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

- 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!

EXTRACTING IOS CRASH LOGS FROM DEVICE

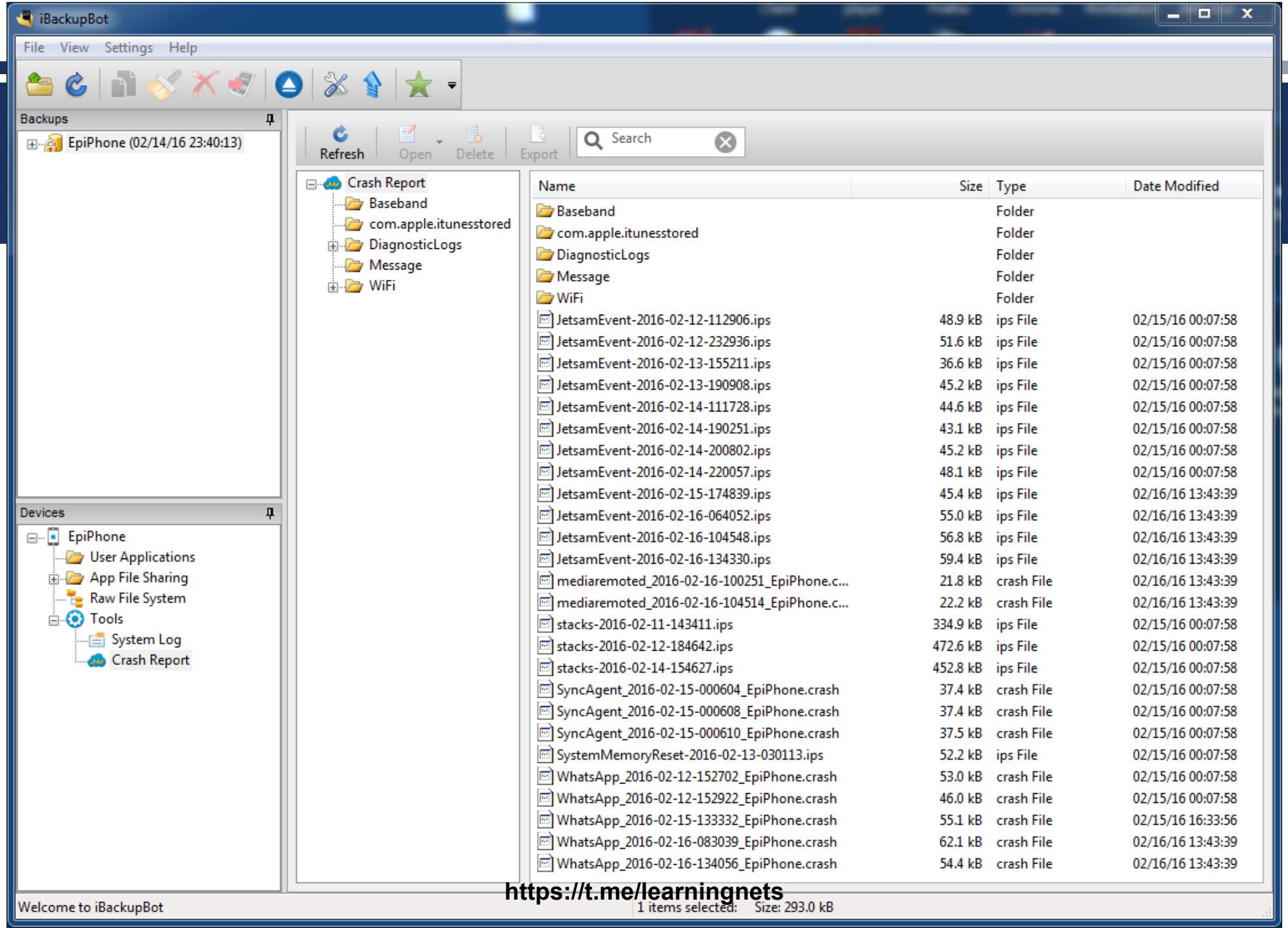
- iOS Crash Logs can be extracted in various ways:

