DEFT 7 MANUAL

DIGITAL EVIDENCE & FORENSIC TOOLKIT

Stefano Fratepietro & Alessandro Rossetti & Paolo Dal Checco

English version by
Giada Dell'Erba, Nicodemo Gawronski (translators)
Neil Torpey (technical review and proofreading)

THE AUTHORS

STEFANO "YOUNGSTER" FRATEPIETRO

Stefano graduated in 2006 with a degree in Information Technology and Management (Science of the Internet) at the University of Bologna. His thesis in Computer Forensics was entitled "A Vierika viruses case study." He is OSCP Offensive Security Certified and ISECOM OPST. Stefano is currently a security specialist at the office of the CSE IT-security (Banking Association) where he performs expert tasks for courts, law enforcement forces and private clients, and has participated as a technical consultant in cases of national fame such as "Good morning! Vitaminic" and "Pirelli-Telecom-Ghioni". Since 2005 he is the creator and project leader of the DEFT system. Occasionally performs teaching activities in Computer Forensics for various Italian Universities and private courses.

SANDRO "BUSBOY" ROSSETTI

Alessandro Rossetti lives and works in Rome. He takes great interest in topics such as Information Technology, Computer Security and Digital Forensics. He is a IACIS member and also Member of the "CyberWorld" Working Group at OSN (National Security Observatory) of Italian Ministry of DEfence.

PAOLO "JESTER" DAL CHECCO

Paolo received his PhD in 2006 from the University of Turin in the Security Group of the Department of Computer Sciences. He has taught classes at different universities, companies and ICT environments in addition to other cooperatives with companies operating in the field of security and communication privacy. He is also a founding partner of the computer forensics firm " Digital Forensics Bureau" (www.difob.it) of Turin.He is an Associate Director of the Digit Law Ltd (www.digitlaw.it).Paolo has also performed as a technical advisor in court cases assisting prosecutors, law enforcement agencies and private sector entities.

END USER LICENSE AGREEMENT

Dedicated to Ele and Silvia for their infinite patience.

Dedicated also to Stefano and Alessandro,

hoping that they take more after their mothers than after their fathers.

To Samanta and Kim.

ACKNOWLEDGEMENTS

We would like to thank all those who in recent years have contributed to our personal growth.

We also thank those who worked behind the scenes for the production of DEFT contributing also indirectly to the creation of the user manual.

Massimiliano Dal Cero
Davide "Rebus" Gabrini
Bartolomeo "Meo" Bogliolo
Valerio Leomporra
Marco Giorgi
Emanuele Gentili

A HUGE “thank you!” also goes to Simone and Ivan for their help in the double-checking of this manual.

We want to thank Architecture Technology Corporation for allowing us to insert "Dropbox Reader ™" in this distribution.

Last but not least: the English version has been done by Giada Dell’Erba, Nicodemo Gawronski (translator) and Neil Torpey (technical review and proofreading)

PREFACE

The purpose of this manual is to offer the reader a taste of the main features and potential of the DEFT distribution; a starting point to stimulate the growth of their technical knowledge using the DEFT.

On these pages you will not find exhaustive explanations on the use of all applications and commands currently in the DEFT distribution.

To try to facilitate the study, we have included some examples that suggest how to perform some of the major activities of Digital Forensics.

- the acquisition and preservation of mass storage devices (hard drives, USB sticks, MP3 players, smartphones, etc..) or telematic traffic over IP networks;
- case analysis and their management.

Happy reading!

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 WHAT IS DEFT?

The Linux distribution[1] **DEFT[2]** is made up of a GNU / Linux and DART (Digital Advanced Response Toolkit), suite dedicated to digital forensics[3] and intelligence[4] activities.

It is currently developed and maintained by Stefano Fratepietro, with the support of Massimo Dal Cero, Sandro Rossetti, Paolo Dal Checco, Davide Gabrini, Bartolomeo Bogliolo, Valerio Leomporra and Marco Giorgi.

The first version of Linux DEFT was introduced in 2005 thanks to the Computer Forensic Course of the Faculty of Law at the University of Bologna.

This distribution is currently used during the laboratory hours of the Computer Forensics course held at the University of Bologna and in many other Italian universities and private entities.

It is also one of the main solutions employed by law enforcement agencies during computer forensic investigations.

In addition to a considerable number of linux applications and scripts, Deft also features the DART suite containing Windows applications (both open source[5] and closed source) which are still viable as there is no equivalent in the Unix world.

DEFT is distributed free of charge with no guarantees.

[1] GNU / Linux is a free Unix-type operating system (or Unix-like), incorporating elements of the Linux kernel with the GNU system and other software devel GNU / Linux is a free Unix-type operating system (or Unix-like), incorporating elements of the Linux kernel with the GNU system and other software developed and distributed under the GNU GPL or other free licenses.Wikipediaoped and distributed under the GNU GPL or other free licenses.*Wikipedia*

[2] Acronym for Digital Evidence & Forensic Toolkit.

[3] Science that studies the identification, preservation, protection, retrieval, documentation, and any other form of computer data processing in order to be evaluated and studied in a legal process, for evidentiary purposes, the techniques and methodological tools for the examination of computer systems. (Wikipedia)

[4] This aspect of the distribution will be addressed in another document.

[5] The term refers to software whose authors allow free study and/or to make changes by other independent programmers.

1.2 WHY CAN DEFT BE USED IN DIGITAL FORENSICS?

Computer Forensics software must be able to ensure the integrity of file structures and metadata[6] on the system being investigated in order to provide an accurate analysis. It also needs to reliably analyze the system being investigated without altering, deleting, overwriting or otherwise changing data.

There are certain characteristics inherent to DEFT that minimize the risk of altering the data being subjected to analysis. [7]

Some of these features are:

1. On boot, the system does not use the swap partitions on the system being analyzed.
2. During system startup there are no automatic mount scripts.
3. There are no automated systems for any activity during the analysis of evidence;
4. All the mass storage and network traffic acquisition tools do not alter the data being acquired.

[6] RFC 3227: "Minimize changes to the data as you are collecting it. This is not limited to content changes; You Should avoid updating file or directory access times. "

[7] Art 247, paragraph 1 bis with changes made by the ratification of the Budapest Convention on the Law March 18, 2008, n. 48: "[...] adopting technical measures aimed at ensuring the preservation of the original data and to prevent tampering"

CHAPTER 2: SYSTEM REQUIREMENTS

2.1 DEFT

You can fully utilize the wide-ranging capabilities of the DEFT toolkit booting from a CDROM or from a DEFT USB stick any system with the following characteristics:

- CD / DVD-ROM or USB port from which the BIOS can support booting.
- CPU x86 (Intel, AMD or Citrix) 166 Mhz or higher to run DEFT Linux in text mode, 200Mhz to run DEFT Linux in graphical mode;
- 64 Mbytes of RAM to run DEFT Linux in text mode or 128 Mbytes to run the DEFT GUI.

DEFT also supports the new Apple Intel-based architectures.

2.2 DART

The DART suite runs on all Microsoft Windows 32-bit systems. Some minor limitations were found for tools that do not guarantee full support to 64bit systems.

DART can run directly in DEFT Linux using Wine[8] .

[8] Wine is a framework for Linux that allows you to run Windows applications that can be installed or launched directly into a Linux distribution (www.winehq.org)

CHAPTER 3: APPLICATION LIST

3.1 DEFT LINUX

Sleuthkit 3.2.3

autopsy 2.24

dff 1.2

ptk forensic 1.0.5

Maltego CE

KeepNote 0.7.6

hunchbackeed file carver 0.6

Findwild 1.3

Bulk Extractor 1.2

Emule Forensic 1.0

dhash 2.0.1

libewf 20120304

aff lib 3.6.14

Disk Utility 2.30.1

guymager 0.6.5-1

dd rescue 1.14

dcfldd 1.3.4.1

dc3dd 7

foremost 1.5.6

photorec 6.13

mount manager 0.2.6

scalpel 2

Wipe 0.21

hex dump

outguess 0.2

sqlite database browser 2.0b1

bitpim 1.0.7

bbwhatsapp database converter

Dropbox reader

iphone backup analyzer 10/2012

iphone analyzer

creepy 0.1.9

xprobe2 0.3

xmount 0.4.6trID 2.11 DEFT edition

readpst 0.6.41

chkrootkit

rkhunter 1.3.8

john 1.7.8

catfish

pasco 1.0

md5sum

sha1sum

sha224sum

sha256sum

sha512sum

md5deep

sha1deep

sha256deep

pdfcrack cracking tool

fcrackzip cracking tool

Clam Antivirus 0.97.3

mc 4.7.0.9

dmraid

testdisk 6.11

ghex, light gtk hex editor

vinetto 0.6

Xplico 1.0 DEFT edition

Wireshark 1.6

ettercap 0.7.3

nmap 5.21

Hydra 7.1

log2timeline 0.60

rifiuti2

Wine 1.3.28

mobius forensic

3.2 DART 1.0

WinAudit 2.28.2

MiTeC

Windows Registry Recovery 1.5.1.0

Zeroview 1.0

FTK Imager 3

Nigilant32 0.1

Windows Forensic Toolchest 3.0.05

MoonSols Win32dd 1.0.2.20100417

MoonSols Win64dd 1.0.2.20100417

Windows File Analyzer 1.0

UltraSearch 1.40

Pre-Search xx.08

XnView 1.97.8

X-AgentRansackk 2010 (build 762)

Index.dat Analyzer 2.5

AccessEnum 1.2

Autoruns 10.03

DiskView 2.4

Filemon

Process eXPlorer 12.04

RAM Map 1.1

Regmon

Rootkit Revealer 1.71

VMMap 2.62

WinObj 2.15

AlternateStreamView 1.15

ChromeCacheView 1.25

CurrPorts 1.83 (x86/x64)

CurrProcess 1.13

FoldersReport 1.21

IE Cache View 1.32

IE Cookies View 1.74

IE History View 1.50

Inside Clipboard 1.11

Live Contacts View 1.07

Mozilla Cache View 1.30

Mozilla History View 1.25

Mozilla Cookie View 1.30

Opened Files View 1.46

Opera Cache View 1.37

Outlook Attack View 1.35 (x86/x64)

Process Activity View 1.11 (x86/x64)

Recent Files View 1.20

RegScanner 1.82 (x86/x64 and win98)

ServiWin 1.40

MUI Cache View 1.01

MyEventView 1.37

SkypeLogView 1.15 SmartSniff 1.71 (x86/x64)

StartupRun 1.22

MyLastSearch 1.44

Mozilla Cookies View 1.30

Opened Files View 1.46

Opera Cache View 1.37

Outlook Attack View 1.35 (x86/x64)

Process Activity View 1.11 (x86/x64)

Recent Files View 1.20

RegScanner 1.82 (x86/x64 and win98)

ServiWin 1.40

USBdeview 1.80 (x86/x64)

User Assist View 1.01

User Profile View 1.01

Video Cache View 1.78

WhatInStartup 1.25

WinPerfectView 1.10

Password Tool

ChromePass 1.10

Dialupass 3.10

IE PassView 1.20

LSA Secrets Dump 1.21 (x86/x64)

LSA Secrets View 1.21 (x86/x64)

Mail PassView 1.65

MessenPass 1.35

Network PassRecovery 1.30 (x86/x64)

Opera PassView 1.1

PasswordFOX 1.25

PC AnyPass 1.12

Protected Pass View 1.63

PST Password 1.12

Remote Desktop PassView 1.01

VNC PassView 1.02

Win9x PassView 1.1

WirelessKeyView 1.34 (x86/x64)

AviScreen Portable 3.2.2.0

Hoverdesk 0.8

File Restore Plus 3.0.1.811

WinVNC 3.3.3.2

TreeSizeFree 2.40

PCTime

LTFViewer 5.2

Sophos Anti-Rootkit 1.5.4

Terminal with tools command line

Spartakus 1.0

Testdisk 6.11.3

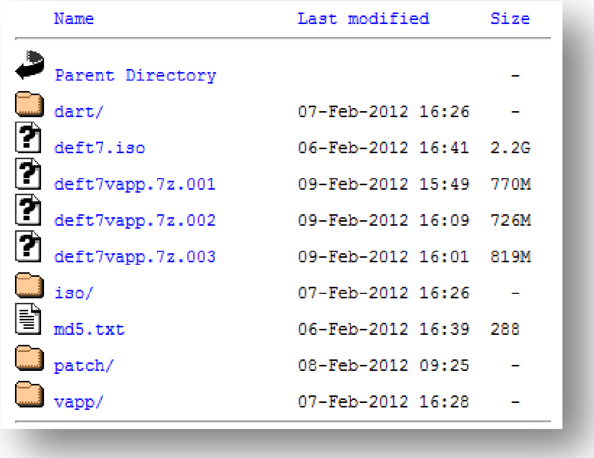
Photorec 6.11.3

CHAPTER 4: START DEFT LINUX LIVE DVD

4.1 DEFT IMAGE FILE : INTEGRITY CHECK OF THE DOWNLOADED FILE.

It is wise to verify the integrity of your downloaded version before performing digital forensics analysis. This ensures that you have an exact match of the copy being hosted online which has not been altered or changed during the download process.

This can be done by calculating the MD5 hash value[9] on the image file or on the archive you downloaded and then subsequently comparing it with the values in *md5.txt* in the *root* of the download directory.



```
Name                         Last modified       Size

Parent Directory                                  -
dart/                        07-Feb-2012 16:26    -
deft7.iso                    06-Feb-2012 16:41   2.2G
deft7vapp.7z.001             09-Feb-2012 15:49   770M
deft7vapp.7z.002             09-Feb-2012 16:09   726M
deft7vapp.7z.003             09-Feb-2012 16:01   819M
iso/                         07-Feb-2012 16:26    -
md5.txt                      06-Feb-2012 16:39   288
patch/                       08-Feb-2012 09:25    -
vapp/                        07-Feb-2012 16:28    -
```

DEFT / DART: Download Directory

For "deft7.iso" image file for instance, the calculation of the MD5 hash value should give the same result as the one indicated in *md5.txt* file, a value similar to "d98307dc53ca83358a2dfdb33afc2672".

To calculate the MD5 hash value of a file, you can use different tools: for example *md5summer*[10] or *hashmyfiles*[11] (Windows) or the *md5sum* command line tool for Linux / MacOS.

If the hash value of the file you downloaded does not match to the one on the WEW site, it could mean that there were errors during the download process which corrupted your file. This is possible even if your downloaded file size is the same as original file size.

4.2 BURNING DEFT LINUX ON OPTICAL MEDIA

[9] http://en.wikipedia.org/wiki/MD5
[10] http://www.md5summer.org/
[11] http://www.nirsoft.net/utils/hash_my_files.htm .This application is already included in DART.

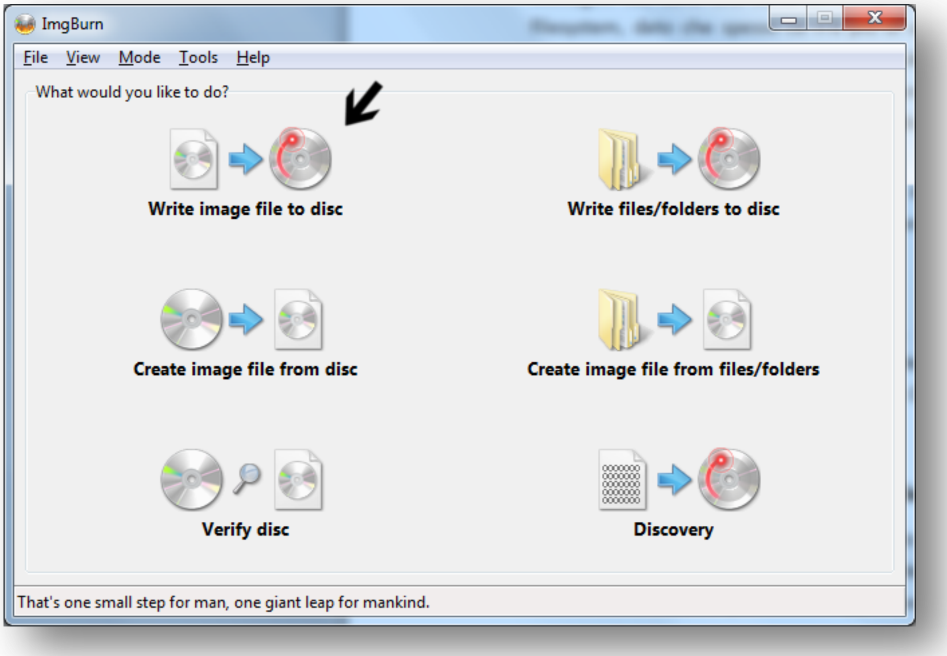
DEFT Linux 7 (the live version being used on physical machines) is distributed as an ISO image which must then be burned to a DVD in order to be bootable[12].

To burn the ISO image you will need disk burning software which is freely available online. Most of these applications are very user-friendly; just follow the steps provided within the program to burn your ISO image to a disk.

ISO images function as a snapshot of an entire system.

This includes the hard drive file systems. Your ISO image serves as a platform for forensic analysis of the target system. The deft ISO must be burned using the original snapshot.

Burning ISO images is possible with almost every burning software[13], simply by selecting the option for the images.


ImgBurn
File View Mode Tools Help
What would you like to do?
Write image file to disc
Write files/folders to disc
Create image file from disc
Create image file from files/folders
Verify disc
Discovery

That's one small step for man, one giant leap for mankind.

ImgBurn can write image files to a disk

Online there are thousands of links and howto's which explain how to burn ISO images to CD / DVD with many different operating systems.

4.3 CREATING A BOOTABLE USB STICK CONTAINING DEFT LINUX

[12] Given their small size, DEFT 6 and earlier versions could also be burned to CD.

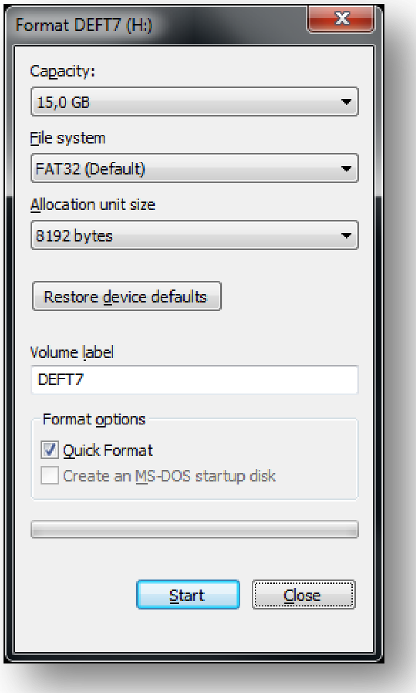
[13] On Windows we suggest you to use, for convenience, free tools such as ImgBurn or InfraRecorder. On Linux the burning software K3B has the functionality required to burn the image file. On Mac OS is sufficient use the Disk Utility application.

An alternative to using optical media, is to create a bootable USB flash drive containing DEFT Linux as if it were a live CD / DVD (only on PCs that support booting from USB device).

There are several ways to create USB mass storage devices containing DEFT Linux Live. For Windows, Linux and Mac systems we recommend using the free universal application UNetbootin[14].

It performs the write operation after the user selects the ISO image to be put on the USB stick and the drive letter the system will acquire.

We recommend you to format the USB stick with the FAT32 file system. You may also want to set a *"volume label"* to remind you which distribution and version is on the usb flash drive.



Format DEFT7 (H:)

Capacity: 15,0 GB

File system: FAT32 (Default)

Allocation unit size: 8192 bytes

Volume label: DEFT7

Format options

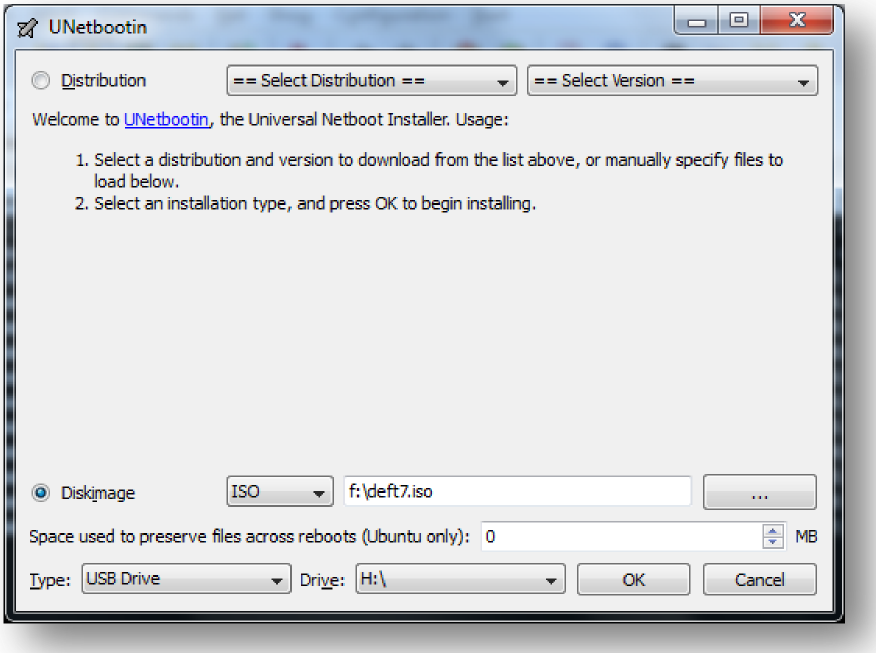
☑ Quick Format

□ Create an MS-DOS startup disk

Preparing the USB flash drive

Start UNetbootin - no installation required - and, by enabling the radio button "DiskImage", select the ISO file you want to convert into a bootable Live USB, select the drive letter of the USB stick you want to use.

[14] http://unetbootin.sourceforge.net/



UNetbootin

○ Distribution == Select Distribution == == Select Version ==

Welcome to UNetbootin, the Universal Netboot Installer. Usage:

1. Select a distribution and version to download from the list above, or manually specify files to load below.
2. Select an installation type, and press OK to begin installing.

● Diskimage ISO f:\deft7.iso ...

Space used to preserve files across reboots (Ubuntu only): 0 MB

Type: USB Drive Drive: H:\ OK Cancel

UNetbootin: Main Screen

At the end of the write operation you will get a Live USB version that will be used to start DEFT Linux on any PC that supports booting from USB port, common feature on most newer machines.

4.4 SETTING THE BIOS AND /OR THE BOOT SELECTION POPUP/MENU

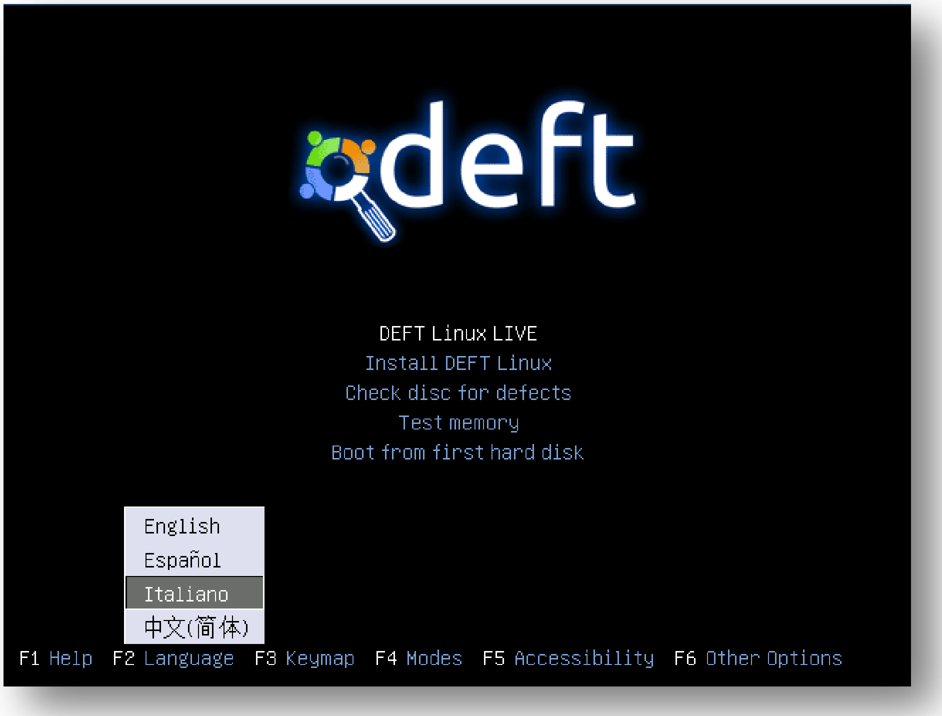
It is important to make sure that the BIOS of the system being analyzed is set to boot from CDROM / DVDROM / BDROM or from external storage devices (according to the media containing DEFT). In any other circumstances, configure the BIOS, save and restart the system either with the DVD already inserted in your CD / DVD drive either with the USB stick already connected[15].

We recommend changing the boot order of the devices directly in the BIOS to prevent an accidental reboot of your PC (e.g. a power surges).

[15] Generally, during startup is indicated which key to press to see the boot menu, often called "Boot Selection Popup" or "Boot Device Menu". The keys usually dedicated to the Boot Menu are F8, F9 and F12, but on some architectures the boot menu can also be accessed by pressing ESC.

4.5 BOOT PARAMETERS OF DEFT

After having started the DEFT boot loader, you will see a screen with several boot options. The first option will require you to select a language for the DEFT[16].



Choice of language

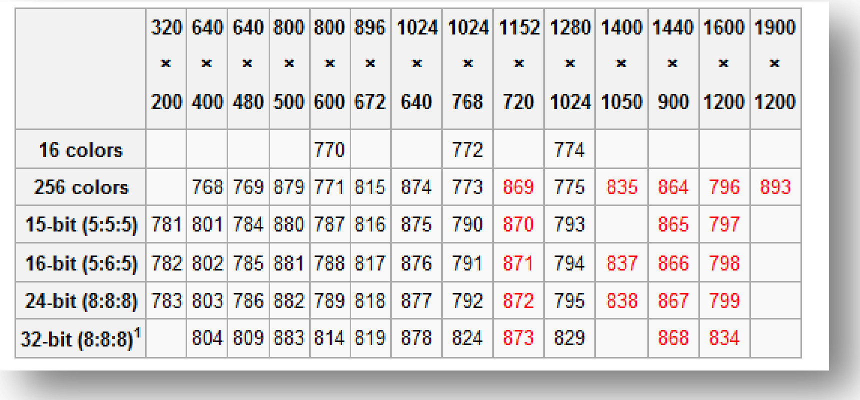
After selecting the language, you can use the up / down keys to move through the drop-down menu. By using the function keys, you can set additional parameters such as:

- Help (F1)
- Language (F2)
- Keyboard (F3)
- Mode (F4)
- Accessibility (F5)
- Other options (F6)

The F6 function key allows you to customize some of the startup parameters of DEFT. You may choose from some pre-set options on the menu, or customize them yourself.

[16] It's accessible by pressing F2 on startup settings window.

