REALITYNET
System Solutions

FORENSICATING THE APPLE TV

MATTIA EPIFANI – CLAUDIA MEDA

DFRWS 2018 EU

FLORENCE, 23 MARCH 2018

APPLE TV

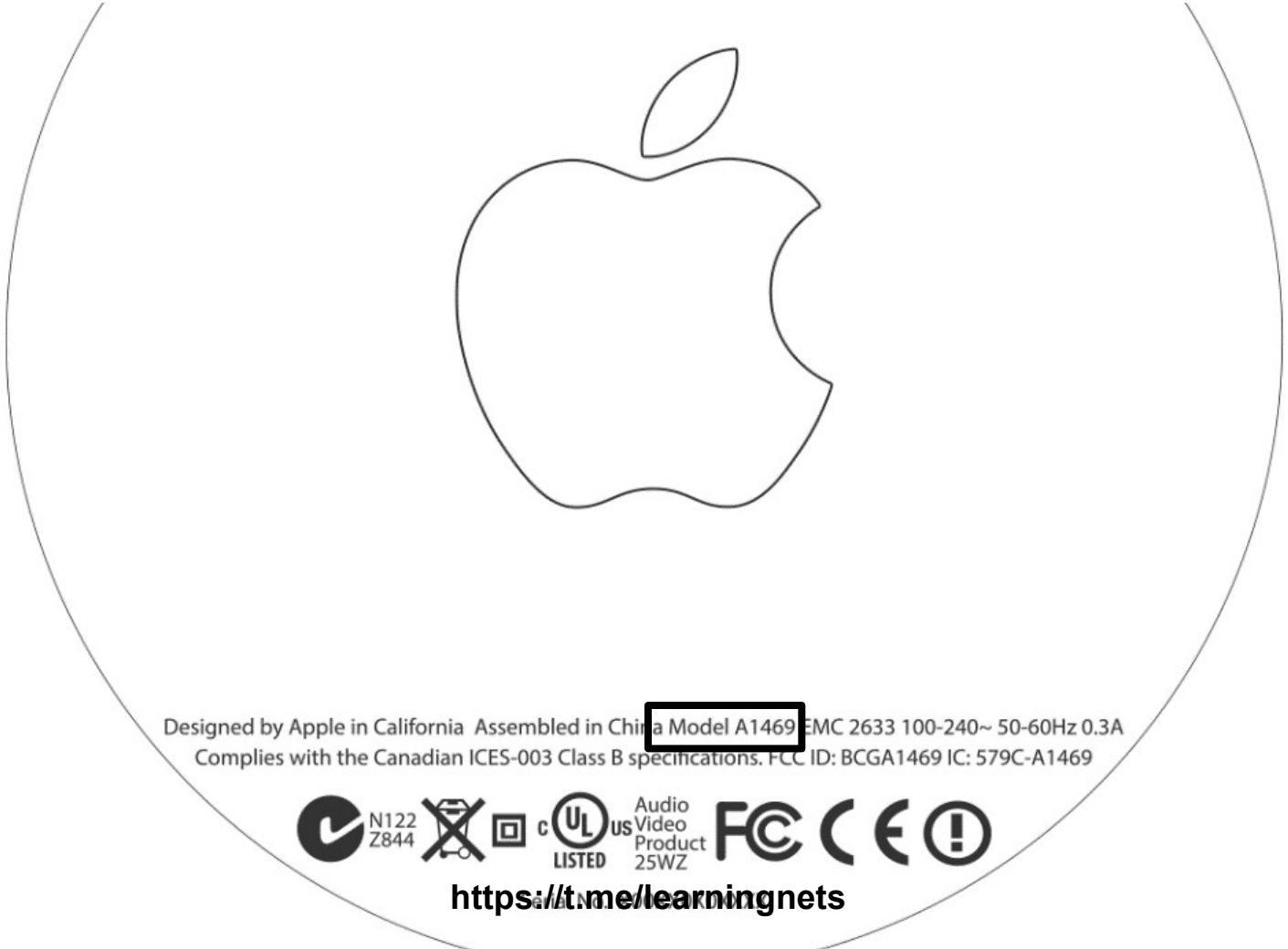
- The **Apple TV** is a **digital media player** manufactured by Apple
- It can **receive digital data** from a number of sources and **stream it to a TV**
- As of March 2018, **6 models were produced**

APPLE TV – IDENTIFICATION

- Observe **device appearance**
- Check **the label under the device**
- Verify through **device settings menu**

Model number	Generation
A1218	I
A1378	II
A1427	III
A1469	III Rev.A
A1625	IV
A1842	4K

APPLE TV – IDENTIFICATION
HTTPS://SUPPORT.APPLE.COM/EN-US/HT200008



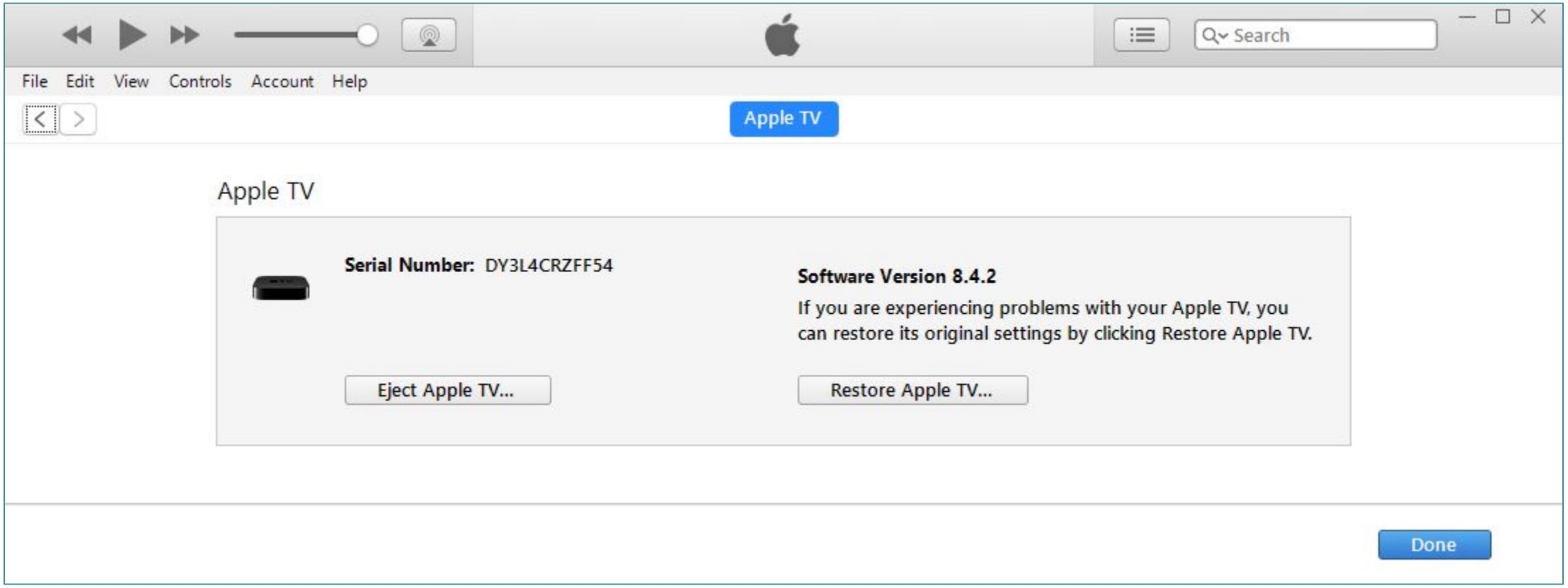
APPLE TV – I° GENERATION – ACQUISITION AND ANALYSIS

- It contains a traditional Hard Drive that **can be extracted and imaged!**
- Traditional approach
- **"Hacking the Apple TV and Where Your Forensic Data Lives"**, Kevin Estis and Randy Robbins, Def Con 2009
- https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-kevin_estis-apple_tv.pdf
- https://www.youtube.com/watch?v=z-WCy3Bdzkc

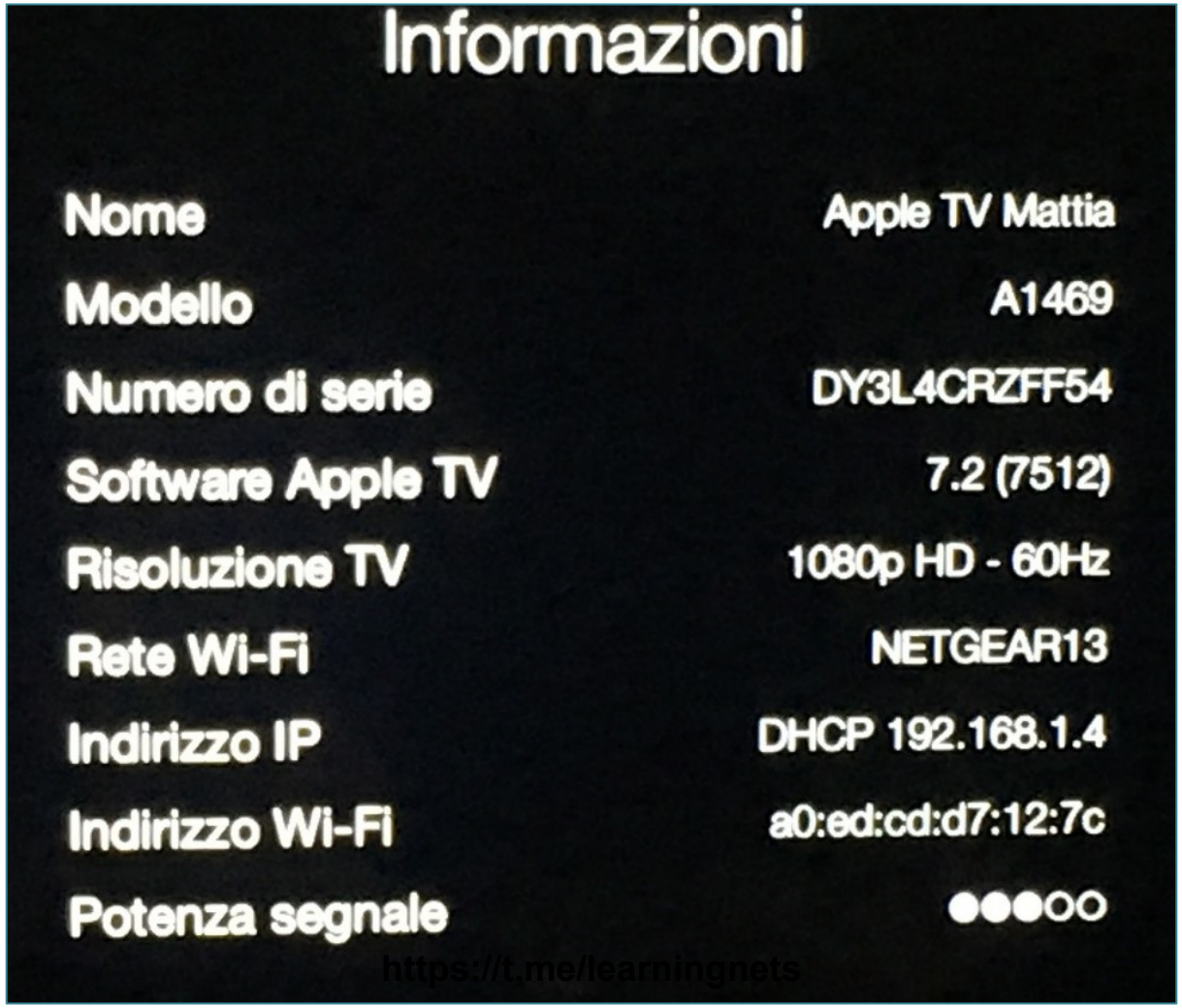
APPLE TV – II° – IV° GENERATION – ACQUISITION

- **Good news** → NO Passcode protection!
- **Bad news** → USB Port used only for "service and support"

APPLE TV – II° – IV° GENERATION ITUNES CONNECTION



APPLE TV – II° – IV° GENERATION
MANUAL ACQUISITION



APPLE TV – II° – IV° GENERATION
USB ACQUISITION

- Not completely true that USB port is only for service and support…
- **Apple File Conduit (AFC) service is active!**
- We can access:
  - Basic **device information**
  - **Real Time** Log (**Syslog**)
  - Part of the **file system («Media» folder)**
  - **Crash** Logs

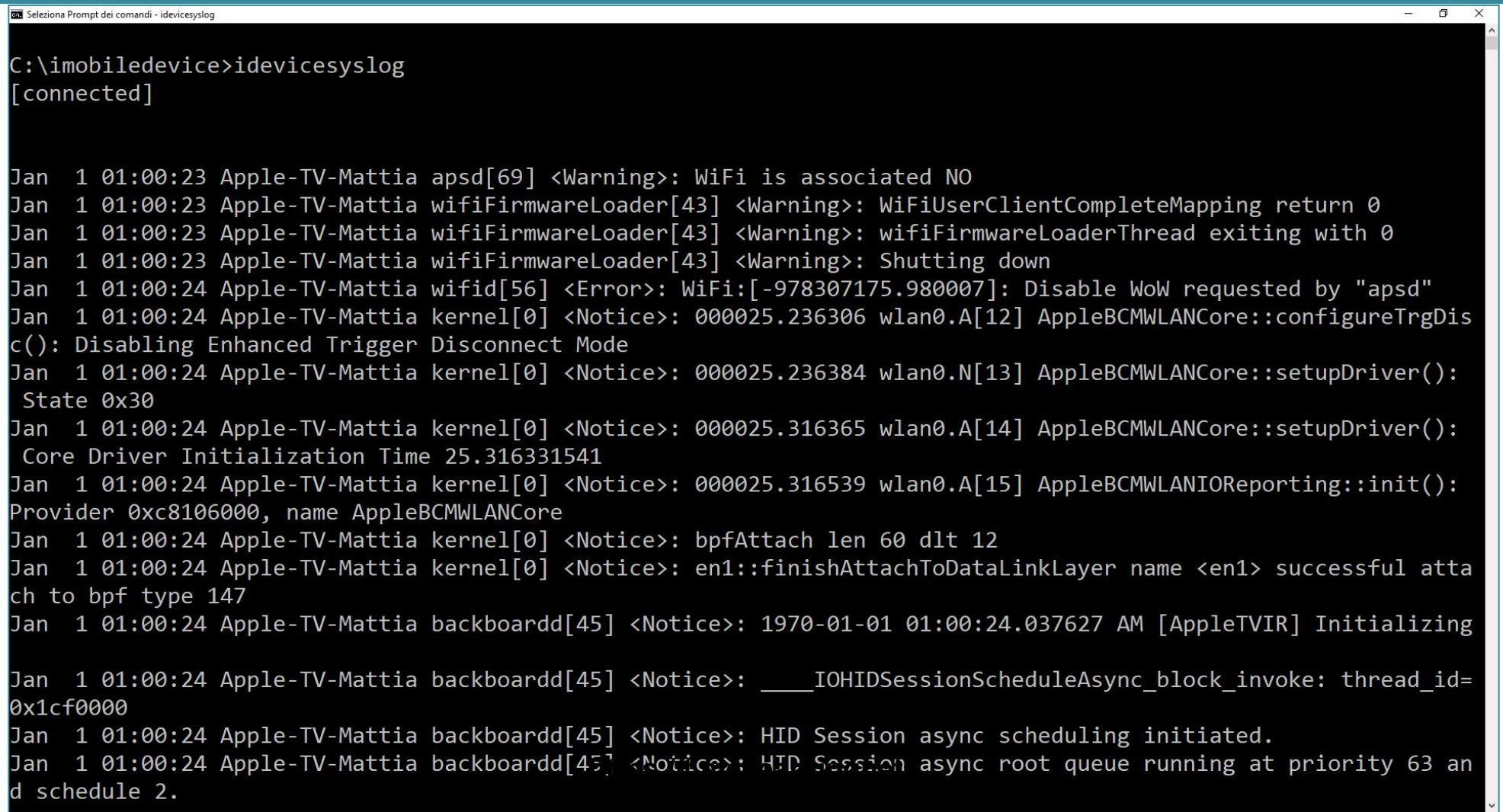
APPLE TV – II° – IV° GENERATION – DEVICE INFORMATION IDEVICEINFO (HTTP://WWW.LIBIMOBILEDEVICE.ORG/)

```
C:\imobiledevice>ideviceinfo
ActivationState: Activated
BasebandStatus: NoTelephonyCapabilty
BluetoothAddress: a0:ed:cd:d7:12:7e
BoardId: 0
BrickState: false
BuildVersion: 12H606
CPUArchitecture: armv7f
ChipID: 35143
DeviceClass: AppleTV
DeviceColor: unknown
DeviceName: Apple TV Mattia
DevicePublicKey: LS0tLS1CRUdJTiBSU0Eg
Y0VCYWNhNEFlbjQ4amJ3K2w0OWdlWVQ5MHNpU
XV4VFhyNDJ2dWpSZgo3c3E1UFZtTy9ZUHVsNl
DieID: 15766959919149636
EthernetAddress: a0:ed:cd:d7:12:7d
FirmwareVersion: iBoot-2261.30.37
FirstFreePairExpired: true
HardwareModel: J33iAP
HardwarePlatform: s5l8947x
HostAttached: true
MLBSerialNumber: C0732951MPPF82PAG
ModelNumber: MD199
```

