

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](https://support.apple.com/en-us/HT200008)



Designed by Apple in California Assembled in China Model A1469 EMC 2633 100-240~ 50-60Hz 0.3A
Complies with the Canadian ICES-003 Class B specifications. FCC ID: BCGA1469 IC: 579C-A1469



<https://t.me/learningnets>

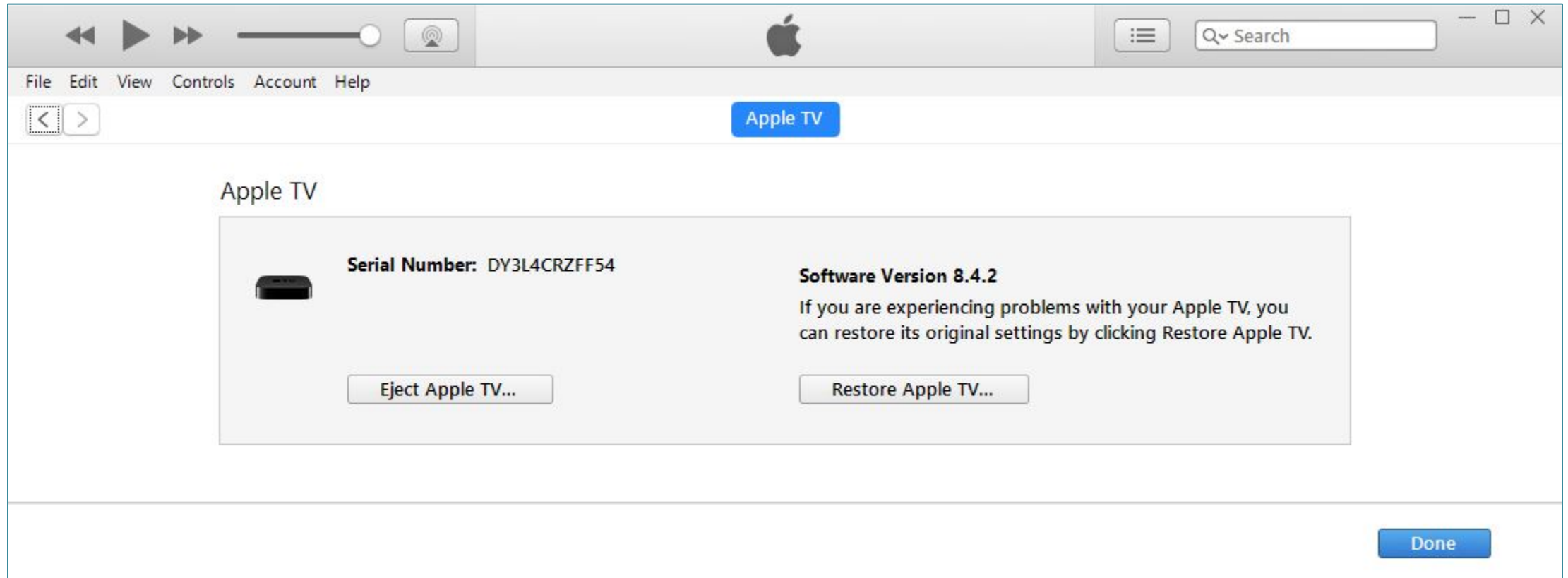
APPLE TV – 1^o GENERATION – ACQUISITION AND ANALYSIS

- 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

Informazioni

Nome	Apple TV Mattia
Modello	A1469
Numero di serie	DY3L4CRZFF54
Software Apple TV	7.2 (7512)
Risoluzione TV	1080p HD - 60Hz
Rete Wi-Fi	NETGEAR13
Indirizzo IP	DHCP 192.168.1.4
Indirizzo Wi-Fi	a0:ed:cd:d7:12:7c
Potenza segnale	●●●○○

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: NoTelephonyCapability
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
Y0VCYWVhNEFlbjQ4amJ3K2w0OWdlWVQ5MHNpU
XV4VFhyNDJ2dWpSZgo3c3E1UFZtTy9ZUHVsn1
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
```

APPLE TV – II° – IV° GENERATION – REAL TIME LOG IDVICESYSLOG ([HTTP://WWW.LIBIMOBILEDEVICE.ORG/](http://www.libimobiledevice.org/))

```
Seleziona Prompt dei comandi - idervicesyslog
C:\imobiledevice>idervicesyslog
[connected]

Jan  1 01:00:23 Apple-TV-Mattia apsd[69] <Warning>: WiFi is associated NO
Jan  1 01:00:23 Apple-TV-Mattia wifiFirmwareLoader[43] <Warning>: WiFiUserClientCompleteMapping return 0
Jan  1 01:00:23 Apple-TV-Mattia wifiFirmwareLoader[43] <Warning>: wifiFirmwareLoaderThread exiting with 0
Jan  1 01:00:23 Apple-TV-Mattia wifiFirmwareLoader[43] <Warning>: Shutting down
Jan  1 01:00:24 Apple-TV-Mattia wifid[56] <Error>: WiFi:[-978307175.980007]: Disable WoW requested by "apsd"
Jan  1 01:00:24 Apple-TV-Mattia kernel[0] <Notice>: 000025.236306 wlan0.A[12] AppleBCMWLANCore::configureTrgDis
c(): Disabling Enhanced Trigger Disconnect Mode
Jan  1 01:00:24 Apple-TV-Mattia kernel[0] <Notice>: 000025.236384 wlan0.N[13] AppleBCMWLANCore::setupDriver():
State 0x30
Jan  1 01:00:24 Apple-TV-Mattia kernel[0] <Notice>: 000025.316365 wlan0.A[14] AppleBCMWLANCore::setupDriver():
Core Driver Initialization Time 25.316331541
Jan  1 01:00:24 Apple-TV-Mattia kernel[0] <Notice>: 000025.316539 wlan0.A[15] AppleBCMWLANIOReporting::init():
Provider 0xc8106000, name AppleBCMWLANCore
Jan  1 01:00:24 Apple-TV-Mattia kernel[0] <Notice>: bpfAttach len 60 dlt 12
Jan  1 01:00:24 Apple-TV-Mattia kernel[0] <Notice>: en1::finishAttachToDataLinkLayer name <en1> successful atta
ch to bpf type 147
Jan  1 01:00:24 Apple-TV-Mattia backboardd[45] <Notice>: 1970-01-01 01:00:24.037627 AM [AppleTVIR] Initializing
Jan  1 01:00:24 Apple-TV-Mattia backboardd[45] <Notice>: ____IOHIDSessionScheduleAsync_block_invoke: thread_id=
0x1cf0000
Jan  1 01:00:24 Apple-TV-Mattia backboardd[45] <Notice>: HID Session async scheduling initiated.
Jan  1 01:00:24 Apple-TV-Mattia backboardd[45] <Notice>: HID Session async root queue running at priority 63 an
d schedule 2.
```

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

The screenshot displays the iBackupBot for iPad iPhone application window. The interface includes a menu bar (File, View, Settings, Help), a toolbar with various icons, and a main content area. On the left, there are two panels: 'Backups' (currently empty) and 'Devices' (showing a tree view for 'Apple TV Mattia' with sub-items like 'Raw File System', 'Tools', 'System Log', and 'Crash Report', and 'iPhone mattia'). The main area features an 'Export' button, a search box, and a 'System Logs' section. The logs contain several entries with timestamps and messages, including warnings about framework loading and notices about syslog relay. At the bottom of the window, there is a status bar with the text 'Welcome to iBackupBot for iPad iPhone' on the left and '5.5.1' on the right. A URL <https://t.me/learningnets> is overlaid at the bottom center of the image.

System Logs

