Hacking the Apple TV and Where your Forensic Data Lives

Presentation for:

Defcon 17

July 30, 2009

Kevin Estis

and

Randy "r3d" Robbins

DMCA Disclaimer

1. Digital Millennium Copyright Act

2. The authors of this presentation respects the intellectual property rights of others and is committed to complying with U.S. Copyright laws. Our policy is to respond to notices of alleged infringement that comply with the Digital Millennium Copyright Act. The Digital Millennium Copyright Act of 1998 ("DMCA") provides recourse for owners of copyrighted material who believe their rights under U.S. copyright law have been infringed on the Internet.

3. If you believe representations of your work has been copied or otherwise runs afoul of DMCA during this presentation that may constitute copyright infringement, please provide notice to our Designated Agent. The notice must include the following information as provided by the Digital Millennium Copyright Act, 17 U.S.C. 512 (c) (3):
4. A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
5. Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site;
6. Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material;
7. Information reasonably sufficient to permit the service provider to contact the complaining party, such as address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted;
8. A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law;
9. A statement that the information in the notification is accurate and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
10. The Designated Agent for notice of copyright infringement claims may be reached as follows:

11. Kevin A. Estis kevin.estis[at]gmail[dot]com
12. Randy Robbins randy.robbins[at]gmail[dot]com

Why Use the Apple TV?

Because its' HOT...

Why Use the Apple TV?

Overview

1. What is the Apple TV?
2. How is it different?
3. How Does it Get Modified?
   - The Old Way
   - The New Way
4. Walkthrough Two Patchsticks
   - atvusb-creator
   - aTV Flash

Overview

5. Forensic Data

- Hardware Analysis from a Forensic Examiner Perspective
- Software Summary from a Forensic Examiner Perspective
- File Structures
- Basic Forensic Considerations
- General Forensic Considerations
  - Discovery
  - Investigations
  - Files (Almost) Always Modified
- Apple TV Files and Directories Important to Forensic Analysis
  - Basic Areas for User Data
  - Areas Where Most Data Resides

What is the Apple TV?

Overview

1. It is a Digital Media Player
2. Appliance made by Apple Computer based upon Mac OS X
   - Works with iTunes & iPhoto (plays what they do)
   - Built-in 802.11a/g/n
   - Uses Quicktime components to play media
   - Apple TV Operating System may be modified easily

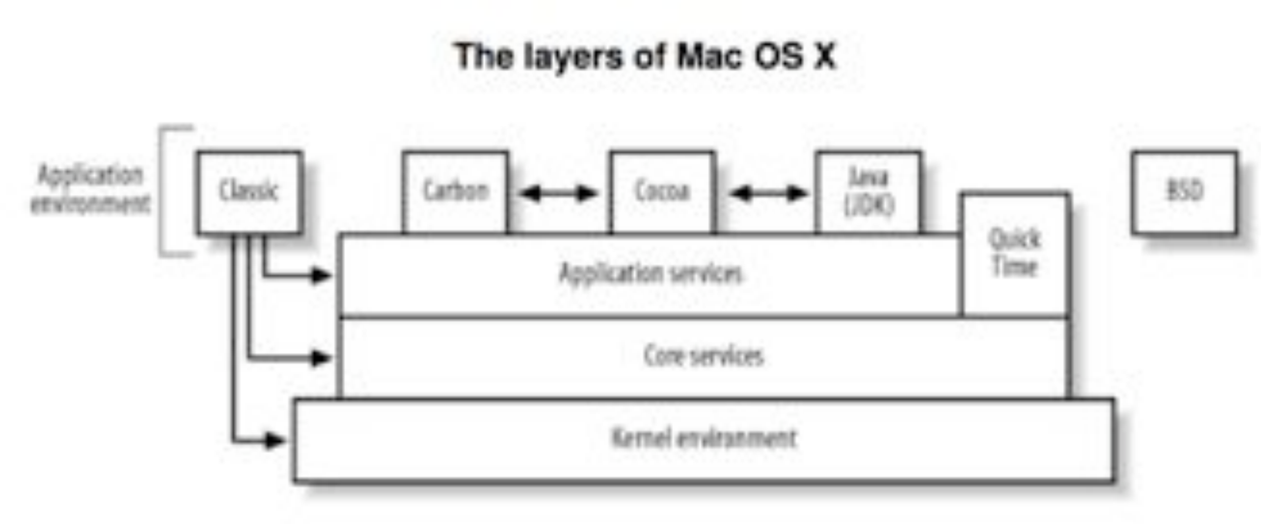
How is it different?

How is it different?

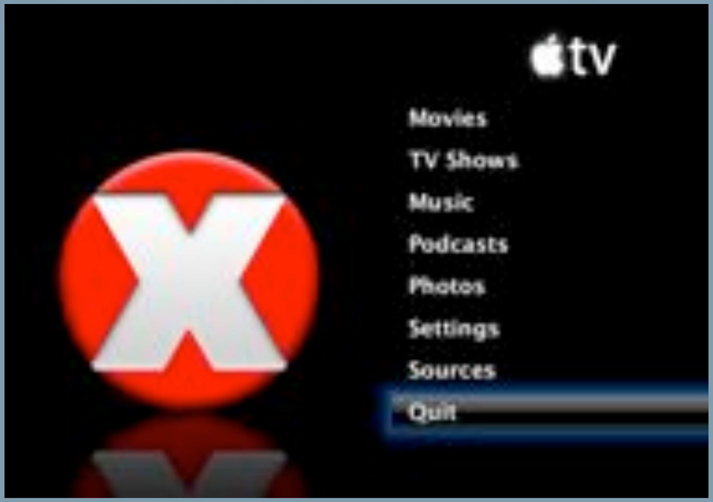
1. Built on an open-source OS
   - *Darwin,* Berkeley Systems Distribution (BSD) Unix…the back-end of Mac OS X
   - Uses the Apple *Frontrow* application as the GUI
2. Does not have digital video recording (DVR) capabilities
3. Synchronizes content with iTunes and iPhoto

Darwin

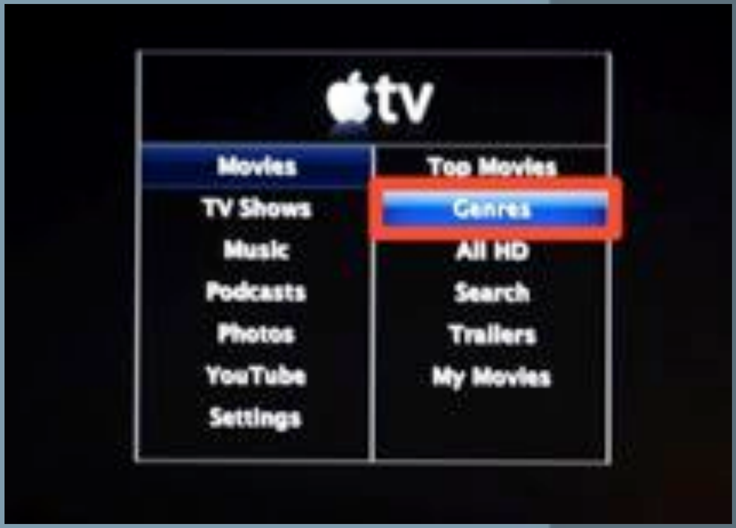
1. Full kernel system for stability
2. Kernel extensions for feature extensibility



Frontrow

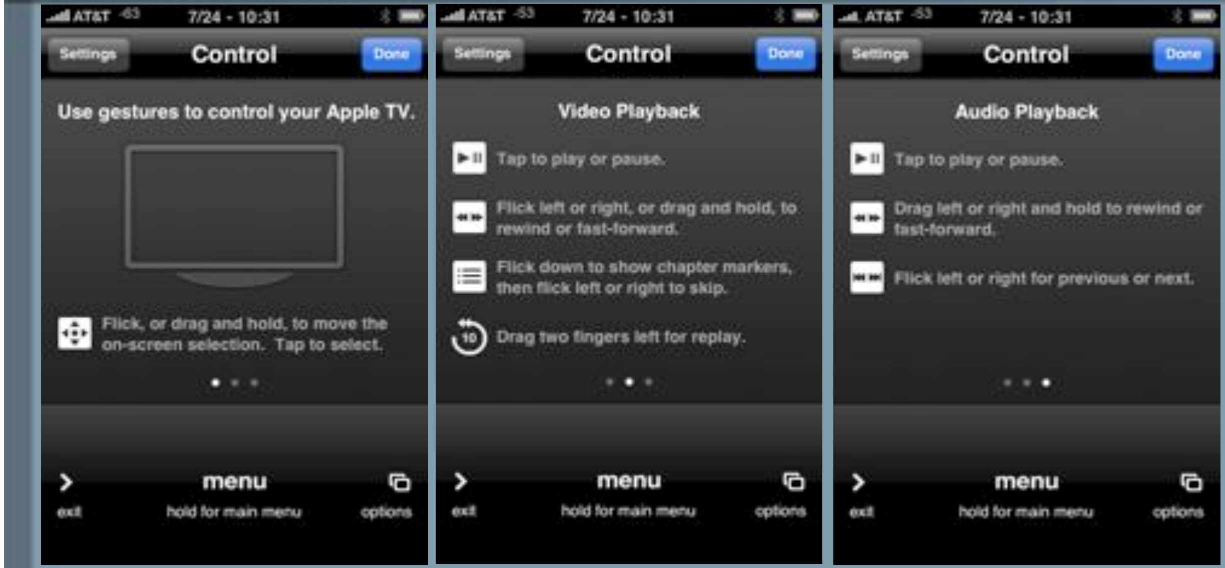


Default Menu for
ATV OS 1.1



Default Menu for
ATV OS 2.0.1

Apple TV and the iPhone



Use gestures to control your Apple TV.

Flick, or drag and hold, to move the on-screen selection. Tap to select.

Video Playback

Tap to play or pause.

Flick left or right, or drag and hold, to rewind or fast-forward.

Flick down to show chapter markers, then flick left or right to skip.

Drag two fingers left for replay.

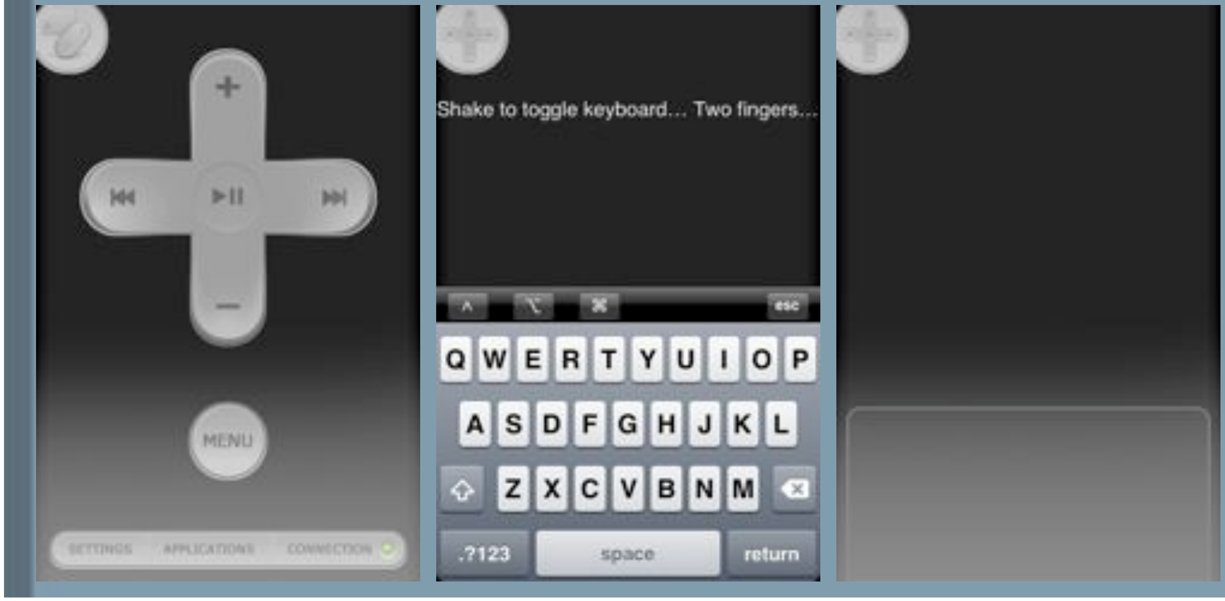
Audio Playback

Tap to play or pause.

Drag left or right and hold to rewind or fast-forward.

Flick left or right for previous or next.

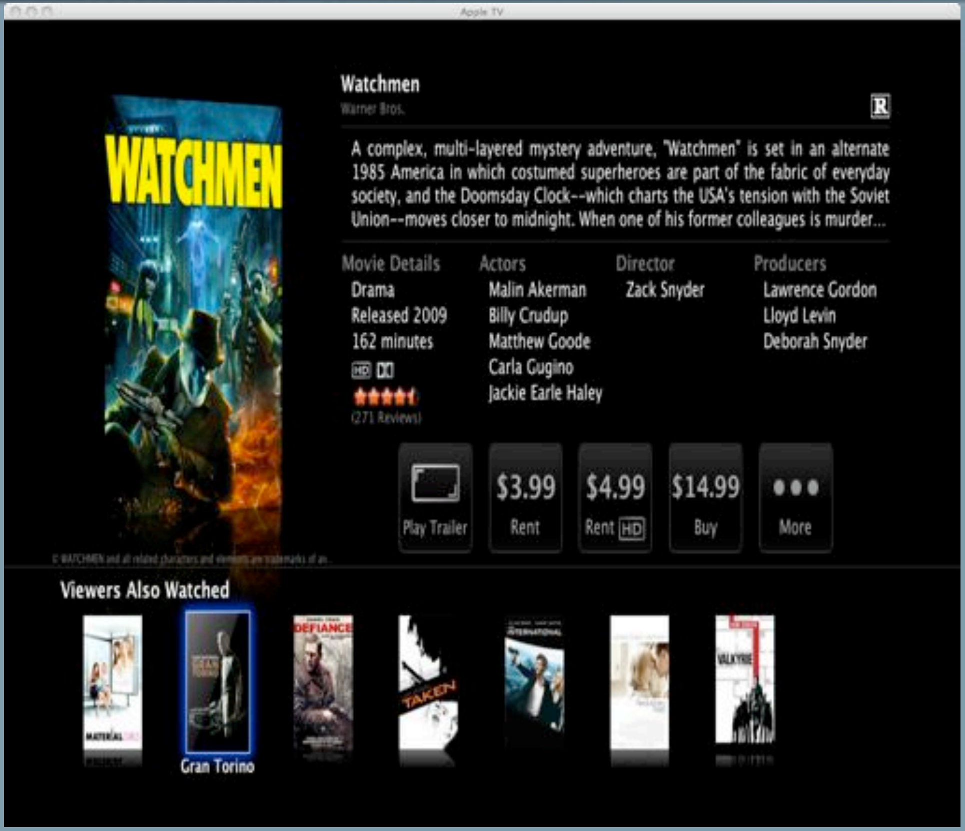
iPhone Remote (Apple)



Shake to toggle keyboard… Two fingers…

iPhone Remote (Rowmote)

iTunes Store



Apple TV

Watchmen

Warner Bros.

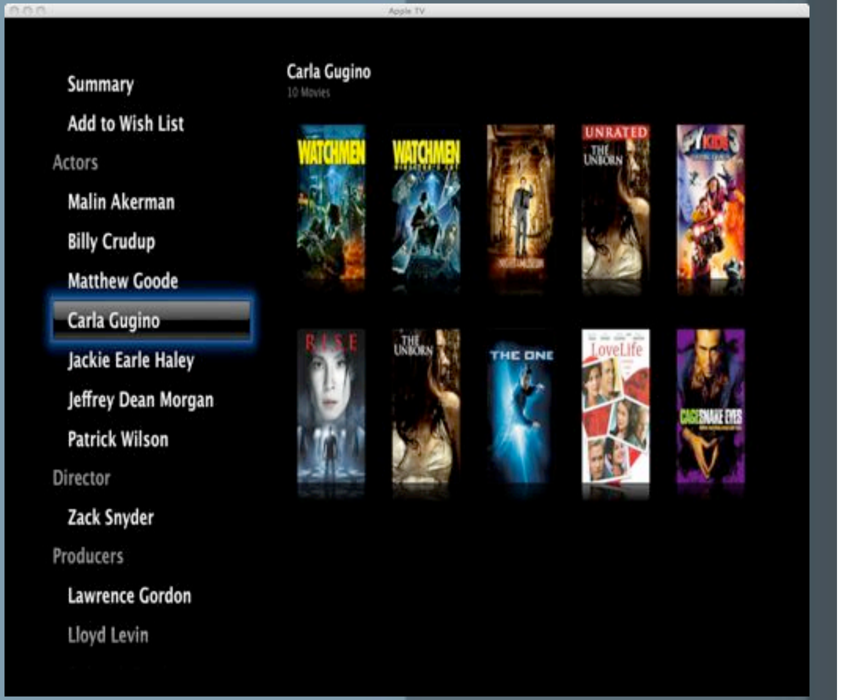
R

A complex, multi-layered mystery adventure, "Watchmen" is set in an alternate 1985 America in which costumed superheroes are part of the fabric of everyday society, and the Doomsday Clock--which charts the USA's tension with the Soviet Union--moves closer to midnight. When one of his former colleagues is murder...

Movie Details	Actors	Director	Producers
Drama	Malin Akerman	Zack Snyder	Lawrence Gordon
Released 2009	Billy Crudup		Lloyd Levin
162 minutes	Matthew Goode		Deborah Snyder
HD	Carla Gugino		
★★★★½	Jackie Earle Haley		
(271 Reviews)			

© WATCHMEN and all related characters and elements are trademarks of an...

