ROMHACK CAMP

Open Source Digital Forensics

First steps in digital investigations with open source and free software.

Alessandro Farina – Cyber Saiyan – forensics@dsa.it

What is digital forensics

NIST (National Institute of Standards and Technology - Special publication - 800-86[1])

Forensic science is generally defined as the application of science to the law. Digital forensics, also known as computer and network forensics, has many definitions.

Generally, it is considered the application of science to the **identification**, **collection**, **examination**, **analysis and reporting** of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

Data refers to distinct pieces of digital information that have been formatted in a specific way. People and organizations have an ever-increasing amount of data from many sources.

For example, data can be stored or transferred by standard computer systems, networking equipment, computing peripherals, personal digital assistants (PDA), consumer electronic devices, and various types of media, among other sources.

Guide to Integrating Forensic Techniques into Incident Response (August 2006)
https://csrc.nist.gov/publications/detail/sp/800-86/final

What is digital forensics

The *four steps* NIJ (U.S. Department of Justice – Office of Justice Programs – National Institute of Justice)

“The process for performing digital forensics comprises the following basic phases:

Collection: identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.

Examination: forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.

Analysis: analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

Reporting: reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.”

Computer/cyber Crime

Computer crime, or cybercrime, is any crime that involves a computer and a network.

The computer may have been used in the commission of a crime, or it may be the target.

Device as a target

Device as a tool

Device as a witness

What is digital forensics

When dealing with digital evidence, general forensic and procedural principles should be applied:

A. **The process of collecting, securing, and transporting digital evidence should not change the evidence;**

B. **Digital evidence should be examined only by those trained specifically for that purpose;**

C. **Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review.**

Locard's Exchange Principle

"Every contact leaves a trace"

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

When perpetrators enter or leave a crime scene, they will leave something behind or take something with them (Such as DNA, fingerprints, hair, fibers, etc.)

Also true of digital forensics (Registry keys, log files, deleted files, etc.)

Scientific Method

Digital Forensic science is new and procedures are still being developed

A scientist is normally regarded as objective, neutral, dealing only with facts.

Must be without bias

Follow the evidence wherever it leads

First responders – inspections

- If the system is on, do not shut down the system until all necessary inspections and acquisitions are completed;
- Evaluate the most appropriate shutdown mode;
- The owner may have altered normal shutdown processes;
- Some information may be lost in a sudden shutdown;
- If the system is off, do not turn it on;
- Do not trust the system: use your own tools, statically compiled and on read-only media;
- Do not use programs that can alter the file timeline;
- The correct user profiling is important to calibrate the investigative procedures.

Chain of Custody

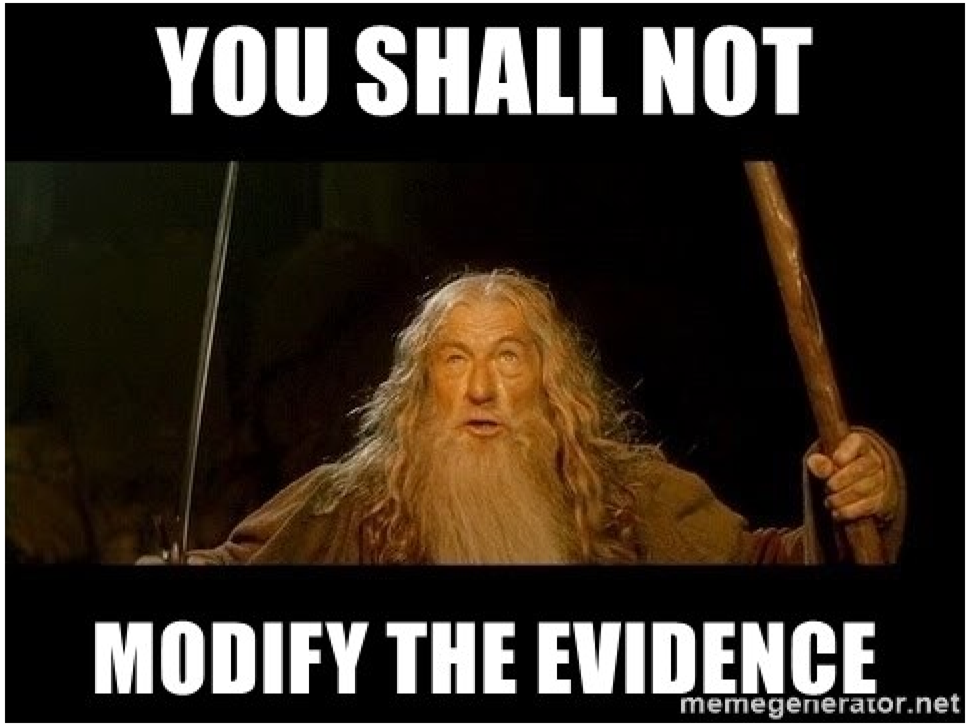
Procedure to track the status of an evidence and its responsibility at every point in its management

Must clearly state:

- Where, when and by whom the evidence was found and acquired;
- Where, when and by whom it was stored and/or analyzed;
- Who had custody of the specimen and during what period;
- How it has been preserved;
- At each handover, it must be indicated where and how it was transferred.

