

Hunchbacked Foremost HB4most

File carving made easy

Un'interfaccia grafica per i piu' utilizzati
programmi di ricerca di file



DEFT Conference 2012



Argomenti trattati

Introduzione a HB4most

File carving

- Foremost
- Scalpel
- Altri tool

HB4most

- Implementazione

La Banda Bassotti

- Come ci siamo conosciuti
- Progetti futuri: SQLite, text search, ...



File carving

Il carving consente la ricerca di file, anche cancellati o nascosti, da un disco o un'immagine

Foremost

- Il piu' noto programma di carving
- Sviluppato da agenti del Air Force Office of Special Investigations e disponibile dal 2000
- Permette di specificare il tipo di file da linea di comando

Scalpel

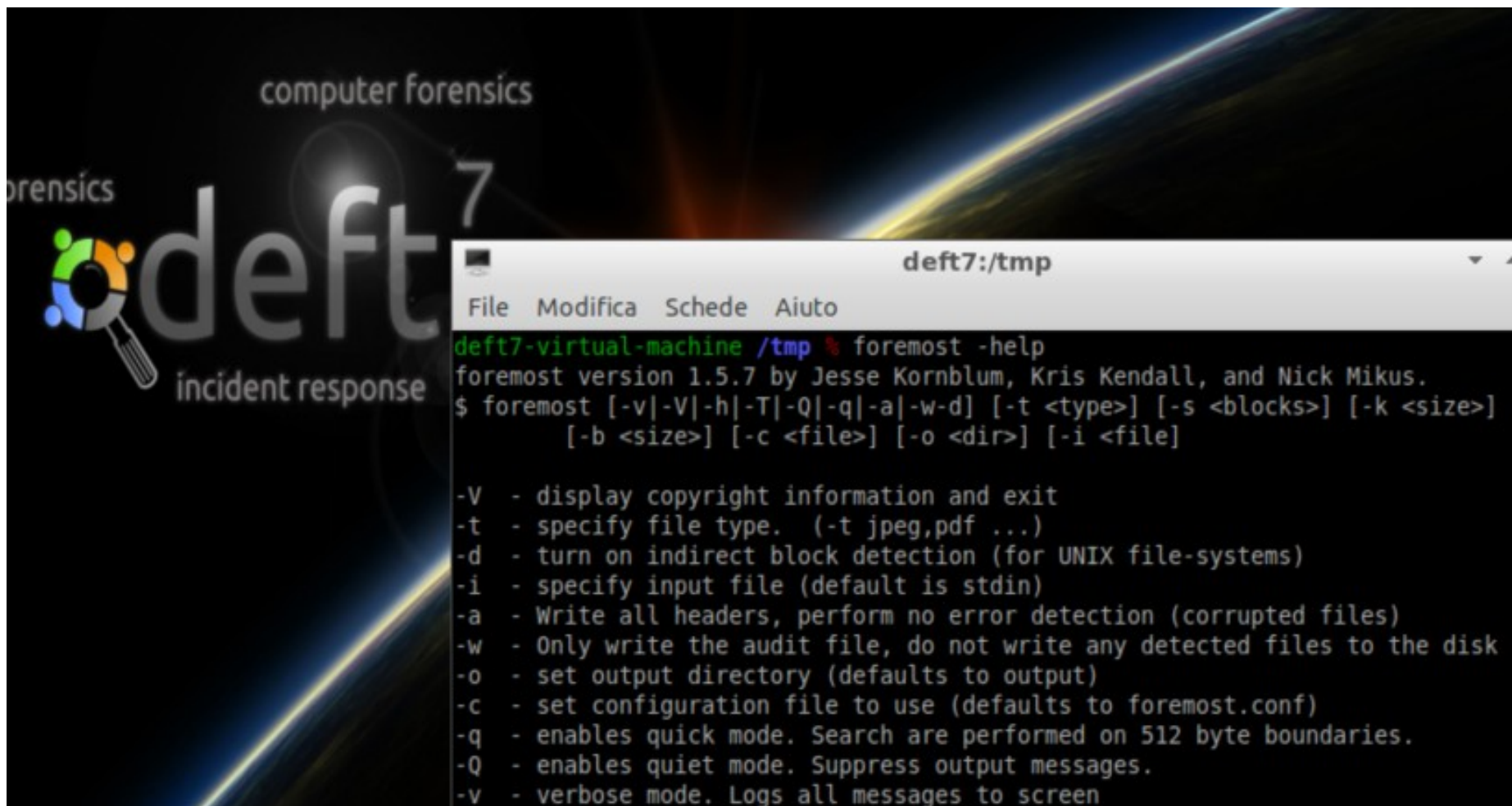
- Nasce come fork da foremost nel 2005
- Spesso piu' veloce di foremost nella ricerca
- Utilizza un file di configurazione come le prime versioni di foremost