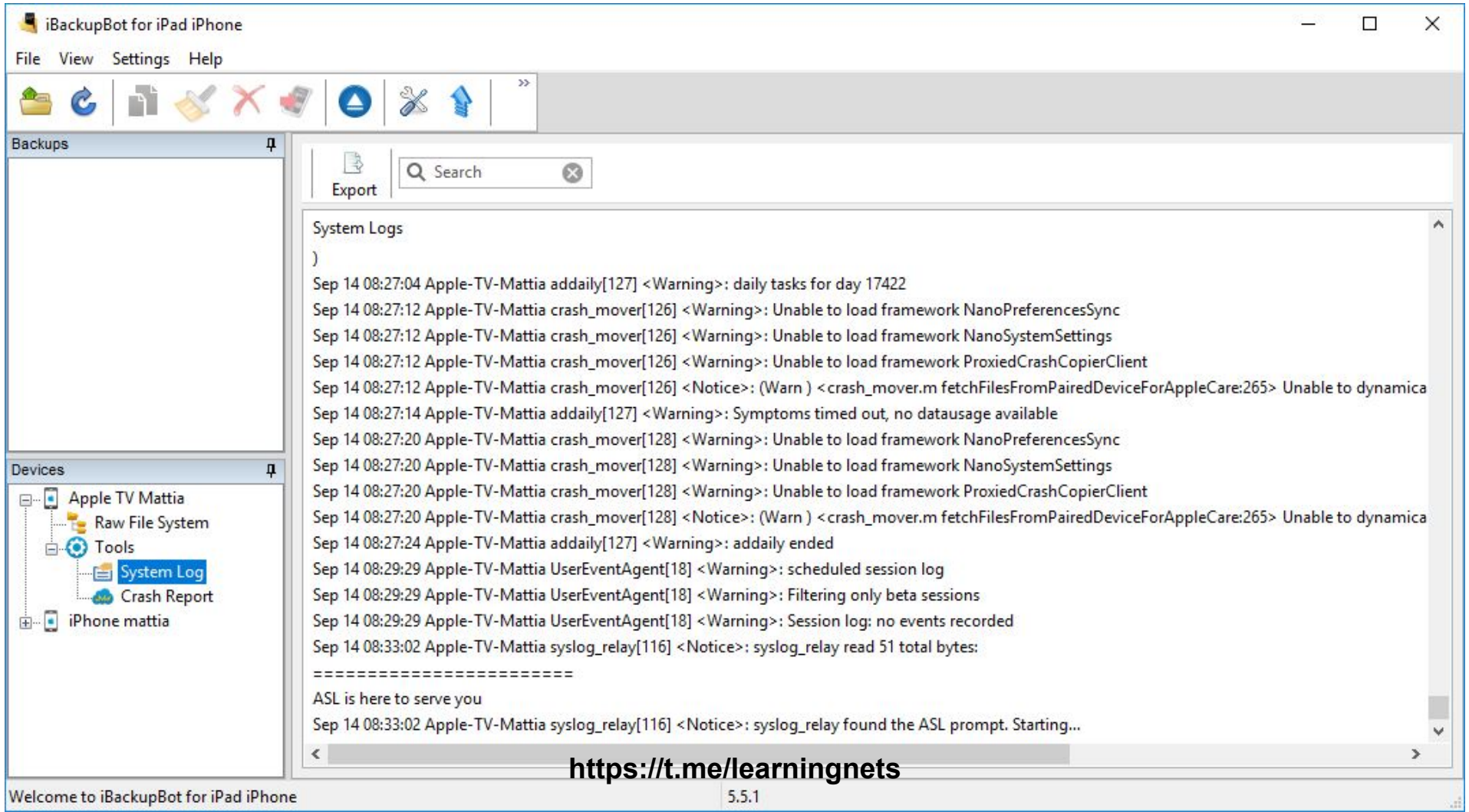
```
NonVolatileRAM:
 auto-boot: dHJ1ZQ==
 boot-args:
 bootdelay: MA==
 ota-brain-version: MTJIMzA1
 ota-original-os-version: MTJINTIz
PartitionType:
PasswordProtected: false
ProductType: AppleTV3,2
ProductVersion: 8.4.2
ProductionSOC: true
ProtocolVersion: 2
RegionInfo: TY/A
SIMStatus: kCTSIMSupportSIMStatusReady
SerialNumber: DY3L4CRZFF54
SoftwareBundleVersion:
SupportedDeviceFamilies[1]:
 0: 3
TelephonyCapability: false
TimeIntervalSince1970: 1505343643.302341
TimeZone: Europe/Rome
TimeZoneOffsetFromUTC: 7200.000000
TrustedHostAttached: true
UniqueChipID: 1538815294831
UniqueDeviceID: d2b0954284f3aeaada50a22b68d5e8b85166d8d5
UntrustedHostBUID: 30607839-76415530746167752
UseRaptorCerts: false
Uses24HourClock: false
WiFiAddress: a0:ed:cd:d7:12:7c
WirelessBoardSerialNumber: 35145C500BF
```

e/learni

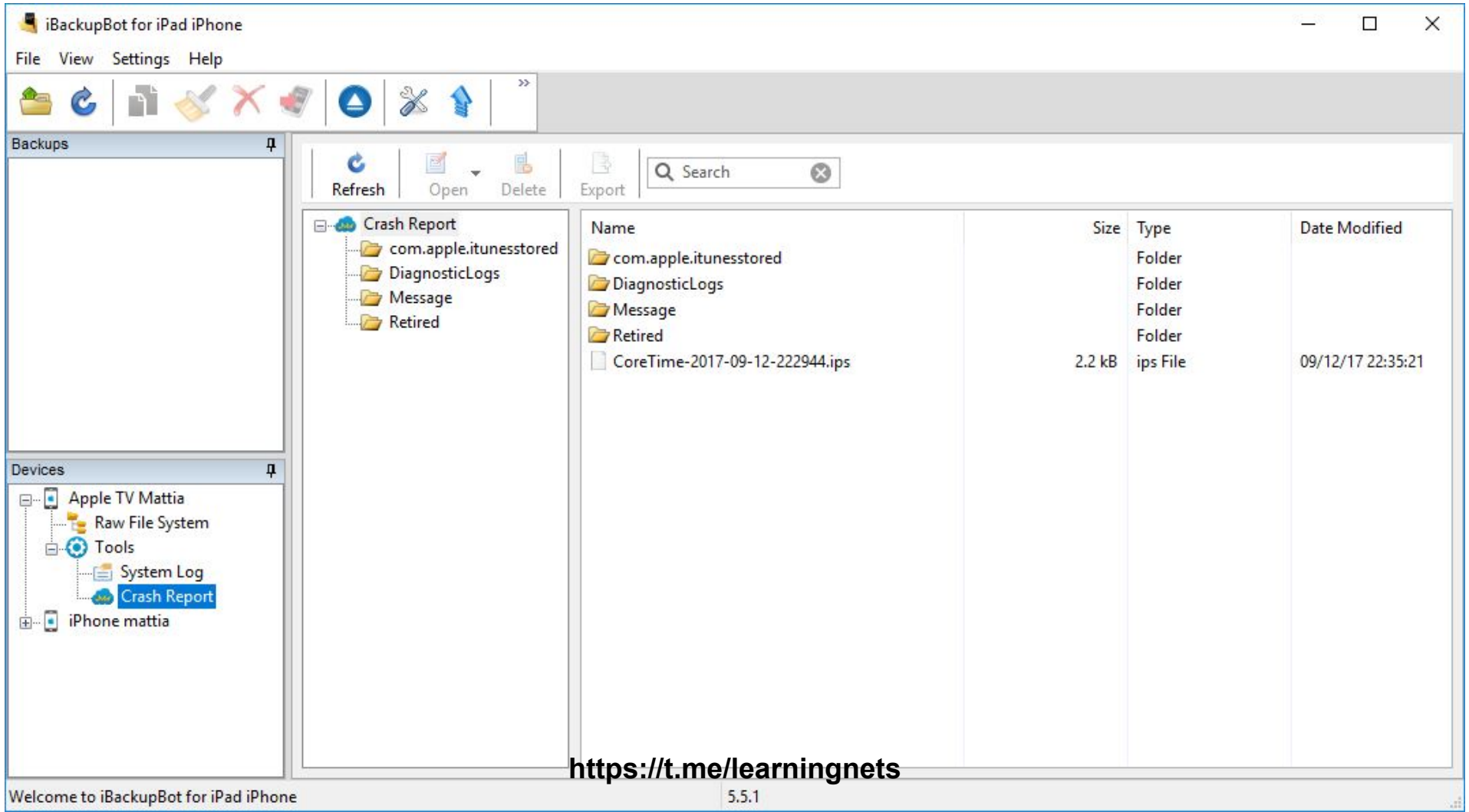
APPLE TV – II° – IV° GENERATION – REAL TIME LOG IDEVICESYSLOG (HTTP://WWW.LIBIMOBILEDEVICE.ORG/)



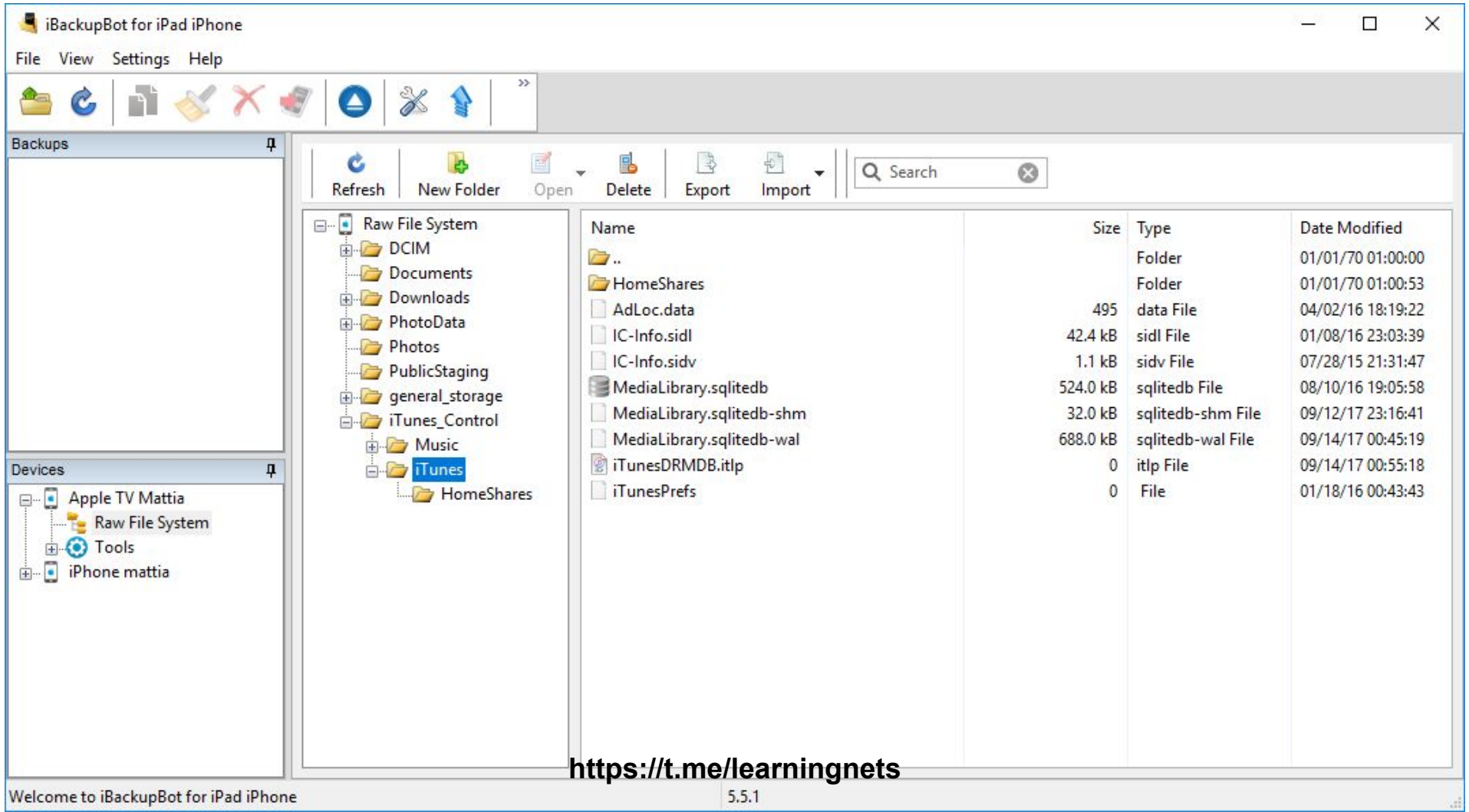
APPLE TV – II° – IV° GENERATION IBACKUPBOT (HTTP://WWW.ICOPYBOT.COM)



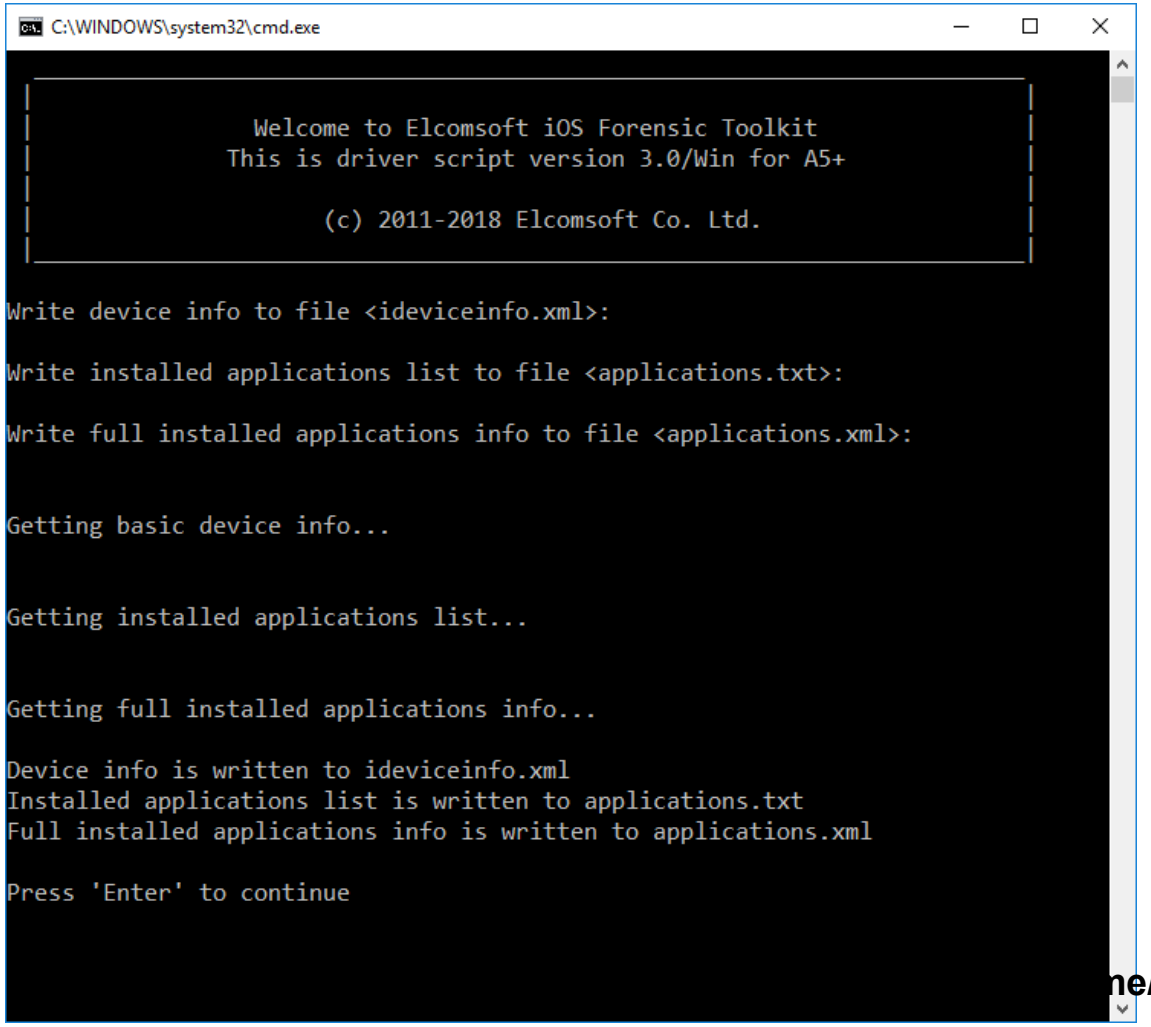
APPLE TV – II° – IV° GENERATION
IBACKUPBOT (HTTP://WWW.ICOPYBOT.COM)

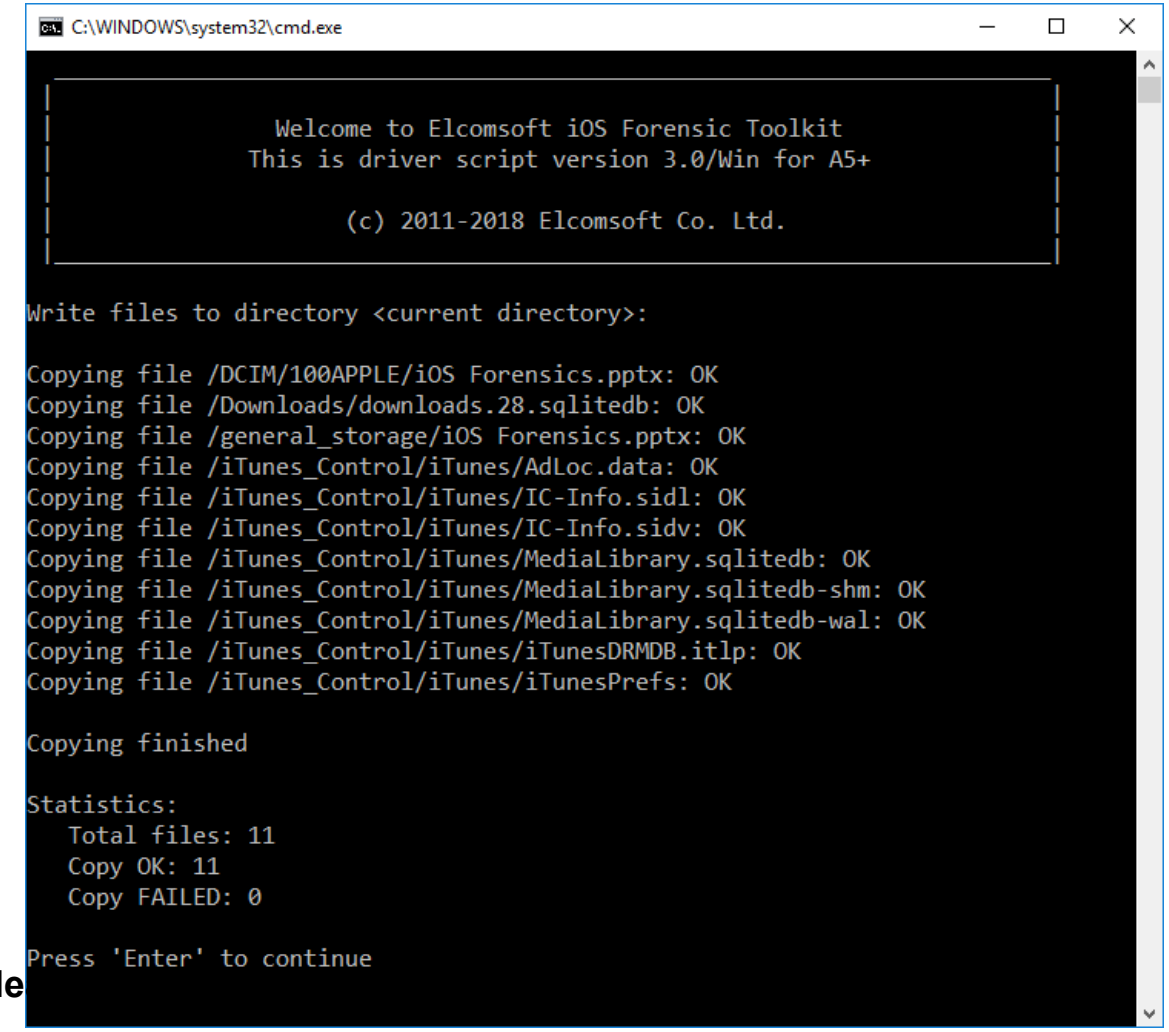


APPLE TV – II° – IV° GENERATION IBACKUPBOT (HTTP://WWW.ICOPYBOT.COM)