The kernel parameters available by pressing the F6 key are:

<table>
<tr><td><b>acpi=off</b></td><td>At boot ACPI functions are not used for managing of the electricity used by your system. Useful in case of problems starting the live, in the case where the PC does not support ACPI or if the ACPI causes problems of rebooting or blocks of the system.</td></tr>
<tr><td><b>noapic</b></td><td>Disables the APIC interrupt controller (Advanced Programmable Interrupt Controller).</td></tr>
<tr><td><b>nolapic</b></td><td>nolapic, disables the APIC functions for Intel CPU-based architectures;</td></tr>
<tr><td><b>edd=on</b></td><td>Enables Enhanced Disk Drive.</td></tr>
<tr><td><b>nodmraid</b></td><td>nodmraid, disables the kernel setting for dmraid raid type of software;</td></tr>
<tr><td><b>vga = xxx</b></td><td>Sets the framebuffer resolution if your video card is in vesa mode You can choose from the following modes:

<table>
<tr><th></th><th>320 × 200</th><th>640 × 400</th><th>640 × 480</th><th>800 × 500</th><th>800 × 600</th><th>896 × 672</th><th>1024 × 640</th><th>1024 × 768</th><th>1152 × 720</th><th>1280 × 1024</th><th>1400 × 1050</th><th>1440 × 900</th><th>1600 × 1200</th><th>1900 × 1200</th></tr>
<tr><td><b>16 colors</b></td><td></td><td></td><td></td><td></td><td>770</td><td></td><td></td><td>772</td><td></td><td>774</td><td></td><td></td><td></td><td></td></tr>
<tr><td><b>256 colors</b></td><td></td><td>768</td><td>769</td><td>879</td><td>771</td><td>815</td><td>874</td><td>773</td><td>869</td><td>775</td><td>835</td><td>864</td><td>796</td><td>893</td></tr>
<tr><td><b>15-bit (5:5:5)</b></td><td>781</td><td>801</td><td>784</td><td>880</td><td>787</td><td>816</td><td>875</td><td>790</td><td>870</td><td>793</td><td></td><td>865</td><td>797</td><td></td></tr>
<tr><td><b>16-bit (5:6:5)</b></td><td>782</td><td>802</td><td>785</td><td>881</td><td>788</td><td>817</td><td>876</td><td>791</td><td>871</td><td>794</td><td>837</td><td>866</td><td>798</td><td></td></tr>
<tr><td><b>24-bit (8:8:8)</b></td><td>783</td><td>803</td><td>786</td><td>882</td><td>789</td><td>818</td><td>877</td><td>792</td><td>872</td><td>795</td><td>838</td><td>867</td><td>799</td><td></td></tr>
<tr><td><b>32-bit (8:8:8)[1]</b></td><td></td><td>804</td><td>809</td><td>883</td><td>814</td><td>819</td><td>878</td><td>824</td><td>873</td><td>829</td><td></td><td>868</td><td>834</td><td></td></tr>
</table>
Deprecated parameters in red, in black parameters founded with no malfunction. For more information on adjustable parameters at boot time, you can refer to Appendix 1.</td></tr>
<tr><td><b>nomodeset</b></td><td>To boot DEFT Linux on a <b>Mac Book Air</b> it is necessary to add the <i>nomodeset</i>[17]parameter. This parameter allows you to properly handle the video drivers and to use the system without screen issues.</td></tr>
</table>

[17] Taken from www.kernel.org/doc/Documentation/kernel-parameters.txt

This is a kernel boot option that tells the kernel not to enable kernel mode setting (KMS). Video support is Usually a combination of a kernel drm driver and Xorg drivers working together. KMS is used with Intel, Nouveau, and Radeon kernel modules. KMS is required for Intel and Nouveau, and optional for Radeon (although, with different features).

If you want to use the vesa Xorg driver, and you have hardware uses the Intel That, Nouveau, or Radeon kernel modules, you may need to boot with nomodeset, or blacklist the matching module, or just delete the module.The modules will be found in /lib/modules/<kernel-version>/kernel/drivers/gpu/drm/

toram	Requires (when possible) to load the entire image of DEFT to RAM, allowing to remove the DVD or the USB stick. The execution speed is greatly increased because you make read operations from disk or flash drive not necessary. Also you can use the DVD player for any forensic acquisitions (for example with guymager[18]) or to burn data (for example with the burning program *Xfburn*[19] in the menu "Sound & Video").The parameter "toram" is triggered only if the RAM is sufficient to contain the image of the DEFT DVD / USB[20].The DEFT 7 distribution takes up about 1.4GB, therefore we recommend that you start it in "toram" mode only when the PC has at least 2GB of memory. The DEFT 6 distribution, however, takes up only 700MB, so it is bootable in "toram" even on PCs that have only 1GB of memory.

To select the kernel parameters shown on the menu, press the spacebar or the Enter key at the chosen ones: an 'X' will be inserted to confirm the addition to the kernel.

If you wish to specify additional kernel parameters, after pressing F6, press the "Esc" key to clear the menu and view in the background the kernel boot line where you can type in the chosen parameters, keeping them separated from each other with spaces.

[18] http://guymager.sourceforge.net/

[19] http://www.xfce.org/projects/xfburn

[20] It is recommended in any case to leave a part of free RAM for the normal activities of the system

4.6 INSTALLING LINUX DEFT 7

By the 7th Release, DEFT can be installed on any x86 system.

The following are the minimum and recommended system requirements for installation:

*** Minimum requirements**

- X86 CPU 200Mhz
- 128 MB RAM
- Hard Drive 20 GB
- Vesa compatible 16MB Video Card
- Network adapter 10/100
- USB 2.0 interfaces
- DVD player

Optimal requirements

- Intel dual core CPU
- 2GB RAM
- Hard Drive SATA 500 GB
- Intel Video card with dedicated memory
- 10/100/1000 Network Card - WiFi N
- USB 3.0 and e-sata interfaces
- DVD player

The system is installed via a standard wizard where the user must answer a few questions. The operation that requires most attention is the partitioning of the mass memory to host the system.

Despite the changes demanded based on the experience and the way the user works, we would like to give some tips on the way to obtain an optimal installation:

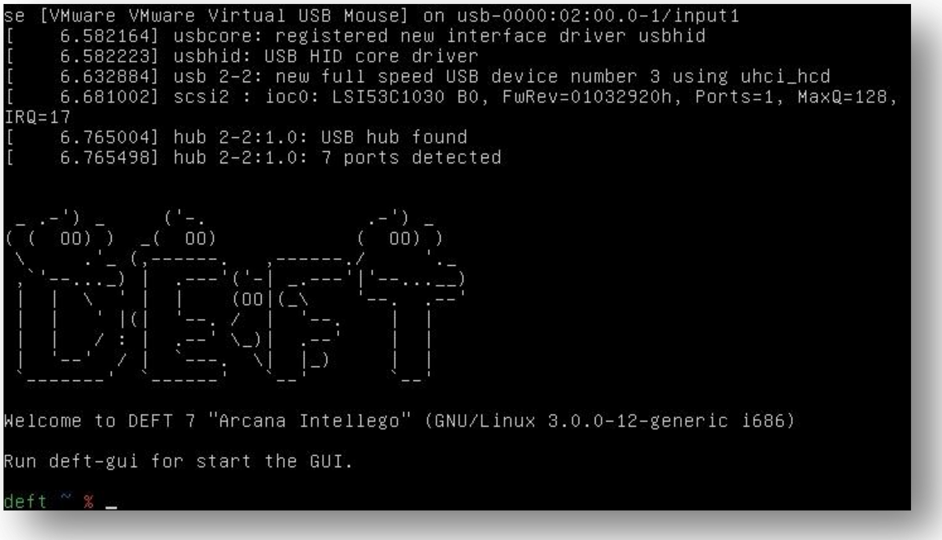
- Keep at least 20GB of hard disk space;
- Partition the disk according to your needs by creating a swap partition with a level of swappiness[21] of 10. This will reduce the sudden slowdowns caused by use of the swap partition[22];
- Create a user during installation, however, remembering always to use DEFT Linux with the root user to avoid problems due to the demand for permission by certain applications;
    - To enable the root account by setting the password, type the command "sudo passwd" and answer the questions;
    - To become root, type "sudo su -" (your password will be required) or "su -" (you will be prompted for the root password);
- Do not remove **FOR ANY REASON** the freezing on updating some packages deliberately blocked: they are part of a process of personalization of all the security mechanisms of the storage devices connected to the system.

[21] For more information https://help.ubuntu.com/community/SwapFaq

[22] If the computer has more than 4GB of RAM, could be considered a solution as not to create a SWAP partition: in this way you will avoid unexpected delays caused by use of the swap partition.

CHAPTER 5: DEFT LINUX TEXT MODE

Once the boot process has finished, the system presents a text-based session (with six terminals accessible through the key combination ALT + F1 -> ALT + F6) with a bash shell with root permissions[23].



```
se [VMware VMware Virtual USB Mouse] on usb-0000:02:00.0-1/input1
[    6.582164] usbcore: registered new interface driver usbhid
[    6.582223] usbhid: USB HID core driver
[    6.632884] usb 2-2: new full speed USB device number 3 using uhci_hcd
[    6.681002] scsi2 : ioc0: LSI53C1030 B0, FwRev=01032920h, Ports=1, MaxQ=128,
IRQ=17
[    6.765004] hub 2-2:1.0: USB hub found
[    6.765498] hub 2-2:1.0: 7 ports detected


 _ .-') _     ('-.             .-') _
( (  OO) )  _(  OO)           (  OO) )
 \     .'_ (,------.   ,------./     '._
 ,`'--..._) |  .---'('-| _.---'|'--...__)
 |  |  \  ' |  |    (OO|(_\    '--.  .--'
 |  |   ' |(|  '--. /  |  '--.    |  |
 |  |   / : |  .--' \_)|  .--'    |  |
 |  '--'  / |  `---.  \|  |_)     |  |
 `-------'  `------'   `--'       `--'

Welcome to DEFT 7 "Arcana Intellego" (GNU/Linux 3.0.0-12-generic i686)

Run deft-gui for start the GUI.

deft ~ % _
```

DEFT: text interface session

5.1 MANAGING STORAGE MEDIA

DEFT supports mass storage devices and popular file systems. As already mentioned, DEFT does not automount as in the typical Live distributions (eg Knoppix, Ubuntu, etc...) so as to avoid accidental alteration of attached storage.

The contents of stored memory can still be altered by the mount operation performed in the read/write mode, an action that DEFT does not run automatically.

[23] This implementation is very useful when you start DEFT Linux on very old computers that do not allow an optimal use of the graphical interface or for the advanced user who prefers to work directly from the command line

5.1.1 USEFUL COMMANDS

Here are some useful commands to perform tasks related to the management of storage devices:

- *fdisk-l:* lists all the partitions and storage devices connected to the system;
- *mmls / dev / xxx* or *mmls filename.dd:* lists the partitions on the device or in the raw image indicating the starting offset of each partition and the unallocated spaces;
- hdparm-Ig / dev / xxx: shows the AC characteristics of the mass memory xxx.
- This implementation is very useful when you start DEFT Linux on very old computers that do not allow an optimal use of the graphical interface or for the advanced user who prefers to work directly from the command linestorage devices.
- *mount:* displays the file system type of storage devices connected to the system and the manner in which they were mounted (read only / read-write);
- *df -h:* displays information about the size of the mounted devices and their free space.

5.1.2 MOUNT OF STORAGE DEVICES

The *mount* command allows you to connect a file system - present on a device or on a file stored on the disk - to a system directory.

In case you want to mount a device such as a hard disk, USB stick, CD / DVD / CD-ROM, floppy disk, etc. ... you will be using, as the source, the device itself that identifies it. In this case:

- */dev/fdX*[24] for floppy disks (usually with a single floppy you have /dev/fd0);
- */dev/hdX* for IDE hard disks;
- */dev/sdX* for SATA hard drives or USB devices;
- */dev/cdrom* for CDROM.

In forensics, the direct mounting of an evidence (i.e. a disk, a USB flash drive, etc ...) must be made as read-only and only when necessary[25]. This ensures that the integrity of the evidence can be guaranteed .

The selected file system, as well as being stored on a device, can be contained within a file on the disk, containing the *dump* or the bit-stream image of the acquired device.We will have, in this case, images:

- in the "bit stream image" format **(dd** or **raw)**[26];
- in the "Encase" format **(ewf);**
- in the "Advanced Forensic Format" format **(aff).**

[24] The X identifies the device number on the system, so you will have /dev/sda for the first disk and /dev/sdb for the second one, while the numbers observed after the device with the command "fdisk -l" (/dev/sda1, /dev/sda2, etc ...) identify the number of partition within the device

[25] Best practices indicate clearly that you should never work on the original mass memory but always and only on a copy.

[26] Often the bit-stream format is divided into files of smaller size (2-4 Gigabytes each) in order to be saved on file systems with filesize limit (eg.FAT32), in this case is defined as **split raw.**

5.1.3 MOUNTING A DEVICE (HARD DISK, USB STICK, FLOPPY DISK, CDROM, ETC ...)

To mount a file system as read-only simply type a command like:

```
mount-t type -o options source mount_point
```

where

- *type* is the type of filesystem, usually vfat, ntfs-3g, ext3 ... etc.., or auto when you are not sure of the type of the file system[27] (if you omit this option, mount will independently try to recognize the filesystem type, and usually succeeds);
- *source* can be a partition such as */ dev/hda1* or */ dev/sda1;*
- *mount-point* is usually a directory *in /media* - that must be created before running the mount command[28] .

The frequently used parameters(which must follow the -o option in the *mount* command) are:

- *ro - read-only:* mount as read-only;
- *rw - read-write:* mount as write mode[29] [29] ;
- *loop* - to mount an image file;
- *noatime* - do not change the time of last access;
- *noexec* - does not allow the execution of files;
- *offset=N* - when you mount a disk image file (topic covered in depth in the next section) it gives the number of bytes to skip to point at the beginning of the logical partition to mount (or recoverable *mmls fdisk-lu).*

Example 1: mount with write access an NTFS partition on which the dump of a device (the result of a forensics acquisition) will be saved :

```
mount -t ntfs-3g -o rw /dev/sdb1 /media /dest
```

Example 2: mount an NTFS partition of a hard disk you want to acquire as read-only e.g. to preview files during fieldwork activities (it is essential to use the *-o ro* option to prevent any accidental writes to disk):

```
mount -t ntfs-3g -o ro /dev/sdb1 /media /evidence
```

[27] Usually, even if omitted, the mount command can identify the type of filesystem independently.

[28] For example with the command *mkdir /media/NameOfTheFolderIWantToCreate*

[29] To be used for the directory where you will save the copy

5.1.4 MOUNT OF A DD/RAW IMAGE FILE

To mount an image file as read-only (containing the dump of an entire disk, not of a single partition) you can use the following command:

*mount -t type -o ro,loop,offset=$((512*partition-start)) options image_file.dd mount_point*

The options and the syntax of the *mount* command are the same as the ones indicated in the previous paragraph.

In this case, however, a method of mount based on *device loop* "converts" (virtually, without altering the source) a (static) image file on a linux device (dynamic), thus allowing the kernel to mount it as if it were an actual device.

The *loop* option allows this type of abstraction and is derived from the implicit and automatic application to the below layer of the *losetup* command, through which you can associate a loop device to the image *image.dd.*

In this way you can run applications working on devices also on images of mass storage.

If you want to avoid using *-o loop*, you must, before mounting, create a loop device using the command:

losetup -r /dev/loop0 /media/disk1/dump.dd

This loop device will be used as if it were a source disk to be mounted in the manner described previously[30] .

So, being able to directly use the *-o loop* you avoid creating a loop device that you should remember to close with the command *"losetup -d /dev/loop0".*

The other essential option when you mount an image file containing the acquisition of an entire disk (and therefore, not of a single partition) is **"offset"**.

Through the mmls utility you can find the starting offset of a disk partition:

mmls dump.dd

the resulting output will be similar to:

```
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    0000002047    0000002048    Unallocated
02:    00:00  0000002048    0000032255    0026624000    Unknown Type (0x27)
03:    00:01  0000032256    0086598247    0000204800    NTFS (0x07)
05:    -----  0086598248    0976773167    0000002048    Unallocated
```

[30] You will need to type a command like *mount-o ro /dev/loop0 /mnt/dest*

Mount the partition identified as 03 by the *mmls* output specifying the offset multiplied by 512[31]:

```
mount -t ntfs ro,loop,noatime,noauto,noexec,offset = 16515072 dump.dd /media/dest
```

Instead of performing the calculation of the offset by multiplying by 512 the "starting" point of the partition obtained with *mmls,* you can use a shell mathematical operator by including as an offset, the value of $((512 * partition-start)), where "partition-start" indicates the byte offset of the partition you want to mount (in the previous example the value **33256).**

Therefore *mount* with the command:

```
mount -t ntfs ro,loop,noatime,noauto,noexec,offset=$((512 * 32256)) dump.dd /media/dest
```

Completed all the operations on the memory devices, before disconnecting the device from the system, it is necesssary to use the umount command:

```
umount /media/mntpoint.
```

As mentioned previously in the manual, these commands may be used to mount a file containing the dump of an entire disk. In the event that - rare but possible - you made the dump of a single partition, it is not necessary to use the parameter "offset" as the beginning of the partition coincides with the one of the file.

5.1.5 MOUNT A DD/RAW IMAGE FILE SPLIT INTO MULTIPLE FILES (SPLIT RAW)

In the case where the dd/raw image file (therefore a bit-stream or bit-to-bit image of a disk) is divided into multiple files, it is necessary to prepare the file which you are going to mount with the mount command shown in the previous section.

Suppose you have an image composed by dump.001, dump.002, dump.003, dump.004 and dump.005 files. You cannot apply directly the instructions outlined in the previous paragraph, because in this case you don't have a single image file on which to run the *mount* command, but five[32].

To mount split raw image files, in split-raw format, you have three possibilities.

The first method consists in the **concatenation** of the individual files into a single image file, bringing you back to the case described in the previous paragraph of a single dump.dd file mounting.The obvious disadvantage is that, in this case, the space required for the operation will be equal to the one occupied by the sum of the individual files because you would make a copy, concatenating them into a single file[33] [33] .

The command to be executed is as follows:

```
cat dump.* > image.raw
```

[31] 512 bytes is the default size of a sector that makes up a memory storage

[32] In fact, in the case of acquisitions of large disks, the number will rise to tens or hundreds.

[33] This solution is illustrated for explanatory purposes only, since one of the two following is generally preferred.

The result is a single file *image.raw* containing the entire disk obtained by the concatenation of individual image segments.

On this file you will proceed as indicated in the preceding paragraph.

The second method is to use the command *affuse* of the *Afflib* suite[34].

It will be used further on to mount the image in the *AFF* format. This command will create a kind of "virtual" image (and therefore visible by the system but not existing in reality[35]) which will be mounted as described in the previous paragraph. The command to be executed, after you created the directory */mnt/raw,* will be:

```
affuse dump.001 /mnt/raw
```

This command will produce, within the directory */mnt/raw,* a "virtual" file containing the dd/raw image made by the concatenation of the various files that make up the real image.This file will be visible as *dump.001.raw* and will be used as a parameter of the mount in the previous section.

```
mount -t ntfs ro,loop,noatime,noauto,noexec,offset=16515072 /mnt/raw/dump.001.raw /media/dest
```

You should remember that, when you set up the mount with the *affuse* command, it is necessary to unmount it addition to the mounted "virtual" file containing the image with the command:

```
fusermount -u /mnt/raw
```

The third method to mount a split-raw image is to use the command line tool *xmount*[36]. Similarly to the *affuse* command*, xmount* creates a virtual file containing the image made by the concatenation of the individual segments that make up the real image.

The command in this case is:

```
xmount -- in dd -- out dd dump.* /mnt/raw
```

A "virtual" file, called "dump", will be created with no extension in the directory */mnt/raw*. This file can be mounted, as shown in the previous case, selecting the offset of the desired file system in read-only mode.

5.1.6 FILE TYPE EWF/ENCASE

Mounting memory acquired in the .EWF format is accomplished with the mount_ewf application.This program is able to virtually convert EWF files to the raw format which allows the device to be mounted as if it was acquired in the dd format.

Example: the memory disk01 is divided into the following files

disk01.E01 disk01.E07 disk01.E13 disk01.E19 disk01.E02 disk01.E08 disk01.E14 disk01.E20 disk01.E03 disk01.E09 disk01.E15 disk01.info disk01.E04 disk01.E10 disk01.E16 disk01.E05 disk01.E11 disk01.E17 disk01.E06 disk01.E12 disk01.E18

[34] http://afflib.org/

[35] Similarly to what happens to the files in the /proc folder of the filesystem

[36] http://www.forensicswiki.org/wiki/Xmount

With the command

```
mount_ewf /media/case1/disk01.E* /mnt/raw
```

it is possible to concatenate the split image and perfom a virtual conversion in the raw format.

The operation will result in the creation of the raw file */ mnt/raw/disk01,* in the folder */mnt/raw/*.

It will be identified by the system as a single dd file, although virtual, and may be mounted following the procedure shown in the previous paragraph.

Example:

```
mount -t ntfs -o ro,loop,offset=$((512 * 63)) /mnt/raw/disk01 /mnt/c
```

5.1.7 FILE TYPE AFF

As for the EWF format,the memories acquired in the AFF format can be mounted with the affuse mount utility.Affuse allows you to use the acquisition in the AFF format as they were raw images.

The command syntax is:

```
affuse /media/disk/disk01.aff /mnt/raw
```

The output file will be */mnt/raw/disk01.aff.raw* which can be mounted following the procedure to mount the raw image, shown previously.

5.2 HASH CALCULATION

The hash of a block of data (eg a file) is a sequence of alphanumeric characters of fixed length calculated by a mathematical function.

This mathematical function is mono-directional: it is impossible to reconstruct the block that has originated a hash string.

Any alteration of the data, albeit minimal, will result in a completely different hash.

With Linux systems you can use one of the following applications to generate an hash string:

- *md5sum;*
- *sha1sum;*
- *md5, sha1 and sha256 deep;*
- *dhash.*

5.2.1 MD5SUM

The acronym MD5[37] (Message Digest algorithm 5) identifies a cryptographic hash algorithm developed by Ronald Rivest in 1991 and standardized with the Request for Comments RFC 1321.

This algorithm, taking as input a string of arbitrary length (such as a file), it produces as output another string of 128 bits used to calculate the digital signature of the input. The calculation is very fast and the output returned (also known as "MD5 Checksum" or "MD5 Hash") is such that it is highly unlikely that a collision will occur between the hashes of two different files. Finally, as for most of the hashing algorithms, the possibility of deriving the initial string from the resulting hash is almost nonexistent[38].

For example, to calculate the MD5 hash value of a disk use the command:

```
md5sum /dev/sda
```

5.2.2 SHA1SUM

The SHA term[39] indicates a family of five cryptographic hash functions developed since 1993 by the National Security Agency (NSA) and published by NIST as a federal standard by the U.S. government.

Like any hash algorithm, SHA generates a fixed length value from a variable length message by using a mono-directional function.

The algorithms of this "family" are called SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. The first type, SHA-1, calculates a string of only 160 bits, while the others calculate digest of a length in bits equal to the number indicated in their acronym[40].

Right now the most widely employed algorithm of the SHA family is the SHA-1 and it is used in many applications and protocols.

To calculate the SHA-1 hash value, of a disk for example, use the command:

```
sha1sum /dev/sda
```

5.2.3 MD5 AND SHA DEEP

Md5, sha1, sha256 and sha512 deep allow you to calculate the hash value of more files recursively.

Example:

```
md5deep -l /root/evidence/ > hash_device.txt
```

The syntax mentioned above calculates the md5 hash of all files in /root/evidence/ directory and saves the hash values in the hash_device.txt file.

[37] http://en.wikipedia.org/wiki/MD5

[38] The range of possible output values is in fact equal to 2 to the power of 128.

[39] Secure Hash Algorithm - http://en.wikipedia.org/wiki/Secure_Hash_Algorithm

[40] Eg: SHA-256 produces a digest of 256 bits.

5.2.4 DHASH

Dhash, available in Italian and English, allows you to calculate the hash values of files and storage devices, providing real time information such as the estimated time before the end of the operation the and progress of the calculation.

You can also generate a report in html format[41].

From lab tests *Dhash* turned out to be 10% faster than the tools listed above.

Example:

```
dhash -t -f /dev/sda --md5 --sha1 -l dhashlog.html
```

The syntax above mentioned allows you to calculate simultaneously the sha1 and md5 hash of the /dev/sda device and save the values in the dhashlog.html file.

5.3 CAPTURE STORAGE MEDIA

The acquisition of a mass memory is the process that allows you to clone a physical memory, object of the analysis. Within Linux systems, this operation is possible by using the following tools:

- *dd;*
- *ddrescue;*
- *dcfldd;*
- *dhash.*

In addition to these commands, the DEFT team has created Cyclone, a wizard executable from the terminal to make a guided acquisition through the simple answer to the questions that appear on the screen.

5.3.1 DD

dd takes as input a file or a device and returns, on a different file or device, the exact binary sequence that composes it.

Example:

```
dd if=/dev/sda of=/media/diskimage.img
```

The command takes as input the mass storage device */dev/sda* and returns as output its clone within the file *diskimage.img* in the */media/* folder.

You can make the acquisition of the mass memory to a file or to a mass storage device (and vice versa)[42].

Example:

```
dd if=/dev/sda of=/dev/sdb
```

[41] Dhash is also able to run at the same time the activities of acquisition and calculation of the hash value.

[42] This practice is much less used in the field of computer forensics.

It is important to pay attention to this command because the destination device (in this example */dev/sdb)* is deleted and overwritten for the size of the source device (in this example */dev/sda).*

This means that if */dev/sda* is a 60GB hard disk and */dev/sdb* is a 250GB hard disk, the above command will overwrite the first 60GB of the target disk *(/dev/sdb)* with the entire bit-to-bit content of the source disk *(/dev/sda),* making its content completely unrecoverable, compromising thereby the data on the disk that is not overwritten.

5.3.2 DDRESCUE

As *dd, ddrescue* allows you to clone the content of a disk and saving it directly to another memory device.

ddrescue is an evolution of dd: it allows to acquire mass memory devices that contain errors while accessing determined disk sectors.The acquisition by *ddrescue* can also include those bad sectors that will be acquired by setting to zero all the unreadable bits.During the acquisition process ddrescue provides updates on how many bytes are read and written, how many errors have been found and the acquisition rate calculated in bytes/s.

Example:

```
ddrescue /dev/sda /media/disco.img
```

5.3.3 DCFLDD

dcfldd is another enhanced version of dd that can be used to calculate the hash value(md5 and sha1, individually or together) during the acquisition of the memory. During the acquisition detailed information is provided on what has been read and written.

Example:

```
dcfldd if=/dev/sda of=/media/disco.img hash=sha1 hash=md5
```

5.3.4 DHASH

This software allows the acquisition in dd format and the simultaneous calculation of the hash.

It turned out to be more than 10% faster than other available programs.

Example:

```
dhash -t -f /dev/sda --md5 --sha1 -o disco.dd
```

The above mentioned syntax allow you to acquire and simultaneously calculate the sha1 and md5 hash value of the /dev/sda device and save the resulting strings in the dhashlog.html log file.

5.4 CREATION OF A TIME LINE

One of the most popular tools for creating time lines is mac-time, application of the Sleuthkit suite developed and maintained by Brian Carrier.

There are two main commands to generate timelines of the filesystem:

- *fls*[43] takes as input a raw file derived from the acquisition of a mass memory (either a single partition either a raw image of a disk with multiple partitions), and returns a list of all files (allocated or not whose, however, the record is still contained in the file allocation table), for subsequent use with mac-time;
- *mactime*[44] takes as input a list, created by *fls,* with all the data contained in the file system under analysis and provides a timeline in ASCII format.

