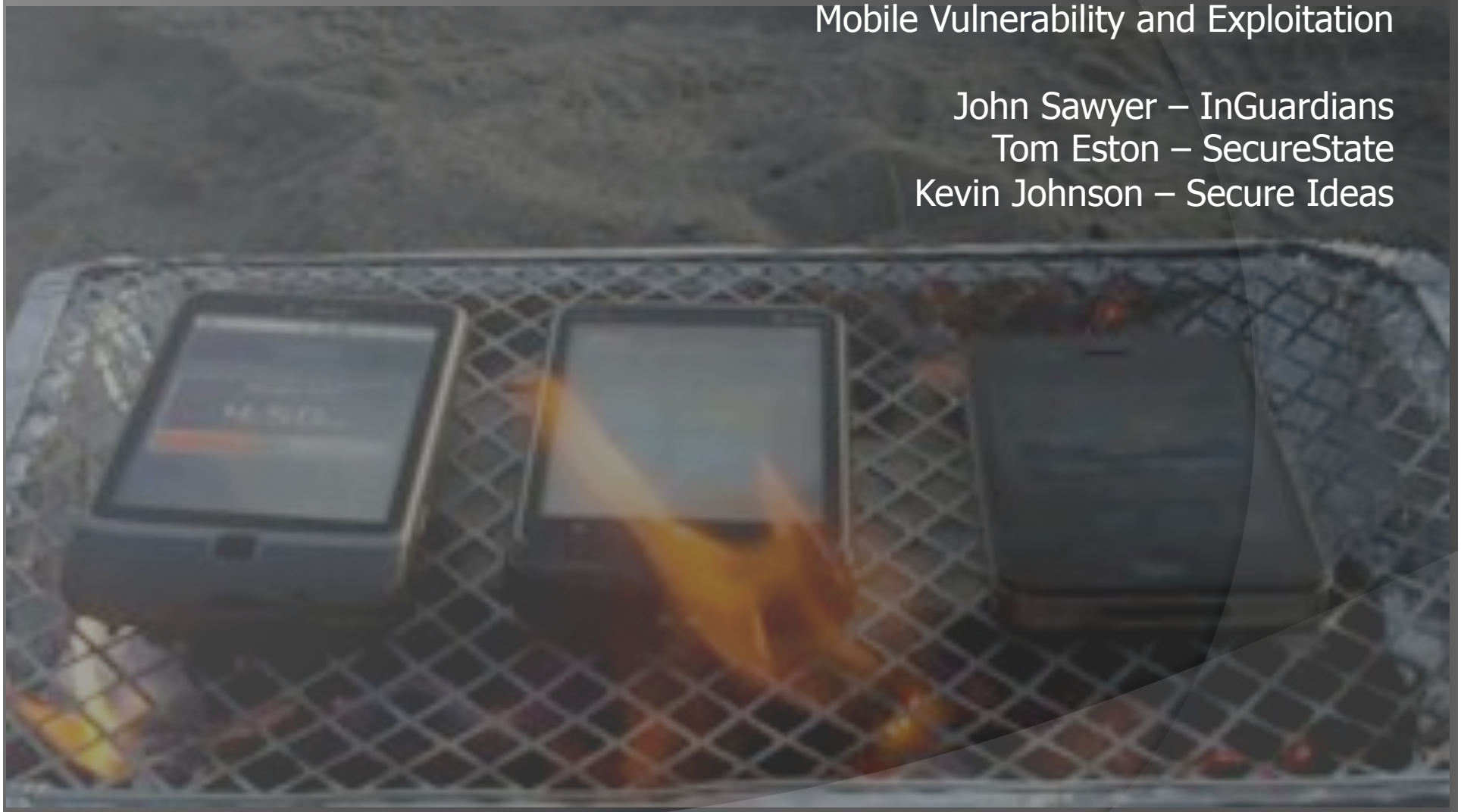
SMART BOMBS

Mobile Vulnerability and Exploitation

John Sawyer – InGuardians
Tom Eston – SecureState
Kevin Johnson – Secure Ideas



John Sawyer

- InGuardians, Inc. - Senior Security Analyst
- DarkReading.com - Author/Blogger
- 1@stplace - Retired CTF packet monkey
  - winners DEFCON 14 & 15
- Avid Mountain Biker…in Florida.