APPLE TV – II° – IV° GENERATION
ELCOMSOFT IOS FORENSIC TOOLIKT (3.0)





APPLE TV
III° GENERATION

III-generation Apple TV
Model A1469

General Information	Network Information	AirPlay Information	Remote Control Information
Name	Wi-Fi MAC address	Devices used	iPhone
Model number	Bluetooth MAC Address	Type	iPad
Serial Number	IP configuration	Name	Telecontrol
OS version	Signal power		Keyboard
Time-zone	Network used		
Date and time			

APPLE TV
III° GENERATION

III-generation Apple TV
Model A1469

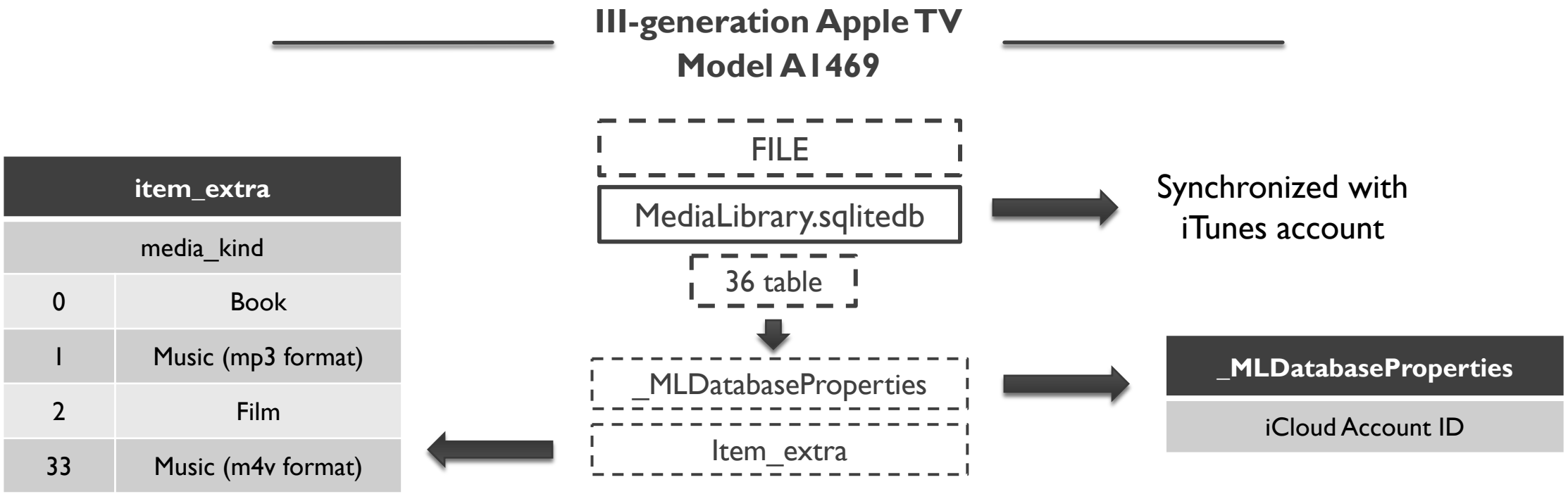
Artifacts	Information
Real Time Log	iCloud Account Name
	iCloud ID
Crash Log	Wi-Fi networks
	Device usage timeline
MediaLibrary.sqlitedb	Shopping database

APPLE TV
III° GENERATION

III-generation Apple TV
Model A1469

```
Aug 12 00:03:07 Apple-TV-Mattia identityservicesd[34] <Warning>:
[Warning] Device identity is not expired
Aug 12 00:03:07 Apple-TV-Mattia identityservicesd[34] <Warning>:
[Warning] Registration failed for Registration info (0x15dc42d0):
[Registered: NO] [Type: AppleID] [Device Name: (null)] [Service
Type: com.apple.private.alloy.multiplex1] [Env: (null)] [Main ID:
[redacted]@hotmail.it] [Phone Number: [redacted]@hotmail.it] [AppleID:
[redacted]@hotmail.it] [UserID: E:[redacted]@hotmail.it] [C2K: NO] [Push
Token: <c4c34f84 f773b25c a69bfefb 677a7b6b c0a578a5 8fe2adc3
11efe04a 996b5351>] [Region ID: R:IT] [Base Number: +390000000000]
[URIs: ()] [Candidates: [redacted]@hotmail.it, +39[redacted])] [Auth
Cert: 0x0] [Reg Cert: 0x0] [Profile ID: D:1321761630] [Auth User ID:
(null)] [Heartbeat Date: (null)]   (Error: 17)
Aug 12 00:03:07 Apple-TV-Mattia identityservicesd[34] <Warning>:
[Warning] Failed, invalid password => Disabling service
```

APPLE TV
MEDIA LIBRARY



item_extra	
media_kind	
0	Book
1	Music (mp3 format)
2	Film
33	Music (m4v format)

APPLE TV
MEDIA LIBRARY

III-generation Apple TV
Model A1469

```
select
    ext.title,
    ext.total_time_ms,
    ext.file_size,
    sto.account_id,
    strftime('%d/%m/%Y %H:%M:%S',
       datetime(sto.date_purchased +
       978307200,'unixepoch'))date_purchased,
    sto.store_item_id
from item_extra ext
join item_store sto using(item_pid)
where ext.media_kind = 1;
```

SQL query

FILE

MediaLibrary.sqlitedb

36 table

_MLDatabaseProperties

Item_extra

APPLE TV – IV° GENERATION – JAILBREAKING HTTPS://WWW.THEIPHONEWIKI.COM/WIKI/JAILBREAK

9.x

tvOS	Jailbreak Tool	Tool Version	Device
			Apple TV (4th generation)
9.0	Pangu9	1.0.0	Yes
9.0.1	Pangu9	1.0.0	Yes
9.1	No Tool Available		No
9.1.1	No Tool Available		No
9.2	No Tool Available		No
9.2.1	No Tool Available		No
9.2.2	No Tool Available		No

10.x

tvOS	Jailbreak Tool	Tool Version	Device
			Apple TV (4th generation)
10.0	LiberTV	1.0	Yes
10.0.1	LiberTV	1.0	Yes
10.1	LiberTV	1.0	Yes
10.1.1	No Tool Available		No
10.2	No Tool Available		No
10.2.1	No Tool Available		No
10.2.2	greeng0blin	1.1	Yes

11.x

tvOS	Jailbreak Tool	Tool Version	Device	
			Apple TV (4th generation)	Apple TV 4K
11.0	LiberTV	1.1	Yes	
11.1	LiberTV	1.1	Yes	
11.2	No Tool Available		No	
11.2.1	No Tool Available		No	
11.2.5	No Tool Available		No	
11.2.6	No Tool Available		No	

REALITYNET
System Solutions

APPLE TV
JAILBREAKING (IV GENERATION)

Requirements

- Mac Computer
  - El Capitan 10.11+
  - Xcode
- Apple TV 4
  - tvOS 9.0-9.0.1
- USB-C Cable
- Apple Development Membership ($99)

Procedures

1. Download atvjb.zip [2]
   a. Extract Files
2. Acquire Apple TV 4 UDID
   a. Launch Xcode
   b. Navigate to: Windows | Devices
   c. Select Your TV
   d. Record Identifier (UDID)
3. Register Apple TV
   a. Enroll in the Apple Developer Program [3]
   b. Login to Apple Development Center [4]
   c. Create name, enter UDID, and register
4. Register new App ID [5]
   a. Enter Name, enter Bundle ID, and register
5. Generate mobile provision file [6]
   a. Select tvOS App Development and click continue
   b. Create your developer certificate
      i. Choose iOS App Development
   c. Select your Apple TV and click continue
   d. Enter Profile Name and click continue
   e. Download to jailbreak folder and rename as *embedded.mobileprovision*
6. Query Common Name and Team ID
   a. Open Keychain Access app
   b. Select "Certificates" in the category section
   c. Open property page of your developer certificate
      i. iPhone Developer = Common Name
      ii. Subject Organization Unit = Team ID
7. Run install script
   a. ./Install_atv_jb.sh <UDID> <Bundle ID> <Team ID> "iPhone Developer: <Common Name ID>"
8. Create a Forensic Image [7]
   a. System Partition: ssh root@<IP address of Apple TV> dd if=/dev/disk0s1s1 conv=noerror,sync | dd of=AppleTV.img
   b. User Partition: ssh root@<IP address of Apple TV> 'tar -cpf - /private/var/' >User.tar
   c. Password: alpine

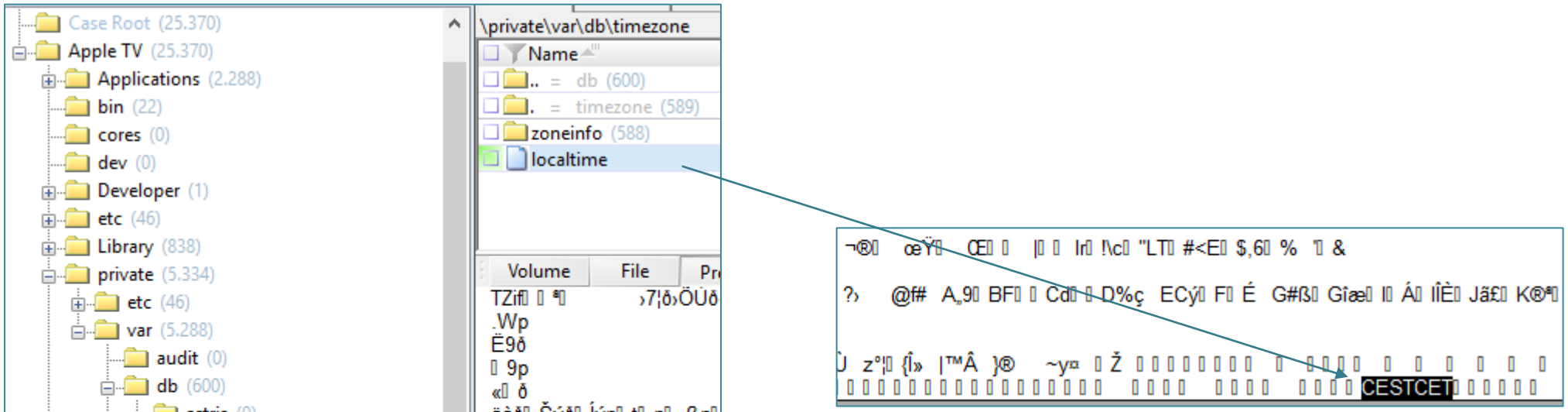
METHODOLOGY

- https://twitter.com/iHarrisThompson/status/715941070543126528

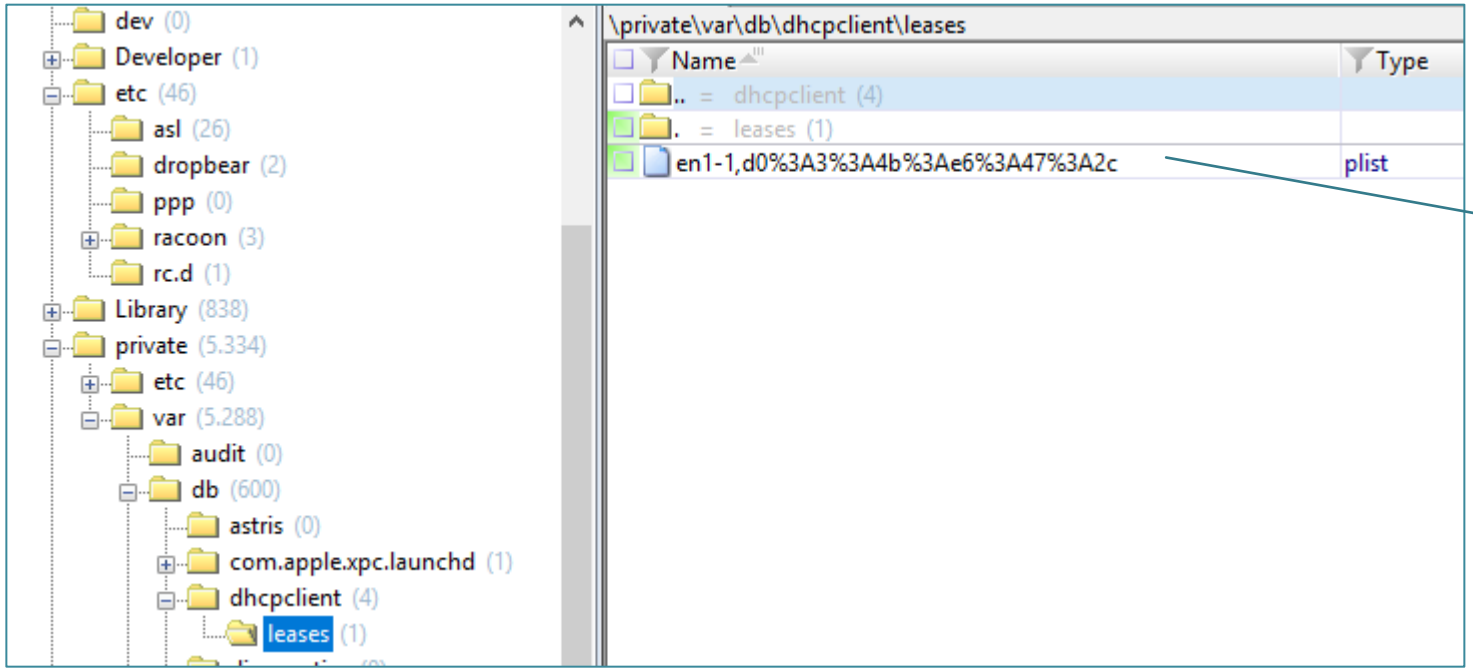
APPLE TV
FILE SYSTEM LAYOUT - /

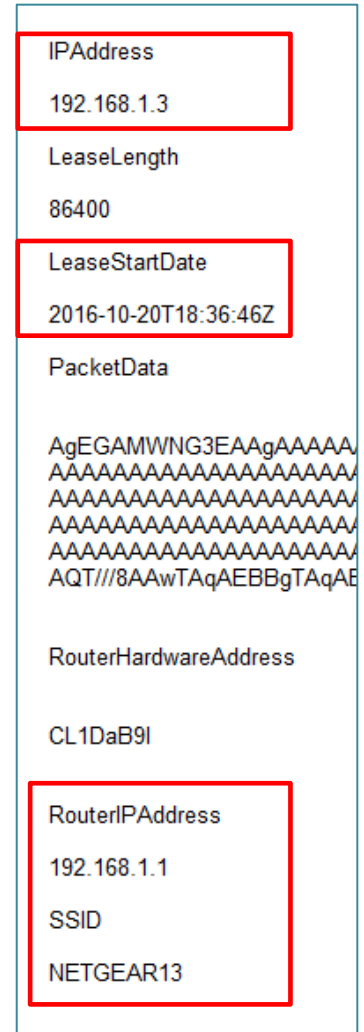
```
Apple-TV:/ root# ls -la /
total 539
drwxrwxr-t  14 root      admin         816 Dec 31  1969 .
drwxrwxr-t  14 root      admin         816 Dec 31  1969 ..
d-wx-wx-wt@  2 _unknown  _unknown       68 Oct 16  2015 .Trashes
----------   1 root      admin           0 Sep 30  2015 .file
drwx------   2 _unknown  _unknown     136 May  1 18:44 .fseventsd
-rw-r--r--   1 root      admin           0 Dec 31  1969 .pg_inst
drwxrwxr-x  26 root      admin         884 Oct 16  2015 Applications
drwxrwxr-x   3 root      admin         102 Apr 23 14:23 Developer
drwxrwxr-x  13 root      admin         578 Apr 23 14:23 Library
drwxr-xr-x   3 root      wheel         102 Sep 30  2015 System
drwxr-xr-x   2 root      wheel         816 Apr 23 14:23 bin
drwxrwxr-t   2 root      admin          68 Sep 30  2015 cores
dr-xr-xr-x   3 root      wheel        1233 Dec 31  1969 dev
lrwxr-xr-x   1 root      admin          11 Oct 16  2015 etc -> private/etc
-rwxr-xr-x   1 root      admin      259488 Apr 23 14:23 pguntether
drwxr-xr-x   4 root      wheel         136 Oct 23  2015 private
drwxr-xr-x   2 root      wheel         612 Apr 23 14:23 sbin
lrwxr-xr-x   1 root      admin          15 Oct 16  2015 tmp -> private/var/tmp
drwxr-xr-x   9 root      wheel         306 Apr 23 14:23 usr
lrwxr-xr-x   1 root      admin          11 Oct 16  2015 var -> private/var
```