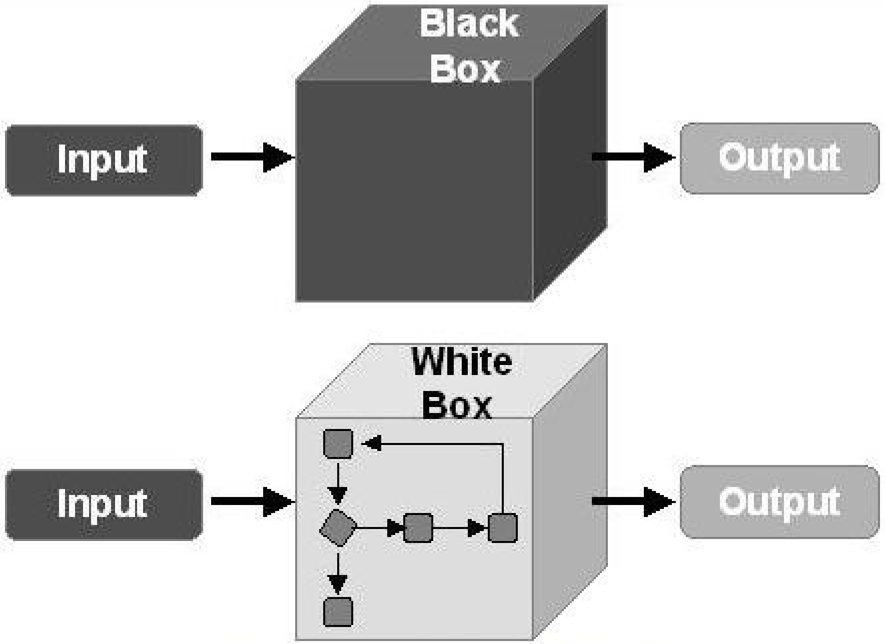
Access to evidences must be restricted and fully documented.

First rule of the forensics club



Fantastic closed and proprietary tools

Black box forensics



What appens on computer power on

1. Physical modification of storage and memory
2. Changes in hundreds to thousands of file implied in system boot-up
3. Changes in files involved in autorun tasks
4. Login script execution
5. Connections to online services (emails, clouds, sharing, etc)
6. Operations made by malware, virus, antivirus, etc

Lost in space

A.Unallocated space

B.Slack space

C.Free space

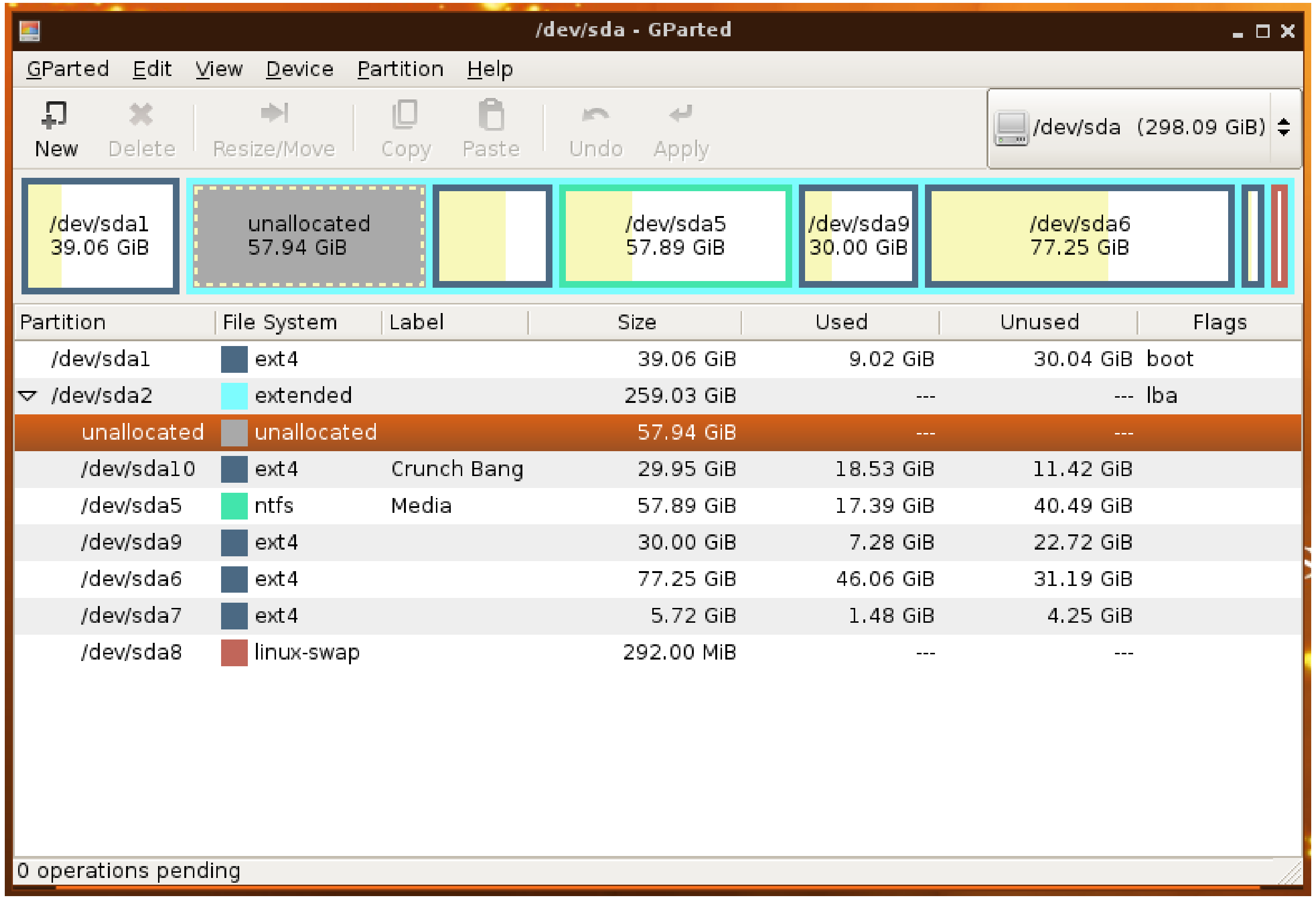
Lost in space

Unallocated space

Unallocated space refers to the area of the drive which no longer holds any file information as indicated by the file system structures like the file table FAT.

In the case of damaged or missing file system structures, this may involve the whole drive. In simple words, many file systems do not zero-out the data when they delete it. Instead, they simply remove the knowledge of where it is. Unless security grade file deletion software is used, data from the 'erased file' remains behind in an area called unallocated storage space.

