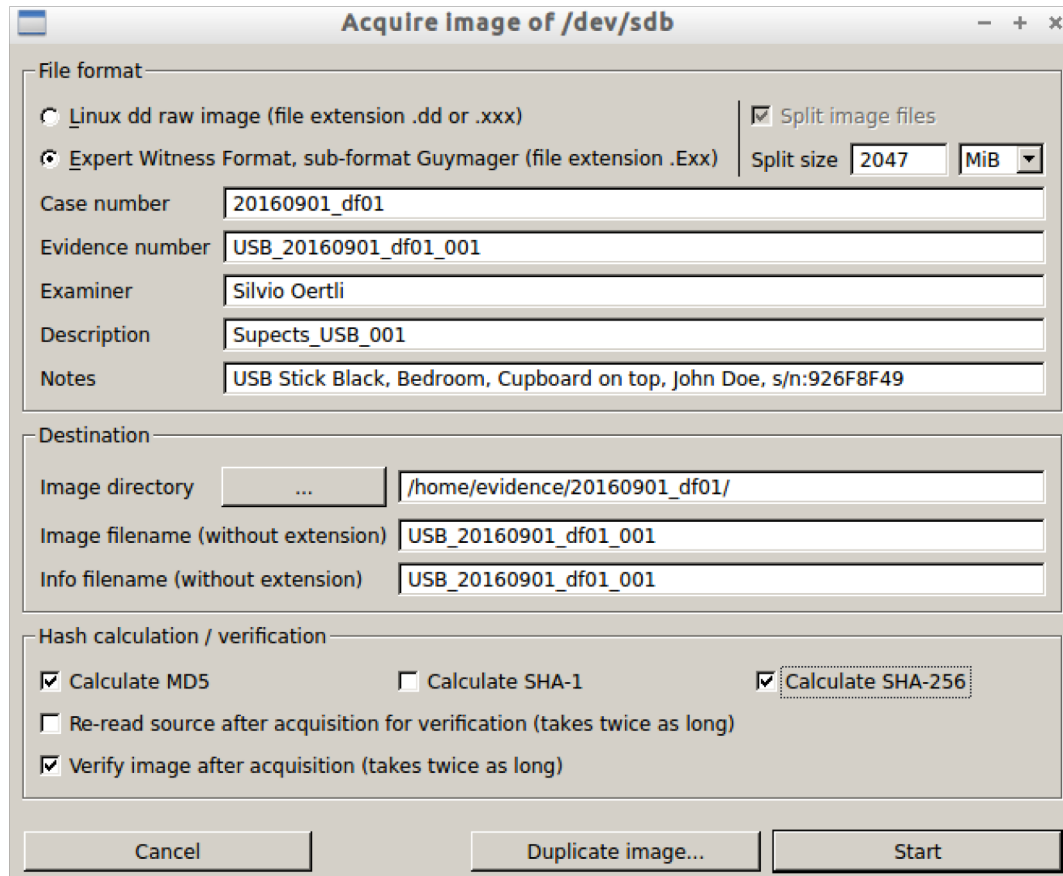
At the bottom of the window, there is a status bar with the following information:

```

Size          4,089,446,400 bytes (3.81GiB / 4.09GB)
Sector size   512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
  
```

Acquisition

- Fill in your Case data



Acquire image of /dev/sdb

File format

Linux dd raw image (file extension .dd or .xxx) Split image files

Expert Witness Format, sub-format Guymager (file extension .Exx) Split size MiB

Case number

Evidence number

Examiner

Description

Notes

Destination

Image directory

Image filename (without extension)

Info filename (without extension)

Hash calculation / verification

Calculate MD5 Calculate SHA-1 Calculate SHA-256

Re-read source after acquisition for verification (takes twice as long)

Verify image after acquisition (takes twice as long)

Cancel Duplicate image... Start

Acquisition

- State turns green after finishing. Your done!

GUYMAGER

Devices Misc Help

Rescan

Serial nr.	Linux device	Model	State	Size	Hidden areas	Bad sectors	Progress	Av s [I
	/dev/loop0	Linux Loop: filesystem.squashfs	<input type="radio"/> Idle	1.8GB	unknown			
	/dev/sda	VMware, VMware Virtual S	<input type="radio"/> Idle	21.5GB	unknown			
926F8F49	/dev/sdb	Generic Flash Disk	<input checked="" type="radio"/> Finished - Verified & ok	4.1GB	unknown	0	100%	
01000000000000000001	/dev/sr0	NECVMWar VMware Virtual SATA CDRW Drive	<input type="radio"/> Idle	3.3GB	unknown			

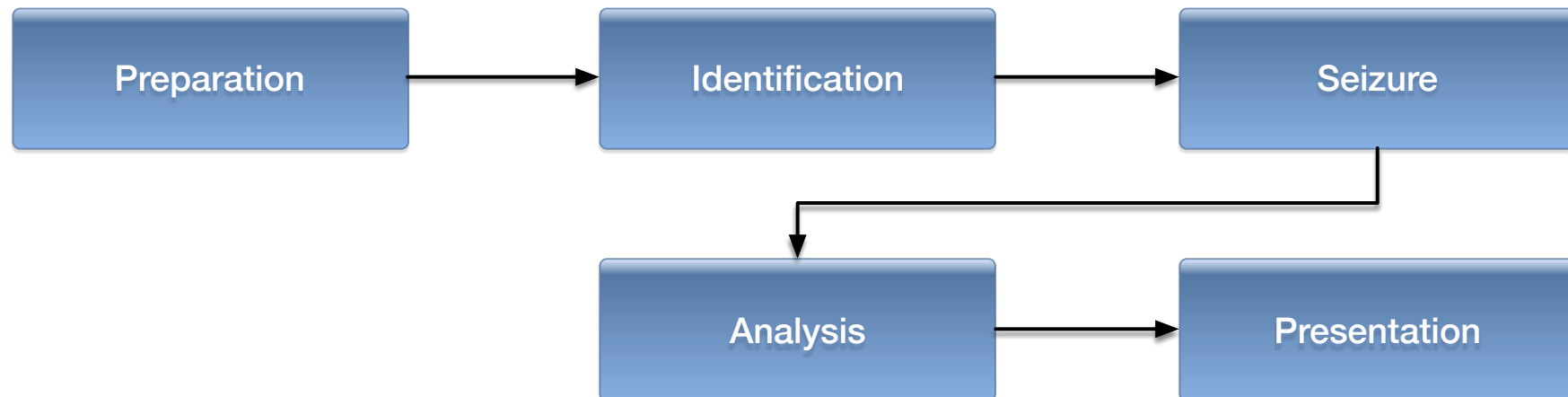
Size 4,089,446,400 bytes (3.81GiB / 4.09GB)
 Sector size 512
 Image file /home/evidence/20160901_df01/USB_20160901_df01_001.Exx
 Info file /home/evidence/20160901_df01/USB_20160901_df01_001.info
 Current speed
 Started 28. August 18:42:55 (00:03:11)
 Hash calculation MD5 and SHA-256
 Source verification off
 Image verification on



Theory in Practice

Scenario

- You're part of the local branch of a global CERT-Team in your country. The main office advice you to seize and analyze all local devices which could contain evidence about dataleakage on Project XXX.



- What to expect on-site...