5.4.1 FLS

Here an example of how to use *fls* in the case where the image *image-1.dd* contains a single file system/partition[45]:

```
fls -z GMT -s 0 -m C: -f ntfs -r /images/disco-c.dd > /workdir/harddisk-c.body
```

In the example, the following parameters have been used:

- *-z:* time zone on the system used to analyse;
- *-s:* mismatch in seconds of system time with the real time [46];
- *-m:* the text that has to be put before the path and file name in the Timeline[47] ;
- *-f:* the file system of the acquired memory;
- */images/disk-c.dd:* the image taken as input for the extraction of the timeline;
- */workdir/harddisk-c.body:* the file, in the *bodyfile* format containing the timeline extracted from the given input.

In the case where the dd image contains more partitions, you must use the parameter *-o* to indicate to *fls* the sector offset (and not bytes, as in the case of the *offset* parameter of the mount command), starting point of the partition you are going to analyse.To get a list of partitions and their offset values (expressed in sectors and not in bytes), it is recommended to use the command *mmls* of the TSK suite or the fdisk command with "-lu" parameters.In the case of an image containing a disk with a partition starting at sector 63 (generally, single partitions and the first partition of a disk always start at sector 63):

```
fls -o 63 -z GMT -s 0 -m C: -f ntfs -r /images/disk-c.dd > /workdir/disk-c.body
```

At this stage you have a file (for convenience with the .body extension) in body format[48] containing the timeline of the system under analysis.

[43] http://wiki.sleuthkit.org/index.php?title=Fls
[44] http://wiki.sleuthkit.org/index.php?title=Mactime
[45] It should be noted the absence of the "offset" parameter.
[46] The difference between system time and real time is obtained from bios, during the acquisition.
[47] It can be obtain checking the difference between the bios time and the real Time (during the acquisition step).
[48] Generally you indicate the letter on which the drive is mounted, "C", "D" and so on.

This format is not immediately accessible by the examiner as it contains unordered coded dates and records. It is therefore necessary to process it so as to make it readable, in order and in the chosen format[49].

Here is an excerpt from a body file which makes clear the difficulties in interpreting the content by the examiner:

```
[...]
          0|C:/WINDOWS/inf/mdmpin.PNF|4718-128-
          3|r/rrwxrwxrwx|0|0|19268|1299255392|1299255392|1299255392|1299257718
          0|C:/WINDOWS/inf/mdmpn1.inf|804-128-
          3|r/rrwxrwxrwx|0|0|6376|1299257379|1092916800|1299257709|1092916800
          0|C:/WINDOWS/inf/mdmpn1.PNF|4717-128-
          3|r/rrwxrwxrwx|0|0|10424|1299255392|1299255392|1299255392|1299257718
          0|C:/WINDOWS/inf/mdmmod.PNF|4747-128-
          3|r/rrwxrwxrwx|0|0|18540|1299255386|1299255386|1299255386|1299257719
          0|C:/WINDOWS/inf/mdmmoto.inf|779-128-
          3|r/rrwxrwxrwx|0|0|96032|1299257378|1092916800|1299257709|1092916800
          [...]
```

5.4.2 MACTIME

Mactime is the tool of the TSK suite that converts the timeline from the body format to the CSV format, ordering items and changing the display parameters based on the examiner needs.

Usually the command to be executed is the following:

MACTIME-B /workdir/disk-c.body -Z GMT -D > /workdir/disk-c.csv

-B specifies the input file, -Z the time zone, *-d > /workdir/disk-c.csv* represents the output file containing the time line in csv format[50].

The *mactime* command has a summary reporting feature of daily and hourly activities detected on the filesystem, which is added to the function of converting in CSV format and to the function of sorting the records generated by *fls* command.This information may be essential to evaluate which days - or at what time - usage activities are detectable on the PC, showing peaks and anomalies perhaps due to weekend activities that hardly jump out in a traditional timeline.

To get a report of daily activities occurred on the filesystem, just add the *parameters -d -i* followed by the name of the file you want to save that report to.The report on time activities is obtained with *-h -i* parameters followed by the name of the file you want to save that report to.

You will obtain, in this way, a file containing records similar to the following:

```
[...]
Wed Oct 12 2011: 801
Thu Oct 13 2011: 987
Fri Oct 14 2011: 252
Sun Oct 16 2011: 25352
Mon Oct 17 2011: 463
Tue Oct 18 2011: 711
[..]
```

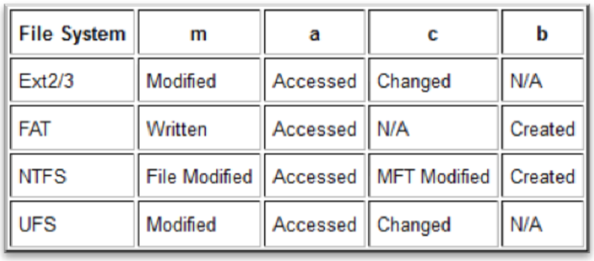
[49] Generally, you will use the .CSV format for compatibility with the editors and spreadsheets.

[50] It is preferable to export in csv format to ease the consultation by applications like OpenOffice or Excel.

In the example above you can see that on October 16, 2011 there were 25,352 activities on files[51]. This value may not be of interest but may, in some cases, be of great importance[52].

it is advisable to check the continuity or the average of the values during most of the analyzed days, which abuts perhaps on a certain value (eg <1000), and reach, as in the example, peaks of tens of thousands in a specific day. The examiner should proceed at this point to analyze in more detail the timeline of the day in which the anomaly was found[53].

The following table is useful to understand the meaning of the values that appear in the "Activity Type" column. They indicate the actions performed on files and folders in a given timeframe.



File System	m	a	c	b
Ext2/3	Modified	Accessed	Changed	N/A
FAT	Written	Accessed	N/A	Created
NTFS	File Modified	Accessed	MFT Modified	Created
UFS	Modified	Accessed	Changed	N/A

Here is an example of the result of processing a body file generated by the mactime command:

```
[...]
Fri Mar 04 2011 16:08:04 618605 .ac. r/rrwxrwxrwx    0       0       10618-128-1
C:/WINDOWS/system32/dllcache/fp4autl.dll
Fri Mar 04 2011 16:08:11 17672 ...b r/rrwxrwxrwx     0       0       10624-128-4
C:/WINDOWS/Prefetch/IMAPI.EXE-0BF740A4.pf
Fri Mar 04 2011 16:11:20 3014 ...b r/rrwxrwxrwx      0       0       10630-128-3
C:/WINDOWS/system32/wbem/Logs/wmiadap.log
Fri Mar 04 2011 16:11:29 10296 ..cb r/rrwxrwxrwx     0       0       10631-128-3
C:/WINDOWS/system32/drivers/ASUSHWIO.SYS
[...]
```

[51] Intend: access, creation or modification of files at MFT entry or file level.

[52] For example, if the PC under analysis is an asset of a company where the work takes place from Monday to Friday, the investigator should investigate why such a high activity has occurred on Sunday.

[53] By performing new analysis of the registry, inserting USB sticks, launching programs, creation of LNK files, etc..

5.5 CREATING A SUPERTIMELINE

The timeline, as outlined in the previous paragraph, are very useful but limited to the activities detected in the filesystem[54]. In addition to the timestamp of the files, there are several metadata on the system under analysis that can be integrated with the timeline of the filesystem[55].

The tools to create this kind of "enriched timelines"[56]are included in deft.

In this case as well, the starting point is the image of a disk or a disk itself, as well as for the traditional timeline made with *fls* + *mactime* (or with the graphical interface *Autopsy).*

The specific tool used is *log2timeline*[57]. The framework was written by Kristinn Gudjonsson, and the development of its plugins involved the entire open source forensics community.

Log2timeline processes (parsing), recursively, the files of a partition mounted with some specific parameters, to allow the access to the filesystem metadata. In particular, the metadata *log2timeline* is able to date to process and insert into a supertimeline are listed in this **input modes** list:

1. Apache2 Access log;
2. Apache2 Error log;
3. Google Chrome history;
4. Encase dirlisting;
5. Windows Event Log files (EVT);
6. Windows Event Log files (EVTX);
7. EXIF;
8. Firefox bookmarks;
9. Firefox 2 history;
10. Firefox 3 history;
11. FTK Imager Dirlisting CSV files;
12. Generic Linux log files;
13. Internet Explorer history file, index.dat parsing;
14. Windows IIS W3C log files;
15. ISA Server text export;
16. Mactime body file;
17. McAfee AntiVirus Log;
18. MS-SQL Error log;
19. Opera Global and Direct browser history;
20. OpenXML metadata (Office 2007);
21. PCAP files;
22. PDF;

[54] So limited to create, edit or access the files.
[55] Some examples: the visits log of a browser, the changes to the registry keys of the system, antivirus logs, the activity of the registry, the link file in the LNK format, the prefetch etc..
[56] In the forensic jargon they are now indicated by the term "supertimeline".
[57] http://log2timeline.net

23. Windows Prefetch directory;
24. Windows Recycle Bin (INFO2 or I$);
25. Windows Restore Point;
26. Safari Browser history file;
27. Windows XP SetupAPI.log file;
28. Adobe Local Shared Object file (SOL/LSO), aka Flash Cookies;
29. Squid Access Logs (httpd_emulate off);
30. TLN (timeline) body files;
31. UserAssist key of the Windows registry;
32. Volatility *(psscan and psscan2* output);
33. Windows Shortcut files (LNK);
34. Windows WMIProv log file;
35. Windows XP Firewall Log file (W3C format).

The supertimeline can be saved in different formats. The most used format is the CSV format[58] and, compatible with several spreadsheets, can be displayed and edited simply with a text editor.
The full list of **output modes** in which the processing of the supertimeline can be currently exported is as follows:

- BeeDocs;
- CEF;
- CFTL;
- CSV;
- Mactime;
- SIMILE;
- SQLite;
- TLN;
- TLNX.

[58] https://en.wikipedia.org/wiki/Comma-separated_values

The first step to generate a supertimeline is-as mentioned previously-possessing the raw image containing the partition that is to be examined. You can use a device (eg */dev/sda),* a dd/raw image file , or even a EWF, AFF file or split raw converted as explained in the previous paragraphs.

Assume you have a *image.dd* file containing the disk image you want to analyse. The first thing is to mount in the way previously described, the partitions you want to obtain a supertimeline from.

You decide to analyse the only NTFS partition of the disk, situated at the offset sector 63 and identified by the letter *C:* on Windows.

With the command:

```
mount -o ro,loop,show_sys_files,streams_interface=windows,offset=$((512 * 63)) /mnt/raw/img.dd /mnt/c
```

The *C:* drive will be mounted in */mnt/c* where we execute *log2timeline:*

```
log2timeline -p -f winxp -r -z Europe/Rome/mnt/c/ -m C: -w c-log2t-unsorted.csv
```

The suggested parameters are:

- *-p:* Tells *log2timeline* to do a recursive "preprocessing" of directory being analyzed in order to obtain useful information for the plugins that will be executed later[59];
- *-f:* indicates the type of operating system (and therefore the set of plugins) that you want to apply to the directory given as input[60];
- *-r:* tells *log2timeline* to scan recursively the files thus not to stop to those in the specified directory;
- *-z:* indicates the time zone set in the PC under analysis [61];
- *-m:* indicates the string to be put before the path and filename in the supertimeline creation output, typically the drive letter of the disk under analysis (eg "C:", "D:", etc..);
- *-w:* specifies the file the supertimeline generated in CSV format has to be saved to.

The result of this process is a CSV file containing the individual items obtained from the analysis of the various artifacts, arranged in the order they were analyzed.

It is therefore necessary to use a tool to sort the entries and if necessary, select a period of interest and simultaneously filter keywords of interest.

The tool provided with these features is *l2t_process,* part of the *log2timeline* framework as well.

To order and view, for example, the PC's activities that took place in 2011, recorded in the *c-log2t-unsorted.csv* file:

[59] For example, the hostname of the pc, the users, the default browser, timezone, etc.. can be obtained.

[60] It could be omitted, thus indicating to log2timeline to test all the plugins on all the files.

[61] It can be obtained automatically with the "-p" parameter but it is often useful to indicate it manually.

```
l2t_process -i -b c-log2t-unsorted.csv -y 2008-01-01..2008-12-31 -k keywords.txt > c-log2t-2008.csv
```

Some of the useful options of *l2t_process* are:

- *-i:* are also included in the output entries outside the specified time range, if these contain information that suggest suspicious activities of timestomping[62];
- *-y:* force the date format as yyyy-mm-dd instead of the default format mm-dd-yyyy;
- *-b* indicates which file must be analysed by the script;
- *-k:* specifies the file containing the keywords you are interested in, excluding from the output the records that do not contain them.

The result of *log2timeline and l2t_process* will be a long list of activities recognized on the filesystem[63] and the metadata extracted from the file types previously indicated (log, events, links, browser history, etc. ...).

The columns of the file will have the following header:

1. Date
2. Time
3. Timezone
4. MACB
5. Source
6. Sourcetype
7. Type
8. User
9. Host
10. Short
11. Desc
12. Version
13. Filename
14. Inode
15. Notes
16. Format
17. Extra

[62] Eg MFT record with the 0 milliseconds value.

[63] In the case of NTFS we will have items obtained from the MFT table.

At this stage, the difficulty lies in focusing on the relevant items within thousands of results.

From the command line, *grep* can provide valuable support for excluding or including in the list certain types of activity.

It is also possible to import the supertimeline in a spreadsheet[64] to filter and analyse the content using the typical features of this kind of application.

One of the main categories on which it is useful to apply filters is the one concerning the type of metadata found in column 6 *SourceType.*Among the available types that you will have interest to filter, there are *NTFS $MFT, REG, Event Log, WEBHIST, XP Prefetch,* etc. ... that will allow you to distinguish between Internet browsing, USB sticks insertion (searching *USBSTOR* in the records concerning the register), opened files *(NTFS $ MFT),* or anything else of interest to you.

5.6 SEARCH FILES AND FOLDERS

You can search for files and folders by using one of the following tools:

- *locate;*
- *find.*

5.6.1 LOCATE

Locate allows you to search for files in a mass storage.

First you must update the indexing database running the command *updatedb*.

Example:

```
locate finance -q -i
```

Search, without distinguishing between uppercase and lowercase characters *(-i),* for files that contain the word *finance* in their own name.Thanks to -q option, errors accessing to a specific directory will be reported as well as the reason of that error (eg "access denied").

Example:

```
locate "*.png" -q
```

it will search for all the png files.

5.6.2 FIND

Find allows you to search for files without a prior indexing.

Example:

```
find . -iwholename "*porn*.png"
```

The tool will find all PNG files which contain the string porn in their name without distinction between the case.

[64] Deft offers the LibreOffice suite that includes the Calc spreadsheet.

Example:

```
find . -ctime -2 > list.txt
```

The tool will find all files created in the last 2 days and it will save a list in the list.txt file.

5.7 CARVING OF FILES

Carving is the process of recovering files no longer referenced by the file system, through the recognition of the header and the footer[65] of the file. It's a long process because the disk is examined from the first to the last bit.

Metaphorically speaking, you can compare this reading process to the one of tape drives.

5.7.1 FOREMOST

Foremost can recover deleted files directly from storage devices, or preferably, from "bit stream image" files.

The command

```
foremost -o outpdir dump.img
```

will start the carving process on dump.img file based on the /etc/foremost.conf configuration file and save the extracted files in the outpdir directory.

The command

```
foremost -t png -o outpdir dump.img
```

will start the carving process of all the png files on the dump.img file and save the extracted files in the outpdir folder.

The -t option will allow you to search for the following types of file:

[65] Header and footer are signatures which characterize the beginning and the end of a given file type; in detail they consist of a group of consecutive octal or hexadecimal values always present in a certain position of a given file at the beginning or end of the same.

jpg
gif
png
bmp
avi
exe
mpg
wav
riff
wmv
mov
pdf
ole
doc
zip
rar
htm
cpp

CHAPTER 6: DEFT LINUX GUI MODE

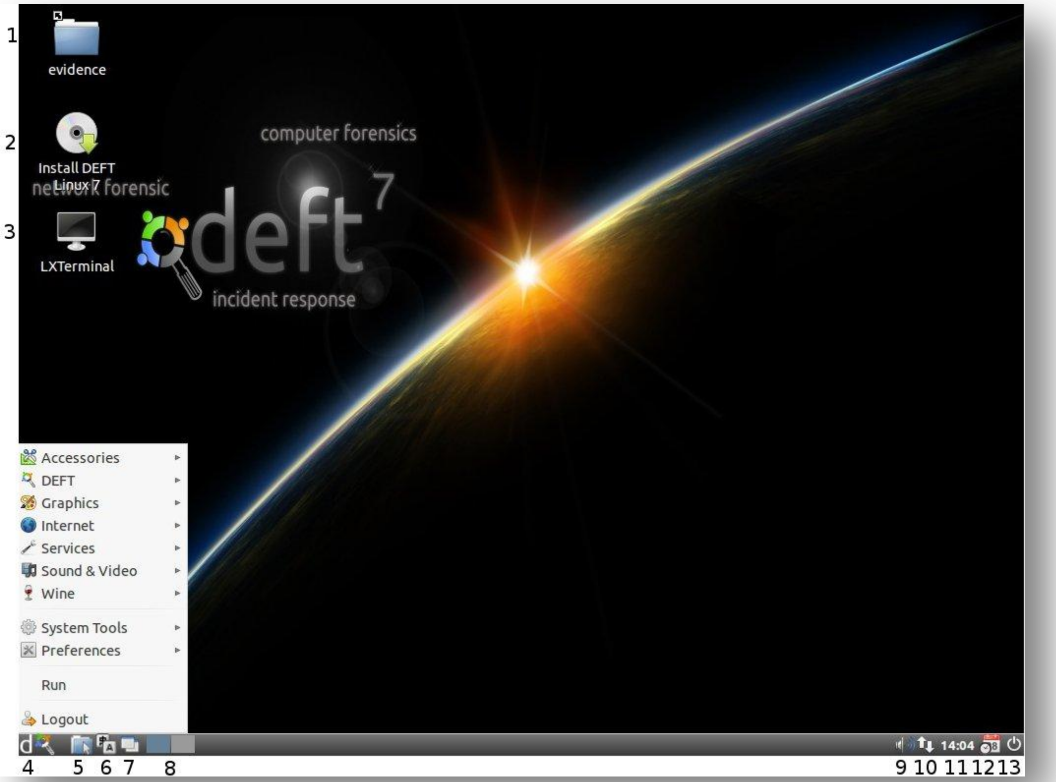
6.1 INTRODUCTION

The DEFT Linux GUI is based on the LXDE "desktop environment"[66] (Lightweight X11 Desktop Environment).The choice of the desktop manager fell on this project because to date it is one of the lightest and most efficient GUIs of the Linux world.

The use of the graphics mode is requested in cases in which programs, not developed for the use in the command line, are to be used, such as, for example, Digital Forensic Framework (DFF)[67] or Catfish.

Since version 6, native Windows applications, of which there is no as powerful equivalent for Linux, have been integrated and emulated directly by DEFT Linux using Wine software[68].

To start the graphical interface of DEFT Linux simply type *deft-gui.*



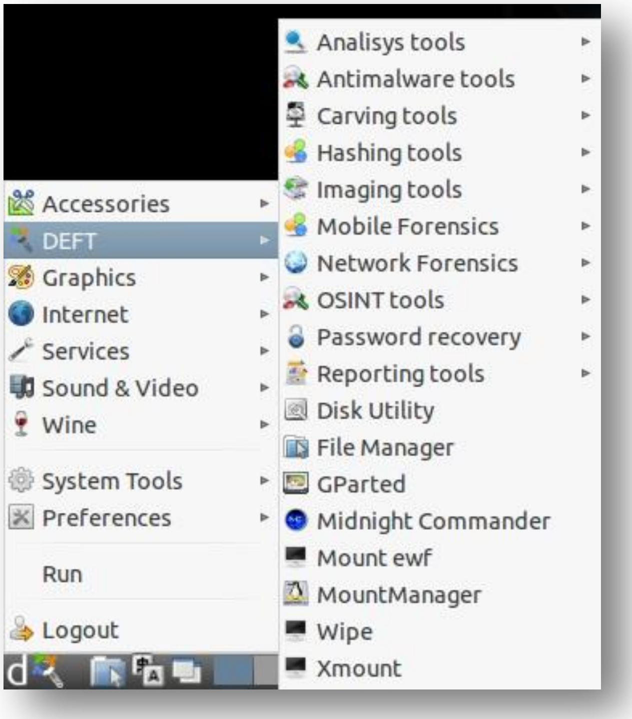
Deft: Linux GUI

[66] http://www.lxde.org
[67] http://www.digital-forensic.org/
[68] http://www.winehq.org/

You can find on the desktop the following elements:

1. A directory for the collection of evidence
2. The procedure to install DEFT Linux
3. The Terminal
4. The Application Menu
5. Pcmanfm File Manager
6. Keyboard Language Manager
7. Show Desktop button
8. Workspace switcher
9. Audio Control System
10. Network manager
11. Date and time
12. Timezone Manager
13. System shutdown and reboot button

The Applications menu has the following sections:



- **Accessories:** Archive Manager, Character Map, Disk Utility, File Manager, Calculator, Image Viewer, Leafpad, LXTerminal, Truecrypt and Xpad.
- **DEFT:** Analysis tool, Antimalware tools, Carving tools, Hashing tools, Imaging tools, Mobile forensics, Network forensics, Osint tools, Password Recovery, Reporting tools, Disk Utility, File Manager, GParted, Midnight Commander, Mount ewf, MountManager, Wipe and Xmount.
- **Graphics:** Document viewer.
- **Internet:** Firefox and Sun Java 6 Web start.
- **Services:** Apache start, Apache stop, Mysql start, MySQL stop, Samba start, Samba stop, SSH start, SSH stop, Xplico start, Xplico stop.
- **Sound & Video:** Audacious, Desktop Recorder, VLC media player and Xfburn.
- **Wine.**
- **System tools:** Gdebi package installer, GParted, Printing, Synaptic package manager, System Profiler and Benchmark, Task Manager, Time and date, update manager, Users and Groups and Windows wireless drivers.
- **Preferences:** Additional drivers, Adobe Flash Player, Customize look, Desktop session settings, Disk Utility, Keyboard and Mouse, language support, Lxkeymap, Monitor settings, Network

connections, Openbox configuration, Preferred applications, Software sources, Sun Java 6 Plugin Control Panel and Sun Java 6 Policy Tool.

6.2 MASS MEMORY MANAGEMENT

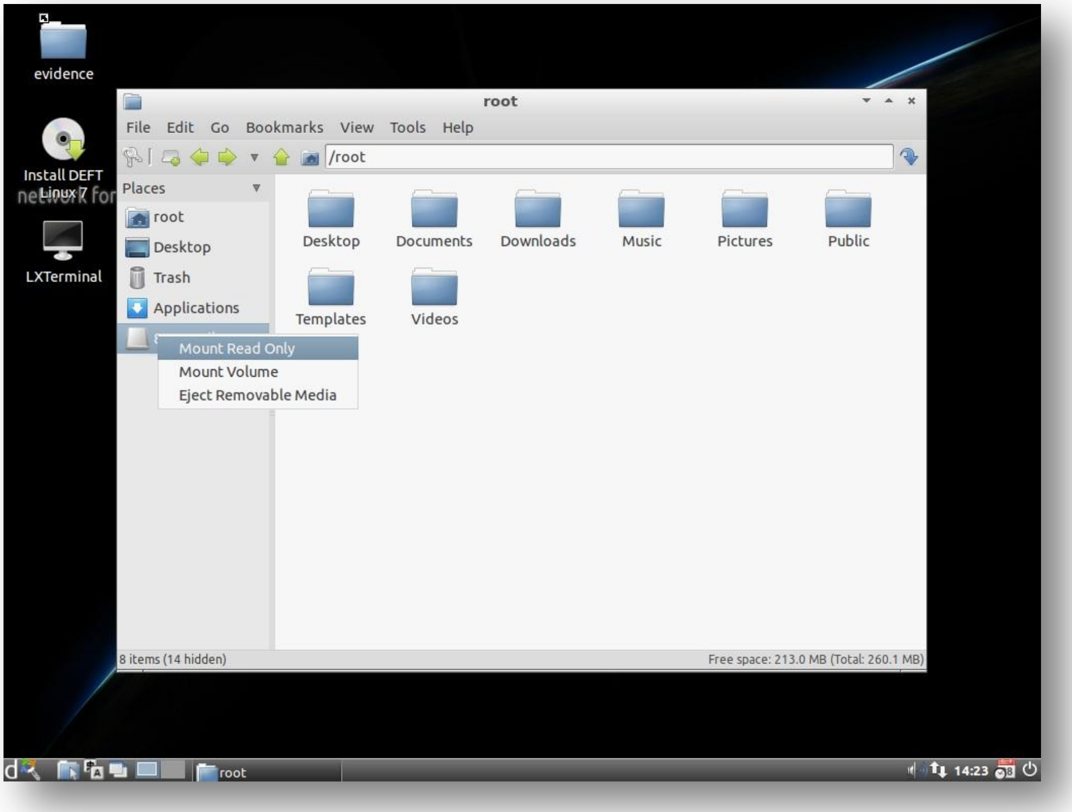
As already mentioned, the system does not perform any action with the exception of the detection of the devices connected to the system.

While using the file manager, all the mass storage devices connected to the system (internal and external) will never be mounted automatically.

Right clicking on the icon of the mass storage device, the policies for the mount will be displayed:

- **Mount Read Only:** Allows the access to the mass storage device as read-only without altering the data stored in the memory device;
- **Mount Volume:** allows the access to the mass memory device with read/write permissions;
- **Eject Volume:** allows the safe removal from the system memory.

With Mount Manager application the examiner can set the mount policies based on its operational needs.