```
)  
Sep 14 08:27:04 Apple-TV-Mattia addaily[127] <Warning>: daily tasks for day 17422  
Sep 14 08:27:12 Apple-TV-Mattia crash_mover[126] <Warning>: Unable to load framework NanoPreferencesSync  
Sep 14 08:27:12 Apple-TV-Mattia crash_mover[126] <Warning>: Unable to load framework NanoSystemSettings  
Sep 14 08:27:12 Apple-TV-Mattia crash_mover[126] <Warning>: Unable to load framework ProxiedCrashCopierClient  
Sep 14 08:27:12 Apple-TV-Mattia crash_mover[126] <Notice>: (Warn ) <crash_mover.m fetchFilesFromPairedDeviceForAppleCare:265> Unable to dynamica  
Sep 14 08:27:14 Apple-TV-Mattia addaily[127] <Warning>: Symptoms timed out, no datausage available  
Sep 14 08:27:20 Apple-TV-Mattia crash_mover[128] <Warning>: Unable to load framework NanoPreferencesSync  
Sep 14 08:27:20 Apple-TV-Mattia crash_mover[128] <Warning>: Unable to load framework NanoSystemSettings  
Sep 14 08:27:20 Apple-TV-Mattia crash_mover[128] <Warning>: Unable to load framework ProxiedCrashCopierClient  
Sep 14 08:27:20 Apple-TV-Mattia crash_mover[128] <Notice>: (Warn ) <crash_mover.m fetchFilesFromPairedDeviceForAppleCare:265> Unable to dynamica  
Sep 14 08:27:24 Apple-TV-Mattia addaily[127] <Warning>: addaily ended  
Sep 14 08:29:29 Apple-TV-Mattia UserEventAgent[18] <Warning>: scheduled session log  
Sep 14 08:29:29 Apple-TV-Mattia UserEventAgent[18] <Warning>: Filtering only beta sessions  
Sep 14 08:29:29 Apple-TV-Mattia UserEventAgent[18] <Warning>: Session log: no events recorded  
Sep 14 08:33:02 Apple-TV-Mattia syslog_relay[116] <Notice>: syslog_relay read 51 total bytes:  
=====  
ASL is here to serve you  
Sep 14 08:33:02 Apple-TV-Mattia syslog_relay[116] <Notice>: syslog_relay found the ASL prompt. Starting...
```

<https://t.me/learningnets>

Welcome to iBackupBot for iPad iPhone 5.5.1

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

The screenshot shows the iBackupBot for iPad iPhone application window. The interface includes a menu bar (File, View, Settings, Help), a toolbar with various icons, and a main workspace. On the left, there are two panes: 'Backups' (currently empty) and 'Devices'. The 'Devices' pane shows a tree structure for 'Apple TV Mattia', including 'Raw File System', 'Tools', 'System Log', and 'Crash Report'. The 'Crash Report' folder is expanded, showing a sub-tree with 'com.apple.itunesstored', 'DiagnosticLogs', 'Message', and 'Retired'. The main workspace displays a table of files and folders.

Name	Size	Type	Date Modified
com.apple.itunesstored		Folder	
DiagnosticLogs		Folder	
Message		Folder	
Retired		Folder	
CoreTime-2017-09-12-222944.ips	2.2 kB	ips File	09/12/17 22:35:21

At the bottom of the window, the status bar reads: 'Welcome to iBackupBot for iPad iPhone' on the left and '5.5.1' on the right.

<https://t.me/learningnets>

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

The screenshot shows the iBackupBot for iPad iPhone application window. The interface includes a menu bar (File, View, Settings, Help), a toolbar with various icons, and a main workspace divided into three panes. The left pane shows a tree view of devices, with 'Apple TV Mattia' selected. The middle pane shows a tree view of the 'Raw File System' for the selected device, including folders like DCIM, Documents, Downloads, PhotoData, Photos, PublicStaging, general_storage, iTunes_Control, Music, iTunes, and HomeShares. The right pane displays a table of files and folders within the 'iTunes' folder.

Name	Size	Type	Date Modified
..		Folder	01/01/70 01:00:00
HomeShares		Folder	01/01/70 01:00:53
AdLoc.data	495	data File	04/02/16 18:19:22
IC-Info.sidl	42.4 kB	sidl File	01/08/16 23:03:39
IC-Info.sidv	1.1 kB	sidv File	07/28/15 21:31:47
MediaLibrary.sqlitedb	524.0 kB	sqlitedb File	08/10/16 19:05:58
MediaLibrary.sqlitedb-shm	32.0 kB	sqlitedb-shm File	09/12/17 23:16:41
MediaLibrary.sqlitedb-wal	688.0 kB	sqlitedb-wal File	09/14/17 00:45:19
iTunesDRMDB.itlp	0	itlp File	09/14/17 00:55:18
iTunesPrefs	0	File	01/18/16 00:43:43

https://t.me/learningnets

Welcome to iBackupBot for iPad iPhone 5.5.1

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

```
C:\WINDOWS\system32\cmd.exe

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 3.0/Win for A5+

(c) 2011-2018 Elcomsoft Co. Ltd.

Write device info to file <ideviceinfo.xml>:

Write installed applications list to file <applications.txt>:

Write full installed applications info to file <applications.xml>:

Getting basic device info...

Getting installed applications list...

Getting full installed applications info...

Device info is written to ideviceinfo.xml
Installed applications list is written to applications.txt
Full installed applications info is written to applications.xml

Press 'Enter' to continue
```

```
C:\WINDOWS\system32\cmd.exe

Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 3.0/Win for A5+

(c) 2011-2018 Elcomsoft Co. Ltd.

Write files to directory <current directory>:

Copying file /DCIM/100APPLE/iOS Forensics.pptx: OK
Copying file /Downloads/downloads.28.sqlitedb: OK
Copying file /general_storage/iOS Forensics.pptx: OK
Copying file /iTunes_Control/iTunes/AdLoc.data: OK
Copying file /iTunes_Control/iTunes/IC-Info.sidl: OK
Copying file /iTunes_Control/iTunes/IC-Info.sidv: OK
Copying file /iTunes_Control/iTunes/MediaLibrary.sqlitedb: OK
Copying file /iTunes_Control/iTunes/MediaLibrary.sqlitedb-shm: OK
Copying file /iTunes_Control/iTunes/MediaLibrary.sqlitedb-wal: OK
Copying file /iTunes_Control/iTunes/iTunesDRMDB.itlp: OK
Copying file /iTunes_Control/iTunes/iTunesPrefs: OK

Copying finished

Statistics:
  Total files: 11
  Copy OK: 11
  Copy FAILED: 0

Press 'Enter' to continue
```

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

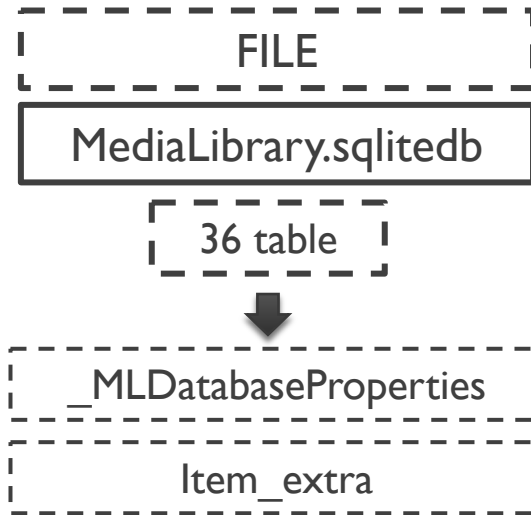
III-generation Apple TV Model A1469

```
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

III-generation Apple TV
Model A1469

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



Synchronized with
iTunes account

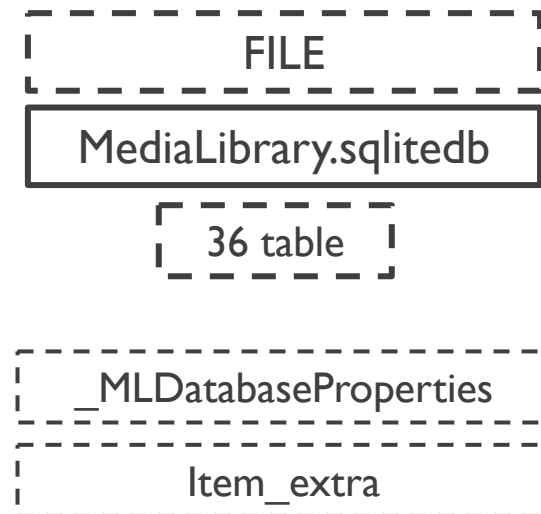
_MLDatabaseProperties
iCloud Account ID

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



APPLE TV – IV° GENERATION – JAILBREAKING

[HTTPS://WWW.THEIPHONEWIKI.COM/WIKI/JAILBREAK](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	

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://www.me/learningsnet> <https://twitter.com/learningnet> <https://www.facebook.com/learningnet> <https://www.instagram.com/learningnet> <https://www.linkedin.com/company/learningnet> <https://www.youtube.com/channel/UCmpson/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

```


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

The image shows a file explorer window with the following structure:

- dev (0)
- Developer (1)
- etc (46)
 - asl (26)
 - dropbear (2)
 - ppp (0)
 - racoon (3)
 - rc.d (1)
- Library (838)
- private (5.334)
 - etc (46)
 - var (5.288)
 - audit (0)
 - db (600)
 - astris (0)
 - com.apple.xpc.launchd (1)
 - dhcpclient (4)
 - leases (1)

The main pane shows the path `\private\var\db\dhcpclient\leases` with a table of files:

Name	Type
.. = dhcpclient (4)	
. = leases (1)	
en1-1,d0%3A3%3A4b%3Ae6%3A47%3A2c	plist

An arrow points from the file `en1-1,d0%3A3%3A4b%3Ae6%3A47%3A2c` to a detailed view of its contents:

```
IPAddress
192.168.1.3

LeaseLength
86400

LeaseStartDate
2016-10-20T18:36:46Z

PacketData

AgEGAMWNG3EAAgAAAAA
AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAA
AQT///8AAwTAqAEBBgTAqAE

RouterHardwareAddress

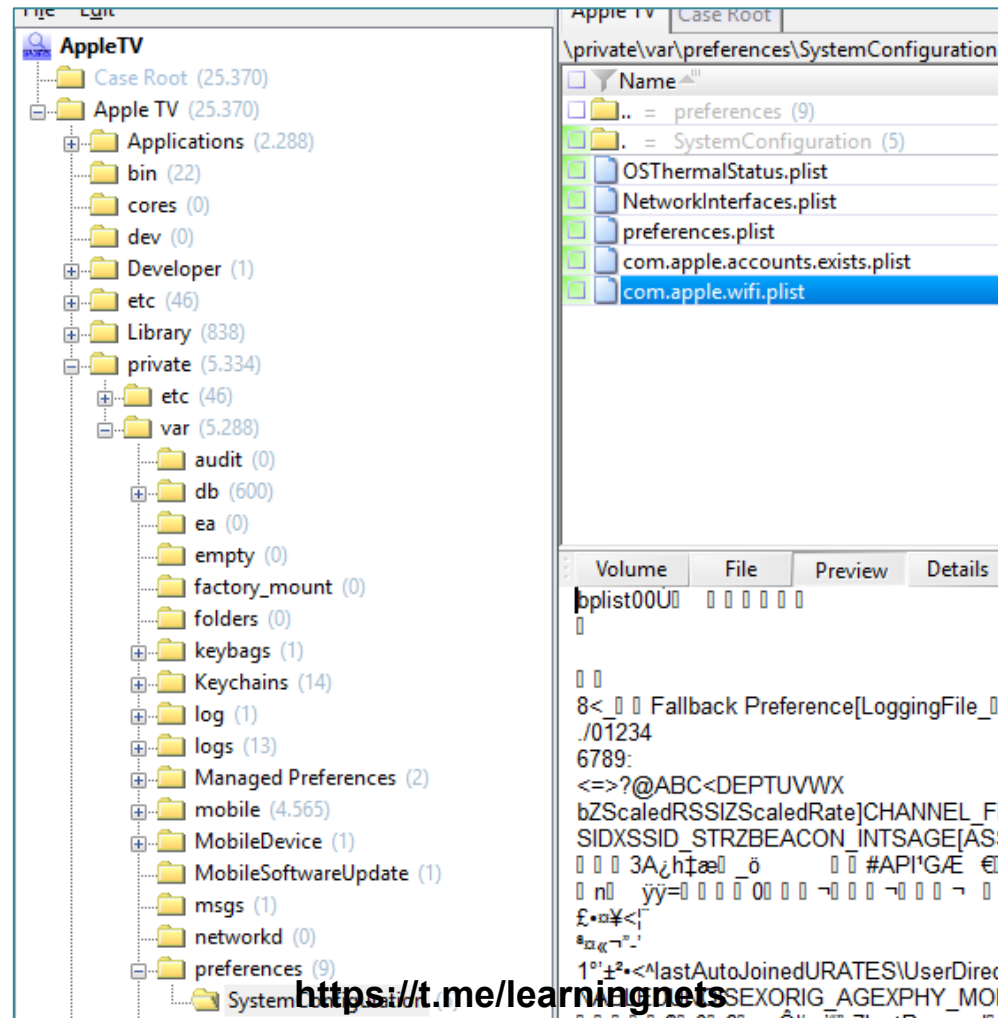
CL1DaB9I

RouterIPAddress
192.168.1.1

SSID
NETGEAR13
```

NETWORK WI-FI HISTORY

/PRIVATE/VAR/PREFERENCES/COM.APPLE.WIFI.PLIST



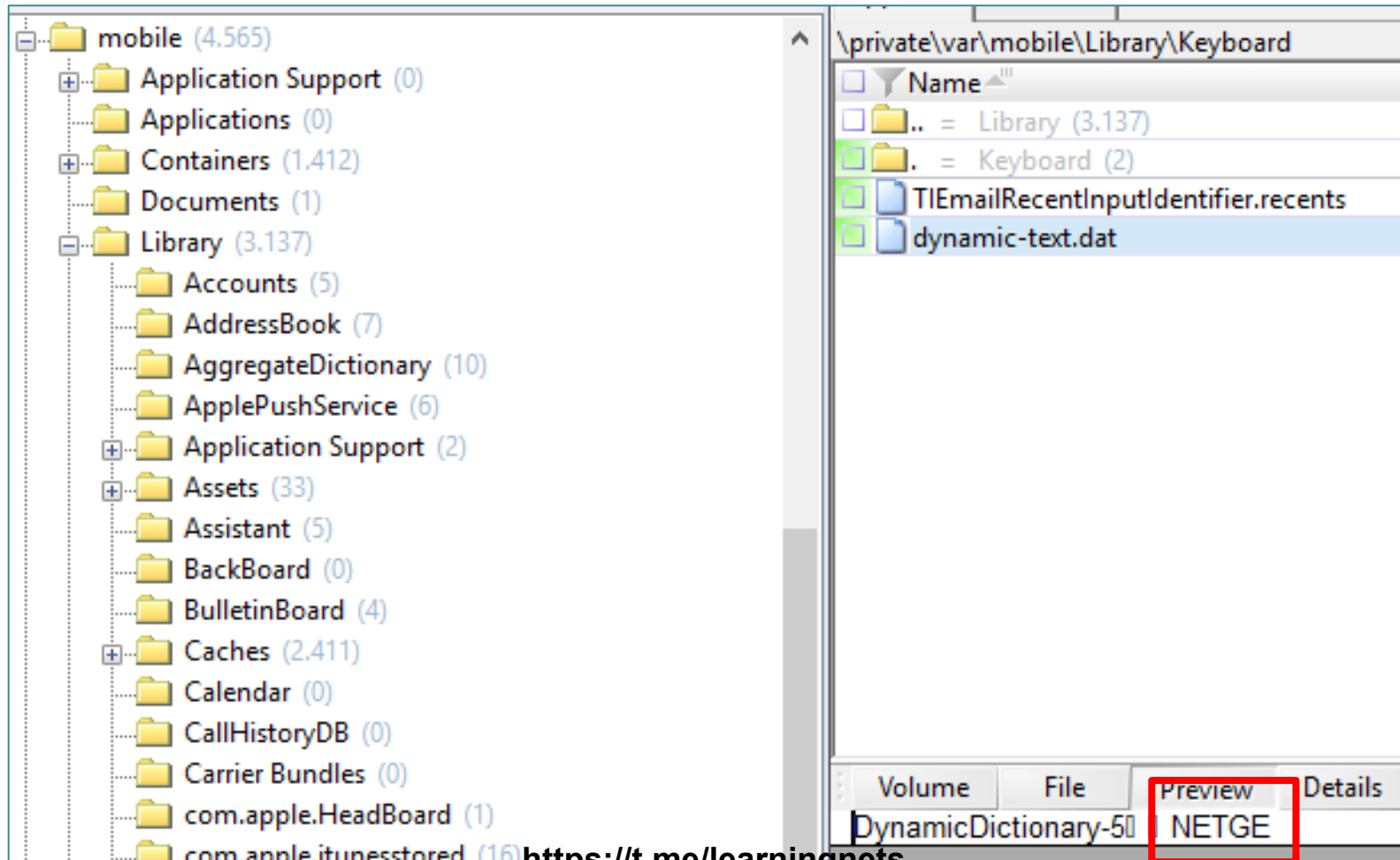
NETWORK WIFELIST HISTORY

List of known networks		
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:...