Preparation



Image Source: <http://images.hayneedle.com/mgen/master:BHI305.jpg>

Image Source: <http://nixuxu.ru/load/344430.jpg>

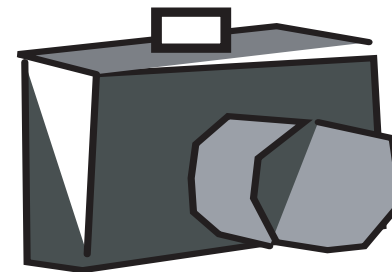


Spot the hidden USB-key...

- Paper and Pencils (yes, even nowadays...)
- Camera
- Tools
 - Screwdrivers (Torx, Crosshead, Flathead, etc.)
 - Tweezers
 - Antistatic wrist strap
 - etc.



Image Source: <http://www.nachi.org/images10/wrap.jpg>





Target Media Preparation

Preparation

- We have to ensure that the target media is empty before we use the device for storing evidence
 - We can re-use storage media if we wipe their content before using it
 - There might even be data on virgin storage media directly coming from the manufacturer
 - Ensure that there is no data from old cases left. This might ruin your day
 - Especially important if no container formats are used (we discuss this in a moment)
 - The commands can be found in the references
- Be careful to specify the right storage media when wiping drives...
- Do not execute the commands in the references during the hands-on exercises!



- Verify your Tools
 - Tools should do what they have to
 - Document the tests

- Use high quality equipment (e.g. Enterprise disks)

Reducing altering

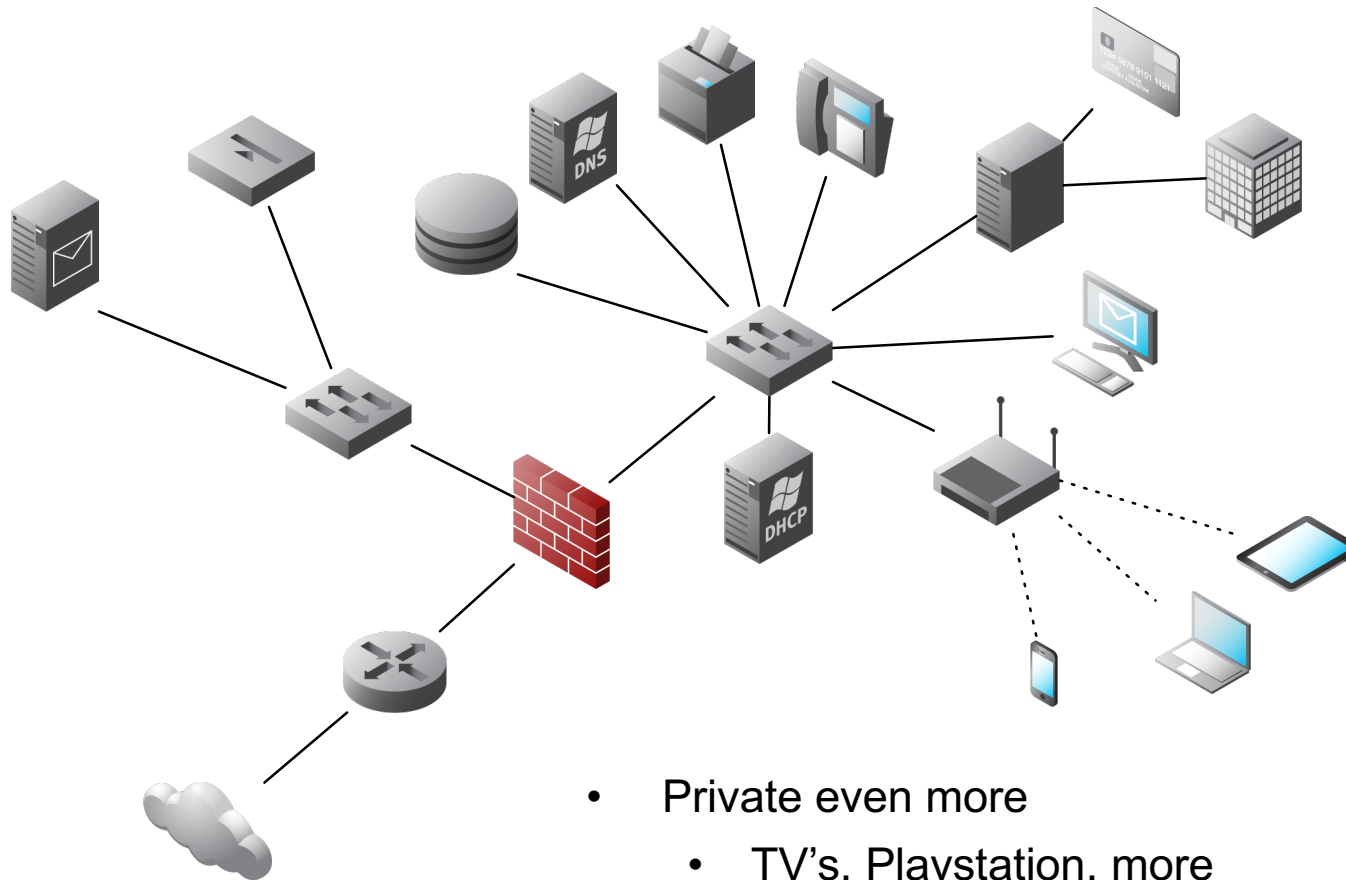
Identification



- Separate Persons from equipment
- Prevent altering evidence by accident or on purpose
- Pay attention on user credential
- Cloud storage

Locating Evidence

Identification



- Private even more
 - TV's, Playstation, more



The ON vs. OFF Debate

Identification

- Depends on the circumstances whether to leave a computer running or to turn it off
- Turning a computer off means losing all volatile evidence
 - RAM
 - Might be a problem with encrypted file systems where the password is not known
- Keeping a computer running means altering evidence
 - Memory content changes constantly
 - Disk is used and file fragments might be overwritten


- Definition from [12]:
 - **Chain of custody** (CoC) refers to the chronological documentation or [paper trail](#), showing the seizure, custody, control, transfer, analysis, and disposition of [evidence](#), physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward [acquittal](#) or to overturning a guilty verdict upon [appeal](#). The idea behind recording the *chain of custody* is to establish that the alleged evidence is in fact related to the alleged crime, rather than having, for example, been *planted* [fraudulently](#) to make someone appear guilty.
- Goal: Prove that the evidence came from or was produced by the suspect and not inserted or altered by the forensics analyst.
- Document who had access (physical and electronic) to the evidence at every given moment.
- Prepare for the worst during an investigation!
 - Quick-and-dirty approach → Other party might sue the investigator afterwards or court rejects the evidence

Evidence Handling

Seizure

- Forensic Logbook

Forensics Workshop
Logbook for exercises




Case No.: _____

Log book No.: _____ / _____

Date: _____

Version: 1.0, March 2016

Classification:  TLP-RED

1. Case Overview

Examiner(s):

