



A FIRST LOOK TO IOS CRASH LOGS FOR FORENSIC PURPOSES

MATTIA EPIFANI

IOS CRASH LOGS

[HTTPS://DEVELOPER.APPLE.COM/LIBRARY/IOS/TECHNOTES/TN2151/_INDEX.HTML](https://developer.apple.com/library/ios/technotes/tn2151/_index.html)

- When an application crashes on an iOS device, a **crash report** is created and stored on the device
- Crash reports describe the **conditions under which the application terminated**, in most cases including a complete backtrace for each executing thread, and are typically very useful for debugging issues in the application
- For more information look at **Understanding Crash Reports on iPhone OS**
<https://developer.apple.com/videos/play/wwdc2010-317/>
- They can contain useful information from a forensic point of view!

<https://t.me/learningnets>

EXTRACTING IOS CRASH LOGS FROM DEVICE

- iOS Crash Logs can be extracted in various ways:

1. Syncing the device with iTunes (PC/Mac)

2. Using Xcode (Mac)

3. Using Third-Party tools

1. iBackup Bot

<http://www.icopybot.com/itunes-backup-manager.htm>

2. iTools

<http://itoolsen.blogspot.de/>

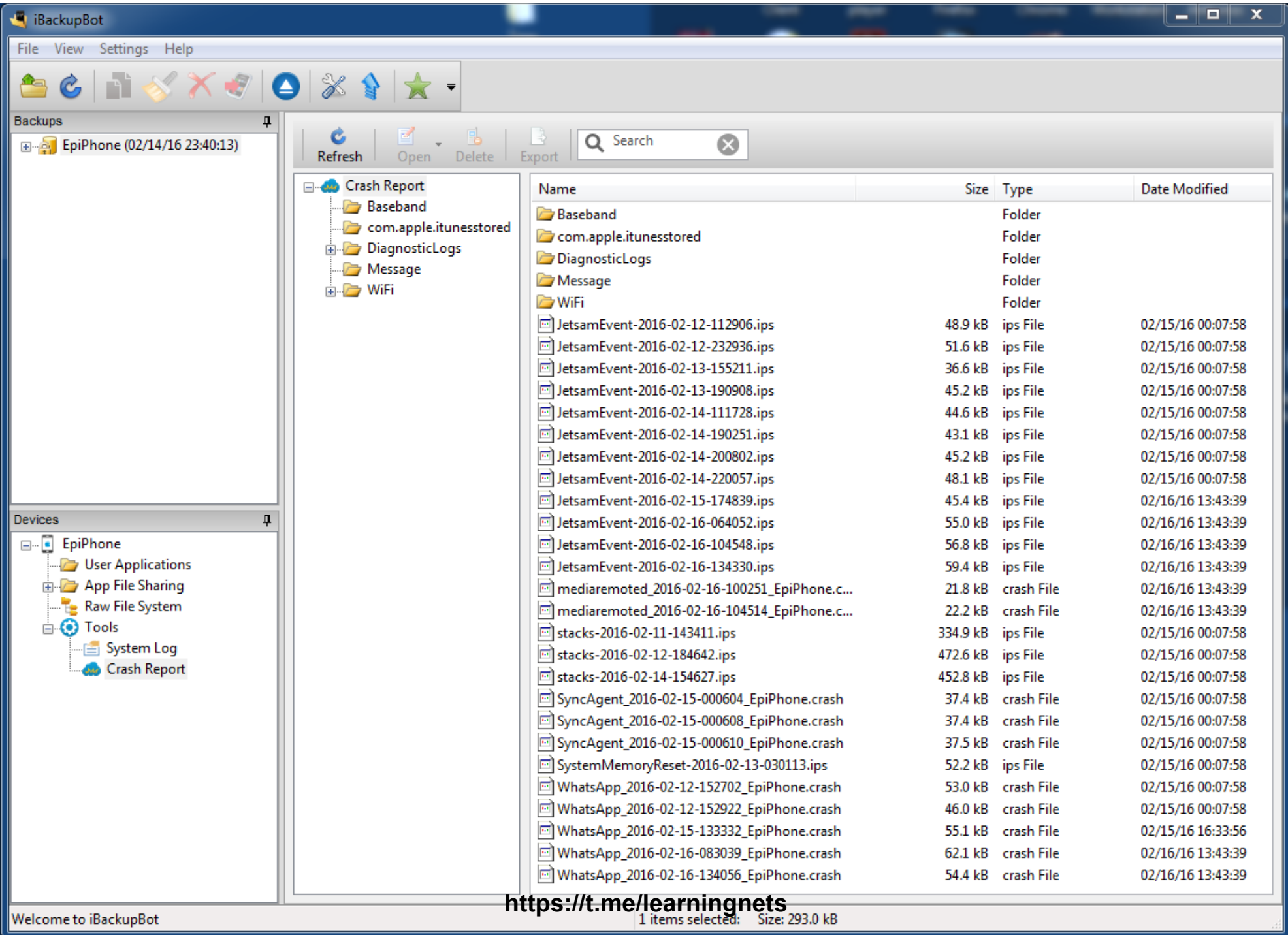
- They can be extracted from

- **Unlocked device**

- **Turned on and locked device with a valid pairing certificate**

EXTRACTING IOS CRASH LOGS WITH ITUNES

- Once Crash Logs are extracted with iTunes you can find them in the following folders, depending on the OS type/version
- **Windows 7/8/10**
C:\Users\<<USERNAME>\AppData\Roaming\Apple computer\Logs\CrashReporter\MobileDevice/<DEVICE_NAME>
- **Mac OS X**
~/Library/Logs/CrashReporter/MobileDevice/<DEVICE_NAME>
- Of course if you have a seized computer **search for these folders because they can contain previously stored Crash Logs** (same concept of an iOS Backup)
- They can be extracted **also if a backup password was set by the user**



<https://t.me/learningnets>

1 items selected: Size: 293.0 kB

RELEVANT INFORMATION FOR FORENSIC ANALYSIS

- **Installed applications list and usage**
 - Various logs like **PowerLog, Security, OnDemand**
- **iTunes username**
 - **itunesstored.2.log** file
- **File name of e-mail attachments**
 - **MobileMail** logs
- **List of WiFi network and history of latest connections**
 - **WiFi** logs

ONDEMAND LOG

```
C:\Users\Mattia\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\DiagnosticLogs\ondemandd\ondemandd_2016-02-15-163740.log