Tom Eston

- Manager, SecureState Profiling & Penetration Team
- Blogger – SpyLogic.net
- Infrequent Podcaster – Security Justice/Social Media Security
- Zombie aficionado
- I like to break new technology

Kevin Johnson

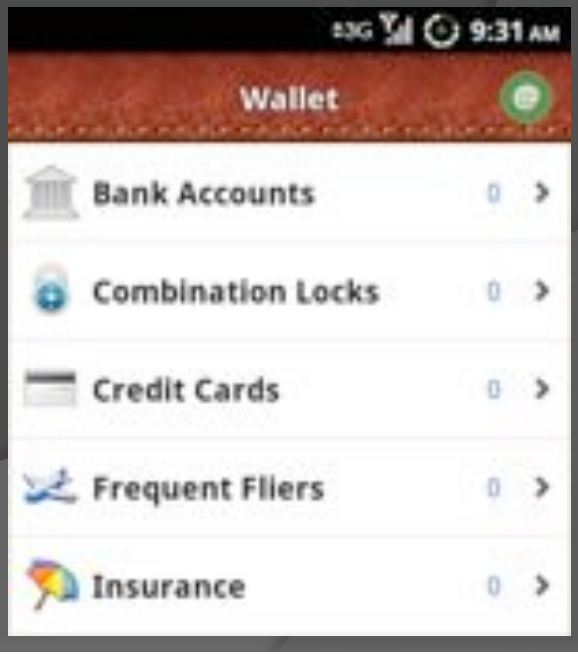
- Father of Brenna and Sarah
- Secure Ideas, Senior Security Consultant
- SANS Instructor and Author
  - SEC542/SEC642/SEC571
- Open-Source Bigot
  - SamuraiWTF, Yokoso, Laudanum
- Ninja

What are we talking about today?

- What's at risk?
- Tools, Testing and Exploitation
- Common vulnerabilities found in popular apps (this is the fun part)

What are Smart Bombs?

- We've got powerful technology in the palm of our hands!
- We store and transmit sensitive data
- Mobile devices are being used by:
  - Major Businesses (PII)
  - Energy Companies (The Grid)
  - The Government(s)
  - Hospitals (PHI)
  - Your Mom (Scary)



That's right…your Mom

Testing Mobile Apps

- What are the 3 major areas for testing?
  - **File System**
    What are apps writing to the file system? How is data stored?
  - **Application Layer**
    How are apps communicating via HTTP and Web Services? SSL?
  - **Transport Layer**
    How are apps communicating over the network? TCP and Third-party APIs

OWASP Top 10 Mobile Risks

1. Insecure Data Storage
2. Weak Server Side Controls
3. Insufficient Transport Layer Protection
4. Client Side Injection
5. Poor Authorization and Authentication

OWASP Top 10 Mobile Risks

6. Improper Session Handling
7. Security Decisions Via Untrusted Inputs
8. Side Channel Data Leakage
9. Broken Cryptography
10. Sensitive Information Disclosure

OWASP Mobile Security Project

- You should get involved!
- https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Other Issues

- Privacy of your data!
  - Mobile apps talk to many third party APIs (ads)
  - What's collected by Google/Apple/Microsoft?