Altri

- Sono disponibili molti altri programmi di carving, spesso specializzati su alcune tipologie di file (eg. PhotoRec)



foremost



DEFT Conference 2012



scalpel

```
Scalpel version 2.0
Written by Golden G. Richard III and Lodovico Marziale.
Scalpel carves files or data fragments from a disk image based on a set of
file carving patterns, which include headers, footers, and other information.

Usage: scalpel [-b] [-c <config file>] [-d] [-e] [-h] [-i <file>]
[-n] [-o <outputdir>] [-O] [-p] [-q <clustersize>] [-r]
[-v] [-V] <imgfile> [<imgfile>] ...

Options:
-b Carve files even if defined footers aren't discovered within
  maximum carve size for file type [foremost 0.69 compat mode].
-c Choose configuration file.
-d Generate header/footer database; will bypass certain optimizations
  and discover all footers, so performance suffers. Doesn't affect
  the set of files carved. **EXPERIMENTAL**
-e Do nested header/footer matching, to deal with structured files that may
  contain embedded files of the same type. Applicable only to
  FORWARD / NEXT patterns.
-h Print this help message and exit.
-i Read names of disk images from specified file. Note that minimal parsing of
  the pathnames is performed and they should be formatted to be compliant C
  strings; e.g., under Windows, backslashes must be properly quoted, etc.
-n Don't add extensions to extracted files.
-o Set output directory for carved files.
-O Don't organize carved files by type. Default is to organize carved files
  into subdirectories.
-p Perform image file preview; audit log indicates which files
  would have been carved, but no files are actually carved. Useful for
  indexing file or data fragment locations or supporting in-place file
  carving.
-q Carve only when header is cluster-aligned.
-r Find only first of overlapping headers/footers [foremost 0.69 compat mode].
-V Print copyright information and exit.
-v Verbose mode.
```



DEFT Conference 2012



Hunchbacked Foremost (HB4most)

Hb4most e' un'interfaccia grafica semplice e multilingua per i due piu' diffusi strumenti di carving: **foremost** e **scalpel**