Name / Examiner _____

Phone _____

Mail _____

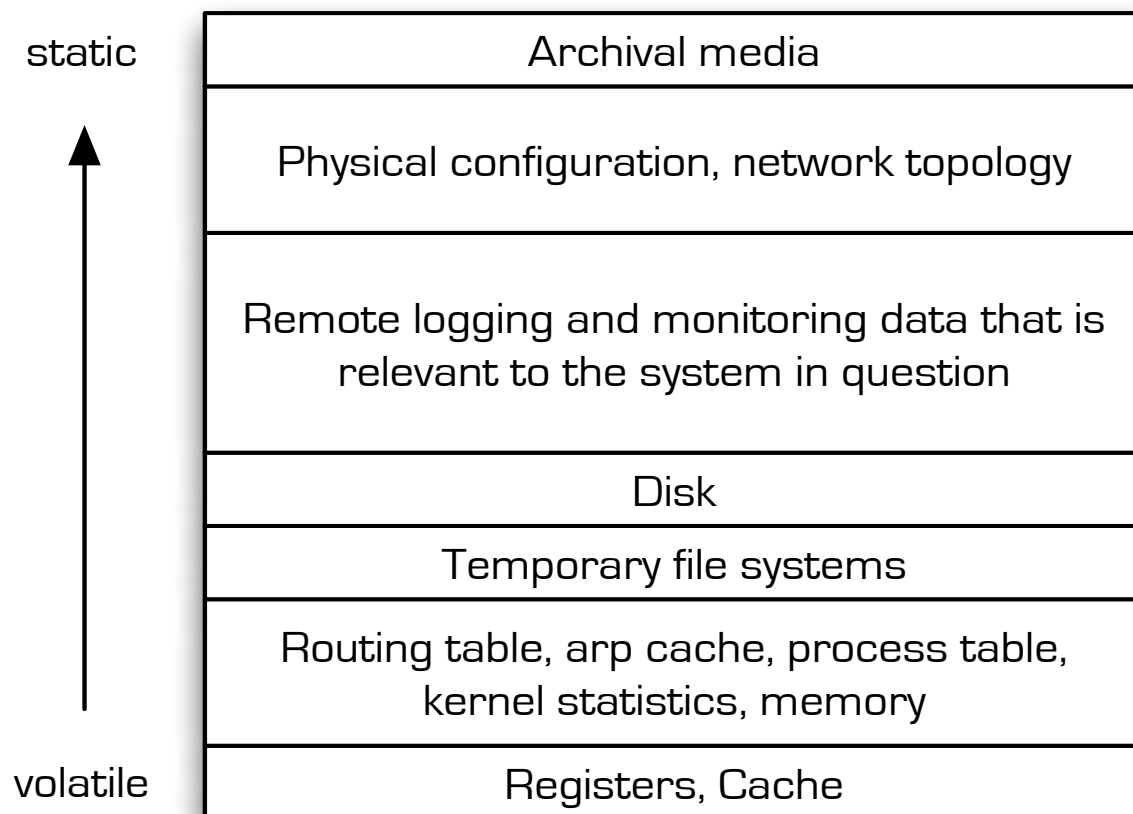
Logbook:

No.	Date	Time	<u>Examiner</u>	Action
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Order of Volatility

Seizure

- Taken from [13]: Guidelines for Evidence Collection and Archiving



Write Blockers

- Altering evidence must be avoided either
 - with software
 - Mounting read-only
 - with hardware
 - Some hard disks (eg. SCSI drives) have jumpers
 - Forensic write blockers
- The suggested way to go is hardware write blockers
 - Depends on circumstances

Seizure

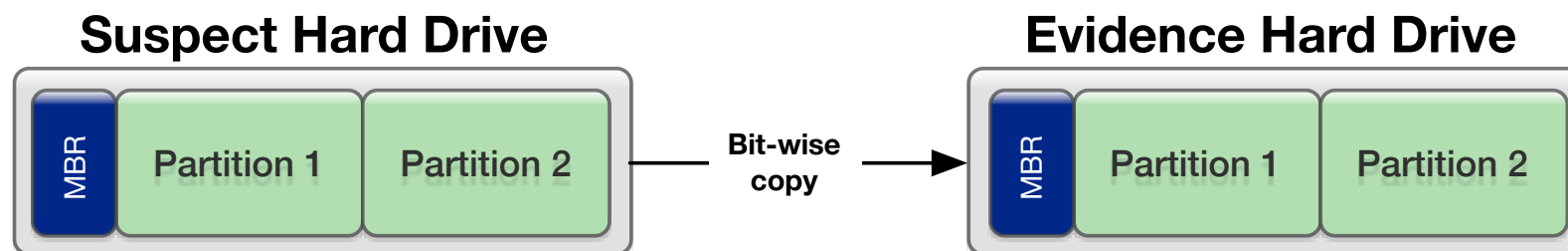


Image Source: <https://www2.guidancesoftware.com/products/Pages/tableau/products/forensic-bridges/t35es-r2.aspx>

Raw Copy vs. Container Format

Seizure

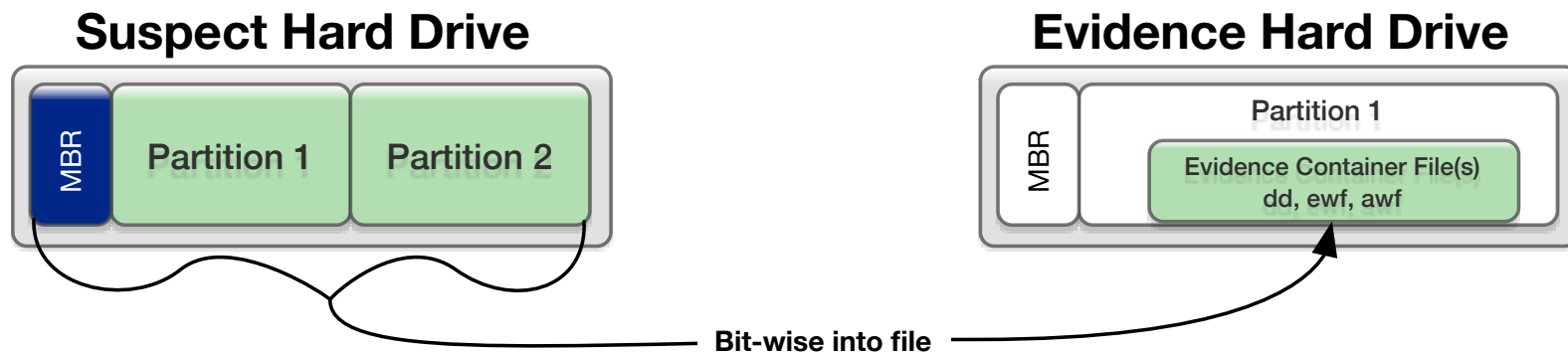
- Raw Copy
 - 1:1 copy using dd from a physical drive to identical physical drive
 - Forensically sound
 - Not very convenient to work with
 - Can only be used for single devices such as hard drives, memory sticks, etc.
 - Not possible to store on servers using this method
 - Deprecated for most situations