Common Tools

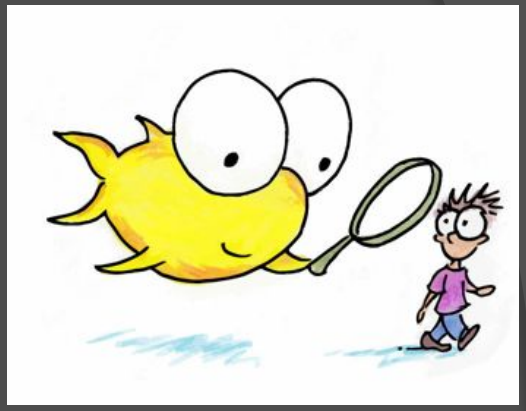
- SSH
- VNC server
- A compiler (gcc / agcc)
- Android SDK (adb!)
- XCode
- Jailbroken iDevice
- Rooted Android Device

Forensics & Incident Response

- Filesystem artifacts
- Timeline analysis
- Log analysis
- Temp files

Forensic Tools

- Mobile Forensic Tools
  - EnCase, FTK, Cellebrite
- Free and/or Open Source
  - file, strings, less, dd, md5sum
  - The Sleuthkit (mactime, mac-robber)



Timelines

- Timelines are awesome
  - Anyone know log2timeline?
- Filesystem
  - mac-robber
  - mactime
- Logs
  - Application- & OS-specific

Filesystem Timelines

- mac-robber
  - C app
  - free & open source
  - must be compiled to run on devices
- mactime
  - Part of The Sleuthkit
  - runs on Mac, Win, Linux

Compiling mac-robber

- Android
  - Install arm gcc toolchain
  - Compile & push via adb

```
sudo add-apt-repository ppa:linaro-maintainers/toolchain
sudo apt-get install gcc-arm-linux-gnueabi

arm-linux-gnueabi-gcc -static -o mac-robber mac-robber.c
```

Compiling mac-robber

- iOS (jailbroken)
  - Download & Install libgcc onto device
  - Install iphone-gcc
  - Download & Install C headers/libraries

```
curl http://iphone-gcc-full.googlecode.com/files/libgcc.deb > libgcc.deb
curl http://iphone-gcc-full.googlecode.com/files/headers-libs.deb > headers-libs.deb
dpkg -i libgcc.deb
aptitude install iphone-gcc
dpkg -i --force-overwrite headers-libs.deb

gcc -o mac-robber mac-robber.c
```

Running mac-robber

- iOS & Android via SSH

```
ssh root@ipad "~/mac-robber /" > iPad-AttachmentOpen.body
mactime -b iPad-AttachmentOpen.body > iPad-AttachmentOpen.tm
```

- Android via adb

```
./adb shell '/system/bin/mac-robber /' > ~/tmp/DrawFree-post.body
mactime -b ~/tmp/DrawFree-post.body > ~/tmp/DrawFree-post.tm
```

- Then, process each with mactime

Filesystem Timelines

```
Mon Mar 12 2012 18:35:48     1792 mac. -rw-------
Mon Mar 12 2012 18:35:51     2422 mac. -rw-------
Mon Mar 12 2012 18:35:54     2377 mac. -rw-------
Mon Mar 12 2012 18:35:57     2377 mac. -rw-------
Mon Mar 12 2012 18:35:59     2377 mac. -rw-------
Mon Mar 12 2012 18:36:02     2377 mac. -rw-------
```

```
Mon Mar 12 2012 18:35:48     1792 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/IMG_20120229_074128-2.jpg
Mon Mar 12 2012 18:35:51     2422 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/IMG_20120229_074432-2.jpg
Mon Mar 12 2012 18:35:54     2377 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-8.png
Mon Mar 12 2012 18:35:57     2377 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-9.png
Mon Mar 12 2012 18:35:59     2377 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-10.png
Mon Mar 12 2012 18:36:02     2377 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-11.png
Mon Mar 12 2012 18:36:05     1085 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/ole0-4.bmp
Mon Mar 12 2012 18:36:08     1085 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/ole0-5.bmp
Mon Mar 12 2012 18:36:13      334 mac. -rw------- 10041    10041    0        /data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/~WRD000-2.jpg
```