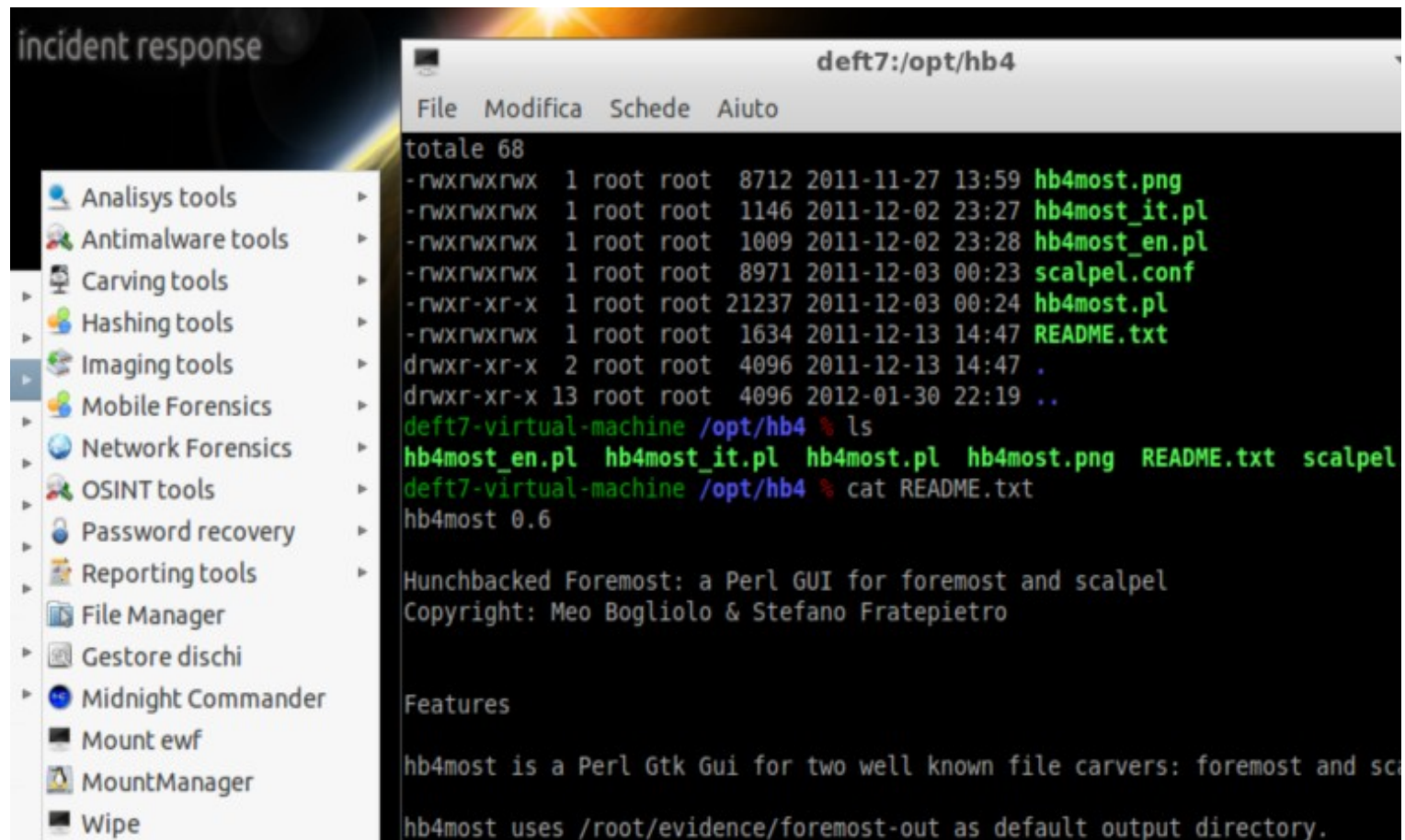
Hb4most e' realizzato in Perl ed utilizza GTK

Hb4most implementa la quasi totalita' delle opzioni di **foremost**

Hb4most consente la semplice modifica del file di configurazione di **scalpel**



hb4most



The screenshot shows the DEFT incident response environment. On the left, a sidebar menu lists various tools, with 'Carving tools' selected. The main window displays a terminal window titled 'deft7:/opt/hb4'. The terminal shows a directory listing of files in the /opt/hb4 directory, including hb4most.png, hb4most_it.pl, hb4most_en.pl, scalpel.conf, hb4most.pl, and README.txt. Below the listing, the terminal shows the output of the 'ls' command and the content of the README.txt file, which describes hb4most as a Perl GUI for foremost and scalpel.

```
deft7:/opt/hb4
File Modifica Schede Aiuto
totale 68
-rwxrwxrwx 1 root root 8712 2011-11-27 13:59 hb4most.png
-rwxrwxrwx 1 root root 1146 2011-12-02 23:27 hb4most_it.pl
-rwxrwxrwx 1 root root 1009 2011-12-02 23:28 hb4most_en.pl
-rwxrwxrwx 1 root root 8971 2011-12-03 00:23 scalpel.conf
-rwxr-xr-x 1 root root 21237 2011-12-03 00:24 hb4most.pl
-rwxrwxrwx 1 root root 1634 2011-12-13 14:47 README.txt
drwxr-xr-x 2 root root 4096 2011-12-13 14:47 .
drwxr-xr-x 13 root root 4096 2012-01-30 22:19 ..
deft7-virtual-machine /opt/hb4 % ls
hb4most_en.pl hb4most_it.pl hb4most.pl hb4most.png README.txt scalpel
deft7-virtual-machine /opt/hb4 % cat README.txt
hb4most 0.6

Hunchbacked Foremost: a Perl GUI for foremost and scalpel
Copyright: Meo Bogliolo & Stefano Fratepietro

Features

hb4most is a Perl Gtk Gui for two well known file carvers: foremost and sc
hb4most uses /root/evidence/foremost-out as default output directory.
```

