

# FileVault 2 Decoded

Rich Trouton

Howard Hughes Medical Institute,

Janelia Farm Research Campus

# Similar Names, Different Beasts

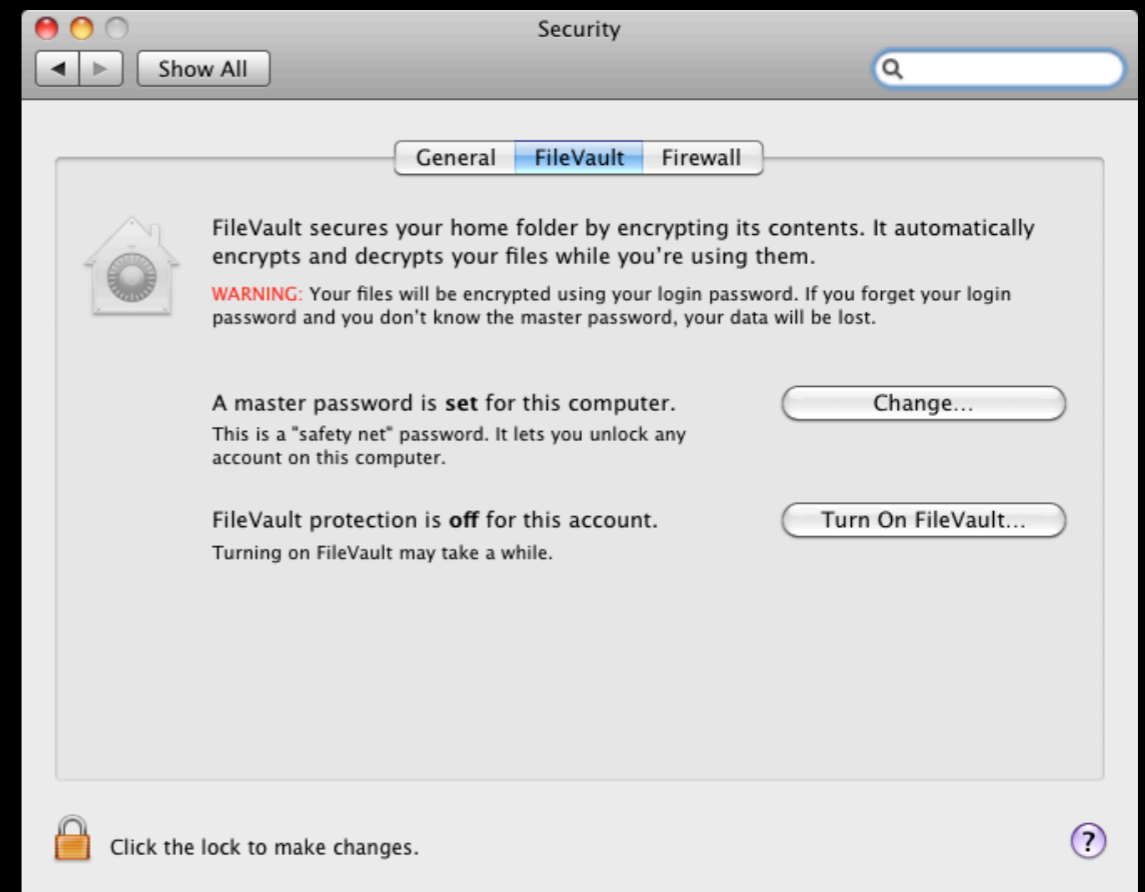
- Apple has completely revamped FileVault in Lion
- Grown from a encryption solution that protected only home folders to one that can protect entire drives.
- For simplicity, the older FileVault encryption will be referred to as “FileVault 1” during this talk.

# Where FileVault Has Been

- Uses encrypted disk images to protect your home folder.
- The contents of the FileVault 1-protected home folder are encrypted and decrypted on the fly.
- The disk image grows and shrinks as needed.