Lost in space



/dev/sda (298.09 GiB)

Partition	File System	Label	Size	Used	Unused	Flags
/dev/sda1	ext4		39.06 GiB	9.02 GiB	30.04 GiB	boot
/dev/sda2	extended		259.03 GiB	---	---	lba
unallocated	unallocated		57.94 GiB	---	---	
/dev/sda10	ext4	Crunch Bang	29.95 GiB	18.53 GiB	11.42 GiB	
/dev/sda5	ntfs	Media	57.89 GiB	17.39 GiB	40.49 GiB	
/dev/sda9	ext4		30.00 GiB	7.28 GiB	22.72 GiB	
/dev/sda6	ext4		77.25 GiB	46.06 GiB	31.19 GiB	
/dev/sda7	ext4		5.72 GiB	1.48 GiB	4.25 GiB	
/dev/sda8	linux-swap		292.00 MiB	---	---	

0 operations pending

Lost in space

Disk formatting is the process of preparing a data storage device such as a hard disk drive, solid-state drive, floppy disk or USB flash drive for initial use.

In some cases, the formatting operation may also create one or more new file systems.

The first part of the formatting process that performs basic medium preparation is often referred to as "low-level formatting".

Partitioning is the common term for the second part of the process, making the data storage device visible to an operating system.

The third part of the process, usually termed "high-level formatting" most often refers to the process of generating a new file system.

In some operating systems all or parts of these three processes can be combined or repeated at different levels and the term "format" is understood to mean an operation in which a new disk medium is fully prepared to store files.

Example: zeroing hard disk for acquisition

The importance of being…on time

Much of the observations made on the evidence collected is based on the date and time that you can associate with the recovered files. The information is contained in the file system as in the metadata associated with each document (eg. Exif information of images). To be reasonably sure of the data that are collected, a crucial first step is to verify the date and time of the BIOS of the devices analyzed, to do that you have to start the device after it has been disconnected from all storage devices available and enter the configuration BIOS to pick the date and time of the system.

Of course, this technique does not mean that we can assure anything for certain, because the suspect could have modified the date and time of the system at a particular moment of its activity, bringing it back to the correct date and time after its actions. In these cases one must proceed with a context analysis, eg. references to events in the content of the texts, dates present in headers and metadata documents such as word, jpeg, etc.

One thing to consider, when analyzing storage is that almost all file systems keep the information on the date of access to a particular object, this date may be crucial to frame a criminal activity in a specific window time … and can be destroyed without hope by an investigator who will be accessing the files of the suspect without observing best practices and procedures.

The importance of being…on time

Timeline

A digital timeline can be defined as the representation of filesystem time-based metadata described in a human-readable manner which contains useful information relating to a specific security event.

It could also be defined as the chronological ordering of filesystem related events as preserved by the filesystem's record-keeping constructs and metadata structures, which are extracted and presented to the investigator in a human-readable manner. (Generating Computer Forensic Supertimelines under Linux, R. Carbone - C. Bean, Defence R&D Canada – Valcartier)

Hashing and digital signature

A hash function is any algorithm that maps data of arbitrary length to data of a fixed length. The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.

https://en.wikipedia.org/wiki/Cryptographic_hash_function

Hardware and software write-blocker

A write blocker is any tool that permits read-only access to data storage devices without compromising the integrity of the data. A write blocker, when used properly, can guarantee the protection of the data chain of custody.

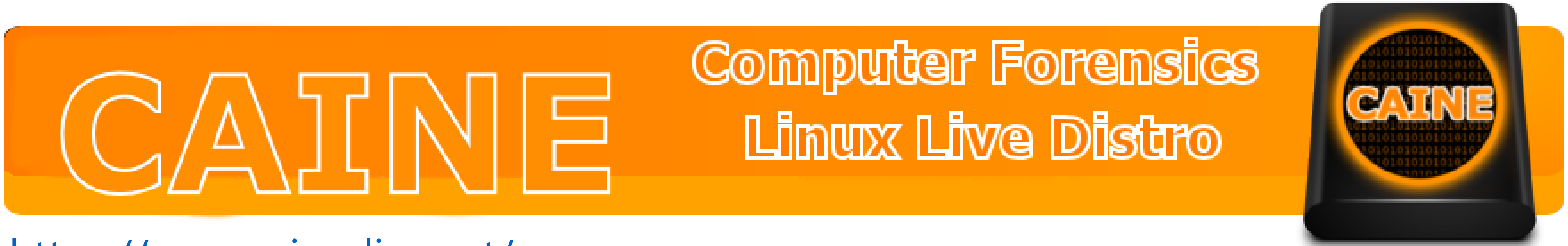
NIST’s general write blocking requirements hold that:

1. The tool shall not allow a protected drive to be changed.
2. The tool shall not prevent obtaining any information from or about any drive.
3. The tool shall not prevent any operations to a drive that is not protected.