TIMEZONE
/PRIVATE/VAR/DB/TIMEZONE/LOCALTIME



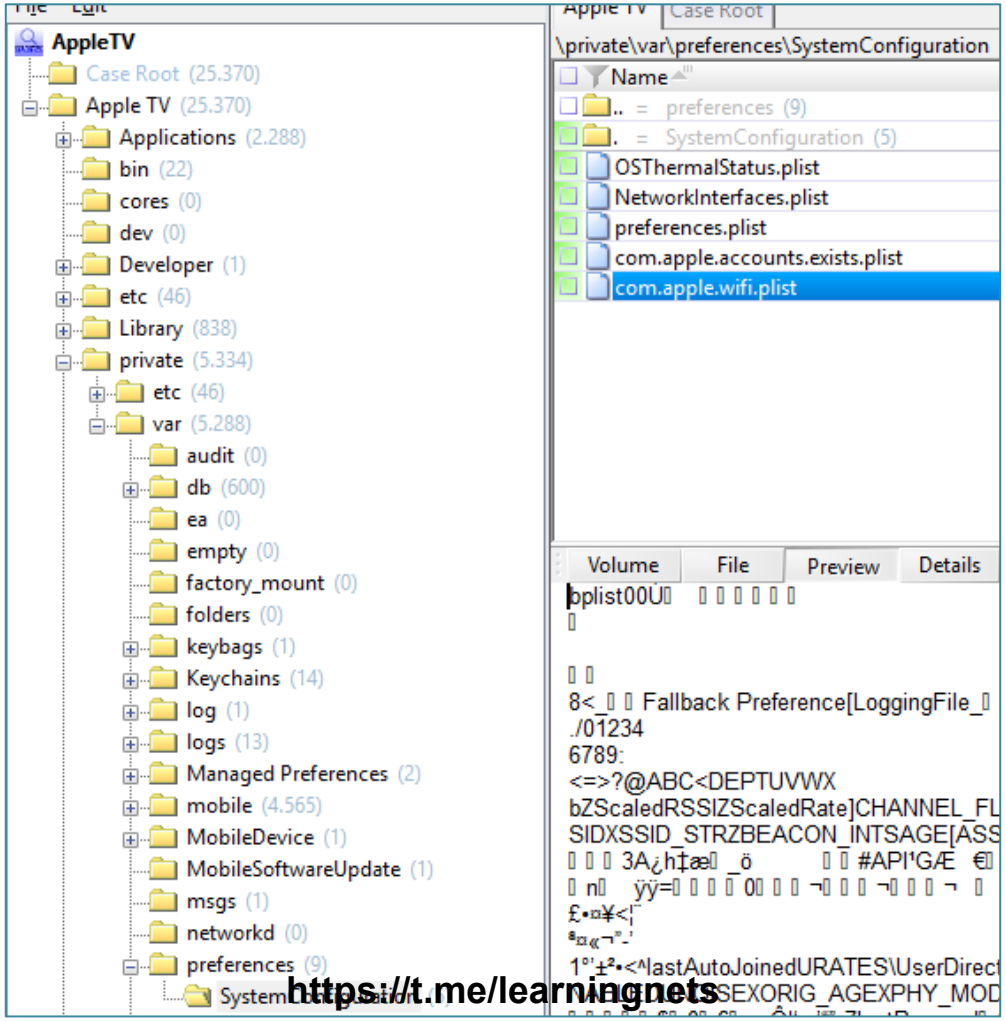
NETWORK TCP/IP LEASE
/PRIVATE/VAR/DB/DHCPCLIENT/LEASES/





REALITYNET
System Solutions

NETWORK WI-FI HISTORY
/PRIVATE/VAR/PREFERENCES/COM.APPLE.WIFI.PLIST



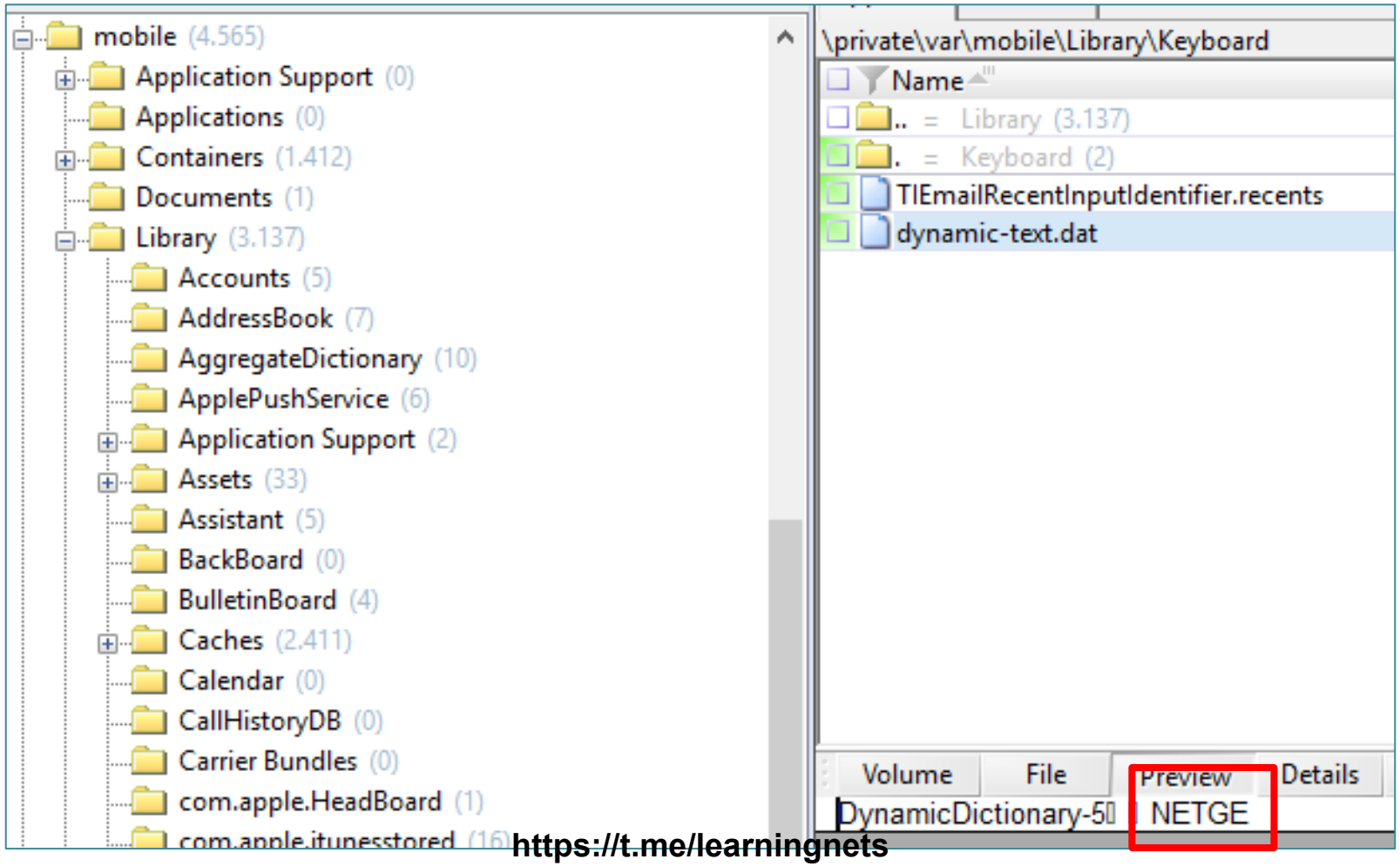
REALITYNET
System Solutions

NETWORK WI-FI HISTORY

List of known networks	array	
	dict	
ScaledRSSI	real	0.953168
ScaledRate	real	1.000000
CHANNEL_FLAGS	integer	12
CAPABILITIES	integer	1041
lastAutoJoined	date	2017-09-12 23:23:50
SCAN_RESULT_FROM_PROBE_RSP	boolean	true
CHANNEL	integer	6
networkUsage	real	4269797.121467
UserDirected	boolean	false
RSSI	integer	-32
NOISE	integer	-95
80211W_ENABLED	boolean	true
WiFiManagerKnownNetworksEventType	integer	1
BSSID	string	8:bd:43:[redacted]
lastJoined	date	2016-10-20 20:36:41
SNR	integer	35
SSID	data	...
SSID_STR	string	NETGEAR13
BEACON_INT	integer	20
AGE	integer	3040
ASSOC_FLAGS	integer	1
CHANNEL_WIDTH	integer	40
RATES	array	
networkKnownBSSListKey	array	
Strength	real	0.953168
PHY_MODE	integer	16
IE	data	...
AP_MODE	integer	2
RSN_IE	dict	
FT_ENABLED	boolean	true
ORIG_AGE	integer	3040
	dict	

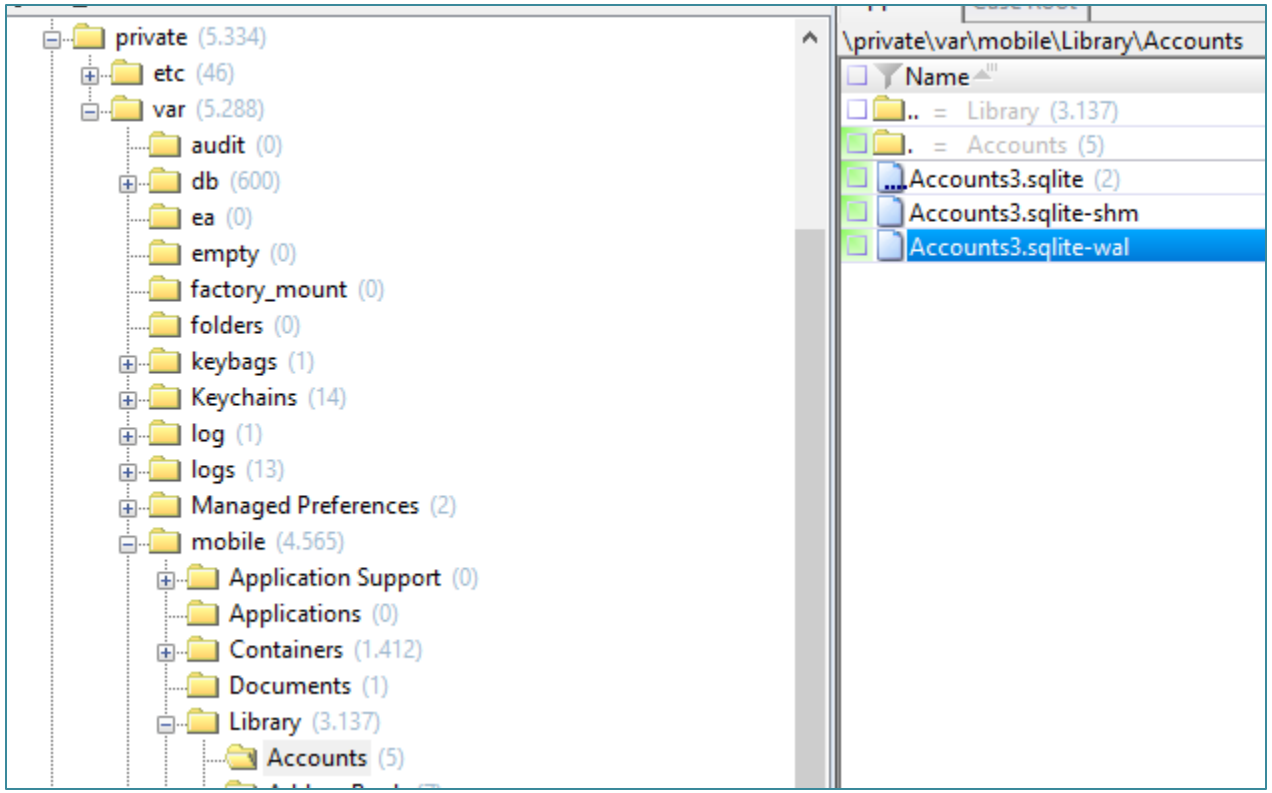
List of known networks	array	
	dict	
	dict	
lastAutoJoined	date	2016-08-26 03:22:10
RATES	array	
UserDirected	boolean	false
networkKnownBSSListKey	array	
RSN_IE	dict	
SCAN_RESULT_FROM_PROBE_RSP	boolean	false
SSID	data	...
SSID_STR	string	veyron
Strength	real	0.901090
80211W_ENABLED	boolean	true
CAPABILITIES	integer	1297
BEACON_INT	integer	20
AGE	integer	2562
SNR	integer	35
ASSOC_FLAGS	integer	1
EXT_CAPS	dict	
ScaledRSSI	real	0.901090
FT_ENABLED	boolean	true
NOISE	integer	0
ORIG_AGE	integer	2562
PHY_MODE	integer	144
RSSI	integer	-49
BSSID	string	8a:dc:96:[redacted]
80211D_IE	dict	
CHANNEL	integer	40
AP_MODE	integer	2
ScaledRate	real	1.000000
networkUsage	real	10122649.659805
CHANNEL_WIDTH	integer	40
IE	data	...
lastJoined	date	2015-10-23 12:02:17
CHANNEL_FLAGS	integer	20
WiFiManagerKnownNetworksEventType	integer	1

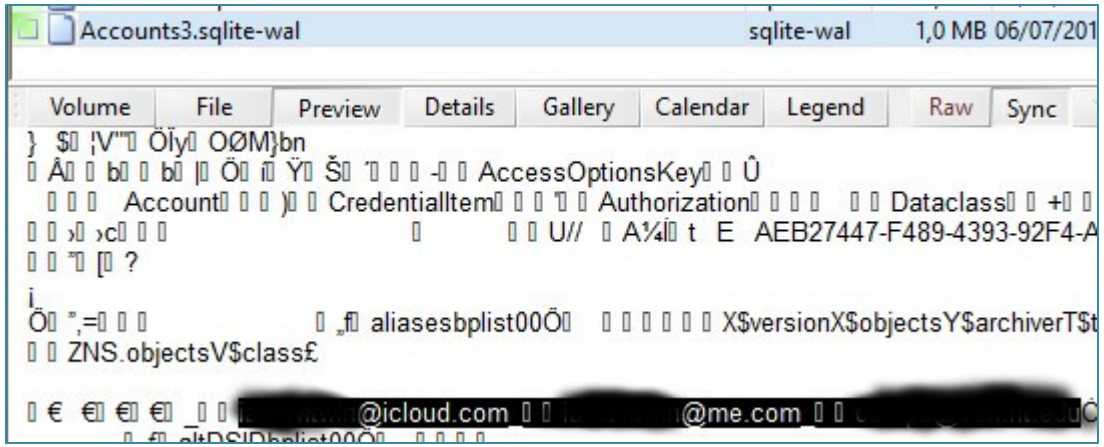
KEYBOARD DICTIONARY
/PRIVATE/VAR/MOBILE/LIBRARY/KEYBOARD/DYNAMIC-TEXT.DAT

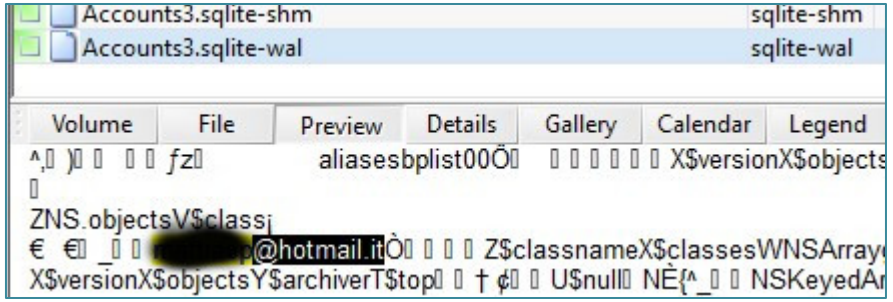


REALITYNET
System Solutions

ACCOUNTS
/PRIVATE/VAR/MOBILE/LIBRARY/ACCOUNTS/







ACCOUNTS

/PRIVATE/VAR/MOBILE/LIBRARY/PREFERENCES/COM.APPLE.IDS.SERVICE.COM

ICLOUD "SYNCED PREFERENCES"