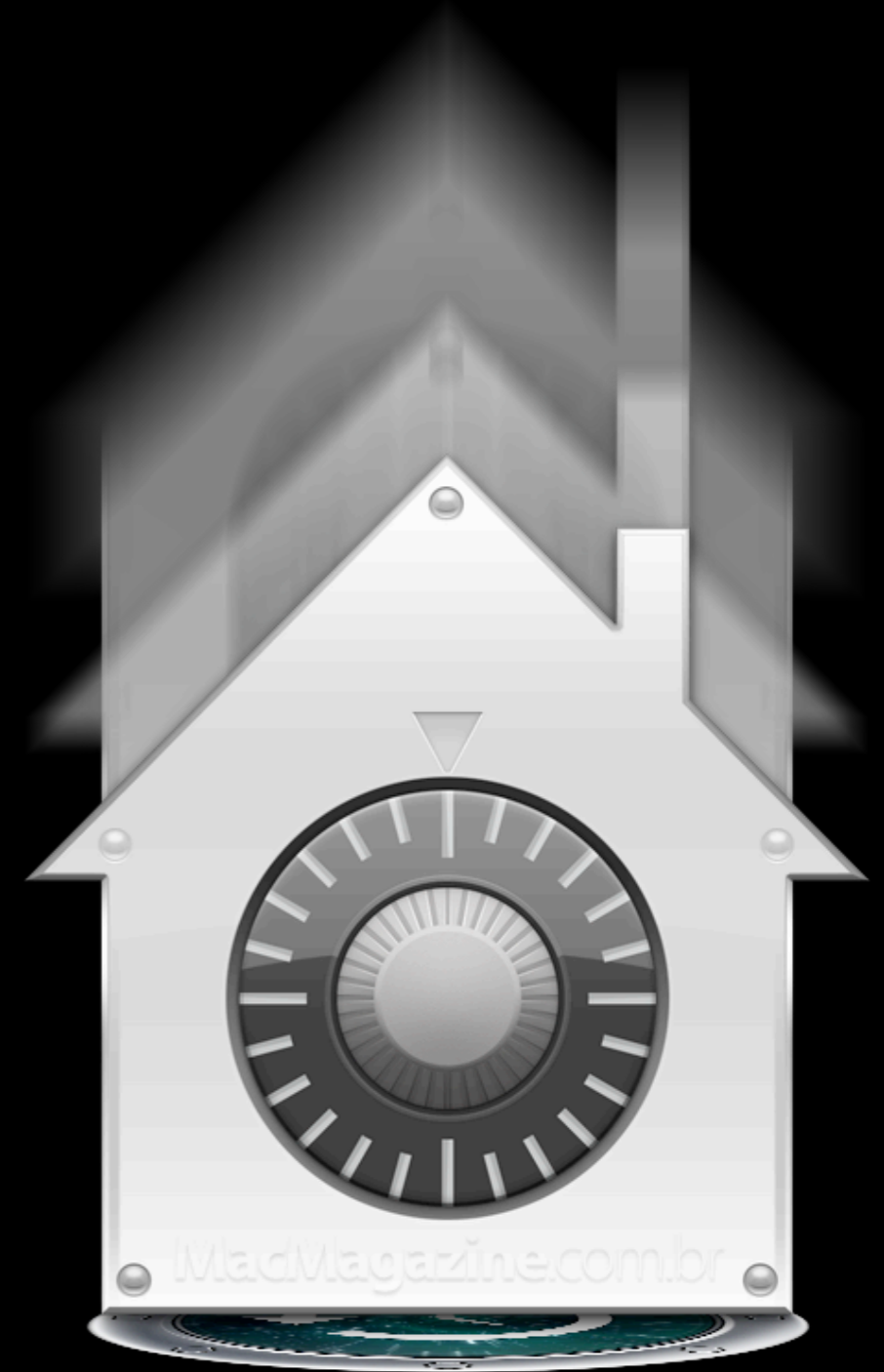
# FileVault | Upsides

- Strong encryption
- Came with the OS, no extra charge to use it.
- Designed to work like an decrypted account wherever possible.



# FileVault | Downsides

- Backups
- Network accounts
- Whole disk encryption not available



# Backing up FileVault 1

- Most backup software not able to handle backing up data reliably from a FileVault-protected home folder.
- User either needed to be logged in (data not encrypted in the backup) or logged out (not able to back up just the files that had changed in the home folder.)

# FileVault I & Network Accounts

- FileVault disk image did not know about password changes made outside of the Mac.
- User could be locked out of their account by a routine password change by the help desk.
- Using the Master Password to help recover FileVault-encrypted network users usually required some command-line work.

# No Whole Disk Encryption

- FileVault I was unable to encrypt the whole boot drive.
- For environments that required the use of whole disk encryption, FileVault I flunked.



# Back to the drawing board

- Complete rebuild of FileVault for Lion
  - Uses new virtual volume storage (Core Storage), whose primary purpose is to provide encrypted volume storage.
- Core Storage encrypted volumes are built on a per-partition basis.
- Allows both encrypted and decrypted partitions on the same physical hard drive.

# How FileVault 2 works

- On startup, the Mac initially boots to a small decrypted partition that only provides access to the tools to unlock the larger encrypted storage.
- When the right authentication is provided, the encryption unlocks and the Mac boots from the Mac's regular OS.
- By unlocking the encryption before the OS boots, the issues with network accounts and backups are solved.

# FileVault 2 and Recovery HD

- One of the other new features in Lion is the Recovery HD partition.
- Small hidden partition that provides tools to fix or reinstall Lion.
- To use FileVault 2, you need to have the Recovery HD partition present.
- Why? Because Recovery HD provides the unencrypted space needed to unlock and boot your encrypted Mac.