Raw Copy vs. Container Format

Seizure

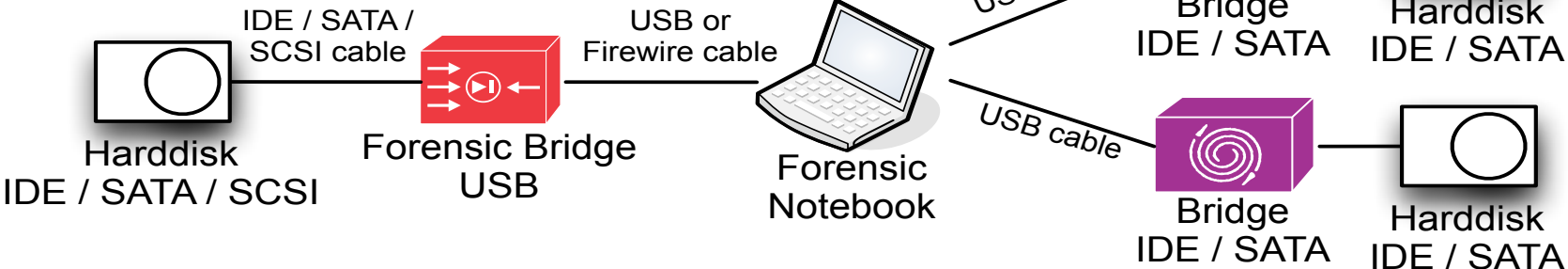
- Container Format
 - 1:1 copy from a physical drive into a (forensic) container file
 - Forensically sound
 - Libraries and tools available to work conveniently with containers
 - Container files can be stored everywhere including Servers
 - This approach is used most often nowadays



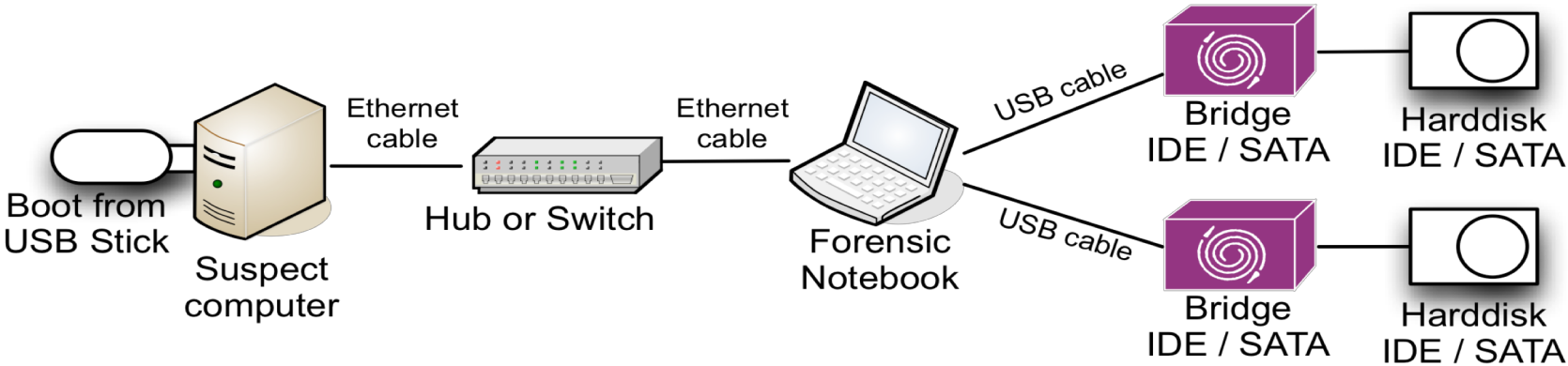
Imaging Scenarios

Seizure

- Disk Imaging



- Imaging over a Network

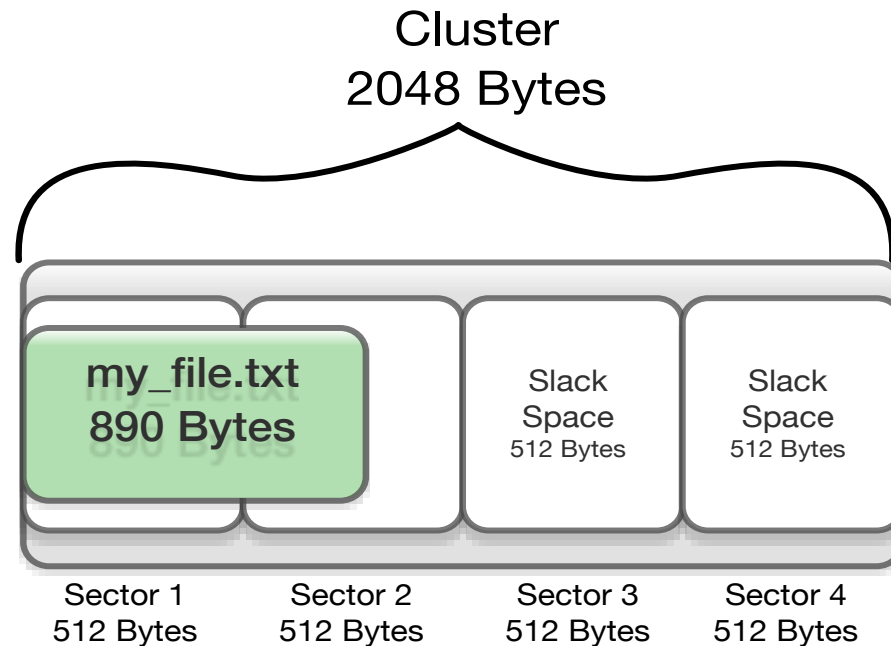


Physical vs. Logical

Seizure

- Physical
 - RAID → disk configuration
 - Good environment 80GB/hour
 - Get all included deleted files

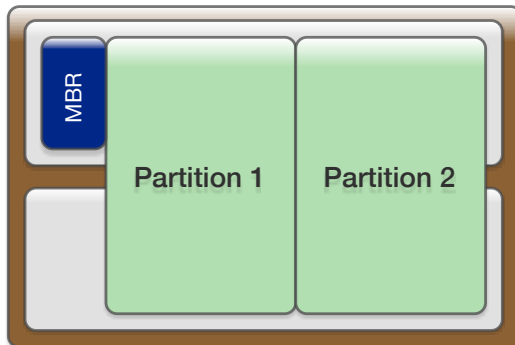
- Logical
 - Fast



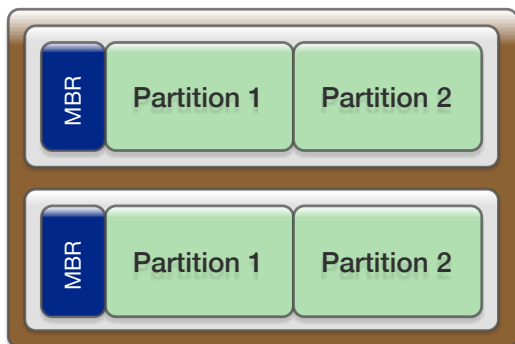
Redundant Array of Independent Disks

Seizure

- RAID 0 (stripe)



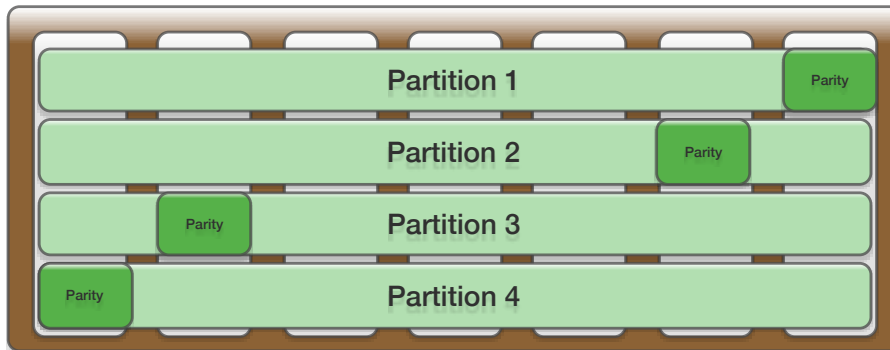
- RAID 1 (mirror)
 - 1:1 copy on both disks



