DFA Open Day 2014

DEFT come strumento di Incident Response

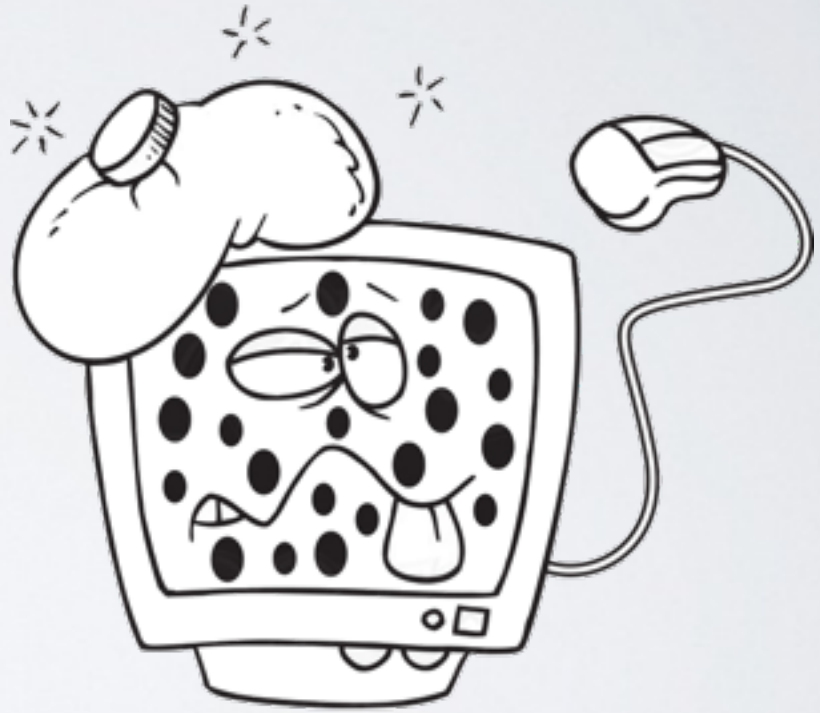
Paolo Dal Checco

Adeft Associazione NO PROFIT

5 giugno 2014, Università degli Studi di Milano

Incidente Informatico

- RFC 2350: Expectations for Computer Security Incident Response
- Un evento che compromette aspetti della sicurezza dei computer e delle reti, con almeno uno dei seguenti fattori:
  - perdita di confidenzialità delle informazioni
  - compromissione dell'integrità delle informazioni
  - interruzione di servizio
  - utilizzo inappropriato di servizi, sistemi, informazioni
  - danneggiamento di sistemi



Incident Reponse

- **Approccio strutturato e organizzato alla gestione delle conseguenze di un incidente informatico**
- **Fasi standard [SANS]: preparazione, identificazione, contenimento, rimozione, recupero, apprendimento**
- **Non si usa l'accetta ma… attenzione a non esagerare con la "response" (esempio di perizia forenZe)**

First Responder

- Tipicamente il soggetto che arriva per primo sulla scena:
  - Identifica gli oggetti
  - Preserva la scena e i dati
  - Raccoglie le informazioni
  - Crea una relazione
  - Appone eventualmente i sigilli

Alcune linee guida

- RFC 3227: Guidelines for Evidence Collection and Archiving
- Procedere metodicamente
- Catturare un'immagine completa del sistema
- Minimizzare le modifiche ai dati
- Isolare se necessario il sistema
- Prima si raccoglie, poi si analizza
- Procedere in ordine di volatilità
- Garantire la catena di custodia

Di cosa abbiamo bisogno

- Organizzazione
- Strumento personalizzabile che non richieda ricompilazione
- Raccolta di applicativi ottimizzati per Incident Response
- Strumento di controllo dell'integrità degli applicativi
- Log delle attività svolte
- Possibilmente read-only

The “dart” side of DEFT

dart

Digital Advanced Response Toolkit

DART 2 - 2014

- DART è la **collezione di programmi portabili** per live forensics inclusa nel sistema DEFT (www.deftlinux.net)
- Oltre 300 programmi per ogni versione di Windows, per Linux e per Mac OSX
- Ulteriore corposa sezione di programmi command line
- Permesso esclusivo fornito da diversi sviluppatori per la distribuzione dei loro tool in DEFT/DART (ViaForensics, MonSools, CrowdInspect, Mandiant, Belkasoft, Carvey, ASH368, CyberMarshall, etc…)
- Istruzioni e script per il completamento del pacchetto con i software non ridistribuibili

Launcher

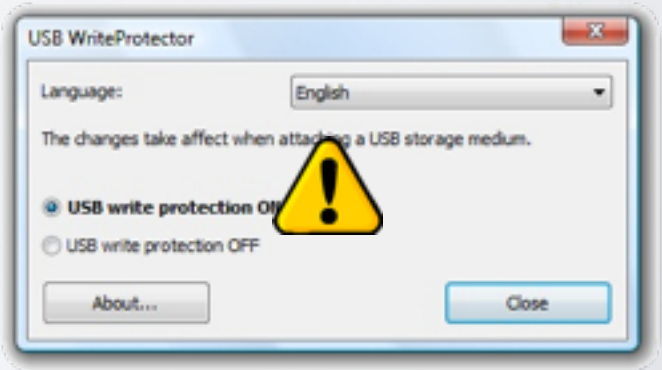
- **Categorizzazione** dei software:
  - Acquisizione
  - Data Recovery
  - Forensics
  - Incident Response
  - Networking
  - Password
  - Visualize
  - Utility
- **Descrizione** di ogni tool
- **Rircerca** veloce
- Verifica dell'**integrità** degli eseguibili
- **Logging** delle applicazioni lanciate con timestamp

Potenzialità

- Acquisizione memorie di massa
- Dump memoria RAM
- Calcolo di hash
- Analisi processi
- Analisi traffico di rete
- Analisi registro di Windows
- Antimalware e Antirootkit
- Time line degli eventi del sistema o del filesystem
- Analisi navigazione Internet e posta elettronica
- Password cracking
- …

Precauzioni

- Vanno bene i controlli di integrità sui binari ma, se possibile, utilizzare supporto read-only



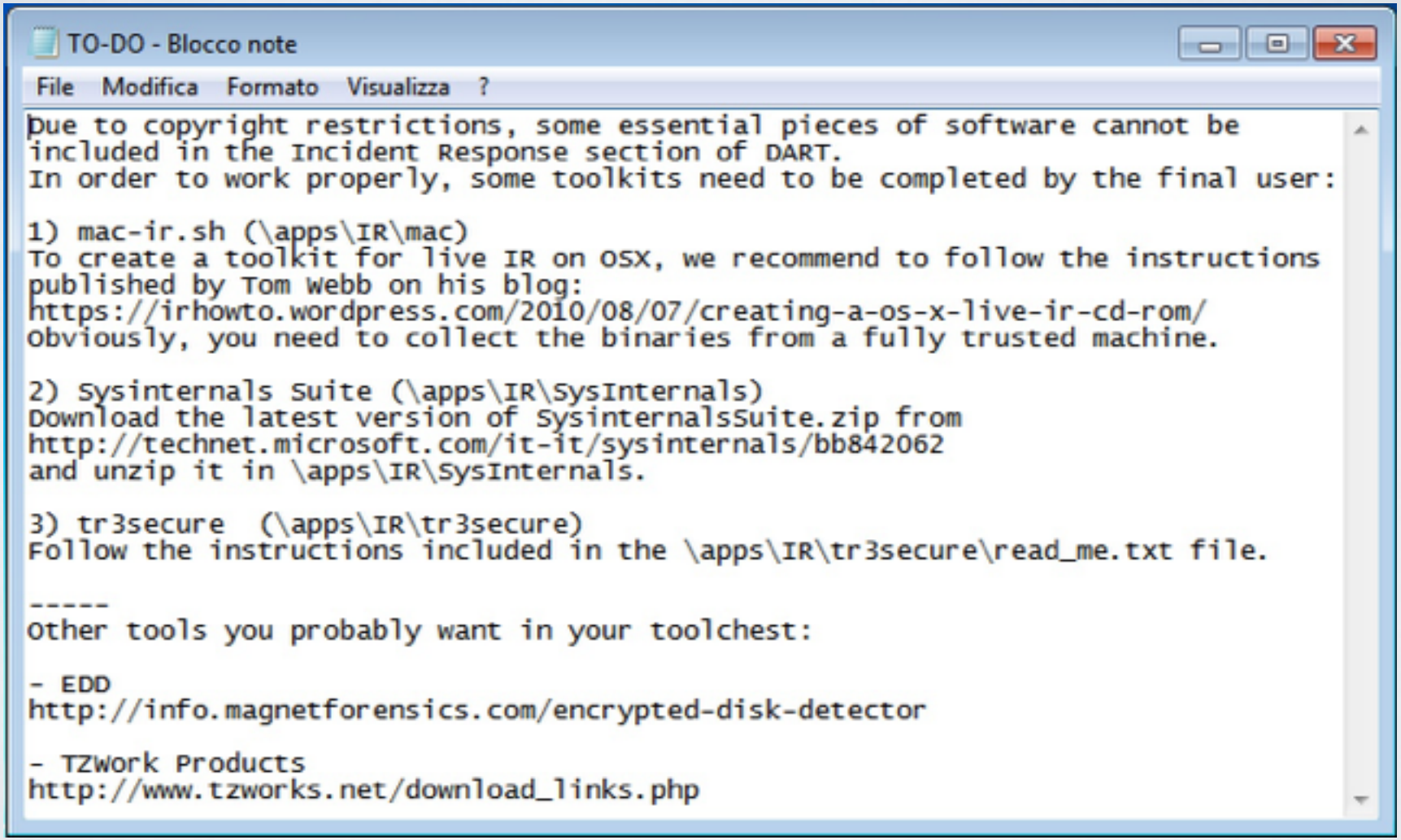
XML

```
<?xml version="1.0"?>
<deft_extra lang="en">
  <alert label="alert">
    <text><![CDATA[WARNING!!    You will run these tools in a Live Windows environment. Th
  </alert>
  <about label="About">
    <text><![CDATA[About...]]></text>
  </about>
  <apps_groups>
    <group label="Acquire" id="1" ico="dart\icons\text-x-copying.png">
      <group label="Burn" id="2"> ... </group>
      <group label="Copy" id="3"> ... </group>
      <group label="Image" id="4"> ... </group>
    </group>
    <group label="Data Recovery" id="5" ico="dart\icons\edit-undelete.png"> ... </group>
    <group label="Forensics" id="6" ico="dart\icons\Forensics.png"> ... </group>
    <group label="Incident Resp." id="17" ico="dart\icons\preferences-desktop-notificatior
    <group label="Networking" id="21" ico="dart\icons\preferences-system-network-2.png">
    <group label="Password" id="22" ico="dart\icons\password.png"> ... </group>
    <group label="Visualize" id="25" ico="dart\icons\eye.png.png"> ... </group>
    <group label="Utility" id="29" ico="dart\icons\perian.png"> ... </group>
  </apps_groups>
</deft_extra>
```

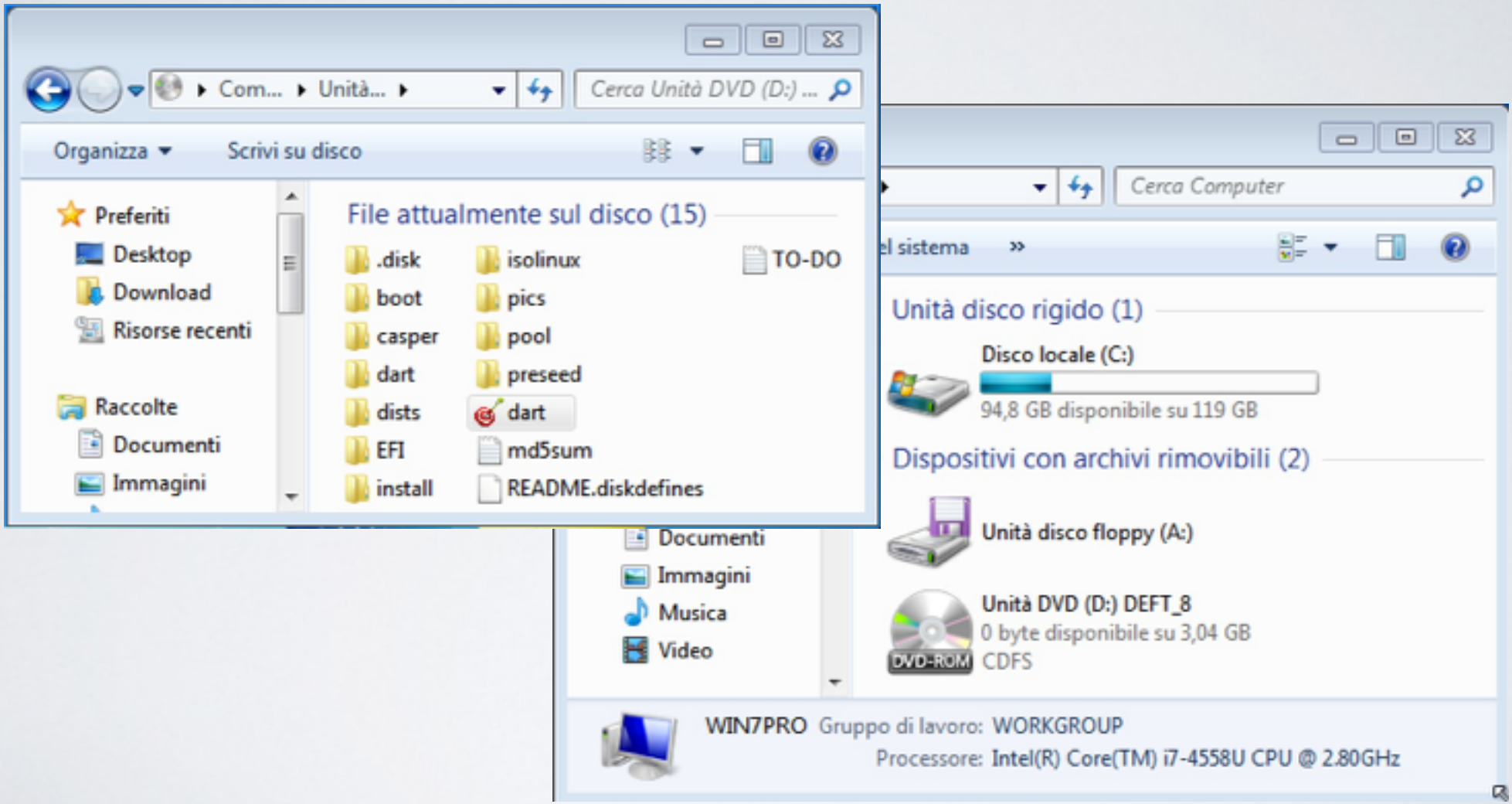
XML

```
  <apps_groups>
    <group label="Acquire" id="1" ico="dart\icons\text-x-copying.png">
      <group label="Burn" id="2"> ⋯ </group>
      <group label="Copy" id="3"> ⋯ </group>
      <group label="Image" id="4">
        <app tags="duplicate" label="FTK Imager"
exepath="dart\apps\Acquire\Image\FtkImager\FTK Imager.exe"
md5hash="aa6c8e9233b43ea7ef013d0e3a071e7b">
          <text><![CDATA[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.<br>]]></text>
        </app>
        <app tags="ram" label="DumpIt" exepath="dart\apps\IR\RAM\moonsols\DumpIt.exe"
md5hash="84f0feb07beae896d471f45527d781b0"> ⋯ </app>
        <app tags="ram,dump,duplicate,analysis" label="Nigilant32"
exepath="dart\apps\Acquire\Image\Nigilant32.exe"
md5hash="7b6056b9df7e16a6e6394659c075411e"> ⋯ </app>
```