Demo





Name

Password



Sleep



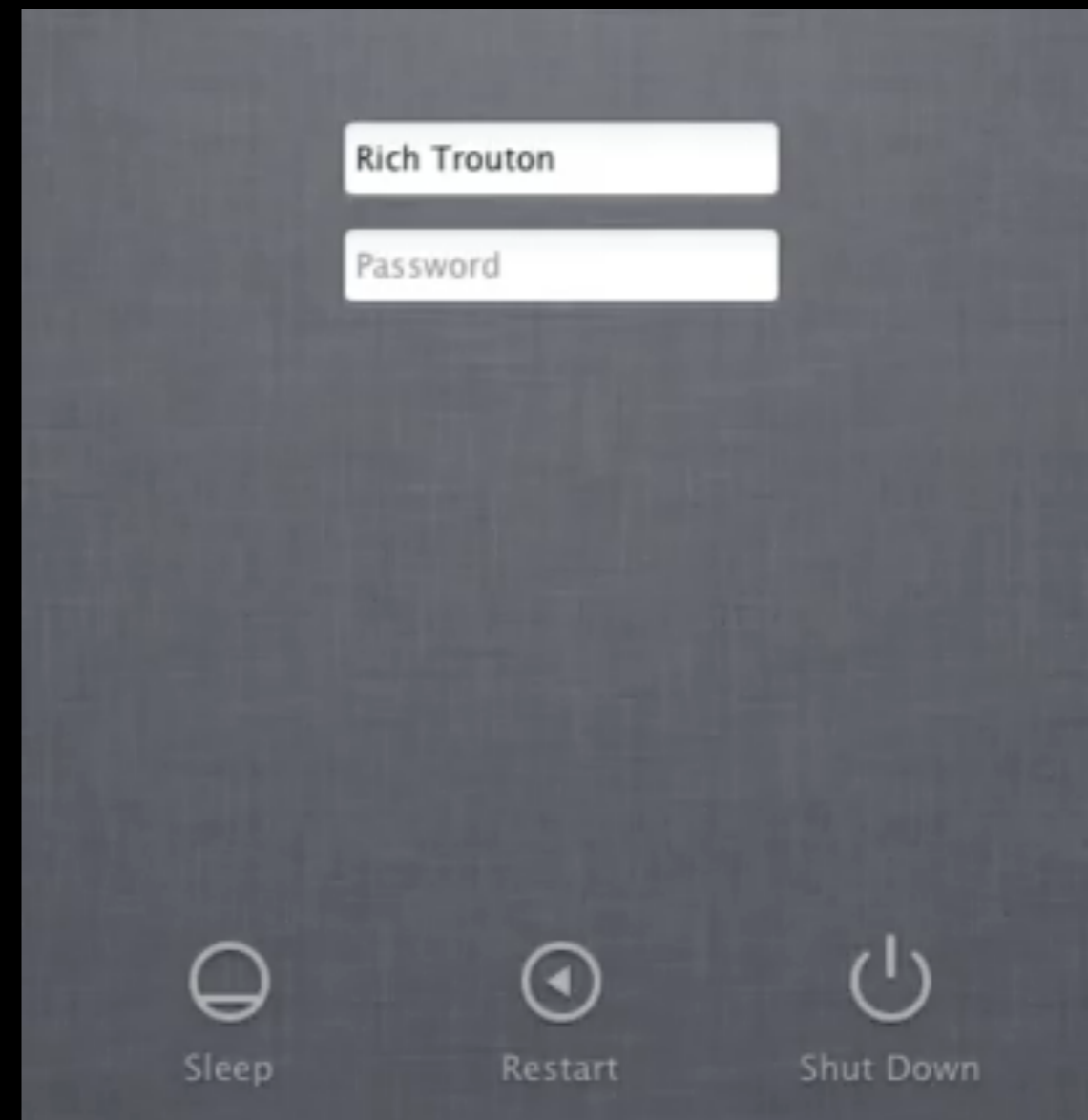
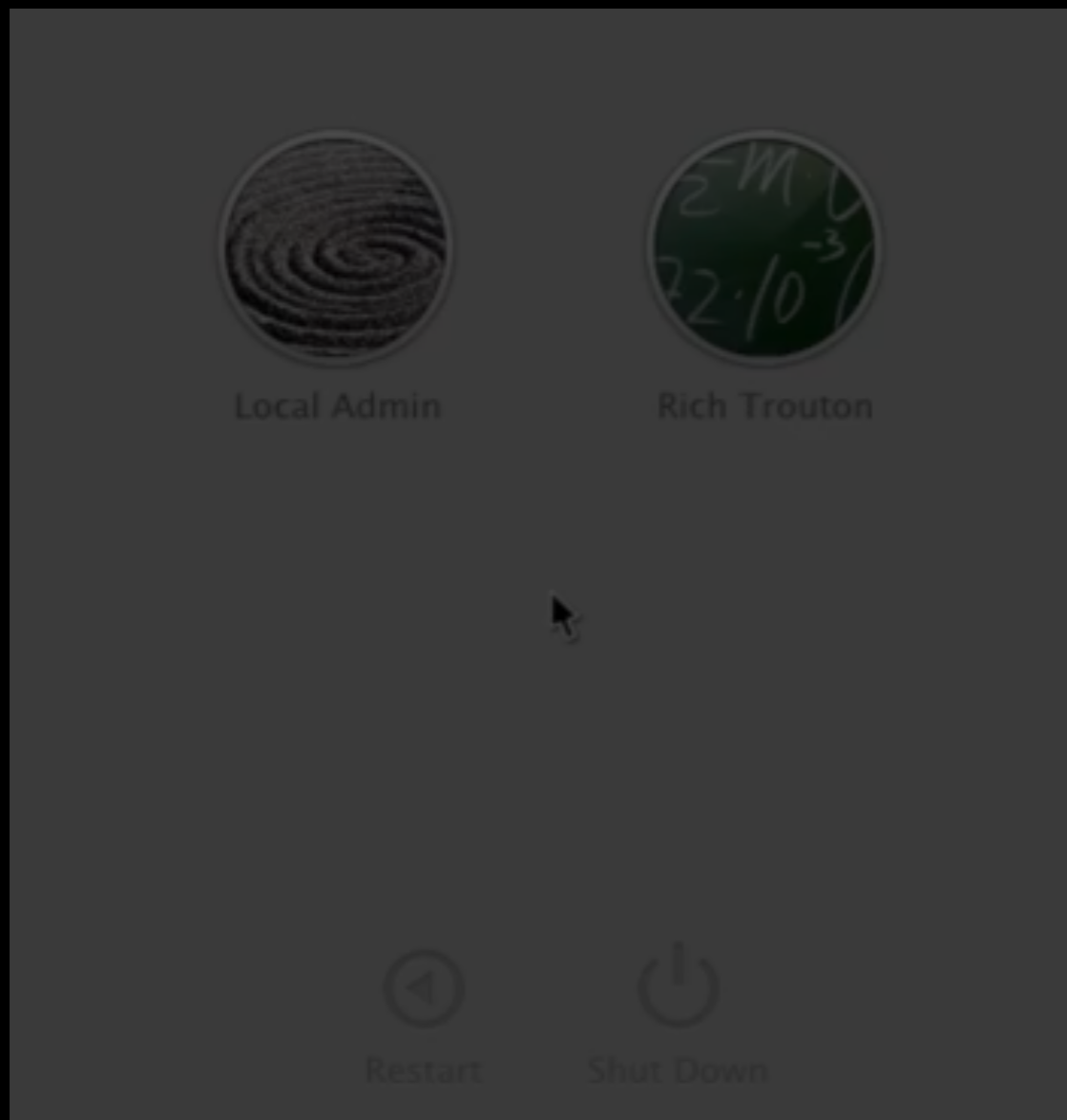
Restart



