theevilbit.blogspot.com

The Evil Bit Blog: Backtrack Forensics: scalpel

http://theevilbit.blogspot.com/2013/01/backtrack-forensics-scalpel.html

Forensics -> Forensic Carving Tools

/usr/local/bin/scalpel

Scalpel is a very similar tool to foremost, it will data carve files, based on their header and footer information, it's also file system independent. It can work on drives directly or on image files.

Usage:

The biggest difference to foremost is that we need to edit the scalpel.conf file (/etc/scalpel/scalpel.conf), and uncomment lines (remove #) that specifies the file type we would like to recover.

Few of the many options:

-c Choose configuration file.

-n Don't add extensions to extracted files.

-o Set output directory for carved files.

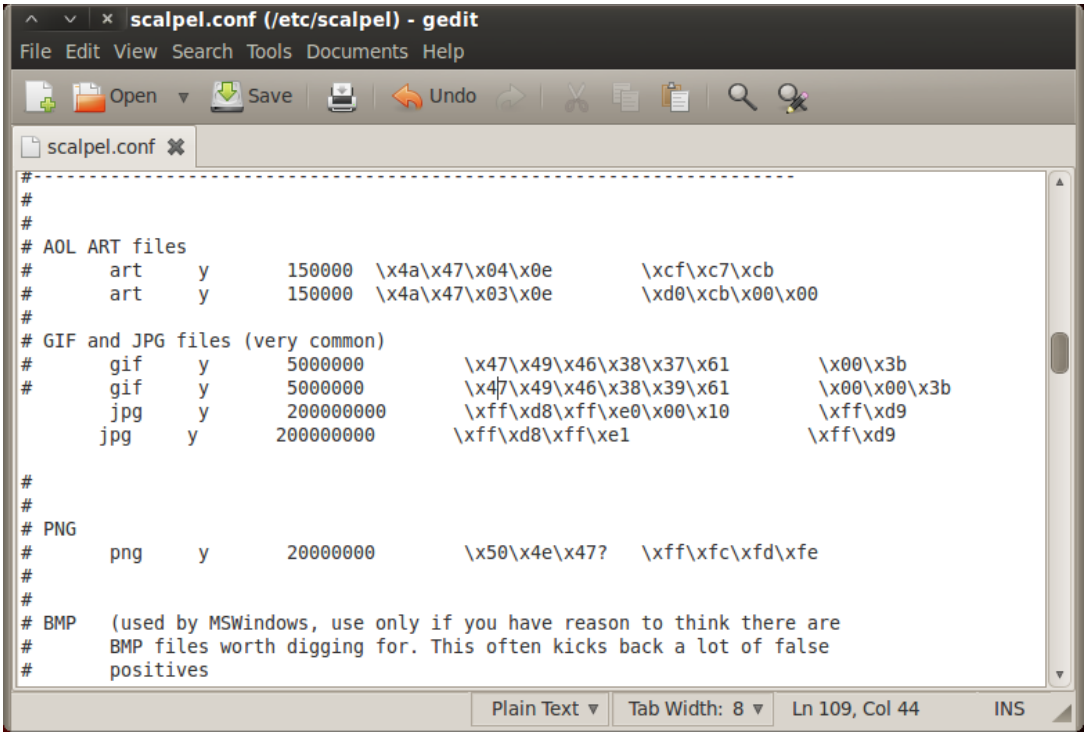
-O Don't organize carved files by type. Default is to organize carved files into subdirectories.

-v Verbose mode.