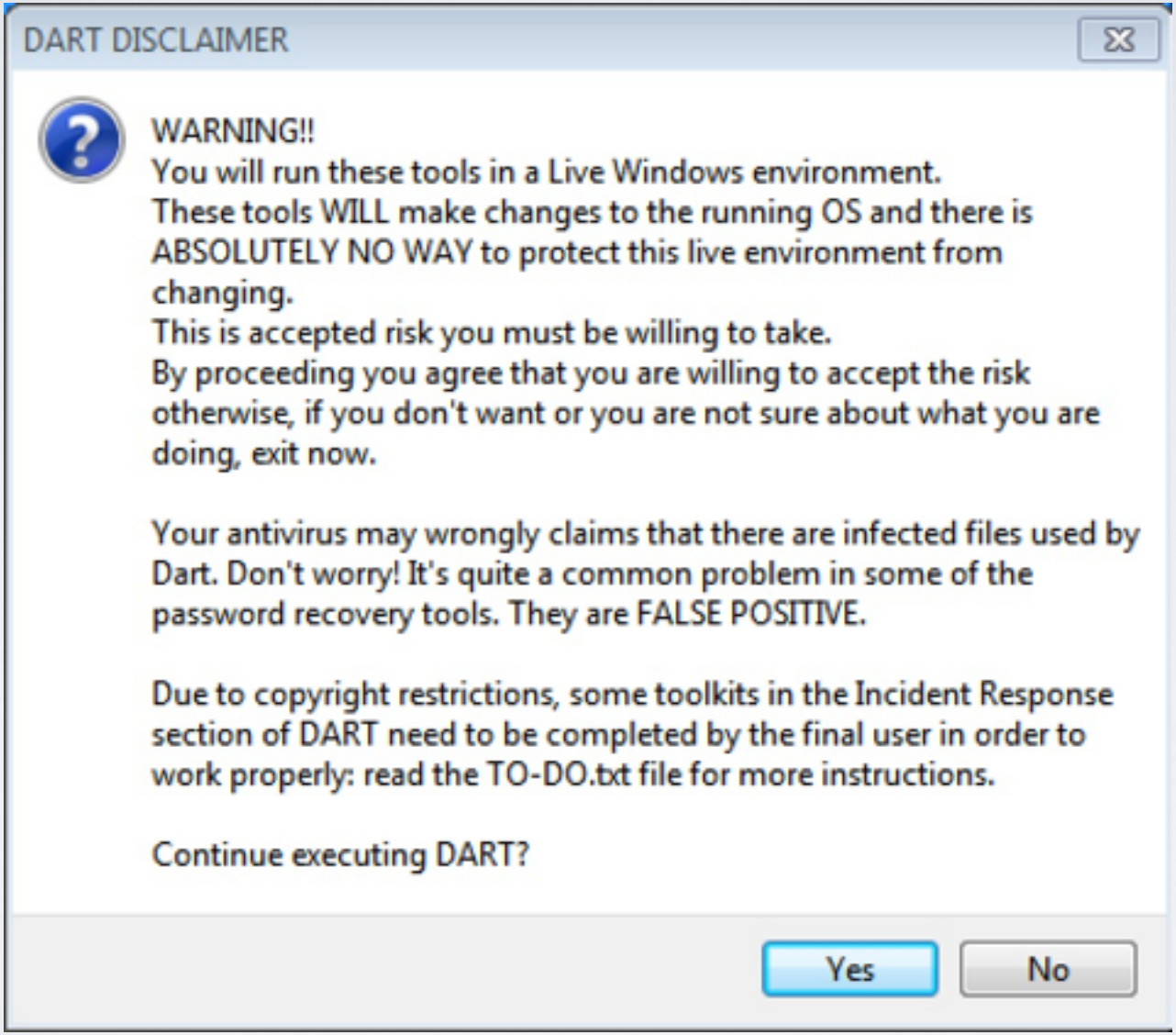
Copyright restrictions…



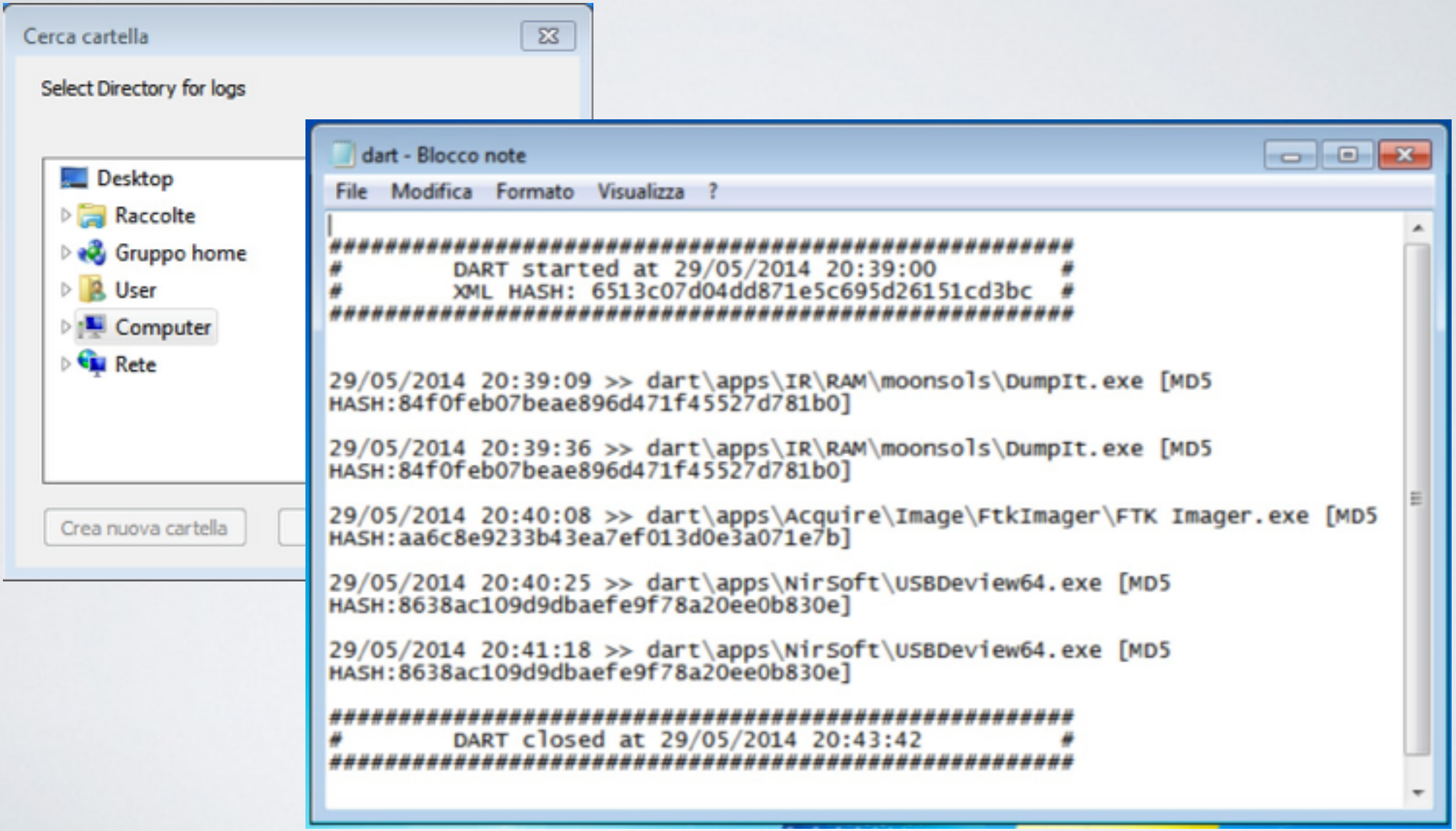
Avvio


Com... ▸ Unità... ▸
Cerca Unità DVD (D:) ...
Organizza
Scrivi su disco
Preferiti
Desktop
Download
Risorse recenti
Raccolte
Documenti
Immagini
File attualmente sul disco (15)
.disk
boot
casper
dart
dists
EFI
install
isolinux
pics
pool
preseed
dart
md5sum
README.diskdefines
TO-DO
Cerca Computer
Unità disco rigido (1)
Disco locale (C:)
94,8 GB disponibile su 119 GB
Dispositivi con archivi rimovibili (2)
Unità disco floppy (A:)
Unità DVD (D:) DEFT_8
0 byte disponibile su 3,04 GB
CDFS
DVD-ROM
Documenti
Immagini
Musica
Video
WIN7PRO Gruppo di lavoro: WORKGROUP
Processore: Intel(R) Core(TM) i7-4558U CPU @ 2.80GHz

Warning


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! It's quite a common problem in some of the password recovery tools. They are FALSE POSITIVE.
Due to copyright restrictions, some toolkits in the Incident Response section of DART need to be completed by the final user in order to work properly: read the TO-DO.txt file for more instructions.
Continue executing DART?
Yes
No