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		
	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:...
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
ASSOC_FLAGS	integer	20
WiFiManagerKnownNetworksEventType	integer	1

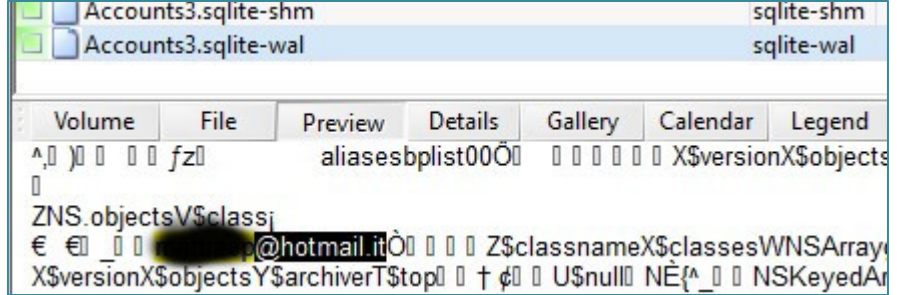
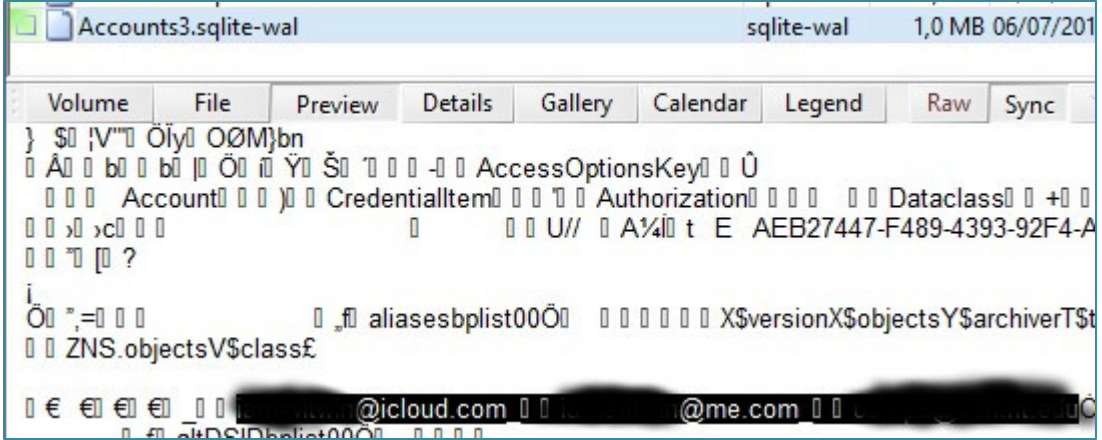
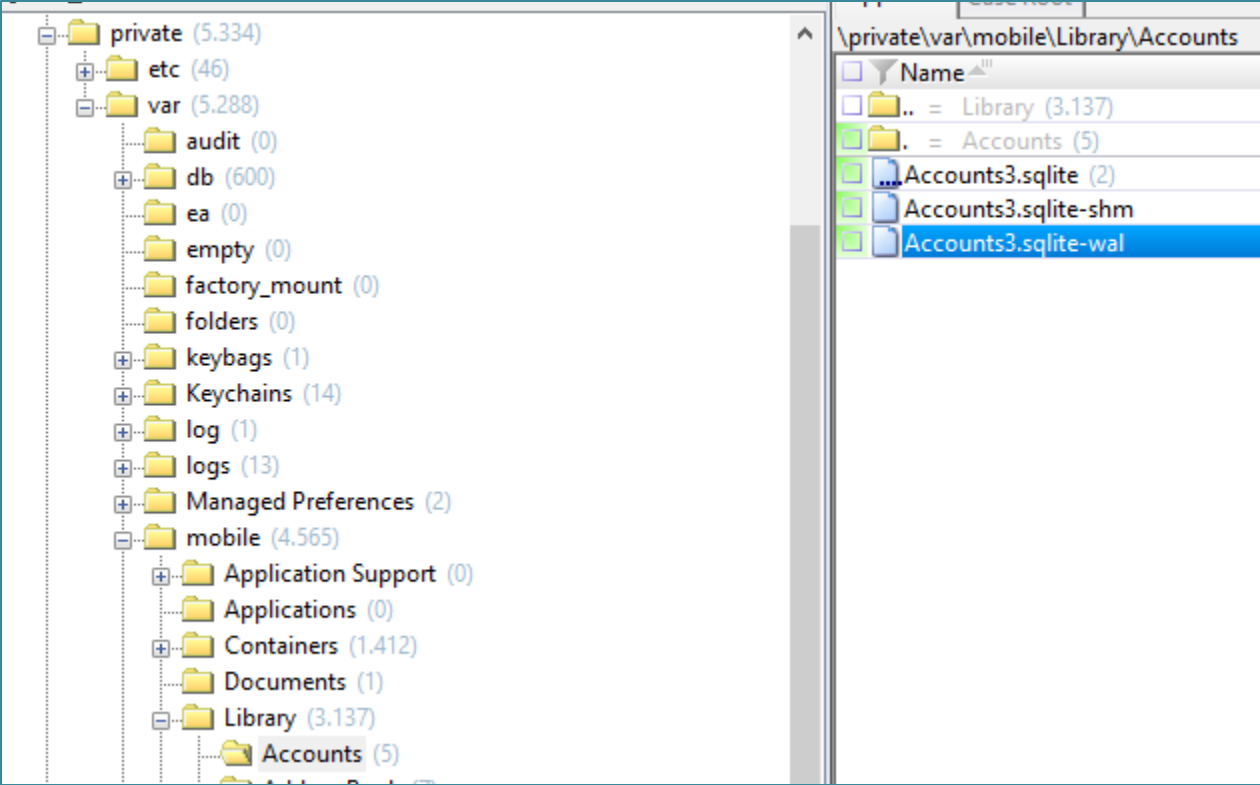
KEYBOARD DICTIONARY

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



ACCOUNTS

/PRIVATE/VAR/MOBILE/LIBRARY/ACCOUNTS/



ACCOUNTS

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