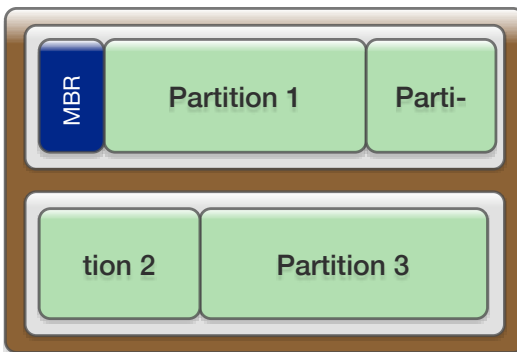
Redundant Array of Independent Disks

Seizure

- RAID 5
 - Speed and Redundancy



- Just a bunch of disks (JBOD)



Hashing

Seizure

54 68 69 73	20 74 65 78	74 20 73 68	6F 75 6C 64	20 73 68 6F	77 20 74 68	65 20 69 6E	66 6C 75 65	This text should show the influence of altering just one bit in a text to the hash-result..2..E0 F.
6E 63 65 20	6F 66 20 61	6C 74 65 72	69 6E 67 20	6A 75 73 74	20 6F 6E 65	20 62 69 74	20 69 6E 20	
61 20 74 65	78 74 20 74	6F 20 74 68	65 20 68 61	73 68 2D 72	65 73 75 6C	74 2E 0A 32	0A 0A 45 4F	
46 0A						74 2E 0A 33		

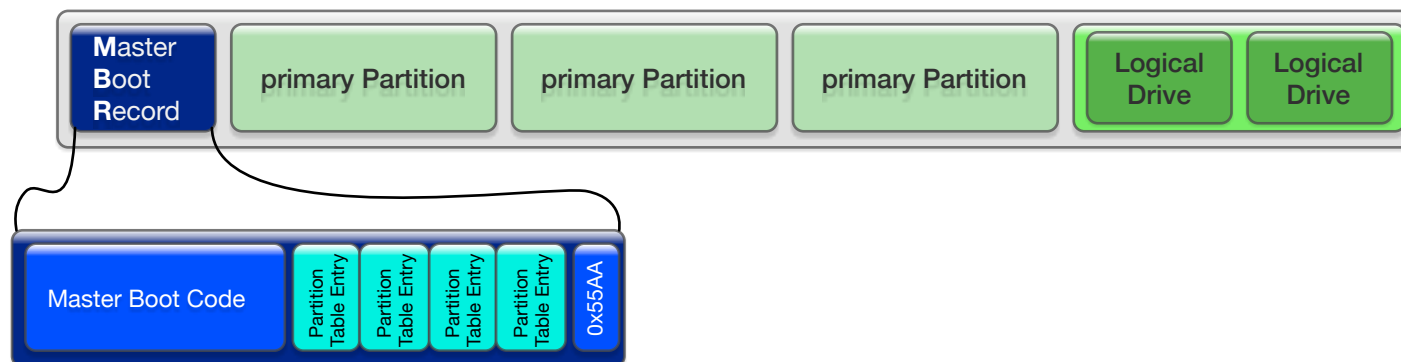
- shasum -a 256 test.txt
 - 2f50fe79a03391be5b8001606b030f26a5e8fe1dfdb137f7e28d74d2accfc3e9

54 68 69 73	20 74 65 78	74 20 73 68	6F 75 6C 64	20 73 68 6F	77 20 74 68	65 20 69 6E	66 6C 75 65	This text should show the influence of altering just one bit in a text to the hash-result..3..E0 F.
6E 63 65 20	6F 66 20 61	6C 74 65 72	69 6E 67 20	6A 75 73 74	20 6F 6E 65	20 62 69 74	20 69 6E 20	
61 20 74 65	78 74 20 74	6F 20 74 68	65 20 68 61	73 68 2D 72	65 73 75 6C	74 2E 0A 33	0A 0A 45 4F	
46 0A						74 2E 0A 33		

- shasum -a 256 test.txt
 - 6f9ea996741487099e783bba8654f2e09c194e8e0eb37f33cd0549c360e493b2

- Master Boot Record (MBR)

- Up to 4 primary Partitions
- Up to 2 TB per Disk



- Globally Unique Identifier Partitiontable (GPT)

- Up to 128 Partitions
- 2^{64} Blocks \rightarrow 9.4 Zetabyte



Mounting an image

Analysis

- ewfmount uses FUSE (Filesystem in Userspace) to mount your evidence
 - sudo mkdir /mnt/evidence
 - ewfmount /home/evidence/20160901_df01/USB_20160901_df01_001.E01 /mnt/evidence

```
root:~  
File Edit Tabs Help  
deft8 ~ % ewfmount /home/evidence/20160901_df01/USB_20160901_df01_001.E01 /mnt/evidence  
ewfmount 20130416  
  
deft8 ~ % ls -la /mnt/evidence/  
total 0  
drwxr-xr-x  2 root root          0 Jan  1  1970 .  
drwxr-xr-x 10 root root        60 Aug 28 18:54 ..  
-r--r--r--  1 root root 4089446400 Aug 28 18:56 ewf1  
deft8 ~ %
```

Mounting an image

Analysis

- Check partition table
 - mmls /mnt/evidence/ewf1

```
root:~/evidence/20160901_df01
File Edit Tabs Help
deft8 ../evidence/20160901_df01 % mmls /mnt/evidence/ewf1
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

  Slot      Start          End            Length        Description
00:  Meta     0000000000    0000000000    0000000001    Primary Table (#0)
01:  -----   0000000000    0000000127    0000000128    Unallocated
02:  00:00    0000000128    0006285439    0006285312    NTFS (0x07)
03:  -----   0006285440    0007987199    0001701760    Unallocated
deft8 ../evidence/20160901_df01 %
```

Mounting an image

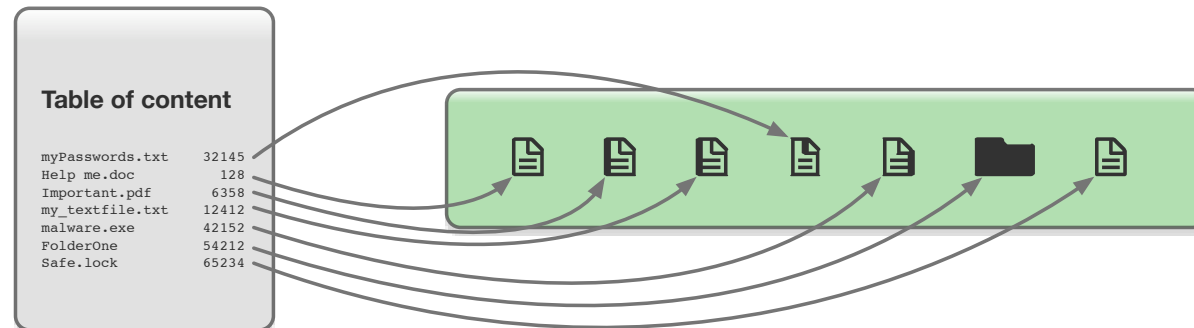
Analysis

- Mount Windowspartition (NTFS)
 - mkdir windows_mount
 - mount -o ro,loop,show_sys_files,streams_interface=windows,offset=65536 -t ntfs /mnt/evidence/ewf1 /mnt/windows_mount