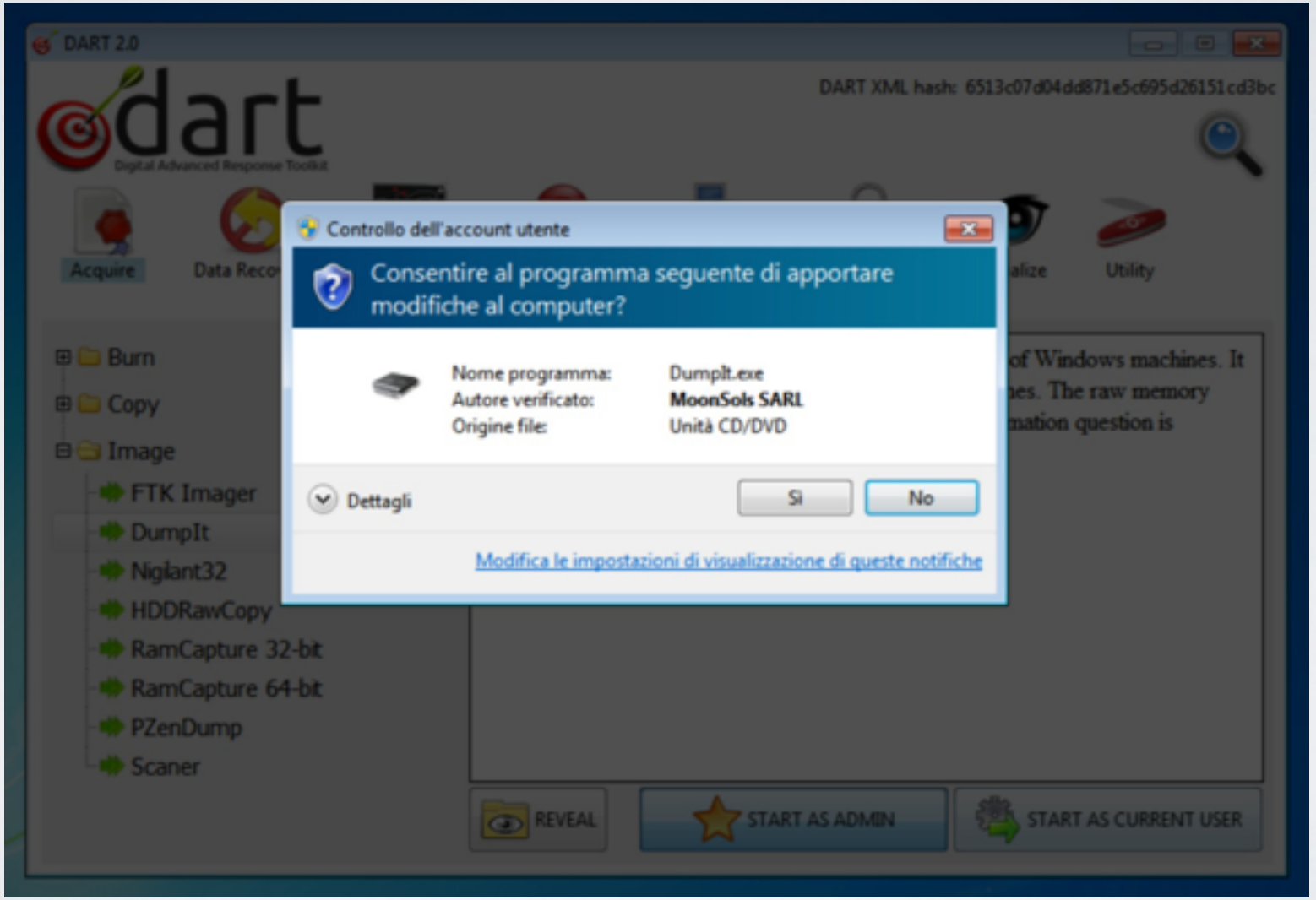
Logs


Cerca cartella
Select Directory for logs
Desktop
Raccolte
Gruppo home
User
Computer
Rete
Crea nuova cartella
dart - Blocco note
File Modifica Formato Visualizza ?
##
DART started at 29/05/2014 20:39:00
XML HASH: 6513c07d04dd871e5c695d26151cd3bc
##
29/05/2014 20:39:09 >> dart\apps\IR\RAM\moonsols\DumpIt.exe [MD5 HASH:84f0feb07beae896d471f45527d781b0]
29/05/2014 20:39:36 >> dart\apps\IR\RAM\moonsols\DumpIt.exe [MD5 HASH:84f0feb07beae896d471f45527d781b0]
29/05/2014 20:40:08 >> dart\apps\Acquire\Image\FtkImager\FTK Imager.exe [MD5 HASH:aa6c8e9233b43ea7ef013d0e3a071e7b]
29/05/2014 20:40:25 >> dart\apps\NirSoft\USBDeview64.exe [MD5 HASH:8638ac109d9dbaefe9f78a20ee0b830e]
29/05/2014 20:41:18 >> dart\apps\NirSoft\USBDeview64.exe [MD5 HASH:8638ac109d9dbaefe9f78a20ee0b830e]
##
DART closed at 29/05/2014 20:43:42
##