1 Feb 15 17:37:40 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 4
2 Feb 15 17:37:55 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 2
3 Feb 15 17:42:55 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 8
4 Feb 15 17:43:54 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 4
5 Feb 15 17:43:55 ondemandd[439] <Debug>: App did change state : com.apple.Preferences(457) 8
6 Feb 15 17:43:57 ondemandd[439] <Debug>: App did change state : com.apple.Preferences(457) 4
7 Feb 15 17:43:57 ondemandd[439] <Debug>: App did change state : com.apple.Preferences(457) 2
8 Feb 15 17:43:57 ondemandd[439] <Debug>: App did change state : com.apple.camera(458) 8
9 Feb 15 17:44:09 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 2
10 Feb 15 17:48:04 ondemandd[439] <Debug>: App did change state : com.apple.camera(458) 4
11 Feb 15 17:48:04 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 8
12 Feb 15 17:48:09 ondemandd[439] <Debug>: App did change state : com.apple.camera(458) 2
13 Feb 15 17:48:21 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 4
14 Feb 15 17:48:21 ondemandd[439] <Debug>: App did change state : com.apple.mobilemail(387) 8
15 Feb 15 17:48:46 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 8
16 Feb 15 17:48:47 ondemandd[439] <Debug>: App did change state : com.apple.mobilemail(387) 4
17 Feb 15 17:50:02 ondemandd[439] <Debug>: App did change state : com.apple.mobilecal(199) 4
18 Feb 15 17:50:10 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 4
19 Feb 15 17:50:10 ondemandd[439] <Debug>: App did change state : com.apple.mobilemail(387) 8
20 Feb 15 17:50:11 ondemandd[439] <Debug>: App did change state : com.apple.mobilecal(199) 2
21 Feb 15 17:51:06 ondemandd[439] <Debug>: App did change state : com.apple.mobilemail(387) 4
22 Feb 15 17:51:09 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 2
23 Feb 15 17:51:24 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 8
24 Feb 15 17:54:03 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 4
25 Feb 15 17:54:20 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 8
26 Feb 15 17:54:22 ondemandd[439] <Debug>: App did change state : net.whatsapp.WhatsApp(388) 4
27 Feb 15 17:54:22 ondemandd[439] <Debug>: App did change state : com.apple.mobilemail(387) 8
28 Feb 15 17:54:47 ondemandd[439] <Debug>: App did change state : com.apple.mobilemail(387) 4
```