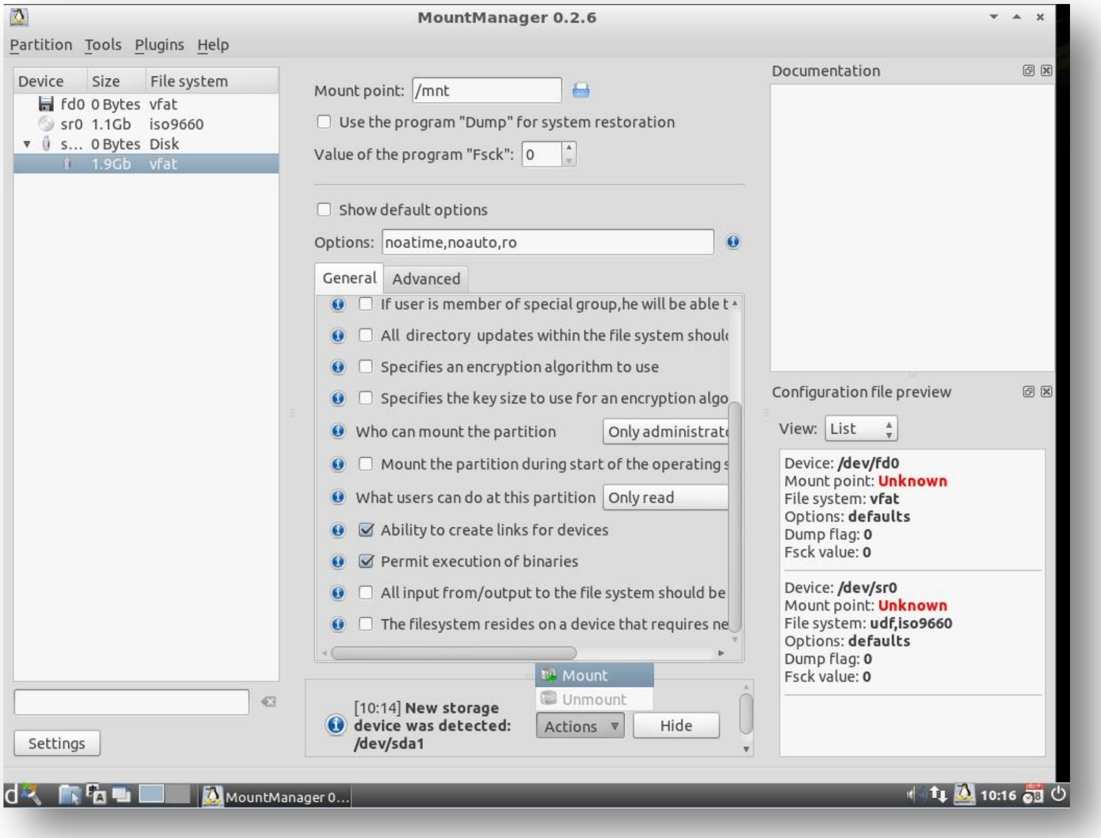


Mount activities using PcmanFMr

6.3 MOUNT MANAGER

Mount manager allows you to create advanced mount policies with just a few clicks.

In the image we quote the procedure to mount a memory storage device as RO (read only) blocking the actions that may alter the file system.



Device	Size	File system
fd0	0 Bytes	vfat
sr0	1.1Gb	iso9660
s...	0 Bytes	Disk
	1.9Gb	vfat

Mount point: /mnt

☐ Use the program "Dump" for system restoration

Value of the program "Fsck": 0

☐ Show default options

Options: noatime,noauto,ro

- ☐ If user is member of special group,he will be able t
- ☐ All directory updates within the file system shoul
- ☐ Specifies an encryption algorithm to use
- ☐ Specifies the key size to use for an encryption algo
- Who can mount the partition: Only administrat
- ☐ Mount the partition during start of the operating s
- What users can do at this partition: Only read
- ☑ Ability to create links for devices
- ☑ Permit execution of binaries
- ☐ All input from/output to the file system should be
- ☐ The filesystem resides on a device that requires ne

[10:14] **New storage device was detected: /dev/sda1**

View: List

Device: **/dev/fd0**
Mount point: **Unknown**
File system: **vfat**
Options: **defaults**
Dump flag: **0**
Fsck value: **0**

Device: **/dev/sr0**
Mount point: **Unknown**
File system: **udf,iso9660**
Options: **defaults**
Dump flag: **0**
Fsck value: **0**

Mount policy to block possible changes to the file system

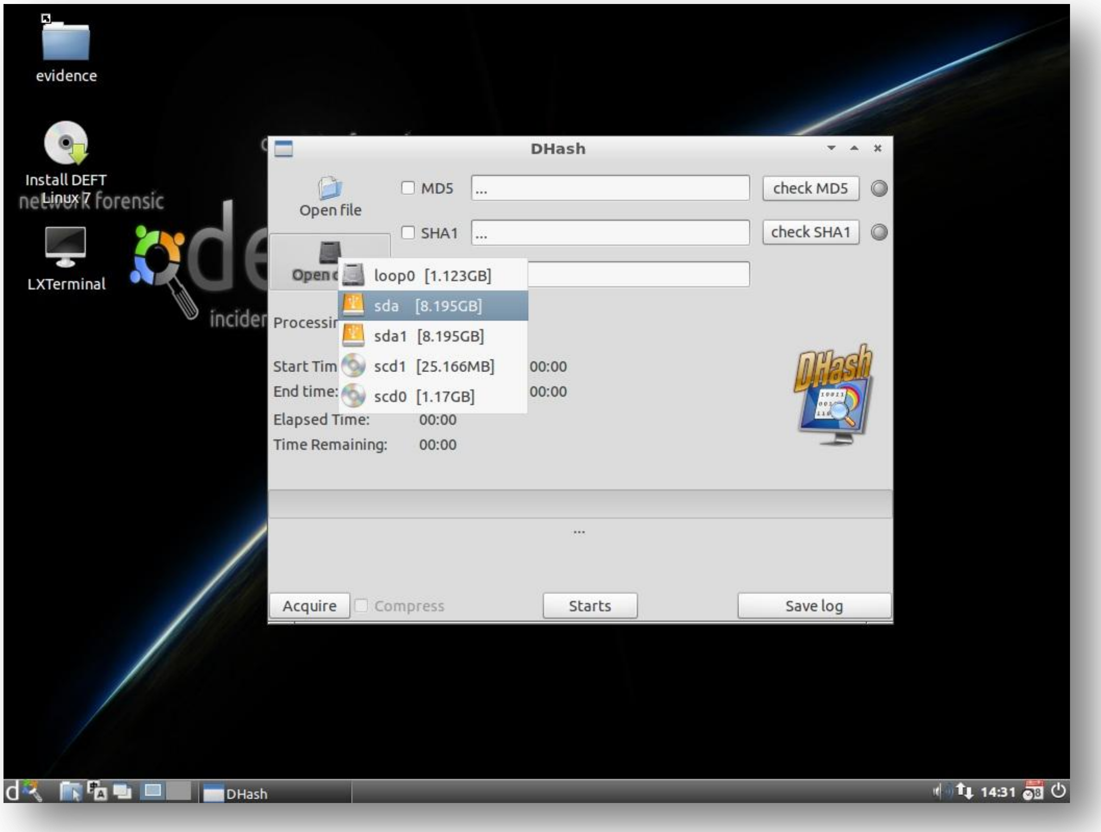
To mount you need to associate an existing directory to a partition in the memory making sure that you have set the parameters *noatime, noauto, ro, noexec,* which ensure that the mass memory is not altered during usage.Only in this way you will have access to the file system as read-only and use it without updating the *access time* inode[69] .

With Mount Manager, you can also mount files acquired in dd format and network file systems such as Samba (Windows share) and NFS.

[69] Timestamp of last access to a file system's file.

6.4 HASH CALCULATION

Dhash is the only tool in DEFT Linux dedicated to the calculation of the hash in graphical mode.



dhash: Calculating the hash value of a device

After starting the application, click *Open device* to select a mass storage device or *Open File* to select a file.

Select the type of hash to be calculated (md5, sha1 or both) and click *Starts.*

After finishing, you can save a html report with the results by clicking "save log".

6.5 MASS MEMORY ACQUISITION

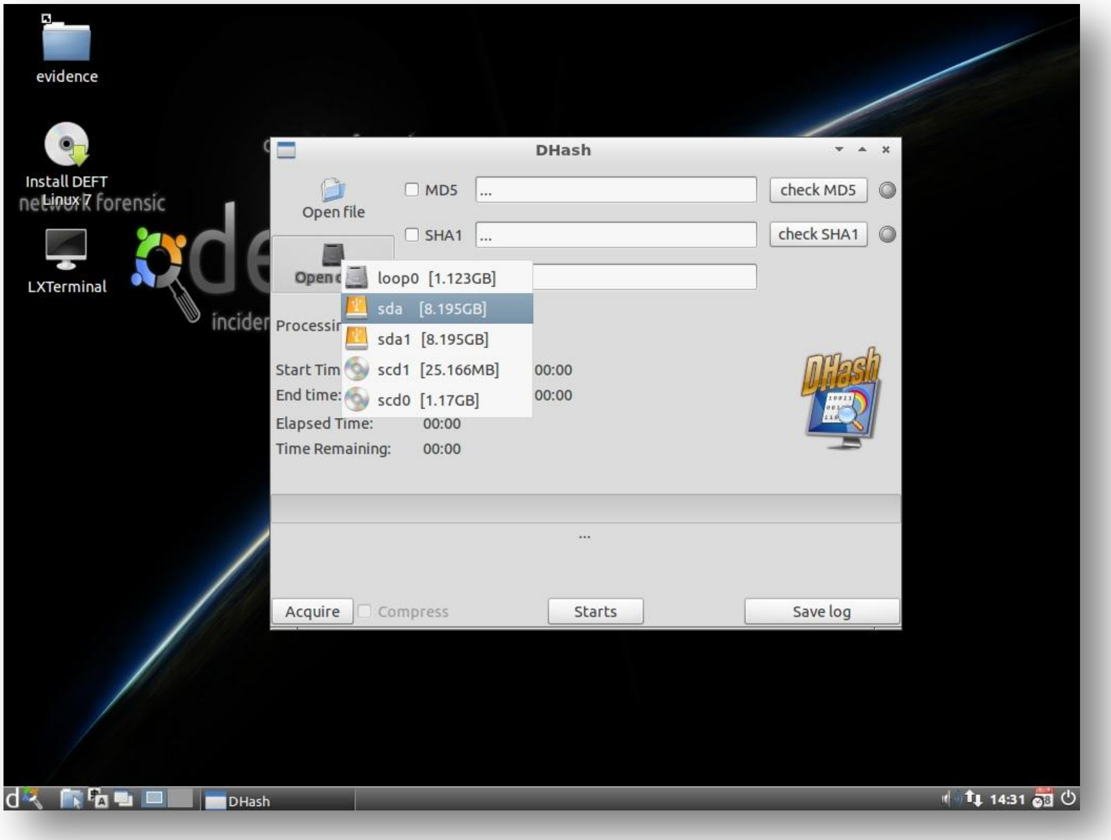
As demonstrated previously, with DEFT Linux you can acquire mass storage memories via graphical interface by using Dhash or Guymager. The former is suitable for acquisitions in the dd format, while the latter one is highly recommended for parallel acquisitions in the ewf format.

6.5.1 DHASH

On Dhash, the procedure for an acquisition is similar to the one for the hash calculation.

Select the device you want to acquire by clicking "open device" and selecting "Acquire".

You can also choose to acquire and compress to gz format by ticking the box *Compress* and/or choose whether to perform the hash calculation of one or more files .



Start Tim 00:00
End time: 00:00
Elapsed Time: 00:00
Time Remaining: 00:00

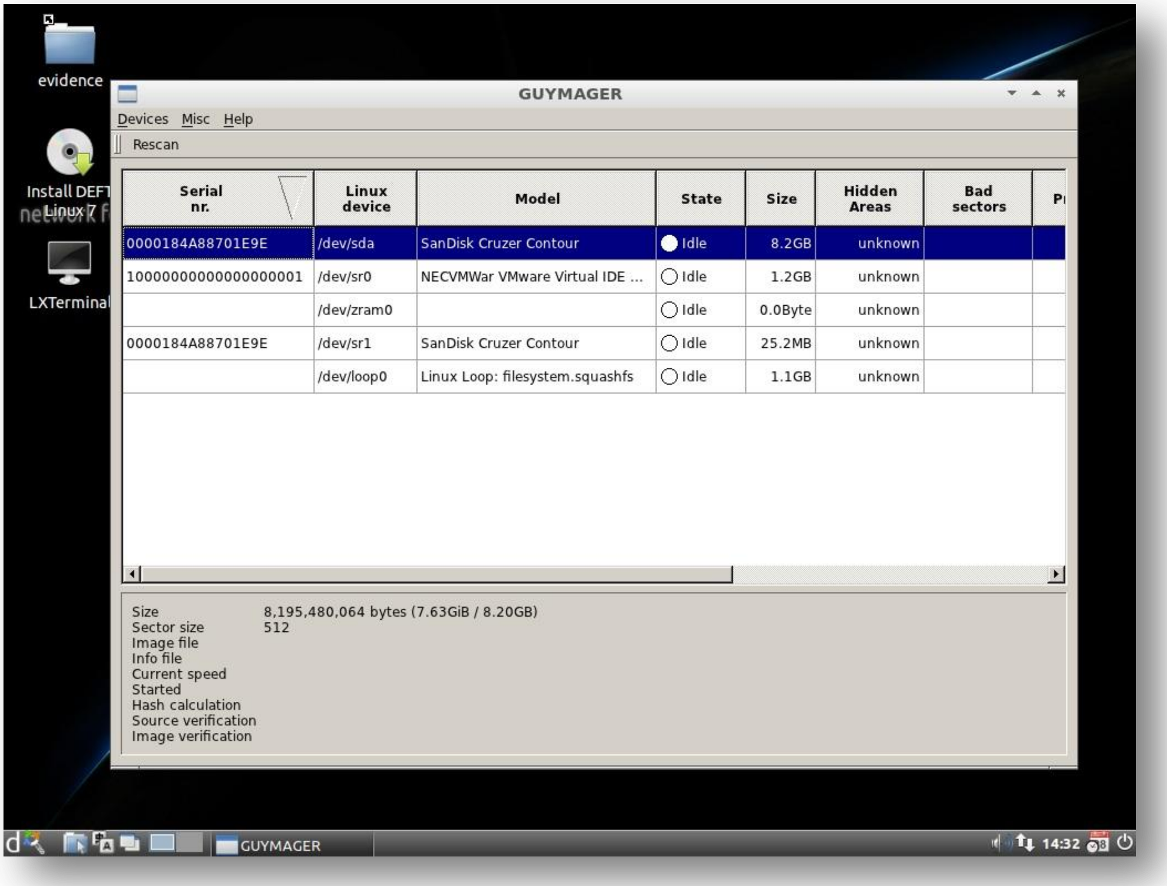
Acquisition with simultaneous calculation of md5 and sha1 hash values

Pressing the *Starts* button the acquisition starts.

At the end of all the activities, you can save a report in the html format by clicking "Save log".

6.5.2 GUYMAGER

Guymager permits a more advanced management of the acquisitions over Dhash.



Serial nr.	Linux device	Model	State	Size	Hidden Areas	Bad sectors	Pr
0000184A88701E9E	/dev/sda	SanDisk Cruzer Contour	● Idle	8.2GB	unknown		
10000000000000000001	/dev/sr0	NECVMWar VMware Virtual IDE ...	○ Idle	1.2GB	unknown		
	/dev/zram0		○ Idle	0.0Byte	unknown		
0000184A88701E9E	/dev/sr1	SanDisk Cruzer Contour	○ Idle	25.2MB	unknown		
	/dev/loop0	Linux Loop: filesystem.squashfs	○ Idle	1.1GB	unknown		

```
Size                 8,195,480,064 bytes (7.63GiB / 8.20GB)
Sector size          512
Image file
Info file
Current speed
Started
Hash calculation
Source verification
Image verification
```

Guymager: Management case for the acquisition phase

Guymager allows, in addition to the simultaneous acquisition of multiple mass storage devices, the inclusion of information such as:

- Case code;
- Evidence cataloging;
- Name of the examiner who is carrying out the operations;
- Description of the object you are acquiring.

The program supports all the major formats of acquisition (dd, aff and encase) and allows you to run the integrity check, through the md5 or sha256 hash value verification, both of the image just created and of the original device (including split images).

To start the acquiring process with *Guymager* right click on the mass memory to be cloned and select Acquire image.

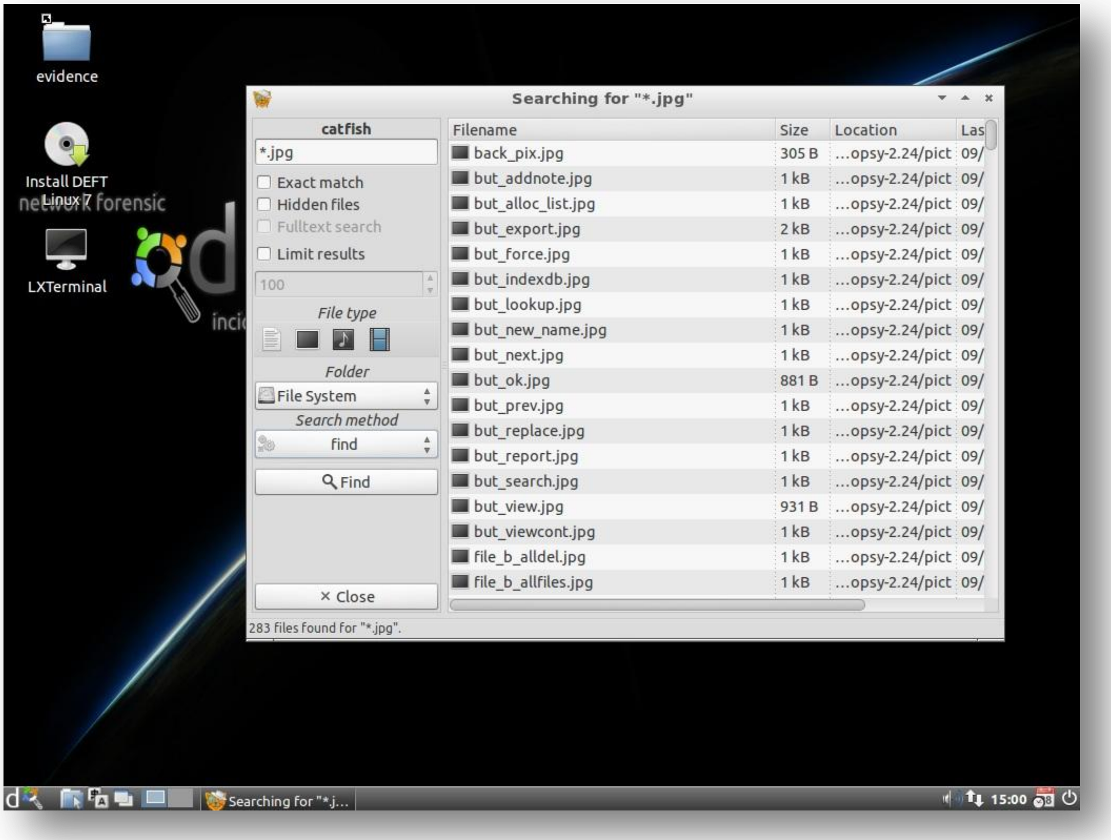
In the *Acquire Image* window you can specify several parameters of the acquisition or management of the case.

6.6 FINDING FILES AND FOLDERS

6.6.1 CATFISH

Catfish can perform the same operations that can be executed via command line commands *find and locate.*

In the example shown below, selected the memory or folder where you want to search, a search is launched for all the files with *JPG* extension by writing *. Jpg in the search field. When the search is completed, you can open the files in the list with a simple double click.



Searching for "*.jpg"

catfish

*.jpg

□ Exact match
□ Hidden files
□ Fulltext search
□ Limit results

100

File type

Folder: File System

Search method: find

Find

× Close

Filename	Size	Location	Las
back_pix.jpg	305 B	...opsy-2.24/pict	09/
but_addnote.jpg	1 kB	...opsy-2.24/pict	09/
but_alloc_list.jpg	1 kB	...opsy-2.24/pict	09/
but_export.jpg	2 kB	...opsy-2.24/pict	09/
but_force.jpg	1 kB	...opsy-2.24/pict	09/
but_indexdb.jpg	1 kB	...opsy-2.24/pict	09/
but_lookup.jpg	1 kB	...opsy-2.24/pict	09/
but_new_name.jpg	1 kB	...opsy-2.24/pict	09/
but_next.jpg	1 kB	...opsy-2.24/pict	09/
but_ok.jpg	881 B	...opsy-2.24/pict	09/
but_prev.jpg	1 kB	...opsy-2.24/pict	09/
but_replace.jpg	1 kB	...opsy-2.24/pict	09/
but_report.jpg	1 kB	...opsy-2.24/pict	09/
but_search.jpg	1 kB	...opsy-2.24/pict	09/
but_view.jpg	931 B	...opsy-2.24/pict	09/
but_viewcont.jpg	1 kB	...opsy-2.24/pict	09/
file_b_alldel.jpg	1 kB	...opsy-2.24/pict	09/
file_b_allfiles.jpg	1 kB	...opsy-2.24/pict	09/

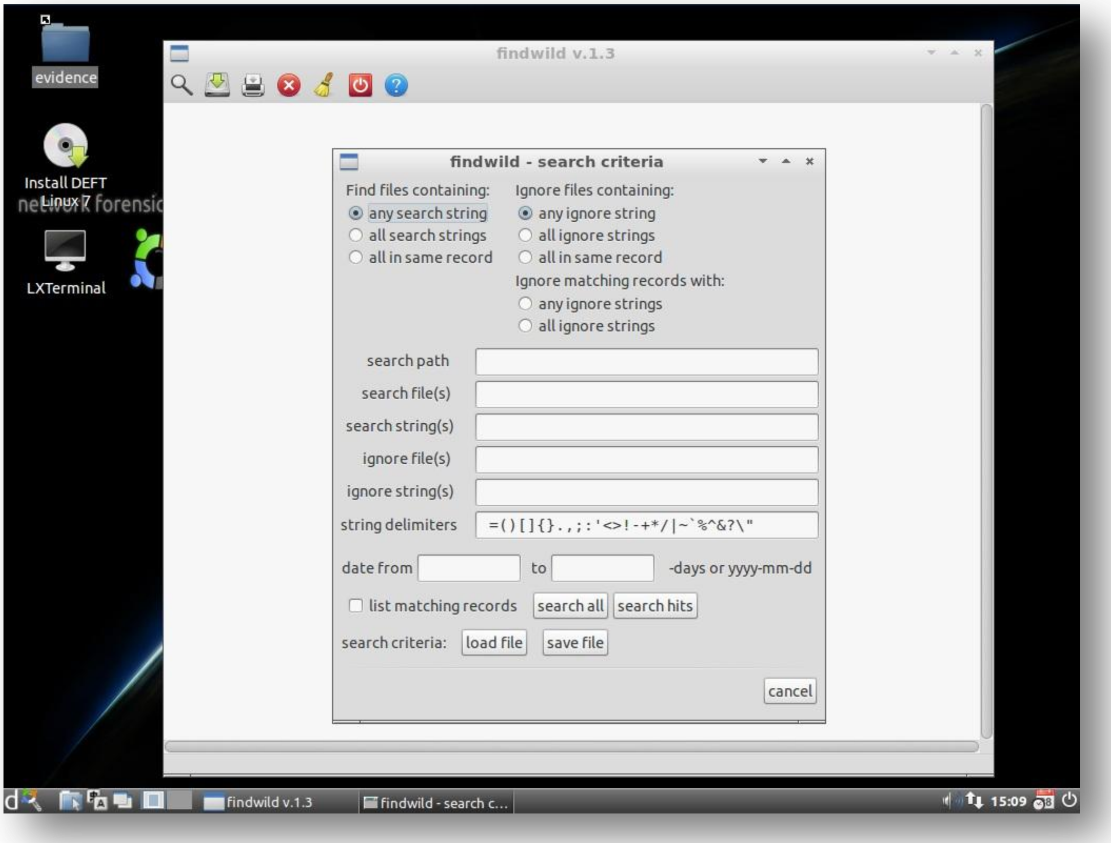
283 files found for "*.jpg".

Catfish: Finding Files

In the window more information of the files are indicated: last modification date, file location and size.

6.7 FINDWILD

Findwild is a program which allow you to search for words within files.Specifying the directory of interest and associated keywords will provide you with a list of files containing the search keys.



findwild - search criteria

Find files containing:
● any search string
○ all search strings
○ all in same record

Ignore files containing:
● any ignore string
○ all ignore strings
○ all in same record

Ignore matching records with:
○ any ignore strings
○ all ignore strings

search path
search file(s)
search string(s)
ignore file(s)
ignore string(s)
string delimiters =()[]{}.,;:'<>!-+*/|~`%^&?\"

date from to -days or yyyy-mm-dd

□ list matching records [search all] [search hits]

search criteria: [load file] [save file]

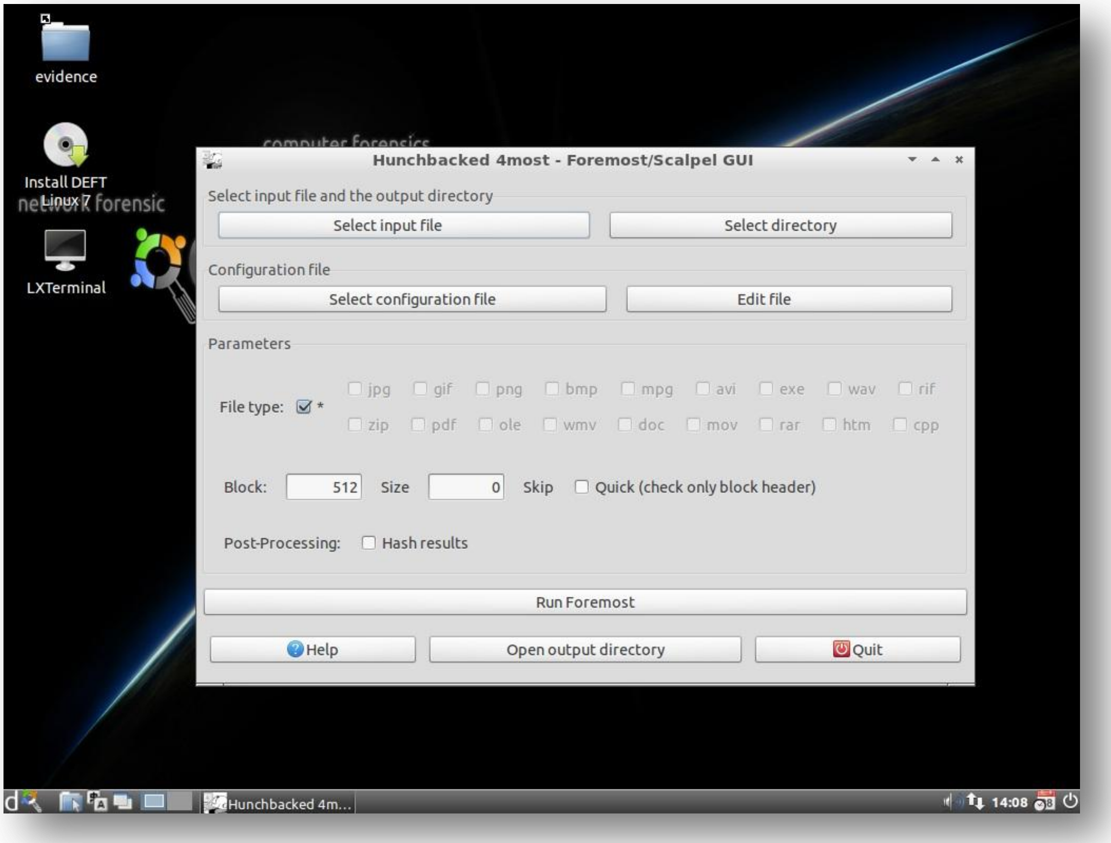
[cancel]

Findwild: Searching for content

6.8 GUI FILES CARVING

Hunchbacked 4most (H4m), available in Italian and English, is a graphical interface for managing the main functions of *foremost and scalpel.*

Through *H4m,* once you choose the program to be used as a file carver, you can run the carving with few simple clicks.