Shut Down

# Using the Recovery Key To Reset Password

# Using the Recovery Key To Reset Password



# Managed Deployment

- With the exception of how the recovery key is generated and handled, setting up FileVault for home use and setting it up for a managed deployment is exactly the same.
- To avoid the administrative headache of tracking multiple individual recovery keys, Apple brought one part of FileVault 1 into FileVault 2.



# Sole Survivor - FileVaultMaster.keychain

- What does FileVaultMaster.keychain do?
  - It sets a backdoor to encrypted Macs and is an alternate way to unlock the encryption when the account passwords don't work.
  - Apple calls this the Master Password.
- What role does the password you set as the Master Password actually play?
  - It's the password used to unlock the FileVaultMaster.keychain.



# Sole Survivor - FileVaultMaster.keychain

- Wait, what? If all the Master Password does is unlock a keychain, how does it do recovery?
  - FileVaultMaster.keychain's contents are what actually do the recovery.
  - Inside the keychain is a public key (shows up as a SSL certificate) and an accompanying private key.
  - When you have both keys available in the FileVaultMaster keychain, you can use them to unlock or decrypt FileVault 2's encryption.



# Sole Survivor - FileVaultMaster.keychain

- Wait, what? If all the Master Password does is unlock a keychain, how does it do recovery?
  - FileVaultMaster.keychain's contents are what actually do the recovery.
  - Inside the keychain is a public key (shows up as a SSL certificate) and an accompanying private key.
  - When you have both keys available in the FileVaultMaster keychain, you can use them to unlock or decrypt FileVault 2's encryption.



# Sole Survivor - FileVaultMaster.keychain

- You can set a recovery key for a FileVault 2 managed deployment in exactly the same way that you set the recovery key in FileVault 1.
- Crucial difference
  - In FileVault 1, you could have both the private and public key stored in the FileVaultMaster.keychain when you encrypted.
  - In FileVault 2, only the public key can be stored in FileVaultMaster.keychain when you encrypt your Mac.

# Preparing FileVaultMaster.keychain

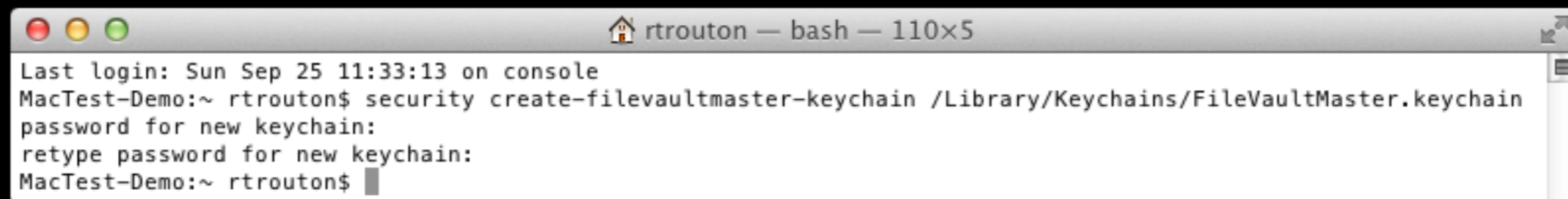
- Make your FileVaultMaster.keychain by setting the Master Password on a specific machine. (You can skip this step if you've already got a set FileVaultMaster.keychain)
  - This FileVaultMaster.keychain will contain both private and public keys.
- Next, make several copies of the FileVaultMaster.keychain file and store the copies in a secure place.
  - A locked safe would be a good place, or in an encrypted disk image on a secured file share.