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**



RELEVANT INFORMATION FOR FORENSIC ANALYSIS

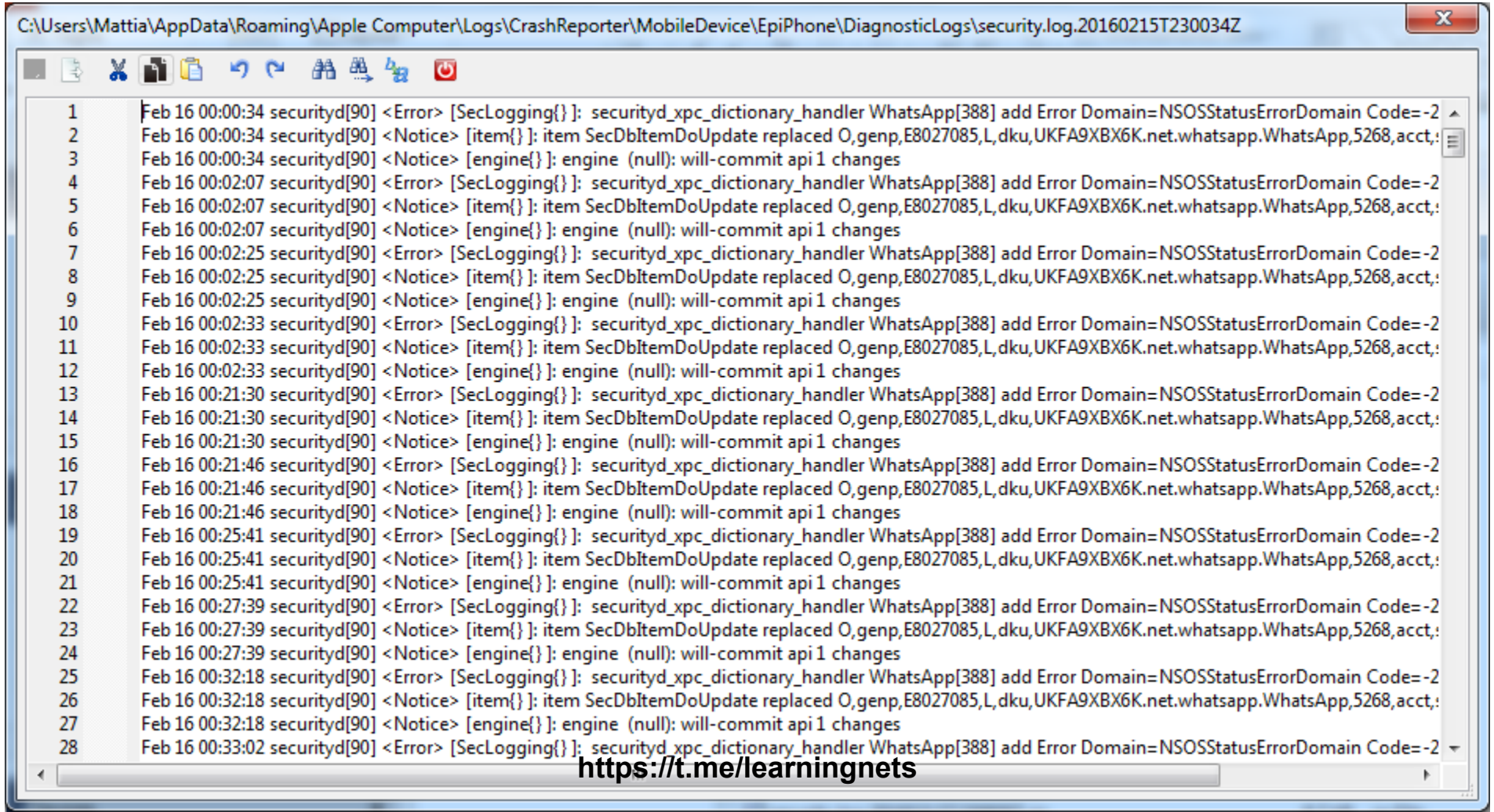
- **Installed applications list and usage**
  - Various logs like **PowerLog, Security, OnDemand**
- **iTunes username**
  - **itunesstored.2.log** file
- **File name of e-mail attachments**
  - **MobileMail** logs
- **List of WiFi network and history of latest connections**
  - **WiFi** logs