Viewers Also Watched



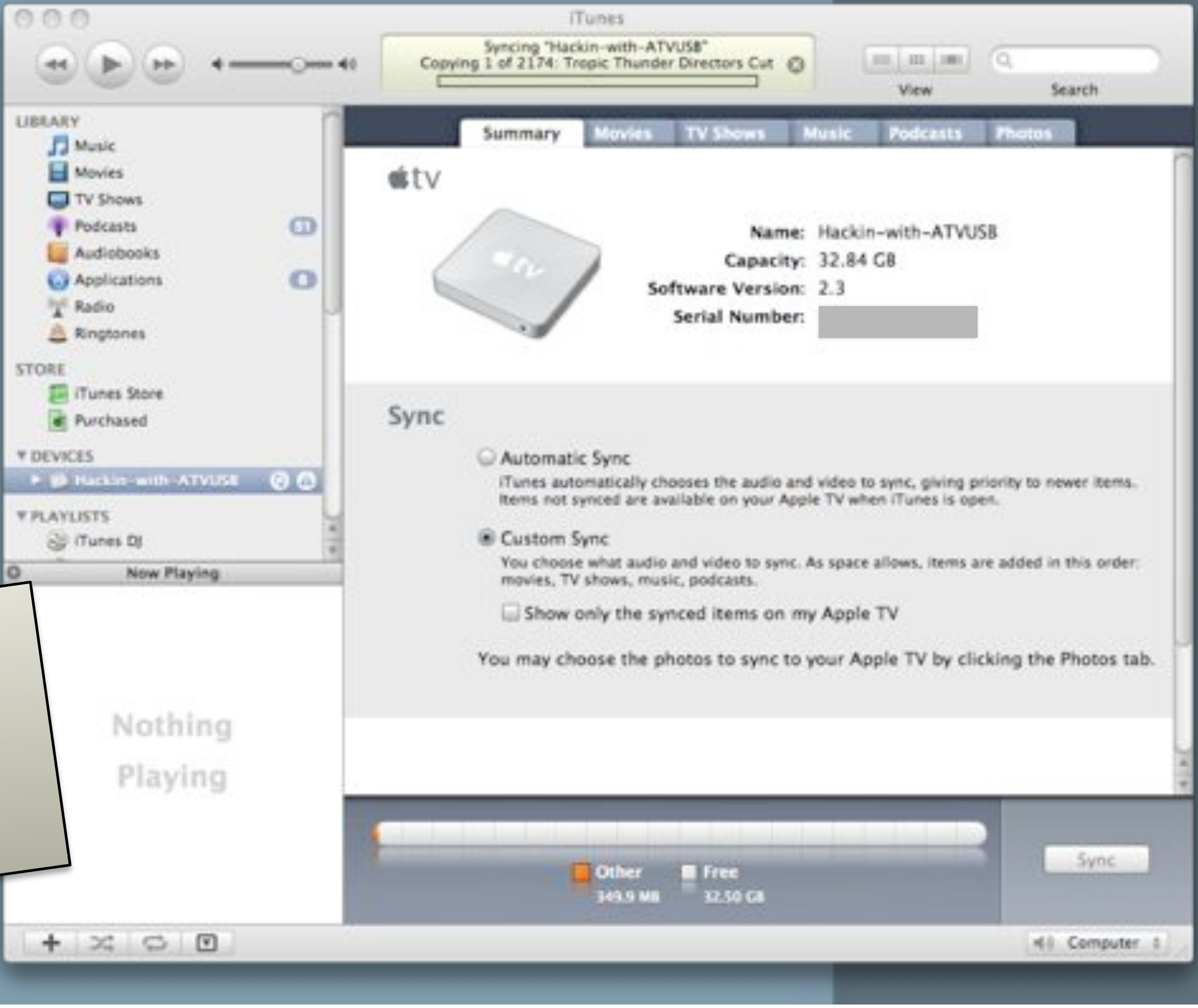
Apple TV

Carla Gugino

10 Movies

iTunes/iPhoto Sync

- Synchronize content from iTunes and iPhoto



Syncing "Hackin-with-ATVUSB"
Copying 1 of 2174: Tropic Thunder Directors Cut

Name: Hackin-with-ATVUSB
Capacity: 32.84 GB
Software Version: 2.3
Serial Number: [redacted]

Sync

○ Automatic Sync
iTunes automatically chooses the audio and video to sync, giving priority to newer items. Items not synced are available on your Apple TV when iTunes is open.

● Custom Sync
You choose what audio and video to sync. As space allows, items are added in this order: movies, TV shows, music, podcasts.

□ Show only the synced items on my Apple TV

You may choose the photos to sync to your Apple TV by clicking the Photos tab.

Firewalls, HIDS, and other security programs **can** make this a challenge…

How Does it Get Modified?

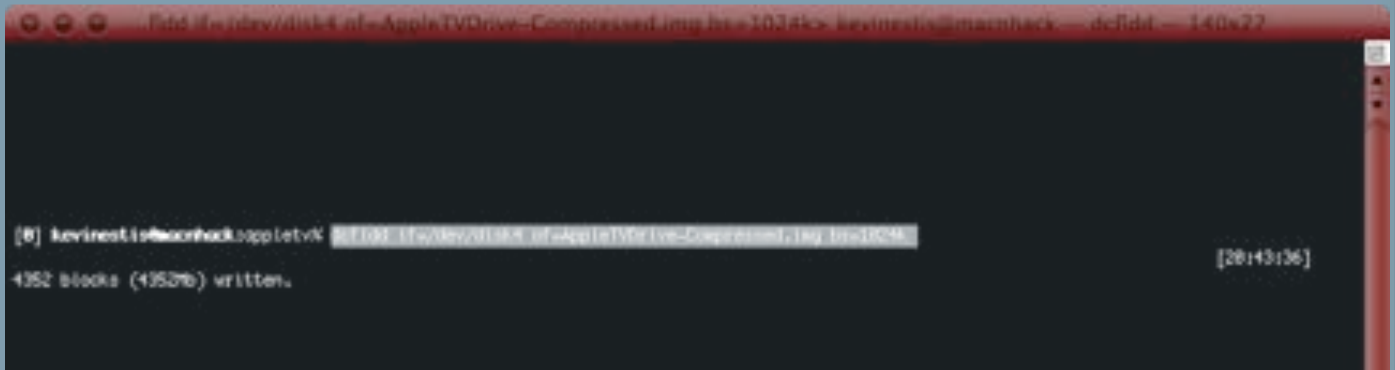
Two Ways to Modify

1. The Old Way
   - Remove the drive (void the warranty)
   - Copy over scripts/binaries manually
   - Generally more reliable but time consuming
2. The New Way
   - Point, click, modify
   - Sometimes stuff doesn't install/ work

The Old Way

Step 1: Make an Image

1. Remove drive and connect to my MacBook Pro via a USB-to-SerialATA cable
2. Image the drive with *dcfldd*

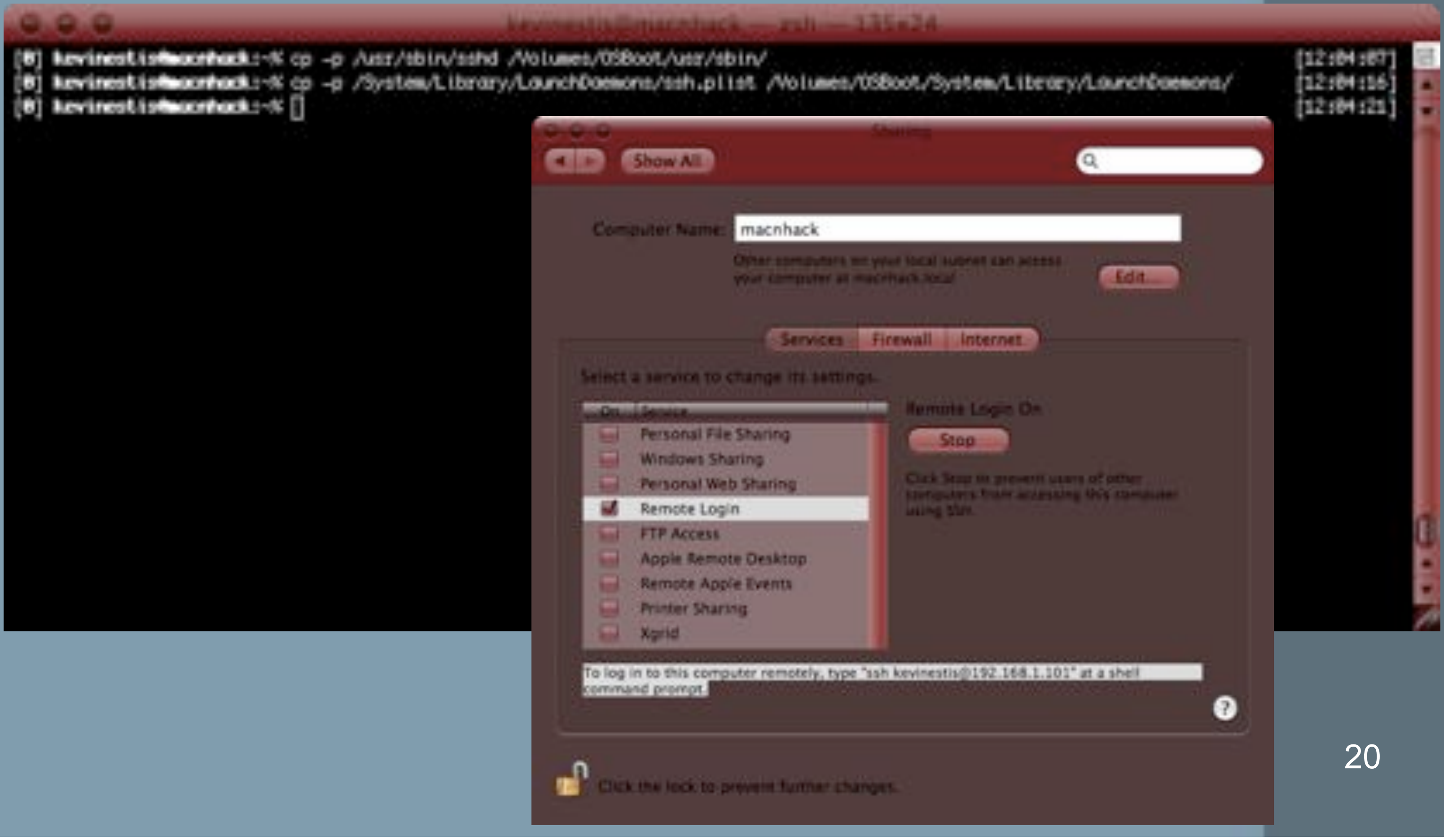


dcfldd if=/dev/disk4 of=AppleTVDrive-Compressed.img bs=1024k> kevinestis@macnhack — dcfldd — 140x22

```
[0] kevinestis@macnhack:appletv% dcfldd if=/dev/disk4 of=AppleTVDrive-Compressed.img bs=1024k
                                                                                         [20:43:36]
4352 blocks (4352Mb) written.
```

Step 2: Enable *SSH*

1. Enable "remote desktop" on MacBook Pro
2. Copy files to the Apple TV hard drive



kevinestis@macnhack — ssh — 135×24

```
[0] kevinestis@macnhack:~% cp -p /usr/sbin/sshd /Volumes/OSBoot/usr/sbin/                                                   [12:04:07]
[0] kevinestis@macnhack:~% cp -p /System/Library/LaunchDaemons/ssh.plist /Volumes/OSBoot/System/Library/LaunchDaemons/      [12:04:16]
[0] kevinestis@macnhack:~% []                                                                                                [12:04:21]
```

Sharing

Computer Name: macnhack

Other computers on your local subnet can access your computer at macnhack.local

Select a service to change its settings.

On	Service
☐	Personal File Sharing
☐	Windows Sharing
☐	Personal Web Sharing
☑	Remote Login
☐	FTP Access
☐	Apple Remote Desktop
☐	Remote Apple Events
☐	Printer Sharing
☐	Xgrid

Remote Login On

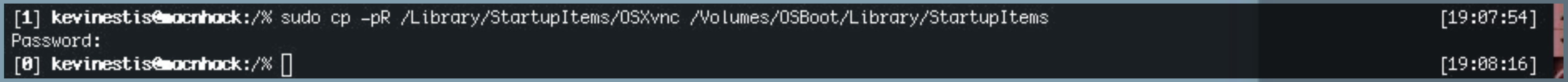
Click Stop to prevent users of other computers from accessing this computer using SSH.

To log in to this computer remotely, type "ssh kevinestis@192.168.1.101" at a shell command prompt.

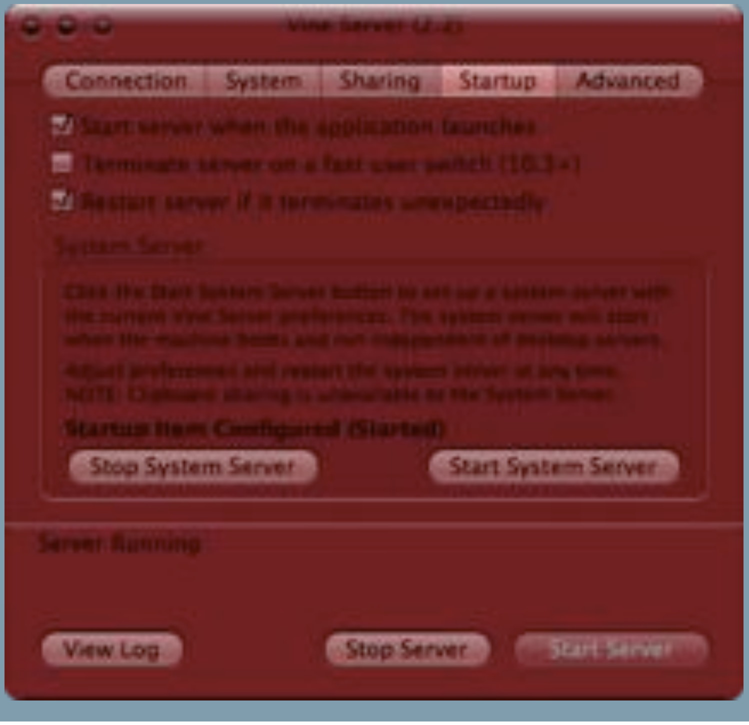
Click the lock to prevent further changes.

Step 3: Enable VNC

1. Start VineVNC server on the MacBook Pro
2. Copy the needed files to the Apple TV hard drive



```
[1] kevinestis@macnhack:/% sudo cp -pR /Library/StartupItems/OSXvnc /Volumes/OSBoot/Library/StartupItems       [19:07:54]
Password:
[0] kevinestis@macnhack:/% ▯                                                                                   [19:08:16]
```



☑ Start server when the application launches

□ Terminate server on a fast user switch (10.3+)

☑ Restart server if it terminates unexpectedly

System Server

Click the Start System Server button to set up a system server with the current Vine Server preferences. The system server will start when the machine boots and run independent of desktop servers.

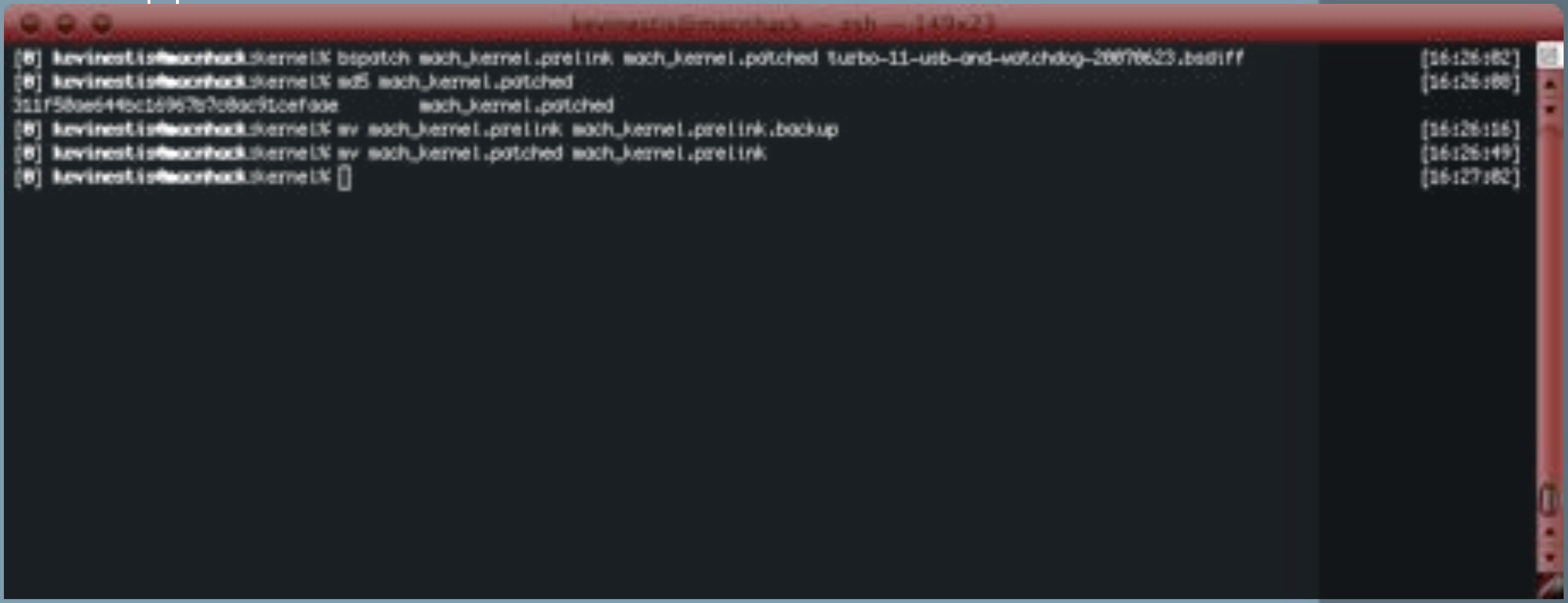
Adjust preferences and restart the system server at any time. NOTE: Clipboard sharing is unavailable to the System Server.