# Preparing FileVaultMaster.keychain

In 10.7.2 and higher, you can create FileVaultMaster.keychain from the command line.

To create a FileVaultMaster.keychain:

*security create-filevaultmaster-keychain /path/to/FileVaultMaster.keychain*



```
rttrouton — bash — 110x5
Last login: Sun Sep 25 11:33:13 on console
MacTest-Demo:~ rttrouton$ security create-filevaultmaster-keychain /Library/Keychains/FileVaultMaster.keychain
password for new keychain:
retype password for new keychain:
MacTest-Demo:~ rttrouton$
```

You'll be prompted to set a password. Please enter the Master Password you want to use at this point.

# Preparing FileVaultMaster.keychain

- Once you've got copies, unlock your FileVaultMaster.keychain by running the command below and entering the Master Password when prompted for the password:

*security unlock-keychain /path/to/FileVaultMaster.keychain*

- After FileVaultMaster.keychain unlocks, go into Keychain Access and access FileVaultMaster.keychain
  - Remove the private key. It will be called **FileVault Master Password Key** and its kind is listed as **private key**.

# Confused?



No problem.

Here's how to do this.





Name

Password



Sleep



Restart



Shut Down

# Deploying FileVaultMaster.keychain

- You can deploy the prepared FileVaultMaster.keychain using a variety of methods.
  - Install it via an installer package
  - Include it with your image
  - Copy it to your Macs using your system management tool(s).
- A FileVaultMaster.keychain can be built once and then deployed to as many Macs as needed.



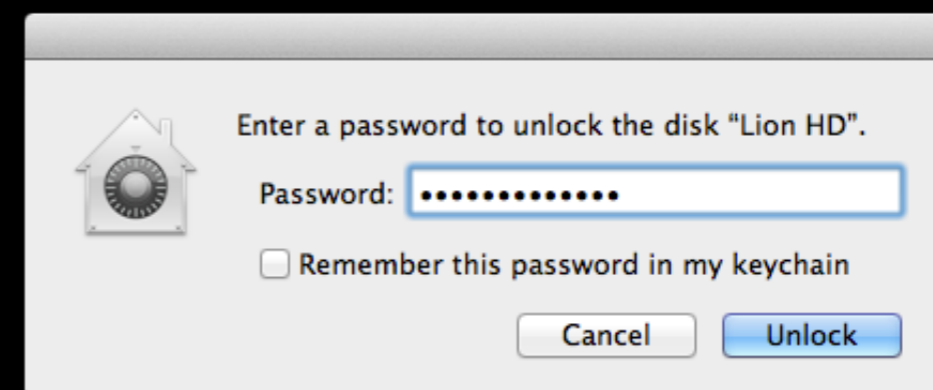
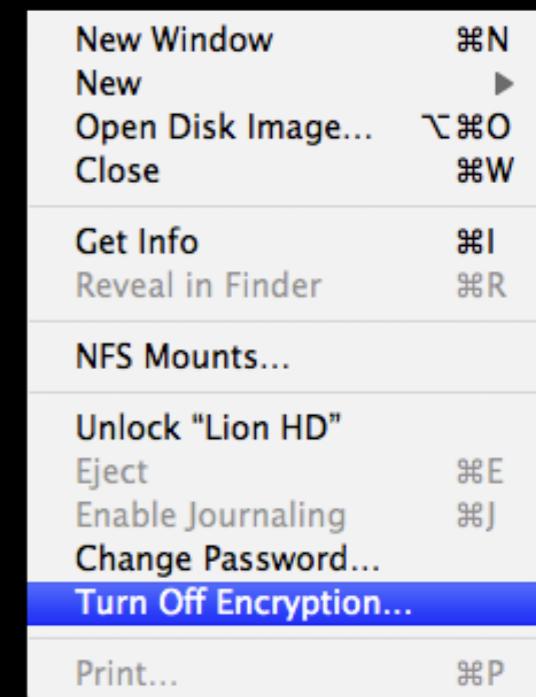
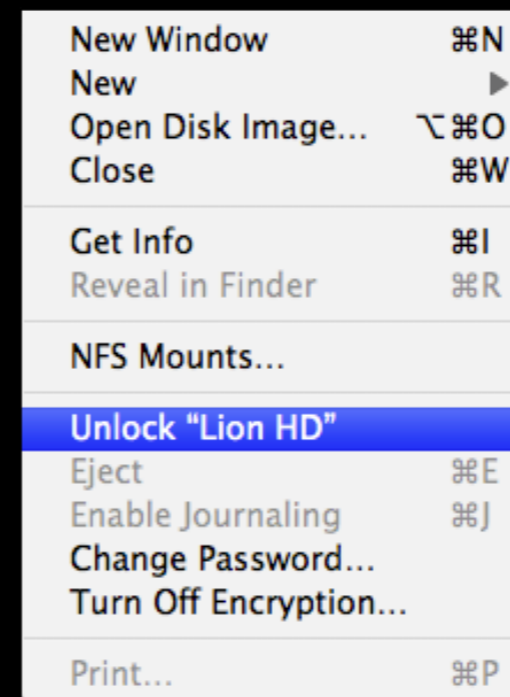
# Disaster Recovery