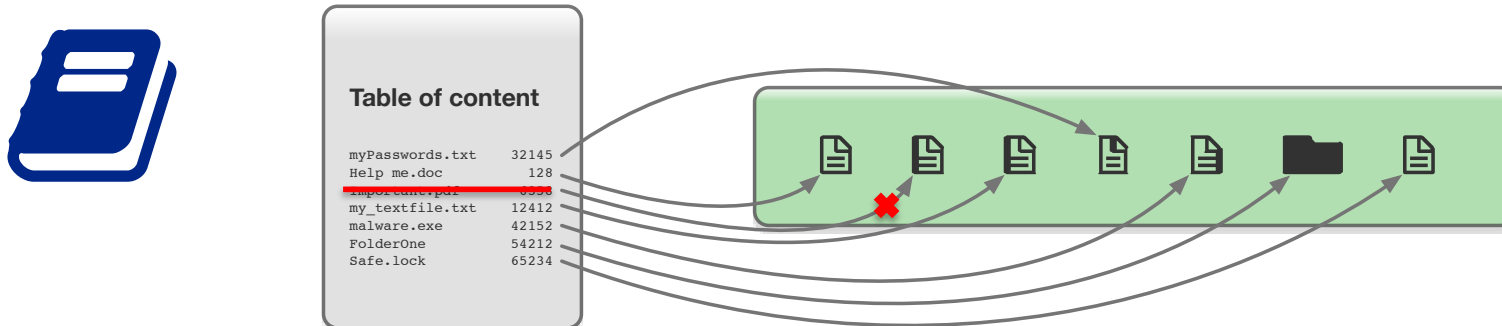
[128*512]

```
root:~  
File Edit Tabs Help  
deft8 ~ % mount -o ro,loop,show_sys_files,streams_interface=windows,offset=65536 -t ntfs /mnt/evidence/ewf1 /mnt/windows_mount/  
deft8 ~ % ls -la /mnt/windows_mount/  
total 7768  
drwxrwxrwx 1 root root 4096 Aug 25 09:36 .  
drwxr-xr-x 11 root root 80 Aug 28 19:23 ..  
-rwxrwxrwx 1 root root 2560 Aug 25 07:39 $AttrDef  
-rwxrwxrwx 1 root root 0 Aug 25 07:39 $BadClus  
-rwxrwxrwx 1 root root 98208 Aug 25 07:39 $Bitmap  
-rwxrwxrwx 1 root root 8192 Aug 25 07:39 $Boot  
drwxrwxrwx 1 root root 0 Aug 25 07:39 $Extend  
-rwxrwxrwx 1 root root 7700480 Aug 25 07:39 $LogFile  
-rwxrwxrwx 1 root root 4096 Aug 25 07:39 $MFTMirr  
drwxrwxrwx 1 root root 0 Aug 25 08:25 $RECYCLE.BIN  
----- 1 root root 0 Aug 25 07:39 $Secure  
drwxrwxrwx 1 root root 0 Aug 25 09:37 System Volume Information  
-rwxrwxrwx 1 root root 131072 Aug 25 07:39 $UpCase  
drwxrwxrwx 1 root root 4096 Aug 25 08:27 Users  
-rwxrwxrwx 1 root root 0 Aug 25 07:39 $Volume  
drwxrwxrwx 1 root root 0 Aug 25 09:45 Windows  
deft8 ~ %
```

- A lot of different Filesystems (ntfs, FAT, HFS+, ext2, ZFS)
- But all like Books (table of contents → pages)



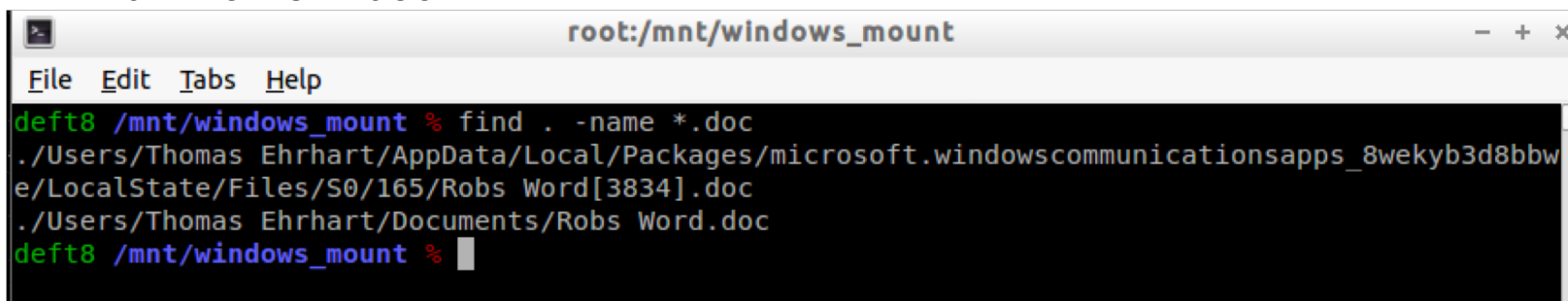
- A lot of different Filesystems (ntfs, FAT, HFS+, ext2, ZFS)
- But all like Books (table of contents → pages)



- Deleting Files just deletes or marks Entry in “Table of content”
 - File still exists on the Harddrive

- Finding Documents by name

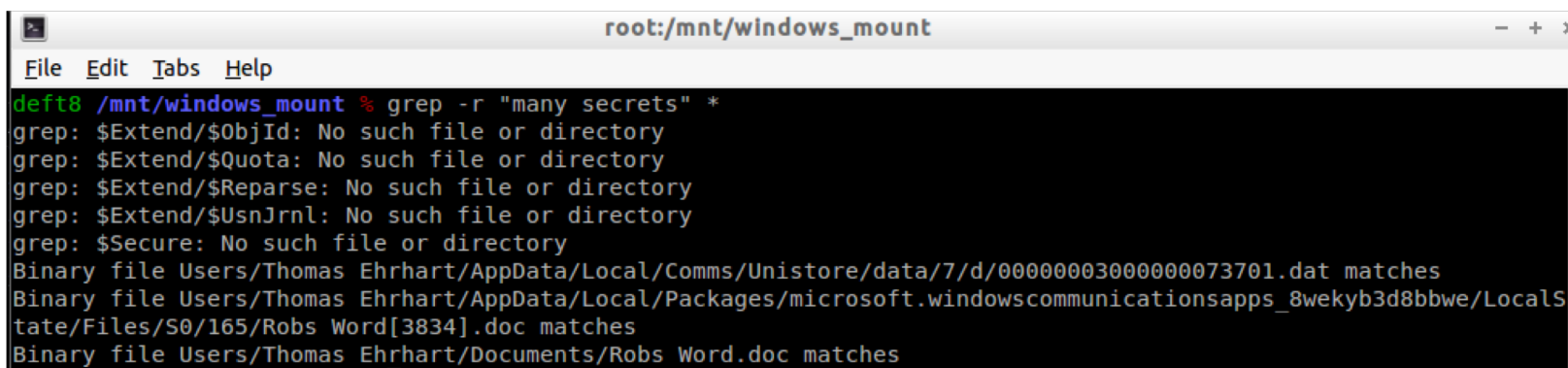
- find . -name "*.doc"



```
root:/mnt/windows_mount
File Edit Tabs Help
deft8 /mnt/windows_mount % find . -name *.doc
./Users/Thomas Ehrhart/AppData/Local/Packages/microsoft.windowscommunicationsapps_8wekyb3d8bbwe/LocalState/Files/S0/165/Robs Word[3834].doc
./Users/Thomas Ehrhart/Documents/Robs Word.doc
deft8 /mnt/windows_mount %
```