Select input file and the output directory

Configuration file

Parameters

File type: ☑ *

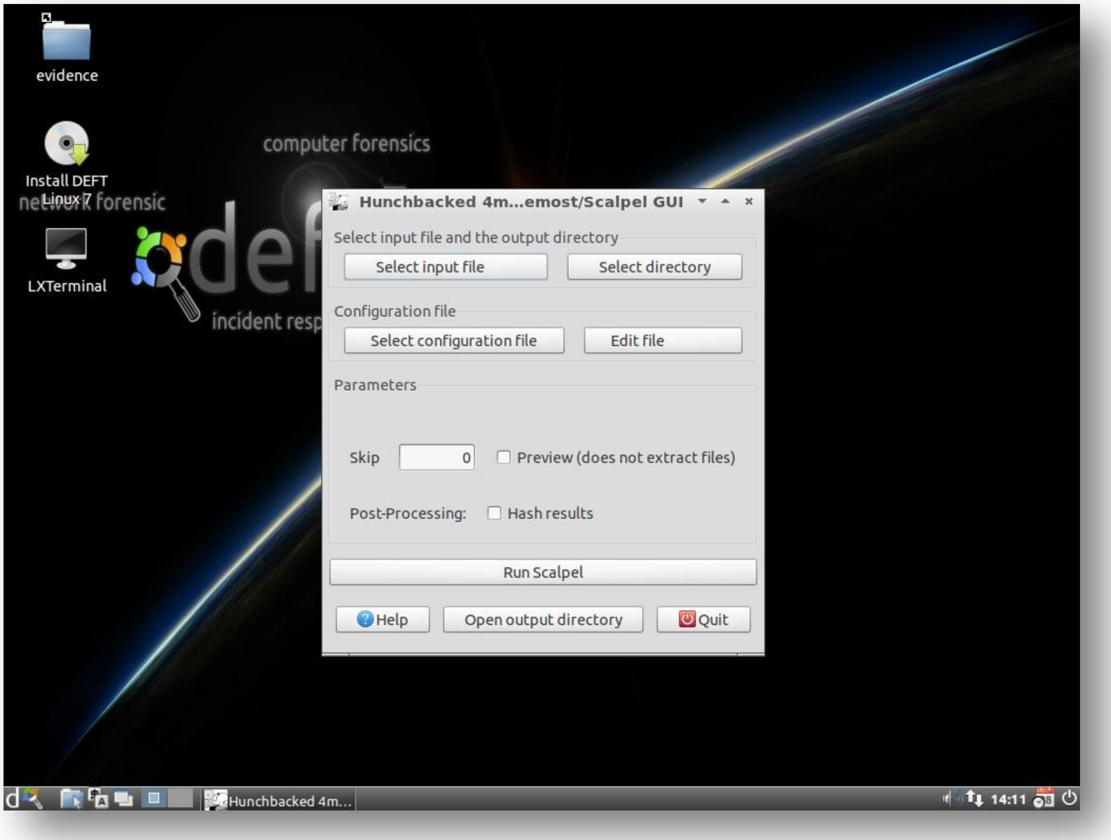
□ jpg □ gif □ png □ bmp □ mpg □ avi □ exe □ wav □ rif
□ zip □ pdf □ ole □ wmv □ doc □ mov □ rar □ htm □ cpp

Block: 512 Size 0 Skip □ Quick (check only block header)

Post-Processing: □ Hash results

Hunchbacked 4most: File Carving with Foremost

H4m, once you indicated the file or device in which to search, and the folder where to store the recovered files, searches and saves all the files with header and footer specified by the examiner.



Skip 0

□ Preview (does not extract files)

Post-Processing: □ Hash results

Hunchbacked 4most: File Carving with Scalpel

In addition to the traditional file formats supported by Foremost and Scalpel, you can customize your search by indicating a new configuration file containing header and footer of interest.

6.9 MANAGING A CASE WITH AUTOPSY

The Autopsy Forensic Browser is a graphical interface for managing the command line digital investigation tools in The Sleuth Kit[70].

It is primarily used for the management of cases in which analysis for mass storage devices is required .

Autopsy allows to:

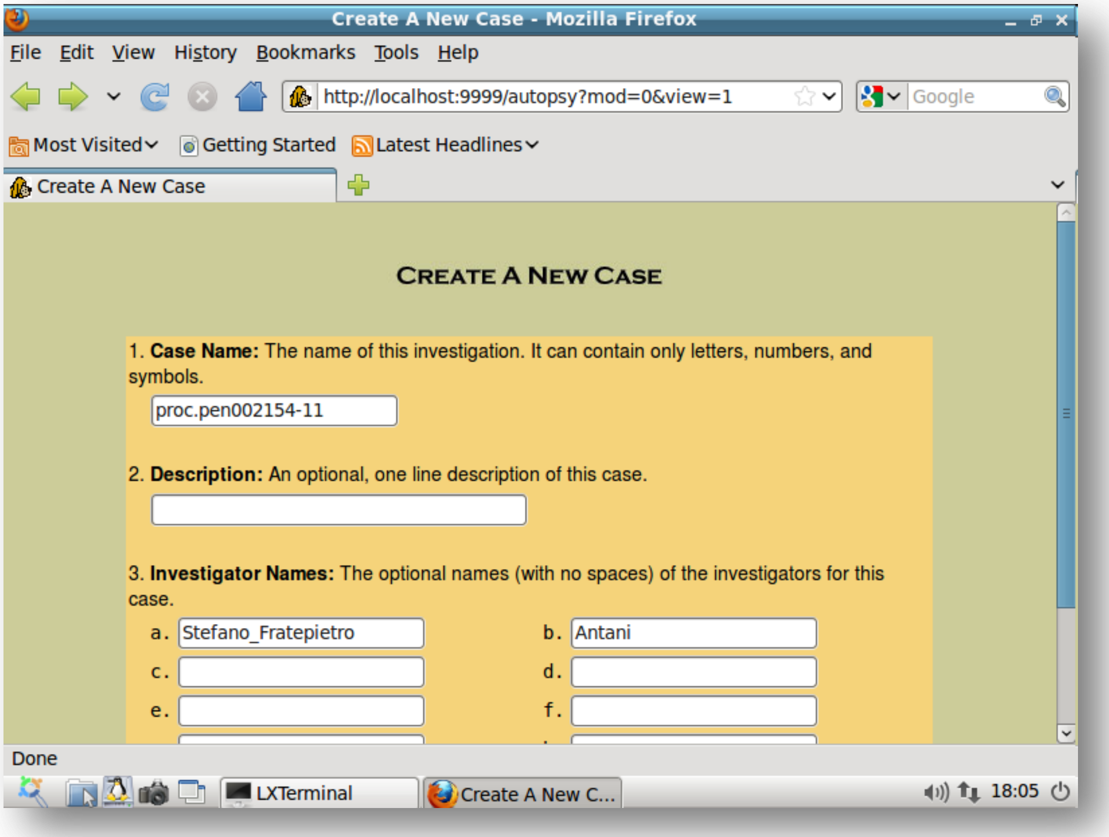
- directly use the device or the acquisitions in the dd format, aff and encase;
- view information about the file system type;
- analyze and identify the contents of files and directories and their time references;
- recover deleted files;

[70] http://www.sleuthkit.org/

- manage a database of hash values of the files of the case under analysis;
- create and analyze timelines;
- search your files by keyword;
- analyze metadata;
- create reports of findings;
- create a case.

Once you started *Autopsy* from the Disk Forensic section, it will request that the examiner specify whether he intends to create a new case or open an existing one.

In this example you click *new* to create a test case and insert the data in your possession for the cataloging, such as name, description and names of examiners:


Create A New Case - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=1
Google
Most Visited
Getting Started
Latest Headlines
Create A New Case
Done
LXTerminal
Create A New C...
18:05

CREATE A NEW CASE

1. **Case Name:** The name of this investigation. It can contain only letters, numbers, and symbols.

proc.pen002154-11

2. **Description:** An optional, one line description of this case.

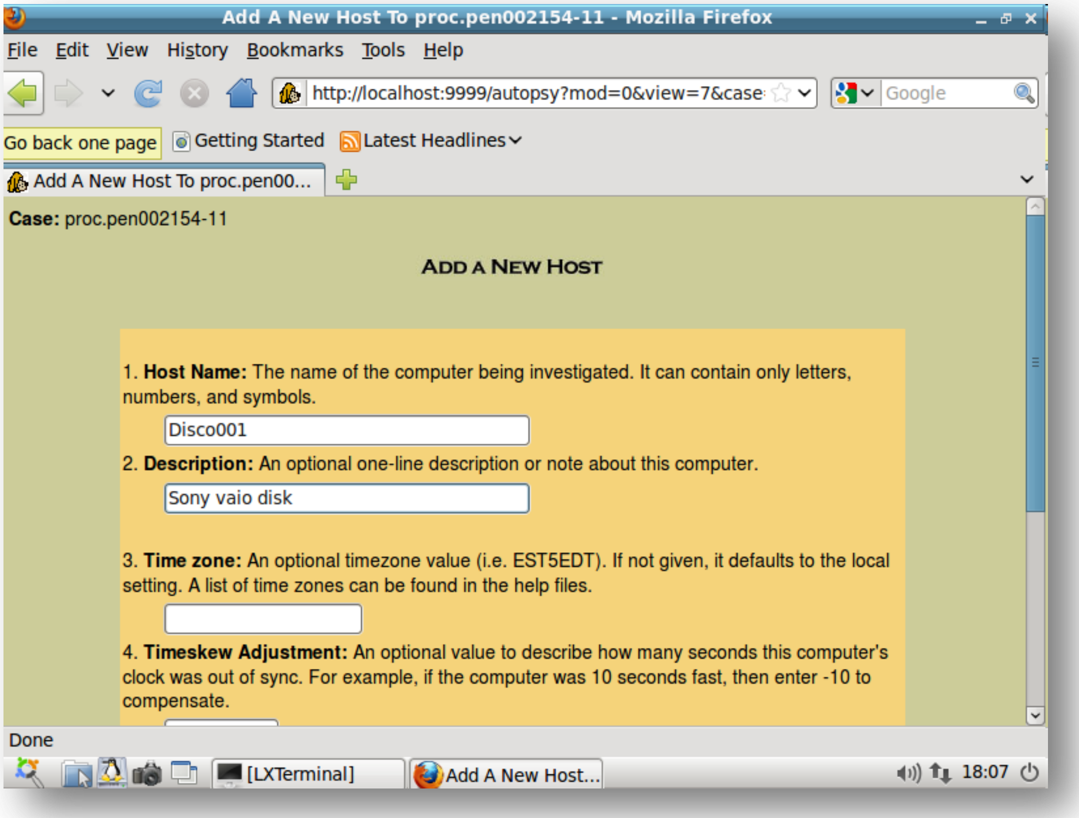
3. **Investigator Names:** The optional names (with no spaces) of the investigators for this case.

a. Stefano_Fratepietro b. Antani
c. d.
e. f.

Creation of a new case

Once you have confirmed your details, in */root/evidence/caseName* a directory containing all the case data is created.

In a case one or more objects (standing either for the members either for the systems) can be added by clicking *add host* inside the case and by entering the required data:


Add A New Host To proc.pen002154-11 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=7&case
Google
Go back one page
Getting Started
Latest Headlines
Add A New Host To proc.pen00...
Done
[LXTerminal]
Add A New Host...
18:07

Case: proc.pen002154-11

ADD A NEW HOST

1. **Host Name:** The name of the computer being investigated. It can contain only letters, numbers, and symbols.

Disco001

2. **Description:** An optional one-line description or note about this computer.

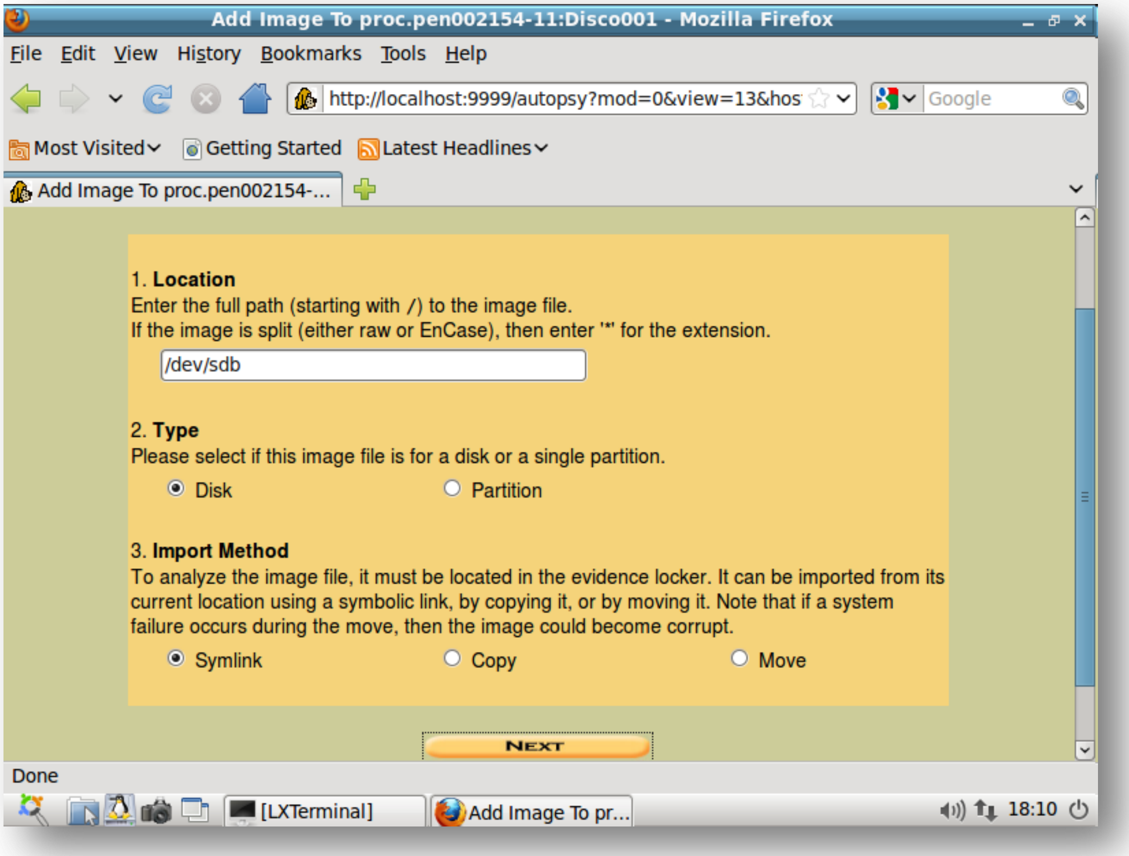
Sony vaio disk

3. **Time zone:** An optional timezone value (i.e. EST5EDT). If not given, it defaults to the local setting. A list of time zones can be found in the help files.

4. **Timeskew Adjustment:** An optional value to describe how many seconds this computer's clock was out of sync. For example, if the computer was 10 seconds fast, then enter -10 to compensate.

Adding case's Hosts

One or more mass storage devices can be added to each object: just click *add image file*, type in the *location* field either the direct link to a mass storage device (eg /dev/sdx) or the path containing the acquired file (eg: /media/forensic/disco001.dd) and specify whether the memory you are adding is a partition or an entire mass storage; concerning the import method, for ease of use is strongly recommended to leave the default *symlinks.*


Add Image To proc.pen002154-11:Disco001 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=13&hos
Google
Most Visited
Getting Started
Latest Headlines
Add Image To proc.pen002154-...
Next
Done
[LXTerminal]
Add Image To pr...
18:10

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.
/dev/sdb

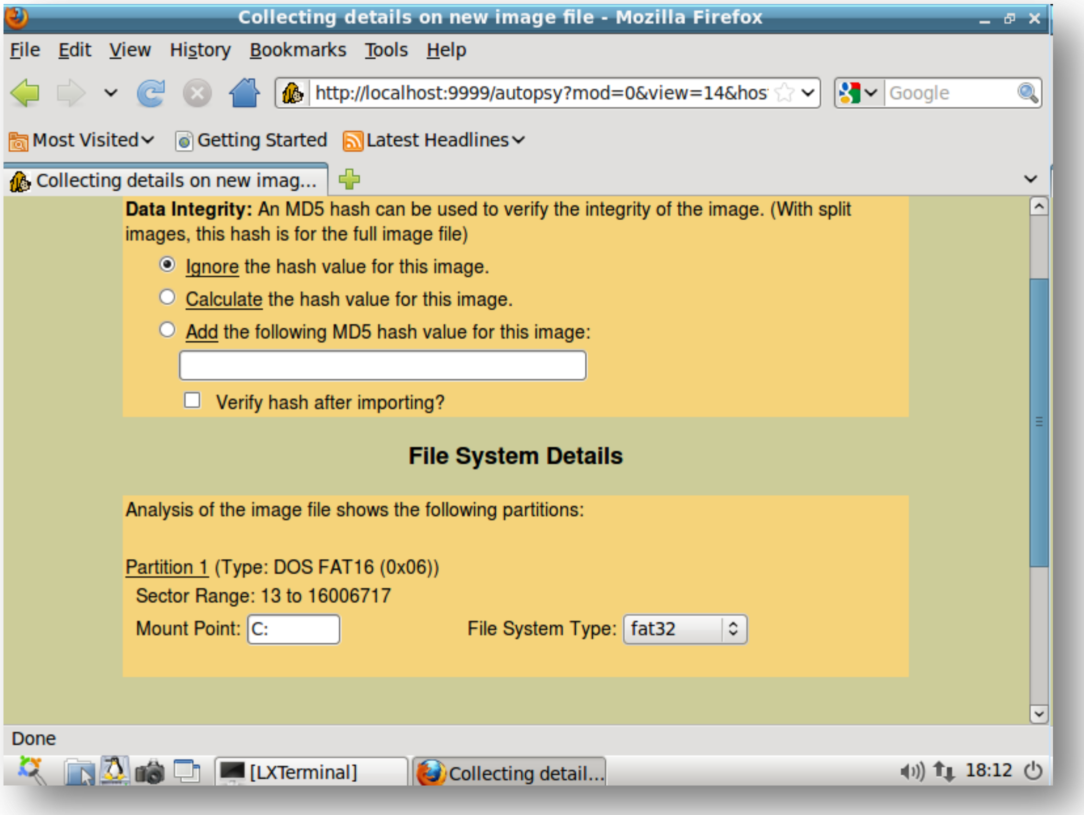
2. **Type**
Please select if this image file is for a disk or a single partition.
● Disk ○ Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
● Symlink ○ Copy ○ Move

Adding a mass memory to the object

After adding the memory, it will be asked whether to calculate, or enter manually if already calculated, the md5 hash value[71] and specify the symbolic name of the partition and its file system.

[71] Autopsy supports only the MD5 hash algorithm.


Collecting details on new image file - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=14&hos
Google
Most Visited
Getting Started
Latest Headlines
Collecting details on new imag...
Done
[LXTerminal]
Collecting detail...
18:12

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

● Ignore the hash value for this image.

○ Calculate the hash value for this image.

○ Add the following MD5 hash value for this image:

□ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

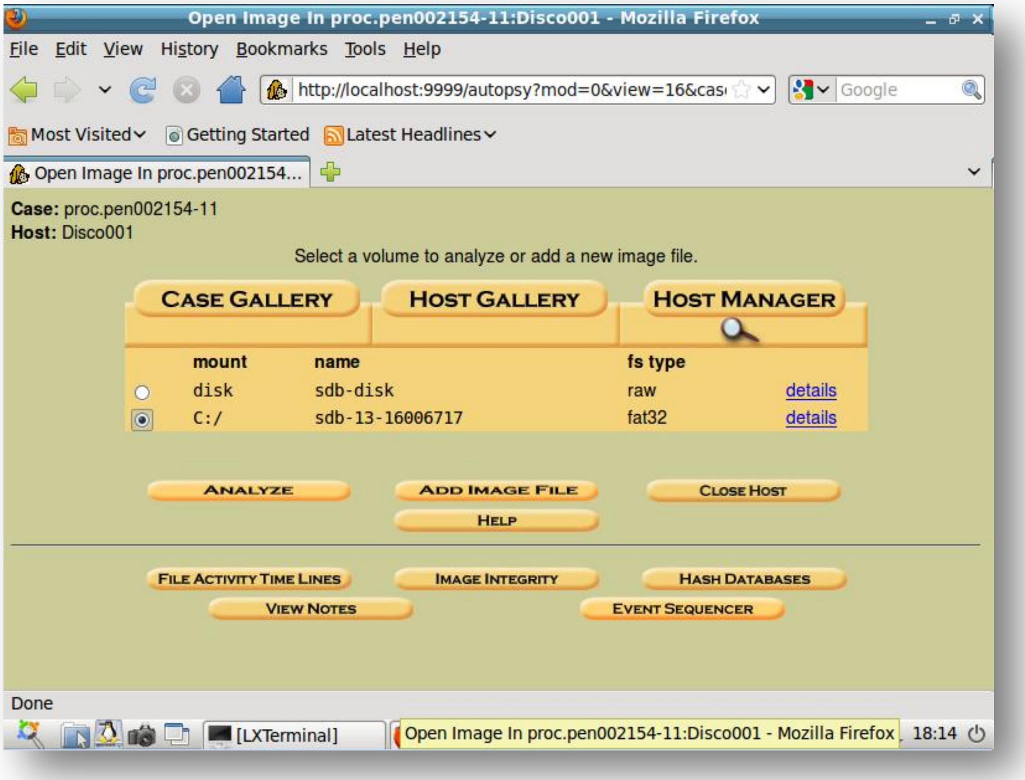
Partition 1 (Type: DOS FAT16 (0x06))

Sector Range: 13 to 16006717

Mount Point: C: File System Type: fat32

Managing the hash value and the type of file system and partitions

The creation of *Disco001* object will be completed at the end of the previous operations. You can continue to add more memories to the object or begin your analysis by clicking *Analyze.*


Open Image In proc.pen002154-11:Disco001 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost:9999/autopsy?mod=0&view=16&cas
Google
Most Visited
Getting Started
Latest Headlines
Open Image In proc.pen002154...
CASE GALLERY
HOST GALLERY
HOST MANAGER
ANALYZE
ADD IMAGE FILE
CLOSE HOST
HELP
FILE ACTIVITY TIME LINES
IMAGE INTEGRITY
HASH DATABASES
VIEW NOTES
EVENT SEQUENCER
Done
[LXTerminal]
Open Image In proc.pen002154-11:Disco001 - Mozilla Firefox
18:14

Case: proc.pen002154-11
Host: Disco001

Select a volume to analyze or add a new image file.

	mount	name	fs type	
○	disk	sdb-disk	raw	details
●	C:/	sdb-13-16006717	fat32	details

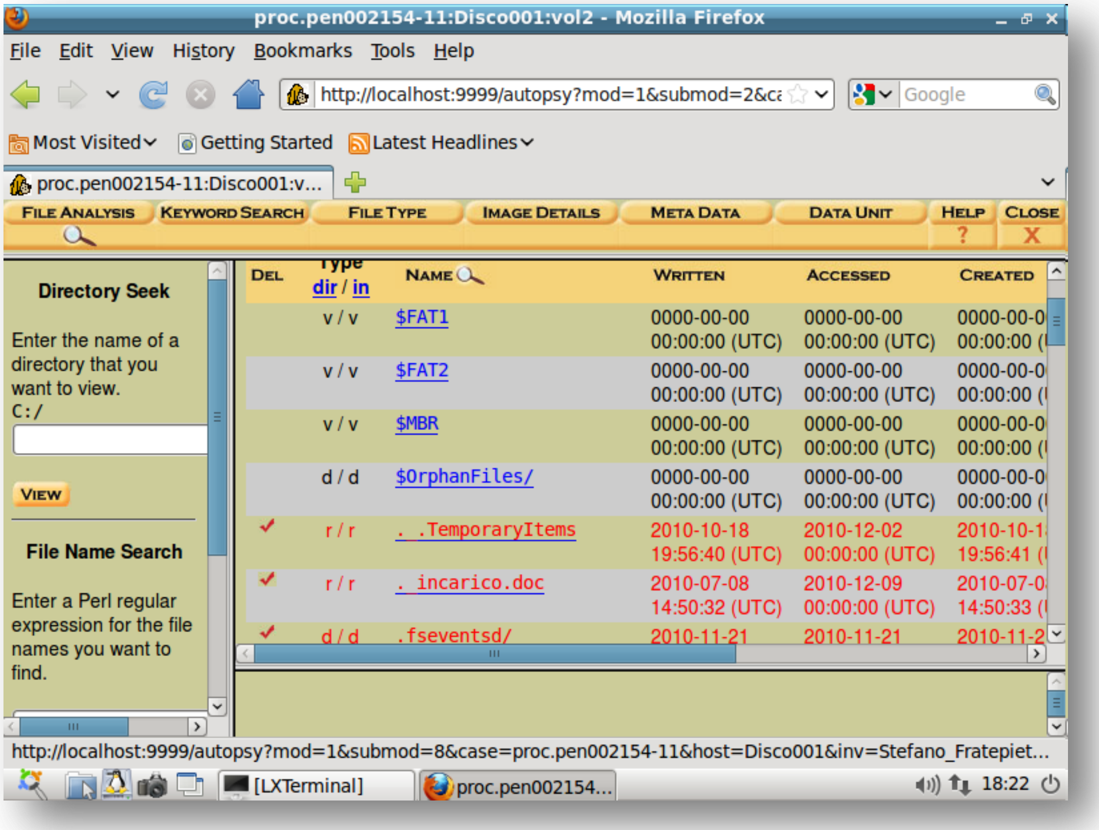
Managing "Disco001" object assigned to the case

The analysis module interface allows the examiner to display the directory tree of the partition under analysis and-once a file is selected-to have a preview of its content.

The access to the file is read only so as not to affect neither the time nor the metadata references.

In the analysis window you can see:

- The file name/directory and its path;
- The time values as creation date, last access and last modification;
- The data type;
- If the data has been deleted or not (in red if deletion of the data was requested).



http://localhost:9999/autopsy?mod=1&submod=2&ca

Directory Seek

Enter the name of a directory that you want to view.
C:/

View

File Name Search

Enter a Perl regular expression for the file names you want to find.

Del	Type dir / in	Name	Written	Accessed	Created
	v / v	$FAT1	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-0 00:00:00 (
	v / v	$FAT2	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-0 00:00:00 (
	v / v	$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-0 00:00:00 (
	d / d	$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-0 00:00:00 (
✓	r / r	_.TemporaryItems	2010-10-18 19:56:40 (UTC)	2010-12-02 00:00:00 (UTC)	2010-10-1 19:56:41 (
✓	r / r	_incarico.doc	2010-07-08 14:50:32 (UTC)	2010-12-09 00:00:00 (UTC)	2010-07-0 14:50:33 (
✓	d / d	.fseventsd/	2010-11-21	2010-11-21	2010-11-2

http://localhost:9999/autopsy?mod=1&submod=8&case=proc.pen002154-11&host=Disco001&inv=Stefano_Fratepiet...