https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-technical/hardware

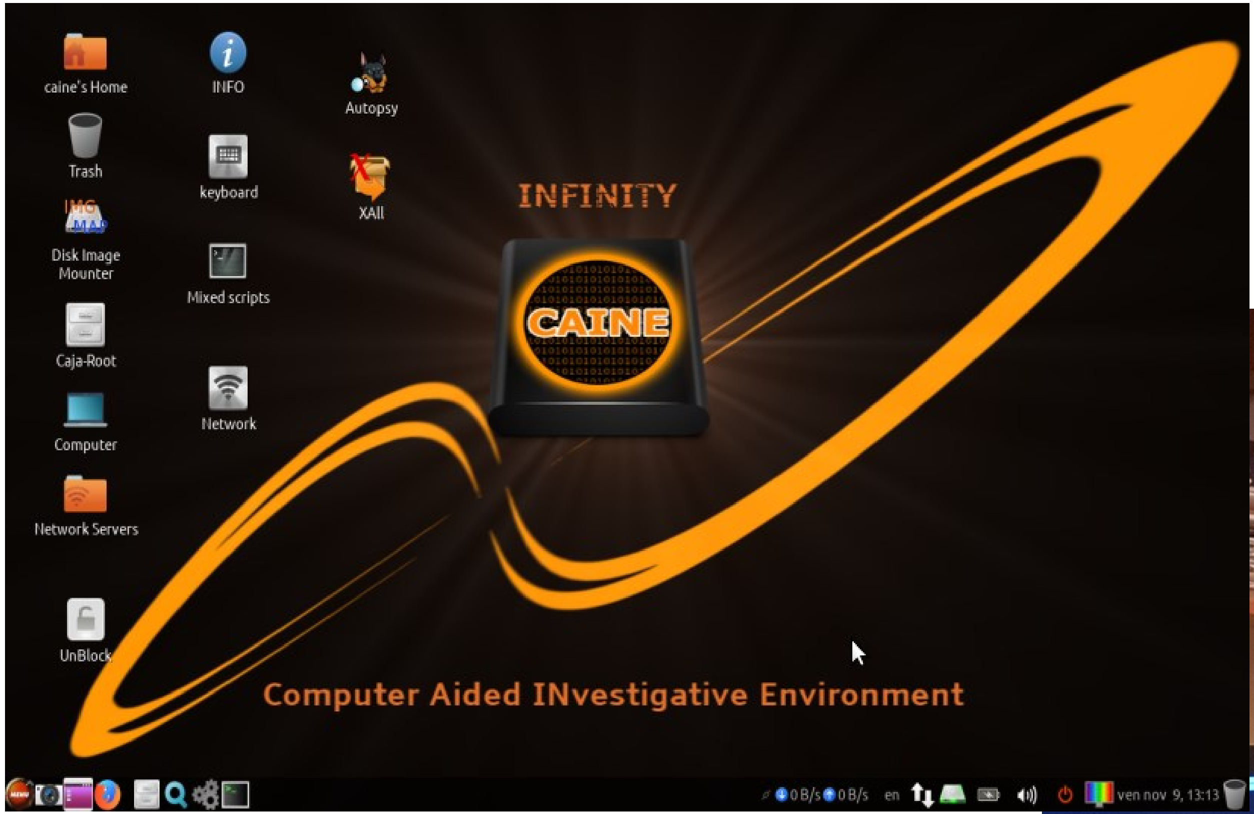
Software and hardware write blockers do the same job. They prevent writes to storage devices. The main difference between the two types is that software write blockers are installed on a forensic computer workstation, whereas hardware write blockers have write blocking software installed on a controller chip inside a portable physical device.

Linux live forensics Distro



https://www.caine-live.net/

https://tsurugi-linux.org/

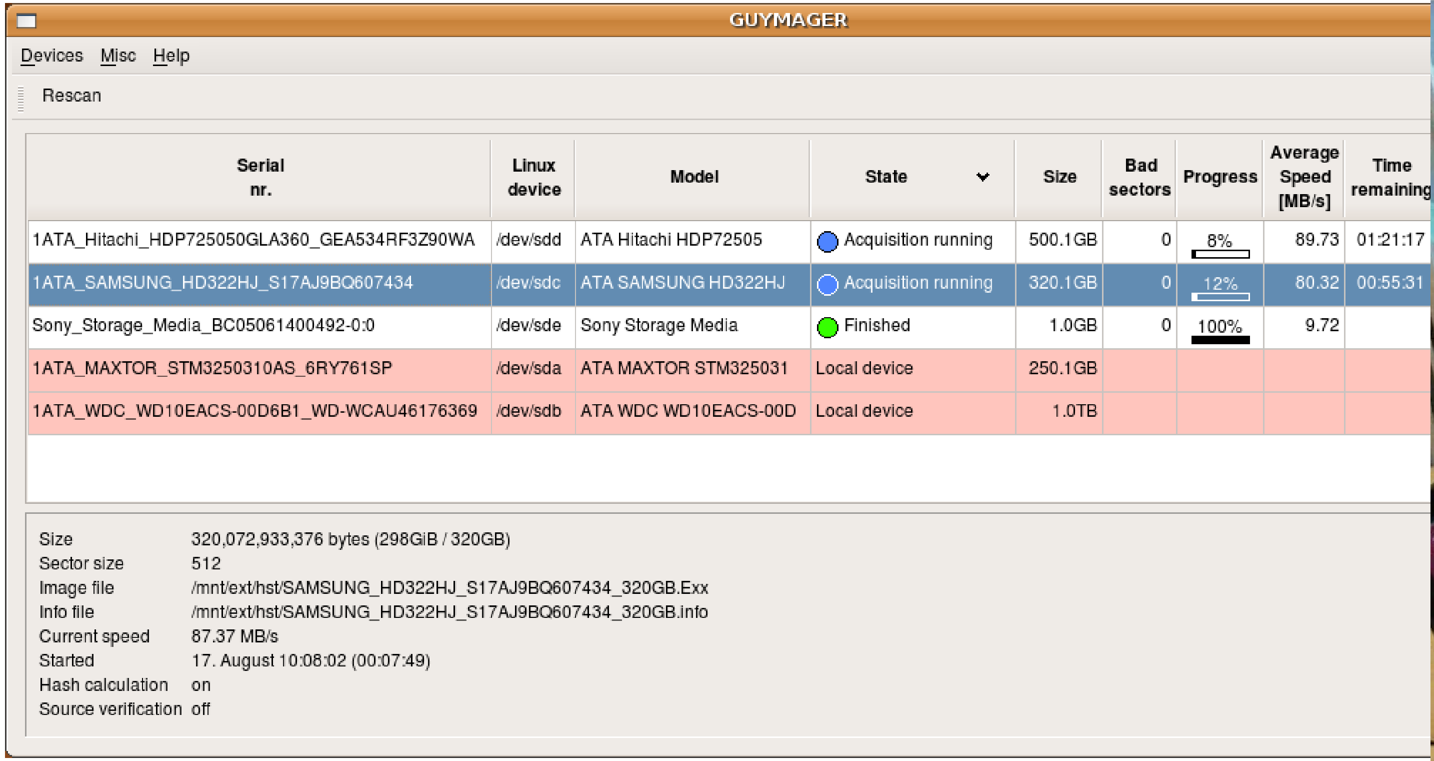

caine's Home
INFO
Autopsy
Trash
keyboard
XAll
Disk Image Mounter
Mixed scripts
Caja-Root
Network
Computer
Network Servers
UnBlock
INFINITY
CAINE
Computer Aided INvestigative Environment
0 B/s 0 B/s
en
ven nov 9, 13:13