- Finding Documents with specific content

- grep -r "many secrets" .



```
root:/mnt/windows_mount
File Edit Tabs Help
deft8 /mnt/windows_mount % grep -r "many secrets" *
grep: $Extend/$ObjId: No such file or directory
grep: $Extend/$Quota: No such file or directory
grep: $Extend/$Reparse: No such file or directory
grep: $Extend/$UsnJrnl: No such file or directory
grep: $Secure: No such file or directory
Binary file Users/Thomas Ehrhart/AppData/Local/Comms/Unistore/data/7/d/00000003000000073701.dat matches
Binary file Users/Thomas Ehrhart/AppData/Local/Packages/microsoft.windowscommunicationsapps_8wekyb3d8bbwe/LocalState/Files/S0/165/Robs Word[3834].doc matches
Binary file Users/Thomas Ehrhart/Documents/Robs Word.doc matches
```

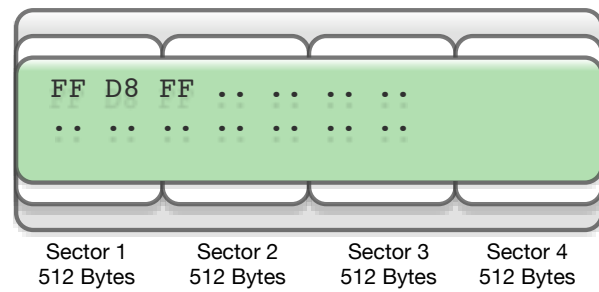
Evidence on File systems

Analysis

- Finding Document of specific format in unallocated space
 - Carving (Scalpel)
 - Filesystems magic numbers

- Officefiles (bin): 0xD0CF11
- Officefiles (zip): 0x504B04
- JPG: 0xFFD8FF
- GIF: 0x474946383761
- PDF: 0x25504446
- EXE: 0x4D5A

- PK..
- ÿØÿ
- GIF87a
- %PDF
- MZ



- Artifacts of programs can be on different places in different formats
 - \$USER/AppData/*
 - Example AppData/Roaming/Mozilla/Firefox/Profiles/m3k5a7px.default/formhistory.sqlite
 - Open with sqlitebrowser

SQLite Database Browser - formhistory.sqlite

File Edit View Help

Database Structure Browse Data Execute SQL

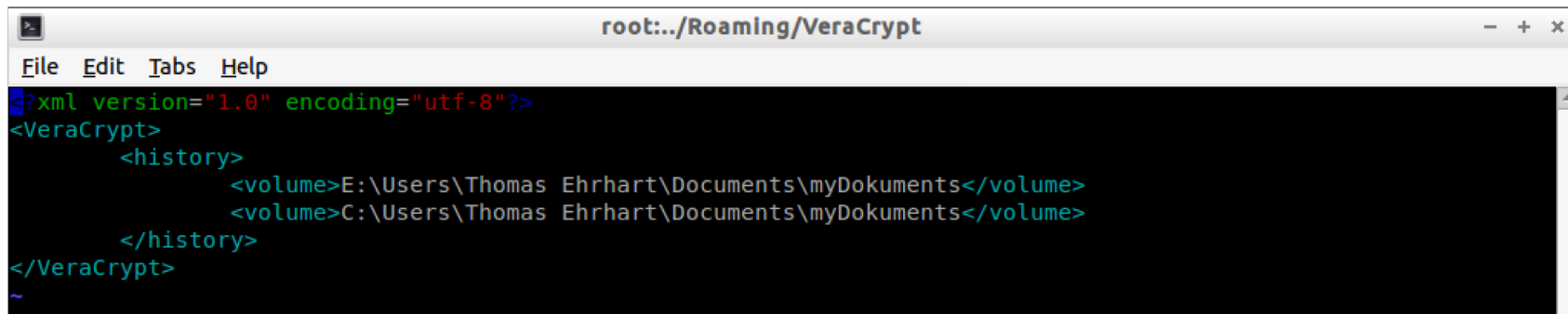
Table: moz_formhistory

id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	1 FirstName	Thomas	4	77119239000	84889523000	218MSrpCRRC
2	2 LastName	Ehrhart	4	77119239000	84889523000	sKUnF/oySFy0
3	3 BirthDay	16	1	77119239000	77119239000	ROvP+KcmRyy
4	4 BirthYear	1971	1	77119239000	77119239000	06QZ/BaDQla
5	5 RecoveryPhon	+355	1	77119239000	77119239000	EORLF/llTam3
6	6 deviceAddress	15735992947	1	77316277000	77316277000	QFjAKac5T/69
7	7 deviceAddress	476856082	1	77358332000	77358332000	20LEOXFFT7Ct
8	8 deviceAddress	0476 856 082	1	77380090000	77380090000	vPExlxFNSDyC
9	9 deviceAddress	76800200313	1	77881027000	77881027000	hTUkg0DQSxn
10	10 deviceAddress	1254375066	1	77928766000	77928766000	2a202yu9QNS
11	11 deviceAddress	1254375054	1	77941097000	77941097000	huY46mbhSxy
12	12 deviceAddress	2048151582	1	77968874000	77968874000	9rRo8vQuR6e
13	13 deviceAddress	2263142727	1	77983690000	77983690000	dmeQmZ1OQ
14	14 deviceAddress	6572564871	1	78002369000	78002369000	9XS0XRMLQX2
15	15 deviceAddress	6572564891	1	78008324000	78008324000	JYA2iyNFQI6FI
16	16 deviceAddress	752913072	1	78090648000	78090648000	QOr5CX94SK6