/var/mobile/Library/SyncedPreferences/

Wi-Fi Access Points

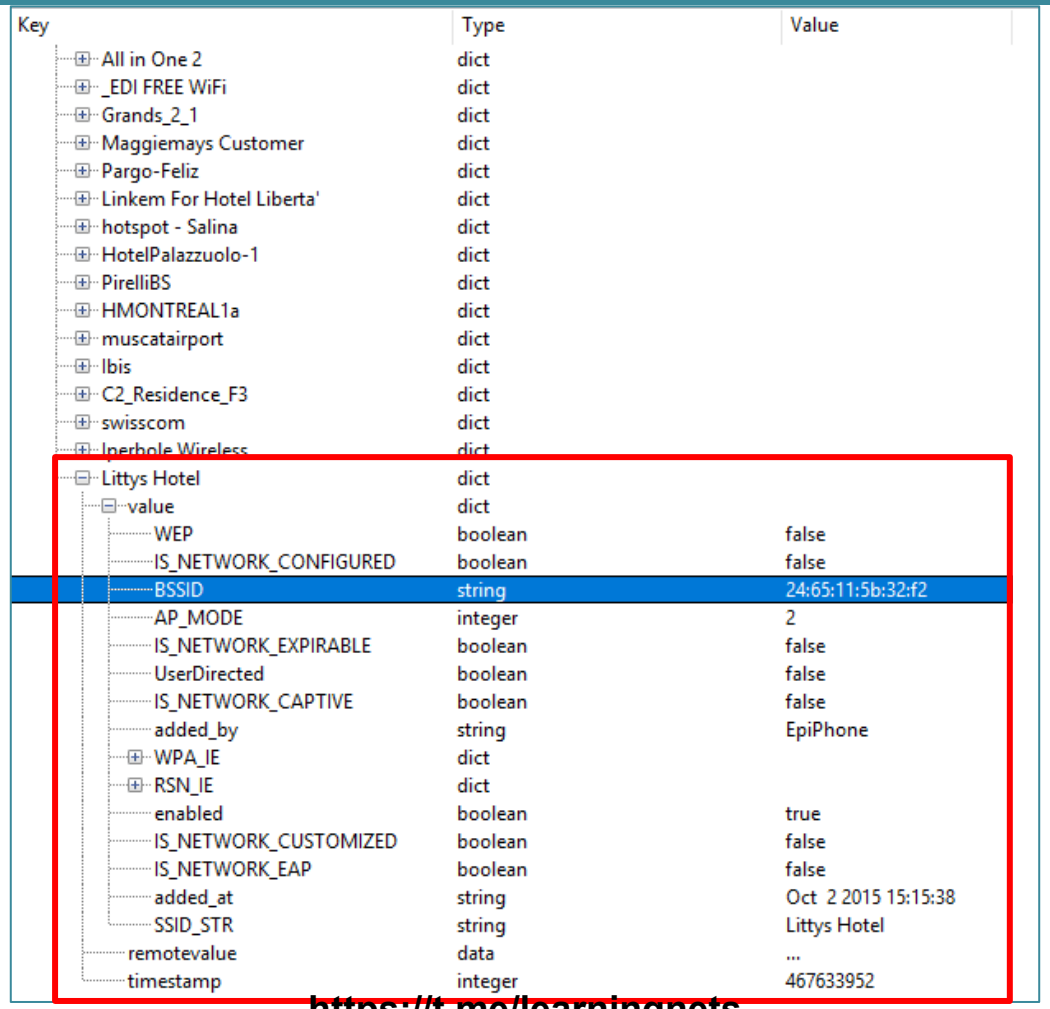
- com.apple.wifid.plist

Weather Cities

- com.apple.nanoweatherprefsd.plist

WI-FI ACCESS POINTS

/PRIVATE/VAR/MOBILE/LIBRARY/SYNCEDPREFERENCES/COM.APPLE.WIFID.PLIST



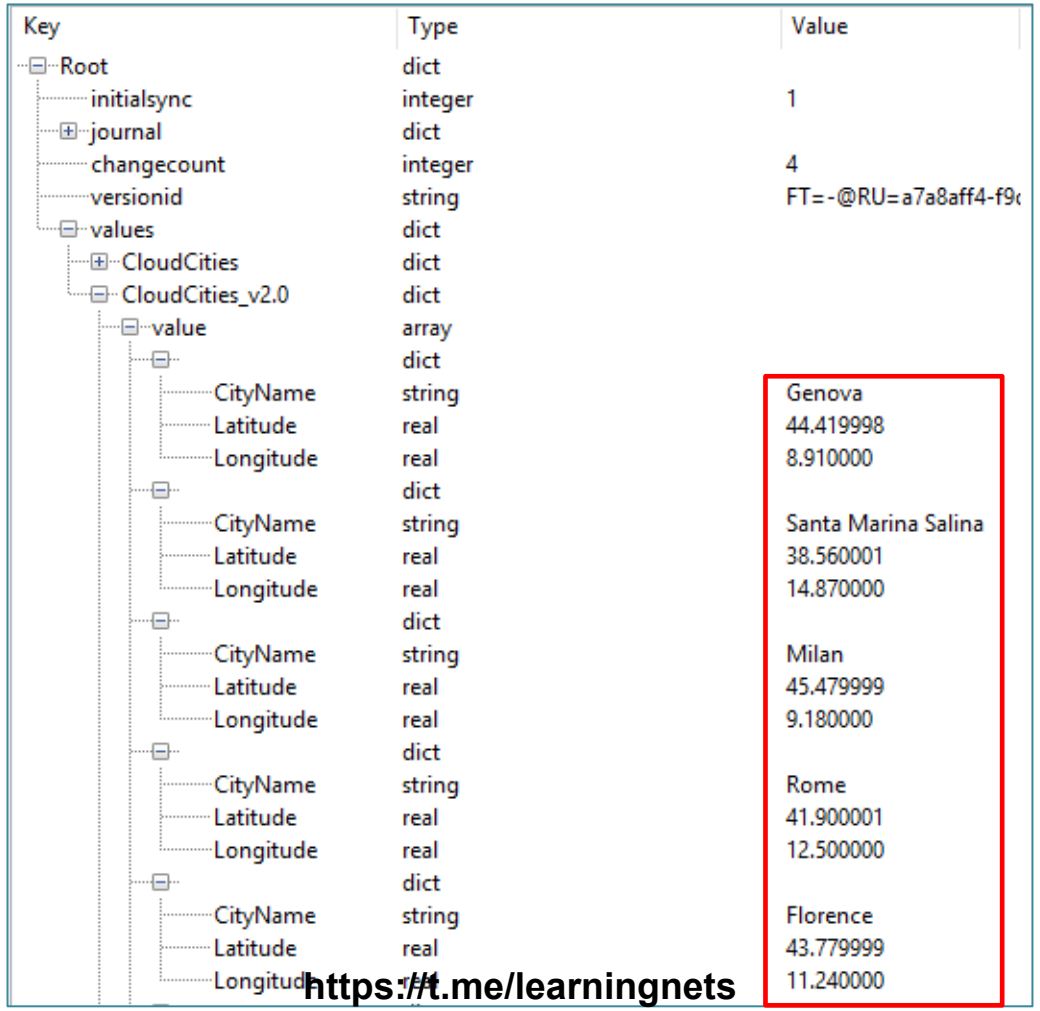
Key	Type	Value
All in One 2	dict	
_EDI FREE WiFi	dict	
Grands_2_1	dict	
Maggiemays Customer	dict	
Pargo-Feliz	dict	
Linkem For Hotel Liberta'	dict	
hotspot - Salina	dict	
HotelPalazzuolo-1	dict	
PirelliBS	dict	
HMONTREAL1a	dict	
muscatairport	dict	
Ibis	dict	
C2_Residence_F3	dict	
swisscom	dict	
Inerbole Wireless	dict	
Littys Hotel	dict	
value	dict	
WEP	boolean	false
IS_NETWORK_CONFIGURED	boolean	false
BSSID	string	24:65:11:5b:32:f2
AP_MODE	integer	2
IS_NETWORK_EXPIRABLE	boolean	false
UserDirected	boolean	false
IS_NETWORK_CAPTIVE	boolean	false
added_by	string	EpiPhone
WPA_IE	dict	
RSN_IE	dict	
enabled	boolean	true
IS_NETWORK_CUSTOMIZED	boolean	false
IS_NETWORK_EAP	boolean	false
added_at	string	Oct 2 2015 15:15:38
SSID_STR	string	Littys Hotel
remotevalue	data	...
timestamp	integer	467633952

WI-FI ACCESS POINTS

/PRIVATE/VAR/MOBILE/LIBRARY/SYNCEDPREFERENCES/COM.APPLE.WIFID.PLIST

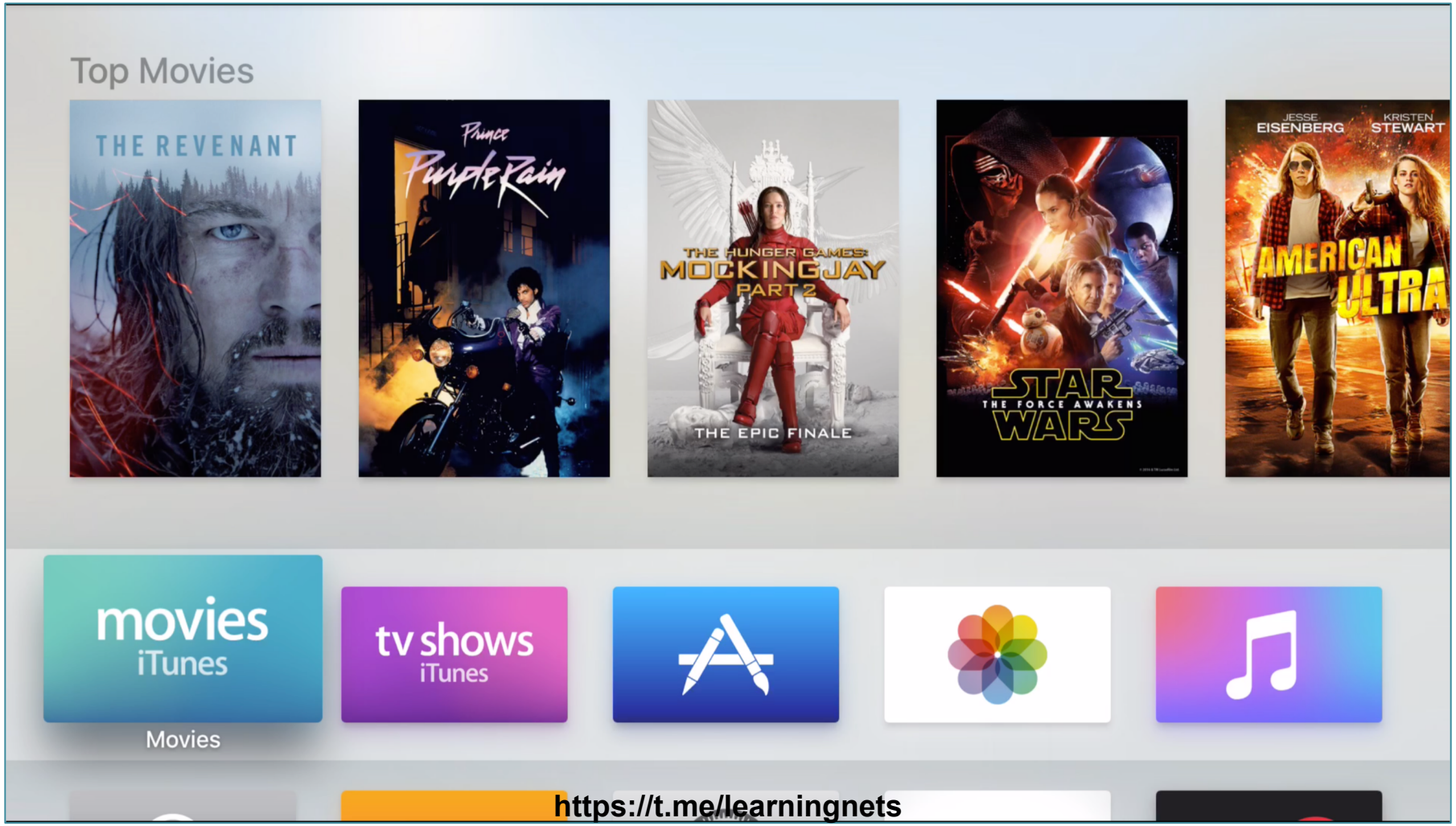
WEATHER CITIES

/PRIVATE/VAR/MOBILE/LIBRARY/SYNCEDPREFERENCES/COM.APPLE.NANOWEATHERPREFSD.PLIST



HEADBOARD

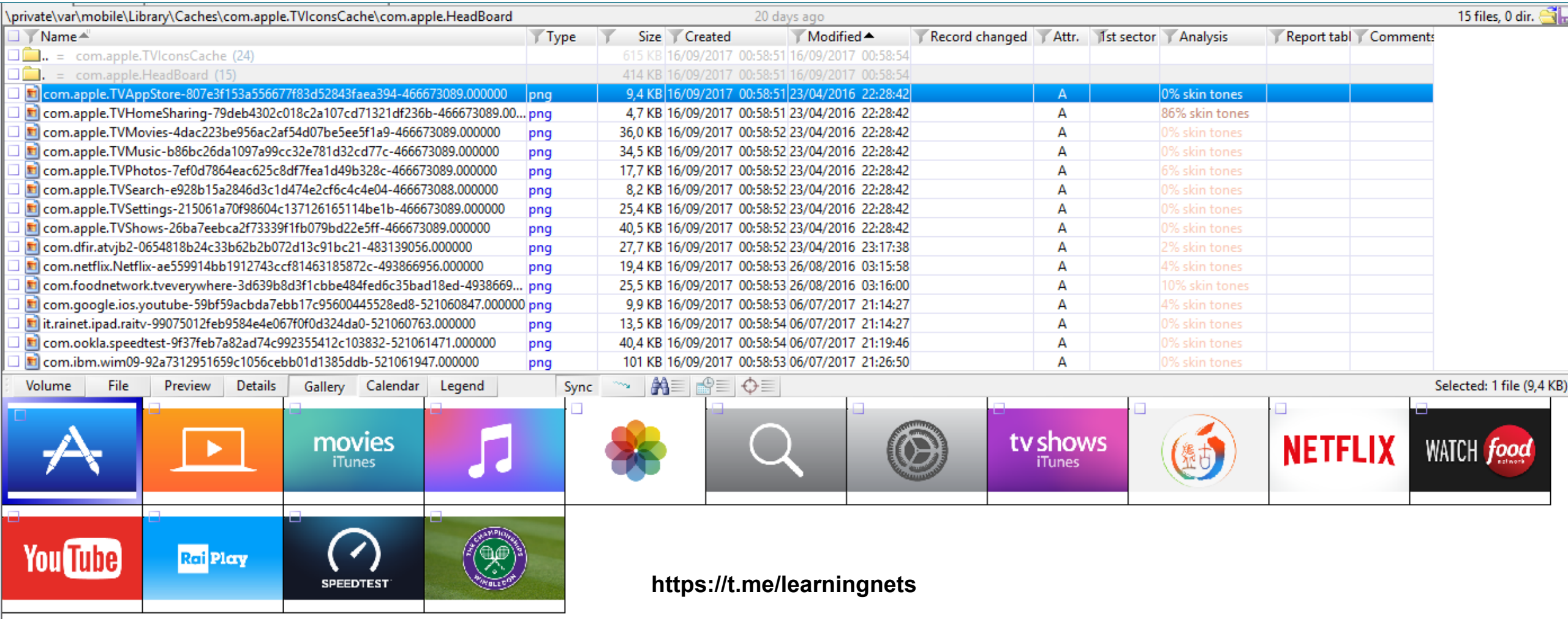
/PRIVATE/VAR/MOBILE/LIBRARY/COM.APPLE.HEADBOARD/APPORDER.PLIST



REALITYNET
System Solutions

HEADBOARD

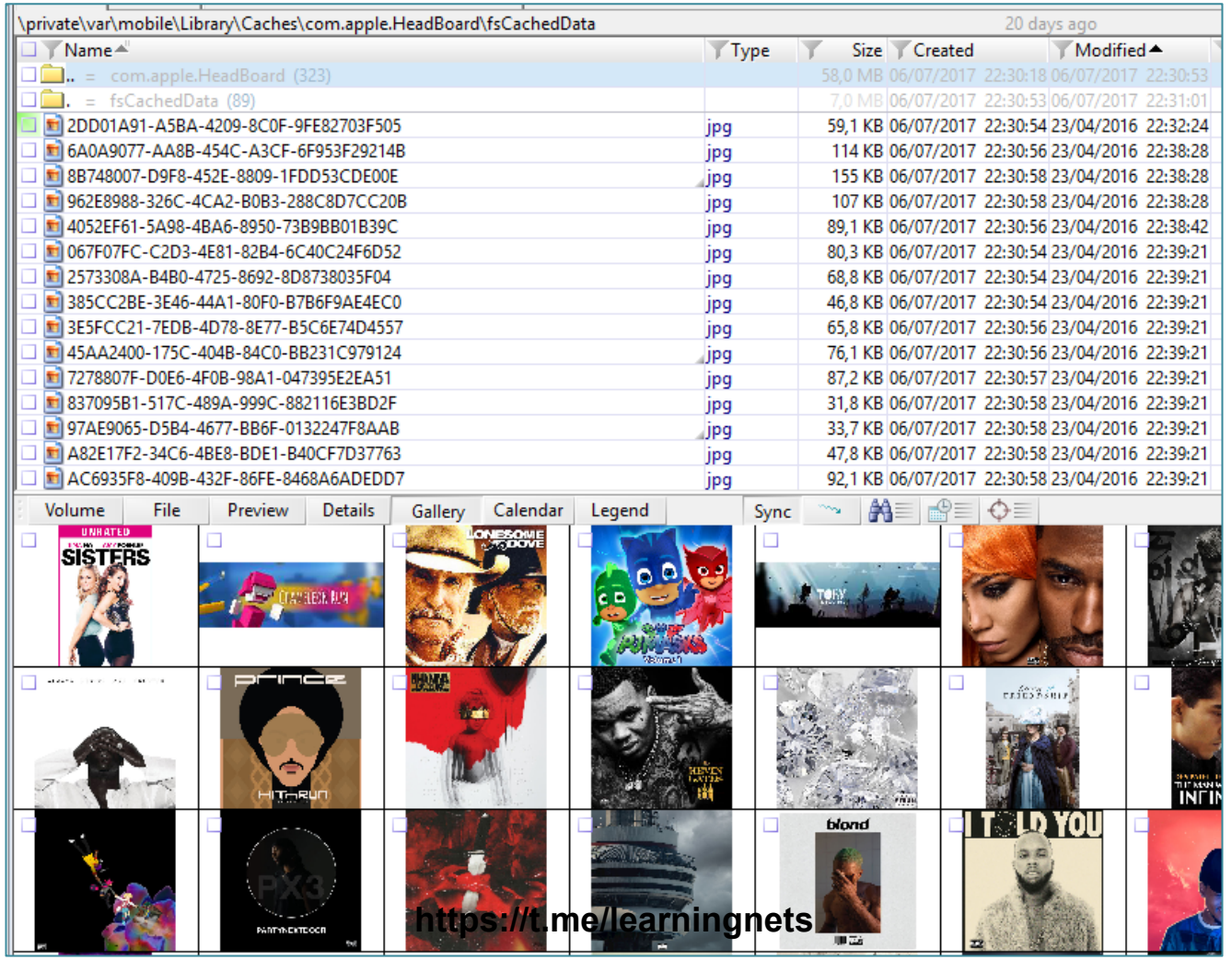
/PRIVATE/VAR/MOBILE/LIBRARY/CACHES/COM.APPLE.TVICONSCACHE/COM.APPLE.HEADBOARD



https://t.me/learningnets

HEADBOARD

/PRIVATE/VAR/MOBILE/LIBRARY/CACHES/COM.APPLE.HEADBOARD/FSCACHEDDATA



REALITYNET
System Solutions

APP SNAPSHOTS

/PRIVATE/VAR/MOBILE/LIBRARY/CACHES/COM.APPLE.PINEBOARD/ASSETLIBRARY/SNAPSHOTS/

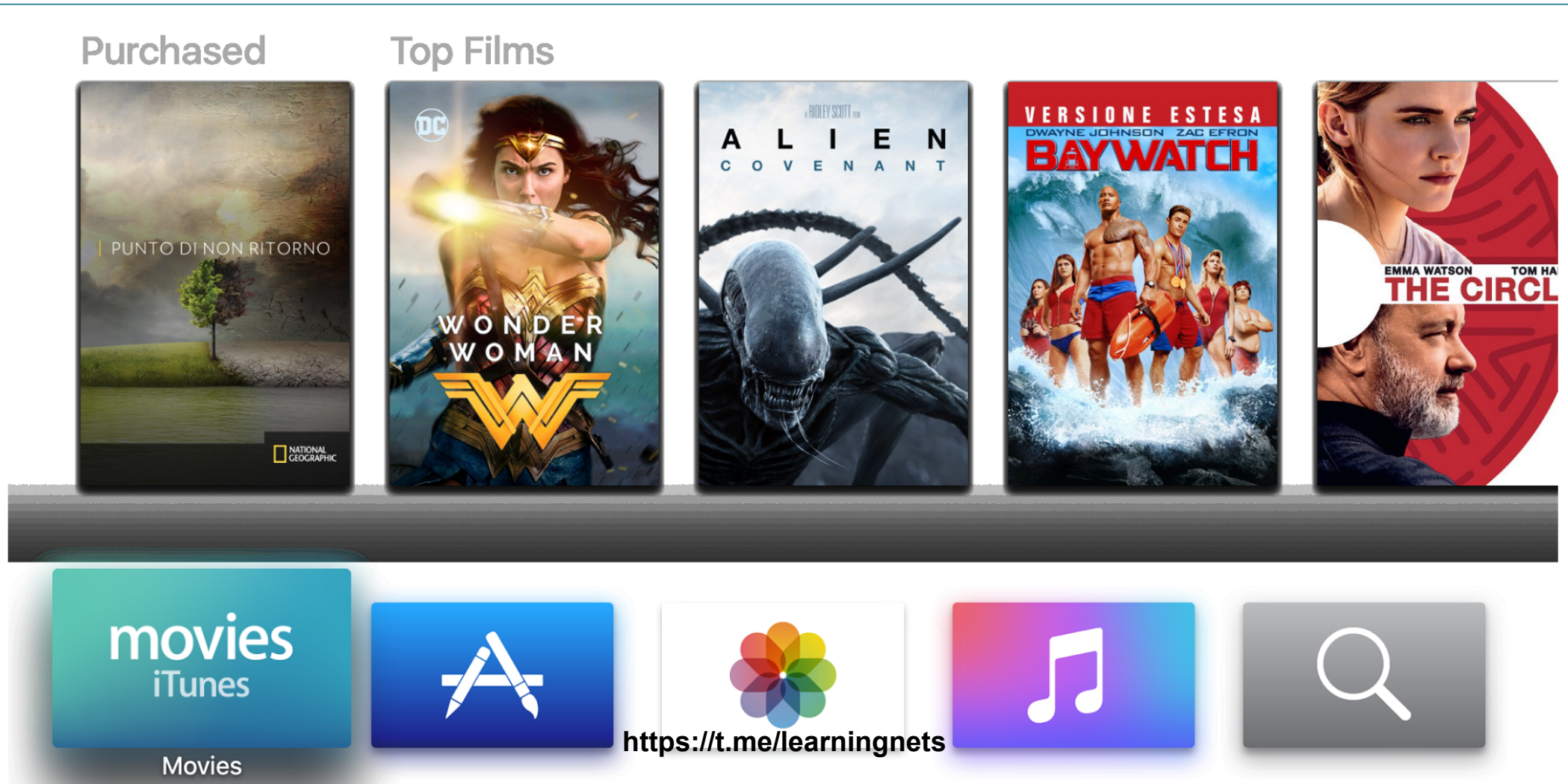
1 \private\var\mobile\Library\Caches\com.apple.PineBoard\AssetLibrary\Snapshots 20 days ago 15 files, 0 dir.

Name	Type	Category	Size	Created	Modified	Record changed	Attr.	1st sector	Analysis	Report tabl	Comr
.. = AssetLibrary (15)			11,6 MB	06/07/2017 22:31:01	06/07/2017 22:31:06						
. = Snapshots (15)			11,6 MB	06/07/2017 22:31:01	16/09/2017 00:51:58						
com.apple.TVShows	png	Pictures	1,5 MB	06/07/2017 22:31:03	23/04/2016 22:44:46		A		3% skin tones	Screenshot?	
com.foodnetwork.tveverywhere	png	Pictures	1,6 MB	06/07/2017 22:31:04	25/04/2016 01:30:41		A		2% skin tones	Screenshot?	
com.dfir.atvjb2	png	Pictures	119 KB	06/07/2017 22:31:04	02/05/2016 03:43:40		A		0% skin tones	Screenshot?	
it.rainet.ipad.raitv	png	Pictures	1,3 MB	06/07/2017 22:31:05	17/10/2016 23:57:02		A		1% skin tones	Screenshot?	
com.apple.TVMusic	png	Pictures	822 KB	06/07/2017 22:31:02	06/07/2017 21:22:35		A		1% skin tones	Screenshot?	
com.apple.TVHomeSharing	png	Pictures	35,5 KB	06/07/2017 22:31:02	13/07/2017 01:05:00		A		b/w	Screenshot?	
com.google.ios.youtube	png	Pictures	1,0 MB	06/07/2017 22:31:05	09/09/2017 23:20:02		A		3% skin tones	Screenshot?	
com.apple.TVAppStore	png	Pictures	1,0 MB	06/07/2017 22:31:02	09/09/2017 23:21:22		A		2% skin tones	Screenshot?	
com.apple.TVSearch	png	Pictures	89,6 KB	06/07/2017 22:31:03	09/09/2017 23:21:25		A		b/w	Screenshot?	
com.netflix.Netflix	png	Pictures	102 KB	06/07/2017 22:31:05	09/09/2017 23:21:57		A		0% skin tones	Screenshot?	
com.ibm.wim09	png	Pictures	1,6 MB	16/09/2017 00:51:58	09/09/2017 23:22:15		A		8% skin tones	Screenshot?	
com.apple.TVPhotos	png	Pictures	63,4 KB	06/07/2017 22:31:03	12/09/2017 23:25:55		A		b/w	Screenshot?	
com.apple.TVMovies	png	Pictures	429 KB	06/07/2017 22:31:02	12/09/2017 23:28:06		A		1% skin tones	Screenshot?	
com.apple.TVSettings	png	Pictures	115 KB	06/07/2017 22:31:03	12/09/2017 23:40:10		A		b/w	Screenshot?	
com.apple.HeadBoard	png	Pictures	1,8 MB	06/07/2017 22:31:02	16/09/2017 00:47:03		A		6% skin tones	Screenshot?	

Volume | File | Preview | Details | Gallery | Calendar | Legend | Sync

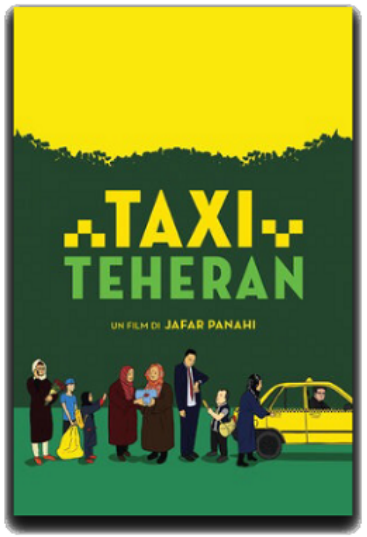
Selected: 1 file (429 KB)

HEADBOARD SNAPSHOTS



TVMOVIES SNAPSHOTS

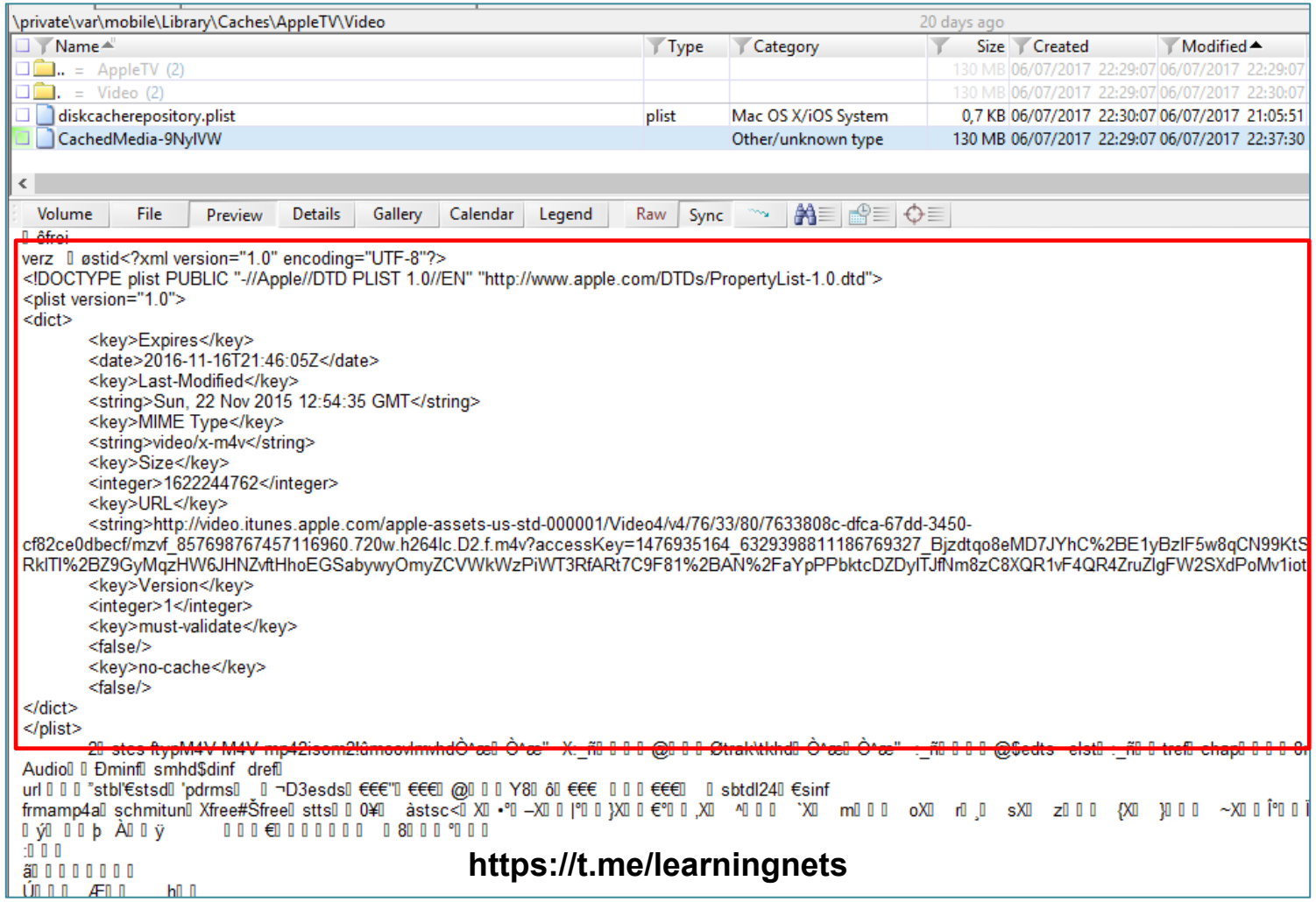
Purchased Top Films Genres Recommended Search



REALITYNET
System Solutions

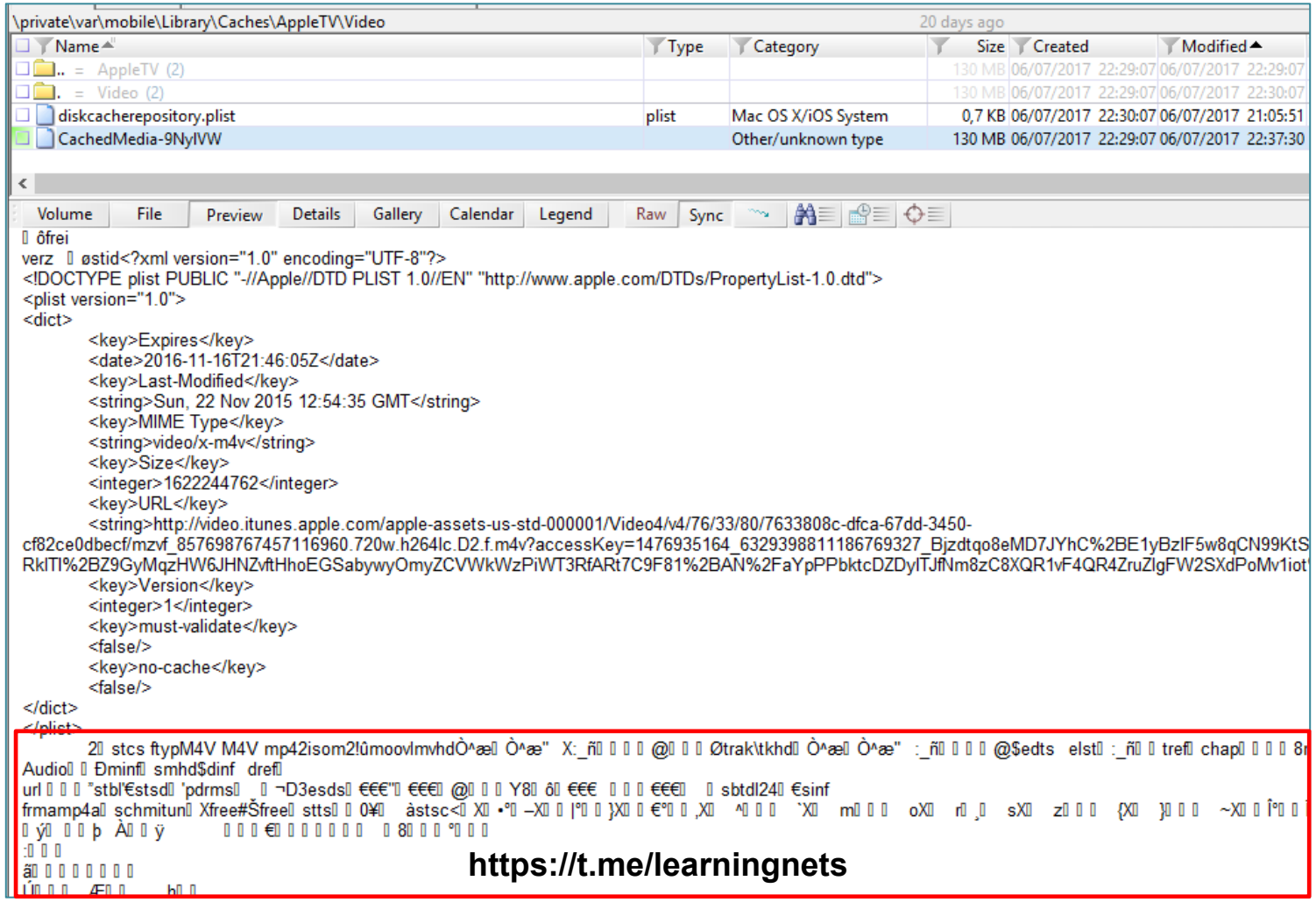
CACHED VIDEO

/PRIVATE/VAR/MOBILE/LIBRARY/CACHES/APPLETV/VIDEO/

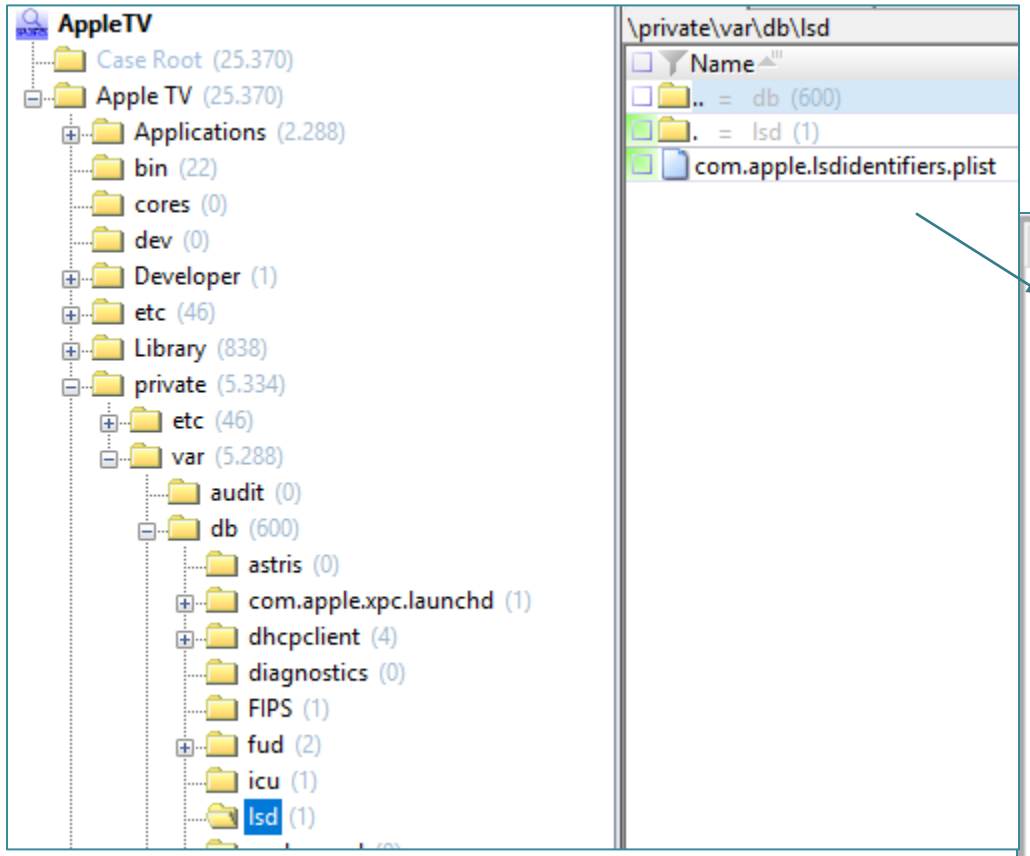


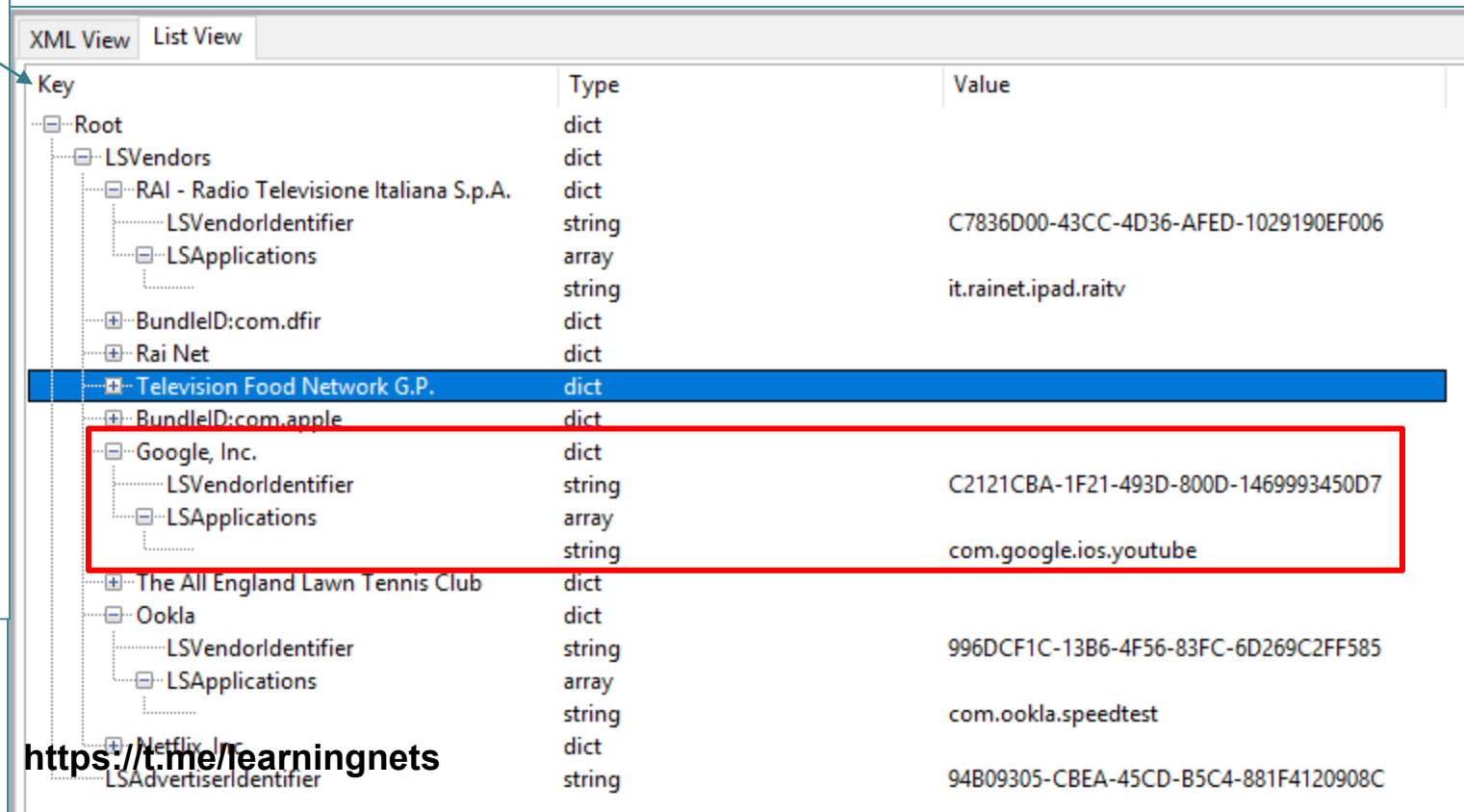
CACHED VIDEO

/PRIVATE/VAR/MOBILE/LIBRARY/CACHES/APPLETV/VIDEO/

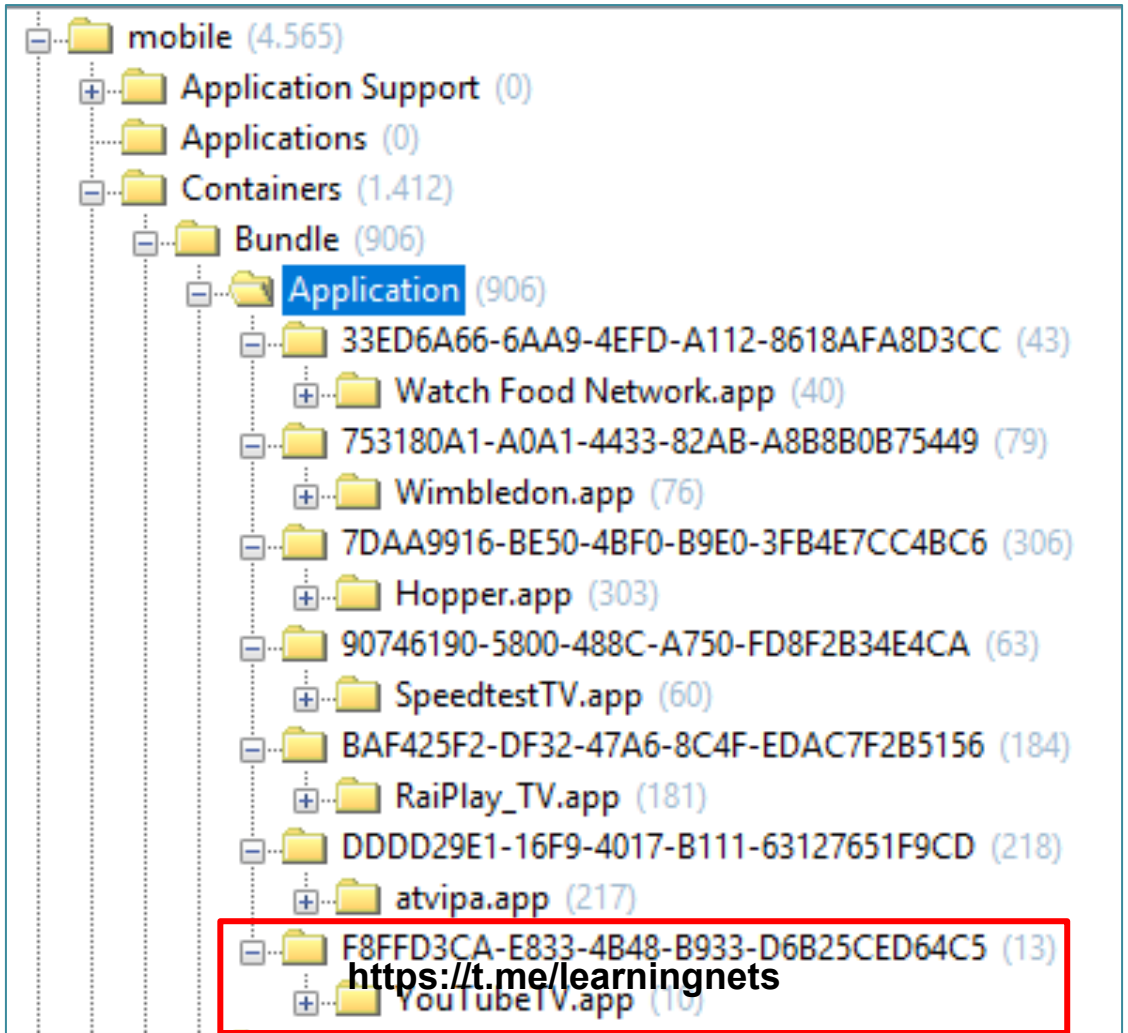


INSTALLED APPLICATIONS
/PRIVATE/VAR/DB/LSD/COM.APPLE.LSDIDENTIFIERS.PLIST

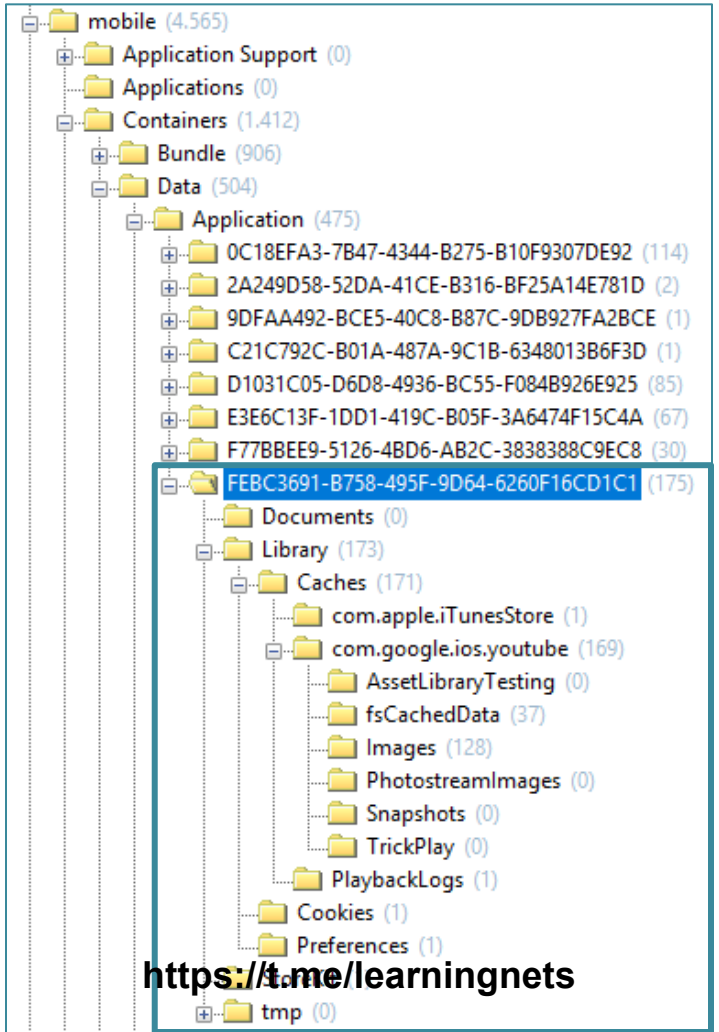




INSTALLED APPLICATIONS
/PRIVATE/VAR/MOBILE/CONTAINERS/BUNDLE/



INSTALLED APPLICATIONS
/PRIVATE/VAR/MOBILE/CONTAINERS/DATA/APPLICATION/

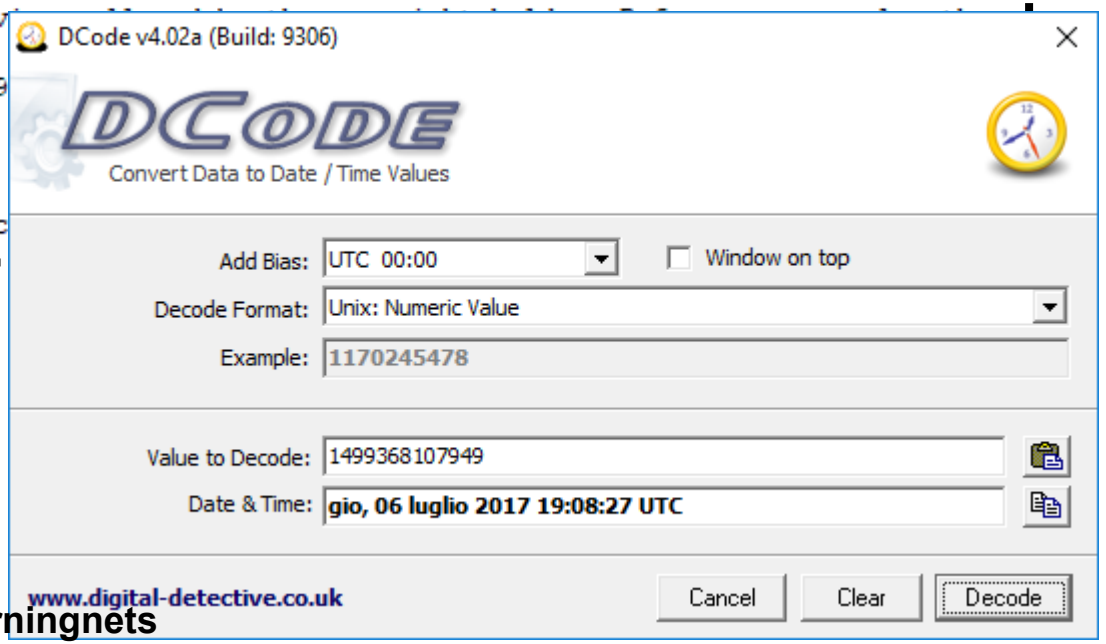


INSTALLED APPLICATIONS
YOU TUBE

mobile (4.565)
- Application Support (0)
- Applications (0)

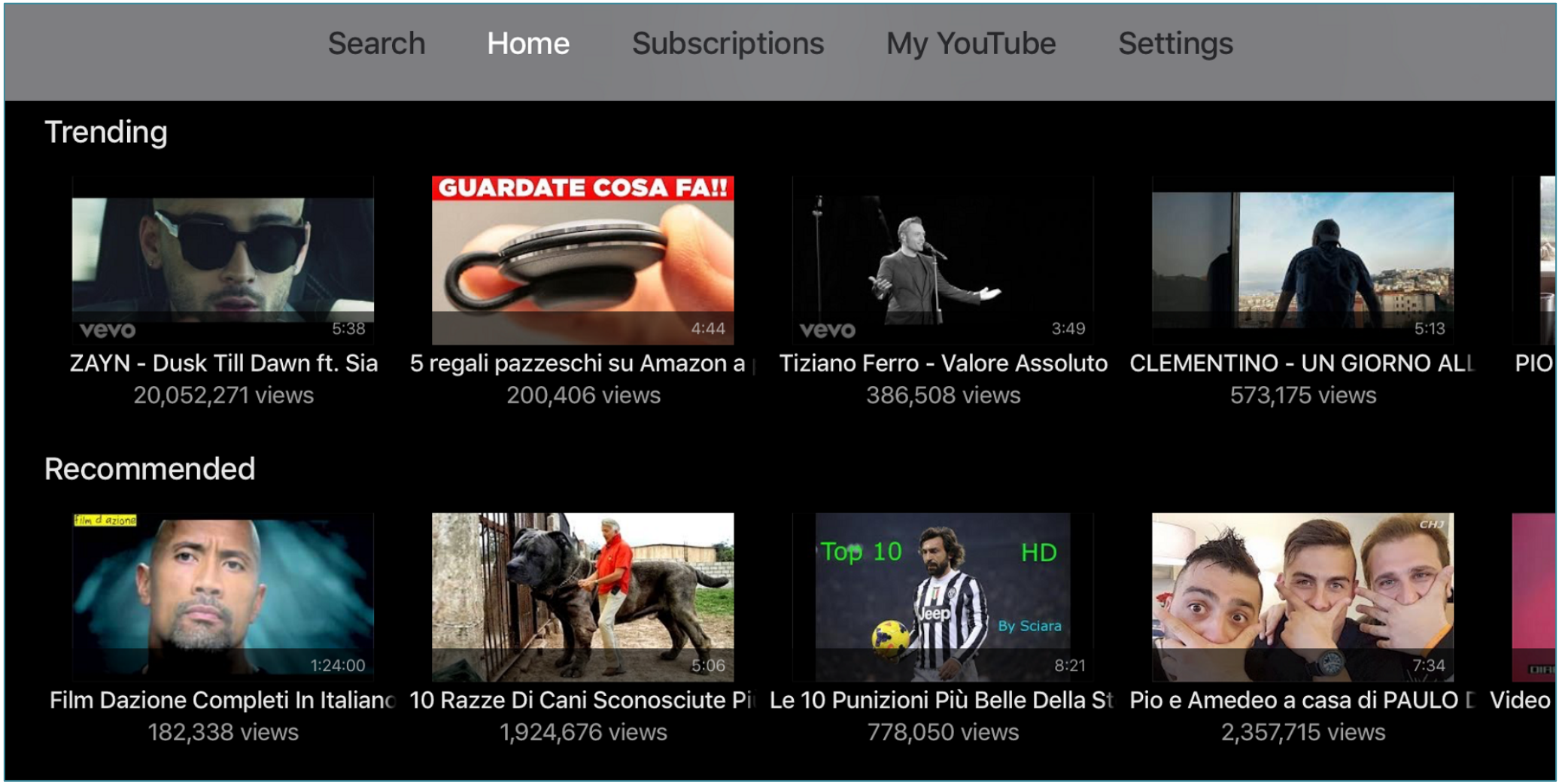
```
<key>preferences.plist</key>
<dict>
   <key>environment</key>
   <string>{"autoplay_disabled":"0","reload_optional_text":"Would you like to update?","reload_mandatory_title":"Update Required","ser
   "YouTube is unavailable. Please try again later.","base_url":"https://www.youtube.com","fps_purchase_not_found":"This video require
   "country":"IT","fps_video_forbidden":"This video is not available.","fps_unsupported_device":"Paid content can't be watched on this
   "default_failure_reason":"We are experiencing problems with our servers. Please try again later.","fps_key_host":"www.youtube.com",
   "device_model":"AppleTV5,3","fps_already_pinned_on_a_device":
   "This video has already been downloaded on the maximum number of dev
   "reload_dialog_button_update":"Update",
   "fexp":"9405991,9422596,9431012,9434289,9443436,9446054,9446364,9449
   <key>last-activity</key>
   <real>1499368107949.000000</real>
   <key>retention-data</key>
   <string>app_anon_id=5cbd0e7d-358a-4739-9c1e-28e8943870cb&amp;firstac
```