Startup Item Configured (Started)

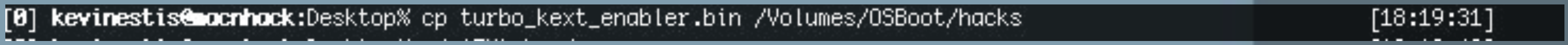
Server Running

Step 4a: Enable kext

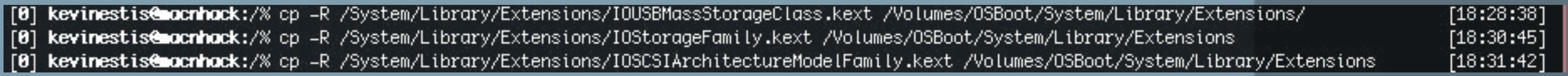
1. Patch the existing Apple TV OS kernel so that the *watchdog* service is disabled and kernel extensions re-enabled
2. Copy the patched kernel, the “enabler” file, and extensions to the Apple TV hard drive



```
[0] kevinestis@macnhack:kernel% bspatch mach_kernel.prelink mach_kernel.patched turbo-11-usb-and-watchdog-20070623.bsdiff      [16:26:02]
[0] kevinestis@macnhack:kernel% md5 mach_kernel.patched                                                                       [16:26:08]
311f58ae644bc16967b7c0ac91cefade        mach_kernel.patched
[0] kevinestis@macnhack:kernel% mv mach_kernel.prelink mach_kernel.prelink.backup                                             [16:26:16]
[0] kevinestis@macnhack:kernel% mv mach_kernel.patched mach_kernel.prelink                                                    [16:26:49]
[0] kevinestis@macnhack:kernel% []                                                                                            [16:27:02]
```



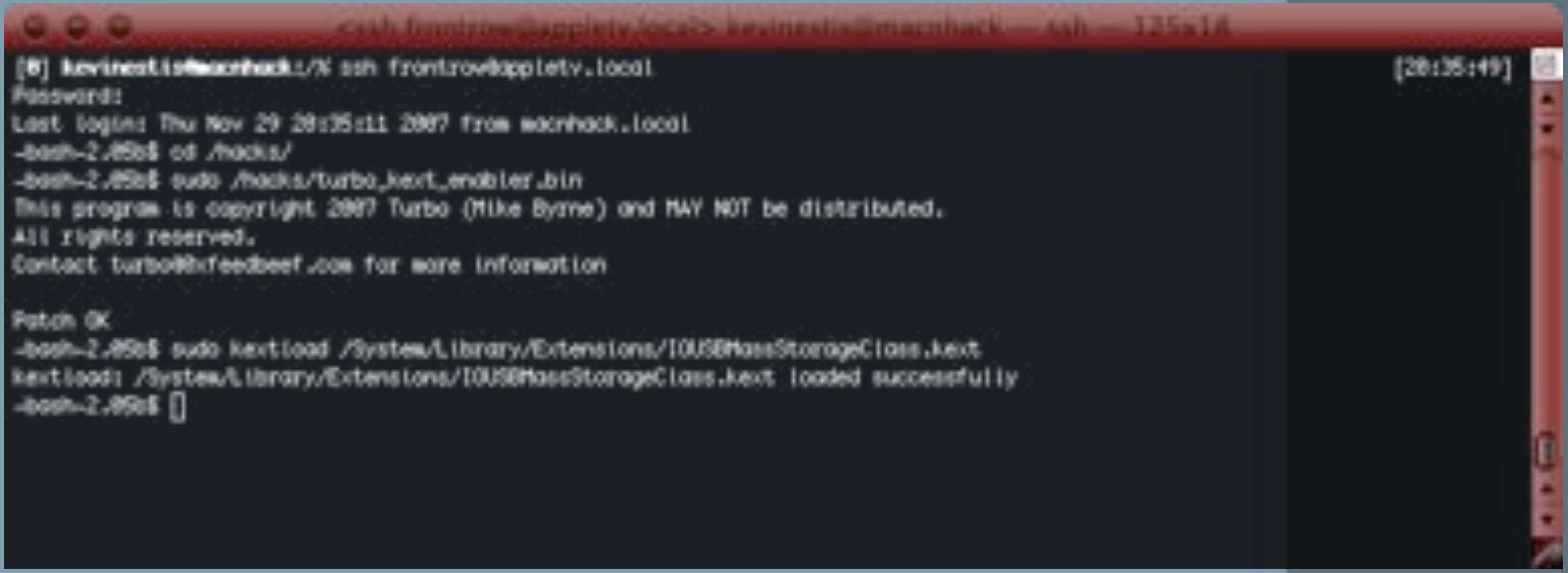
```
[0] kevinestis@macnhack:Desktop% cp turbo_kext_enabler.bin /Volumes/OSBoot/hacks                    [18:19:31]
```



```
[0] kevinestis@macnhack:/% cp -R /System/Library/Extensions/IOUSBMassStorageClass.kext /Volumes/OSBoot/System/Library/Extensions/       [18:28:38]
[0] kevinestis@macnhack:/% cp -R /System/Library/Extensions/IOStorageFamily.kext /Volumes/OSBoot/System/Library/Extensions              [18:30:45]
[0] kevinestis@macnhack:/% cp -R /System/Library/Extensions/IOSCSIArchitectureModelFamily.kext /Volumes/OSBoot/System/Library/Extensions   [18:31:42]
```

Step 4b: Enable kext

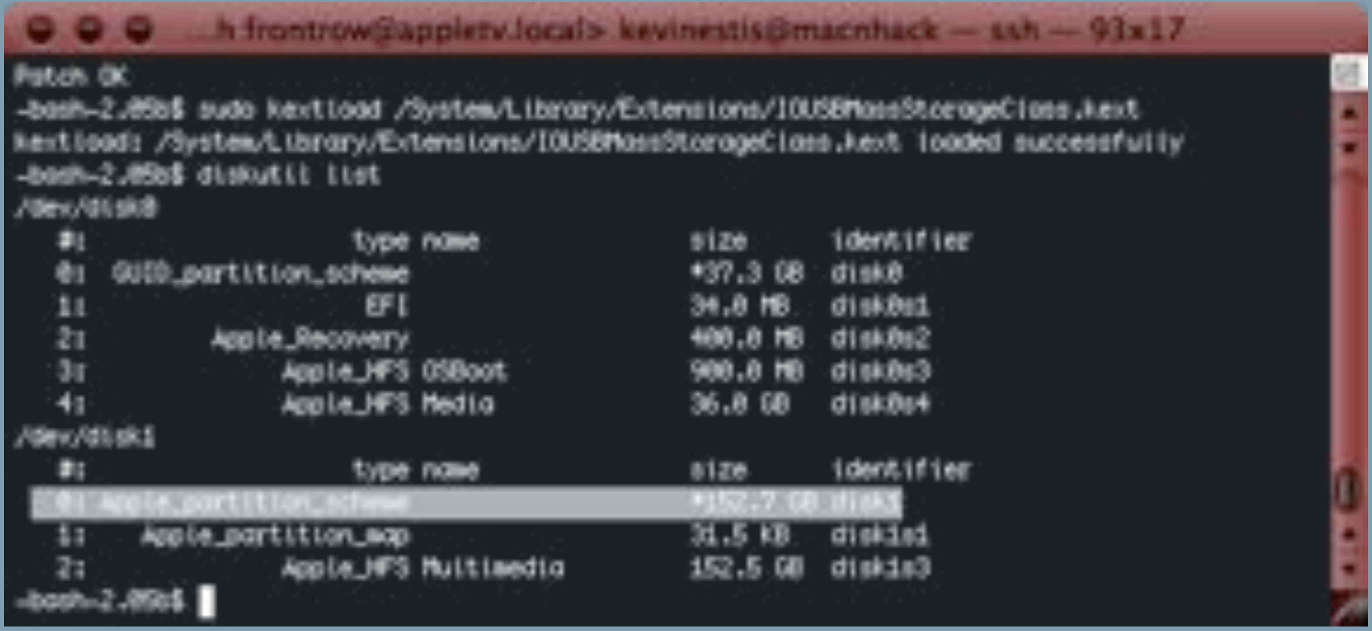
1. Put Apple TV hard drive back in Apple TV
2. Connect from MacBook Pro to Apple TV via *SSH*
3. Execute the kext enabler to start *kextload*
4. Use *kextload* to start USB drivers


<ssh frontrow@appletv.local> kevinestis@macnhack — ssh — 125x14
[20:35:49]

```
[0] kevinestis@macnhack:~/% ssh frontrow@appletv.local
Password:
Last login: Thu Nov 29 20:35:11 2007 from macnhack.local
-bash-2.05b$ cd /hacks/
-bash-2.05b$ sudo /hacks/turbo_kext_enabler.bin
This program is copyright 2007 Turbo (Mike Byrne) and MAY NOT be distributed.
All rights reserved.
Contact turbo@0xfeedbeef.com for more information

Patch OK
-bash-2.05b$ sudo kextload /System/Library/Extensions/IOUSBMassStorageClass.kext
kextload: /System/Library/Extensions/IOUSBMassStorageClass.kext loaded successfully
-bash-2.05b$ ▯
```

Step 5: Verify USB Drive

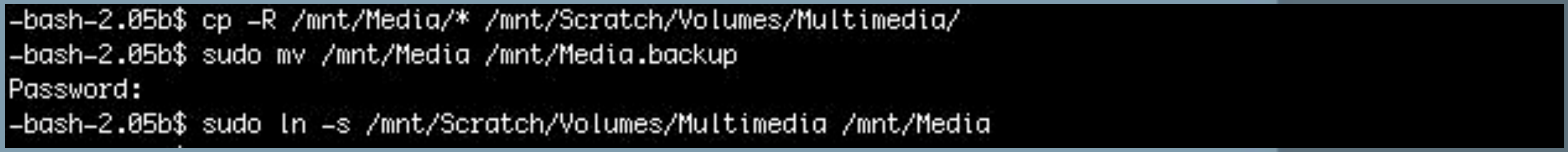
Run *diskutil list* via *SSH*


...h frontrow@appletv.local> kevinestis@macnhack — ssh — 93x17

```
Patch OK
-bash-2.05b$ sudo kextload /System/Library/Extensions/IOUSBMassStorageClass.kext
kextload: /System/Library/Extensions/IOUSBMassStorageClass.kext loaded successfully
-bash-2.05b$ diskutil list
/dev/disk0
   #:                   type name               size      identifier
   0:  GUID_partition_scheme                    *37.3 GB  disk0
   1:                    EFI                    34.0 MB   disk0s1
   2:         Apple_Recovery                    400.0 MB  disk0s2
   3:              Apple_HFS OSBoot             900.0 MB  disk0s3
   4:              Apple_HFS Media              36.0 GB   disk0s4
/dev/disk1
   #:                   type name               size      identifier
   0: Apple_partition_scheme                    *152.7 GB disk1
   1:    Apple_partition_map                    31.5 KB   disk1s1
   2:              Apple_HFS Multimedia         152.5 GB  disk1s3
-bash-2.05b$
```

Step 6: Use Only USB

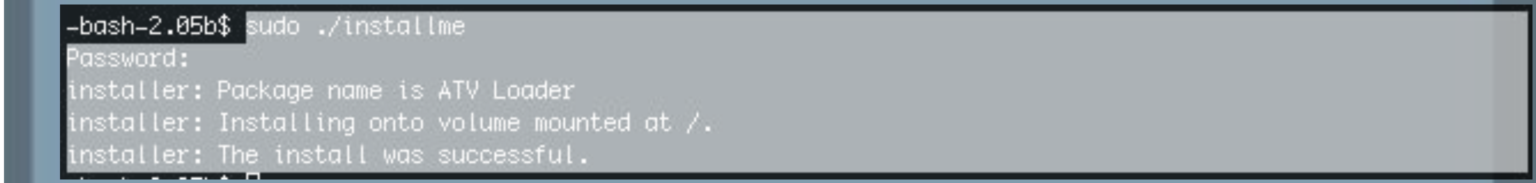
1. Copy the data from the “default” location to the USB drive
2. Make a backup of the data located in the default location
3. Make a symbolic link from the default location to the new location



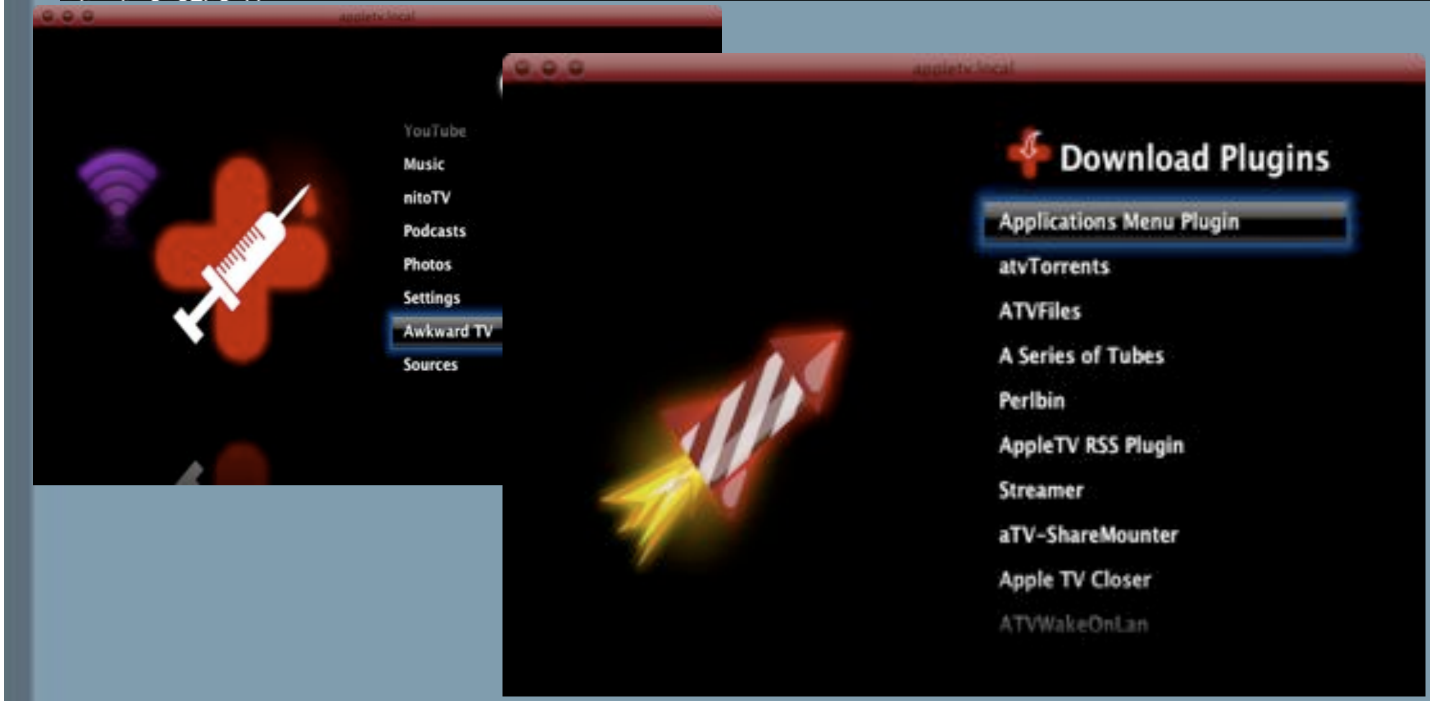
```
-bash-2.05b$ cp -R /mnt/Media/* /mnt/Scratch/Volumes/Multimedia/
-bash-2.05b$ sudo mv /mnt/Media /mnt/Media.backup
Password:
-bash-2.05b$ sudo ln -s /mnt/Scratch/Volumes/Multimedia /mnt/Media
```

Step 7: Install ATV

Install AwkwardTV via *SSH*

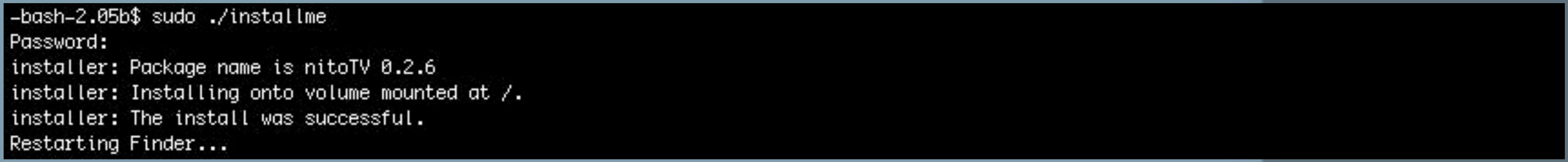


```
-bash-2.05b$ sudo ./installme
Password:
installer: Package name is ATV Loader
installer: Installing onto volume mounted at /.
installer: The install was successful.
```

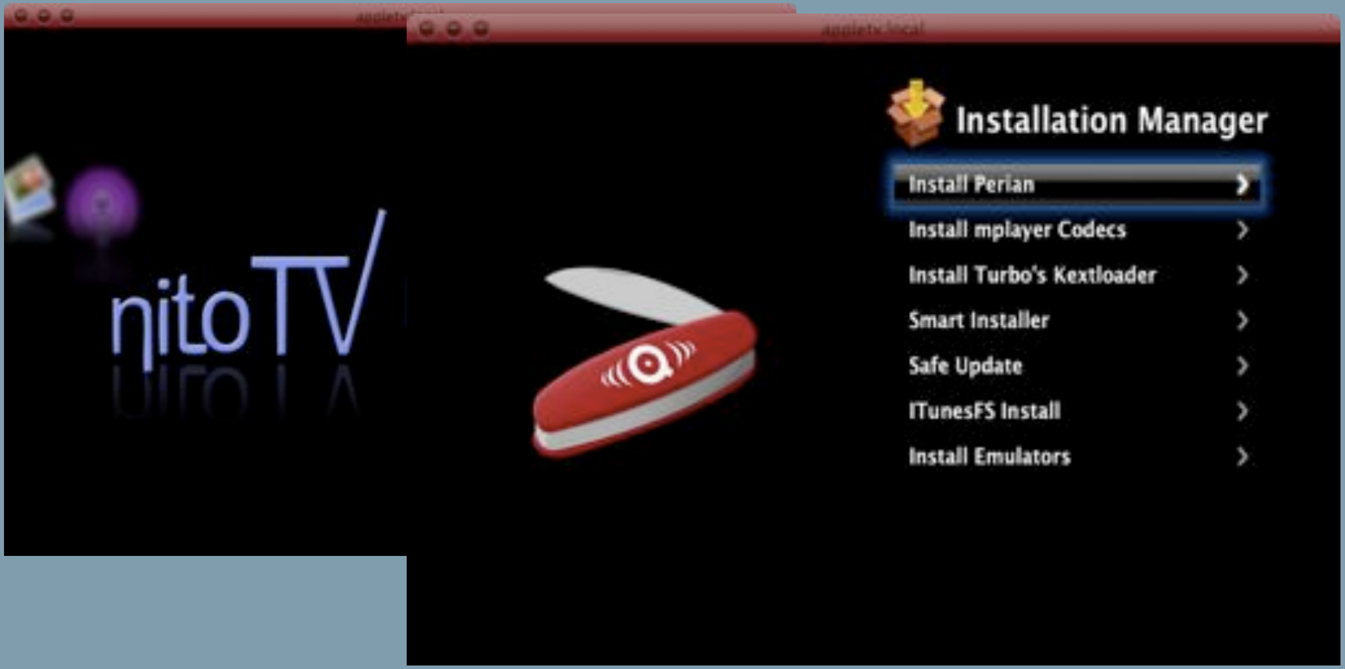


Step 8: Install nitoTV

Install nitoTV via *SSH*



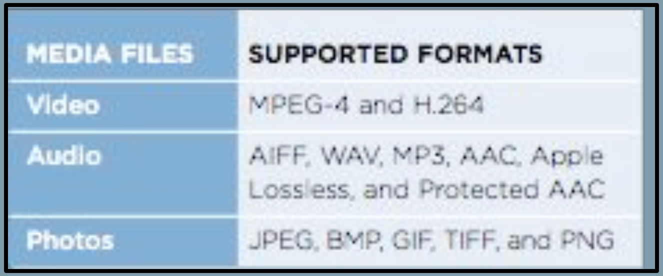
```
-bash-2.05b$ sudo ./installme
Password:
installer: Package name is nitoTV 0.2.6
installer: Installing onto volume mounted at /.
installer: The install was successful.
Restarting Finder...
```



Step 9: Install *Perian*

- Manual installation (nitoTV install didn't work)
- Lots of command line

Apple TV by default supports this:

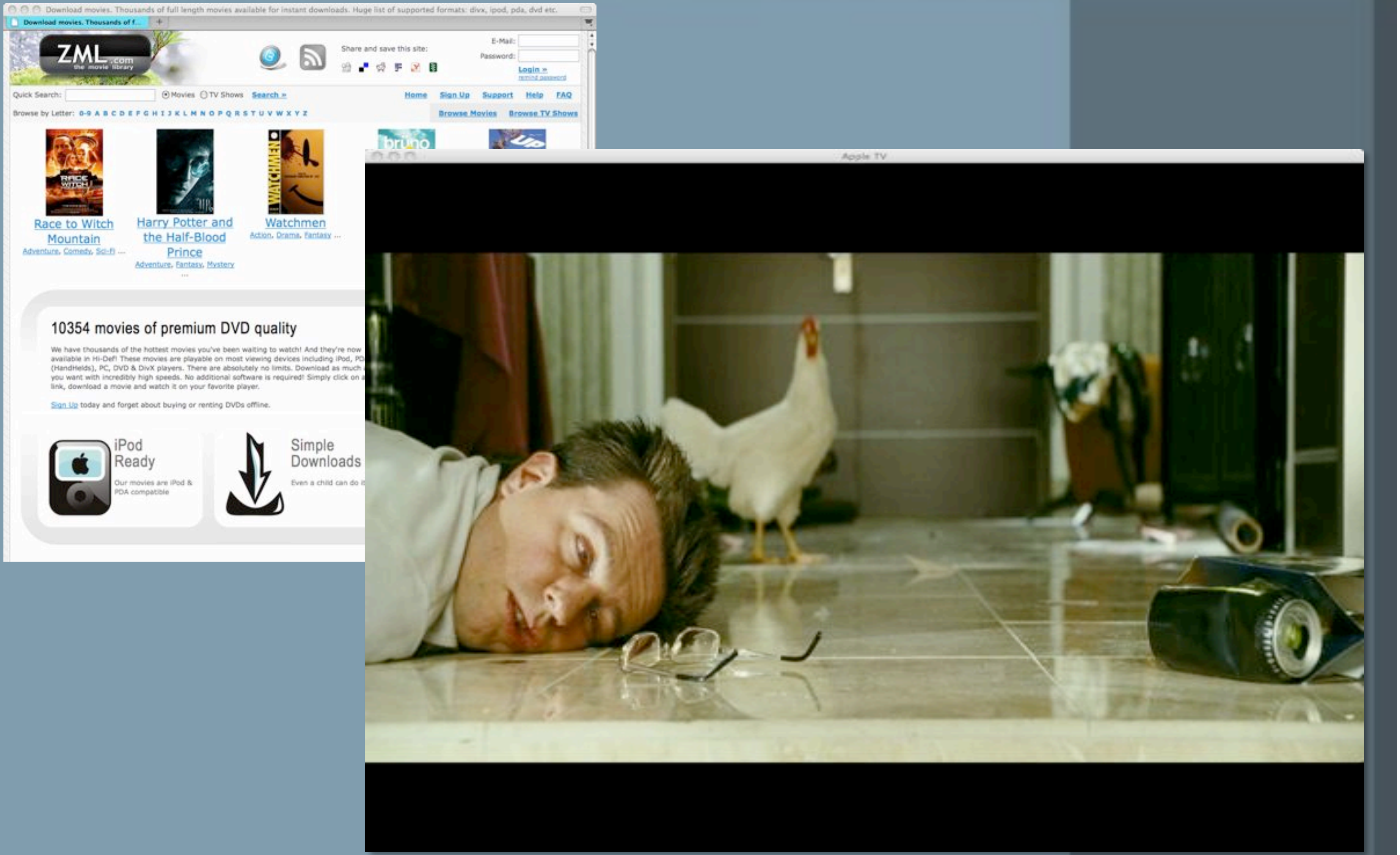


MEDIA FILES	SUPPORTED FORMATS
Video	MPEG-4 and H.264
Audio	AIFF, WAV, MP3, AAC, Apple Lossless, and Protected AAC
Photos	JPEG, BMP, GIF, TIFF, and PNG

Perian supports

- AVI, FLV, and MKV file formats
- MS-MPEG4 v1 & v2, DivX, 3ivX, H.264, FLV1, FSV1, VP6, H263I, VP3, HuffYUV, FFVHuff, MPEG1 & MPEG2 Video, Fraps, Windows Media Audio v1 & v2, Flash ADPCM, Xiph Vorbis (in Matroska), MPEG Layer II Audio
- AVI support for: AAC, AC3 Audio, H.264, MPEG4, and VBR MP3Subtitle support for SSA and SRT

Step 10: Rip/Download & Enjoy Copy, Play



Download movies. Thousands of full length movies available for instant downloads. Huge list of supported formats: divx, ipod, pda, dvd etc.
Download movies. Thousands of f...
ZML.com
the movie library
Share and save this site:
E-Mail:
Password:
Login »
remind password
Quick Search:
◉ Movies ○ TV Shows
Search »
Home
Sign Up
Support
Help
FAQ
Browse by Letter: 0-9 A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Browse Movies
Browse TV Shows
Race to Witch Mountain
Adventure, Comedy, Sci-Fi ...
Harry Potter and the Half-Blood Prince
Adventure, Fantasy, Mystery ...
Watchmen
Action, Drama, Fantasy ...
Apple TV

10354 movies of premium DVD quality

We have thousands of the hottest movies you've been waiting to watch! And they're now available in Hi-Def! These movies are playable on most viewing devices including iPod, PD (HandHelds), PC, DVD & DivX players. There are absolutely no limits. Download as much you want with incredibly high speeds. No additional software is required! Simply click on a link, download a movie and watch it on your favorite player.

Sign Up today and forget about buying or renting DVDs offline.

iPod Ready

Our movies are iPod & PDA compatible

Simple Downloads

Even a child can do it

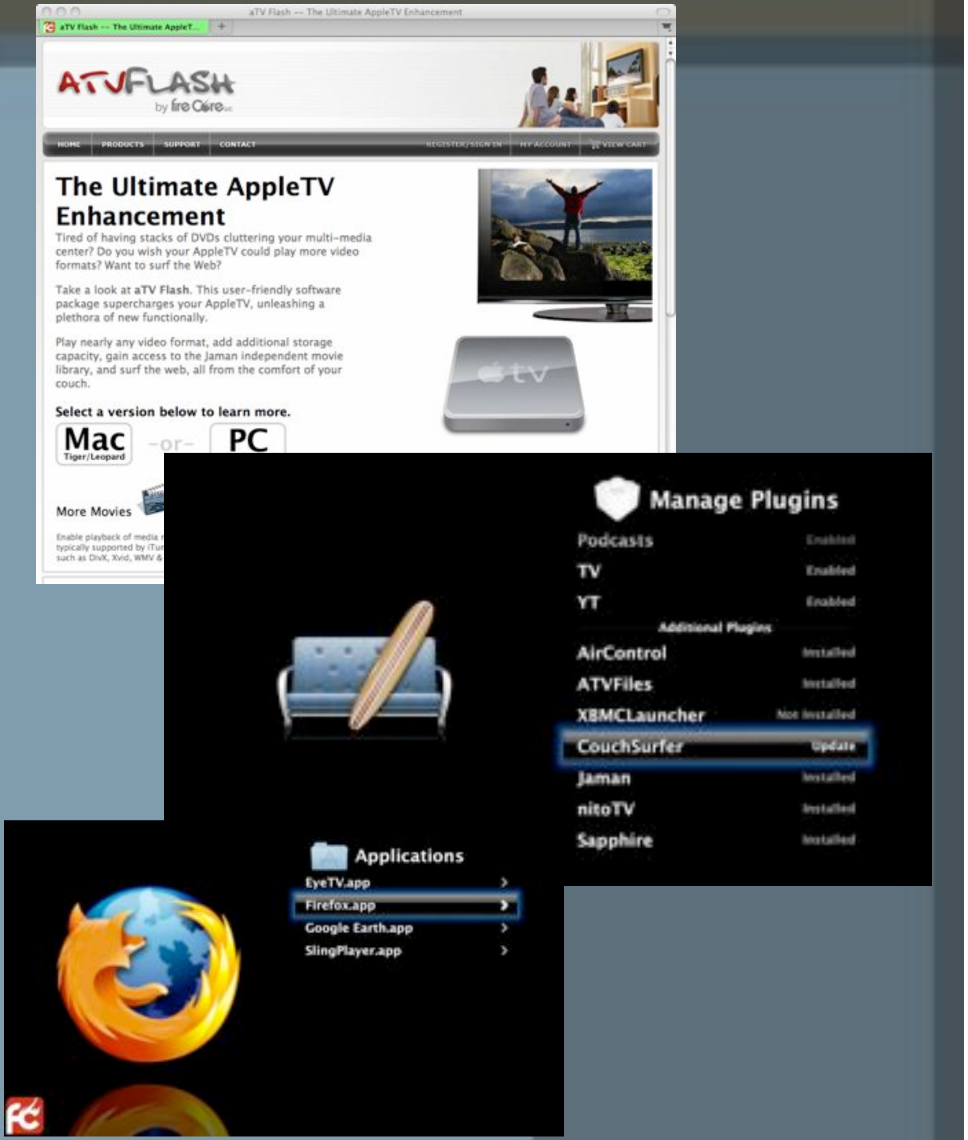
The New Way

Patchstick Summary

- Requires a USB drive
- Uses *boot.efi* from an existing Apple TV OS disk image
- Some version of bootable Linux
- Enable SSH and add *Finder.app* appliances (*.frappliance)
- Made for use by people with basic understanding of computers

aTV Flash - Overview

- Commercial patchstick ($49.95, includes 1-year of updates)
- Code has comments and subdirectories
- Mac and PC versions
- Installs a lot of applications others don't
- Integrates with NitoTV (tracks Smart Installer and places "extras" in NitoTV App menu)



aTV Flash -- The Ultimate AppleTV Enhancement
aTV Flash -- The Ultimate AppleT...
ATVFLASH
by fireCore
HOME
PRODUCTS
SUPPORT
CONTACT
REGISTER/SIGN IN
MY ACCOUNT
VIEW CART

The Ultimate AppleTV Enhancement

Tired of having stacks of DVDs cluttering your multi-media center? Do you wish your AppleTV could play more video formats? Want to surf the Web?

Take a look at **aTV Flash**. This user-friendly software package supercharges your AppleTV, unleashing a plethora of new functionally.

Play nearly any video format, add additional storage capacity, gain access to the Jaman independent movie library, and surf the web, all from the comfort of your couch.

Select a version below to learn more.

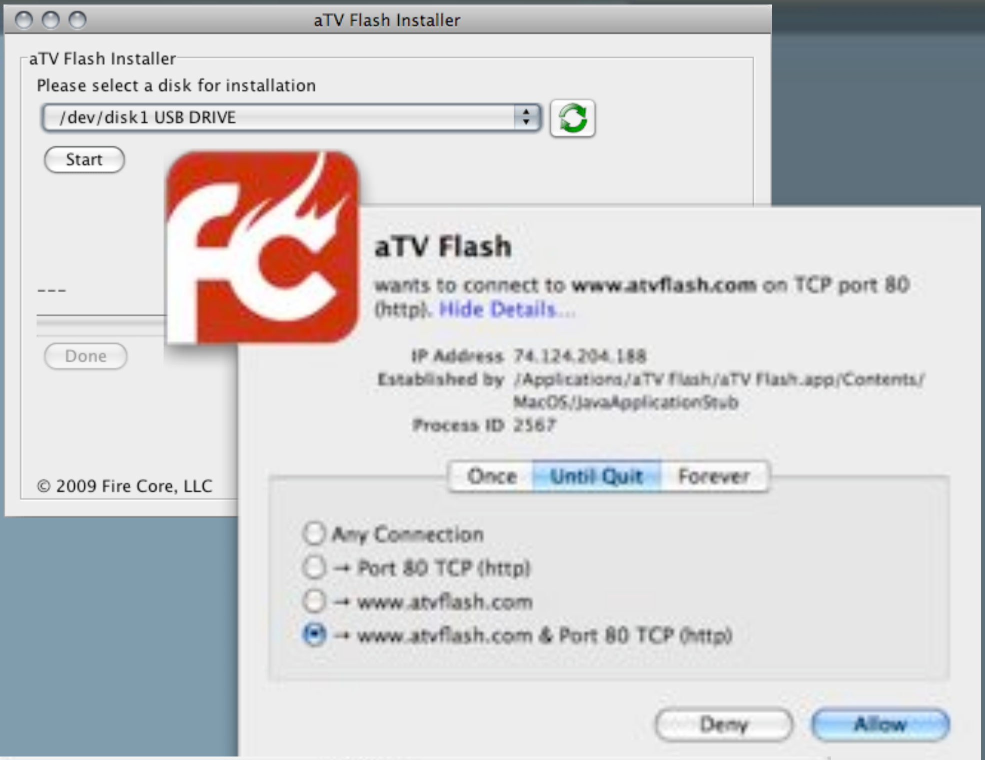
Enable playback of media
typically supported by iTu
such as DivX, Xvid, WMV &

Manage Plugins

Podcasts	Enabled
TV	Enabled
YT	Enabled
Additional Plugins	
AirControl	Installed
ATVFiles	Installed
XBMCLauncher	Not Installed
CouchSurfer	Update
Jaman	Installed
nitoTV	Installed
Sapphire	Installed

aTV Flash – Patchstick Setup

- Selects a USB drive



aTV Flash Installer

aTV Flash Installer

Please select a disk for installation

/dev/disk1 USB DRIVE

© 2009 Fire Core, LLC

aTV Flash

wants to connect to **www.atvflash.com** on TCP port 80 (http). Hide Details...

IP Address 74.124.204.188

Established by /Applications/aTV Flash/aTV Flash.app/Contents/MacOS/JavaApplicationStub

Process ID 2567

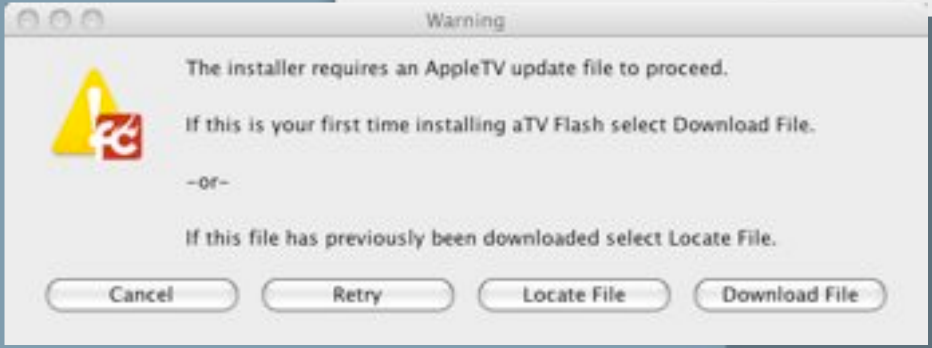
○ Any Connection

○ → Port 80 TCP (http)

○ → www.atvflash.com

● → www.atvflash.com & Port 80 TCP (http)

- Calls home to check for Internet connectivity



Warning

The installer requires an AppleTV update file to proceed.

If this is your first time installing aTV Flash select Download File.

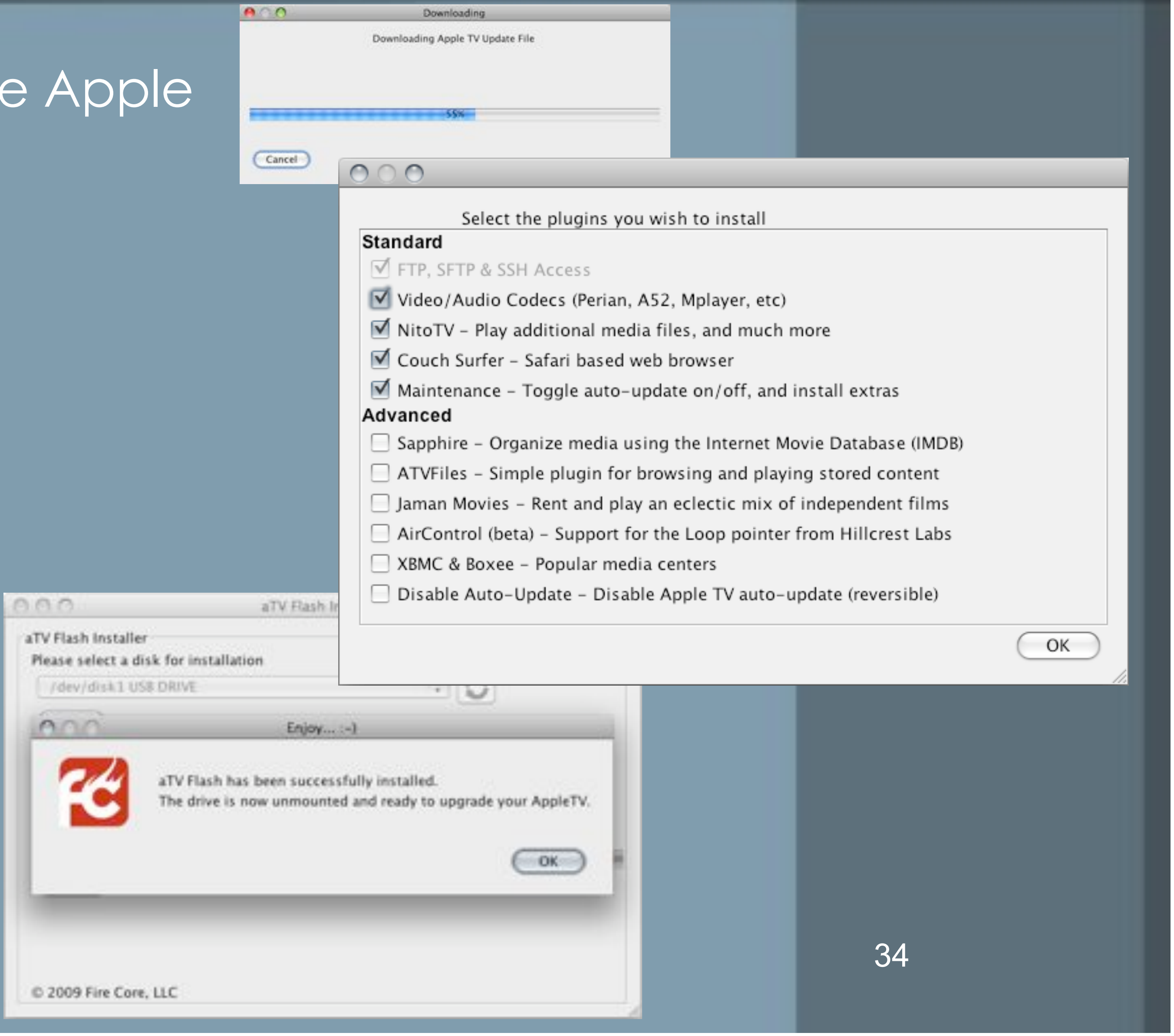
-or-

If this file has previously been downloaded select Locate File.

- Either download the update or tell it where the file exists

aTV Flash – Patchstick Setup

- Downloads the Apple TV OS Update
- Tell it what you want to do
- Done



Downloading Apple TV Update File

Select the plugins you wish to install

Standard

☑ FTP, SFTP & SSH Access
☑ Video/Audio Codecs (Perian, A52, Mplayer, etc)
☑ NitoTV – Play additional media files, and much more
☑ Couch Surfer – Safari based web browser
☑ Maintenance – Toggle auto-update on/off, and install extras

Advanced

☐ Sapphire – Organize media using the Internet Movie Database (IMDB)
☐ ATVFiles – Simple plugin for browsing and playing stored content
☐ Jaman Movies – Rent and play an eclectic mix of independent films
☐ AirControl (beta) – Support for the Loop pointer from Hillcrest Labs
☐ XBMC & Boxee – Popular media centers
☐ Disable Auto-Update – Disable Apple TV auto-update (reversible)

aTV Flash Installer

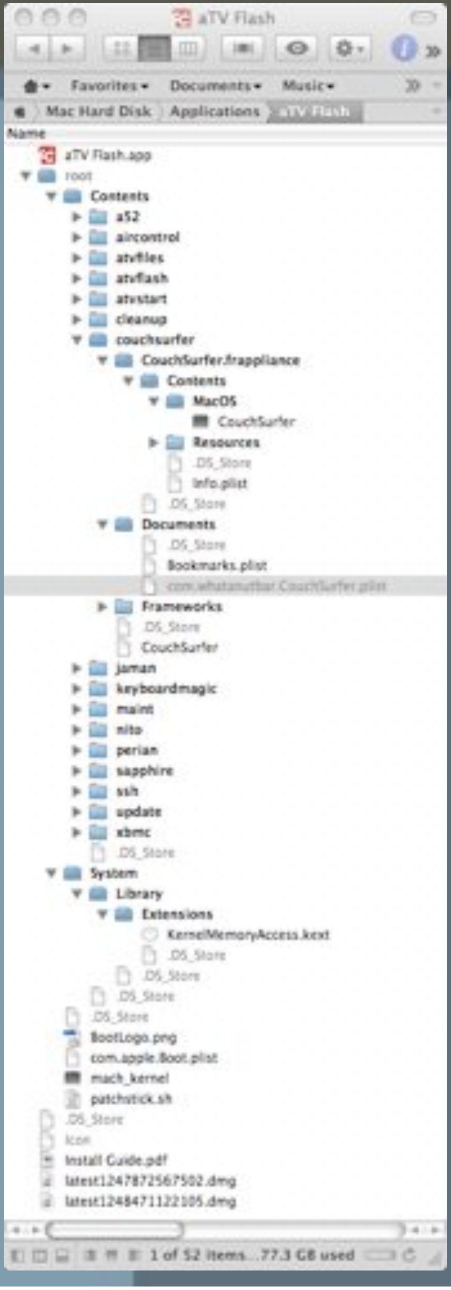
Please select a disk for installation: /dev/disk1 USB DRIVE

aTV Flash has been successfully installed.
The drive is now unmounted and ready to upgrade your AppleTV.