<https://t.me/learningnets>

SECURITY LOG

```
C:\Users\Mattia\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\DiagnosticLogs\security.log.20160215T230034Z

1 Feb 16 00:00:34 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
2 Feb 16 00:00:34 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
3 Feb 16 00:00:34 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
4 Feb 16 00:02:07 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
5 Feb 16 00:02:07 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
6 Feb 16 00:02:07 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
7 Feb 16 00:02:25 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
8 Feb 16 00:02:25 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
9 Feb 16 00:02:25 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
10 Feb 16 00:02:33 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
11 Feb 16 00:02:33 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
12 Feb 16 00:02:33 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
13 Feb 16 00:21:30 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
14 Feb 16 00:21:30 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
15 Feb 16 00:21:30 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
16 Feb 16 00:21:46 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
17 Feb 16 00:21:46 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
18 Feb 16 00:21:46 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
19 Feb 16 00:25:41 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
20 Feb 16 00:25:41 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
21 Feb 16 00:25:41 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
22 Feb 16 00:27:39 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
23 Feb 16 00:27:39 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
24 Feb 16 00:27:39 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
25 Feb 16 00:32:18 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
26 Feb 16 00:32:18 securityd[90] <Notice> [item{}]: item SecDbItemDoUpdate replaced O,genp,E8027085,L,dku,UKFA9XBX6K.net.whatsapp.WhatsApp,5268,acct:
27 Feb 16 00:32:18 securityd[90] <Notice> [engine{}]: engine (null): will-commit api 1 changes
28 Feb 16 00:33:02 securityd[90] <Error> [SecLogging{}]: securityd_xpc_dictionary_handler WhatsApp[388] add Error Domain=NSOSStatusErrorDomain Code=-2
```

<https://t.me/learningnets>

ITUNESSTORED.2.LOG

```
C:\Users\Mattia\Desktop\iPhone Logs\Apple iPhone Logs\Apple iPhone Logs\EpiPhone\com.apple.itunesstored\itunesstored.2.log - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ?
itunesstored.2.log x
4196 2016-01-31 11:59:52.930 [114]: ISProtocolDataProvider: Saw token failure: 2002
4197 2016-01-31 11:59:52.930 [114]: ISProtocolDataProvider: Error processing protocol: Error Domain=SSErrorDomain Code=18 "Cannot connect to iTunes Store" UserInfo={NSLocali
4198 2016-01-31 11:59:52.930 [114]: ISStoreURLOperation: Attempt retry after token error: Error Domain=SSErrorDomain Code=18 "Cannot connect to iTunes Store" UserInfo={NSLoc
4199 2016-01-31 11:59:52.938 [114]: PushNotificationController: Adding APS client for itunesstored
4200 2016-01-31 11:59:52.938 [114]: AuthenticateOperation: Token is expired (type: 0)
4201 2016-01-31 11:59:52.939 [114]: PushNotificationController: Environment is now production
4202 2016-01-31 11:59:52.939 [114]: PushNotificationController: Posting 1 environment tokens
4203 2016-01-31 11:59:52.940 [114]: AuthenticateOperation: Running authenticate attempt 0
4204 2016-01-31 11:59:52.940 [114]: AuthenticateAttemptOperation: Authenticating with context: <SSAuthenticationContext: 0x13df5eff0>: (0, 1321761630, mattiaer@hotmail.it)
4205 2016-01-31 11:59:52.942 [114]: PostPushNotificationTokenOperation: Posting APS token for production
4206 2016-01-31 11:59:52.942 [114]: ISStoreURLOperation: Resolved bag entry [0-1321761630-itunesstored/1.0 iOS/9.2.1 model/iPhone8,1 hwp/s8003 build/13D15 (6; dt:141)-143450
4207 2016-01-31 11:59:52.949 [114]: ISStoreURLOperation: Making POST request, with service type: 0, for URL: https://p36-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/reg
4208 2016-01-31 11:59:52.951 [114]: ISStoreURLOperation: Sending headers for https://p36-buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/registerSuccess:
4209 {
4210     "Accept-Language" = "en-IT";
4211     "Content-Type" = "application/x-apple-plist";
4212     Cookie = "itre=1; mt-asn-1321761630=13; amp=udroRiI/w5f0QJSXEU7DXxDvGpOwd03FPNcfcGths68jwTJTBR1up2CWQAiyVUEz1dZ9g5G13GFnPXib9HgUWTmuRbYL2YpS/aqof9frawEUsrD8XNbKsnjb
4213     "User-Agent" = "itunesstored/1.0 iOS/9.2.1 model/iPhone8,1 hwp/s8003 build/13D15 (6; dt:141)";
4214     "X-Apple-ActionSignature" = "Aq43ssOfXkX8yMYWLGGLi55C+hr95wWPI8PPSP0cz+wnAAABUAMAAACNAAAAGJ7ISJpPzyxW6HY9YHV4qZs0SE555mP3FZAY+vy7nS2866MzLme2Ba6uudfZyjP9KEPAvp8OC/4
4215     "X-Apple-Client-Versions" = "GameCenter/2.0";
4216     "X-Apple-Connection-Type" = WiFi;
Normal text file length: 4194336 lines: 43602 Ln: 4204 Col: 155 Sel: 8 | 0 UNIX UTF-8 w/o BOM INS
```