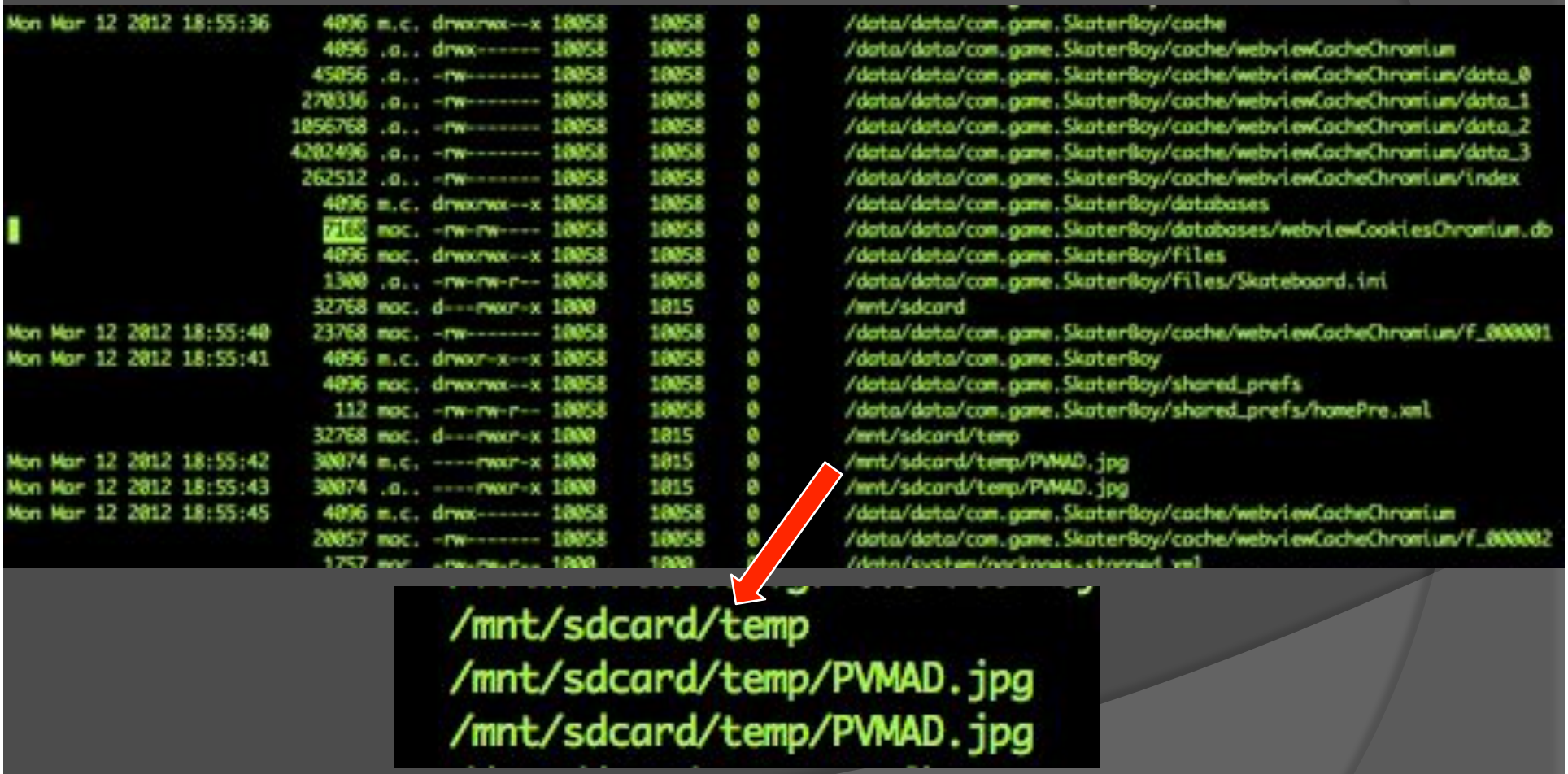
```
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-8.png
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-9.png
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-10.png
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/image001-11.png
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/ole0-4.bmp
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/ole0-5.bmp
/data/data/com.google.android.gm/cache/johnhsawyer@gmail.com/~WRD000-2.jpg
```