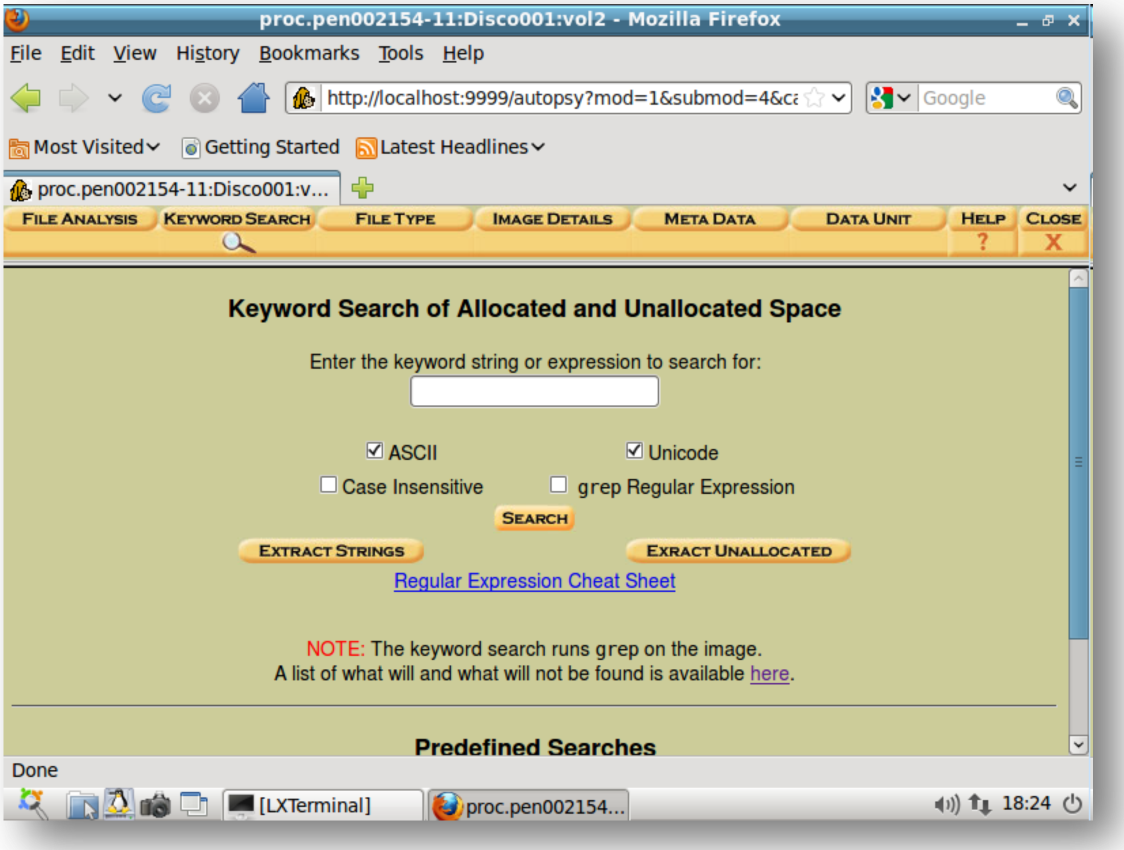
Autopsy: File Analysis

Another interesting feature is the keyword search. This feature allows you to perform searches using the *grep* command and runs on the entire file system tree, including unallocated space.

This operation may be very slow when you search patterns on storage devices containing many files or have large capacities.

In these cases we suggest you to open a "system shell" and perform your search, using grep, from the command line.

The same recommendation applies to the creation of timelines.



Keyword Search of Allocated and Unallocated Space

Enter the keyword string or expression to search for:

☑ ASCII ☑ Unicode

□ Case Insensitive □ grep Regular Expression

NOTE: The keyword search runs grep on the image.
A list of what will and what will not be found is available here.

Predefined Searches

Finding files by topic

6.10 XPLICO

DEFT supported the Xplico project evolution since the earliest releases[72].

The use of Xplico is very simple: given as input a pcap file[73] containing a dump of IP network traffic, the program is able to reconstruct the contents of any data passed at that time in the IP network, making them available and accessible through a convenient web interface.

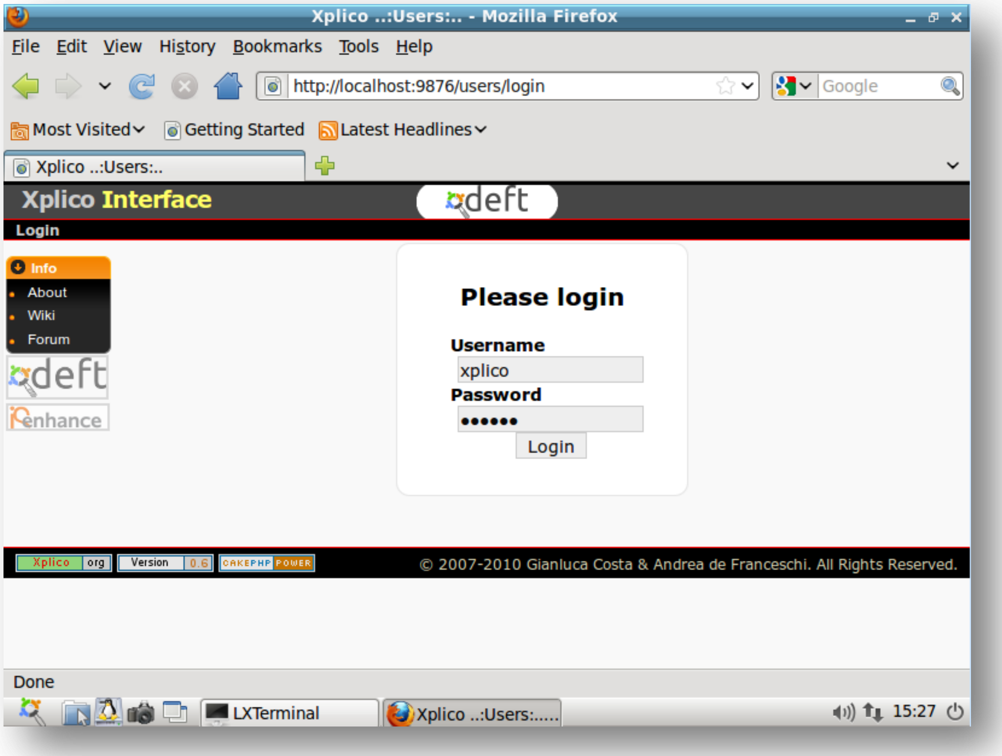
Since DEFT 7th release, Xplico is managed as a service. Therefore, in order to run the application, you must start the following services in sequence:

1. Apache web server;
2. Xplico.

The start of the services mentioned above can be performed by DEFT > menu *services* , or by using the command line.

Once the services started, you can launch Xplico from the Network Forensics menu.

6.10.1 CREATION OF A CASE



http://localhost:9876/users/login

Username
xplico

Password
••••••

[72] The tool, available at this address http://www.xplico.org/ , is right now one of the most powerful open source Network Forensic Tool.

[73] This data file contains packets captured by the programs "packet sniffing".They are usually packets that were recorded during a network transmission.

Run Xplico from the Network Forensics section of DEFT menu and type the following login information to gain access to the case manager:

user: xplico

password: xplico

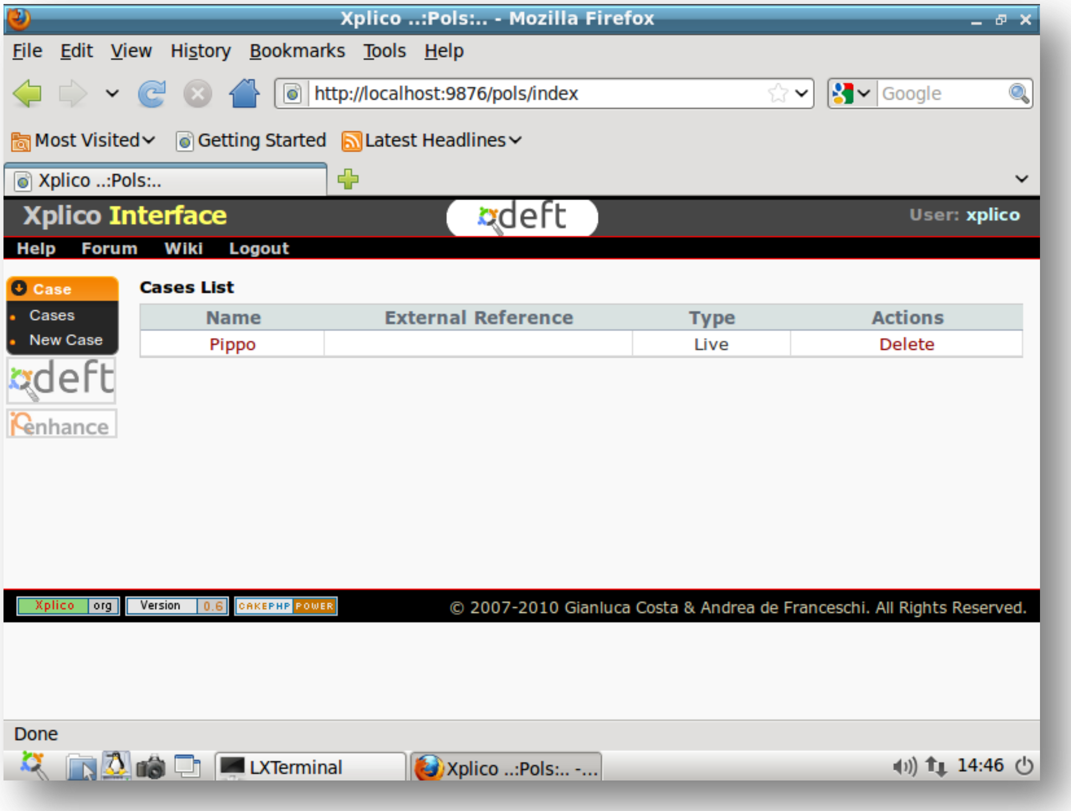
This will log you in as a default user that can only create and manage the cases but not change the settings of the application.

If you want to customize the control panel settings, create new users, etc., you must login with administrator credentials:

user: admin

password: xplico

In the following example, we have created a new case called Foo where all the traffic that in that moment is passed through the eth0 interface of our location, then acquired and analyzed.



Cases List

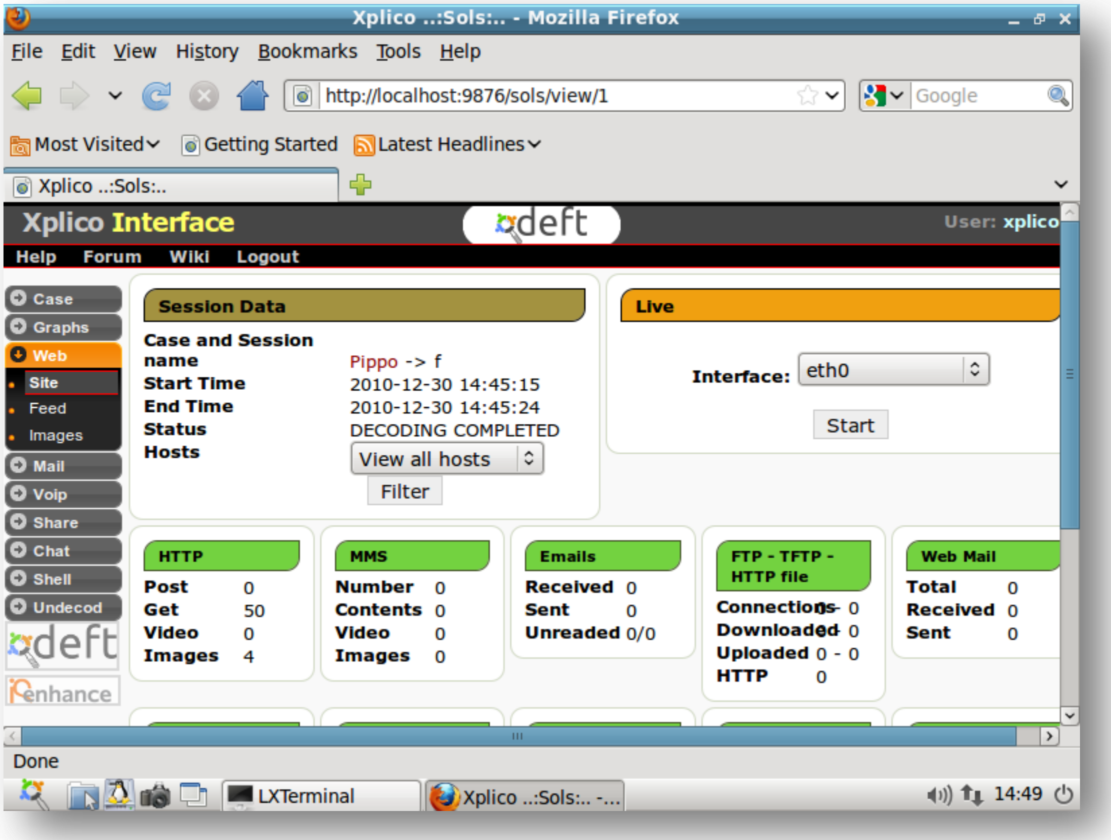
Name	External Reference	Type	Actions
Pippo		Live	Delete

© 2007-2010 Gianluca Costa & Andrea de Franceschi. All Rights Reserved.

Xplico: case manager

At the end of acquisition phase, Xplico have already decode and reconstruct all supported data type, as:

- http
- dns
- web mail
- smtp
- pop3
- imap
- sip
- telnet
- ftp
- tftp
- rtp
- pjl
- facebook chat
- msn
- irc



Case and Session name: Pippo -> f
Start Time: 2010-12-30 14:45:15
End Time: 2010-12-30 14:45:24
Status: DECODING COMPLETED
Hosts: View all hosts

HTTP
Post 0
Get 50
Video 0
Images 4

MMS
Number 0
Contents 0
Video 0
Images 0

Emails
Received 0
Sent 0
Unreaded 0/0

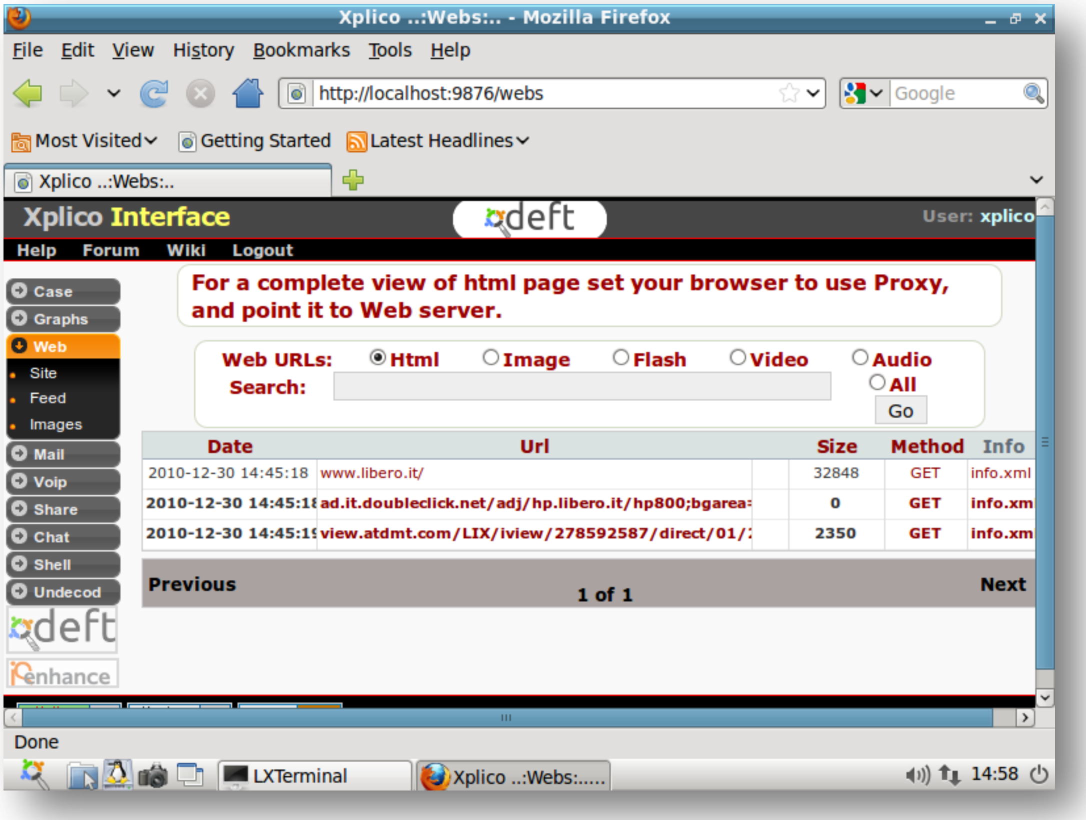
FTP - TFTP - HTTP file
Connections 0
Downloaded 0
Uploaded 0 - 0
HTTP 0

Web Mail
Total 0
Received 0
Sent 0

Report of the reconstructed data

In the previous example, we visited the "http://www.libero.it" site requested by the user.

The list containing the reconstructions of all the Web sites and all contents is displayed under the section *site* of the web menu.



For a complete view of html page set your browser to use Proxy, and point it to Web server.

Web URLs: ● Html ○ Image ○ Flash ○ Video ○ Audio ○ All

Search:

Go

Date	Url		Size	Method	Info
2010-12-30 14:45:18	www.libero.it/		32848	GET	info.xml
2010-12-30 14:45:18	ad.it.doubleclick.net/adj/hp.libero.it/hp800;bgarea=		0	GET	info.xm
2010-12-30 14:45:19	view.atdmt.com/LIX/iview/278592587/direct/01/		2350	GET	info.xm

Previous 1 of 1 Next

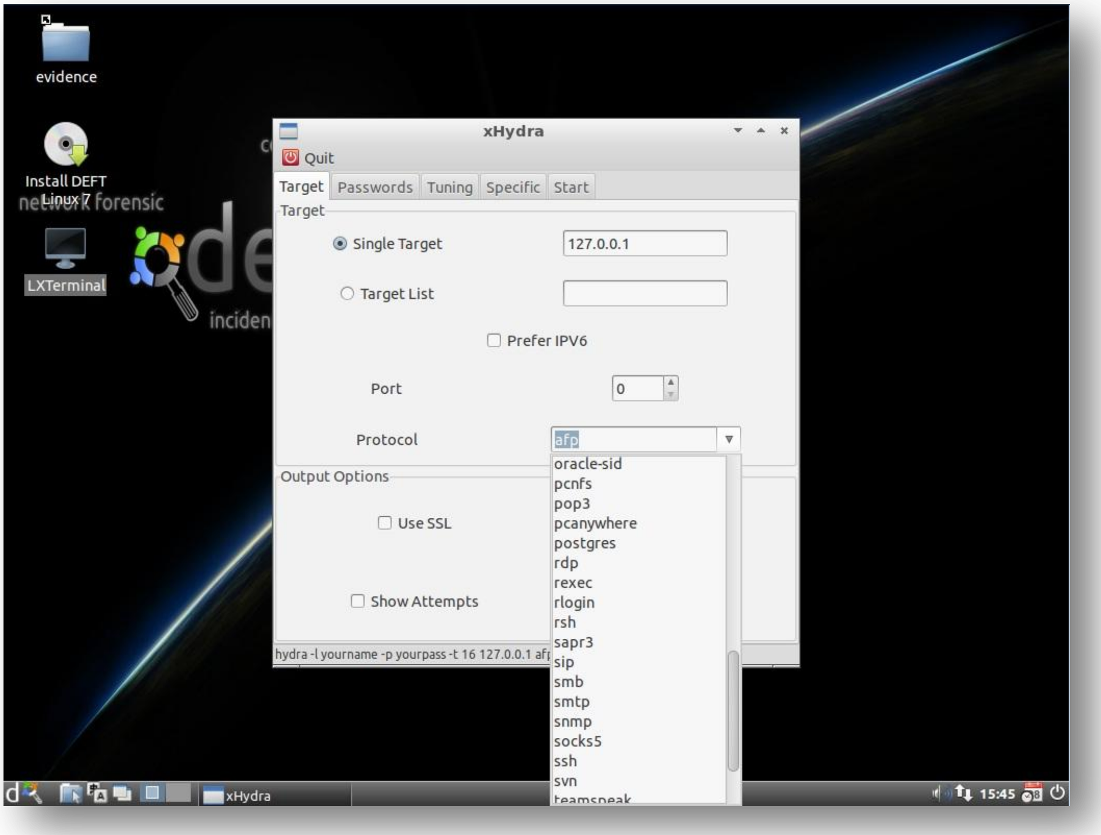
List of all the get done in the browser

It must take into account that the list of all the *get*[74] performed, includes also those that the user performs involuntarily like all the requests that are made from the web page to the various url containing advertisements or tracking scripts.

[74] Request to a web server to display a specific url.

6.11 HYDRA

Hydra is one of the most popular software used for forcing login and passwords using brute-force attack[75].



● Single Target 127.0.0.1

○ Target List

□ Prefer IPV6

Port 0

Protocol afp

□ Use SSL

□ Show Attempts

```
hydra -l yourname -p yourpass -t 16 127.0.0.1 afp
```

Hydra: protocols selection

The following list shows the protocols and applications on which you can run a brute force attack using Hydra:

[75] http://en.wikipedia.org/wiki/Brute-force_search

- *AFP*
- *Cisco AAA*
- *Cisco auth*
- *Cisco enable*
- *CVS*
- *Firebird*
- *FTP*
- *HTTP-FORM-GET*
- *HTTP-FORM-POST*
- *HTTP-GET*
- *HTTP-HEAD*
- *HTTP-PROXY*
- *HTTPS-FORM-GET*
- *HTTPS-FORM-POST*
- *HTTPS-GET*
- *HTTPS-HEAD*
- *HTTP-PROXY*
- *ICQ*
- *IMAP*
- *IRC*
- *LDAP*
- *MS-SQL*
- *MYSQL*
- *NCP*
- *NNTP*
- *Oracle Listener*
- *Oracle SID*
- *Oracle*
- *PC-Anywhere*
- *PCNFS*
- *POP3*
- *POSTGRES*
- *RDP*
- *Rexec*
- *Rlogin*
- *Rsh*
- *SAP/R3*
- *SIP*
- *SMB*
- *SMTP*
- *SMTP Enum*
- *SNMP*
- *SOCKS5*
- *SH (v1 and v2)*
- *Subversion*
- *Teamspeak (TS2)*
- *Telnet*
- *VMware-Auth*
- *VNC*
- *XMPP*

Within DEFT dictionaries to perform the activities to breach password Linux are not included.

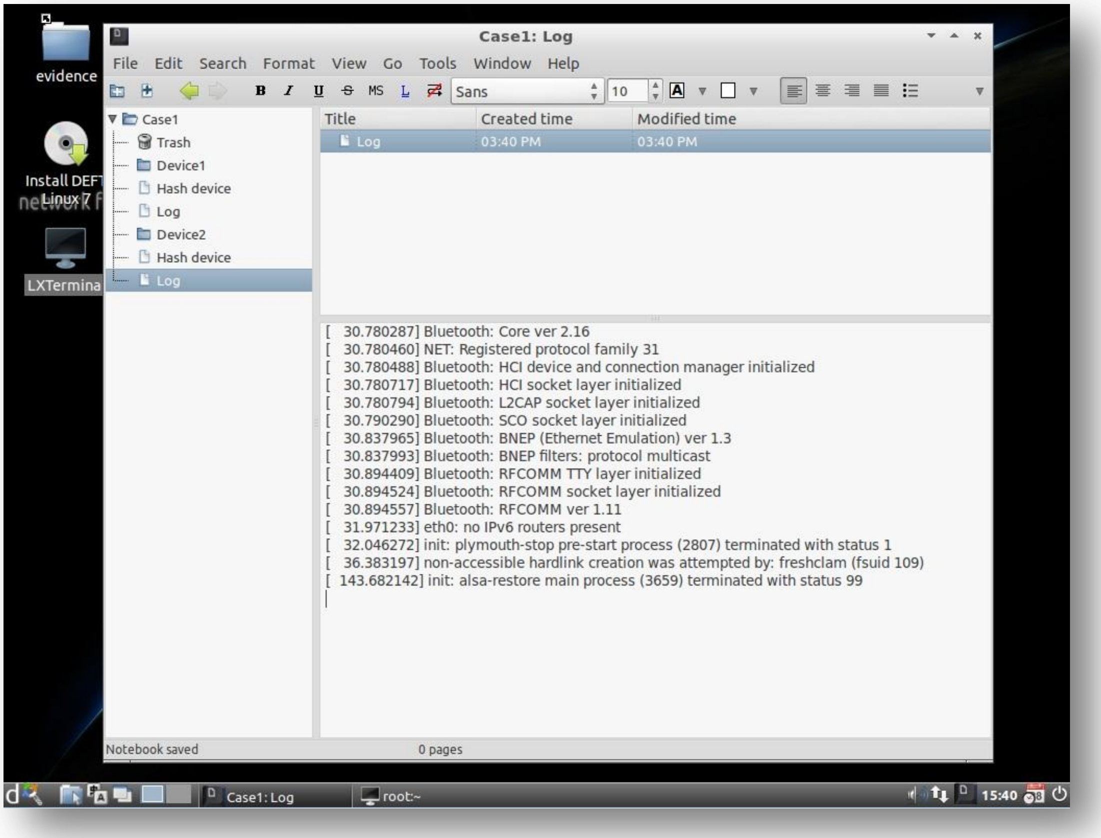
With *cupp*, you can create custom dictionaries: answering the questions the application asks, you can generate a list of keywords based on the information present in the pc protected by the credentials that you want to force[76].

[76] A wordlist can be found easily on the internet in different types: languages, collections of passwords, etc.. such as ftp://ftp.ox.ac.uk/pub/wordlists/ or http://wordlist.sourceforge.net/

6.12 KEEPNOTE

Keepnote is a software used for the collection and classification of information.

In the field of Computer Forensics it could be used for managing evidence by cataloging the mass memories and all the results of the analysis within other objects.