```
<string>init.ess.apple.com</string>
<key>Aliases</key>
<array>
  <dict>
    <key>Alias</key>
    <string>[REDACTED]@hotmail.it</string>
    <key>Status</key>
    <integer>3</integer>
  </dict>
  <dict>
    <key>Alias</key>
    <string>+393[REDACTED]</string>
    <key>Status</key>
    <integer>3</integer>
  </dict>
</array>
<key>UserDisabled</key>
<false/>
<key>AuthID</key>
<string>D:[REDACTED]https://t.me/learningnets</string>
<key>HasEverRegistered</key>
```

ICLOUD “SYNCED PREFERENCES”

`/var/mobile/Library/SyncedPreferences/`

Wi-Fi Access Points

- `com.apple.wifid.plist`

Weather Cities

- `com.apple.nanoweatherprefs.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	
⊕ Inerhole 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

Network Search

General Search | Network Detail

Set coordinates by address...

Address:
1060 W Addison St, Chicago, IL 60613, USA

Update Search Parameters

Network Location

Map showing location near Munich, Germany. Locations include Aichach, Moosburg an der Isar, Frisinga, Erding, Dachau, Garching bei München, Fürstenfeldbruck, Germering, Poing, Unterhaching, Starnberg, Wolfratshausen, Bad Aibling, and Weilheim in Oberbayern.

Map data ©2017 GeoBasis-DE/BKG (©2009), Google

Click for interactive map

Showing records 1 to 1

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS
map	24-65:11:5B:32:F2	Littys Hotel		infra	2012-08-01T00:00:00			48.13635635	11.5599966	1	0	7

<https://t.me/learningnets>

WEATHER CITIES

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

Key	Type	Value
Root	dict	
initialsync	integer	1
journal	dict	
changeCount	integer	4
versionid	string	FT=-@RU=a7a8aff4-f9c
values	dict	
CloudCities	dict	
CloudCities_v2.0	dict	
value	array	
dict	dict	
CityName	string	Genova
Latitude	real	44.419998
Longitude	real	8.910000
dict	dict	
CityName	string	Santa Marina Salina
Latitude	real	38.560001
Longitude	real	14.870000
dict	dict	
CityName	string	Milan
Latitude	real	45.479999
Longitude	real	9.180000
dict	dict	
CityName	string	Rome
Latitude	real	41.900001
Longitude	real	12.500000
dict	dict	
CityName	string	Florence
Latitude	real	43.779999
Longitude	real	11.240000

HEADBOARD

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

Top Movies



Movies



HEADBOARD

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

20 days ago 15 files, 0 dir.

Name	Type	Size	Created	Modified	Record changed	Attr.	1st sector	Analysis	Report tab	Comments
.. = com.apple.TVIconsCache (24)		615 KB	16/09/2017 00:58:51	16/09/2017 00:58:54						
. = com.apple.HeadBoard (15)		414 KB	16/09/2017 00:58:51	16/09/2017 00:58:54						
com.apple.TVAppStore-807e3f153a556677f83d52843faea394-466673089.000000	png	9,4 KB	16/09/2017 00:58:51	23/04/2016 22:28:42		A		0% skin tones		
com.apple.TVHomeSharing-79deb4302c018c2a107cd71321df236b-466673089.00...	png	4,7 KB	16/09/2017 00:58:51	23/04/2016 22:28:42		A		86% skin tones		
com.apple.TVMovies-4dac223be956ac2af54d07be5ee5f1a9-466673089.000000	png	36,0 KB	16/09/2017 00:58:52	23/04/2016 22:28:42		A		0% skin tones		
com.apple.TVMusic-b86bc26da1097a99cc32e781d32cd77c-466673089.000000	png	34,5 KB	16/09/2017 00:58:52	23/04/2016 22:28:42		A		0% skin tones		
com.apple.TVPhotos-7ef0d7864eac625c8df7fea1d49b328c-466673089.000000	png	17,7 KB	16/09/2017 00:58:52	23/04/2016 22:28:42		A		6% skin tones		
com.apple.TVSearch-e928b15a2846d3c1d474e2cf6c4c4e04-466673088.000000	png	8,2 KB	16/09/2017 00:58:52	23/04/2016 22:28:42		A		0% skin tones		
com.apple.TVSettings-215061a70f98604c137126165114be1b-466673089.000000	png	25,4 KB	16/09/2017 00:58:52	23/04/2016 22:28:42		A		0% skin tones		
com.apple.TVShows-26ba7eebca2f73339f1fb079bd22e5ff-466673089.000000	png	40,5 KB	16/09/2017 00:58:52	23/04/2016 22:28:42		A		0% skin tones		
com.dfir.atvjb2-0654818b24c33b62b2b072d13c91bc21-483139056.000000	png	27,7 KB	16/09/2017 00:58:52	23/04/2016 23:17:38		A		2% skin tones		
com.netflix.Netflix-ae559914bb1912743ccf81463185872c-493866956.000000	png	19,4 KB	16/09/2017 00:58:53	26/08/2016 03:15:58		A		4% skin tones		
com.foodnetwork.tveverywhere-3d639b8d3f1cbb4e48fed6c35bad18ed-4938669...	png	25,5 KB	16/09/2017 00:58:53	26/08/2016 03:16:00		A		10% skin tones		
com.google.ios.youtube-59bf59acbda7ebb17c95600445528ed8-521060847.000000	png	9,9 KB	16/09/2017 00:58:53	06/07/2017 21:14:27		A		4% skin tones		
it.rainet.ipad.raitv-99075012feb9584e4e067f0f0d324da0-521060763.000000	png	13,5 KB	16/09/2017 00:58:54	06/07/2017 21:14:27		A		0% skin tones		
com.ookla.speedtest-9f37feb7a82ad74c992355412c103832-521061471.000000	png	40,4 KB	16/09/2017 00:58:54	06/07/2017 21:19:46		A		0% skin tones		
com.ibm.wim09-92a7312951659c1056cebb01d1385ddb-521061947.000000	png	101 KB	16/09/2017 00:58:53	06/07/2017 21:26:50		A		0% skin tones		

Selected: 1 file (9,4 KB)

HEADBOARD

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

\private\var\mobile\Library\Caches\com.apple.HeadBoard\fsCachedData 20 days ago

Name	Type	Size	Created	Modified
.. = com.apple.HeadBoard (323)		58,0 MB	06/07/2017 22:30:18	06/07/2017 22:30:53
. = fsCachedData (89)		7,0 MB	06/07/2017 22:30:53	06/07/2017 22:31:01
2DD01A91-A5BA-4209-8C0F-9FE82703F505	jpg	59,1 KB	06/07/2017 22:30:54	23/04/2016 22:32:24
6A0A9077-AA8B-454C-A3CF-6F953F29214B	jpg	114 KB	06/07/2017 22:30:56	23/04/2016 22:38:28
8B748007-D9F8-452E-8809-1FDD53CDE00E	jpg	155 KB	06/07/2017 22:30:58	23/04/2016 22:38:28
962E8988-326C-4CA2-B0B3-288C8D7CC20B	jpg	107 KB	06/07/2017 22:30:58	23/04/2016 22:38:28
4052EF61-5A98-4BA6-8950-73B9BB01B39C	jpg	89,1 KB	06/07/2017 22:30:56	23/04/2016 22:38:42
067F07FC-C2D3-4E81-82B4-6C40C24F6D52	jpg	80,3 KB	06/07/2017 22:30:54	23/04/2016 22:39:21
2573308A-B4B0-4725-8692-8D8738035F04	jpg	68,8 KB	06/07/2017 22:30:54	23/04/2016 22:39:21
385CC2BE-3E46-44A1-80F0-B7B6F9AE4EC0	jpg	46,8 KB	06/07/2017 22:30:54	23/04/2016 22:39:21
3E5FCC21-7EDB-4D78-8E77-B5C6E74D4557	jpg	65,8 KB	06/07/2017 22:30:56	23/04/2016 22:39:21
45AA2400-175C-404B-84C0-BB231C979124	jpg	76,1 KB	06/07/2017 22:30:56	23/04/2016 22:39:21
7278807F-D0E6-4F0B-98A1-047395E2EA51	jpg	87,2 KB	06/07/2017 22:30:57	23/04/2016 22:39:21
837095B1-517C-489A-999C-882116E3BD2F	jpg	31,8 KB	06/07/2017 22:30:58	23/04/2016 22:39:21
97AE9065-D5B4-4677-BB6F-0132247F8AAB	jpg	33,7 KB	06/07/2017 22:30:58	23/04/2016 22:39:21
A82E17F2-34C6-4BE8-BDE1-B40CF7D37763	jpg	47,8 KB	06/07/2017 22:30:58	23/04/2016 22:39:21
AC6935F8-409B-432F-86FE-8468A6ADEDD7	jpg	92,1 KB	06/07/2017 22:30:58	23/04/2016 22:39:21

Volume File Preview Details Gallery Calendar Legend Sync

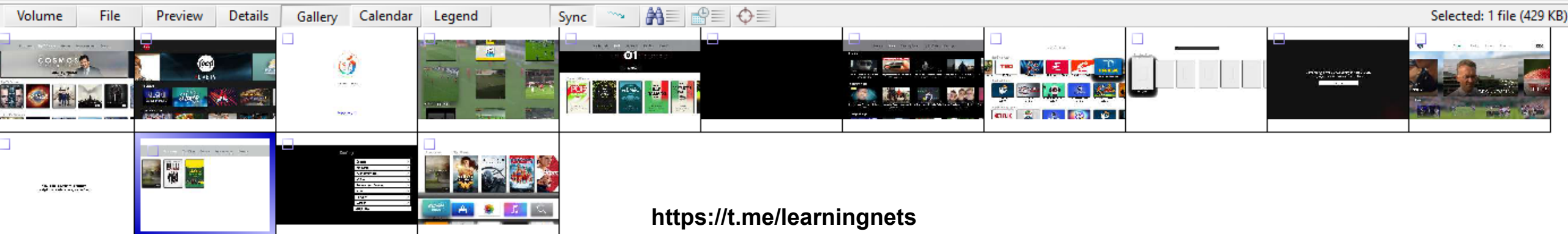
https://t.me/learningnets

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?	



HEADBOARD SNAPSHOTS

Purchased



Top Films



Movies



<https://t.me/learningnets>



TVMOVIES SNAPSHOTS

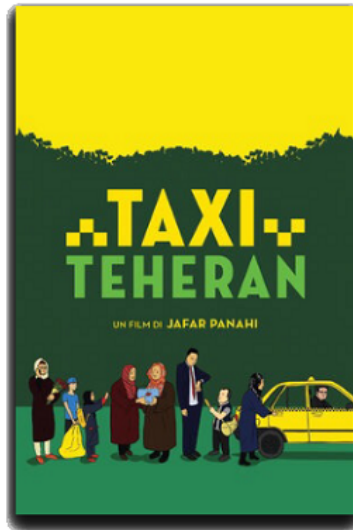
Purchased

Top Films

Genres

Recommended

Search



CACHED VIDEO

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

20 days ago

Name	Type	Category	Size	Created	Modified
AppleTV (2)			130 MB	06/07/2017 22:29:07	06/07/2017 22:29:07
Video (2)			130 MB	06/07/2017 22:29:07	06/07/2017 22:30:07
diskcacherepository.plist	plist	Mac OS X/iOS System	0,7 KB	06/07/2017 22:30:07	06/07/2017 21:05:51
CachedMedia-9NyIVW		Other/unknown type	130 MB	06/07/2017 22:29:07	06/07/2017 22:37:30

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Expires</key>
  <date>2016-11-16T21:46:05Z</date>
  <key>Last-Modified</key>
  <string>Sun, 22 Nov 2015 12:54:35 GMT</string>
  <key>MIME Type</key>
  <string>video/x-m4v</string>
  <key>Size</key>
  <integer>1622244762</integer>
  <key>URL</key>
  <string>http://video.itunes.apple.com/apple-assets-us-std-000001/Video4/v4/76/33/80/7633808c-dfca-67dd-3450-
cf82ce0dbecf/mzvf_857698767457116960.720w.h264lc.D2.f.m4v?accessKey=1476935164_6329398811186769327_Bjzdtqo8eMD7JYhC%2BE1yBzIF5w8qCN99KtS
RkiTI%2BZ9GyMqzHW6JHNZvtHhOEGSabywyOmyZCVWkWzPiWT3RfArt7C9F81%2BAN%2FaYpPbktcDZDyITJfNm8zC8XQR1vF4QR4ZruZlgFW2SXdPoMv1iot
  <key>Version</key>
  <integer>1</integer>
  <key>must-validate</key>
  <false/>
  <key>no-cache</key>
  <false/>
</dict>
</plist>
  