MOBILEMAIL LOG

```
*C:\Users\Mattia\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\Message\MobileMail_2016_02_11_14_03_100100.log - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ?
MobileMail_2016_02_11_14_03_100100.log
1 2016-02-11 14:03:10.182|[164:0x14ed86d40]|LogOther: ERROR: MFMessageErrorDomain/Inaccessible Password - The password for "Reality" cannot be used at this time.
2 2016-02-11 15:22:21.386|[164:0x14ee0dcf0]|LogOther: ERROR: NSPOSIXErrorDomain/60 - The mail server "imap.gmail.com" is not responding. Verify that you have entered the correct account.
3 2016-02-11 22:48:51.206|[385:0x125511300]|LogAttachments: [Attachment] Failed to fetch data for attachment
4 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9648/2/Verbale_5%20febbraio%202016.docx]
5 2016-02-12 06:06:31.389|[405:0x100512d30]|LogAttachments: [Attachment] Failed to fetch data for attachment
6 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9653/1.2/od_for610_b01_01.5.docx]
7 2016-02-12 06:06:31.394|[405:0x100512d30]|LogAttachments: [Attachment] Failed to fetch data for attachment
8 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9653/1.3/2016%20SANS%20OnDemand%20Quiz%20Key%20Points%20Form.docx]
9 2016-02-12 06:06:42.825|[405:0x100512d30]|LogAttachments: [Attachment] Failed to fetch data for attachment
10 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9654/1.2/od_for610_b01_01.5.docx]
11 2016-02-12 06:35:54.598|[405:0x103965110]|LogLibraryErrors: skipping cleaning up protected tables because protected data is not available
12 2016-02-13 02:36:38.562|[405:0x100512d30]|LogAttachments: [Attachment] Failed to fetch data for attachment
13 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9763/1/mime-attachment]
14 2016-02-13 02:36:38.572|[405:0x100512d30]|LogAttachments: [Attachment] Failed to fetch data for attachment
15 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9763/2/encrypted.asc]
16 2016-02-13 17:36:33.904|[163:0x13ed04de0]|LogOther: ERROR: MFMessageErrorDomain/Socket Read - The connection to the server failed.
17 2016-02-13 20:03:05.026|[163:0x140776860]|LogLibraryErrors: skipping cleaning up protected tables because protected data is not available
18 2016-02-13 20:10:02.808|[163:0x13ed04de0]|LogAttachments: [Attachment] Failed to fetch data for attachment
19 [file:///var/mobile/Library/Mail/IMAP-mattia.epifani@realityvnet.it@imap.gmail.com/%5CInbox.imapmbbox/Attachments/9796/2/EVIDENCE.D5.1-TechnicalSpecifications-v2.0-scl_rev.CNR.docx]
20 2016-02-14 11:59:35.713|[587:0x158958dc0]|LogLibraryErrors: skipping cleaning up protected tables because protected data is not available
Find result - 22 hits
Normal text file length: 3160 lines: 24 Ln: 22 Col: 1 Sel: 0|0 UNIX UTF-8 w/o BOM OVR
```