© 2009 Fire Core, LLC

aTV Flash – File Structure

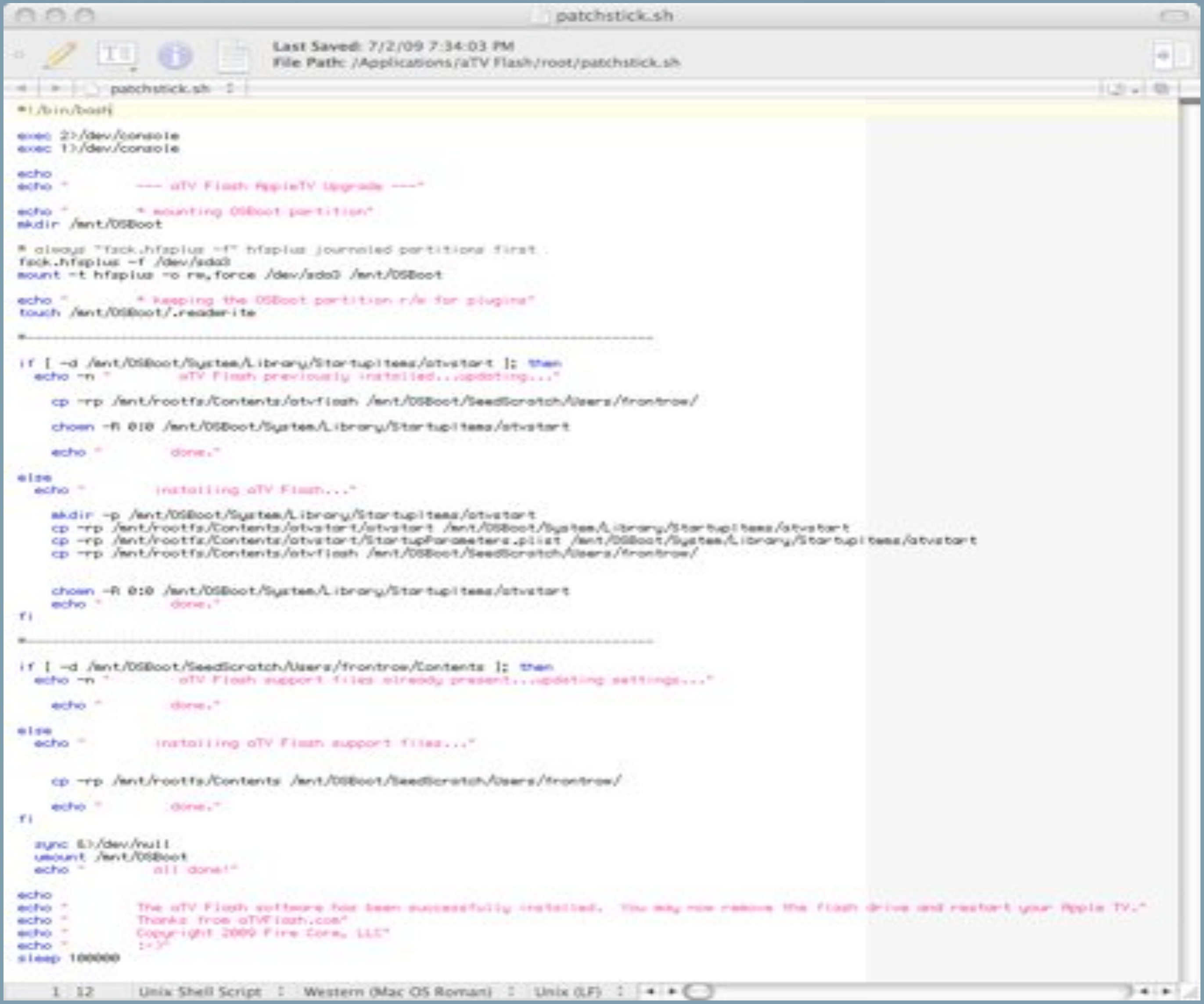
- aTV Flash.app is the actual application
- A hidden subdirectory *root* is created; this is what is put on the thumbdrive
- Notice the directory structure of applications (including the .plist for CouchSurfer) and the *latestXXXX.dmg* at the bottom of the window



```
aTV Flash.app
▼ root
    ▼ Contents
        ▶ a52
        ▶ aircontrol
        ▶ atvfiles
        ▶ atvflash
        ▶ atvstart
        ▶ cleanup
        ▼ couchsurfer
            ▼ CouchSurfer.frappliance
                ▼ Contents
                    ▼ MacOS
                        CouchSurfer
                    ▶ Resources
                    .DS_Store
                    Info.plist
                .DS_Store
            ▼ Documents
                .DS_Store
                Bookmarks.plist
                com.whatanutbar.CouchSurfer.plist
            ▶ Frameworks
            .DS_Store
            CouchSurfer
        ▶ jaman
        ▶ keyboardmagic
        ▶ maint
        ▶ nito
        ▶ perian
        ▶ sapphire
        ▶ ssh
        ▶ update
        ▶ xbmc
        .DS_Store
    ▼ System
        ▼ Library
            ▼ Extensions
                KernelMemoryAccess.kext
                .DS_Store
            .DS_Store
        .DS_Store
    .DS_Store
    BootLogo.png
    com.apple.Boot.plist
    mach_kernel
    patchstick.sh
.DS_Store
Icon
Install Guide.pdf
latest1247872567502.dmg
latest1248471122105.dmg
```

1 of 52 items, 77.3 GB used

aTV Flash – Patchstick.sh

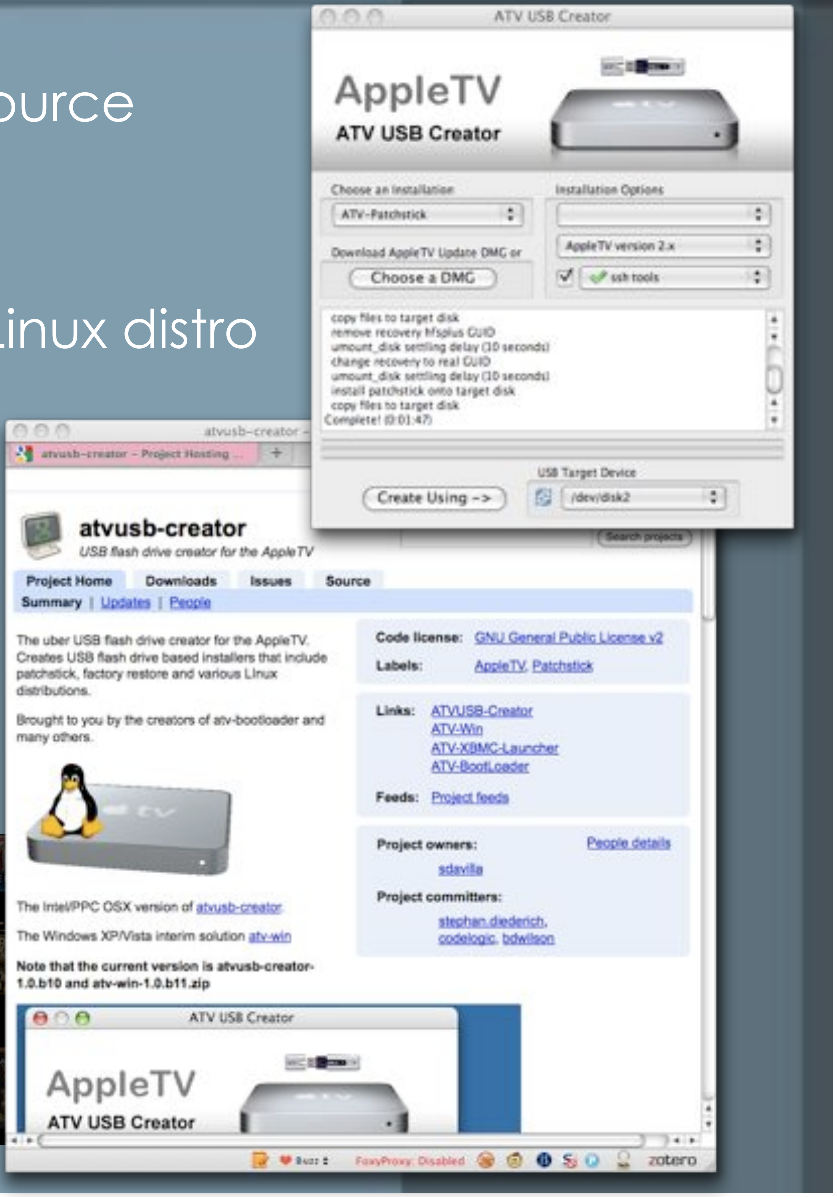


Last Saved: 7/2/09 7:34:03 PM
File Path: /Applications/aTV Flash/root/patchstick.sh

```
#!/bin/bash

exec 2>/dev/console
exec 1>/dev/console

echo
echo "          ---- aTV Flash AppleTV Upgrade ---"

echo "          * mounting OSBoot partition"
mkdir /mnt/OSBoot

# always "fsck.hfsplus -f" hfsplus journaled partitions first .
fsck.hfsplus -f /dev/sda3
mount -t hfsplus -o rw,force /dev/sda3 /mnt/OSBoot

echo "          * keeping the OSBoot partition r/w for plugins"
touch /mnt/OSBoot/.readwrite

#------------------------------------------------------------------------------

if [ -d /mnt/OSBoot/System/Library/StartupItems/atvstart ]; then
  echo -n "          aTV Flash previously installed...updating..."

    cp -rp /mnt/rootfs/Contents/atvflash /mnt/OSBoot/SeedScratch/Users/frontrow/

    chown -R 0:0 /mnt/OSBoot/System/Library/StartupItems/atvstart

    echo "          done."

else
  echo "          installing aTV Flash..."

    mkdir -p /mnt/OSBoot/System/Library/StartupItems/atvstart
    cp -rp /mnt/rootfs/Contents/atvstart/atvstart /mnt/OSBoot/System/Library/StartupItems/atvstart
    cp -rp /mnt/rootfs/Contents/atvstart/StartupParameters.plist /mnt/OSBoot/System/Library/StartupItems/atvstart
    cp -rp /mnt/rootfs/Contents/atvflash /mnt/OSBoot/SeedScratch/Users/frontrow/


    chown -R 0:0 /mnt/OSBoot/System/Library/StartupItems/atvstart
    echo "          done."
fi

#------------------------------------------------------------------------------

if [ -d /mnt/OSBoot/SeedScratch/Users/frontrow/Contents ]; then
  echo -n "          aTV Flash support files already present...updating settings..."

    echo "          done."

else
  echo "          installing aTV Flash support files..."


    cp -rp /mnt/rootfs/Contents /mnt/OSBoot/SeedScratch/Users/frontrow/

    echo "          done."
fi

  sync &>/dev/null
  umount /mnt/OSBoot
  echo "          all done!"

echo
echo "          The aTV Flash software has been successfully installed.  You may now remove the flash drive and restart your Apple TV."
echo "          Thanks from aTVFlash.com"
echo "          Copyright 2009 Fire Core, LLC"
echo "          :-)"
sleep 100000
```

ATVUSB-Creator Overview

- ATVUSB-Creator creates an open-source patchstick.
- ATVUSB-Creator can also create a "Bootstick"…if you want to boot a Linux distro
- Windows and Mac versions
- Application is being actively developed and improved
- Adds SSH, File Utils, Software Menu, and XMBC/Boxee to Apple TV



ATV USB Creator

AppleTV

ATV USB Creator

Choose an Installation: ATV-Patchstick

Installation Options: AppleTV version 2.x

☑ ssh tools

Download AppleTV Update DMG or

Choose a DMG

```
copy files to target disk
remove recovery hfsplus GUID
umount_disk settling delay (10 seconds)
change recovery to real GUID
umount_disk settling delay (10 seconds)
install patchstick onto target disk
copy files to target disk
Complete! (0:01:47)
```

USB Target Device: /dev/disk2

Create Using ->

atvusb-creator – Project Hosting ...

Search projects

atvusb-creator

USB flash drive creator for the AppleTV

Project Home | Downloads | Issues | Source

Summary | Updates | People

The uber USB flash drive creator for the AppleTV. Creates USB flash drive based installers that include patchstick, factory restore and various Linux distributions.

Brought to you by the creators of atv-bootloader and many others.

The Intel/PPC OSX version of atvusb-creator.

The Windows XP/Vista interim solution atv-win

Note that the current version is atvusb-creator-1.0.b10 and atv-win-1.0.b11.zip

ATV USB Creator

AppleTV

ATV USB Creator

Code license: GNU General Public License v2

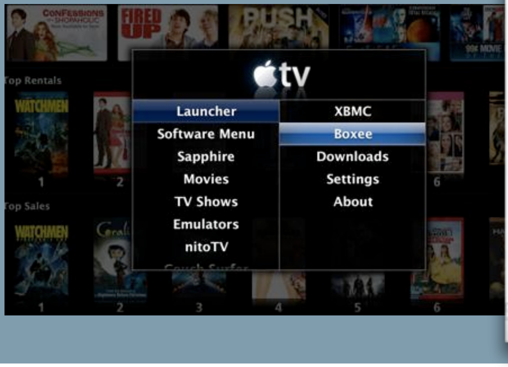
Labels: AppleTV, Patchstick

Links: ATVUSB-Creator
ATV-Win
ATV-XBMC-Launcher
ATV-BootLoader

Feeds: Project feeds

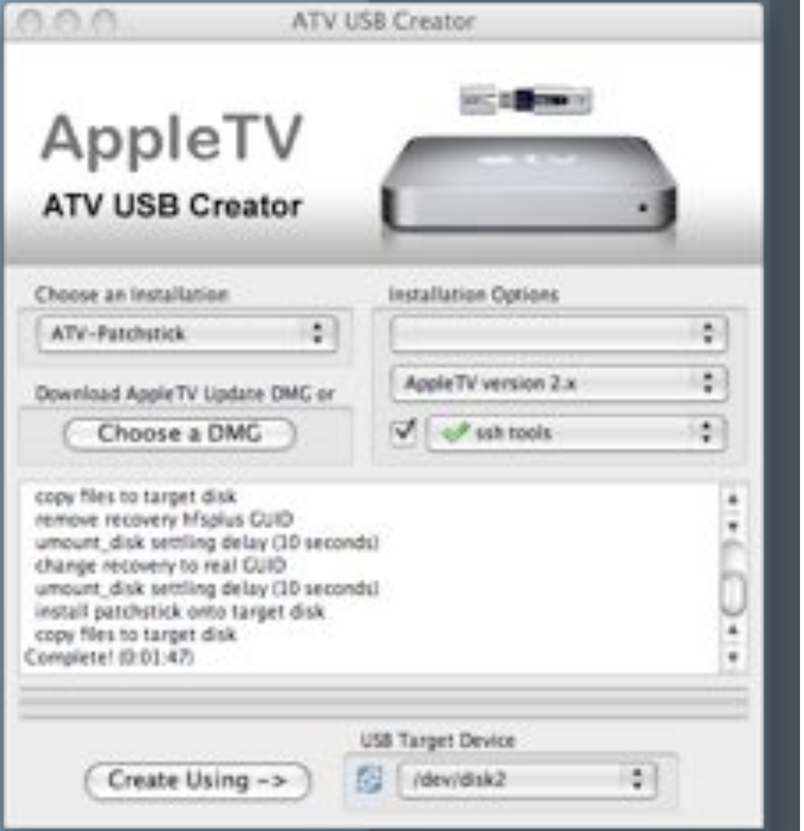
Project owners: People details
sdavila

Project committers:
stephan.diederich, codelogic, bdwilson



ATVUSB-Creator - Patchstick Setup

- Locate a compatible USB thumb drive (not all are created equal)
- Determine appropriate /dev/<*target-drive*>
- Ensure the tools you want are selected
- Click “Create Using ->”…unless you are rolling your own “uber” ATV Recovery DMG
- In about two minutes, you have a handy-dandy ATV-USB Creator patchstick



Choose an installation: ATV-Patchstick

Download AppleTV Update DMG or

Installation Options: AppleTV version 2.x

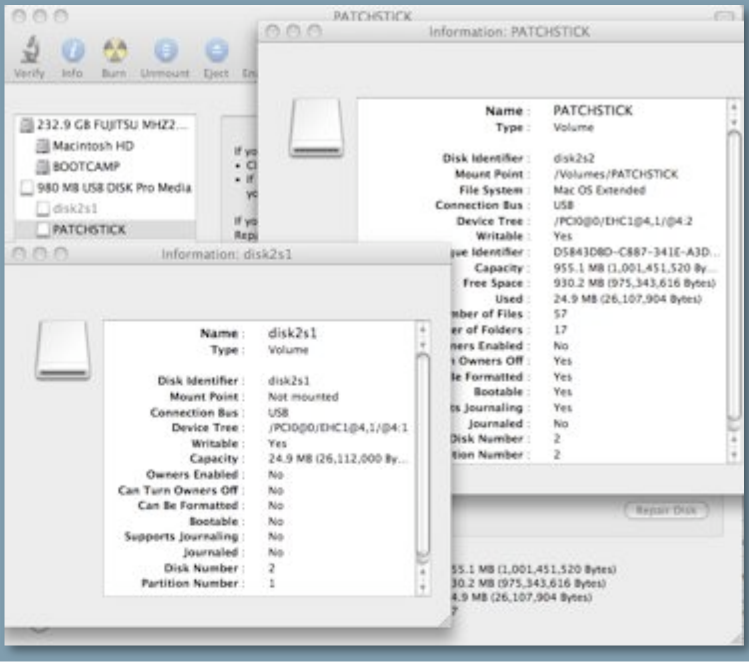
☑ ssh tools

```
 copy files to target disk
 remove recovery hfsplus GUID
 umount_disk settling delay (10 seconds)
 change recovery to real GUID
 umount_disk settling delay (10 seconds)
 install patchstick onto target disk
 copy files to target disk
Complete! (0:01:47)
```

USB Target Device: /dev/disk2

ATVUSB-Creator - Patchstick Setup

- ATVUSB-Creator makes two partitions on the thumb drive
- Uses EFI to mount ATV drive and make modifications



```
232.9 GB FUJITSU MHZ2...
  Macintosh HD
  BOOTCAMP
980 MB USB DISK Pro Media
  disk2s1
  PATCHSTICK
```

Information: PATCHSTICK

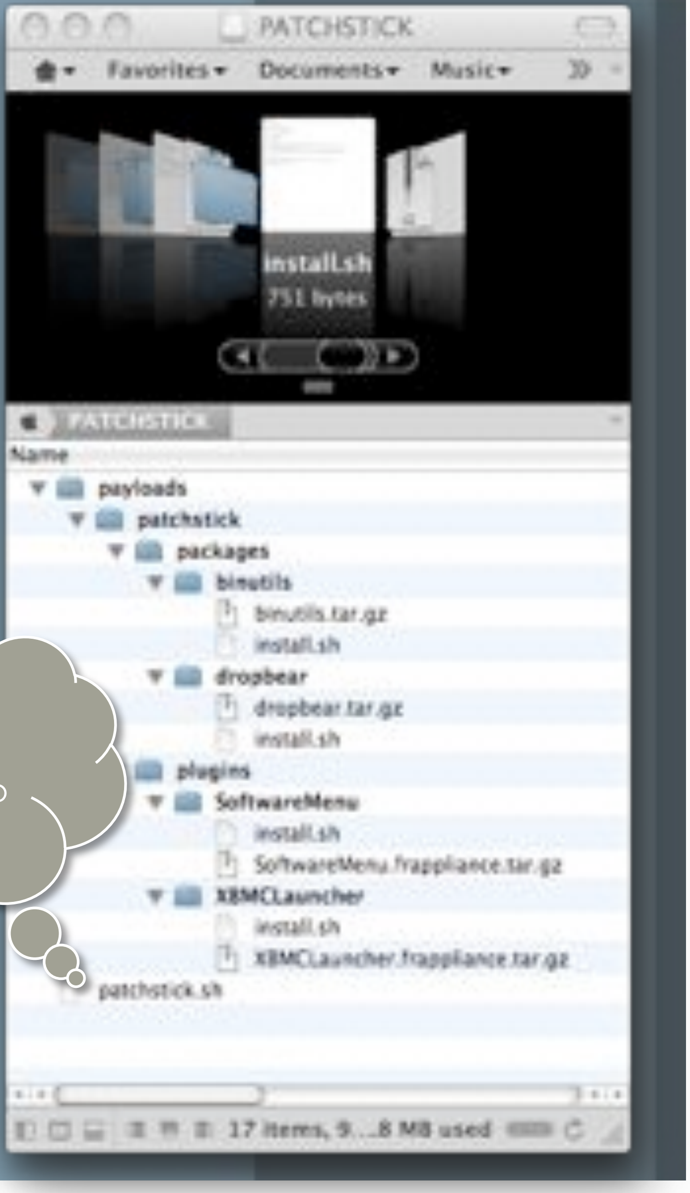
```
               Name :  PATCHSTICK
               Type :  Volume

    Disk Identifier :  disk2s2
        Mount Point :  /Volumes/PATCHSTICK
        File System :  Mac OS Extended
     Connection Bus :  USB
        Device Tree :  /PCI0@0/EHC1@4,1/@4:2
           Writable :  Yes
       ue Identifier :  D5843D8D-C887-341E-A3D...
           Capacity :  955.1 MB (1,001,451,520 By...
         Free Space :  930.2 MB (975,343,616 Bytes)
               Used :  24.9 MB (26,107,904 Bytes)
       mber of Files :  57
      er of Folders :  17
       ners Enabled :  No
        Owners Off :  Yes
        e Formatted :  Yes
           Bootable :  Yes
        s Journaling :  Yes
          Journaled :  No
        Disk Number :  2
        tion Number :  2
```

Information: disk2s1

```
               Name :  disk2s1
               Type :  Volume

    Disk Identifier :  disk2s1
        Mount Point :  Not mounted
     Connection Bus :  USB
        Device Tree :  /PCI0@0/EHC1@4,1/@4:1
           Writable :  Yes
           Capacity :  24.9 MB (26,112,000 By...
     Owners Enabled :  No
Can Turn Owners Off :  No
   Can Be Formatted :  No
           Bootable :  No
Supports Journaling :  No
          Journaled :  No
        Disk Number :  2
   Partition Number :  1
```

```
55.1 MB (1,001,451,520 Bytes)
30.2 MB (975,343,616 Bytes)
4.9 MB (26,107,904 Bytes)
```

Hum…wonder if you can edit "patchstick.sh to add your own custom items

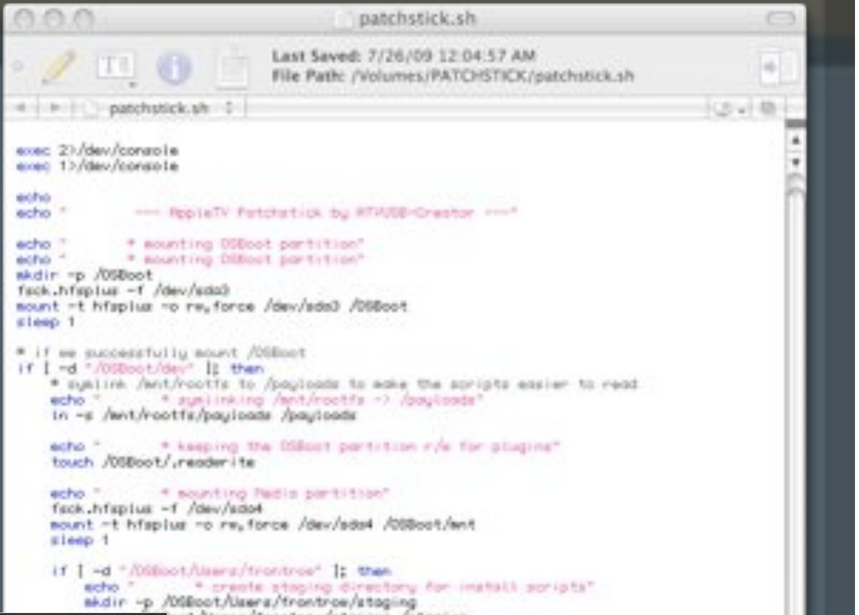


```
payloads
  patchstick
    packages
      binutils
        binutils.tar.gz
        install.sh
      dropbear
        dropbear.tar.gz
        install.sh
    plugins
      SoftwareMenu
        install.sh
        SoftwareMenu.frappliance.tar.gz
      XBMCLauncher
        install.sh
        XBMCLauncher.frappliance.tar.gz
patchstick.sh
```

17 items, 9...8 MB used

ATVUSB-Creator - Patchstick script

- ATVUSB-Creator mounts ATV hard drive in RW
- Creates some links and then searches for “install.sh” scripts
- Each “install.sh” configures and installs its package…

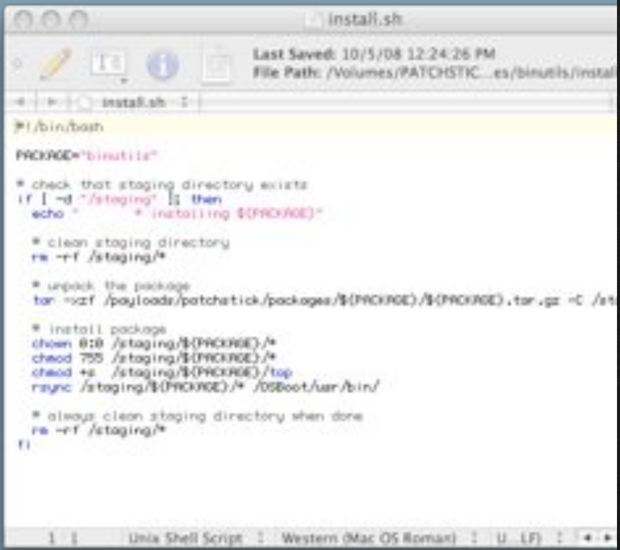


patchstick.sh

Last Saved: 7/26/09 12:04:57 AM
File Path: /Volumes/PATCHSTICK/patchstick.sh

```
exec 2>/dev/console
exec 1>/dev/console

echo
echo "        --- AppleTV Patchstick by ATVUSB-Creator ---"

echo "       * mounting OSBoot partition"
echo "       * mounting OSBoot partition"
mkdir -p /OSBoot
fsck.hfsplus -f /dev/sda3
mount -t hfsplus -o rw,force /dev/sda3 /OSBoot
sleep 1

# if we successfully mount /OSBoot
if [ -d "/OSBoot/dev" ]; then
    # symlink /mnt/rootfs to /payloads to make the scripts easier to read
    echo "       * symlinking /mnt/rootfs -> /payloads"
    ln -s /mnt/rootfs/payloads /payloads

    echo "       * keeping the OSBoot partition r/w for plugins"
    touch /OSBoot/.readwrite

    echo "       * mounting Media partition"
    fsck.hfsplus -f /dev/sda4
    mount -t hfsplus -o rw,force /dev/sda4 /OSBoot/mnt
    sleep 1

    if [ -d "/OSBoot/Users/frontrow" ]; then
        echo "       * create staging directory for install scripts"
        mkdir -p /OSBoot/Users/frontrow/staging
              oot/Users/frontrow/staging /staging

              t in $( find /payloads/ -name install.sh -print ); do
              bash "${script}"
               1

               * error mounting Media partition"

              * error mounting OSBoot partition"

              sers/frontrow/staging" ]; then
              * removing staging directory"
              t/Users/frontrow/staging

              ease unplug your Apple TV to reboot/reset the device."

              you received no errors above, then you can plug in your Apple TV, "
              ait 3 minutes, then open Terminal and type: ssh frontrow@appletv.local "
              n prompted for a password, enter: frontrow"

              other ssh clients (putty, etc): "
              stname: appletv.local  Username: frontrow  Password: frontrow"
```

Shell Script | Western (Mac OS Roman) | Unix (LF)

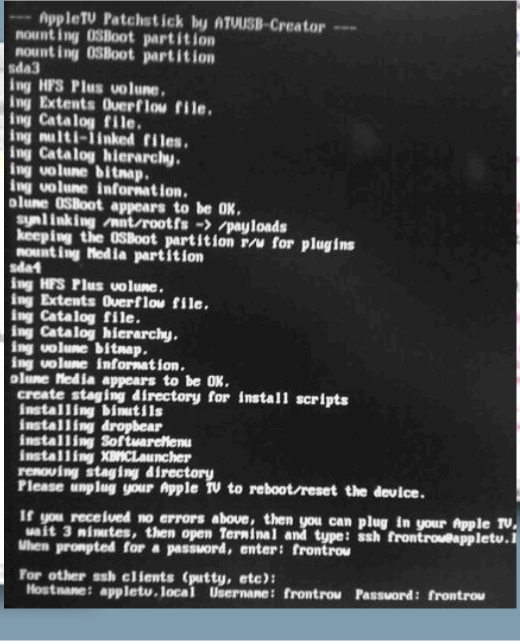


install.sh

Last Saved: 10/5/08 12:24:26 PM
File Path: /Volumes/PATCHSTIC...es/binutils/instal

```
#!/bin/bash

PACKAGE="binutils"

# check that staging directory exists
if [ -d "/staging" ]; then
  echo "        * installing ${PACKAGE}"

  # clean staging directory
  rm -rf /staging/*

  # unpack the package
  tar -xzf /payloads/patchstick/packages/${PACKAGE}/${PACKAGE}.tar.gz -C /st

  # install package
  chown 0:0 /staging/${PACKAGE}/*
  chmod 755 /staging/${PACKAGE}/*
  chmod +s  /staging/${PACKAGE}/top
  rsync /staging/${PACKAGE}/* /OSBoot/usr/bin/

  # always clean staging directory when done
  rm -rf /staging/*
fi
```

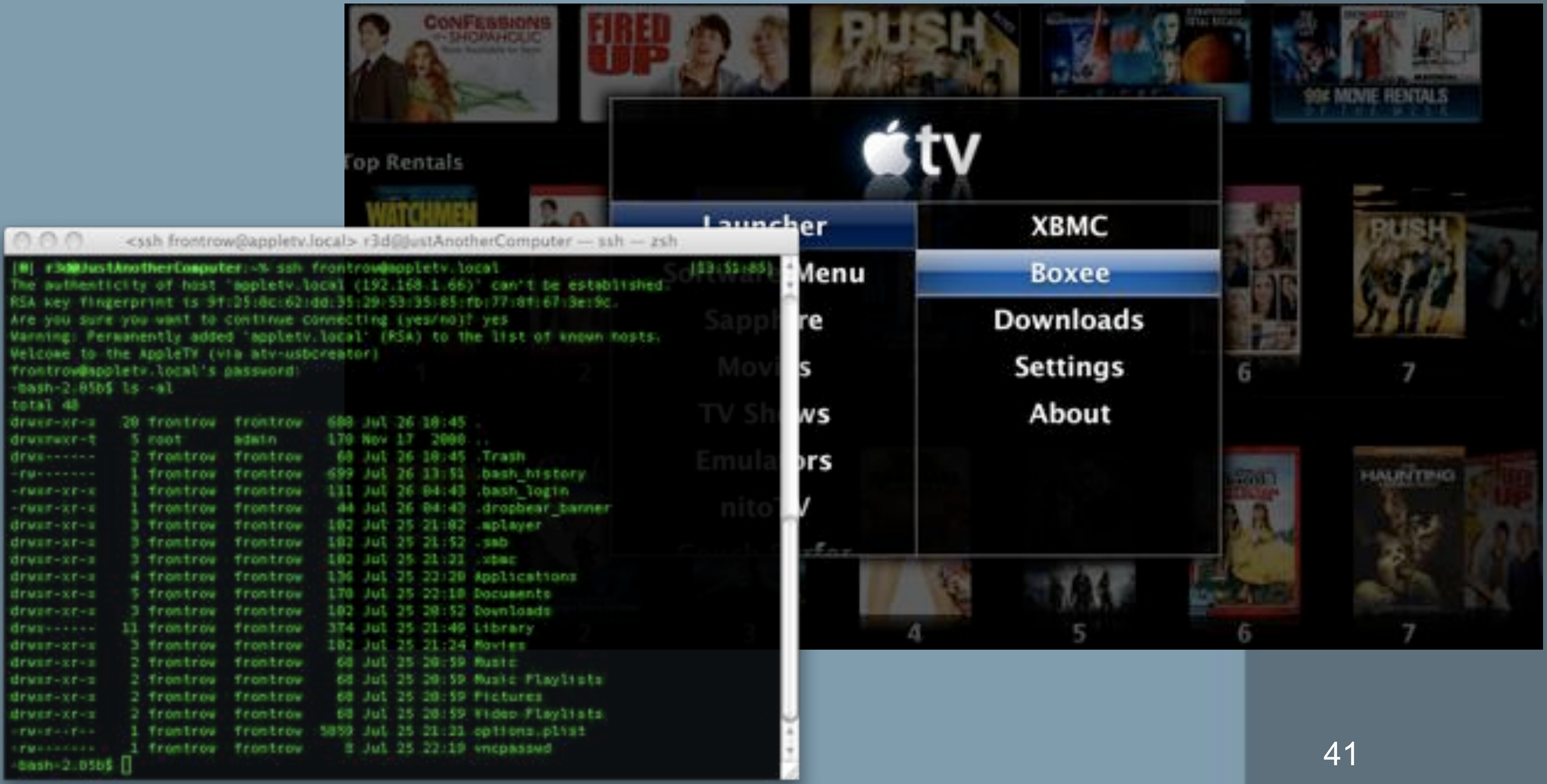
1 | Unix Shell Script | Western (Mac OS Roman) | U...LF)



```
--- AppleTV Patchstick by ATVUSB-Creator ---
 mounting OSBoot partition
 mounting OSBoot partition
sda3
ing HFS Plus volume.
ing Extents Overflow file.
ing Catalog file.
ing multi-linked files.
ing Catalog hierarchy.
ing volume bitmap.
ing volume information.
olume OSBoot appears to be OK.
 symlinking /mnt/rootfs -> /payloads
 keeping the OSBoot partition r/w for plugins
 mounting Media partition
sda4
ing HFS Plus volume.
ing Extents Overflow file.
ing Catalog file.
ing Catalog hierarchy.
ing volume bitmap.
ing volume information.
olume Media appears to be OK.
 create staging directory for install scripts
 installing binutils
 installing dropbear
 installing SoftwareMenu
 installing XBMCLauncher
 removing staging directory
 Please unplug your Apple TV to reboot/reset the device.

 If you received no errors above, then you can plug in your Apple TV,
  wait 3 minutes, then open Terminal and type: ssh frontrow@appletv.l
 When prompted for a password, enter: frontrow

 For other ssh clients (putty, etc):
  Hostname: appletv.local  Username: frontrow  Password: frontrow
```

ATVUSB-Creator - Complete

- Unplug and plug in the ATV…wait 2 minutes and *`ssh frontrow@appletv.local`*



<ssh frontrow@appletv.local> r3d@JustAnotherComputer — ssh — zsh

```
[M] r3d@JustAnotherComputer:~% ssh frontrow@appletv.local                    [13:51:05]
The authenticity of host 'appletv.local (192.168.1.66)' can't be established.
RSA key fingerprint is 9f:25:0c:62:dd:35:29:53:35:85:fb:77:8f:67:3e:9c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'appletv.local' (RSA) to the list of known hosts.
Welcome to the AppleTV (via atv-usbcreator)
frontrow@appletv.local's password:
-bash-2.05b$ ls -al
total 48
drwxr-xr-x   20 frontrow  frontrow   680 Jul 26 10:45 .
drwxrwxr-t    5 root      admin      170 Nov 17  2008 ..
drwx------    2 frontrow  frontrow    68 Jul 26 10:45 .Trash
-rw-------    1 frontrow  frontrow   699 Jul 26 13:51 .bash_history
-rwxr-xr-x    1 frontrow  frontrow   111 Jul 26 04:43 .bash_login
-rwxr-xr-x    1 frontrow  frontrow    44 Jul 26 04:43 .dropbear_banner
drwxr-xr-x    3 frontrow  frontrow   102 Jul 25 21:02 .mplayer
drwxr-xr-x    3 frontrow  frontrow   102 Jul 25 21:52 .smb
drwxr-xr-x    3 frontrow  frontrow   102 Jul 25 21:21 .xbmc
drwxr-xr-x    4 frontrow  frontrow   136 Jul 25 22:20 Applications
drwxr-xr-x    5 frontrow  frontrow   170 Jul 25 22:10 Documents
drwxr-xr-x    3 frontrow  frontrow   102 Jul 25 20:52 Downloads
drwx------   11 frontrow  frontrow   374 Jul 25 21:40 Library
drwxr-xr-x    3 frontrow  frontrow   102 Jul 25 21:24 Movies
drwxr-xr-x    2 frontrow  frontrow    68 Jul 25 20:59 Music
drwxr-xr-x    2 frontrow  frontrow    68 Jul 25 20:59 Music Playlists
drwxr-xr-x    2 frontrow  frontrow    68 Jul 25 20:59 Pictures
drwxr-xr-x    2 frontrow  frontrow    68 Jul 25 20:59 Video Playlists
-rw-r--r--    1 frontrow  frontrow  5859 Jul 25 21:21 options.plist
-rw-------    1 frontrow  frontrow     8 Jul 25 22:19 vncpasswd
-bash-2.05b$ []
```