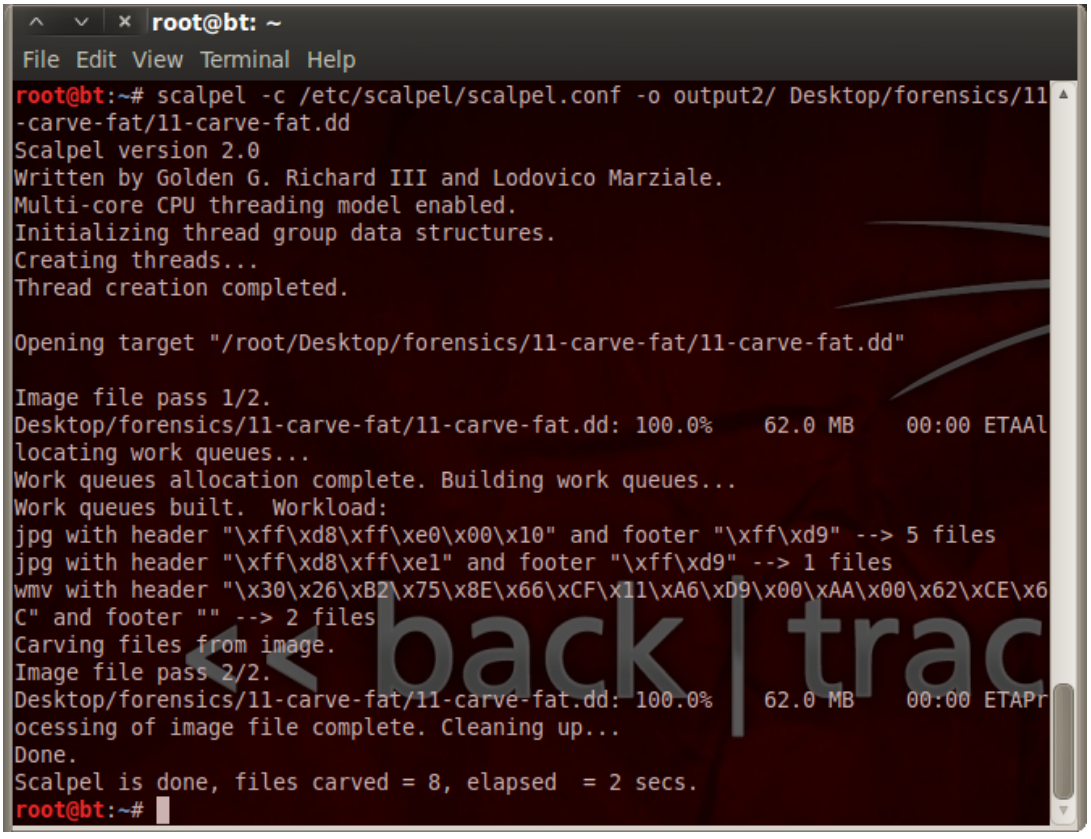
scalpel -c /etc/scalpel/scalpel.conf -o output2/ Desktop/forensics/11-carve-fat/11-carve-fat.dd

I used the same test forensic image as with foremost.

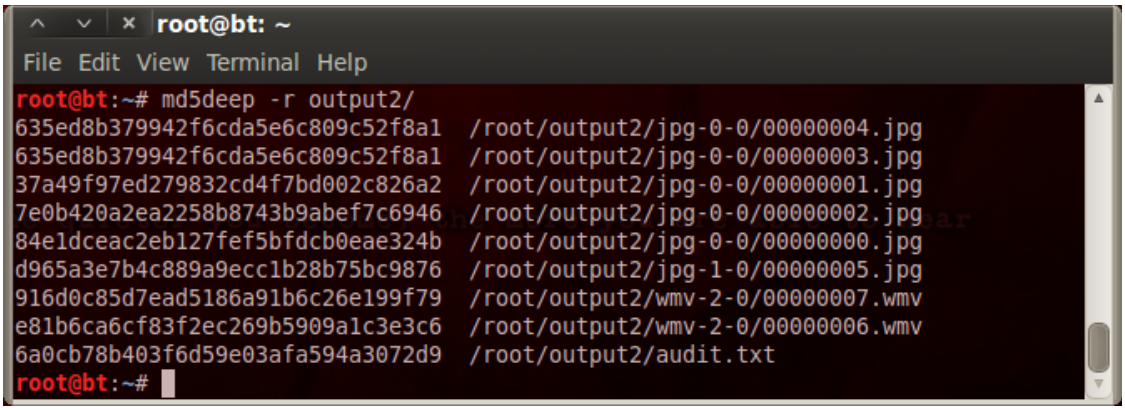
Editing the conf file:



Running the command:



MD5 check, based on this it successfully extracted only 2 files, which means that foremost performed better in this case.



audit file: