

WMLUG January 2015

Introduction to Tomb

By Patrick A. TenHoopen



Tomb

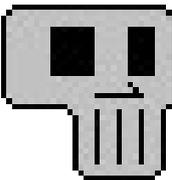
The Crypto Undertaker

What is Tomb?

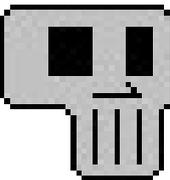
Tomb is a free and open source system for encrypting files on Linux utilizing encrypted storage folders.

Where to get Tomb?

Tomb is available for download from <https://files.dyne.org/tomb>



Installation and Set Up



Requirements

Tomb relies on the following components:

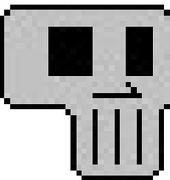
zsh

sudo

gnupg

cryptsetup

pinentry-curses (and/or -gtk-2, -x11, -qt)



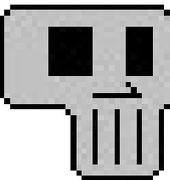
Installation

Extract the downloaded file:

```
tar xvfz Tomb-2.0.1.tar.gz
```

Install it:

```
cd Tomb-2.0.1  
sudo make install
```

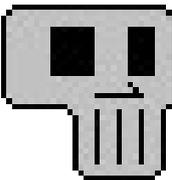


Optional Tools

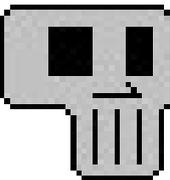
Tomb can use these tools to extend its functions:

executable	function
dcfldd	show progress while digging tombs and keys
steghide	bury and exhume keys inside images
resizefs	extend the size of existing tomb volumes
qrencode	engrave keys into printable qrcode sheets
mlocate	have fast search of file names inside tombs
swish++	have fast search of file contents inside tombs
unoconv	have fast search of contents in PDF and DOC files
haveged	have fast entropy generation for key forging

Tomb will find the tools automatically they are installed.



Basic Usage



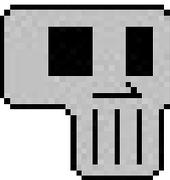
Help

Help

```
tomb -h  
man tomb
```

Manage also available as PDF

http://tomb.dyne.org/tomb_manpage.pdf



Creating a Tomb

Create a new empty tomb (10 MB):

```
tomb dig -s 10 tombname.tomb
```

Temporarily turn off swap to avoid security risk:

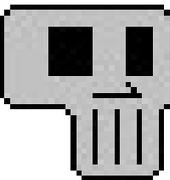
```
sudo swapoff -a
```

Forge (seed) a key file using entropy from system activity:

```
tomb forge tombname.tomb.key
```

Encrypt and format the tomb:

```
tomb lock tombname.tomb -k tombname.tomb.key
```



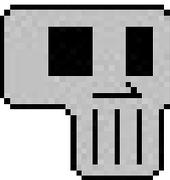
Opening a Tomb

Temporarily turn off swap to avoid security risk:

```
sudo swapoff -a
```

Open the tomb file:

```
tomb open tombname.tomb -k tombname.tomb.key
```



Closing a Tomb

Close a tomb:

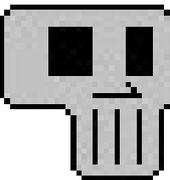
```
tomb close tombname
```

Close all open tombs:

```
tomb close all
```

Alternatively, this will close all open tombs:

```
tomb slam
```



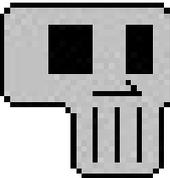
Hide the Key in an Image (requires StegHide)

Using the bury option to embed the key in an image:

```
tomb bury -k tombname.tomb.key image.jpg
```

Using that image to open the tomb:

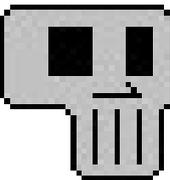
```
tomb open -k image.jpg tombname.tomb
```



Create a QR Code as an Alternate Key (requires QREncode)

Using the engrave option to create a QR image file:

```
tomb engrave -k tombname.tomb.key
```



Demo