```

<https://t.me/learningnets>

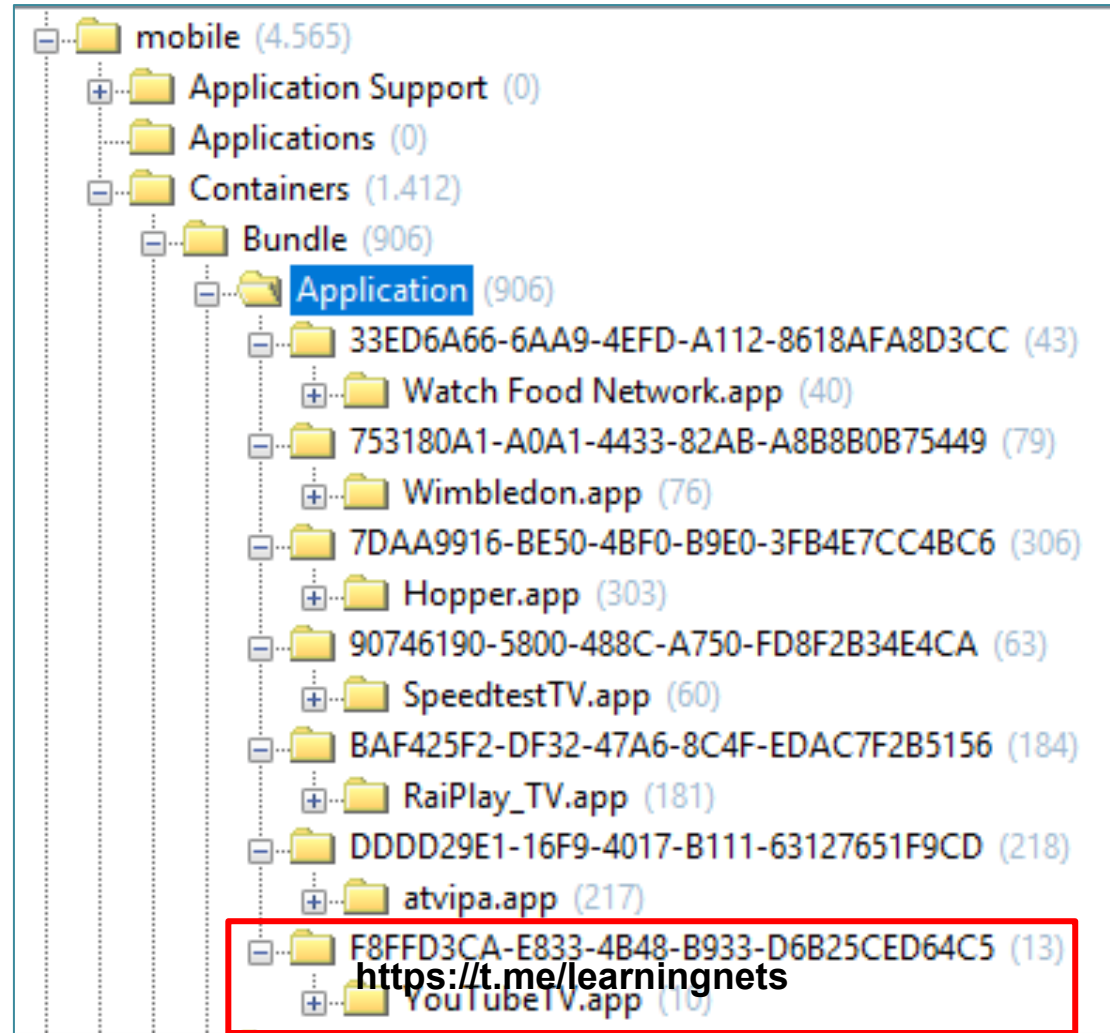
INSTALLED APPLICATIONS

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

The image shows a file explorer on the left with the path `/private/var/db/lspd` selected. The file `com.apple.lsdidentifiers.plist` is highlighted. An arrow points from this file to a plist editor window on the right. The editor shows the XML view of the plist, with a red box highlighting the entry for Google, Inc. The entry details are as follows:

Key	Type	Value
Root	dict	
LSVendors	dict	
RAI - Radio Televisione Italiana S.p.A.	dict	
LSVendorIdentifier	string	C7836D00-43CC-4D36-AFED-1029190EF006
LSApplications	array	
BundleID:com.dfir	dict	
Rai Net	dict	
Television Food Network G.P.	dict	
BundleID:com.apple	dict	
Google, Inc.	dict	
LSVendorIdentifier	string	C2121CBA-1F21-493D-800D-1469993450D7
LSApplications	array	
	string	com.google.ios.youtube
The All England Lawn Tennis Club	dict	
Ookla	dict	
LSVendorIdentifier	string	996DCF1C-13B6-4F56-83FC-6D269C2FF585
LSApplications	array	
	string	com.ookla.speedtest
Netflix, Inc.	dict	
LSAdvertiserIdentifier	string	94B09305-CBEA-45CD-B5C4-881F4120908C

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



INSTALLED APPLICATIONS YOUTUBE

The image shows a file explorer window displaying the contents of a `preferences.plist` file. The file is located within the `com.google.ios.youtube` application directory. The XML content of the file is as follows:

```
<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-4739-9cle-28e8943870cb&amp;firststac
</dict>
```

The `last-activity` key is highlighted with a red box, and its value `1499368107949.000000` is also highlighted. A `DCode` utility window is overlaid on the right side of the image. The window title is `DCode v4.02a (Build: 9306)`. The main text reads `DCODE Convert Data to Date / Time Values`. The window contains the following fields and controls:

- `Add Bias:` `UTC 00:00` (dropdown menu) `Window on top`
- `Decode Format:` `Unix: Numeric Value` (dropdown menu)
- `Example:` `1170245478` (text input)
- `Value to Decode:` `1499368107949` (text input)
- `Date & Time:` `gio, 06 luglio 2017 19:08:27 UTC` (text input)
- Buttons: `Cancel`, `Clear`, `Decode`
- Footer: `www.digital-detective.co.uk`

APP SNAPSHOTS YOUTUBE

Search

Home

Subscriptions

My YouTube

Settings

Trending



vevo

5:38

ZAYN - Dusk Till Dawn ft. Sia
20,052,271 views



GUARDATE COSA FA!!

4:44

5 regali pazzeschi su Amazon a
200,406 views



vevo

3:49

Tiziano Ferro - Valore Assoluto
386,508 views



5:13

CLEMENTINO - UN GIORNO ALL
573,175 views



PIO

Recommended



film d azione

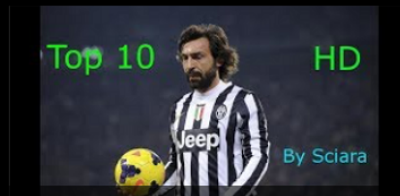
1:24:00

Film Dazione Completi In Italiano
182,338 views



5:06

10 Razze Di Cani Sconosciute Pi
1,924,676 views



Top 10

HD

By Sciarà

8:21

Le 10 Punizioni Più Belle Della St
778,050 views



CH3

7:34

Pio e Amedeo a casa di PAULO
2,357,715 views

IN

- mobile (4.565)
 - Application Support (0)
 - Applications (0)
 - Containers (1.412)
 - Bundle (906)
 - Data (504)
 - Application (475)
 - 0C18EFA3-7B47-4344-B275-B10F9307DE92 (114)
 - 2A249D58-52DA-41CE-B316-BF25A14E781D (2)
 - 9DFAA492-BCE5-40C8-B87C-9DB927FA2BCE (1)
 - C21C792C-B01A-487A-9C1B-6348013B6F3D (1)
 - D1031C05-D6D8-4936-BC55-F084B926E925 (85)
 - E3E6C13F-1DD1-419C-B05F-3A6474F15C4A (67)
 - F77BBEE9-5126-4BD6-AB2C-3838388C9EC8 (30)
 - FEBC3691-B758-495F-9D64-6260F16CD1C1 (175)**
 - Documents (0)
 - Library (173)
 - Caches (171)
 - com.apple.iTunesStore (1)
 - 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)

<input type="checkbox"/>	https__i.ytimg.com_vi_CevxZvSjLk8_mqdefault.jpg_438x247_o	jpg	20,1 KB	06/07/2017 22:28:44	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_E0Xz3UMf1zk_mqdefault.jpg_438x247_o	jpg	26,3 KB	06/07/2017 22:28:44	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_sDGJRVwHGtK_mqdefault.jpg_438x247_o	jpg	22,7 KB	06/07/2017 22:28:49	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_1G4isv_Fylg_mqdefault.jpg_438x247_o	jpg	17,6 KB	06/07/2017 22:28:42	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_o99rV03Vp0Q_mqdefault.jpg_438x247_o	jpg	21,4 KB	06/07/2017 22:28:49	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_2KUANQyexF0_mqdefault.jpg_438x247_o	jpg	31,8 KB	06/07/2017 22:28:42	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_nfWlot6h_JM_mqdefault.jpg_438x247_o	jpg	20,4 KB	06/07/2017 22:28:48	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_H0fhlwTYsj8_mqdefault.jpg_438x247_o	jpg	22,0 KB	06/07/2017 22:28:45	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_MtU0lrlGSAE_mqdefault.jpg_438x247_o	jpg	21,2 KB	06/07/2017 22:28:46	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_5Z7hOjrUrnw_mqdefault.jpg_438x247_o	jpg	16,8 KB	06/07/2017 22:28:43	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_XNl0xeGLdoM_mqdefault.jpg_438x247_o	jpg	21,0 KB	06/07/2017 22:28:47	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_QtXby3twMml_mqdefault.jpg_438x247_o	jpg	28,9 KB	06/07/2017 22:28:46	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_Ro_S6M9Mqml_mqdefault.jpg_438x247_o	jpg	16,9 KB	06/07/2017 22:28:46	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_6WNzcc66ap-g_mqdefault.jpg_438x247_o	jpg	24,1 KB	06/07/2017 22:28:43	06/07/2017 21:13:26
<input type="checkbox"/>	https__i.ytimg.com_vi_K00loUF4wjE_mqdefault.jpg_438x247_o	jpg	15,5 KB	06/07/2017 22:28:45	06/07/2017 21:13:26

Volume File Preview Details Gallery Calendar Legend Sync

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 jailbreaking is applicable (type and OS version)
 1. **Jailbreak and acquire the whole file system**
<https://t.me/learningnets>

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/>
<https://t.me/learningnets>

THANKS!

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

Q&A?

Mattia Epifani

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

 mattia.epifani@realitynet.it

 [@mattiaep](https://twitter.com/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://twitter.com/KlodiaMaida)

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

 <http://www.realitynet.it>

 <http://blog.digital-forensics.it>

APPLE TV – MODEL IDENTIFICATION

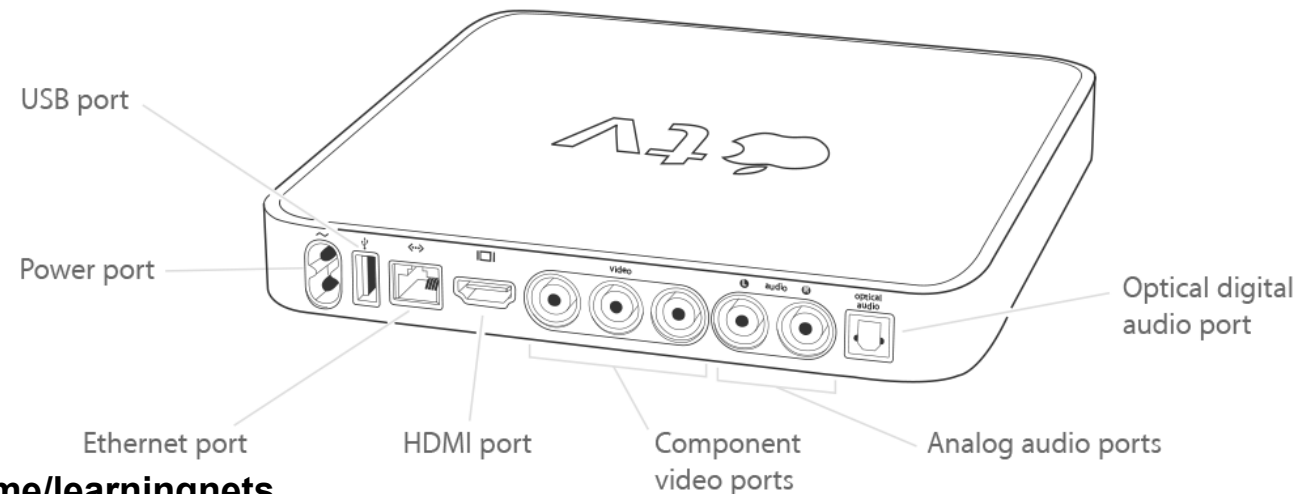
MATTIA EPIFANI – CLAUDIA MEDA

DFRWS 2018 EU

FLORENCE, 23 MARCH 2018

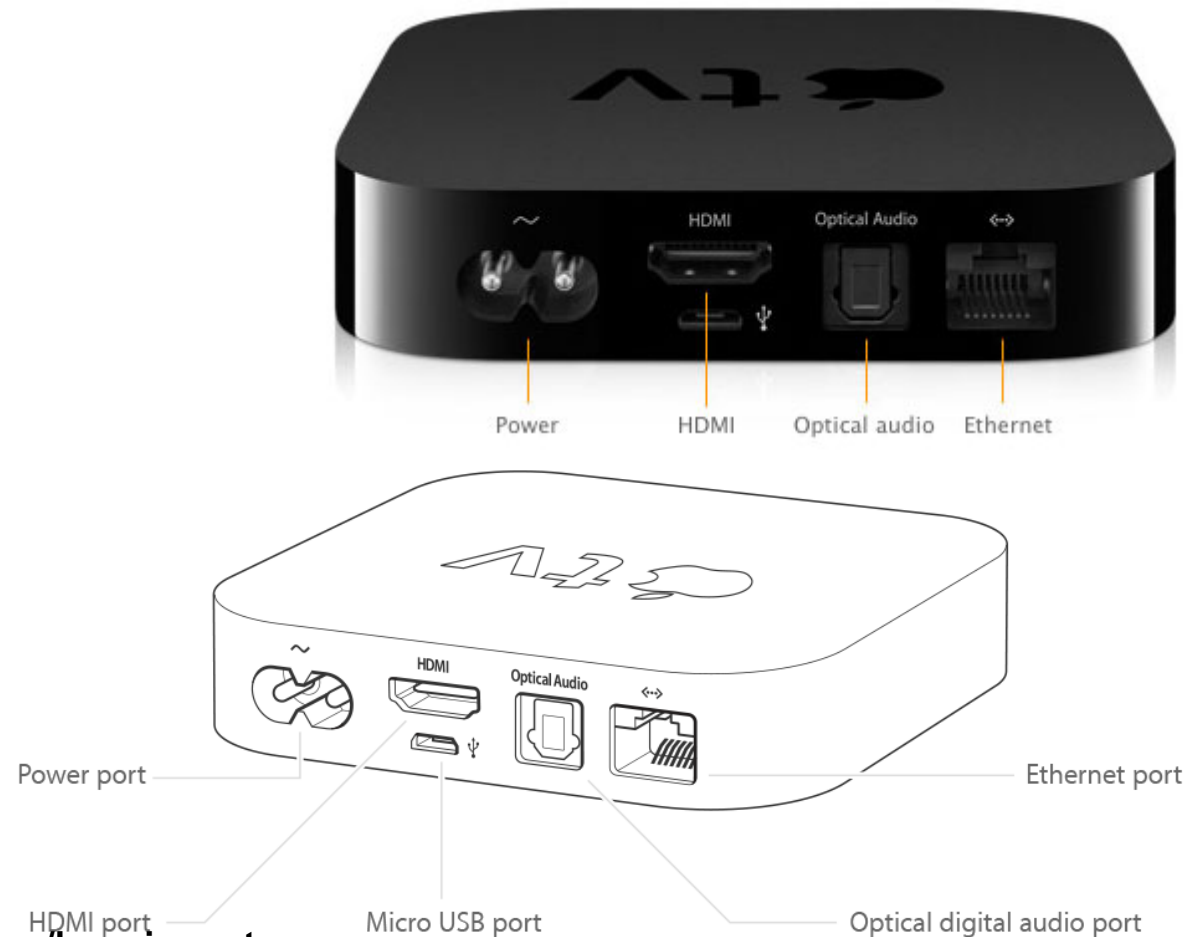
APPLE TV – 1° GENERATION

- 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



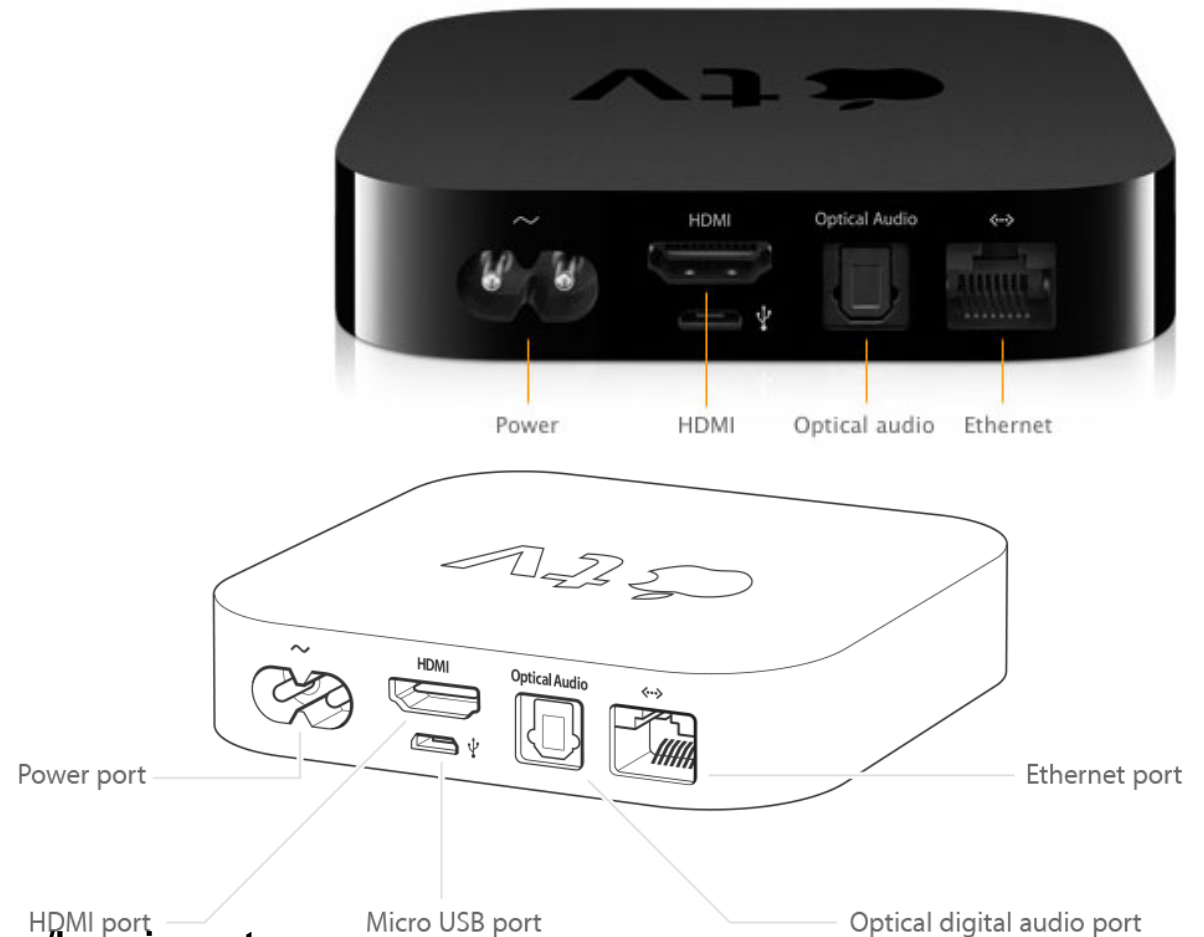
APPLE TV – II° GENERATION

- 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



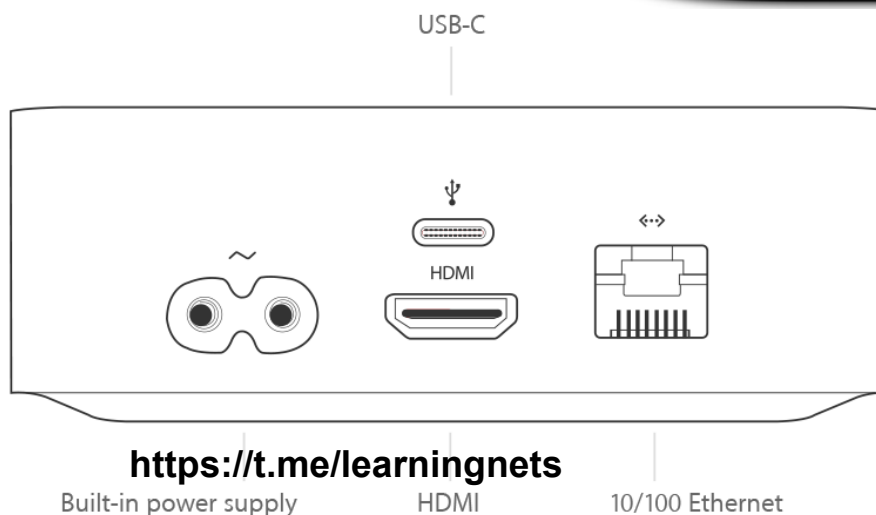
APPLE TV – III° GENERATION / III° GENERATION REV.A

- 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



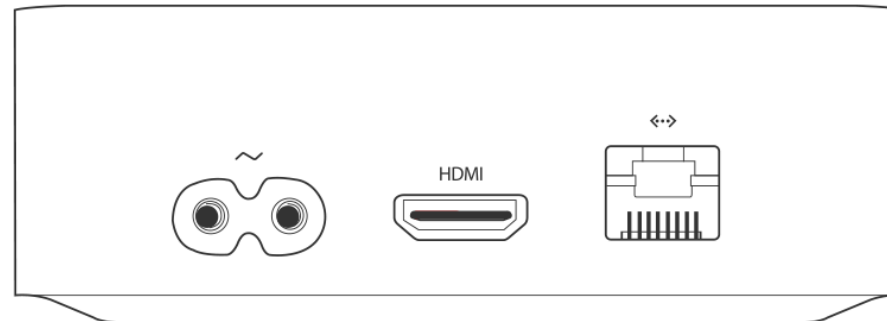
APPLE TV – IV° GENERATION

- 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



<https://t.me/learningnets>

HDMI

Gigabit Ethernet