THE RED
STREET FIGHTER
CHAMPION EDITION

Tools we’ll use in the lab

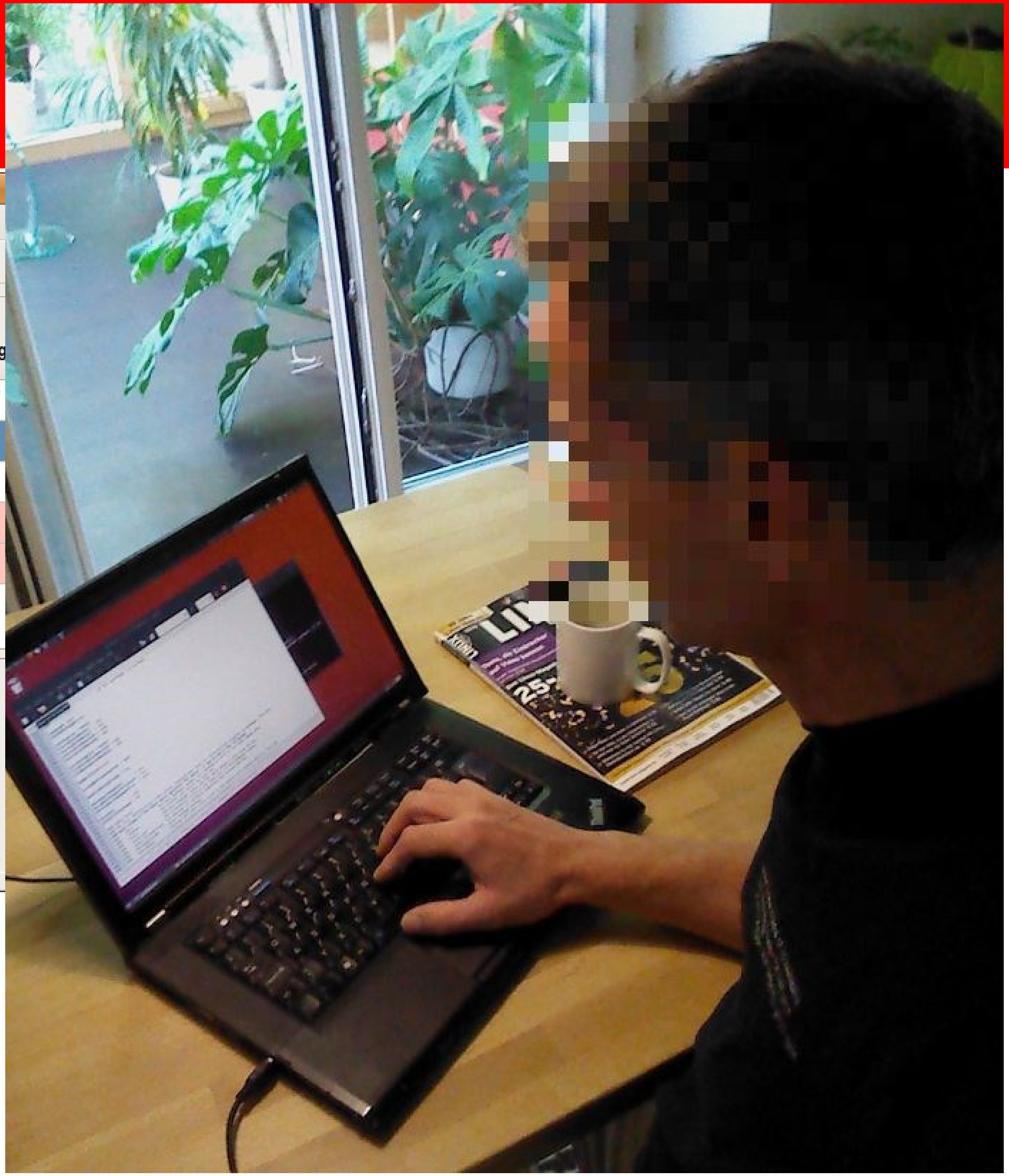
Name	Description
Guymager	Forensical acquisition of storage devices
ewfinfo	View ewf image file info
ewfverify	Verify hash of the image
imount	Mount image to browse files and folders
tsk_recover	Extract unallocated files
photorec	File carving