Sometimes bad things happen  
to good Macs

- If you have the password to an authorized account available, you can unlock and/or decrypt from Disk Utility or the command line.
- You can also use your recovery key to unlock and/or decrypt from the command line.

# Recovering using your password

- Boot your Mac and hold down ⌘-R (Command – R) to boot from the Mac's Recovery HD partition.
- Use Disk Utility and the password of an authorized user to either unlock or turn off the encryption.



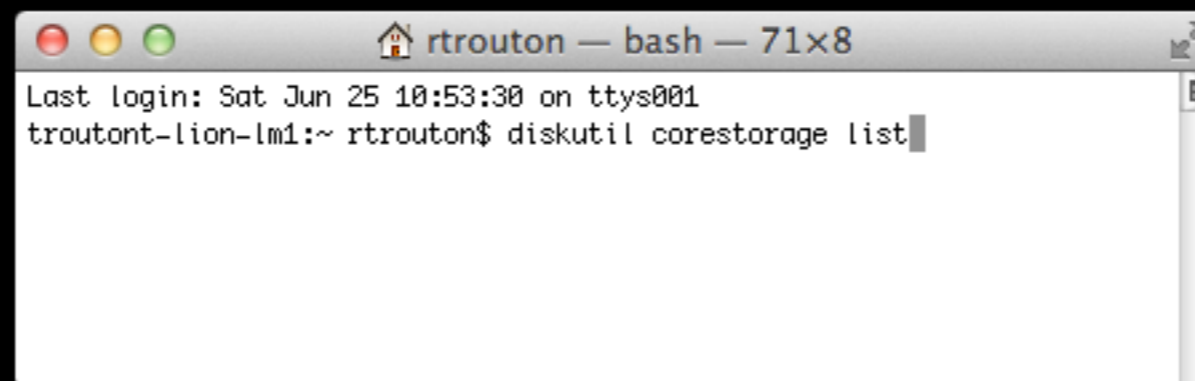


# Recovering from Terminal

Boot your Mac and hold down ⌘-R (Command -R) to boot from the Mac's Recovery HD partition.

Open Terminal and use the following to you need to identify the Logical Volume UUID of the encrypted drive.

*diskutil corestorage list*

A screenshot of a macOS Terminal window. The title bar shows a home icon, the text 'rtrouton — bash — 71x8', and window control buttons. The terminal content shows 'Last login: Sat Jun 25 10:53:30 on ttys001' followed by the prompt 'troutont-lion-lm1:~ rtrouton\$' and the command 'diskutil corestorage list' with a cursor at the end.

```
⏏ ⏏ ⏏ rtrouton — bash — 71x8
Last login: Sat Jun 25 10:53:30 on ttys001
troutont-lion-lm1:~ rtrouton$ diskutil corestorage list
```

# Recovering from Terminal

Once you have the UUID, you'll use it to identify the disk to be unlocked or decrypted.

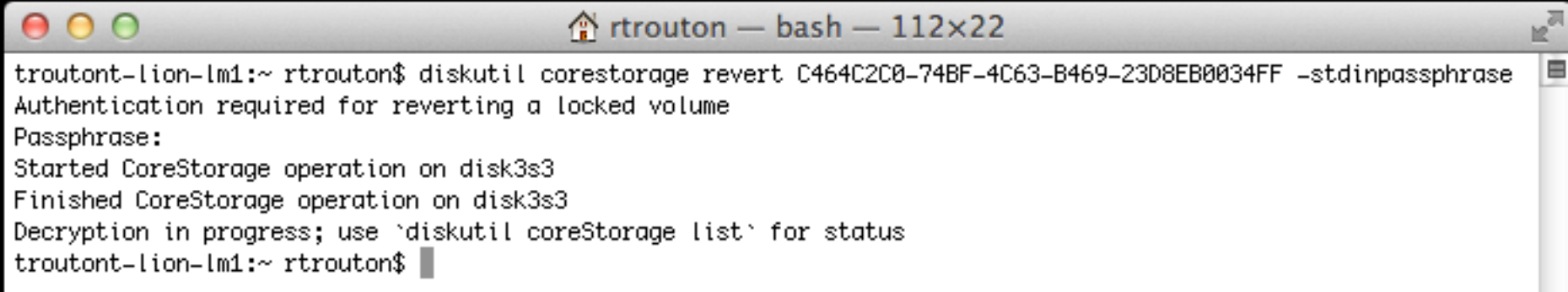
```
rtrouton — bash — 68x33
=====
Name:      Lion HD
Sequence:  1
Free Space: 0 B (0 B)
|
+--< Physical Volume 8C54C06F-4412-4130-BA26-2F226EB6AB11
-----
|
|  Index:      0
|  Disk:      disk3s3
|  Status:    Online
|  Size:      69477036032 B (69.5 GB)
|
+--> Logical Volume Family 14BBCFCC-21D0-4191-93A5-265AAE1EB57B
-----
|
|  Sequence:      10
|  Encryption Status: Locked
|  Encryption Type:  AES-XTS
|  Encryption Context: Present
|  Conversion Status: Complete
|  Has Encrypted Extents: Yes
|  Conversion Direction: -none-
|
+--> Logical Volume C464C2C0-74BF-4C63-B469-23D8EB0034FF
-----
|
|  Disk:      -none-
|  Status:    Locked
|  Sequence:  4
|  Size (Total): 69158264832 B (69.2 GB)
|  Size (Converted): -none-
|  Revertible:  Yes (unlock and decryption required)
|  LV Name:    Lion HD
|  Content Hint: Apple_HFS
|
troutont-lion-lm1:~ rtrouton$
```