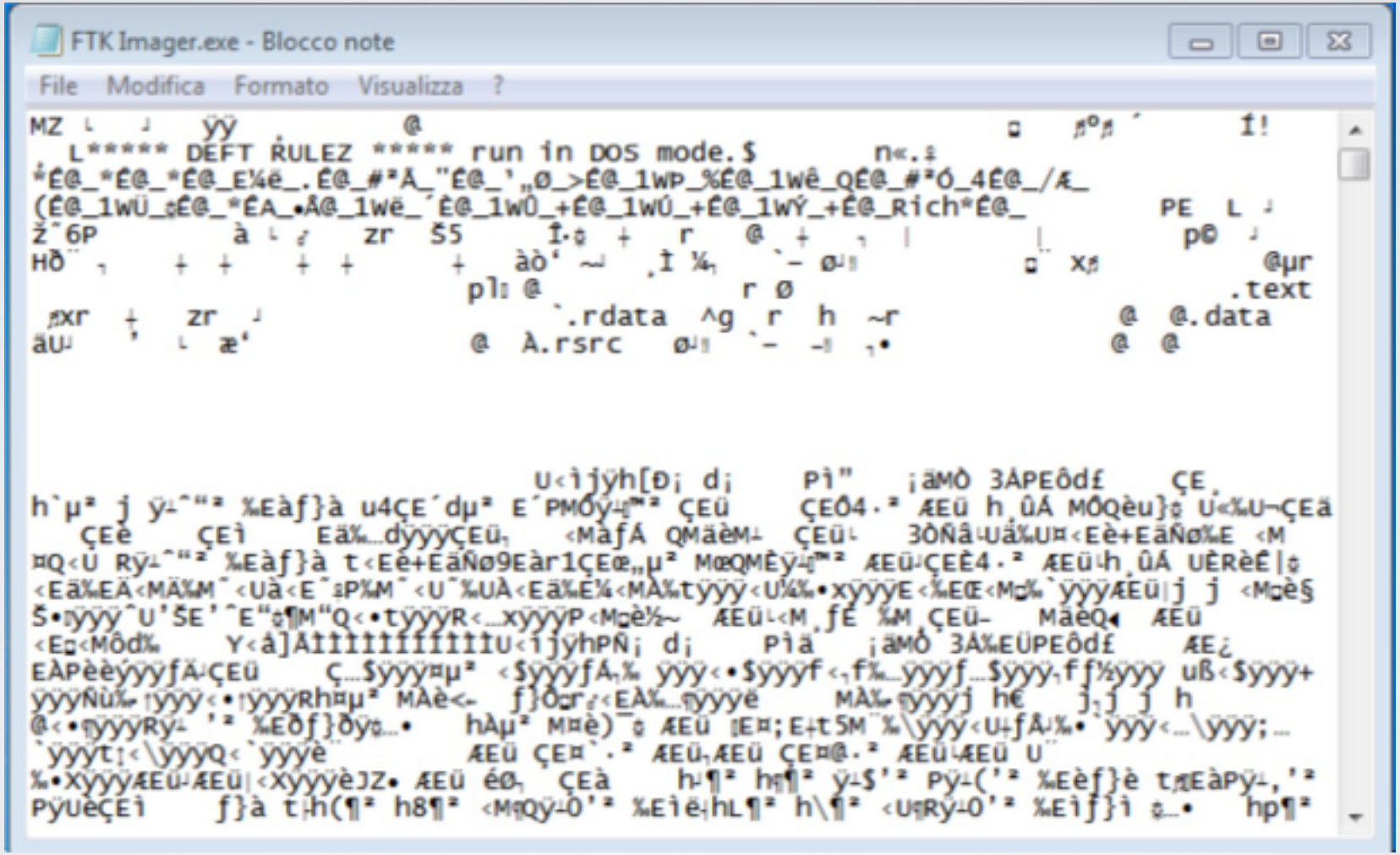
GUI - Launcher

Ricerca veloce

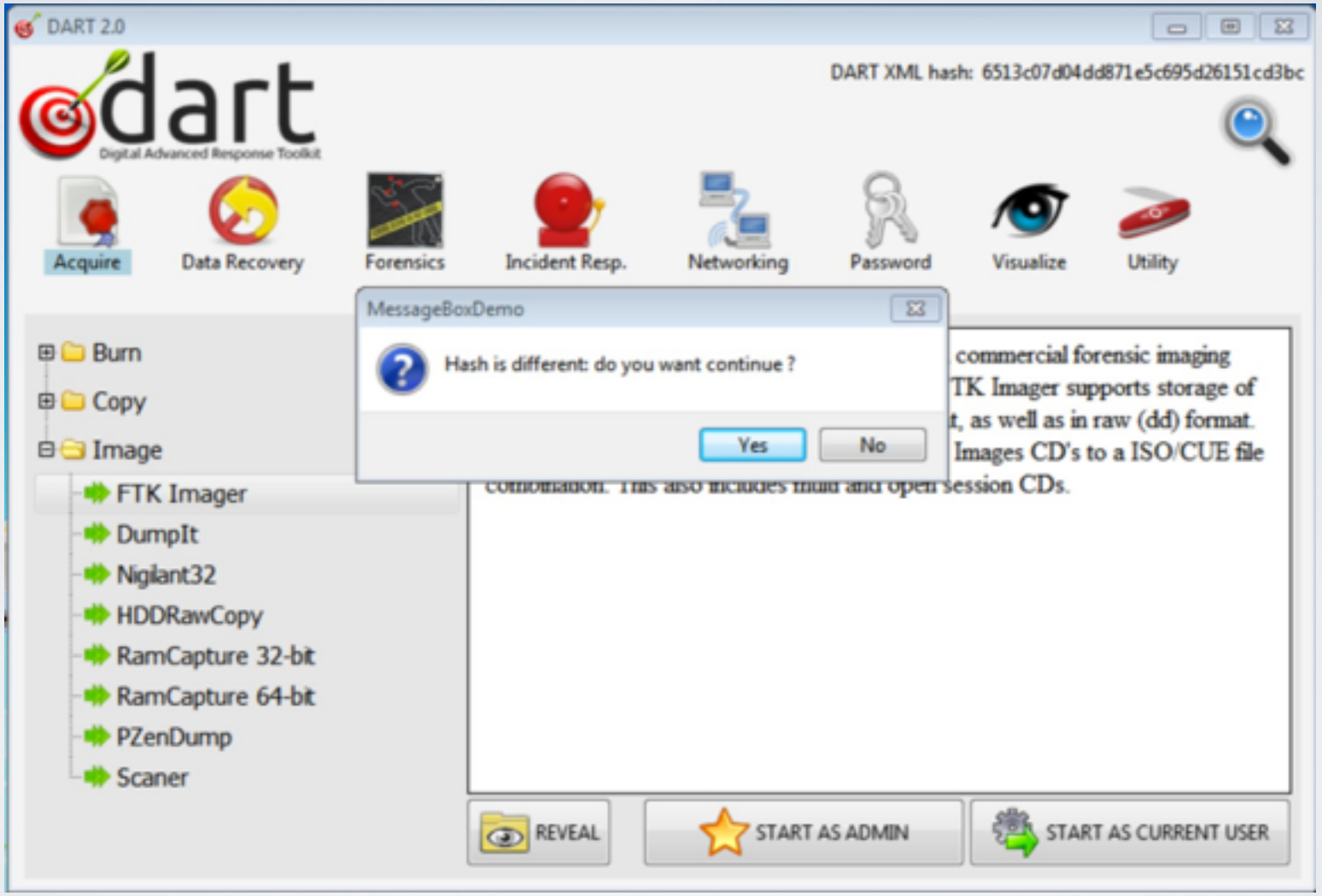
Avvia come admin/current user



Controllo integrità

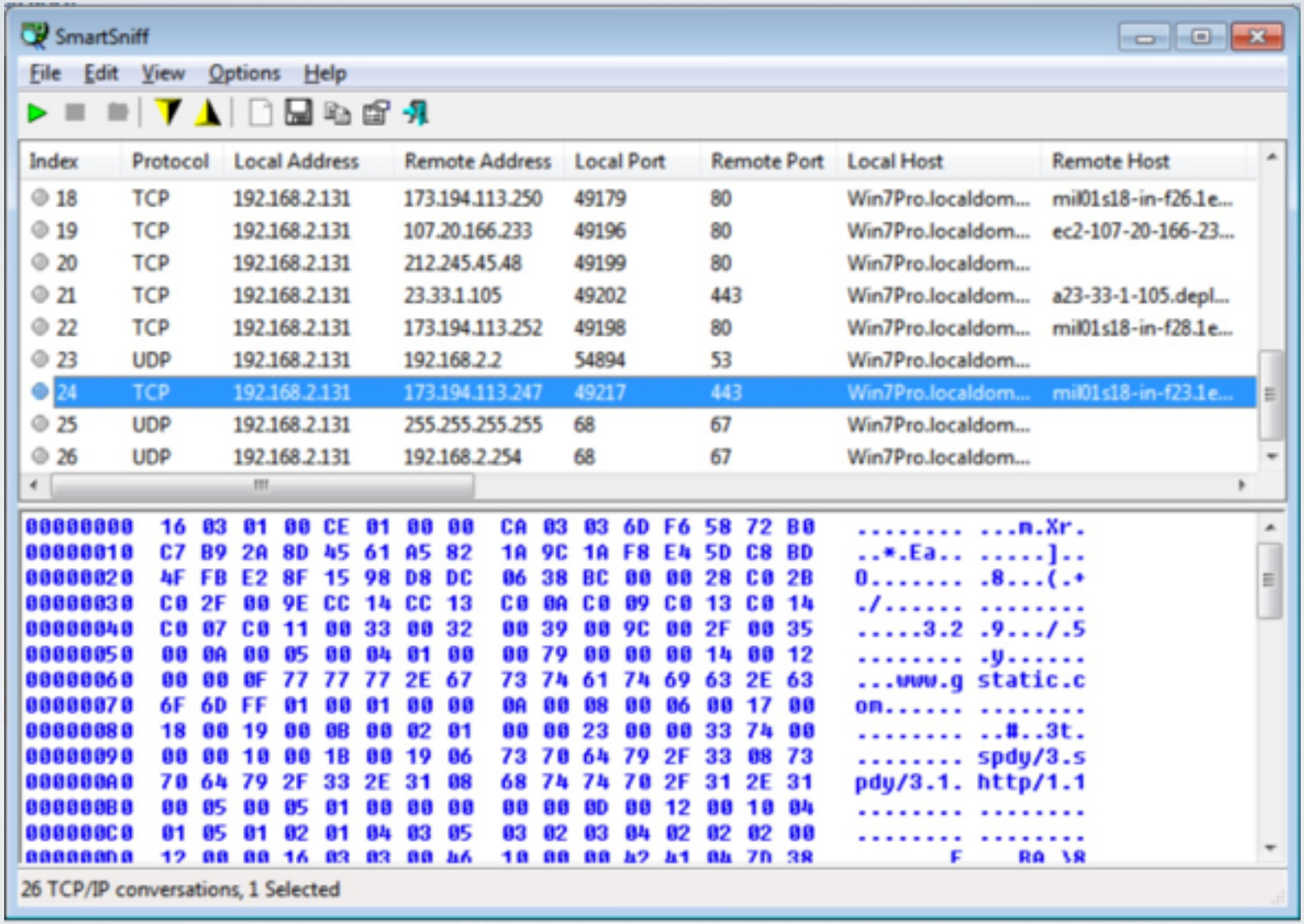


Controllo integrità

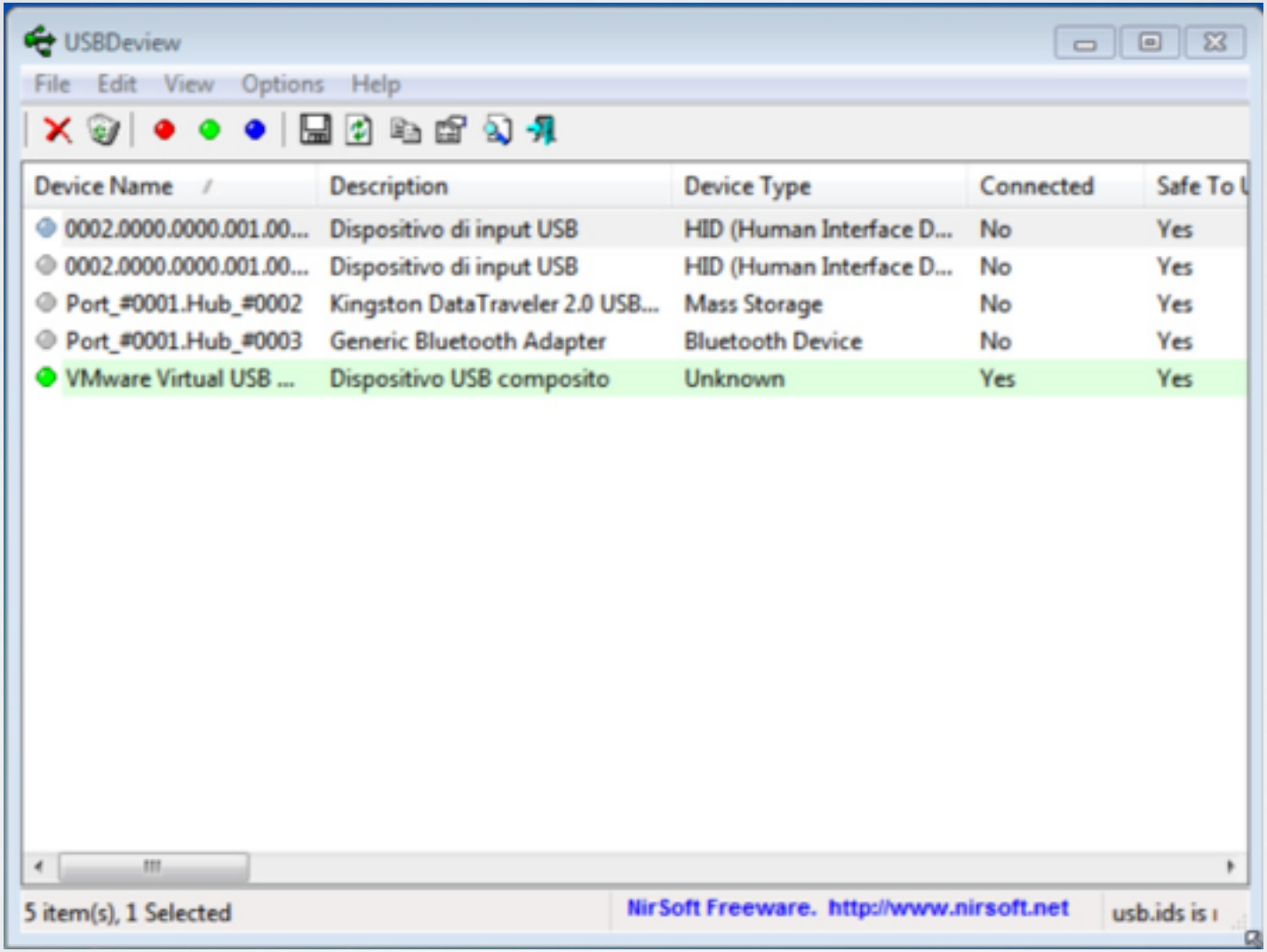


Alcuni esempi

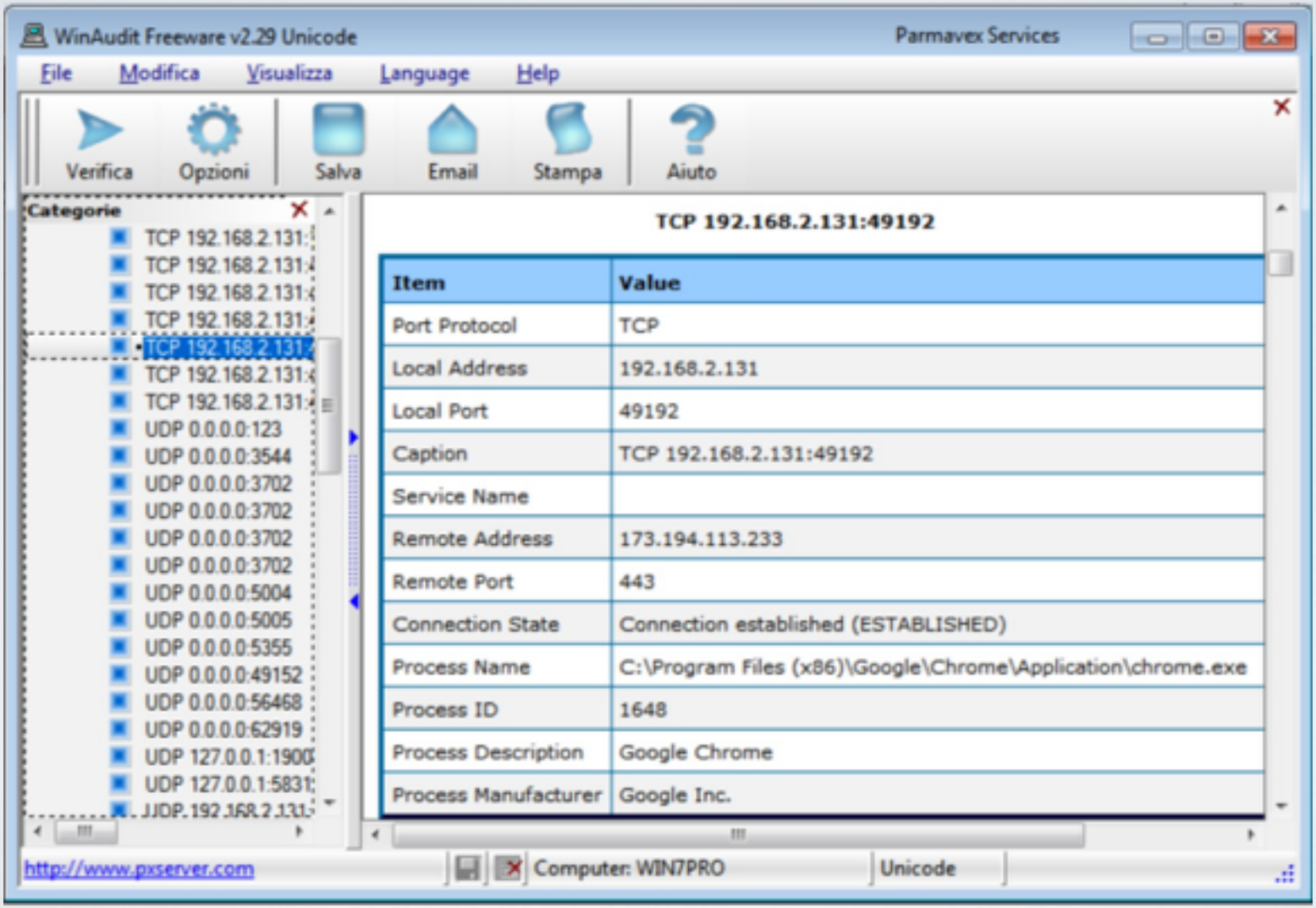
Attività di rete



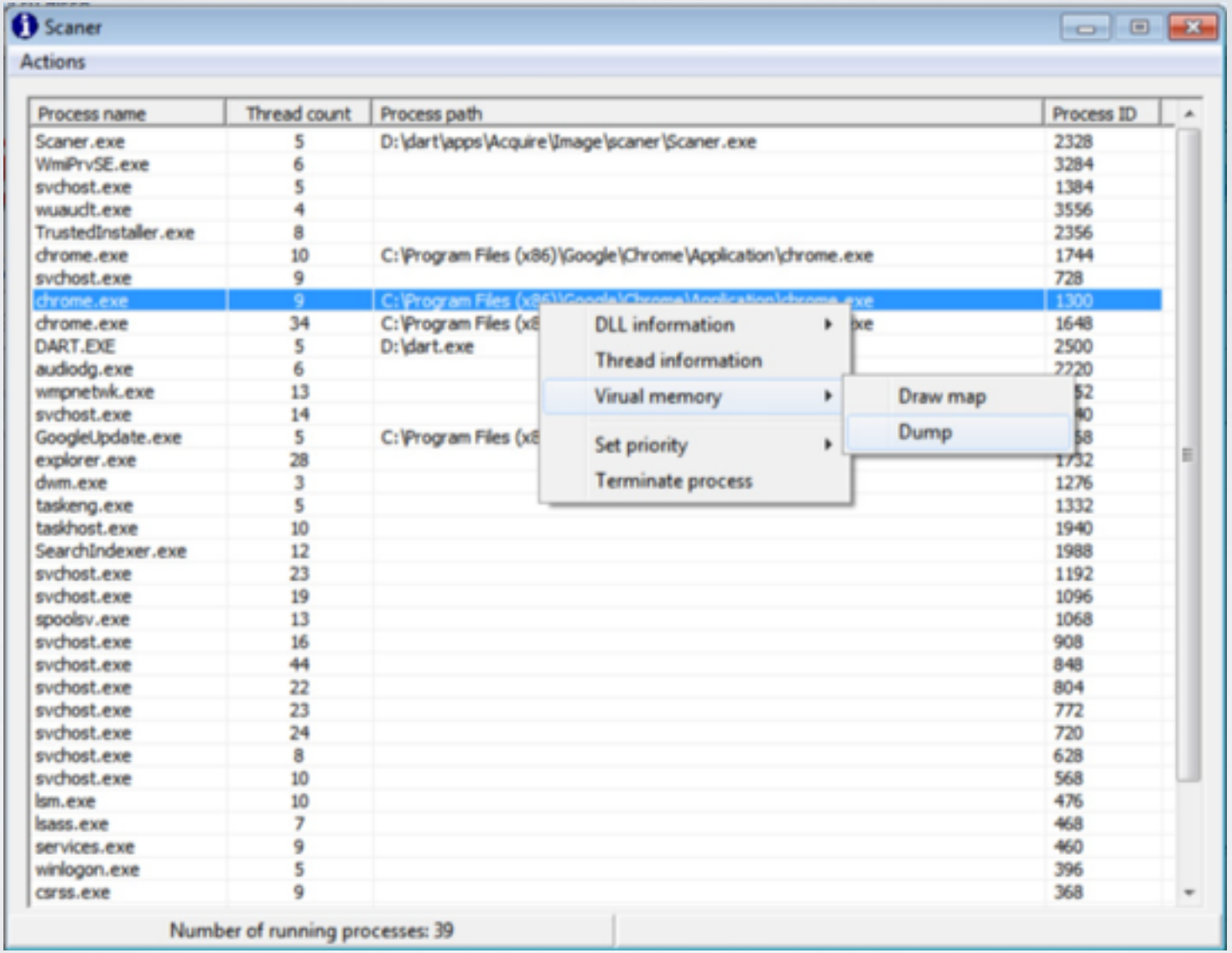
Periferiche USB



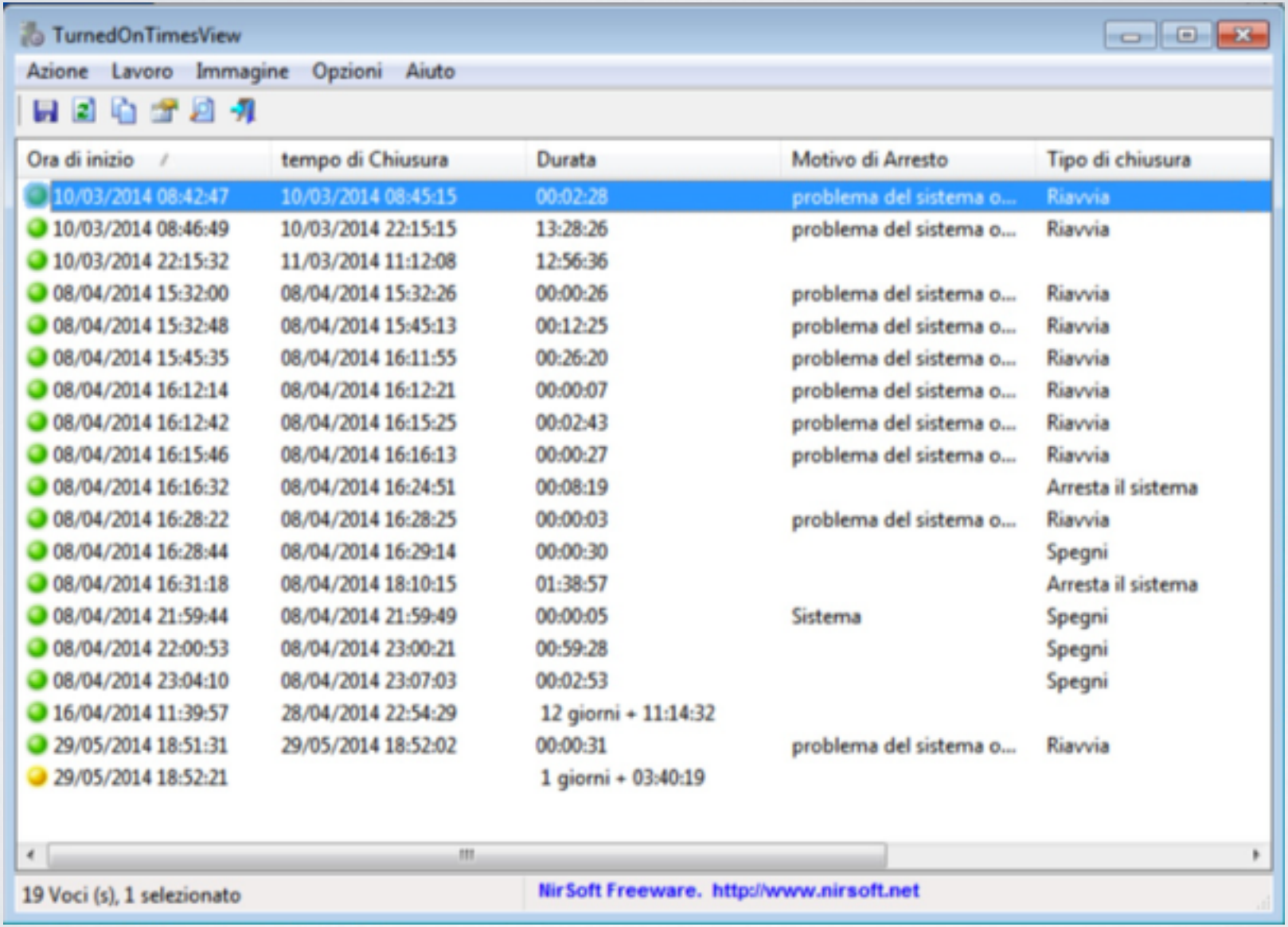
Socket


WinAudit Freeware v2.29 Unicode
Parmavex Services
File
Modifica
Visualizza
Language
Help
Verifica
Opzioni
Salva
Email
Stampa
Aiuto
Categorie
TCP 192.168.2.131:49192
Item
Value
Port Protocol
TCP
Local Address
192.168.2.131
Local Port
49192
Caption
TCP 192.168.2.131:49192
Service Name
Remote Address
173.194.113.233
Remote Port
443
Connection State
Connection established (ESTABLISHED)
Process Name
C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
Process ID
1648
Process Description
Google Chrome
Process Manufacturer
Google Inc.
http://www.pxserver.com
Computer: WIN7PRO
Unicode

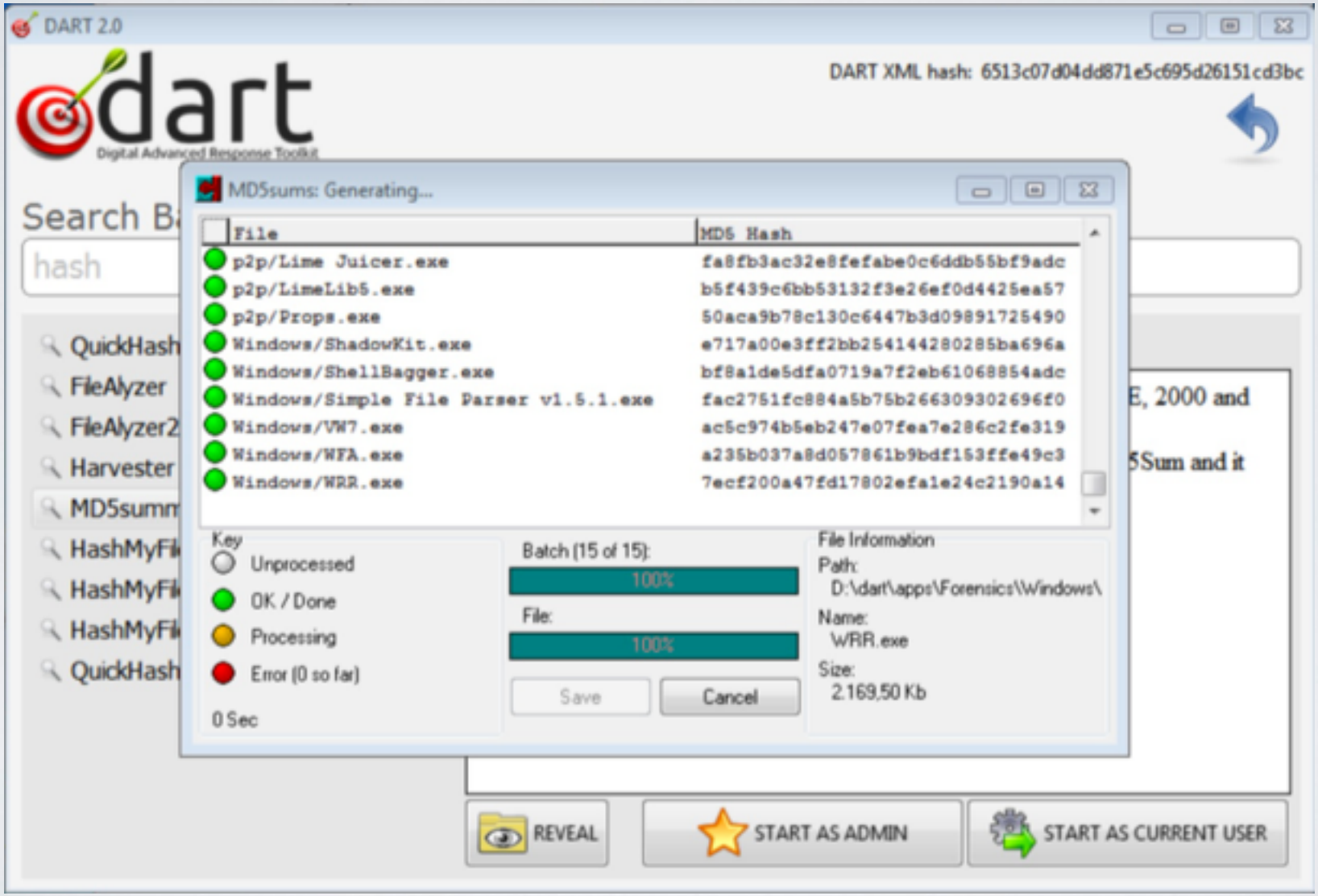
Processi


Scaner
Actions
Process name
Thread count
Process path
Process ID
Scaner.exe 5 D:\dart\apps\Acquire\Image\scaner\Scaner.exe 2328
WmiPrvSE.exe 6 3284
svchost.exe 5 1384
wuaudt.exe 4 3556
TrustedInstaller.exe 8 2356
chrome.exe 10 C:\Program Files (x86)\Google\Chrome\Application\chrome.exe 1744
svchost.exe 9 728
chrome.exe 9 1300
chrome.exe 34 1648
DART.EXE 5 D:\dart.exe 2500
audiodg.exe 6
wmpnetwk.exe 13
svchost.exe 14
GoogleUpdate.exe 5
explorer.exe 28
dwm.exe 3 1276
taskeng.exe 5 1332
taskhost.exe 10 1940
SearchIndexer.exe 12 1988
svchost.exe 23 1192
svchost.exe 19 1096
spoolsv.exe 13 1068
svchost.exe 16 908
svchost.exe 44 848
svchost.exe 22 804
svchost.exe 23 772
svchost.exe 24 720
svchost.exe 8 628
svchost.exe 10 568
lsm.exe 10 476
lsass.exe 7 468
services.exe 9 460
winlogon.exe 5 396
csrss.exe 9 368
DLL information
Thread information
Virual memory
Draw map
Dump
Set priority
Terminate process
Number of running processes: 39