Where is the data?

```
Mon Mar 12 2012 23:30:47     4096 m.c. drwxrwx--x 10089    10089    0        /data/data/com.guardam.personalNotes/files
                               64 ..c. -rw------- 10089    10089    0        /data/data/com.guardam.personalNotes/files/@12.03.12-23:30
                              400 mac. -rw------- 10089    10089    0        /data/data/com.guardam.personalNotes/files/notes
                            32768 mac. d---rwxr-x 1000     1015     0        /mnt/sdcard
                              400 mac. ----rwxr-x 1000     1015     0        /mnt/sdcard/notes
```

```
localhost / # md5sum /mnt/sdcard/notes
9a69aea24b92f6a57e6e818386c0269a  /mnt/sdcard/notes
localhost / # md5sum /data/data/com.guardam.personalNotes/files/notes
9a69aea24b92f6a57e6e818386c0269a  /data/data/com.guardam.personalNotes/files/notes
```

Temp Files

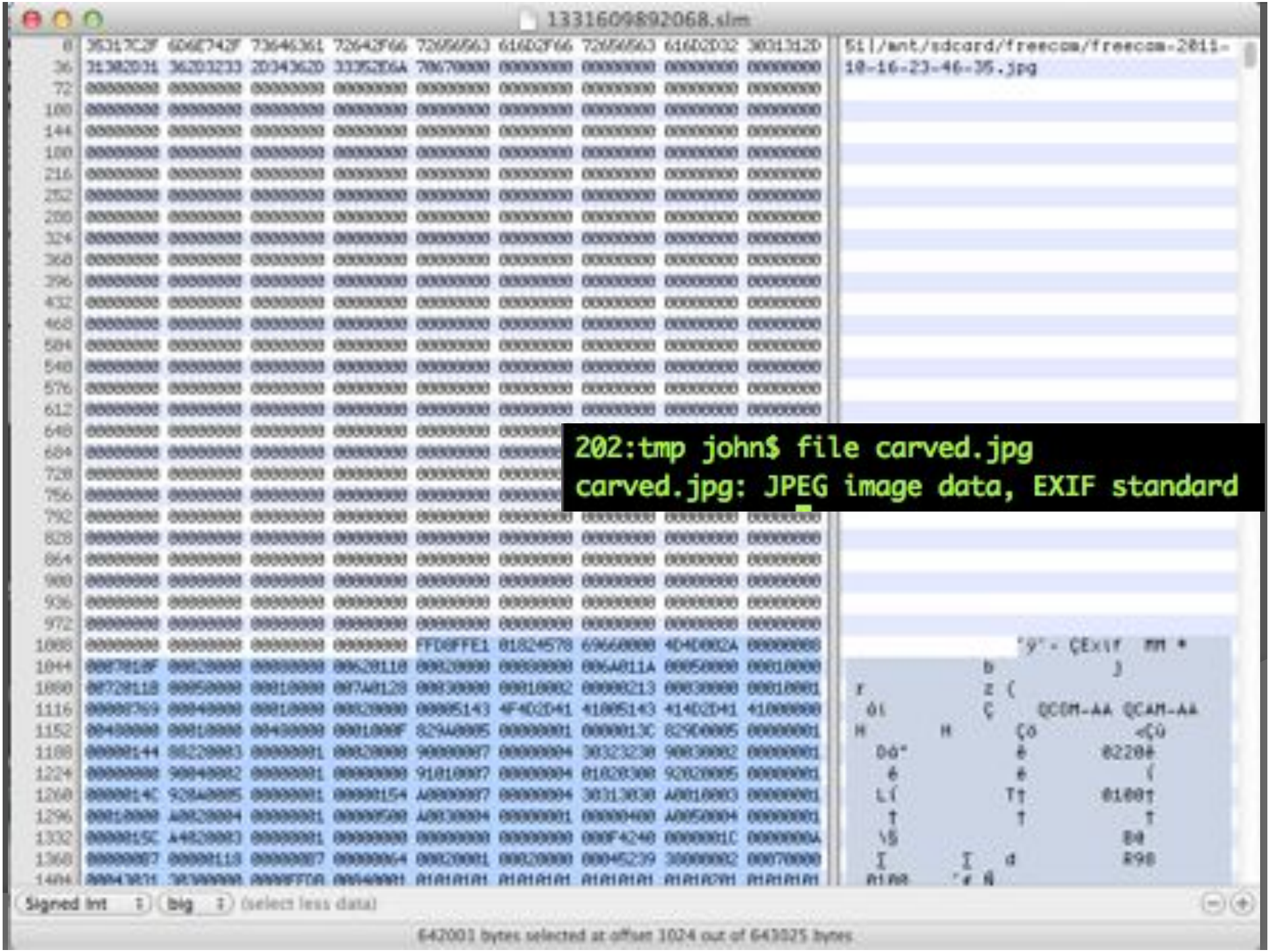

Mon Mar 12 2012 18:55:36 4096 m.c. drwxrwx--x 10058 10058 0 /data/data/com.game.SkaterBoy/cache
4096 .a.. drwx------ 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium
45056 .a.. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/data_0
270336 .a.. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/data_1
1056768 .a.. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/data_2
4202496 .a.. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/data_3
262512 .a.. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/index
4096 m.c. drwxrwx--x 10058 10058 0 /data/data/com.game.SkaterBoy/databases
7168 mac. -rw-rw---- 10058 10058 0 /data/data/com.game.SkaterBoy/databases/webviewCookiesChromium.db
4096 mac. drwxrwx--x 10058 10058 0 /data/data/com.game.SkaterBoy/files
1300 .a.. -rw-rw-r-- 10058 10058 0 /data/data/com.game.SkaterBoy/files/Skateboard.ini
32768 mac. d---rwxr-x 1000 1015 0 /mnt/sdcard
Mon Mar 12 2012 18:55:40 23768 mac. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/f_000001