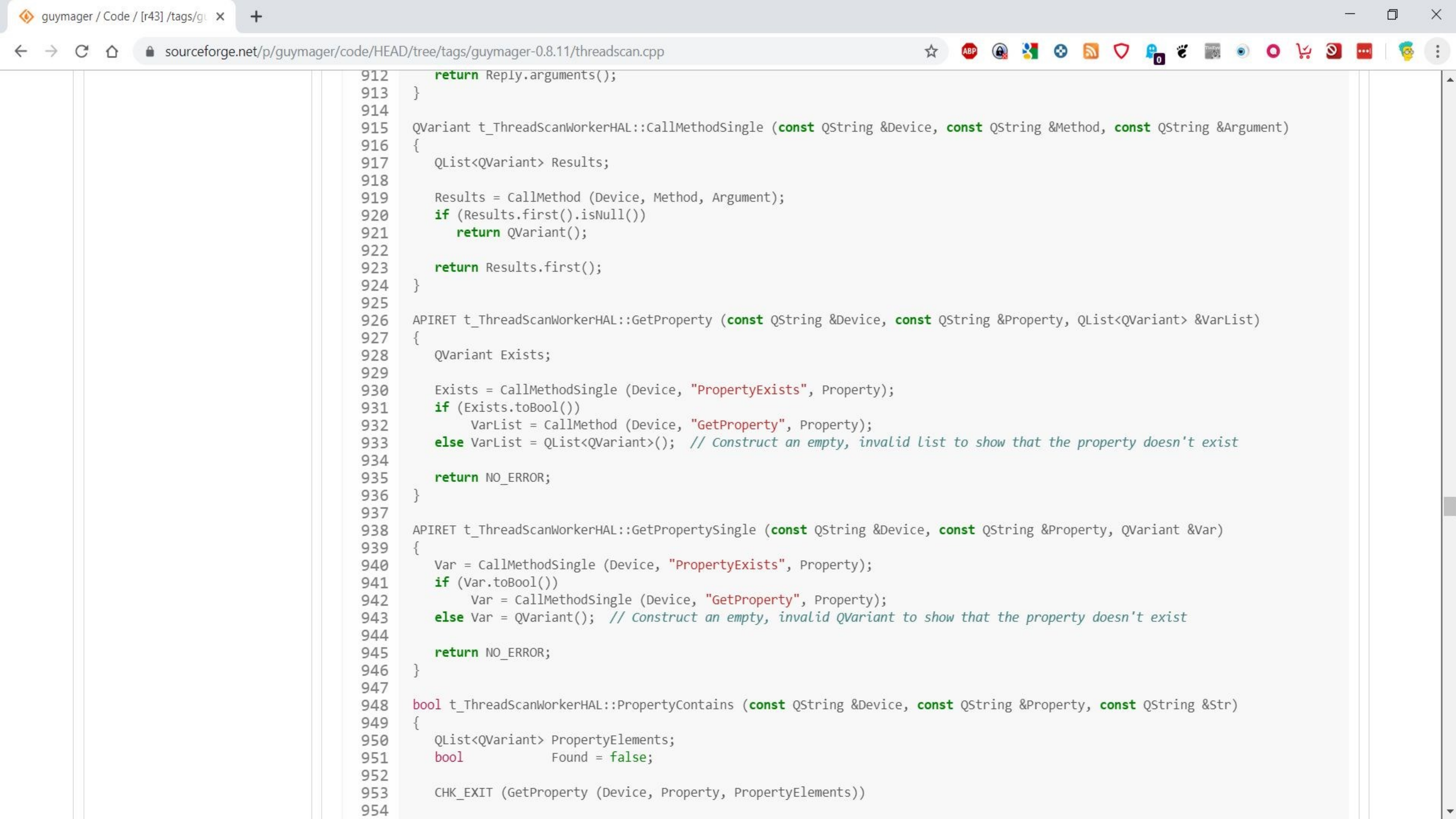
Guymager



Serial nr.	Linux device	Model	State	Size	Bad sectors	Progress	Average Speed [MB/s]	Time remaining
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA	/dev/sdd	ATA Hitachi HDP72505	● Acquisition running	500.1GB	0	8%	89.73	01:21:17
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434	/dev/sdc	ATA SAMSUNG HD322HJ	● Acquisition running	320.1GB	0	12%	80.32	00:55:31
Sony_Storage_Media_BC05061400492-0:0	/dev/sde	Sony Storage Media	● Finished	1.0GB	0	100%	9.72	
1ATA_MAXTOR_STM3250310AS_6RY761SP	/dev/sda	ATA MAXTOR STM325031	Local device	250.1GB				
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369	/dev/sdb	ATA WDC WD10EACS-00D	Local device	1.0TB				

Size	320,072,933,376 bytes (298GiB / 320GB)
Sector size	512
Image file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed	87.37 MB/s
Started	17. August 10:08:02 (00:07:49)
Hash calculation	on
Source verification	off