# Recovering from Terminal

Unlocking or encrypting using your password

To unlock: *diskutil corestorage unlockVolume UUID -stdinpassphrase*

To decrypt: *diskutil corestorage revert UUID -stdinpassphrase*



```
troutont-lion-lm1:~ rtrouton$ diskutil corestorage revert C464C2C0-74BF-4C63-B469-23D8EB0034FF -stdinpassphrase
Authentication required for reverting a locked volume
Passphrase:
Started CoreStorage operation on disk3s3
Finished CoreStorage operation on disk3s3
Decryption in progress; use `diskutil coreStorage list` for status
troutont-lion-lm1:~ rtrouton$
```

The *-stdinpassphrase* flag will cause the command to prompt you for the password/passphrase of an account that's authorized to unlock the encryption.

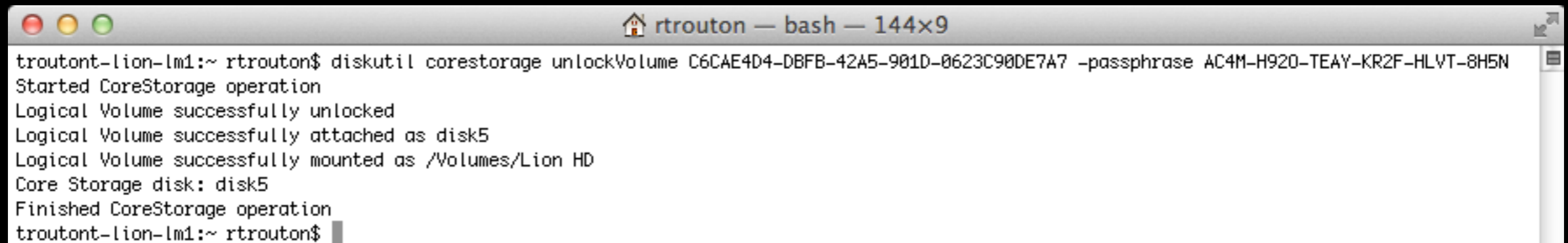


# Recovering from Terminal

Unlocking or decrypting with an individually-set recovery key

To unlock: *diskutil corestorage unlockVolume UUID -passphrase recoverykey*

To decrypt: *diskutil corestorage revert UUID -passphrase recoverykey*

A screenshot of a macOS terminal window titled "rtrouton — bash — 144x9". The terminal shows the following output for the command `diskutil corestorage unlockVolume C6CAE4D4-DBFB-42A5-901D-0623C90DE7A7 -passphrase AC4M-H920-TEAY-KR2F-HLVT-8H5N`:

```
troutont-lion-lm1:~ rtrouton$ diskutil corestorage unlockVolume C6CAE4D4-DBFB-42A5-901D-0623C90DE7A7 -passphrase AC4M-H920-TEAY-KR2F-HLVT-8H5N
Started CoreStorage operation
Logical Volume successfully unlocked
Logical Volume successfully attached as disk5
Logical Volume successfully mounted as /Volumes/Lion HD
Core Storage disk: disk5
Finished CoreStorage operation
troutont-lion-lm1:~ rtrouton$
```

This command would be used only if FileVault 2 generated the recovery key. This would not apply if you're using a managed recovery key using FileVaultMaster.keychain for your recovery key.