- com.google.ios.youtube (169)
  - AssetLibraryTesting (0)
  - fsCachedData (37)
  - Images (128)
  - PhotostreamImages (0)
  - Snapshots (0)
  - TrickPlay (0)
  - PlaybackLogs (1)
- Cookies (1)
- Preferences (1)
- StoreKit (1)
- tmp (0)



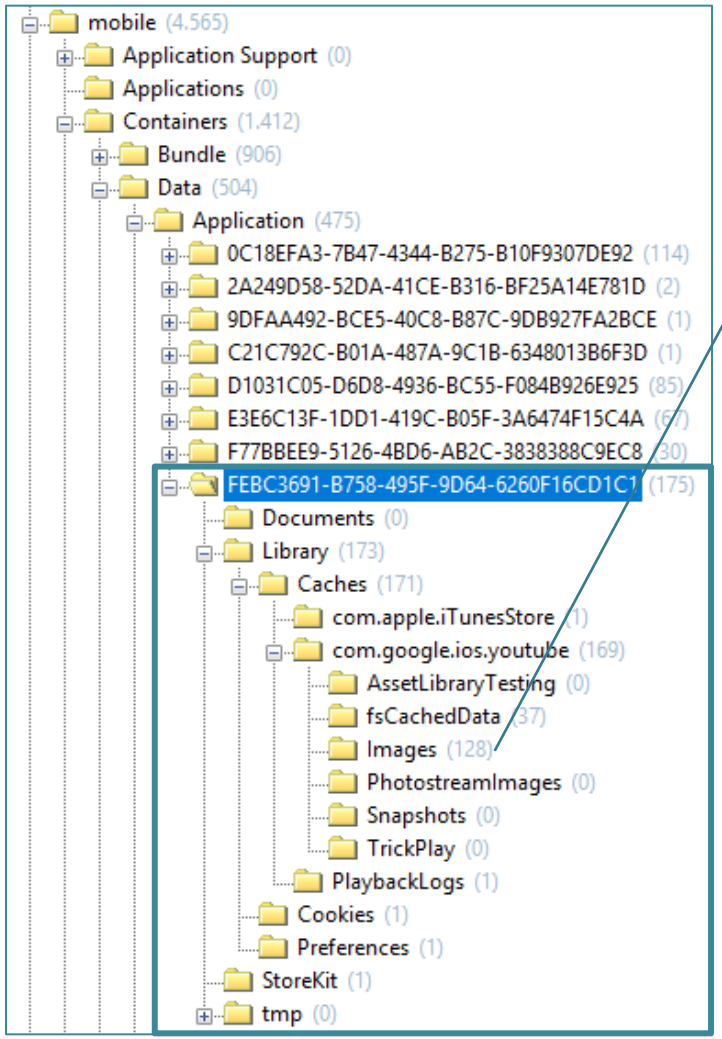
REALITYNET
System Solutions

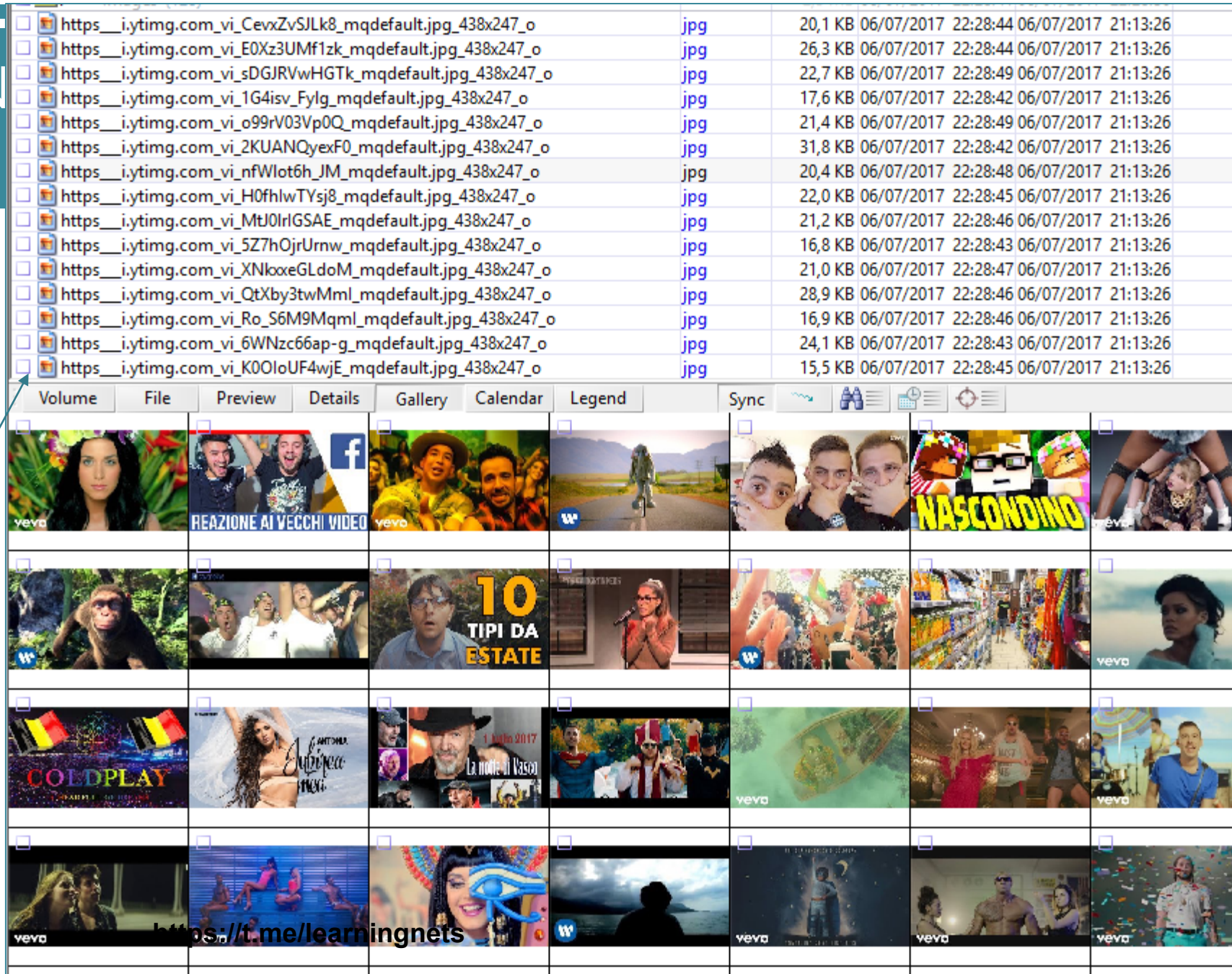
APP SNAPSHOTS
YOU TUBE



REALITYNET
System Solutions

IN





APPLE TV FORENSICS GUIDELINES

1. Identify the model
2. **Apple TV I Gen** → Acquire the hard drive and analyze it
3. **Apple TV II - IV Gen**
    1. Acquire **Real Time Logs**
    2. Acquire **Crash Logs**
    3. Acquire **File System via AFC**
    4. Acquire information via **Manual Acquisition**
    5. Verify if jailibreaking is applicable (type and OS version)
        1. **Jailbreak and acquire the whole file system**

APPLE TV
USEFUL TOOLS

- **Libimobiledevice** http://www.libimobiledevice.org/
- **iMobileDevice** http://docs.quamotion.mobi/en/latest/imobiledevice/download.html
- **iBackupBot** http://www.icopybot.com/itunes-backup-manager.htm
- **iExplorer** https://macroplant.com/iexplorer
- **iFunBox** http://www.i-funbox.com/
- **iOSLogInfo** http://support.blackberry.com/kb/articleDetail?articleNumber=000036986
- **Jailbreak**
  - **Pangu** **tvOS 9.0/9.1** http://dl.pangu.25pp.com/jb/Pangu9_ATV_v1.0.zip
  - **LiberTV** **tvOS 10.0/10.1** http://newosxbook.com/forum/viewtopic.php?f=12&t=16823
  - **LiberTV** **tvOS 11.0/11.1** http://newosxbook.com/libertv/
  - **Greengoblin** **tvOS 10.2.2** https://nito.tv/

THANKS!

Thanks to **Sarah Edwards** (**@iamevltwin**) for providing us a jailbroken AppleTV for testing and research!!

REALITYNET
System Solutions

Q&A?

Mattia Epifani

- Digital Forensics Analyst
- CEO @ REALITY NET – System Solutions
- GCFA, GCFE, GASF, GMOB, GNFA, GREM, GCWN

 mattia.epifani@realitynet.it

 @mattiaep

 http://www.linkedin.com/in/mattiaepifani

 http://www.realitynet.it

 http://blog.digital-forensics.it

Claudia Meda

- Digital Forensics Analyst
  @ REALITY NET – System Solutions

 claudia.meda@realitynet.it

 @KlodiaMaida

 https://www.linkedin.com/in/claudia-meda/

 http://www.realitynet.it

 http://blog.digital-forensics.it

REALITYNET
System Solutions

APPLE TV – MODEL IDENTIFICATION

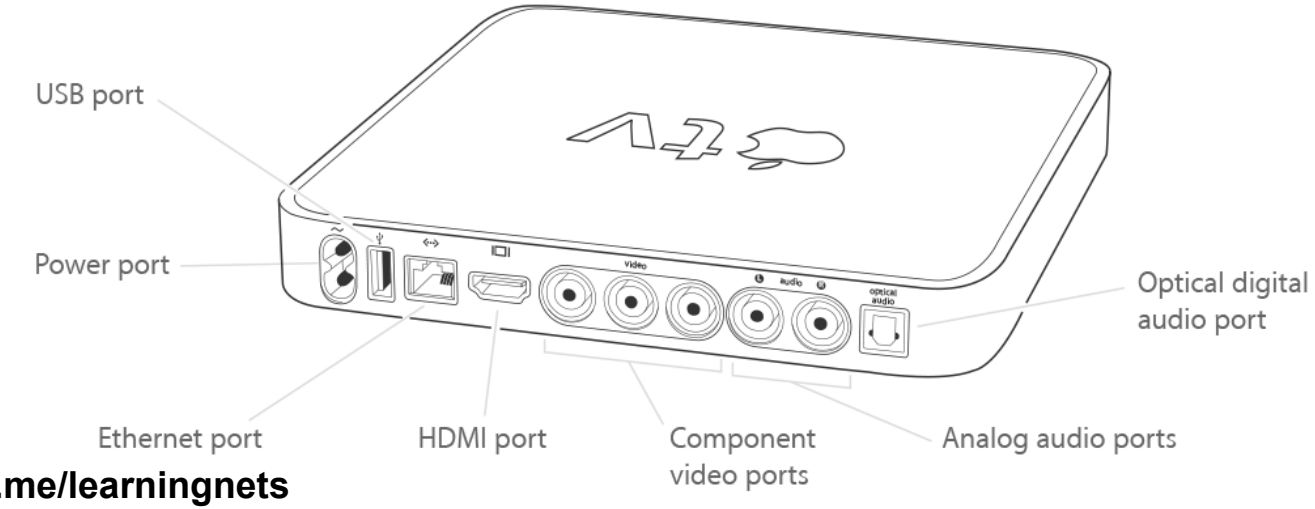
MATTIA EPIFANI – CLAUDIA MEDA

DFRWS 2018 EU

FLORENCE, 23 MARCH 2018

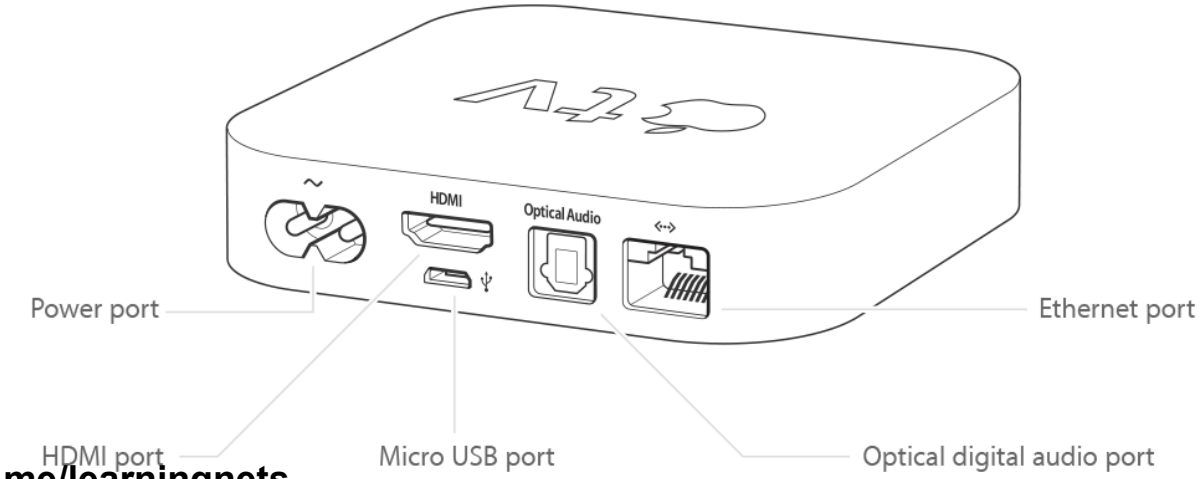
APPLE TV – 1° GENERATION

- Released in **2007**
- It contains a **traditional hard drive** (40 or 160 GB)
- The OS is based on **Mac OS X**
- Connectivity
  - Wi-Fi
  - Ethernet 10/100
  - USB 2.0
  - HDMI



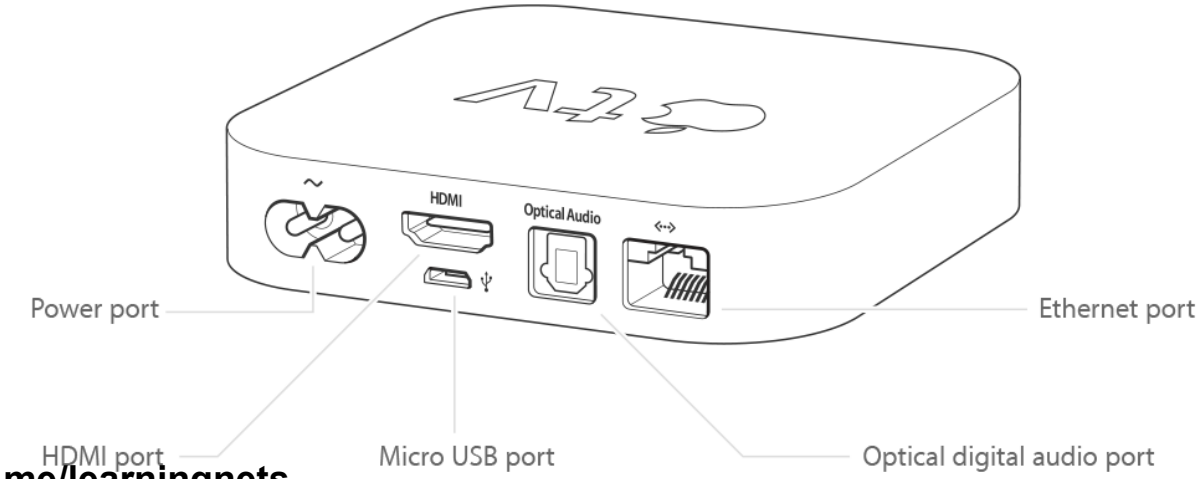
APPLE TV – II° GENERATION

- Released in **2010**
- It contains a **NAND flash memory (8 GB)**
- The OS is based on **iOS**
- Connectivity
  - Wi-Fi
  - Ethernet 10/100
  - Micro USB
  - HDMI



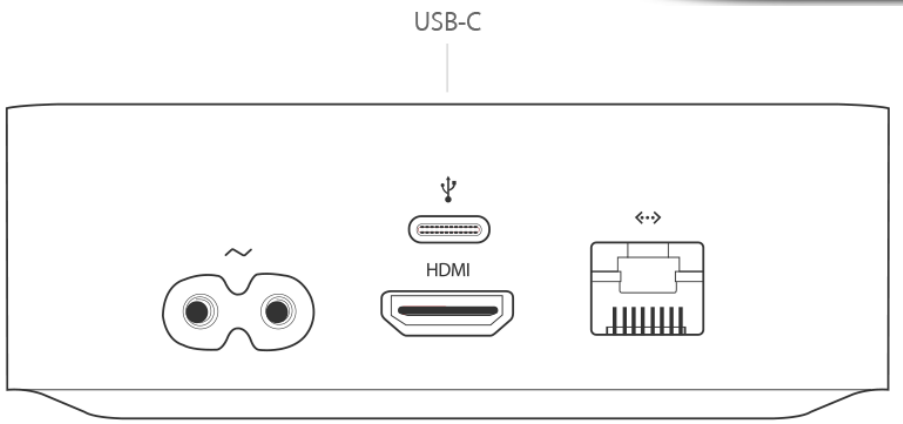
APPLE TV – III° GENERATION / III° GENERATION REV.A

- Released in **2012**
- It contains a **NAND flash memory (8 GB)**
- The OS is based on **iOS**
- Connectivity
  - Wi-Fi
  - Ethernet 10/100
  - Micro USB
  - HDMI



APPLE TV – IV° GENERATION

- Released in **2015**
- It contains a **NAND flash memory (32 or 64 GB)**
- The OS (**tvOS**) is based on **iOS**
- Connectivity
  - Wi-Fi
  - Ethernet 10/100
  - Bluetooth
  - USB-C
  - HDMI



APPLE TV – 4K (V° GENERATION)

- Released in **September 2017**
- It contains a **NAND flash memory (32 or 64 GB)**
- The OS (**tvOS**) is based on **iOS**
- Connectivity
  - Wi-Fi
  - Gigabit Ethernet
  - Bluetooth
  - HDMI