1 - 22 of 22

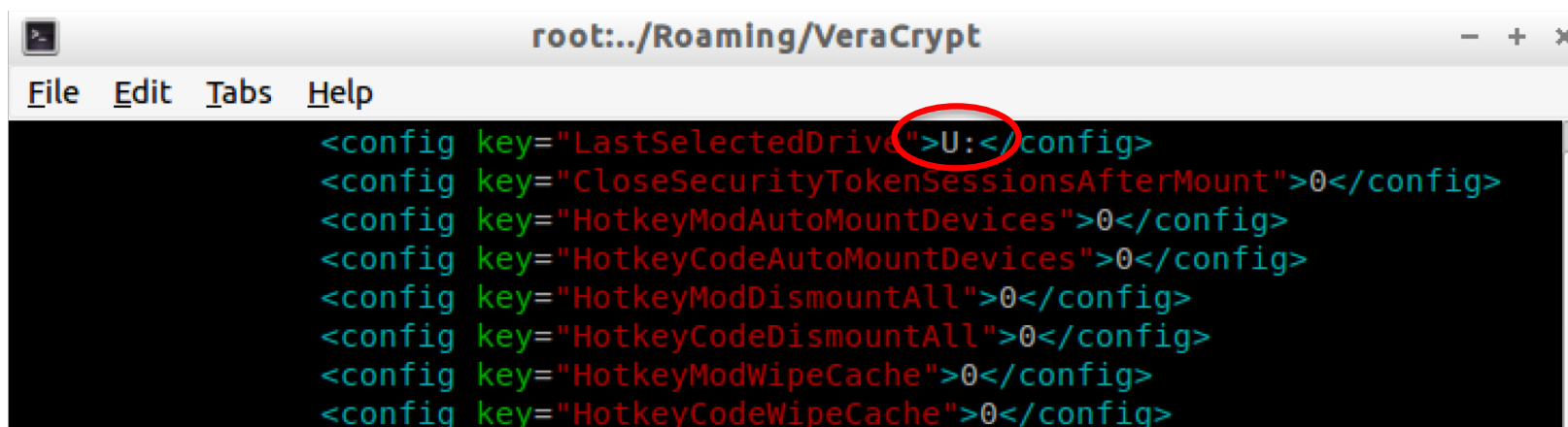
Go to: 0

- Artifacts of programs can be on different places in different formats
 - \$USER/AppData/*
 - Example AppData/Roaming/VeraCrypt/History.xml
 - Open with vi



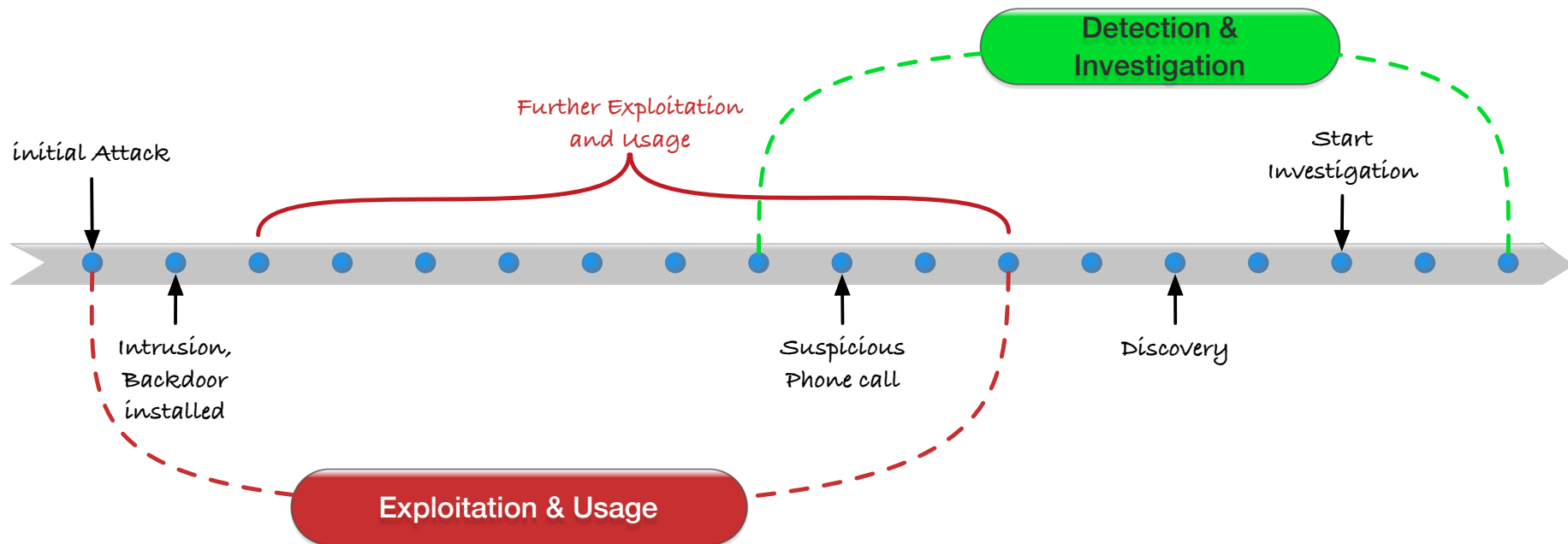
```
root:~/Roaming/VeraCrypt
File Edit Tabs Help
<?xml version="1.0" encoding="utf-8"?>
<VeraCrypt>
  <history>
    <volume>E:\Users\Thomas Ehrhart\Documents\myDokuments</volume>
    <volume>C:\Users\Thomas Ehrhart\Documents\myDokuments</volume>
  </history>
</VeraCrypt>
~
```

- Artifacts of programs can be on different places in different formats
 - \$USER/AppData/*
 - Example AppData/Roaming/VeraCrypt/Configuration.xml
 - Open with vi
 - Look for LastSelectedDrive



```
root:~/Roaming/VeraCrypt
File Edit Tabs Help
<config key="LastSelectedDrive">U:</config>
<config key="CloseSecurityTokenSessionsAfterMount">0</config>
<config key="HotkeyModAutoMountDevices">0</config>
<config key="HotkeyCodeAutoMountDevices">0</config>
<config key="HotkeyModDismountAll">0</config>
<config key="HotkeyCodeDismountAll">0</config>
<config key="HotkeyModWipeCache">0</config>
<config key="HotkeyCodeWipeCache">0</config>
```

- If you are investigating an event in the past, you want to know what happened when in order to create a timeline of events
- End result for the report



- timescanner
 - Perlscript uses log2timeline to scan recursive directory and write csv file
 - timescanner -d /mnt/windows_mount/ -w /home/evidence/20160901_df01/timeline.csv

```
root:/mnt/windows_mount
File Edit Tabs Help
deft8 /mnt/windows_mount % timescanner -d /mnt/windows_mount/ -w /home/evidence/20160901_df01/timeline.csv
-----
/usr/local/bin/timescanner [version 0.65] run with options [-d /mnt/windows_mount/ -w /home/evidence/20160901_df01/timeline.csv]
Date of run (localtime): 15:31:49, Mon Aug 29 2016
Timezone used: local
Local timezone is: UTC (UTC)
Using output module: csv
Using file '/home/evidence/20160901_df01/timeline.csv' for output
-----
Local timezone is: UTC (UTC)
```

- Open it with LibreOffice Spreadsheet



Registry

Analysis

- Registry is a system wide Database in Windows divided in Hive-Files
 - Windows/System32/config/SAM
 - Windows/System32/config/SECURITY
 - Windows/System32/config/SYSTEM
 - Windows/System32/config/SOFTWARE
 - <\$USER>/NTUSER.DAT



Hashlist

Analysis

- There are known files by from the Systems which you don't like to investigate.
- Elimination through Hashlist
- NSRL Downloads (<http://www.nsrl.nist.gov>)



Reporting

Presentation

- Report your findings in a document
- An other Digital Forensic Expert should follow your Document and
 - Come to the same findings
 - Can proof your findings
- Report Facts, not guesses