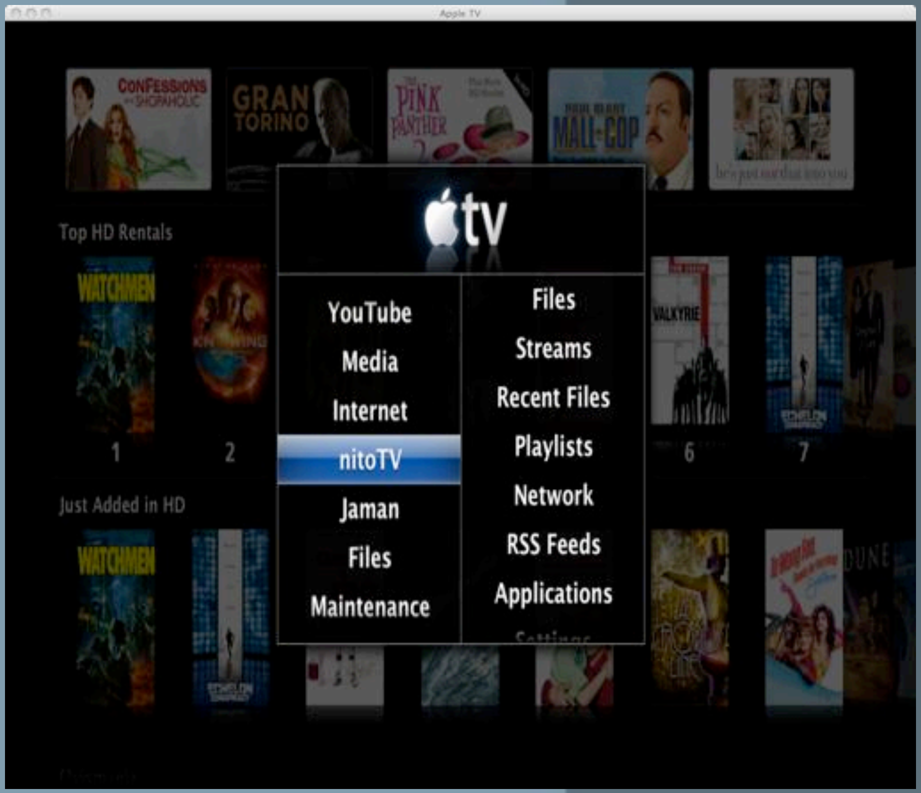
ATVUSB-Creator Demo

Popular Applications

nitoTV - Overview

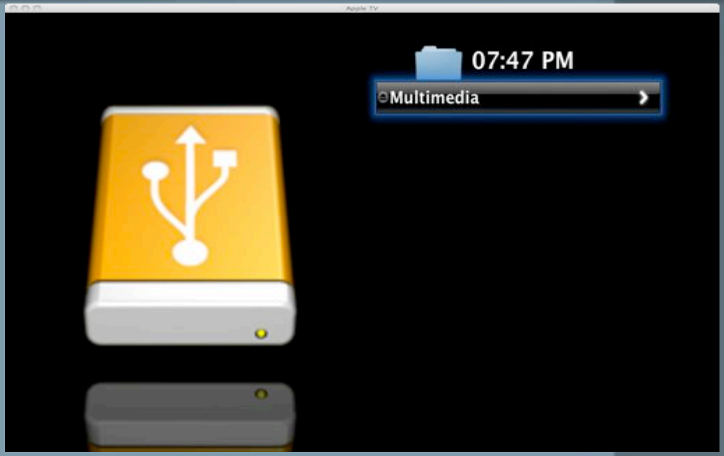
- Installed by almost all patchsticks

- Massive amount of functionality including mounting USB drives, viewing RSS feeds, and installation of 3rd-party applications

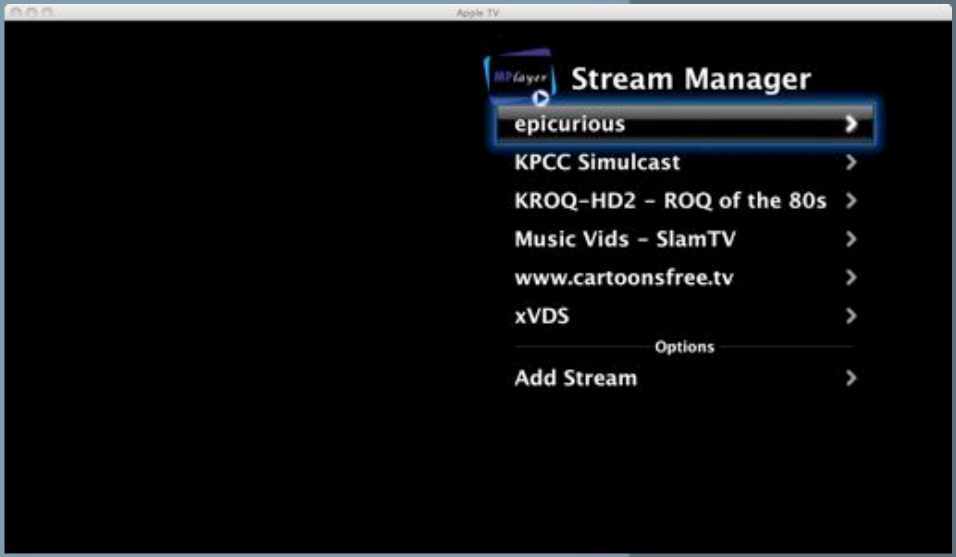


nitoTV - Overview

- *Files* menu will access USB drives

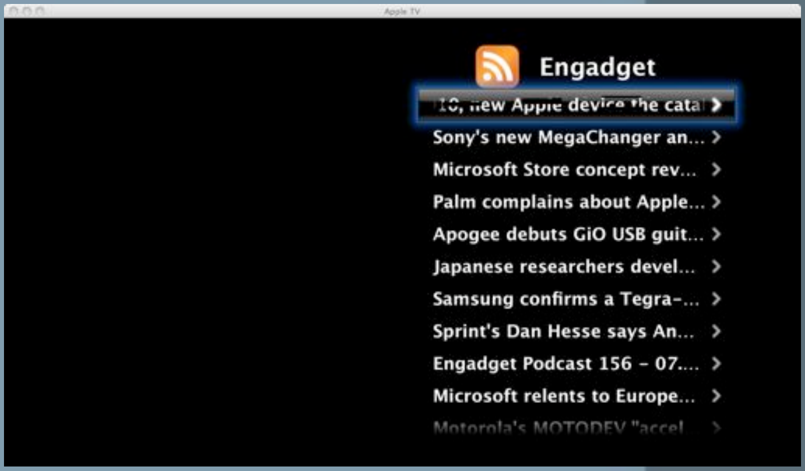


- Streams will access streaming audio/video feeds and play via mPlayer

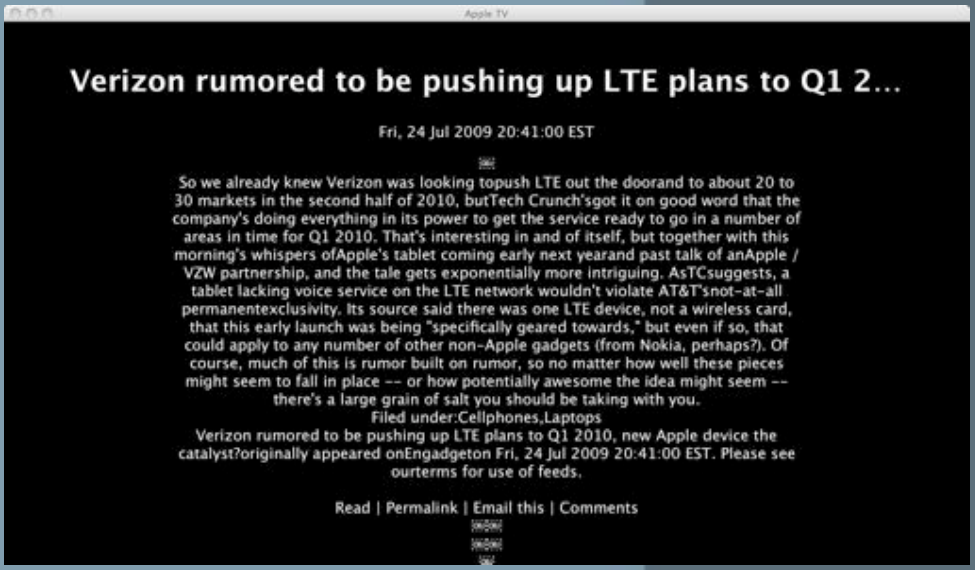


nitoTV - Overview

- *RSS* menu will load RSS feeds you configure


Apple TV
Engadget
10, new Apple device the cata
Sony's new MegaChanger an...
Microsoft Store concept rev...
Palm complains about Apple...
Apogee debuts GiO USB guit...
Japanese researchers devel...
Samsung confirms a Tegra-...
Sprint's Dan Hesse says An...
Engadget Podcast 156 - 07....
Microsoft relents to Europe...
Motorola's MOTODEV "accel

- Although articles are limited to text only



Verizon rumored to be pushing up LTE plans to Q1 2...

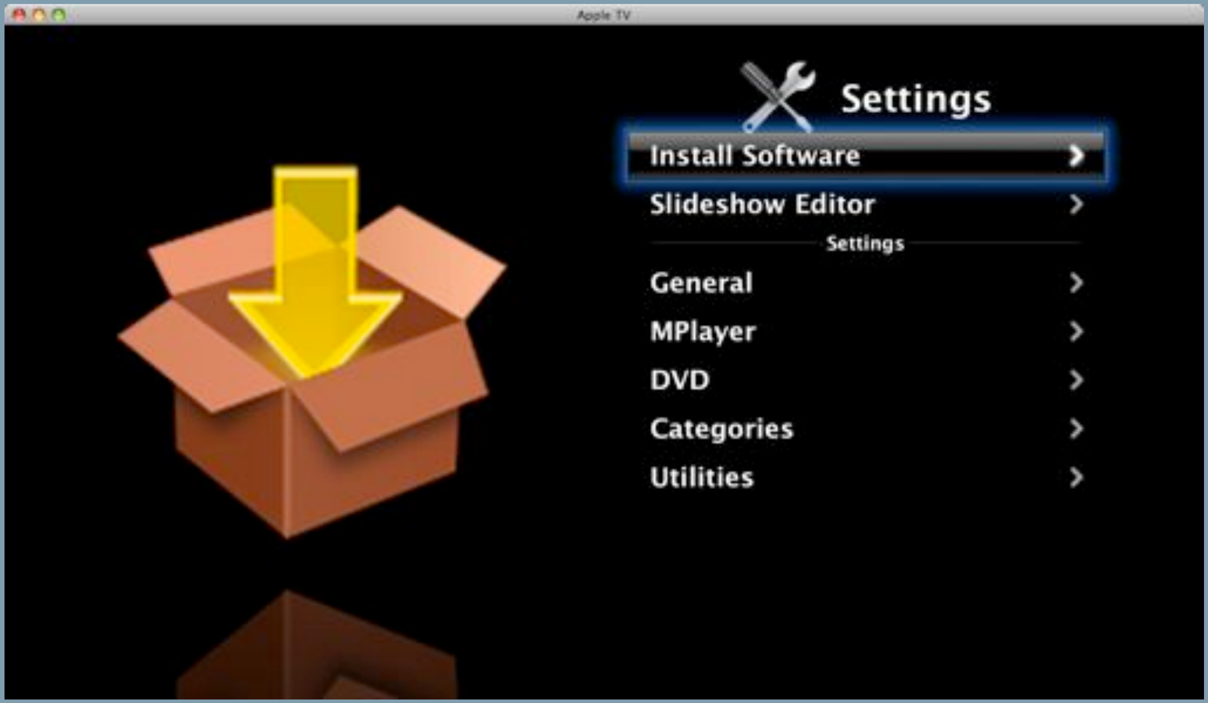
Fri, 24 Jul 2009 20:41:00 EST

So we already knew Verizon was looking topush LTE out the doorand to about 20 to 30 markets in the second half of 2010, butTech Crunch'sgot it on good word that the company's doing everything in its power to get the service ready to go in a number of areas in time for Q1 2010. That's interesting in and of itself, but together with this morning's whispers ofApple's tablet coming early next yearand past talk of anApple / VZW partnership, and the tale gets exponentially more intriguing. AsTCsuggests, a tablet lacking voice service on the LTE network wouldn't violate AT&T'snot-at-all permanentexclusivity. Its source said there was one LTE device, not a wireless card, that this early launch was being "specifically geared towards," but even if so, that could apply to any number of other non-Apple gadgets (from Nokia, perhaps?). Of course, much of this is rumor built on rumor, so no matter how well these pieces might seem to fall in place -- or how potentially awesome the idea might seem -- there's a large grain of salt you should be taking with you.
Filed under:Cellphones,Laptops
Verizon rumored to be pushing up LTE plans to Q1 2010, new Apple device the catalyst?originally appeared onEngadgeton Fri, 24 Jul 2009 20:41:00 EST. Please see ourterms for use of feeds.

Read | Permalink | Email this | Comments

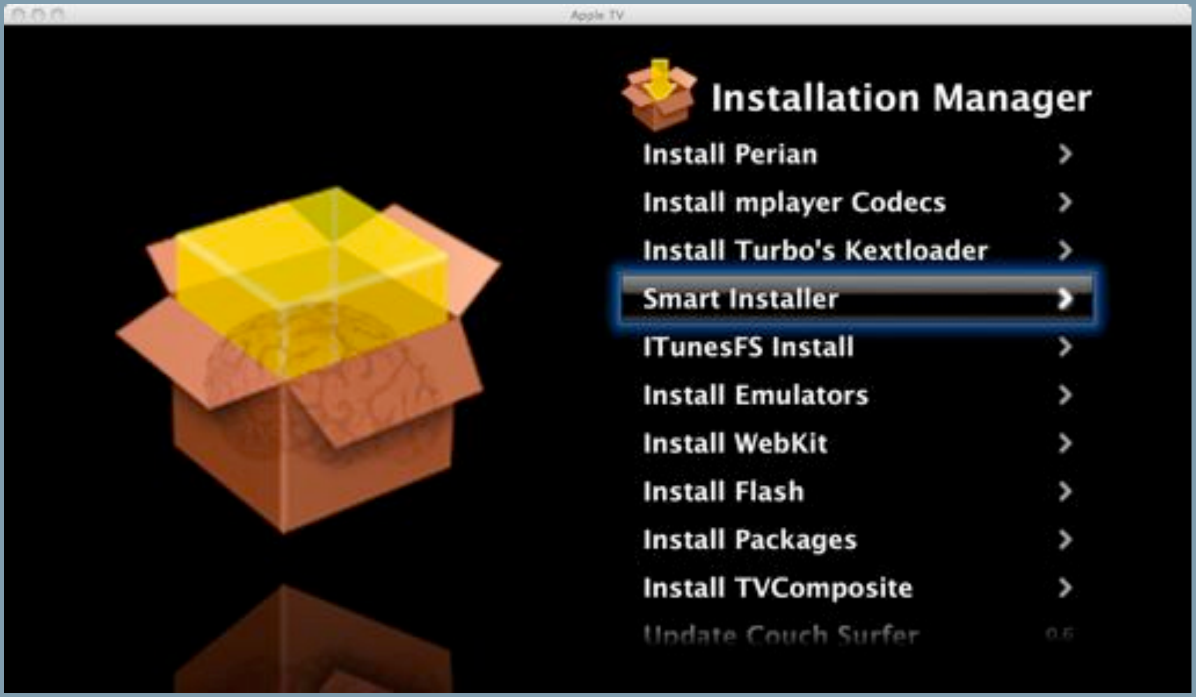
nitoTV – Overview - *Settings*

- Most nitoTV functionality and benefit is on the back-end utilities



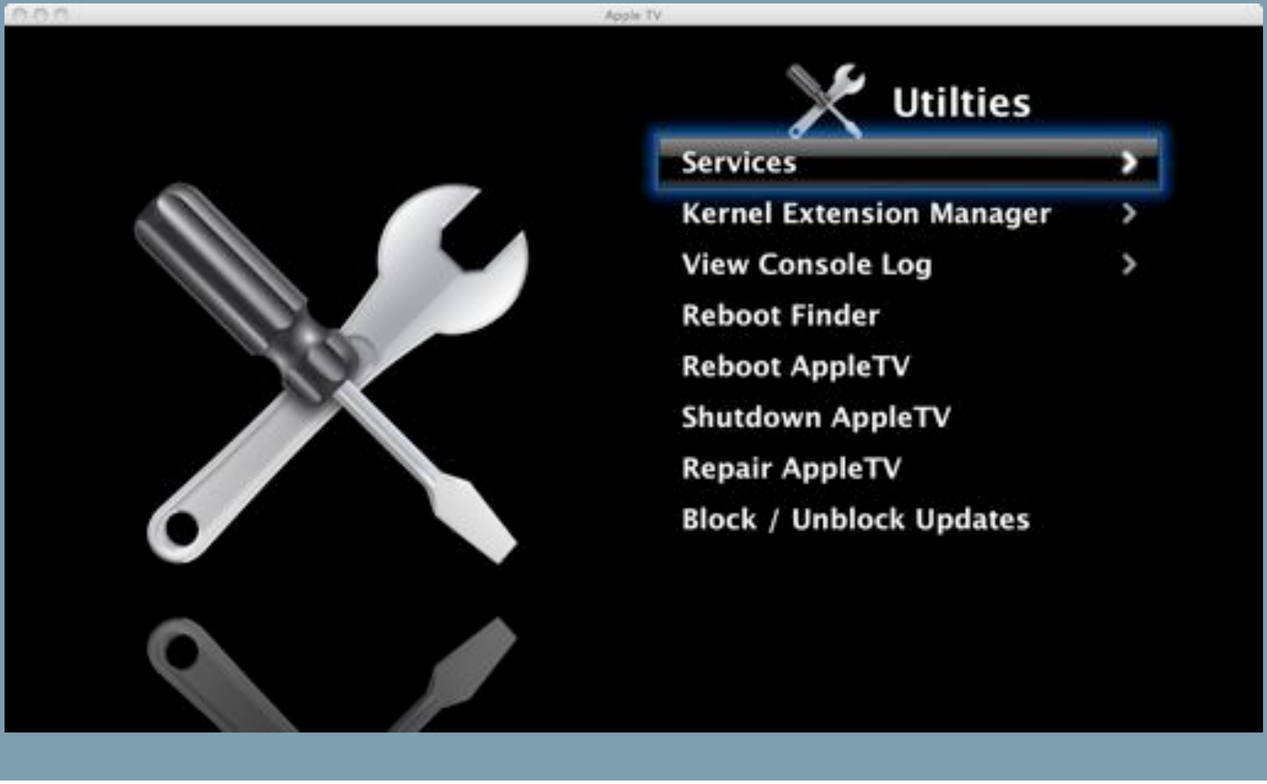
nitoTV – Overview - *Settings*

- nitoTV *Smart Installer* will not only go out and retrieve (most) of what you need it will automatically install components for you as long as the source files are present



