Attention dinosaure survive (RZT #92)
solution by madness

I solved this challenge a few months ago, and never intended to submit a write-up. But I was looking at the ones available, and didn't see anyone mention `libewf`.

We are presented with a file called "`0b02119984a7cee0ba83d55425b9491f.E01`". From the extension `.E01` we know that this is an EnCase/Expert Witness disk image. If in doubt, use the `file` utility:

```
$ file 0b02119984a7cee0ba83d55425b9491f.E01https://github.com/libyal/libewf
0b02119984a7cee0ba83d55425b9491f.E01: EWF/Expert Witness/EnCase image file format
```

EnCase images have checksums and optional compression, so trying to `grep` the flag from this file does not work. Hence the need for `libewf`. This library comes with some utilities for manipulating EnCase images. You can get it from

```
https://github.com/libyal/libewf
```

Installing is done in the usual way (note that I have an old version, because I have had it for a long time):

```
$ tar -xf libewf-experimental-20150126.tar.gz
$ cd libewf-20150126
$ ./configure --prefix=/usr --libdir=/usr/lib64 --mandir=/usr/share/man
$ make
$ sudo make DESTDIR="$PWD/../build" install
```

Now you have the library and a few utilities. For example, we can use the `ewfinfo` utility to see the metadata for the image:

```
$ ewfinfo 0b02119984a7cee0ba83d55425b9491f.E01
ewfinfo 20150126

Acquiry information
        Case number:
        Description:            untitled
        Examiner name:
        Evidence number:
        Notes:
        Acquisition date:       Tue Mar 11 05:11:46 2014
        System date:            Tue Mar 11 05:11:46 2014
        Operating system used:  Windows 7
        Software version used:  ADI3.1.4.6
        Password:       N/A

EWF information
        File format:            FTK Imager
        Sectors per chunk:      64
        Compression method:     deflate
        Compression level:      no compression

Media information
        Media type:             fixed disk
        Is physical:            no
        Bytes per sector:       512
        Number of sectors:      26624
        Media size:             13 MiB (13631488 bytes)

Digest hash information
        MD5:            78b0e4ea60f6d022711dc0541c2f0ea8
        SHA1:           9810dc263bf6a2094f80d556e2b8ebfca3fd6a4d
```

But how to get at its contents? I will use the `ewfmount` utility. It mounts the EnCase image so that the raw image can be extracted.

```
$ mkdir temp
$ ewfmount 0b02119984a7cee0ba83d55425b9491f.E01 temp
```

The raw image is at `temp/ewf1`. *Now* we can `grep` for the flag:

```
$ strings temp/ewf1 | grep -i flag

/Flags 262176
/Flags 262240
/Flags 96
/Flags 32
flag-pc
flag-6b96e212b3f85968db654f7892f06122
flag-6b96e212b3f85968db654f7892f06122
flag-6b96e212b3f85968db654f7892f06122
```

Clean up:

```
$ sudo umount temp
$ rmdir temp
```

And the flag is

```
flag-6b96e212b3f85968db654f7892f06122
```

You may be disappointd that I didn’t examine the raw image and uncover alternate data streams, but you can read about that in other write-ups.