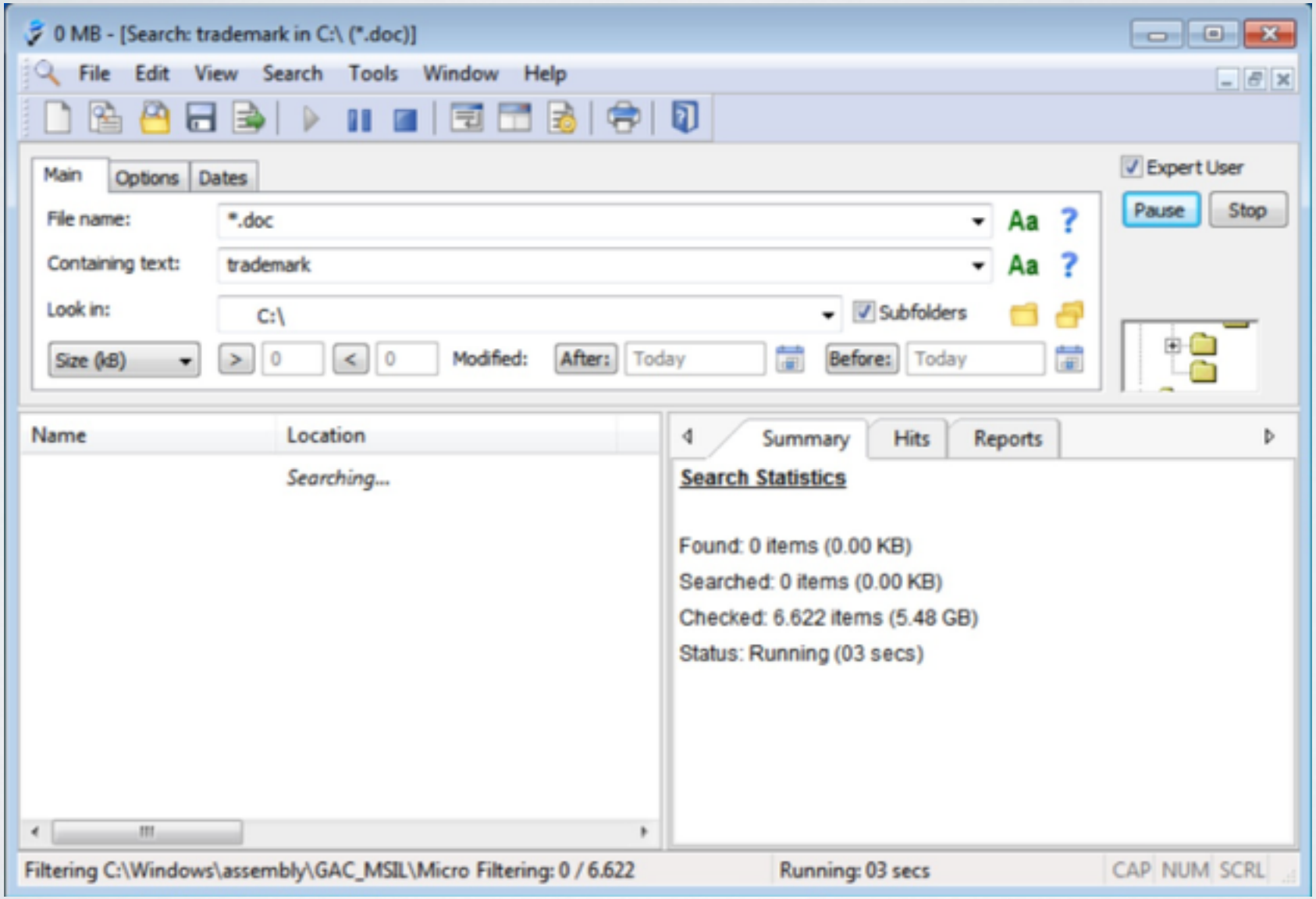
Avvio e spegnimento



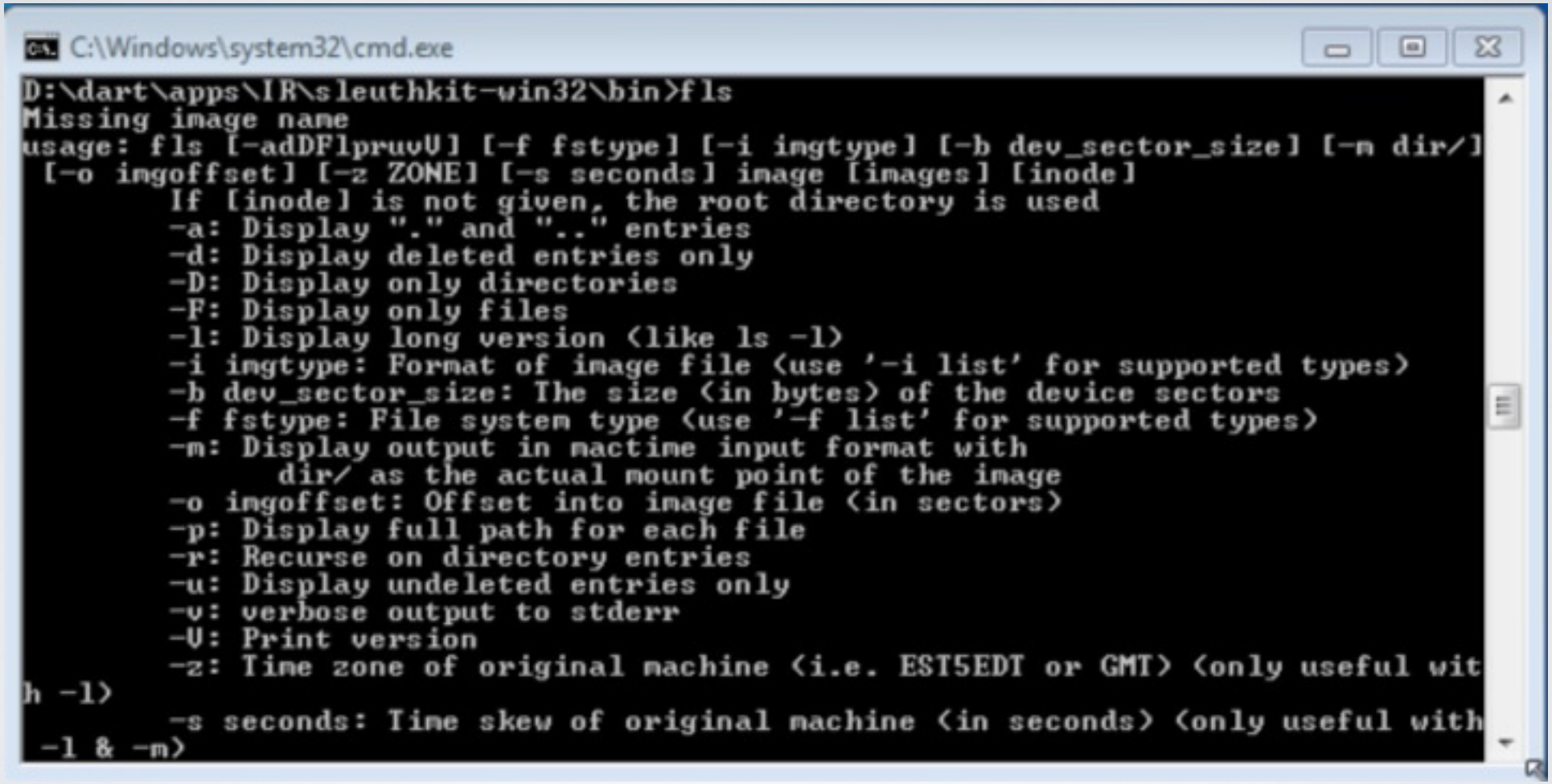
Hash


DART 2.0
dart
Digital Advanced Response Toolkit
DART XML hash: 6513c07d04dd871e5c695d26151cd3bc
MD5sums: Generating...
File
MD5 Hash
p2p/Lime Juicer.exe fa8fb3ac32e8fefabe0c6ddb55bf9adc
p2p/LimeLib5.exe b5f439c6bb53132f3e26ef0d4425ea57
p2p/Props.exe 50aca9b78c130c6447b3d09891725490
Windows/ShadowKit.exe e717a00e3ff2bb254144280285ba696a
Windows/ShellBagger.exe bf8a1de5dfa0719a7f2eb61068854adc
Windows/Simple File Parser v1.5.1.exe fac2751fc884a5b75b26630930269 6f0
Windows/VW7.exe ac5c974b5eb247e07fea7e286c2fe319
Windows/WFA.exe a235b037a8d057861b9bdf153ffe49c3
Windows/WRR.exe 7ecf200a47fd17802efa1e24c2190a14
Key
Unprocessed
OK / Done
Processing
Error (0 so far)
0 Sec
Batch (15 of 15):
100%
File:
100%
Save
Cancel
File Information
Path:
D:\dart\apps\Forensics\Windows\
Name:
WRR.exe
Size:
2.169,50 Kb
Search Ba
hash
QuickHash
FileAlyzer
FileAlyzer2
Harvester
MD5summ
HashMyFi
HashMyFi
HashMyFi
QuickHash
E, 2000 and
5Sum and it
REVEAL
START AS ADMIN
START AS CURRENT USER

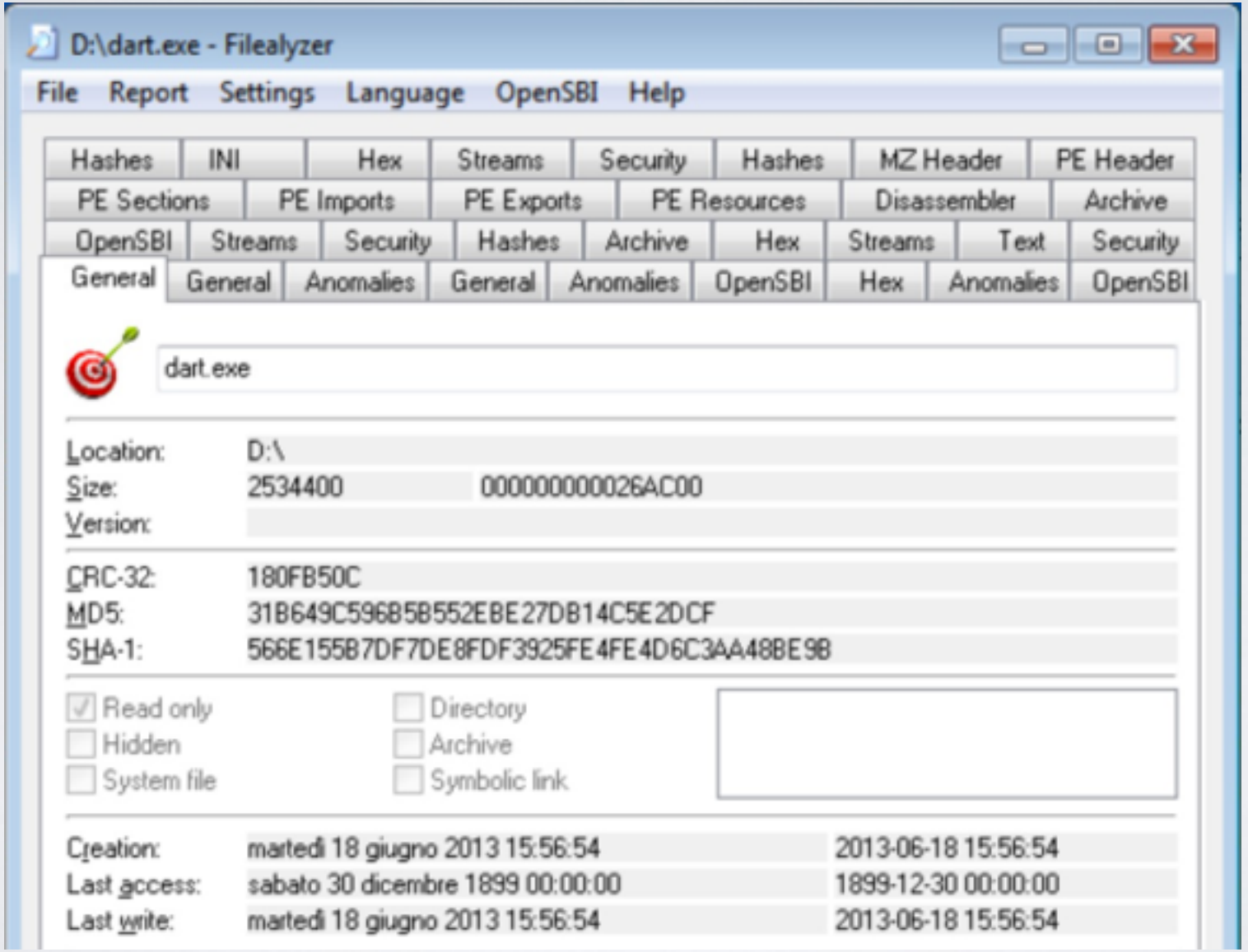
Ricerca avanzata su file



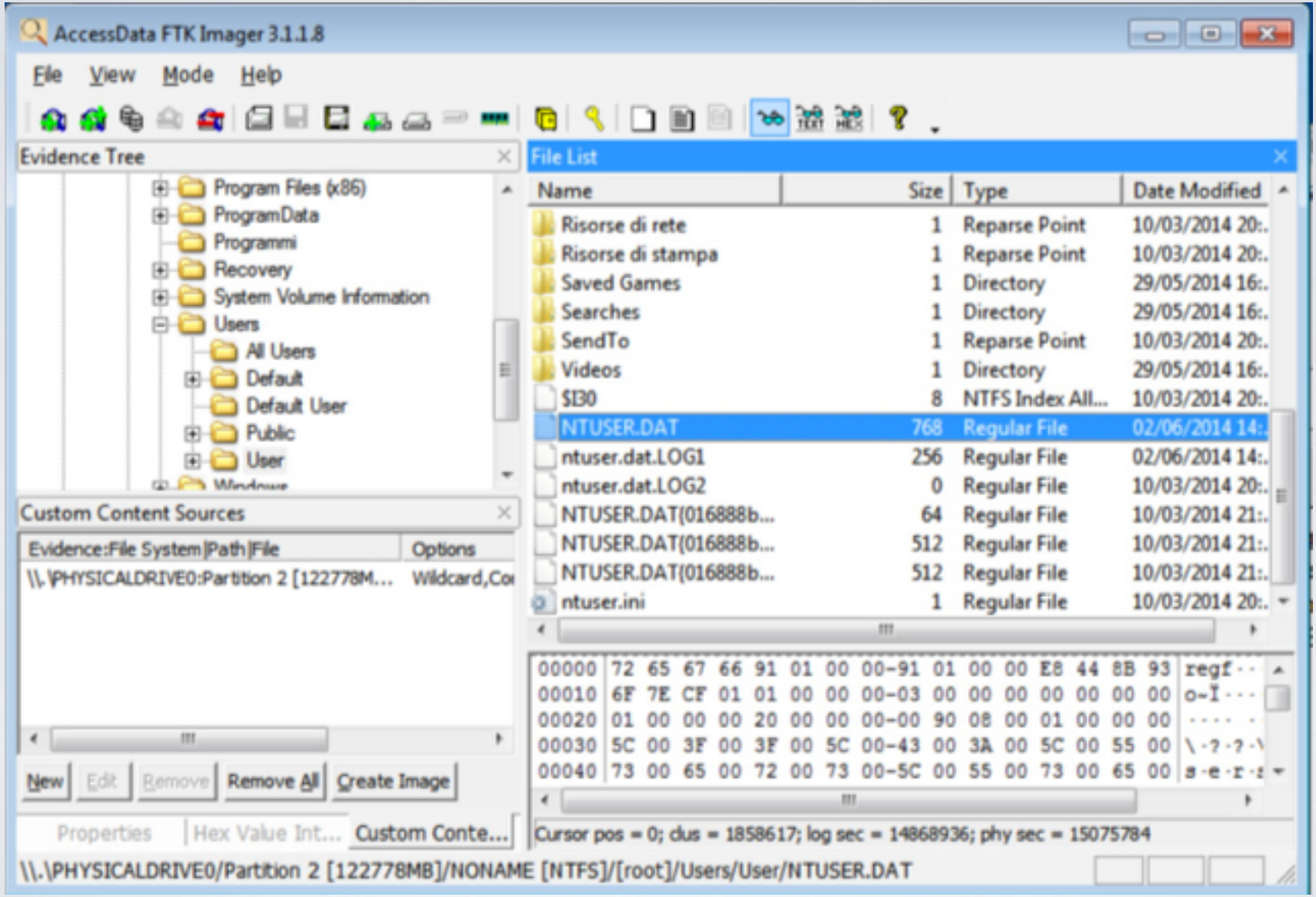
Timeline


C:\Windows\system32\cmd.exe
D:\dart\apps\IR\sleuthkit-win32\bin>fls
Missing image name
usage: fls [-adDFlpruvV] [-f fstype] [-i imgtype] [-b dev_sector_size] [-m dir/]
[-o imgoffset] [-z ZONE] [-s seconds] image [images] [inode]
If [inode] is not given, the root directory is used
-a: Display "." and ".." entries
-d: Display deleted entries only
-D: Display only directories
-F: Display only files
-l: Display long version (like ls -l)
-i imgtype: Format of image file (use '-i list' for supported types)
-b dev_sector_size: The size (in bytes) of the device sectors
-f fstype: File system type (use '-f list' for supported types)
-m: Display output in mactime input format with
dir/ as the actual mount point of the image
-o imgoffset: Offset into image file (in sectors)
-p: Display full path for each file
-r: Recurse on directory entries
-u: Display undeleted entries only
-v: verbose output to stderr
-V: Print version
-z: Time zone of original machine (i.e. EST5EDT or GMT) (only useful wit
h -l)
-s seconds: Time skew of original machine (in seconds) (only useful with
-l & -m)