Mon Mar 12 2012 18:55:41 4096 m.c. drwxr-x--x 10058 10058 0 /data/data/com.game.SkaterBoy
4096 mac. drwxrwx--x 10058 10058 0 /data/data/com.game.SkaterBoy/shared_prefs
112 mac. -rw-rw-r-- 10058 10058 0 /data/data/com.game.SkaterBoy/shared_prefs/homePre.xml
32768 mac. d---rwxr-x 1000 1015 0 /mnt/sdcard/temp
Mon Mar 12 2012 18:55:42 30074 m.c. ----rwxr-x 1000 1015 0 /mnt/sdcard/temp/PVMAD.jpg
Mon Mar 12 2012 18:55:43 30074 .a.. ----rwxr-x 1000 1015 0 /mnt/sdcard/temp/PVMAD.jpg
Mon Mar 12 2012 18:55:45 4096 m.c. drwx------ 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium
20057 mac. -rw------- 10058 10058 0 /data/data/com.game.SkaterBoy/cache/webviewCacheChromium/f_000002
/mnt/sdcard/temp
/mnt/sdcard/temp/PVMAD.jpg
/mnt/sdcard/temp/PVMAD.jpg

Gallery Lock Lite

- “Protects” your images

```
Mon Mar 12 2012 23:37:08    32768 mac. d---rwxr-x 1000     1015     0        /mnt/sdcard/.gallery_lock/media/20120312233708
                           361569 ..c. ----rwxr-x 1000     1015     0        /mnt/sdcard/.gallery_lock/media/20120312233708/1331609828596.slm
                             4307 m.c. ----rwxr-x 1000     1015     0        /mnt/sdcard/.gallery_lock/media/20120312233708/1331609828596.slt
                            32768 ma.. d---rwxr-x 1000     1015     0        /mnt/sdcard/downloads
Mon Mar 12 2012 23:37:14     4307 .a.. ----rwxr-x 1000     1015     0        /mnt/sdcard/.gallery_lock/media/20120312233708/1331609828596.slt
Mon Mar 12 2012 23:37:15   361569 .a.. ----rwxr-x 1000     1015     0        /mnt/sdcard/.gallery_lock/media/20120312233708/1331609828596.slm
```

```
202:tmp john$ file 1331609892068.*
1331609892068.slm: data
1331609892068.slt: JPEG image data, JFIF standard 1.01
202:tmp john$ strings 1331609892068.slm | head -5
51|/mnt/sdcard/freecam/freecam-2011-10-16-23-46-35.jpg
Exif
QCOM-AA
```