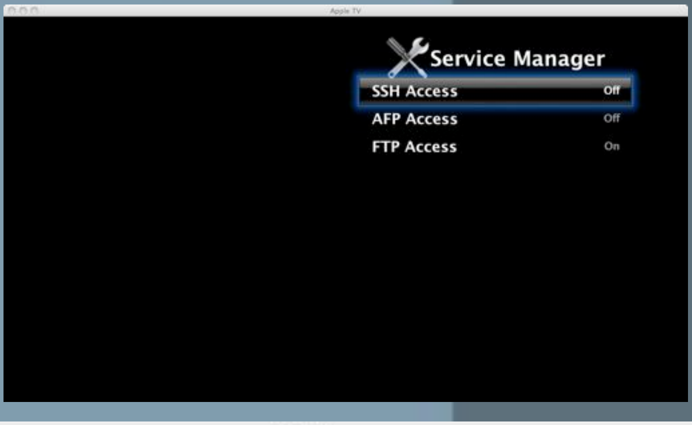
nitoTV – Overview - *Settings*

- nitoTV *Utilities* menu provides access to several sub-menus and scripts
- The reboot/shutdown scripts are most helpful since there is no other easy way



nitoTV – Overview - *Settings*

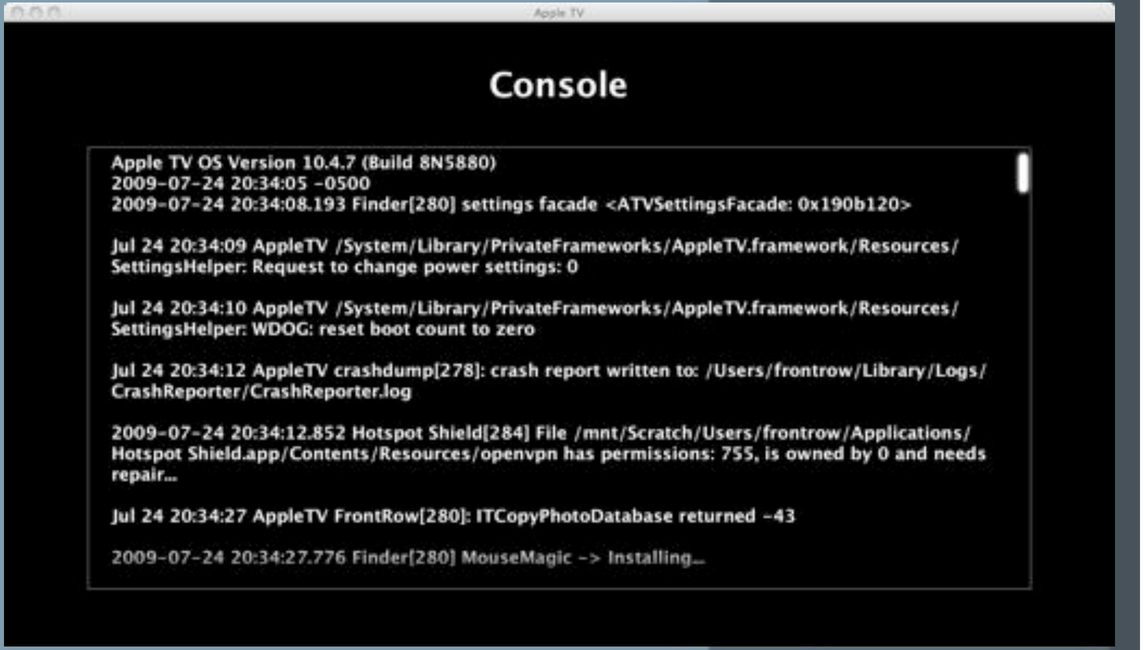
- nitoTV *Utilities – Services* menu provides access to enable/disable SecureShell, Apple Filing Protocol, and File Transfer Protocol



Service Manager

SSH Access	Off
AFP Access	Off
FTP Access	On

- nitoTV *Utilities – Console* provides read access to console logs



Console

```
Apple TV OS Version 10.4.7 (Build 8N5880)
2009-07-24 20:34:05 -0500
2009-07-24 20:34:08.193 Finder[280] settings facade <ATVSettingsFacade: 0x190b120>

Jul 24 20:34:09 AppleTV /System/Library/PrivateFrameworks/AppleTV.framework/Resources/
SettingsHelper: Request to change power settings: 0

Jul 24 20:34:10 AppleTV /System/Library/PrivateFrameworks/AppleTV.framework/Resources/
SettingsHelper: WDOG: reset boot count to zero

Jul 24 20:34:12 AppleTV crashdump[278]: crash report written to: /Users/frontrow/Library/Logs/
CrashReporter/CrashReporter.log

2009-07-24 20:34:12.852 Hotspot Shield[284] File /mnt/Scratch/Users/frontrow/Applications/
Hotspot Shield.app/Contents/Resources/openvpn has permissions: 755, is owned by 0 and needs
repair...

Jul 24 20:34:27 AppleTV FrontRow[280]: ITCopyPhotoDatabase returned -43

2009-07-24 20:34:27.776 Finder[280] MouseMagic -> Installing...
```

nitoTV Demo

Boxee Walk-through

Where Your Data Lives

Forensics Data – Topics

- What are the big ticket items?
  - Hardware Analysis from a Forensic Examiner Perspective
  - Software Summary from a Forensic Examiner Perspective
  - File Structures
  - Basic Forensic Considerations
    - General Forensic Considerations
    - Discovery
    - Investigations
    - Files (Almost) Always Modified
  - Apple TV Files and Directories Important to Forensic Analysis
    - Basic Areas for User Data
    - Areas Where Most Data Resides

Hardware Analysis

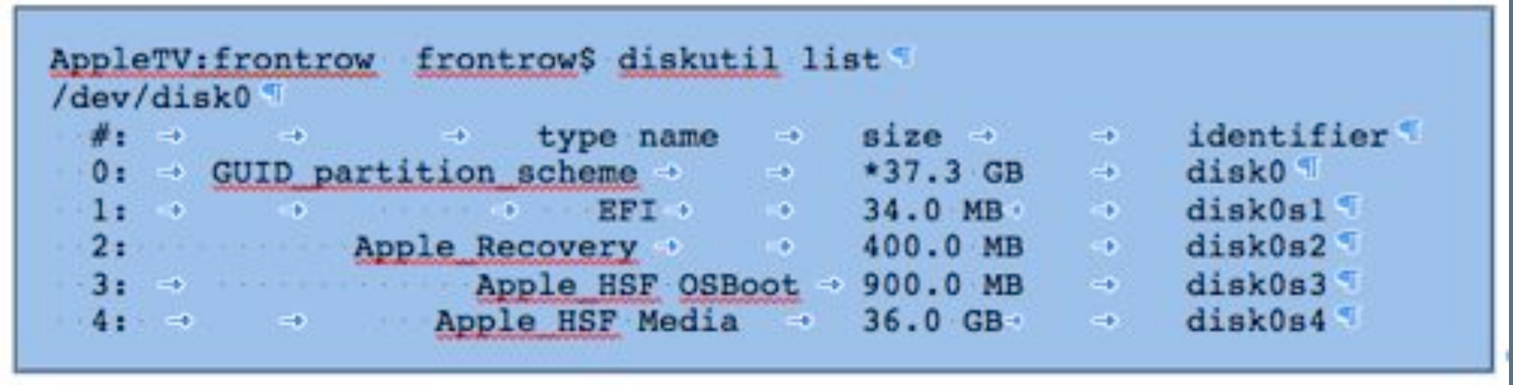
- Small form factor and low noise (no fan)
- Has both 802.11n (which includes 802.11b and 802.11g backwards compatibility) and 10/100Base-T Ethernet abilities, so that either type of network connectivity may be utilized
- Video output from the device is processed via HDMI or component video, and audio output is processed via optical or RCA composite connections.

Software Summary

- By default, runs a modified version of the full Apple OS X operating system
- Built upon FreeBSD (a derivative of Berkeley Software Distribution Unix); very powerful and equally functional
- Capability to run the same programs and applications as other Linux/BSD servers
- Functionality for multiple video, audio, and picture formats already built-in
- Two primary variants of the Apple TV OS: version 1.0/1.1 and version 2.x (also known as Take 2); 2.x removed a lot of "unnecessary" applications

Software Summary

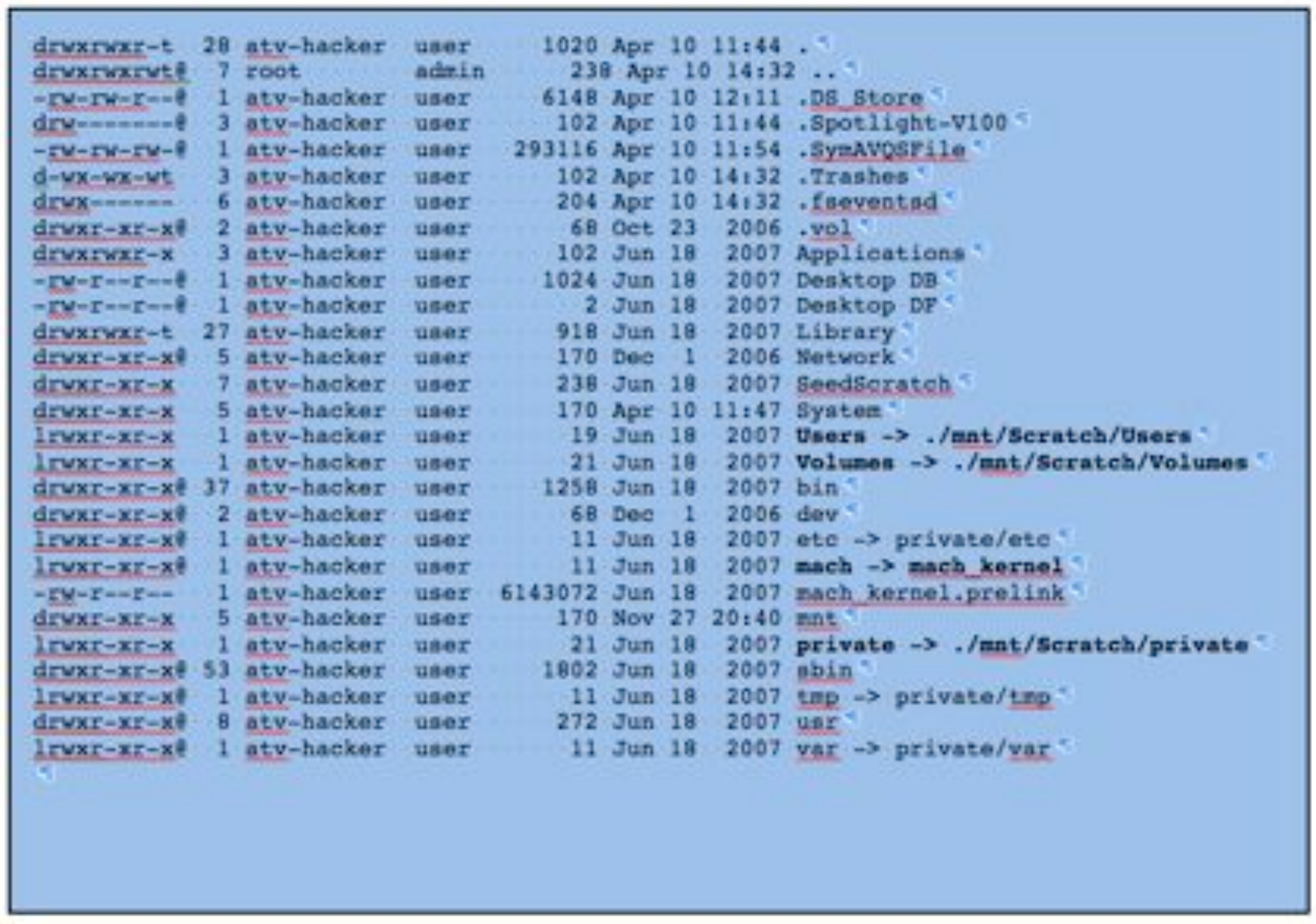
- GUID partition scheme, formatted as HFS+, and (by default) should have four separate disk partitions:
  - Extensible Firmware Interface [EFI]
  - Apple Recovery for system restores to factory original
  - OSBoot for the boot files
  - Media for the media files



```
AppleTV:frontrow  frontrow$ diskutil list
/dev/disk0
   #:                      type name           size           identifier
   0:     GUID partition scheme                *37.3 GB       disk0
   1:                         EFI              34.0 MB        disk0s1
   2:            Apple Recovery                400.0 MB       disk0s2
   3:                Apple HSF OSBoot          900.0 MB       disk0s3
   4:              Apple HSF Media             36.0 GB        disk0s4
```

Software Summary

OS takes advantage of the ability to use symbolic links (and even has some of the same links)



```
drwxrwxr-t  28 atv-hacker  user      1020 Apr 10 11:44 .
drwxrwxrwt@  7 root        admin      238 Apr 10 14:32 ..
-rw-rw-r--@  1 atv-hacker  user      6148 Apr 10 12:11 .DS_Store
drw-------@  3 atv-hacker  user       102 Apr 10 11:44 .Spotlight-V100
-rw-rw-rw-@  1 atv-hacker  user    293116 Apr 10 11:54 .SymAVQSFile
d-wx-wx-wt   3 atv-hacker  user       102 Apr 10 14:32 .Trashes
drwx------   6 atv-hacker  user       204 Apr 10 14:32 .fseventsd
drwxr-xr-x@  2 atv-hacker  user        68 Oct 23  2006 .vol
drwxrwxr-x   3 atv-hacker  user       102 Jun 18  2007 Applications
-rw-r--r--@  1 atv-hacker  user      1024 Jun 18  2007 Desktop DB
-rw-r--r--@  1 atv-hacker  user         2 Jun 18  2007 Desktop DF
drwxrwxr-t  27 atv-hacker  user       918 Jun 18  2007 Library
drwxr-xr-x@  5 atv-hacker  user       170 Dec  1  2006 Network
drwxr-xr-x   7 atv-hacker  user       238 Jun 18  2007 SeedScratch
drwxr-xr-x   5 atv-hacker  user       170 Apr 10 11:47 System
lrwxr-xr-x   1 atv-hacker  user        19 Jun 18  2007 Users -> ./mnt/Scratch/Users
lrwxr-xr-x   1 atv-hacker  user        21 Jun 18  2007 Volumes -> ./mnt/Scratch/Volumes
drwxr-xr-x@ 37 atv-hacker  user      1258 Jun 18  2007 bin
drwxr-xr-x@  2 atv-hacker  user        68 Dec  1  2006 dev
lrwxr-xr-x@  1 atv-hacker  user        11 Jun 18  2007 etc -> private/etc
lrwxr-xr-x@  1 atv-hacker  user        11 Jun 18  2007 mach -> mach_kernel
-rw-r--r--   1 atv-hacker  user   6143072 Jun 18  2007 mach_kernel.prelink
drwxr-xr-x   5 atv-hacker  user       170 Nov 27 20:40 mnt
lrwxr-xr-x   1 atv-hacker  user        21 Jun 18  2007 private -> ./mnt/Scratch/private
drwxr-xr-x@ 53 atv-hacker  user      1802 Jun 18  2007 sbin
lrwxr-xr-x@  1 atv-hacker  user        11 Jun 18  2007 tmp -> private/tmp
drwxr-xr-x@  8 atv-hacker  user       272 Jun 18  2007 usr
lrwxr-xr-x@  1 atv-hacker  user        11 Jun 18  2007 var -> private/var
```

Basic Forensic Considerations

- Discovery
  - Conduct a wireless assessment to determine if wireless networking is allowing the device to communicate on the LAN or local WiFi networks.
  - The WAP being utilized may or may not belong to the individual being investigated and/or area being searched; information about all local WAP should be collected
  - MAC addresses, IP addresses, and signal strength mapping can provide valuable data
  - Remember USB drives, iPhones, and network file services (SMB/Samba, FTP, AFP, SSH)

Basic Forensic Considerations

- Investigations
  - Hard drive is has a GUID partition table formatted as HFS+; investigation workstation will need file system drivers for reading HFS/HFS + drives
  - All OS X derivatives utilize Property List (.plist) files for configuration and some log data. Use OS X Property List Editor or another viewer capable of processing XML
  - OS X uses a database called NetInfo for storing some configuration data; normally accessed via NetInfo Manager in OS X prior to version 10.5 (Leopard) (possibly use NetInfo for Linux by PADL Software)

Files (Almost) Always Modified

- The ATV OS kernel must be patched to run kernel extensions (mach_kernel)
  - Located in /OSBoot/
  - Systems modified with patchsticks generally have copies of the original saved as *mach_kernel.prelink.og*
- New kernel extensions loaded into /*OSBoot/System/Library/Extensions*
- Secure Shell
  - SSHD into */Volumes/OSBoot/usr/sbin*
  - Dropbear into */Volumes/OSBoot/usr/bin*

Files and Directories Important to Forensic Analysis

- Most user data is located in:
  - */Media/Scratch/Users/frontrow*
- However, your data is ***EVERYWHERE***:
  - /OSBoot/System/Library/Filesystems - Used for file-system component applications, by default contains 2 items but may have user-added items (such as fusefs.fs for mounting shares via SSH).
  - /OSBoot/System/Library/Frameworks - by default has 49 items but users/3rd parties may have added more (such as AppleShareClient.framework for enabling AFS connections)
  - /OSBoot/usr/libexec - Contains executable libraries used by the OS, By default has 27 items but user/3rd party may place others (like sftp-server, etc.)
  - /OSBoot/usr/sbin - by default has 59 items but may contain others added by user/3rd parties like sshd

Files and Directories Important to Forensic Analysis

- */Media/Photos/Pxx* - each folder will have a picture and a 'thumbnail' file for every photo synced with iPhoto.
- */Media/Scratch/Library/Preferences/SystemConfiguration/autodiskmount.plist* - configuration data for disks to mount without user intervention, not present by default so it indicates the user utilizes removable disks
- */Media/Scratch/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist* - configuration data for the Apple TV airport connection (includes list of known networks)
- */Media/Scratch/private/var/run/resolv.conf* – contains DNS servers used to resolve DNS queries by the Apple TV (this file is configurable by the user).

Files and Directories Important to Forensic Analysis

- Areas Where Most Data Resides
  - Log information in .plist files and the Spotlight index; Spotlight can be hit or miss
    - */OSBoot* partition contains some log files normally found in */var/log* on a standard Apple OS X system
    - */Media* partition has logs in */var/log* generally different than */OSBoot*
  - Generally, /user/frontrow has all 3rd party apps and data
- Applications also track a ***LOT*** of data
  - nitoTV places data in *\Media\Scratch\Users\frontrow\Library\Application Support\nito*
  - Boxee places a lot of data in *\Media\Scratch\Users\frontrow\Library\Application Support\BOXEE\*

Remnants of Data

Remnants of Data

Questions?