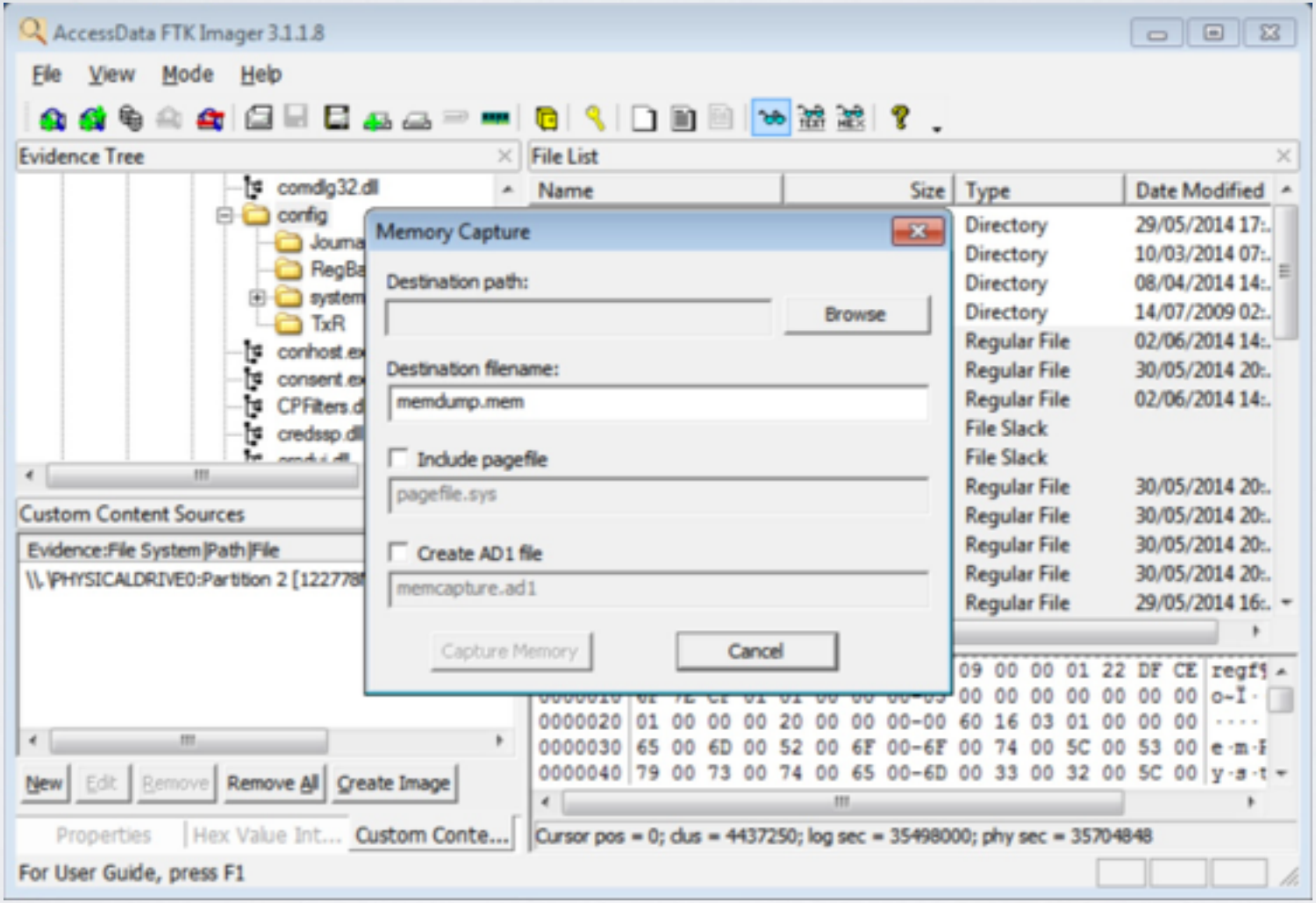
File analysis



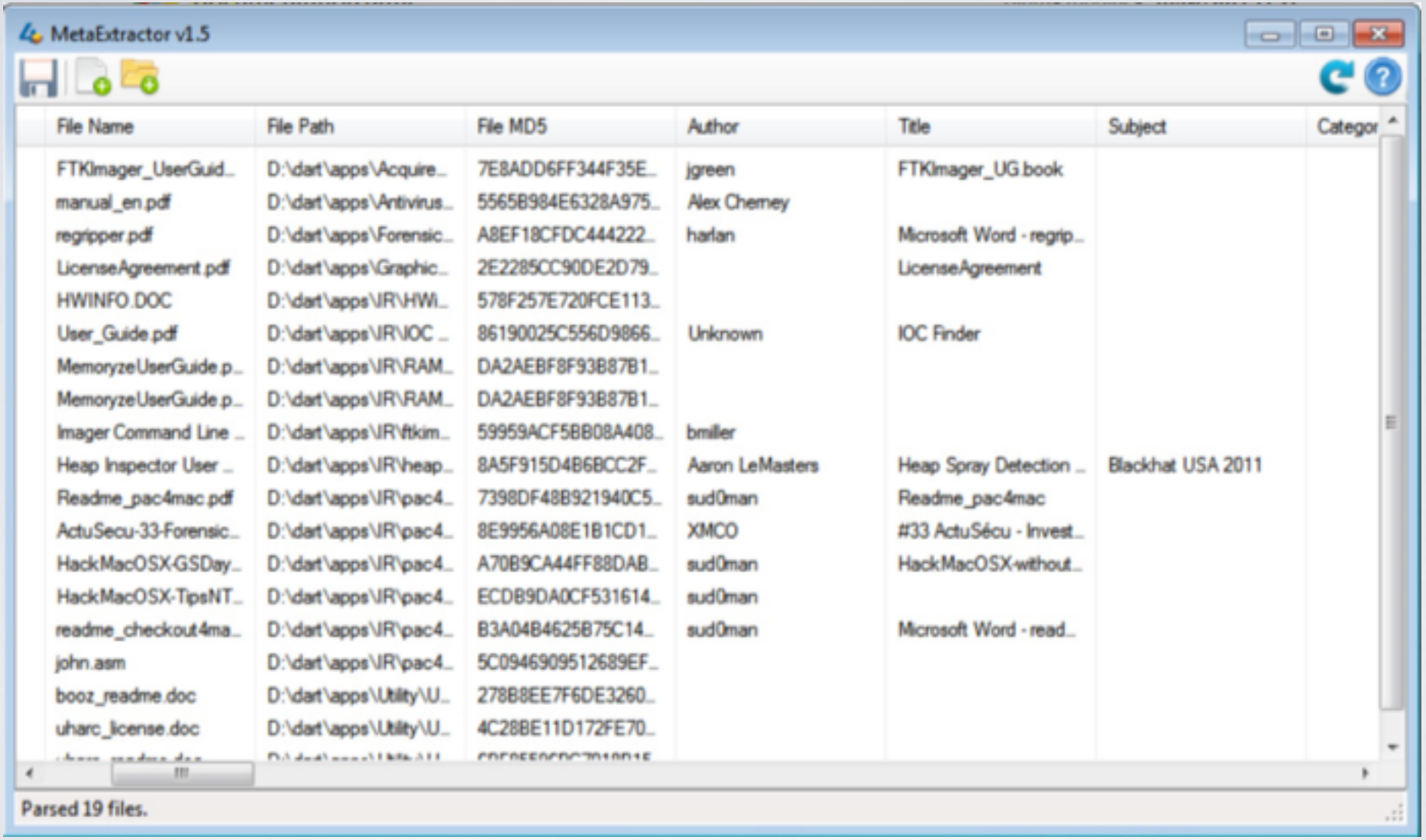
Disk/Folder Image



RAM Dump


AccessData FTK Imager 3.1.1.8
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Memory Capture
Destination path:
Browse
Destination filename:
memdump.mem
Include pagefile
pagefile.sys
Create AD1 file
memcapture.ad1
Capture Memory
Cancel
Custom Content Sources
Evidence:File System|Path|File
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Cursor pos = 0; clus = 4437250; log sec = 35498000; phy sec = 35704848
For User Guide, press F1

Metadati


MetaExtractor v1.5
File Name
File Path
File MD5
Author
Title
Subject
Categor
FTKImager_UserGuid...
D:\dart\apps\Acquire...
7E8ADD6FF344F35E...
jgreen
FTKImager_UG.book
manual_en.pdf
D:\dart\apps\Antivirus...
5565B984E6328A975...
Alex Cherney
regripper.pdf
D:\dart\apps\Forensic...
A8EF18CFDC444222...
harlan
Microsoft Word - regrip...
LicenseAgreement.pdf
D:\dart\apps\Graphic...
2E2285CC90DE2D79...
LicenseAgreement
HWINFO.DOC
D:\dart\apps\IR\HWi...
578F257E720FCE113...
User_Guide.pdf
D:\dart\apps\IR\IOC ...
86190025C556D9866...
Unknown
IOC Finder
MemoryzeUserGuide.p...
D:\dart\apps\IR\RAM...
DA2AEBF8F93B87B1...
MemoryzeUserGuide.p...
D:\dart\apps\IR\RAM...
DA2AEBF8F93B87B1...
Imager Command Line ...
D:\dart\apps\IR\ftkim...
59959ACF5BB08A408...
bmiller
Heap Inspector User ...
D:\dart\apps\IR\heap...
8A5F915D4B6BCC2F...
Aaron LeMasters
Heap Spray Detection ...
Blackhat USA 2011
Readme_pac4mac.pdf
D:\dart\apps\IR\pac4...
7398DF48B921940C5...
sud0man
Readme_pac4mac
ActuSecu-33-Forensic...
D:\dart\apps\IR\pac4...
8E9956A08E1B1CD1...
XMCO
#33 ActuSécu - Invest...
HackMacOSX-GSDay...
D:\dart\apps\IR\pac4...
A70B9CA44FF88DAB...
sud0man
HackMacOSX-without...
HackMacOSX-TipsNT...
D:\dart\apps\IR\pac4...
ECDB9DA0CF531614...
sud0man
readme_checkout4ma...
D:\dart\apps\IR\pac4...
B3A04B4625B75C14...
sud0man
Microsoft Word - read...
john.asm
D:\dart\apps\IR\pac4...
5C0946909512689EF...
booz_readme.doc
D:\dart\apps\Utility\U...
278B8EE7F6DE3260...
uharc_license.doc
D:\dart\apps\Utility\U...
4C28BE11D172FE70...
Parsed 19 files.

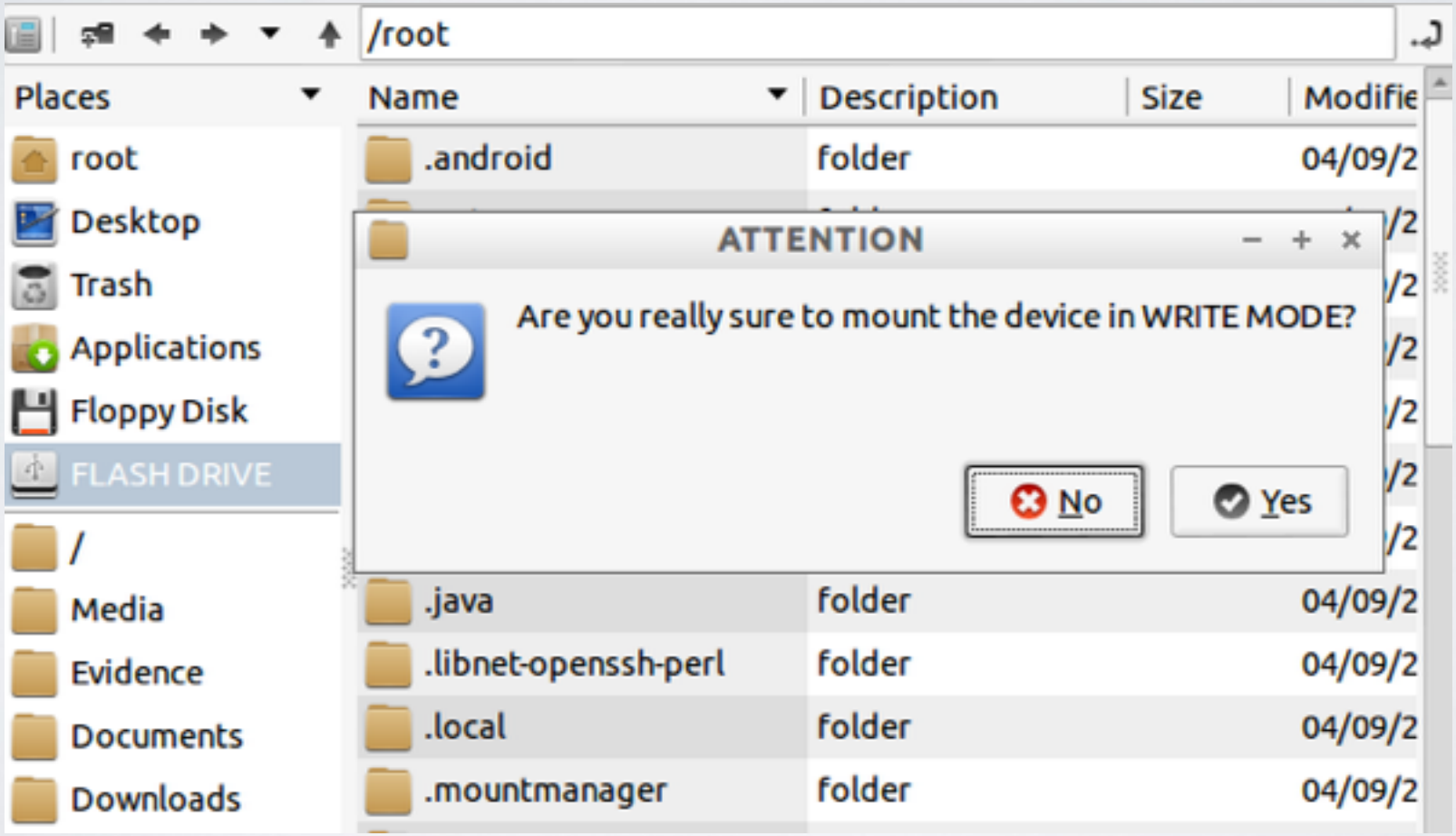
DART
Futuri sviluppi

- Launcher grafico anche per Linux e Mac
- Creazione di un repository su server DEFT
- Funzioni di aggiornamento e autocompletamento del pacchetto
- Rilascio riservato Law Enforcement con software dedicati
- Localizzazione in italiano