WIFI LOG

```
*C:\Users\Mattia\AppData\Roaming\Apple Computer\Logs\CrashReporter\MobileDevice\EpiPhone\WiFi\WiFiManager\wifi-02-16-2016_074920.log - Notepad++
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ?
wifi-02-16-2016_074920.log x
2596
2597 2/16/2016 7:42:37.393 Aborting EAP
2598 2/16/2016 7:42:37.393 Aborted current auto-join session.
2599 2/16/2016 7:42:37.393 WiFiDeviceManagerSetNetworks: shouldDisassociate 0
2600 2/16/2016 7:42:37.393 __WiFiDeviceManagerAutoAssociate: Already connected to m3connect.
2601 2/16/2016 7:42:37.395 __CreateBGScanRequest Hotspot m3connect added to BGScan List
2602 2/16/2016 7:42:37.395 __CreateBGScanRequest Hotspot ibis added to BGScan List
2603 2/16/2016 7:42:37.395 __CreateBGScanRequest Hotspot San Martino Hospital Free added to BGScan List
2604 2/16/2016 7:42:37.395 __CreateBGScanRequest Hotspot Airport_Free_WiFi added to BGScan List
2605 2/16/2016 7:42:37.395 __CreateBGScanRequest Hotspot WiFi in de trein added to BGScan List
2606 2/16/2016 7:42:37.396 Preparing background scan request for
2607 "m3connect" "ibis" "lrz" "Marriott_CONFERENCE" "rnsys" "NETGEAR13" "EPIFANI_DLINK" "San Martino Hospital Free"
2608 "212genova" "Vodafone-25344705" "Telecom-45376345" "Airport_Free_WiFi" "WiFi in de trein" "Babylon Free WiFi"
2609 "Meeting Center" "Leidse Square Hotel" "60:c5:47:4f:51:1d ~ EN" "60:c5:47:4d:cd:6f ~ EN" "60:c5:47:4f:51:1c ~ EN"
2610 2/16/2016 7:42:37.403 WiFiDeviceRequestAssociatedSleep: ActiveDuringSleepRequested is already set (<CFBasicHash (
2611 entries =>
2612 }
2613 ).
2614 2/16/2016 7:42:37.415 __WiFiDeviceManagerAutoAssociate: Already connected to m3connect.
2615 2/16/2016 7:42:37.417 No Change in Background Scan Networks, Skip Re-Programming Background Scan_
2616
2617 2/16/2016 7:42:38.342 WiFiManagerCellularTransmitCallback block invoke: Cellular Transmit Started = FALSE
Find result - 22 hits
https://t.me/learningnets
```

REFERENCES

- **Understanding Crash Reports on iPhone OS**
<https://developer.apple.com/videos/play/wwdc2010-317>
- **Understanding and Analyzing iOS Application Crash Reports**
https://developer.apple.com/library/ios/technotes/tn2151/_index.html
- **Demystifying iOS Application Crash Logs**
<http://www.raywenderlich.com/23704/demystifying-ios-application-crash-logs>
- **Retrieving Crash Reports on iOS**
<https://www.chromium.org/developers/how-tos/retrieving-crash-reports-on-ios>
- **iBackup Bot**
<http://www.icopybot.com/itunes-backup-manager.htm>
- **iTools**
<http://itoolsen.blogspot.de> <https://t.me/learningnets>

Q&A?

Mattia Epifani

- Digital Forensics Analyst and Mobile Device Security Analyst
- CEO @ REALITY NET – System Solutions
- Member of CLUSIT, DFA, IISFA, ONIF, Tech and Law Center
- GREM, GCFA, GNFA, GMOB, CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

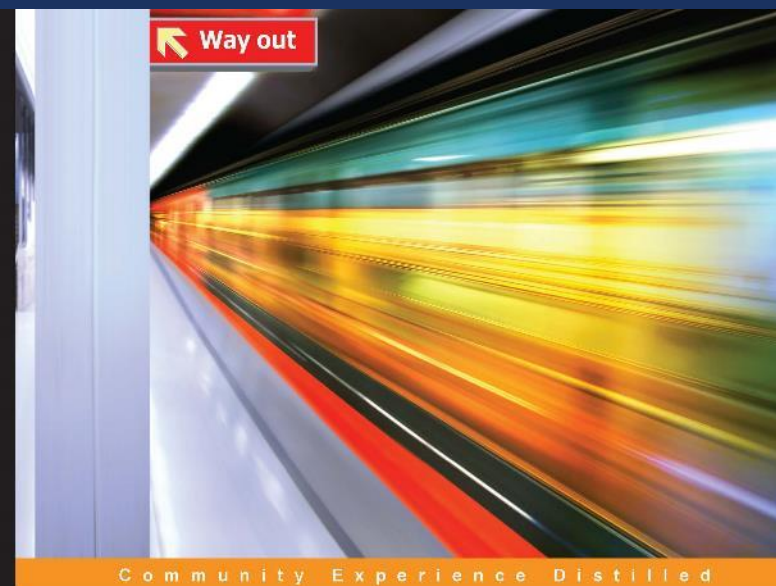
Mail mattia.epifani@realitynet.it

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

Linkedin <http://www.linkedin.com/in/mattiaepifani>

Blog <http://mattiaep.blogspot.com>

<https://t.me/learningnets>



Learning iOS Forensics

A practical hands-on guide to acquire and analyze iOS devices
with the latest forensic techniques and tools

Mattia Epifani
Pasquale Stirparo

[PACKT] open source
PUBLISHING community experience distilled