Title	Created time	Modified time
Log	03:40 PM	03:40 PM

```
[   30.780287] Bluetooth: Core ver 2.16
[   30.780460] NET: Registered protocol family 31
[   30.780488] Bluetooth: HCI device and connection manager initialized
[   30.780717] Bluetooth: HCI socket layer initialized
[   30.780794] Bluetooth: L2CAP socket layer initialized
[   30.790290] Bluetooth: SCO socket layer initialized
[   30.837965] Bluetooth: BNEP (Ethernet Emulation) ver 1.3
[   30.837993] Bluetooth: BNEP filters: protocol multicast
[   30.894409] Bluetooth: RFCOMM TTY layer initialized
[   30.894524] Bluetooth: RFCOMM socket layer initialized
[   30.894557] Bluetooth: RFCOMM ver 1.11
[   31.971233] eth0: no IPv6 routers present
[   32.046272] init: plymouth-stop pre-start process (2807) terminated with status 1
[   36.383197] non-accessible hardlink creation was attempted by: freshclam (fsuid 109)
[  143.682142] init: alsa-restore main process (3659) terminated with status 99
```

Notebook saved   0 pages

KeepNote: the collection of evidence

You can create a tree of objects (directories and pages), and structure it according to your needs and fit within the information of the page, such as:

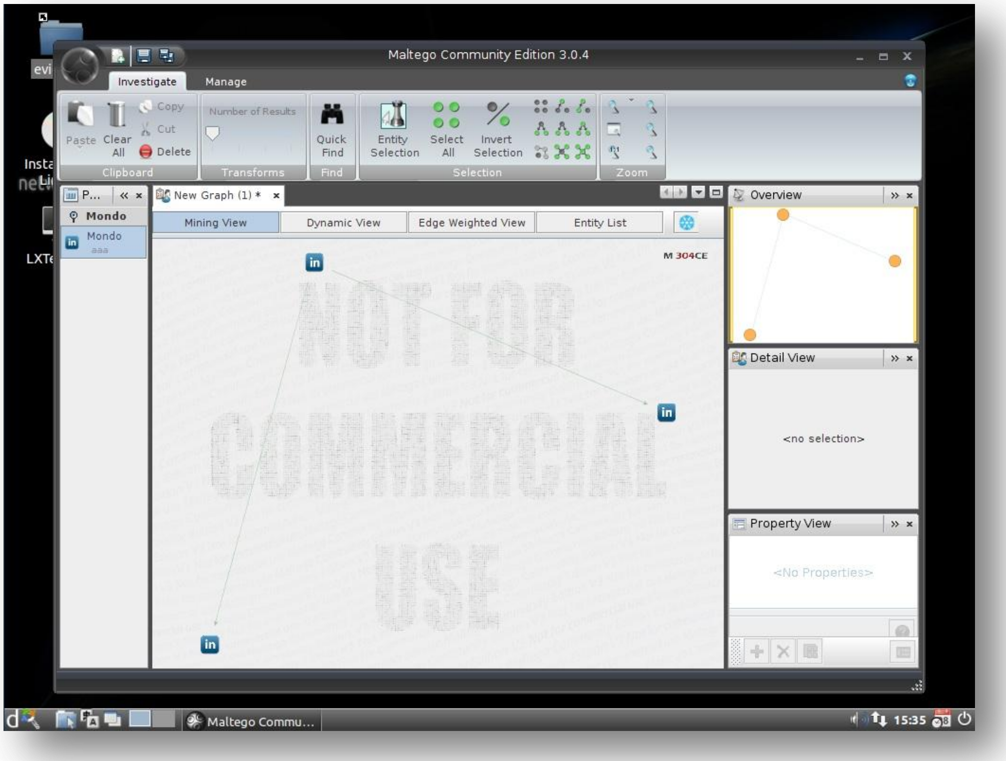
- Unformatted text;
- Html;
- Pictures;
- Files.

The information entered in the notebook created with *KeepNote* can be saved in a KeepNote file or exported to html.

6.13 MALTEGO

Maltego[77] can be used both in the Computer Forensics and Cyber Intelligence.

Maltego is multi-platform compatible, written in Java and can find and visually demonstrate connections between people, groups, companies, websites, cities, streets, e-mail, phone numbers, IP addresses, domain names, files, documents, etc..



Maltego CE, creating a diagram

As the use of this program is beyond the scope of this document, its functioning is not discussed in detail.

We suggest you to refer to the exhaustive official documentation at this URL:

http://www.paterva.com/web5/documentation/userguide.php

[77] http://www.paterva.com/

CHAPTER 7: MOBILE FORENSICS

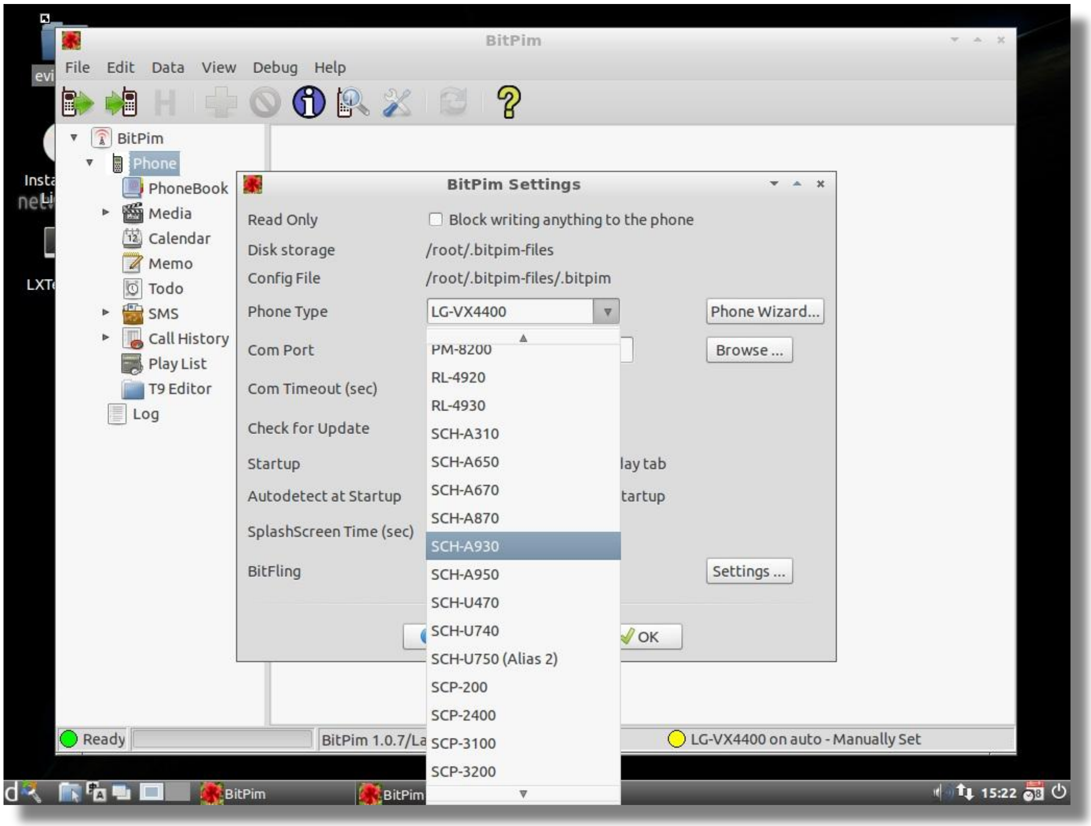
The 7th release of DEFT Linux includes some tools for the analysis of mobile devices.

It is now available *Sqlite database browser* to allow the analysis of Sqlite databases, used in most applications for Android, Iphone and Ipad.

For the mobile phones analysis, it is included:

- *Ipddump* for the analysis of backups in BlackBerry devices;
- *Iphone Analyzer* for the analysis of iPhone from version 3 to previous versions;
- *Iphone backup analyzer* for analyzing backups in iPhone devices;
- *Bitpim* that supports the following devices:

Audiovox CDM8900
LG AX-8600
LG C2000
LG G4015
LG LX570
LG PM225
LG UX-5000
LG VX-3200
LG VX-4400
LG VX-4500
LG VX-4650
LG VX-5200
LG VX-5300
LG VX-6000
LG VX-6100
LG VX-7000
LG VX-8000
LG VX-8100
LG VX-8300
LG VX-8500
LG VX-8560
LG VX-8600
LG VX-8610
LG VX-8700
LG VX-8600
LG VX-8800
LG VX-9100
LG VX-9200 LG VX-9600
LG VX-9700
LG VX-9800
LG VX-9900
LG VX-10000
LG VX-11000
Motorola E815
Motorola E815m
Motorola K1m
Motorola V325
Motorola V325M
Motorola V3c
Motorola V3cm
Motorola V3m
Motorola V3mM
Motorola V710
Motorola V710m
Samsung SCH-A870
Samsung SCH-A930
Samsung SCH-A950
Samsung SCH-U470
Samsung SCH-U740
Samsung SCH-U750
Samsung SPH-M300
Sanyo SCP-6600 (Katana)
Other Sanyo Phones
Toshiba VM-4050



BitPim Settings

Read Only ☐ Block writing anything to the phone

Disk storage /root/.bitpim-files

Config File /root/.bitpim-files/.bitpim

Phone Type LG-VX4400

PM-8200
RL-4920
RL-4930
SCH-A310
SCH-A650
SCH-A670
SCH-A870
SCH-A930
SCH-A950
SCH-U470
SCH-U740
SCH-U750 (Alias 2)
SCP-200
SCP-2400
SCP-3100
SCP-3200

Com Port

Com Timeout (sec)

Check for Update

Startup

Autodetect at Startup

SplashScreen Time (sec)

BitFling

Ready | BitPim 1.0.7/La | LG-VX4400 on auto - Manually Set

Bitpim: the list of supported phones

7.1 ANDROID

Android is an open source operating system derived from Linux which is designed for mobile devices (smartphones, tablets, netbooks).

Particularly common in Chinese low cost systems, it is present in a wide variety of devices, bypassing in terms of diffusion iOS (you can even install it on Apple iPhone[78]) and the now dated but still widely used Nokia OS[79].

The system, currently developed by the Open Handset Alliance[80] (OHA) led by Google, has seen the light for the first time in November 2007 and, for each release, it has been enriched with features that have ensured its remarkable maturity.

Right now the latest versions of the operating system are:

- 4.1.x Jellybean: widespread especially among smartphones and low-end tablets;
- 3.2 Honeycomb: dedicated to tablets, has introduced more support for larger screens, multiprocessors and graphics acceleration hardware.

[78] http://www.giardiniblog.com/guida-installare-android-su-iphone-3g [Italian]

[79] All operating systems installed on Nokia devices, created by Nokia must be considered: http://en.wikipedia.org/wiki/Nokia_OS

[80] http://www.openhandsetalliance.com/

In this chapter, for reasons of space, we will direct our attention only to version 4.1.x Jellybean

However, the OHA does not deal with the update of the operating system installed on each device, but it delegates this task to each producer, who is free to decide patches releases to correct security problems or implement new features. This market policy has indirectly caused the birth of a large number of "Cooked Rom", taken from version 2.3, customized for each model and more efficient than the default version of the device.

This dramatically affects the work of the operator who wants to perform a forensic analysis, because they do not know for sure which version of Android is installed in the device to examine[81].

The basic operating system supports the essential features of a smartphone:

- connections via GSM / EDGE, UMTS, Bluetooth, Wi-Fi, WiMAX;
- calls;
- transmission and reception of SMS and MMS;
- multilingual support;
- web browsing;
- "Dalvik virtual machine"[82];
- audio/video multimedia support;
- multitasking;
- voice commands;
- tethering.

Additional features may be available depending on the type of hardware (touchscreen, GPS, accelerometer, 3D card, etc.) or the addition of specific applications (client for social networks, all kind of management, security, games, etc.).

The hardware used in smartphones is closely related to the design features determined by the manufacturer: it varies according to the budget allocated to production and the target market.

With regard to the device memory, in most cases the operating system is installed within the flash memory, generally not removable without unsoldering of the memory itself from the motherboard. It is often supported by an expansion slot for external memory (MicroSD).

Different choices from those indicated in the previous paragraph are carried out often by smaller producers, companies usually of Chinese origin, who can design the architecture so drastically different. For example, in regard to the storage of the operating system, it it is sometimes beneficial to use MicroSD cards; they cost less and are quickly removable.

The difficulty in accessing the phone memory can vary enormously depending on the device being analyzed.

It is often necessary to use the procedures that will enable us to go and read the contents of partitions accessible only with root permissions, without having to remove the solid-state memory from the device.

[81] For example the CyanogenMod rom (www.cyanogenmod.com) or the MIUI rom (miui.nexus-lab.com) both developed around version 2.3 and 4.0.

[82] Java Virtual Machine optimized to work with reduced power consumption on devices with reduced computing power .

The main weakness of this type of procedure is that the contents of the mass storage will be altered, albeit minimally.Therefore it is desirable that the operator, when acting in criminal proceedings, requires a non-repeatable expert testimony regime for the activity of data acquisition[83].

7.2 BRIEF OVERVIEW OF GOOGLE APPLICATIONS

Although common for the operating system to have been customised by smart phone manufacturers or by the phone company, it is likely that google applications[84] are included and may constitute a primary source of information for the report.

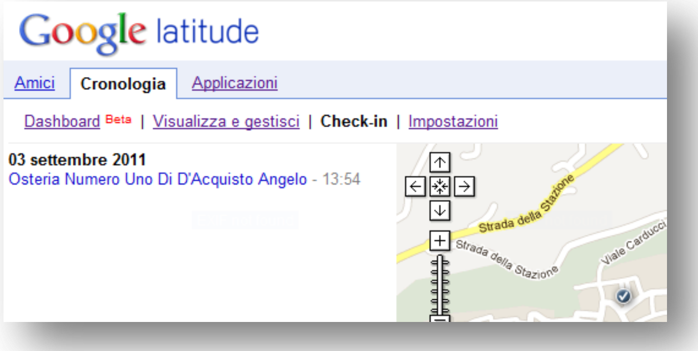
Among the different applications, the two main ones are Gmail profile and Market[85].

7.2.1 GMAIL

For the purpose of investigation, it is worth considering the deep connection between the smartphone internal management and a Google Account. Many of the internal features (contact management, calendar, google talk, google market, etc.) depend on, or can depend on, an active account on the Google systems.

Some examples:

- You must register a Google account to download/purchase applications from the Android Market;
- Contacts and calendar data can be saved automatically even in the Google profile;
- If it is installed, Google+ client offers the opportunity to upload automatically any photos taken by the internal camera in a private album of a Google+ profile, not necessarily relevant to your default Google account[86];
- The function Latitude, in the Maps application, it is supported by the registered Google Profile and stores the phone location, checks in , etc. Then, these data are transmitted and recorded in the profile, where they are stored until deleted by the user.



03 settembre 2011
Osteria Numero Uno Di D'Acquisto Angelo - 13:54

[83] Article 360 Code of Criminal Procedure(Accertamenti tecnici non ripetibili}

[84] View http://www.google.com/mobile/android/

[85] There are many exceptions to what has been written, an example may be the Toshiba Netbook AC 100: Google applications are absent and the app Store for the applications is the Camangi Market (www.camangimarket.com).

[86] http://www.google.com/support/mobile/bin/answer.py?answer=1304818

7.2.2 PLAY MARKET

Similar to what occurs within the iOS system with the App Store, the Android Play Market[87] is used to download and/or purchase games or applications that increase the functionality of your smartphone. You can get updates of installed applications through the market as well[88].

In addition to this mode, the Android operating system provides the ability to install applications via third party (applibs, Amazon Android Market, etc..) or via direct copy of the application inside the phone.

It should be pointed out that the policies adopted by Google have allowed in recent months the presence of malware and the subsequent proliferation of various infections[89].The spread of malware has been partly hampered both by the rapid release of updates by Google and by the remote uninstallation of the malware application[90].

The security of applications is even less impressive, if not absent, in the case of third party markets. There are many reported cases of various malware present in these channels[91].

The effect of the activities mentioned above was limited by effective management, and the release of special firmware updates from smartphone manufacturers and telephone providers who distribute Android smartphones. This seriously affects the possibility to close security holes in the various models in circulation and contributes to the persistence and spread of malware.The presence of cooked free ROM[92] would alleviate the problem, but installing non-original ROM is often discouraged by the manufacturers.

In theory, the selling and releasing of update policies could create the possibility of attacking specific geographical areas or the users of certain providers.

7.2.3 FILE SYSTEM IN USE

YAFFS2 (Yet Another Flash File System) is the file system used in Android devices up to version 2.2.Created by Charles Manning for the Finnish company Aleph One, is currently licensed under the GPL license.

Today it is officially supported by the following operating systems:

- Android
- Linux
- Windows CE
- pSOS

[87] The Play store is also accessible via the web page https://market.android.com. It enables also to remotely install the applications.

[88] The software house companies are also able to limit the availability of the applications to specific geographical areas or telephone service providers based on their sales requirements.

[89] https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf

[90] One recent example of malware is Anserverbot (http://www.csc.ncsu.edu/faculty/jiang/pubs/AnserverBot_Analysis.pdf)

[91] https://www.mylookout.com/_downloads/lookout-mobile-threat-report-2011.pdf

[92] See for example Cyanogen mod (http://www.cyanogenmod.com/devices) or MIUI (http://miuiandroid.com/)

- eCos
- ThreadX

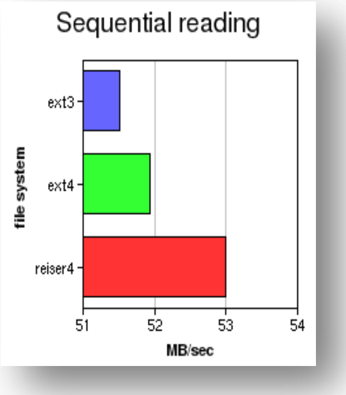
The second version of this file system ensures a high level of integrity of data written into memory and, at the same time, attempts to maintain the highest possible performance when accessing data[93]. Compared to the first version of the file system, the performance of writing a file has been improved by 500% and the performance of deleting[94] by 400%.

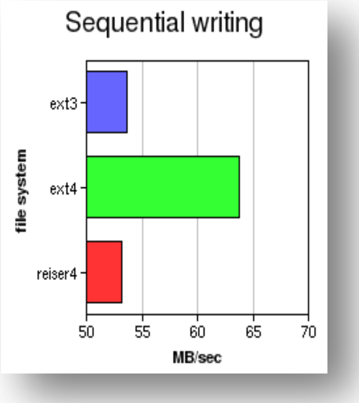
Since Android version 2.3, the developers decided to abandon this file system migrating to EXT4.

7.2.4 EXT4 FILE SYSTEM

Ext4[95] (fourth extended file system) is a journaled file system[96] born as an improvement of the Ext3 to increase the 64-bits storage limits and improve its performance. With regard to file reading, despite the performances are lower than those of competitors file system[97], Ext4 uses less CPU resources and is more powerful in writes procedures.

Today it is considered safer than other Linux file systems because of its simplicity and the wider installation base for testing purposes.





[93] It is also considered that the hardware is "portable" and the type of drive in 99% of cases is solid-state.
[94] http://www.yaffs.net/yaffs-2-specification-and-development-notes.
[95] To date, ext4 is natively supported by any Linux distribution, by Windows thanks to the Ext2 project and by the main applications, commercial or not, for Computer Forensics.
[96] It is a technology used by many modern file systems to preserve data integrity from any power failures or sudden shutdowns. It is based on the concept of transaction, every write to disk is interpreted by the file system as a transaction.
[97] Such as for example JFS, ReiserFS and XFS, Ext4.

The main characteristics of EXT4 are:

- file system sizes up to 1 exabyte (1,000,000 terabytes);
- Removal of the limit of 32000 subdirectories;
- Persistent pre-allocation[98];
- Backward compatibility. Being able to mount ext2 and ext3 file system as ext4;
- Increased performance for file system integrity check (fsck);
- Online defragmentation drastically reducing file system fragmentation.

Native support for ext4 has been introduced in Android version 2.3 for its new features related to the improvement in the writing of files and their guarantee of integrity.

From a forensic point of view, this implementation has made it much easier to analyse file systems because, to date, there are no tools, free or commercial, that support natively the YAFFS file system.

7.2.5 POLICY OF MASS STORAGE USE

In most of Android devices, the end user can decide how to use the mass memory, internal and external, at their disposal.

Generally all applications downloaded and installed from the Android Market are stored in the internal memory, except to those which have implemented the function to select the mass memory in which to be installed. Even in the case of files produced by the present applications[99], it is given the end user the opportunity to decide whether to save them in the internal or the external memory.

7.2.6 ACCESS TO THE FILE SYSTEM OF THE OPERATING SYSTEM

All Android devices of the major manufacturers are distributed without the root user enabled and without the possibility to directly access the file system which contains the operating system[100].

However, there is the possibility to overcome these restrictions virtually for all devices currently on the market provided that changes invasive to the system itself (by altering the original file system) are accepted. This process is colloquially known as "rooting"[101], which is achieved differently depending on the device and respective operating system. Smartphone manufacturers discourage rooting your device, and it will more than likely void your warranty.

From the forensic point of view, this type of alteration is strictly necessary to be able to access information of interest such as the call log, SMS, Internet browsing history and everything that an application could write in a given directory.

[98] In other words, the applications have the ability to pre-allocate disk space.

[99] For example, saving attachments or pictures taken with your device.

[100] The devices of the minor Asian manufacturer companies, in some cases, do not apply this type of restriction, therefore facilitating the access to the information of interest to us.

[101] http://en.wikipedia.org/wiki/Rooting_(Android_OS)

7.3 SAMSUNG GALAXY S I9000 - HARDWARE FEATURES

The device being analyzed is a Samsung Galaxy S i9000 with Android 2.3.3.

Samsung, like other smartphones manufacturers, has decided to heavily customize the Android architecture in their devices.

The file system in use on this device is a proprietary implementation belonging to Samsung and named RFS (Robust FAT File System). This is a FAT file system to which was added a journaling system that should make it safer, preventing data loss in case of error.

This implementation has actually been rather unsuccessful because the majority of users have complained about the device performances, related to poor performance that RFS would provide in terms of reading and writing speed.

From a forensic point of view, the partitions of type RFS can be treated as VFAT. Therefore, all the software for the Computer Forensic that support VFAT file systems can read a RFS file system[102].

The main hardware features of this device are:

Processor:

S5PC110 CPU, 45 nm 1 GHz ARM Cortex-A8-based
PowerVR SGX 540 GPU that supports OpenGL ES 1.1/2.0.

Memory:

512 MB LPDDR2 dedicated RAM,
16-32 MB DRAM,
8GB of solid-state memory with the possibility of expansion up to 32 GB through the use of a microSD card.

[102] It is therefore possible to imagine that all Linux distributions and commercial software for the Computer Forensics are already prepared for analysis for this type of device.

7.3.1 ROOTING PROCEDURES

The procedure for obtaining the rooting of this device substantially consists in the modification of the smathphone kernel by the addition of a program called busybox[103] .

This procedure is the less invasive for the system and allows to presever the memory integrity(nor overwritten nor deleted), keeping unchanged the content of the file system partitions containing files produced by the applications and the applications themselves.

The tools needed for the rooting of the Android device are:

- The synchronization software Samsung Keies (installed and started at least once)[104];
- The CF-ROOT[105] version suitable for the device under investigation (check the build number in settings -> phone info) that can be downloaded from the site of xda developers[106] .

After you get everything you need, you can proceed with the steps:

1. Enable USB debugging mode from the menu settings > applications > development, thus allowing the phone to transmit files via the USB connection;
2. Turn off the Galaxy S and reboot into upgrade/recovery mode by pressing at the same time the middle button, volume down key and power key (you should see a danger sign that warns you about potential harmful actions)[107];
3. Connect the device to PC via USB and launch Odin. If the field ID:COM is yellow, then the smartphone was recognized correctly, otherwise there is probably a problem with the operating system drivers[108];
4. Extract the archive CF-Root.zip, click PDA and select the unzipped file;
5. Select only the Auto-Reboot and F. Reset Time[109] from the options available;
6. Click START and after about 15 seconds the display will show "PASS" highlighted in green. From that moment on, the device will reboot automatically with the rooted system.

[103] http://www.busybox.net/about.html

[104] http://www.samsungapps.com/about/onPc.as

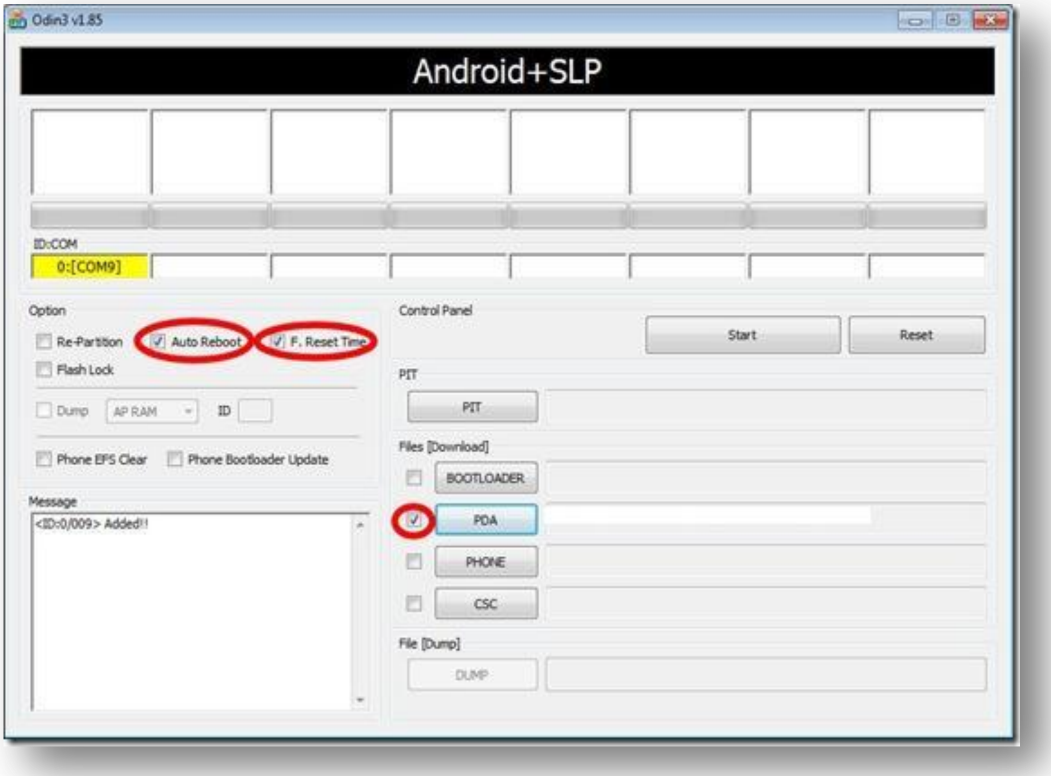
[105] file for editing the kernel of the device

[106] http://forum.xda-developers.com/showpost.php?p=12651359&postcount=6

[107] This procedure allows to start the device in a mode dedicated to the acquisition of files for the flash operations of the memory.

[108] It is necessary to start Kies with a Galaxy S (preferably not the one being tested) connected via USB and from the tools menu click "install drive".

[109] DO NOT select the Re-Partition: This function will delete the current running kernel!



ID:COM
0:[COM9]

Option
□ Re-Partition ☑ Auto Reboot ☑ F. Reset Time
□ Flash Lock
□ Dump AP RAM ID
□ Phone EFS Clear □ Phone Bootloader Update

Message
<ID:0/009> Added!!

□ BOOTLOADER
☑ PDA
□ PHONE
□ CSC

7.3.2 SAMSUNG GALAXY S - ACQUISITION OF THE INTERNAL FLASH MEMORY

Acquisition of the internal memory of the device is certainly very inconvenient and dangerous if compared to that of a hard disk.

The only available method is to use the dd command to be executed either using the virtual keyboard of the device (after installing an app as "Terminal emulator") either over the network by using *ssh* (after installing a "ssh daemon").The output of the *dd* command can only be saved in the memories recognized by the device: either the internal flash memory or a MicroSD.

In our case we chose to save the *bit stream image* inside the MicroSD for convenience and portability of the external memory.

For architectural reasons, unlike the classical mass storage, it is not possible to clone the entire memory in a single session, but we areobliged to execute the *dd* command for each partition mounted by the device.

In order to know the number of all partitions used by the system it is necessary to view them through the *mount* command.