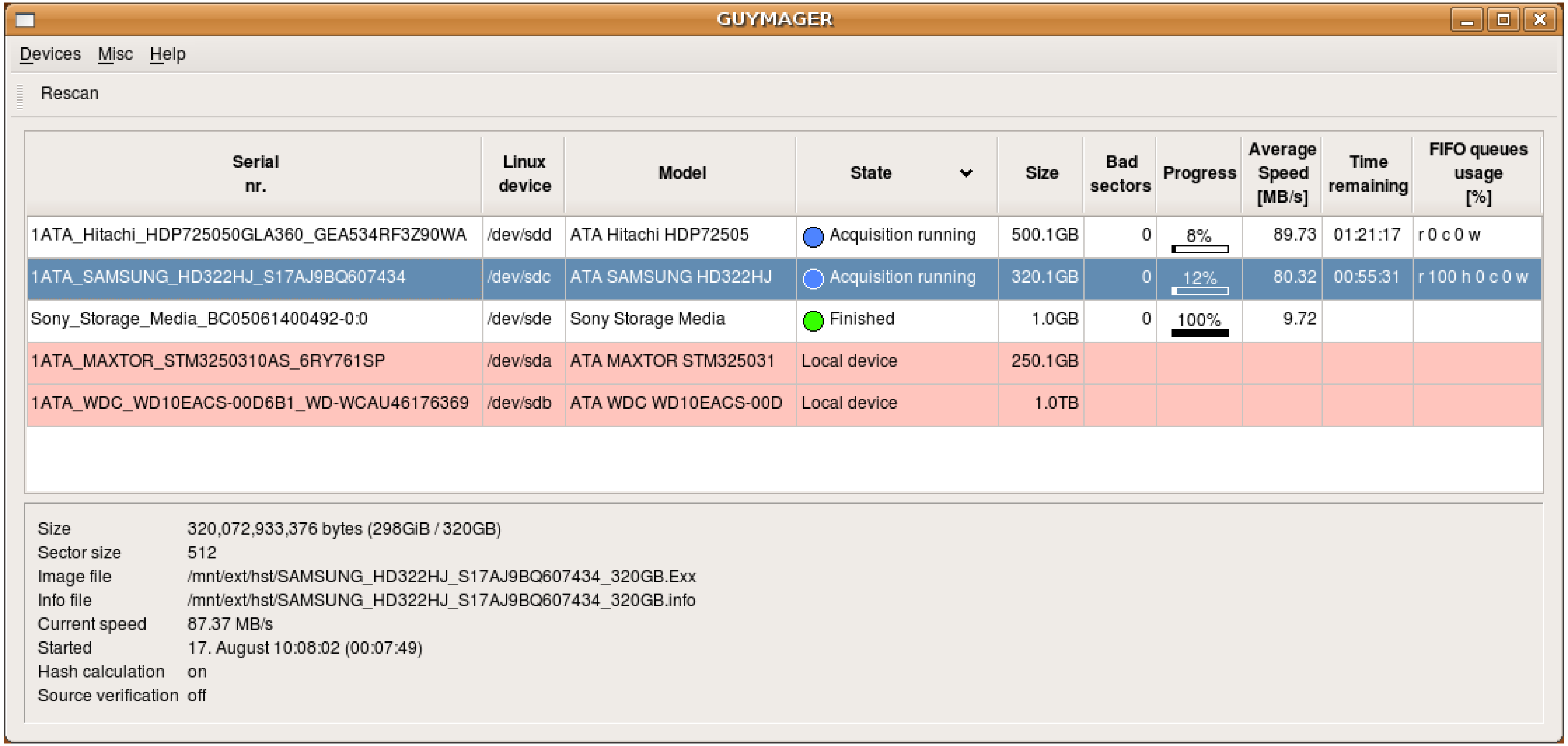



guymager / Code / [r43] /tags/g
sourceforge.net/p/guymager/code/HEAD/tree/tags/guymager-0.8.11/threadscan.cpp

```
   return Reply.arguments();
}

QVariant t_ThreadScanWorkerHAL::CallMethodSingle (const QString &Device, const QString &Method, const QString &Argument)
{
   QList<QVariant> Results;

   Results = CallMethod (Device, Method, Argument);
   if (Results.first().isNull())
      return QVariant();

   return Results.first();
}

APIRET t_ThreadScanWorkerHAL::GetProperty (const QString &Device, const QString &Property, QList<QVariant> &VarList)
{
   QVariant Exists;

   Exists = CallMethodSingle (Device, "PropertyExists", Property);
   if (Exists.toBool())
        VarList = CallMethod (Device, "GetProperty", Property);
   else VarList = QList<QVariant>();  // Construct an empty, invalid list to show that the property doesn't exist

   return NO_ERROR;
}

APIRET t_ThreadScanWorkerHAL::GetPropertySingle (const QString &Device, const QString &Property, QVariant &Var)
{
   Var = CallMethodSingle (Device, "PropertyExists", Property);
   if (Var.toBool())
        Var = CallMethodSingle (Device, "GetProperty", Property);
   else Var = QVariant();  // Construct an empty, invalid QVariant to show that the property doesn't exist

   return NO_ERROR;
}

bool t_ThreadScanWorkerHAL::PropertyContains (const QString &Device, const QString &Property, const QString &Str)
{
   QList<QVariant> PropertyElements;
   bool            Found = false;

   CHK_EXIT (GetProperty (Device, Property, PropertyElements))