# Recovering from Terminal

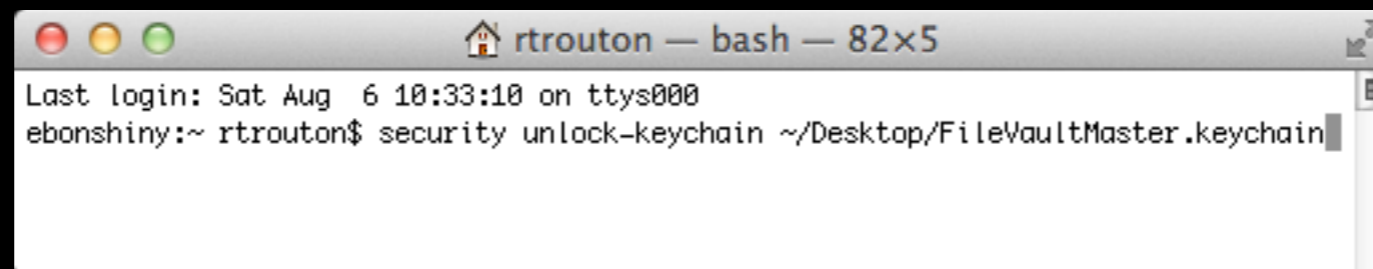
Unlocking or decrypting with a managed recovery key

First, copy the FileVaultMaster.keychain with the private key in the keychain from its secured place to a convenient place on the Mac.

Next, to allow the Mac to get access to both the keys inside, unlock the FileVaultMaster.keychain.

To unlock FileVaultMaster.keychain:

*security unlock-keychain /path/to/FileVaultMaster.keychain*

A screenshot of a macOS Terminal window. The title bar reads "rtrouton — bash — 82x5". The terminal content shows "Last login: Sat Aug 6 10:33:10 on ttys000" followed by the prompt "ebonshiny:~ rtrouton\$" and the command "security unlock-keychain ~/Desktop/FileVaultMaster.keychain" being entered. The cursor is at the end of the command line.

```
rtrouton — bash — 82x5
Last login: Sat Aug 6 10:33:10 on ttys000
ebonshiny:~ rtrouton$ security unlock-keychain ~/Desktop/FileVaultMaster.keychain
```

You'll be prompted a password. Please enter the Master Password at this point.

# Recovering from Terminal

Unlocking or decrypting with an managed recovery key

Once you've unlocked FileVaultMaster.keychain, you can unlock or decrypt the disk.

To unlock:

```
diskutil corestorage unlockVolume UUID -recoveryKeychain /path/to/FileVaultMaster.keychain
```

To decrypt:

```
diskutil corestorage revert UUID -recoveryKeychain /path/to/FileVaultMaster.keychain
```

As long as FileVaultMaster.keychain is unlocked, you should not be prompted for a password.



# Mac OS X Utilities



## Restore From Time Machine Backup

You have a backup of your system that you want to restore.



## Reinstall Mac OS X

Set up and install a new copy of Lion.



## Get Help Online

Browse the Apple Support website to find help for your Mac.



## Disk Utility

Repair or erase a disk using Disk Utility.

Continue

# Limitations of FileVault 2

- FileVault 2 is an overall better solution than FileVault 1 is, but it does not necessarily cover all workplaces' requirements for full disk encryption.
  - Can't use remote management tools at the pre-boot login screen
  - Can't use authentication methods other than password/passphrases
  - Can't have a policy banner at the pre-boot login screen.

# FileVault 2 and the Law

- For folks who need to satisfy regulatory requirements for encryption:
  - FileVault 2 is not FIPS 140-2 validated.
  - FileVault 2's underlying low level encryption uses Apple's new Common Crypto implementation
  - Common Crypto is just starting to undergo FIPS evaluation

# FileVault 2 and the Law

- If you're planning to roll out FileVault 2 in your regulated environment:
  - Make sure it meets your workplace's regulatory requirements.
  - Double-check with your data-protection folks.
  - Be prepared to do some justification writing.

# The Guest User

- As of 10.7.2, some people started seeing an account named **Guest User** appear at the pre-boot login screen.
- When selected, there was no password needed.
- It took you into Safari. Nothing was available but Safari and the network.





# The Guest User

- The **Guest User** account appears when you do two things:
  - Sign into iCloud on the Mac.
  - Enable **Find My Mac**.
- When you log in with the **Guest User** account, **Find My Mac** phones home with the Mac's location.



# Tips for Improving FileVault 2 Performance

- FileVault 2 is able to encrypt and decrypt SSDs much faster than conventional hard drives.
- Processors that have built-in AES-NI support provide additional performance improvements for FileVault 2-encrypted Macs.

# Useful Links

- ✦ OS X Lion: About FileVault 2 - <http://support.apple.com/kb/HT4790>
- ✦ Using Institutional Keys with FileVault 2 - <http://www.afp548.com/article.php?story=FileVault-2-Keys>
- ✦ Using a login banner with FileVault 2 - <http://tinyurl.com/mactechfv2-1>
- ✦ Displaying expiring password notifications when using FileVault 2 with Active Directory accounts - <http://tinyurl.com/mactechfv2-2>

# For More Information

See the July and August 2011 issues of MacTech



MACTECH



July 2011 - FileVault Decrypted  
August 2011 - FileVault Decrypted for Enterprise

# Questions?

Bring them to the Security IT Lab

Thursday: 11:30 AM - 1:00 PM

**Answers guaranteed\***

\*Correct answers not guaranteed.

# Thank You For Attending

Enjoy the rest of the conference

**@rtrouton**

FOLLOW ME ON [twitter](#)