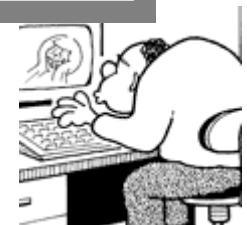
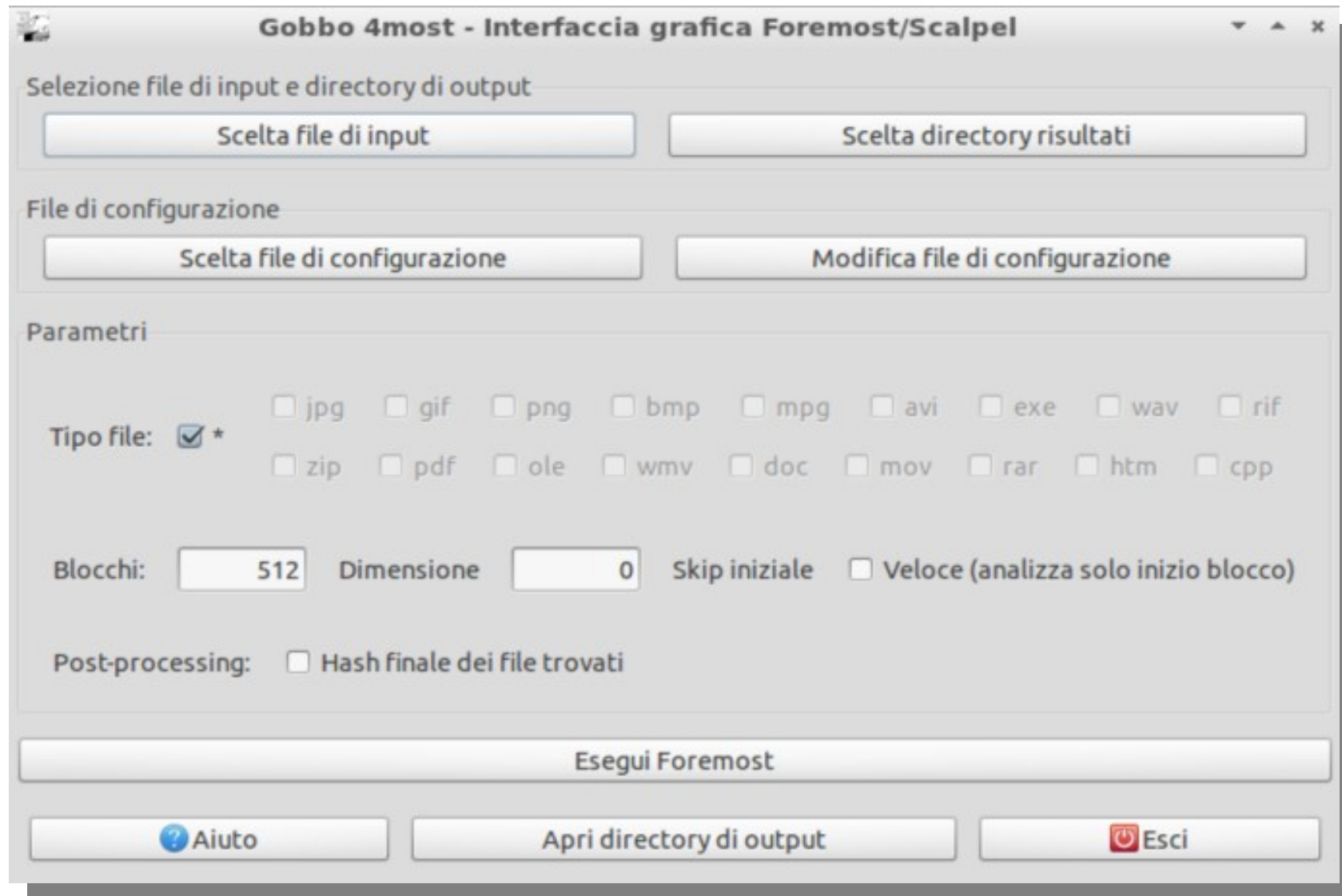
hb4most si richiama dal menu DEFT – Carving tools