```

Bitstream imaging with open source tools

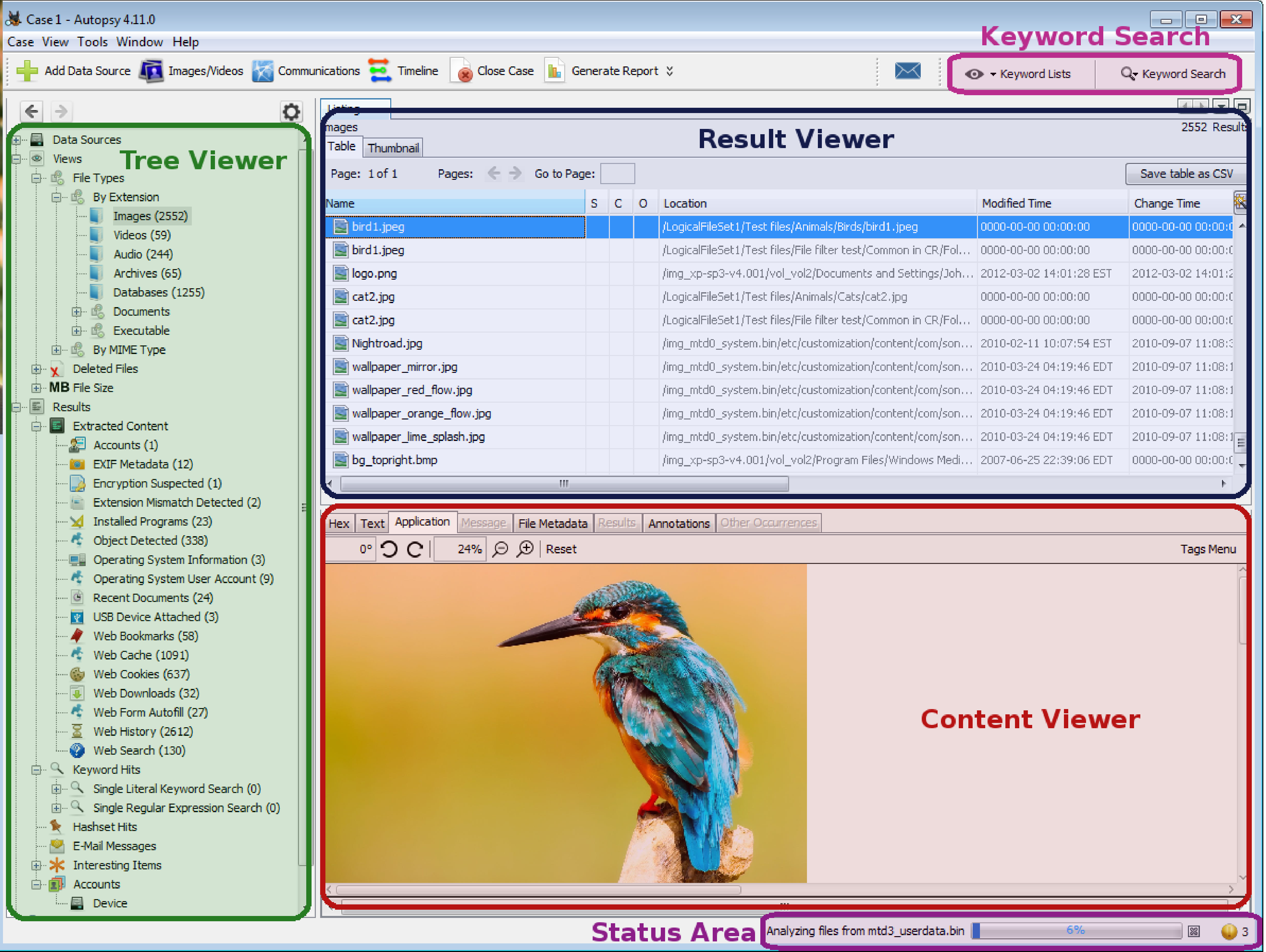
HANDS ON: GUYMAGER



Serial nr.	Linux device	Model	State	Size	Bad sectors	Progress	Average Speed [MB/s]	Time remaining	FIFO queues usage [%]
1ATA_Hitachi_HDP725050GLA360_GEA534RF3Z90WA	/dev/sdd	ATA Hitachi HDP72505	● Acquisition running	500.1GB	0	8%	89.73	01:21:17	r 0 c 0 w
1ATA_SAMSUNG_HD322HJ_S17AJ9BQ607434	/dev/sdc	ATA SAMSUNG HD322HJ	● Acquisition running	320.1GB	0	12%	80.32	00:55:31	r 100 h 0 c 0 w
Sony_Storage_Media_BC05061400492-0:0	/dev/sde	Sony Storage Media	● Finished	1.0GB	0	100%	9.72		
1ATA_MAXTOR_STM3250310AS_6RY761SP	/dev/sda	ATA MAXTOR STM325031	Local device	250.1GB					
1ATA_WDC_WD10EACS-00D6B1_WD-WCAU46176369	/dev/sdb	ATA WDC WD10EACS-00D	Local device	1.0TB					

Size	320,072,933,376 bytes (298GiB / 320GB)
Sector size	512
Image file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.Exx
Info file	/mnt/ext/hst/SAMSUNG_HD322HJ_S17AJ9BQ607434_320GB.info
Current speed	87.37 MB/s
Started	17. August 10:08:02 (00:07:49)
Hash calculation	on
Source verification	off

Starting modules...



- Data Sources
- Views
  - File Types
    - By Extension
      - Images (2552)
      - Videos (59)
      - Audio (244)
      - Archives (65)
      - Databases (1255)
      - Documents
      - Executable
    - By MIME Type
  - Deleted Files
  - MB File Size
- Results
  - Extracted Content
    - Accounts (1)
    - EXIF Metadata (12)
    - Encryption Suspected (1)
    - Extension Mismatch Detected (2)
    - Installed Programs (23)
    - Object Detected (338)
    - Operating System Information (3)
    - Operating System User Account (9)
    - Recent Documents (24)
    - USB Device Attached (3)
    - Web Bookmarks (58)
    - Web Cache (1091)
    - Web Cookies (637)
    - Web Downloads (32)
    - Web Form Autofill (27)
    - Web History (2612)
    - Web Search (130)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Accounts
    - Device

mages

2552 Result

Page: 1 of 1 Pages: Go to Page:

Name	S	C	O	Location	Modified Time	Change Time
bird1.jpeg				/LogicalFileSet1/Test files/Animals/Birds/bird1.jpeg	0000-00-00 00:00:00	0000-00-00 00:00:0
bird1.jpeg				/LogicalFileSet1/Test files/File filter test/Common in CR/Fol...	0000-00-00 00:00:00	0000-00-00 00:00:0
logo.png				/img_xp-sp3-v4.001/vol_vol2/Documents and Settings/Joh...	2012-03-02 14:01:28 EST	2012-03-02 14:01:2
cat2.jpg				/LogicalFileSet1/Test files/Animals/Cats/cat2.jpg	0000-00-00 00:00:00	0000-00-00 00:00:0
cat2.jpg				/LogicalFileSet1/Test files/File filter test/Common in CR/Fol...	0000-00-00 00:00:00	0000-00-00 00:00:0
Nightroad.jpg				/img_mtd0_system.bin/etc/customization/content/com/son...	2010-02-11 10:07:54 EST	2010-09-07 11:08:3
wallpaper_mirror.jpg				/img_mtd0_system.bin/etc/customization/content/com/son...	2010-03-24 04:19:46 EDT	2010-09-07 11:08:1
wallpaper_red_flow.jpg				/img_mtd0_system.bin/etc/customization/content/com/son...	2010-03-24 04:19:46 EDT	2010-09-07 11:08:1
wallpaper_orange_flow.jpg				/img_mtd0_system.bin/etc/customization/content/com/son...	2010-03-24 04:19:46 EDT	2010-09-07 11:08:1
wallpaper_lime_splash.jpg				/img_mtd0_system.bin/etc/customization/content/com/son...	2010-03-24 04:19:46 EDT	2010-09-07 11:08:1
bg_topright.bmp				/img_xp-sp3-v4.001/vol_vol2/Program Files/Windows Medi...	2007-06-25 22:39:06 EDT	0000-00-00 00:00:0

Analyzing files from mtd3_userdata.bin 6%

Data analysis

HANDS ON

AUTOPSY

FTK Imager

HANDS ON

APK Downgrade WhatsApp

In order to collect app evidence data, mobile forensic experts tried to use **adb backup** to acquire app data. At first, it worked, but today it doesn't anymore because recently many apps have disabled **adb backup** permission in consideration of user's private data security.

The solution is: downgrade and backup.

The idea of downgrade backup is simple, we downgrade the target app to an old version where **adb backup** is allowed, and we use this old version to create a backup and then use a forensic tool to analyze it.

Thanks

http://www.linuxleo.com/
(introduzione alla CF)

AUTOPSY
DIGITAL FORENSICS
https://www.autopsy.com/

Cyber Saiyan

Per approfondimenti

Alessandro Farina

forensics@dsa.it