An example of output of the command can be the following:

```
rootfs on / type rootfs (ro,noatime,nodiratime) tmpfs on /dev type tmpfs
(rw,noatime,nodiratime,mode=755)
devpts on /dev/pts type devpts (rw,noatime,nodiratime,mode=600)
proc on /proc type proc (rw,noatime,nodiratime)
sysfs on /sys type sysfs (rw,noatime,nodiratime)
none on / acct type cgroups (rw,relatime,cpuacct)
tmpfs on /mnt/asec type tmpfs (rw,noatime,nodiratime,mode=755,gid=1000)
tmpfs on /mnt/obb type tmpfs (rw,noatime,nodiratime,mode=755,gid=1000)
none on /dev/cpuctl type cgroup (rw,relatime,cpu)
/dev/block/stl9 on /system type rfs (ro,noatime,nodiratime,vfat,log_off,check=no,gid/uid/rwx,
iocharset=utf8)
/dev/block/stl3 on /efs type rfs (rw,nosuid,nodev,noatime,nodiratime,vfat,llw,check=no,gid/uid/rwx,
iocharset=utf8)
/dev/block/mmcblk0p2 on /data type rfs (rw,nosuid,nodev,noatime,nodiratime,vfat,llw,
check=no,gid/uid/rwx,iocharset=utf8)
/dev/block/stl10 on /dbdata type rfs (rw,nosuid,nodev,noatime,nodiratime,vfat,llw,
check=no,gid/uid/rwx,iocharset=utf8)
/dev/block/stl11 on /cache type rfs (rw,nosuid,nodev,noatime,nodiratime,vfat,llw, check=no,gid/uid/rwx,
iocharset=utf8)
/dev/block/stl6 on /mnt/.lfs type j4fs (rw,noatime,nodiratime)
/sys/kernel/debug on /sys/kernel/debug type debugfs (rw,noatime,nodiratime)
/dev/block/vold/179:1 on /mnt/sdcard type vfat
(rw,dirsync,nosuid,nodev,noexec,noatime,nodiratime,uid=1000,gid=1015,fmask=0002,dmask=0002,all
ow_utime=0020,codepage=cp437,iocharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/vold/179:9 on/mnt/sdcard/external_sd type vfat
(rw,dirsync,nosuid,nodev,noexec,noatime,nodiratime,uid=1000,gid=1015,fmask=0002,dmask=0002,all
ow_utime=0020,codepage=cp437,iocharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/vold/179: 9 on /mnt/secure/asec type vfat
tmpfs on /mnt/sdcard/external_sd/.android_secure type tmpfs (ro,relatime,size=0k, mode=000)
/dev/block/dm-0 on /mnt/asec/android.androidVNC-2 type vfat
(ro,dirsync,nosuid,nodev,relatime,uid=1000,fmask=0222,dmask=0222,codepage=cp437,iocharset=iso
8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/dm-1 on /mnt/asec/net.androgames.level-2 type vfat
(ro,dirsync,nosuid,nodev,relatime,uid=1000,fmask=0222,dmask=0222,codepage=cp437,iocharset=iso
8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/dm-2 on /mnt/asec/punteroanull.app.androick-1 type vfat
```

```
(ro,dirsync,nosuid,nodev,relatime,uid=1000,fmask=0222,dmask=0222,codepage=cp437,iocharset=iso
8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/dm-3 on /mnt/asec/com.natenai.glowhockey-1 type vfat
(ro,dirsync,nosuid,nodev,relatime,uid=1000,fmask=0222,dmask=0222,codepage=cp437,iocharset=iso
8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/dm-4 on / mnt/asec/com.feelingtouch.bocce-1 type vfat
(ro,dirsync,nosuid,nodev,relatime,uid=1000,fmask=0222,dmask=0222,codepage=cp437,iocharset=iso
8859-1,shortname=mixed,utf8,errors=remount-ro)
/dev/block/dm-5 on /mnt/asec/com.fridgecat.android.atiltlite-1 type vfat
(ro,dirsync,nosuid,nodev,relatime,uid=1000,fmask=0222,dmask=0222,codepage=cp437,iocharset=iso
8859-1,shortname=mixed,utf8,errors=remount-ro)
```

Before starting the acquisition it is necessary to obtain root permissions by typing the su *command.*After a few seconds the terminal will ask whether to confirm the request to authorize the program to run with administrator privileges.

Once you have these permissions, the command to be executed for the acquisition is the classic *dd* configured as follows:

dd if=partition of=/mnt/sdcard/filename.img

Therefore in the case we want to acquire the /system partition, the command will be

dd if=/dev/block/stl9 of=/mnt/sdcard/system.img

Once the acquisition is over, it is possible to access the cloned partition by using the mount command, treating the RFS partition as a vfat:

mount -o loop -t vfat -o ro system.img /mnt/evidence/system

where

- *-o loop* allows you to mount images in bit stream format;
- *-t vfat* declares that the type of partition you want to use is vfat;
- *-o ro* allows read-only access to the partition;
- */mnt/evidence/system* is the path created to display the contents of the acquired memory inside the directory.

7.4 SAMSUNG GALAXY S - ACQUISITION OF THE EXTERNAL MEMORY

Unlike flash memory within the device, the acquisition of the MicroSD can be carried out by following the directions of best practices in computer forensics and do not need root access:

1. remove the MicroSD card;
2. connect it to a write blocker[110] or to a system that has equivalent features[111];
3. calculate the hash value[112] of the original memory;
4. *acquisition by using the application you prefer[113] and verify that the cloned memory hash is the same as the hash of the original.*

7.4.1 WORKING DIRECTLY ON THE SMARTPHONE

In cases of particular urgency, you can research files of interest directly from the touchscreen of the device through the use of some applications available for free from the Android Market.

A very useful application for this type of activity, although not a software designed specifically for the Computer Forensics, is File ManagerHD[114].Activating the "Root Explorer" in the settings of the application, you can browse the file system even in protected directories such as data, dbdata and system, searching the files of interest using the appropriate function of search and copy them to microSD card for a more thorough analysis on a workstation equipped with the necessary tools.

7.4.2 LOCATION AND ANALYSIS OF APPLICATIONS AND FILES OF COMMON INTEREST

Typically, an application is made by its executable file with .apk extension and its configuration files or database[115] .

The folders that are more interesting to the examiner:

- */system/app/:* contains basic applications provided by the manufacturer of the device;
- */data/app/:* contains the applications that the user has installed via the Android Market;
- */data/data/:* contains the configuration files and the databases of the applications;

[110] Device used to prevent writes to the storage system being analyzed.

[111] Linux distributions for Computer Forensics.

[112] The hash is a mathematical function unique and unidirectional (ie which cannot be reversed), which transforms a text of any length (input) into a fixed-length text (output) relatively limited, in practice by applying a hash function to a file or to a whole hard disk, you obtain a sequence of characters, eg. of 32 characters, representing a kind of "fingerprint" of the file, and is called the hash value.

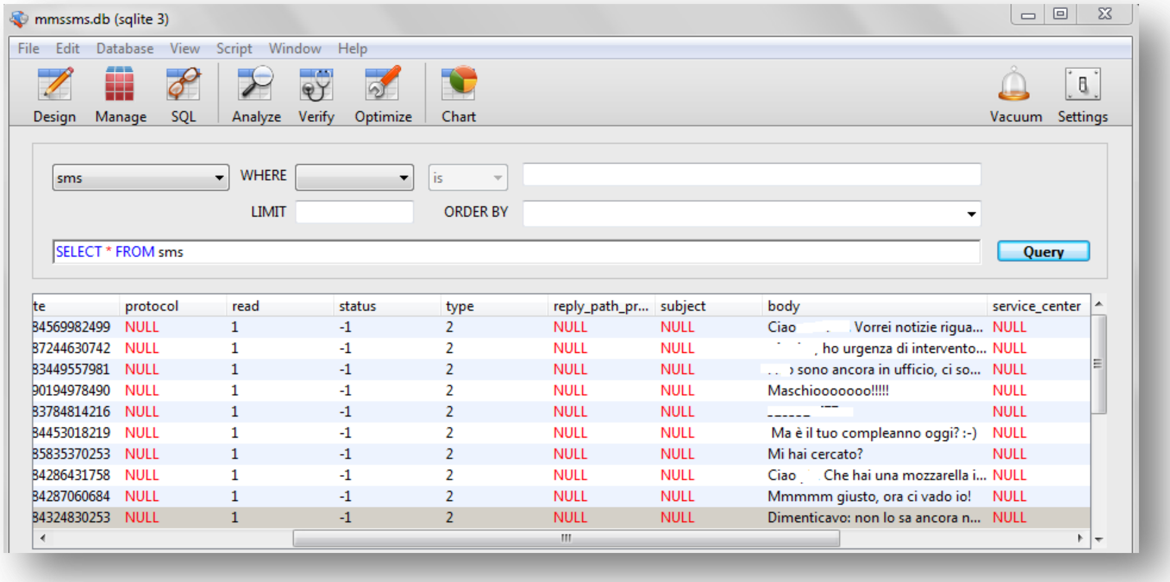
[113] Example: FTK Imager for Windows or Guymager dd for Linux-

[114] https://market.android.com/details?id=com.rhmsoft.fm

[115] Samsung, like all the other device manufacters, prefers not to change the standard portion of memory where to group the applications.

- */dbdata/database/*: here there are databases containing SMS, MMS, contacts and everything related to voice part.

The analysis of the configuration files and the database of the applications can be performed using tools like text editor for text and xml configurations and with a standard SQLite[116] client for the database with .db extension.



sms

SELECT * FROM sms

te	protocol	read	status	type	reply_path_pr...	subject	body	service_center
84569982499	NULL	1	-1	2	NULL	NULL	Ciao . Vorrei notizie rigua...	NULL
87244630742	NULL	1	-1	2	NULL	NULL	, ho urgenza di intervento...	NULL
83449557981	NULL	1	-1	2	NULL	NULL	. . › sono ancora in ufficio, ci so...	NULL
90194978490	NULL	1	-1	2	NULL	NULL	Maschioooooooo!!!!!	NULL
83784814216	NULL	1	-1	2	NULL	NULL	------	NULL
84453018219	NULL	1	-1	2	NULL	NULL	Ma è il tuo compleanno oggi? :-)	NULL
85835370253	NULL	1	-1	2	NULL	NULL	Mi hai cercato?	NULL
84286431758	NULL	1	-1	2	NULL	NULL	Ciao , Che hai una mozzarella i...	NULL
84287060684	NULL	1	-1	2	NULL	NULL	Mmmmm giusto, ora ci vado io!	NULL
84324830253	NULL	1	-1	2	NULL	NULL	Dimenticavo: non lo sa ancora n...	NULL

In the example shown in the image, we used a client to open the sms and mms SQLite database named *mmssms.db* stored in

/dbdata/database/com.android.providers.telephony/

and to analyze its contents, by exporting useful data in the desired format (txt, xml or csv).

The analysis of the tables in a SQLite database can also be performed by using sql query[117] without using dedicated tools[118].

Examples:

You can view all the fields contained in the sms table with the request:

*Select * from sms*

In the event that only the content of all text messages interests :

Select body from sms

[116] Sqlite (http://www.sqlite.org) allows you to create a database, including tables, queries, forms and reports in a single file.

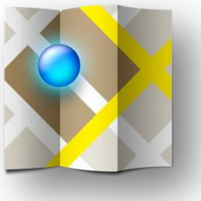
[117] Querying a database to perform certain operations (select, insert, delete data, etc. ..) to be executed in one or more databases. A query is usually interpreted by the SQL language to make it more understandable to the DBMS.

[118] Such as http://www.filesig.co.uk/sqlite-forensic-reporter.html

If we wanted to display only text messages received by +3912345 number:

*Select * from sms where address='+3912345'*

7.4.3 EXAMPLE OF ANALYSIS ON GOOGLE MAPS



Google Maps application[119] offers on Android systems both the map function and the navigation system with voice commands.

The application, just like the web version of the same name, is able to show the area both in 3D graphic and via satellite images, to provide information on local traffic, on pubs and on services in the vicinity and, through the Latitude feature, provide information on the position of your contacts (also via Checkin/checkout).

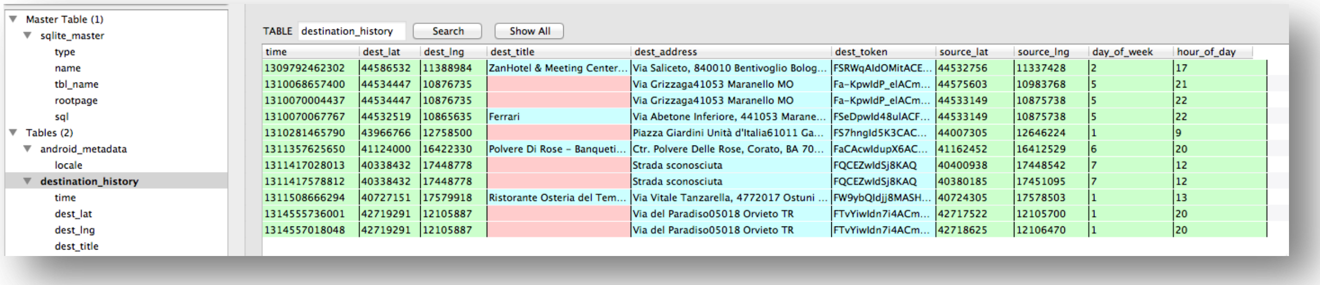
The directories of interest for the examiner are

/data/data/com.google.android.apps.maps/

in the SD memory card

/mnt/sdcard/Android/data/com.google.android.apps.maps/

among the most interesting database for analysis we recommend *da_destination_history* [120]

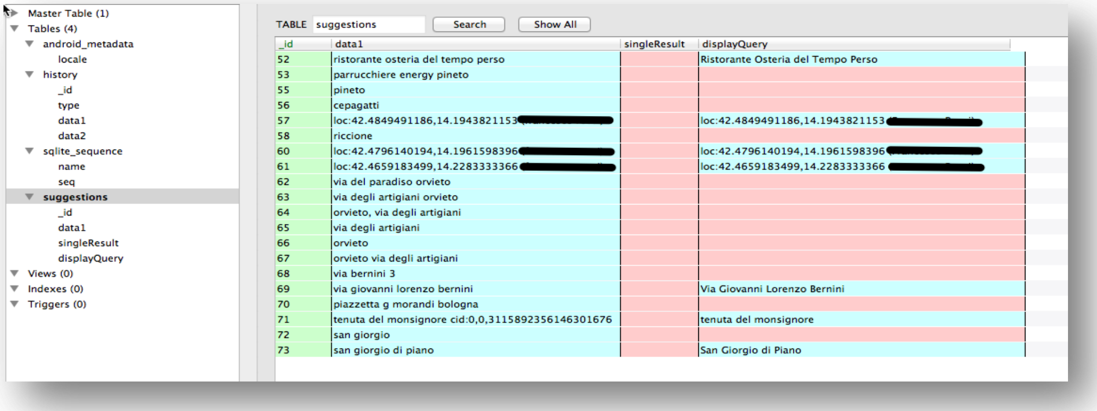


- Master Table (1)
  - sqlite_master
    - type
    - name
    - tbl_name
    - rootpage
    - sql
- Tables (2)
  - android_metadata
    - locale
  - **destination_history**
    - time
    - dest_lat
    - dest_lng
    - dest_title

time	dest_lat	dest_lng	dest_title	dest_address	dest_token	source_lat	source_lng	day_of_week	hour_of_day
1309792462302	44586532	11388984	ZanHotel & Meeting Center…	Via Saliceto, 840010 Bentivoglio Bolog…	FSRWqAldOMitACE…	44532756	11337428	2	17
1310068657400	44534447	10876735		Via Grizzaga41053 Maranello MO	Fa-KpwldP_elACm…	44575603	10983768	5	21
1310070004437	44534447	10876735		Via Grizzaga41053 Maranello MO	Fa-KpwldP_elACm…	44533149	10875738	5	22
1310070067767	44532519	10865635	Ferrari	Via Abetone Inferiore, 441053 Marane…	FSeDpwld48ulACF…	44533149	10875738	5	22
1310281465790	43966766	12758500		Piazza Giardini Unità d'Italia61011 Ga…	FS7hngld5K3CAC…	44007305	12646224	1	9
1311357625650	41124000	16422330	Polvere Di Rose - Banqueti…	Ctr. Polvere Delle Rose, Corato, BA 70…	FaCAcwldupX6AC…	41162452	16412529	6	20
1311417028013	40338432	17448778		Strada sconosciuta	FQCEZwldSj8KAQ	40400938	17448542	7	12
1311417578812	40338432	17448778		Strada sconosciuta	FQCEZwldSj8KAQ	40380185	17451095	7	12
1311508666294	40727151	17579918	Ristorante Osteria del Tem…	Via Vitale Tanzarella, 4772017 Ostuni …	FW9ybQldjj8MASH…	40724305	17578503	1	13
1314555736001	42719291	12105887		Via del Paradiso05018 Orvieto TR	FTvYiwldn7i4ACm…	42717522	12105700	1	20
1314557018048	42719291	12105887		Via del Paradiso05018 Orvieto TR	FTvYiwldn7i4ACm…	42718625	12106470	1	20

[119] Available at http://www.google.com/mobile/maps/

[120] Note that this SQLite database does NOT have the .db extension like other databases.



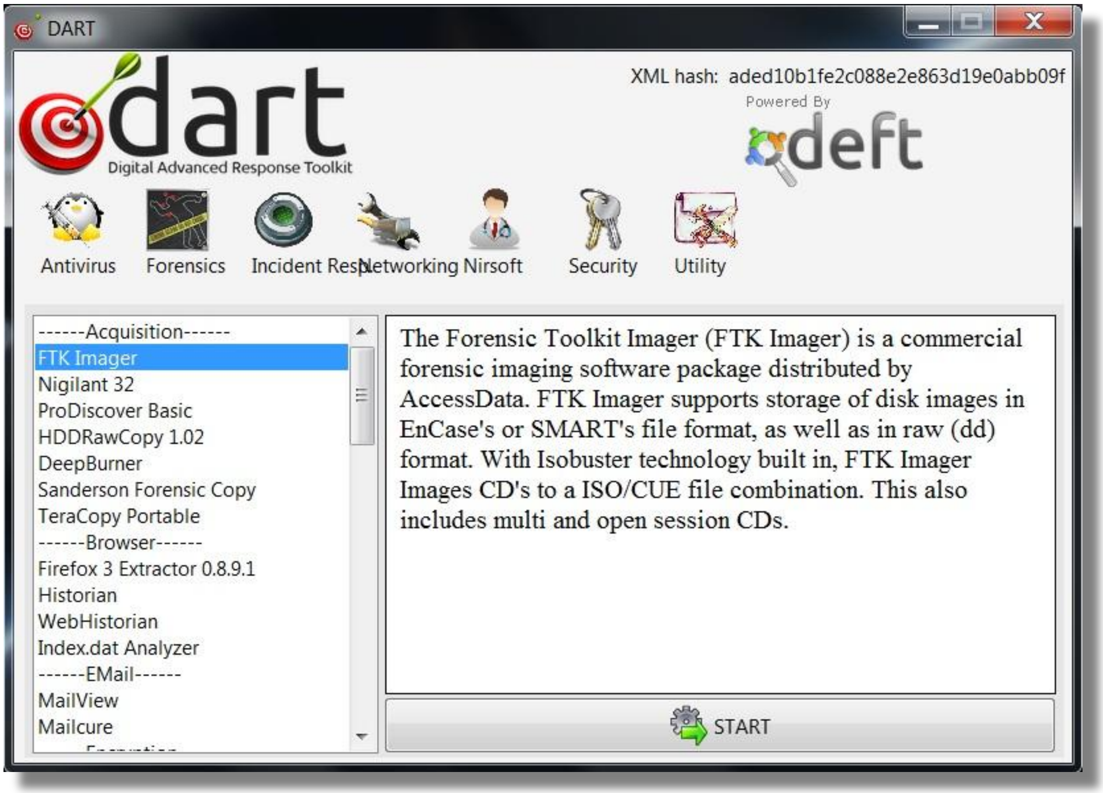
_id	data1	singleResult	displayQuery
52	ristorante osteria del tempo perso		Ristorante Osteria del Tempo Perso
53	parrucchiere energy pineto		
55	pineto		
56	cepagatti		
57	loc:42.4849491186,14.1943821153 [redacted]		loc:42.4849491186,14.1943821153 [redacted]
58	riccione		
60	loc:42.4796140194,14.1961598396 [redacted]		loc:42.4796140194,14.1961598396 [redacted]
61	loc:42.4659183499,14.2283333366 [redacted]		loc:42.4659183499,14.2283333366 [redacted]
62	via del paradiso orvieto		
63	via degli artigiani orvieto		
64	orvieto, via degli artigiani		
65	via degli artigiani		
66	orvieto		
67	orvieto via degli artigiani		
68	via bernini 3		
69	via giovanni lorenzo bernini		Via Giovanni Lorenzo Bernini
70	piazzetta g morandi bologna		
71	tenuta del monsignore cid:0,0,3115892356146301676		tenuta del monsignore
72	san giorgio		
73	san giorgio di piano		San Giorgio di Piano

These are just two of the databases used by the applications, additional information can and should be gained from other files (eg *data_laywe_24* if present).

Of great interest is also the content of the folder on the SD card: In addition to the cache of the maps downloaded by the applications during its use, there are also single audio files containing the audio directions for the user. The analysis of the timestamp[121] files, combined with the navigation data contained within the root folder can provide precise information on when a particular path has been suggested and followed.

[121] http://en.wikipedia.org/wiki/Timestamp

CHAPTER 8: DART - DIGITAL ADVANCED RESPONSE TOOLKIT



XML hash: aded10b1fe2c088e2e863d19e0abb09f

The Forensic Toolkit Imager (FTK Imager) is a commercial forensic imaging software package distributed by AccessData. FTK Imager supports storage of disk images in EnCase's or SMART's file format, as well as in raw (dd) format. With Isobuster technology built in, FTK Imager Images CD's to a ISO/CUE file combination. This also includes multi and open session CDs.

DART

DART (Digital Advanced Response Toolkit) is an application that organizes, collects and runs software in safe mode for the purpose of live forensic analysis and incident response.

You can customize DART by modifying the *dart.xml* file which maintains the list of applications that DART can run.

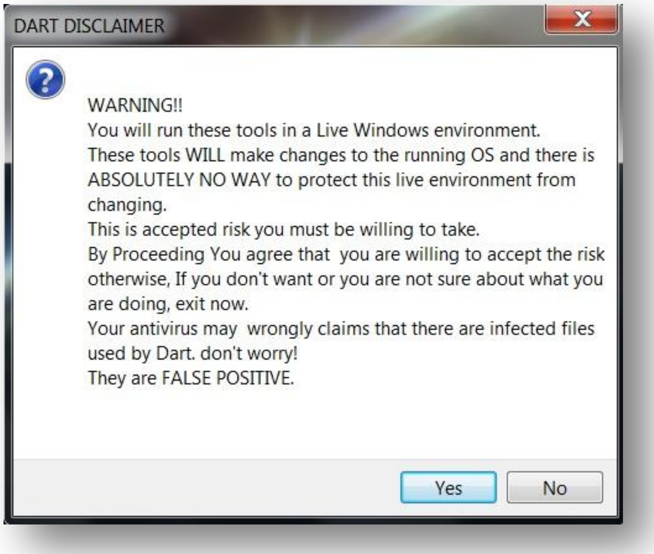
If requested, DART can create an audit log to keep track of all the performed operations and any encountered problems.

One of the major features is that to run applications in safe mode an integrity check launches before the start of each program, this way the examiner is sure to run their own tools safely. This excludes any preexisting damage of the binaries by malware.

The hash values of the applications are contained within the xml file which in turn is checked each time the DART starts[122].This allows the examiner to verify that the content of their xml file has not been altered[123].

[122] The hash value of the XML file is shown in the upper right corner of the window.

[123] For example, the hash of an executable.

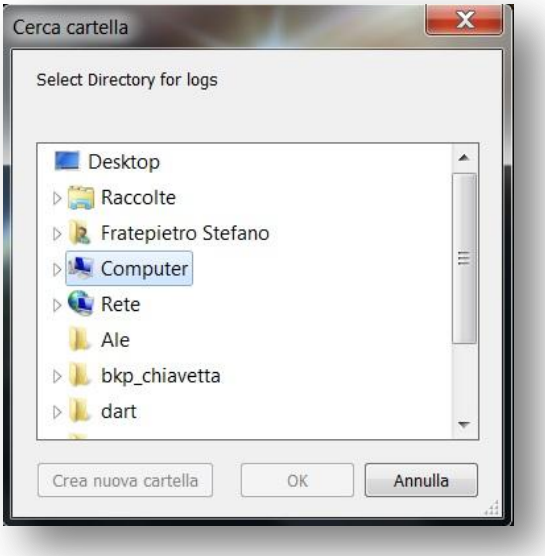

DART DISCLAIMER

WARNING!!
You will run these tools in a Live Windows environment.
These tools WILL make changes to the running OS and there is ABSOLUTELY NO WAY to protect this live environment from changing.
This is accepted risk you must be willing to take.
By Proceeding You agree that you are willing to accept the risk otherwise, If you don't want or you are not sure about what you are doing, exit now.
Your antivirus may wrongly claims that there are infected files used by Dart. don't worry!
They are FALSE POSITIVE.

DART: initial notice

Once started, DART has to be run as the system administrator or as an account with administrator privileges. DART will inform you that there is no guarantee of avoiding alterations to the system in use since some software may conduct analysis in an invasive manner.

At the same time the user is informed that some software could be considered malware or hacking tools by the antivirus software. It may be necessary to disable your antivirus software or firewall.


Cerca cartella

Select Directory for logs

DART: Saving the audit log

dart.xml contains the hash values of all the applications, therefore in the case where an executable included in the DART package is updated, its hash also must be updated within the xml file. If this is not done then the examiner will be informed that the has values do not match.

The structure of the xml file starts with the tag "deft_extra"[124].The tag "alert" contains the text of the initial disclaimer, *dart disclaimer.* Within it, there must be a tag "text" which will show the description for the application enclosed in *<! [CDATA [and]]>.*

Example:

```
<text>
        <! [CDATA [
                insert text
        ]]>
</ text>
```

The tag *apps_groups* indicates the groups with which the applications are divided.

"group" has the following attributes:

- *id:* it must contain a unique id, but not necessarily a numeric one;
- *label:* the text that will appear below the icon on the application window;
- *ico:* path of the icon which will represent the group.

Inside the tag *group* you find the tag *app* with the following attributes:

- *label:* the text shown in the left application menu;
- *exepath:* relative or absolute path where you can find the executable;
- *md5hash:* hash value to be checked (not mandatory).

Within the *app* tag there is a "text" tag which contains the description of the application, also in HTML format, which is also enclosed in *<! [CDATA [and]]>.*

Example:

```
<text>
        <! [CDATA [
                insert text
        ]]>
</ text>
```

[124] The "lang" attribute will allow you to access the multilingual manager. Currently this feature is not active.

CHAPTER 9: TO DEEPEN

The aforementioned content in this manual touches lightly upon the potential of Deft in the field of Digital Forensics.

We would like to suggest a few books that elucidate the topics we have covered in this manual.

NIST Guidelines

Guidelines on Cell Phone and PDA Security - SP 800-124

Computer Security Incident Handling Guide - SP 800-61

Digital Forensics

Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers and the Internet

Eoghan Casey

ISBN-10: 0123742684

Academic Press

Digital Forensics with Open Source Tools

Cory Altheide & Harlan Carvey

ISBN-10: 1597495867

Syngress

Android Forensics: Investigation, Analysis, and Mobile Security for Google Android

Andrew Hoog

ISBN-10: 1597496510

Syngress