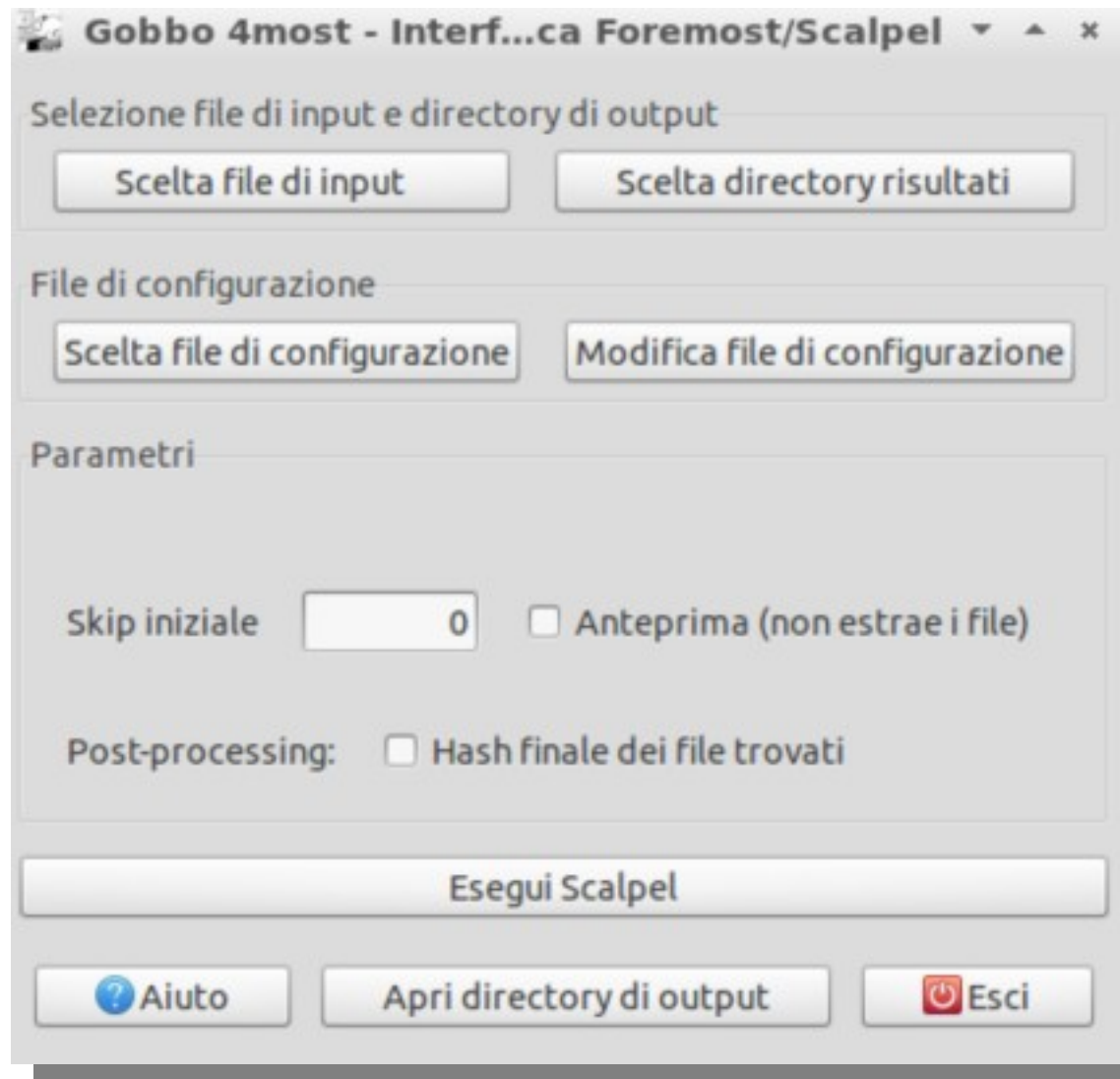
DEFT Conference 2012



hb4most



hb4most



Varie ed eventuali

◆ Domande e risposte

◆ Link utili

<http://www.deftlinux.net/>

Sito ufficiale DEFT

by meo bogliolo



DEFT Conference 2012