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
```

SECURITY LOG



ITUNESSTORED.2.LOG

C:\Users\Mattia\Desktop\iPhone Logs\Apple iPhone Logs\Apple iPhone Logs\EpiPhone\com.apple.itunesstored\itunesstored.2.log - Notepad++

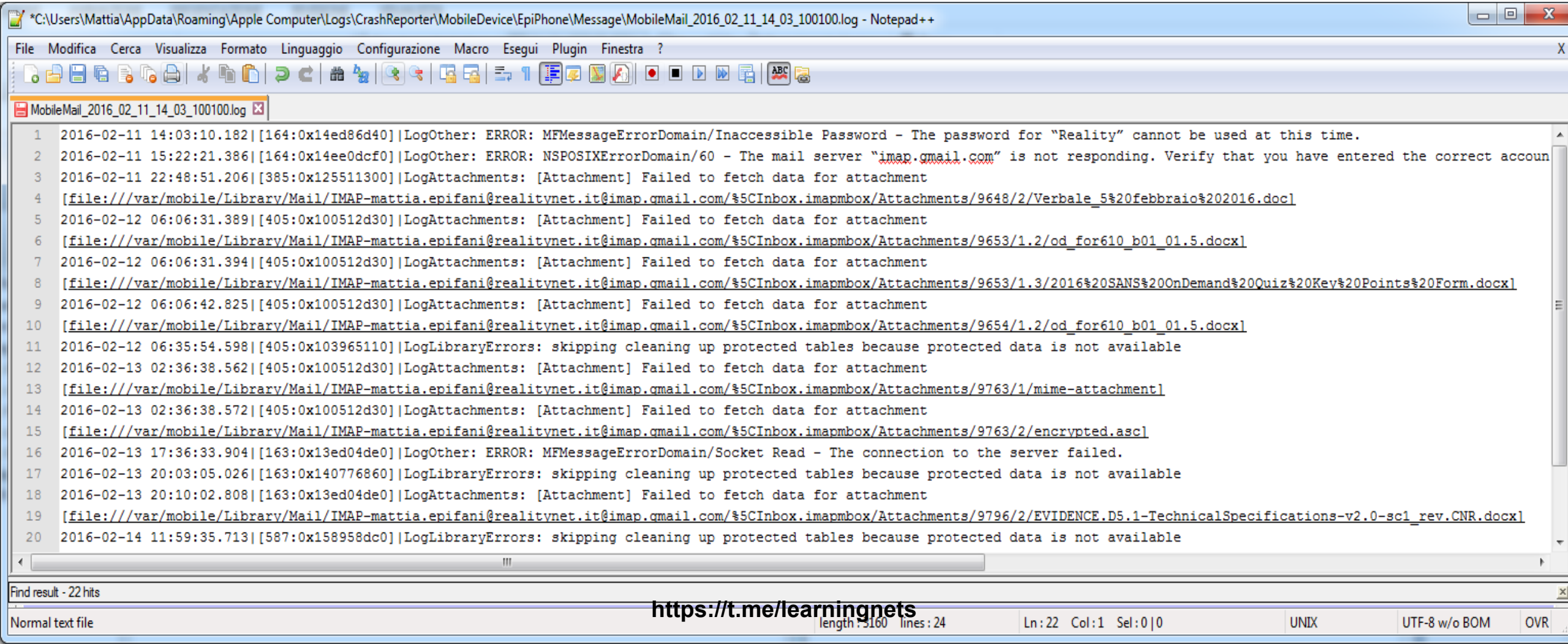
File Modifica Cerca Visualizza Formato Linguaggio Configurazione Macro Esegui Plugin Finestra ?

itunesstored.2.log

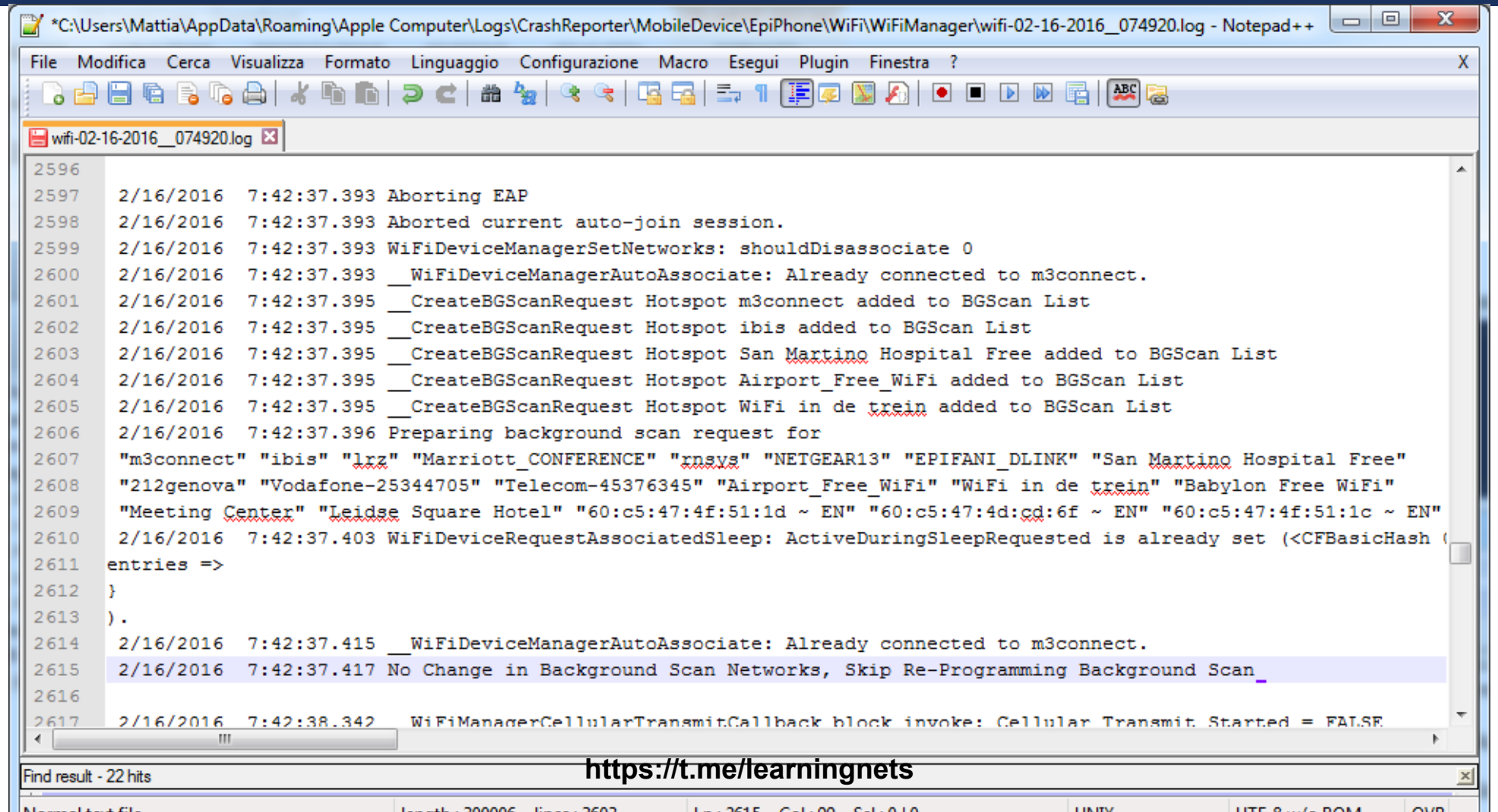
```
4196 2016-01-31 11:59:52.930 [114]: ISProtocolDataProvider: Saw token failure: 2002
4197 2016-01-31 11:59:52.930 [114]: ISProtocolDataProvider: Error processing protocol: Error Domain=SSErrorDomain Code=18 "Cannot connect to iTunes Store" UserInfo={NSLocali
4198 2016-01-31 11:59:52.930 [114]: ISStoreURLOperation: 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/req
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/w5f0QJSXEU7DXxDvGpOwdO3FPNcfcGths68jwTJTBR1up2CWQAiyVUEz1dZ9g5G13GFnPXib9HgUWTmuRbYL2YpS/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



WIFI LOG



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

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**
Linkedin	**http://www.linkedin.com/in/mattiaepifani**
Blog	**http://mattiaep.blogspot.com**