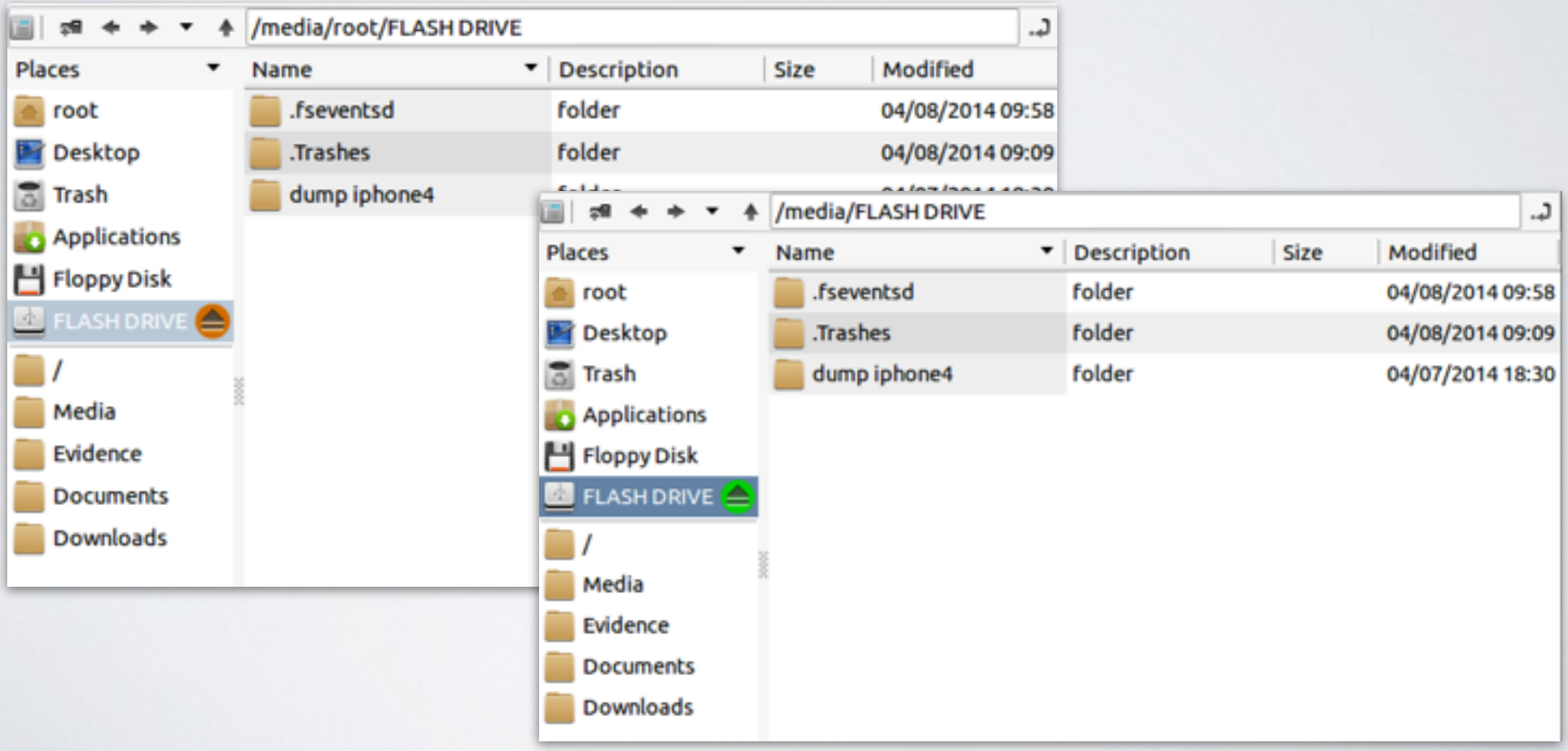
Ma non dimentichiamo la DEFT Linux side

- UBUNTU Linux based
- Deve essere avviata al boot via DVD o USB
- Ideale per eseguire copie forensi o triage
- Toolkit per acquisizione e analisi (timeline, metadati, supertimeline, registro, eventi, etc…)

Mount read-only delle periferiche



Mount read-only delle periferiche



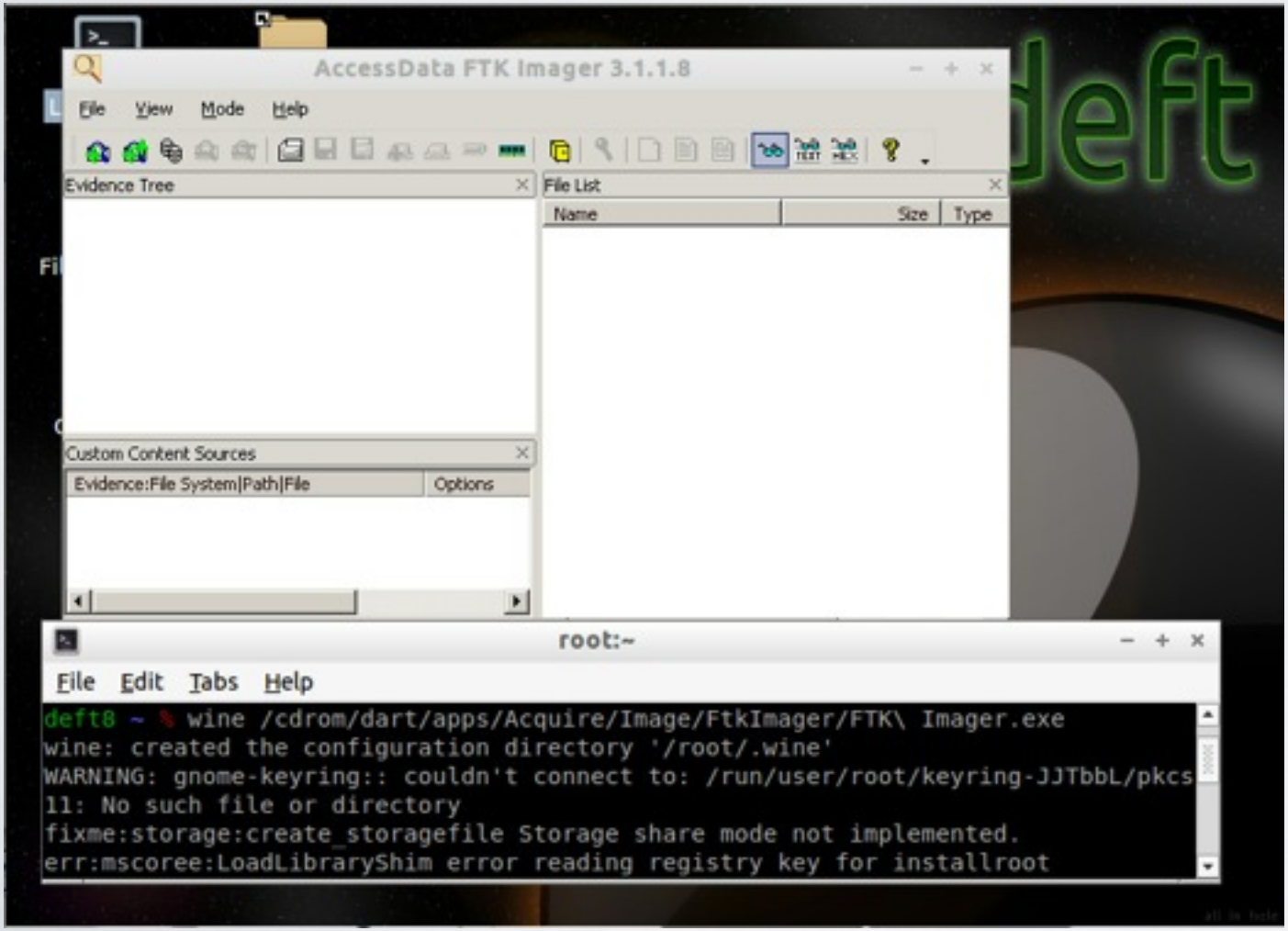
Solo per Law Enforcement ed enti governativi

deft

- The Sleuthkit 4.1.3
- Digital Forensics Framework 1.3
- Implementato il supporto a Bitlocker - libbde
- Mobile Forensics, Android & iOS
- Skype Extractor
- Osint Browser
- Maltego Thungsten
- Centinaia di tool

deft

E⁹ possibile eseguire applicazioni di DART anche su Linux

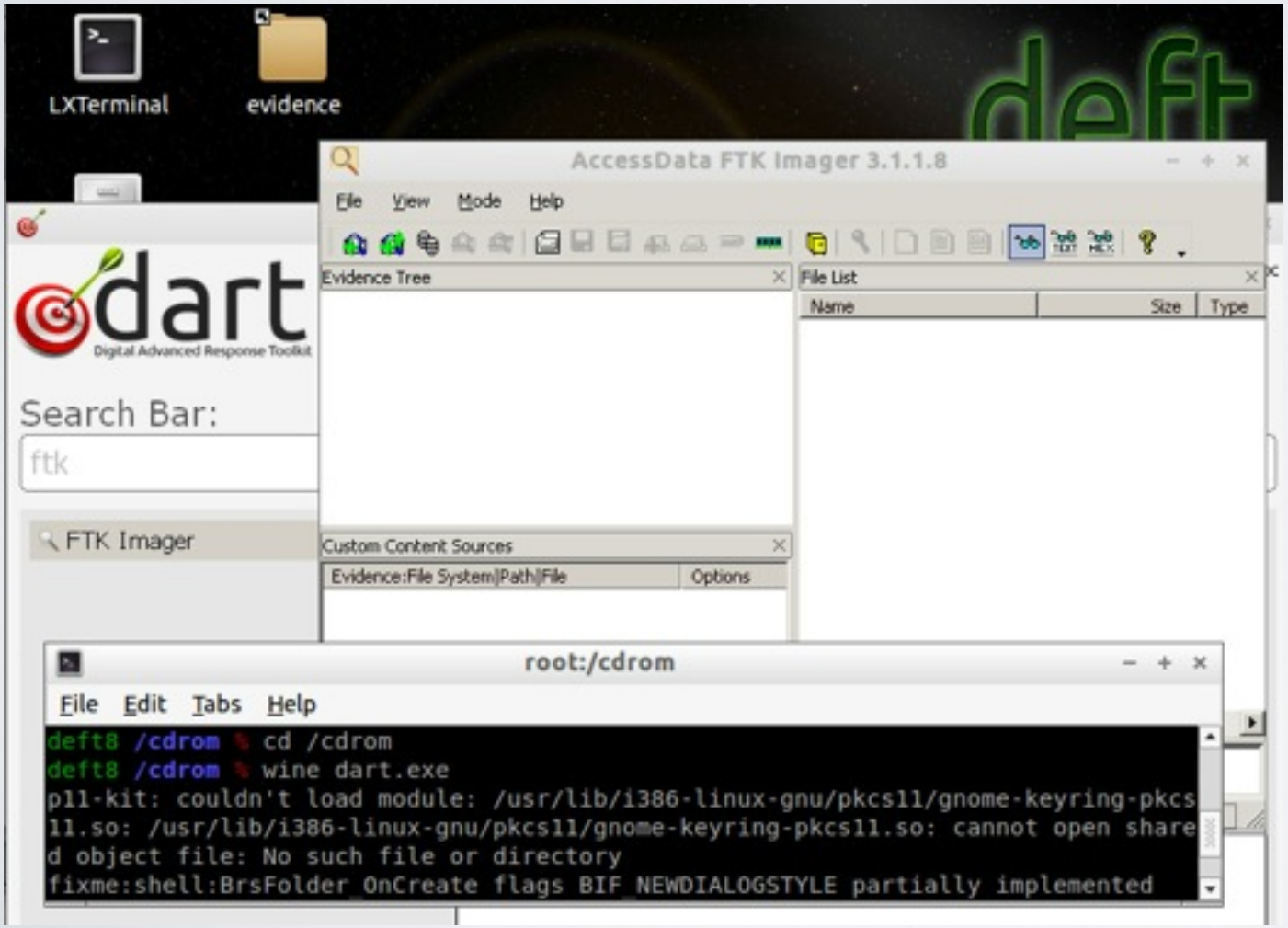


Lanciando i singoli exe

% wine /cdrom/dart/apps/Acquire/FtkImager/Ftk Imager.exe

deft

E' possibile eseguire applicazioni di DART anche su Linux



Tramite DART

% cd /cdrom

% wine dart.exe

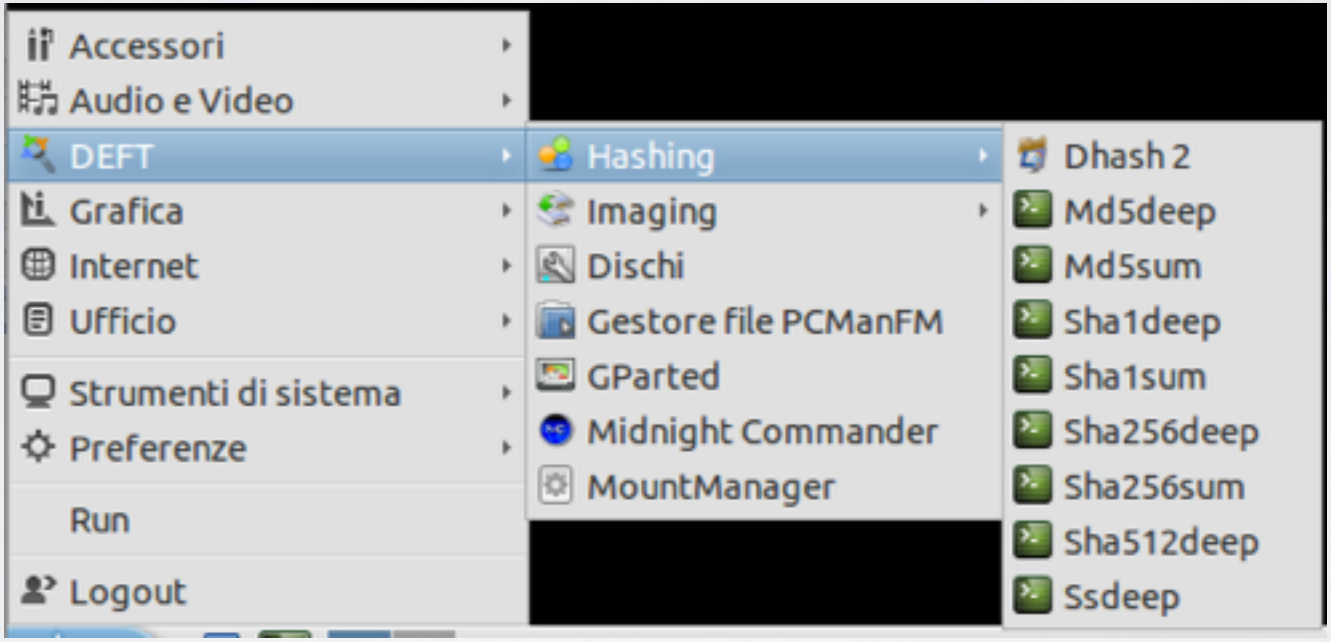
deft zero

SUGAR FREE

- Basato su Lubuntu 13.10 x86 - EFI
- La solidità di deft 8 in una nuova release di soli 400 MB di Iso
- Ottimizzato per le sole acquisizioni
  - Guymager, command line tool

deft zero

SUGAR FREE



Usi noti di DEFT e DART

Grazie per l'attenzione!

Domande?

www.dalchecco.it / paolo@dalchecco.it / @forensico

www.difob.it / pdc@difob.it / @studiodifob