1331609892068.slm
202:tmp john$ file carved.jpg
carved.jpg: JPEG image data, EXIF standard
Signed Int
Big
(select less data)
642001 bytes selected at offset 1024 out of 643025 bytes

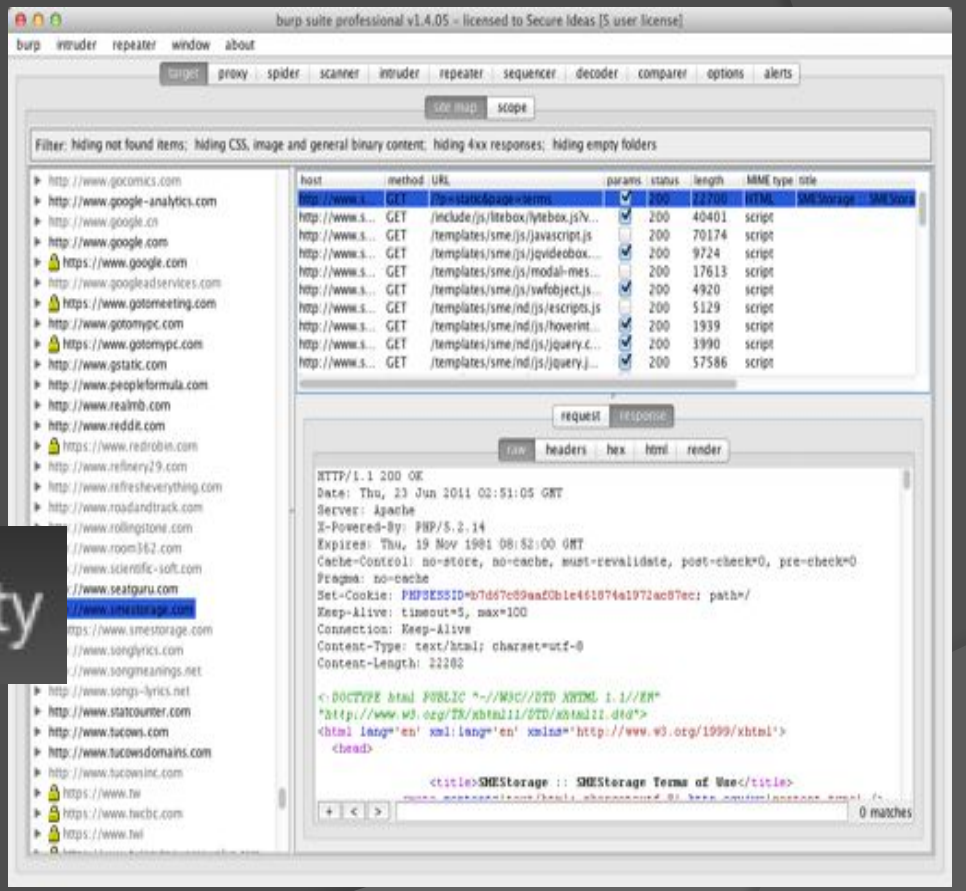
Viewing & Searching Files

- cat, less, vi, strings, grep
- SQLite files
  - GUI browser, API (Ruby, Python, etc)
- Android apps
  - ashell, aSQLiteManager, aLogViewer

```
1|root@android:/ # grep psk /data/misc/wifi/wpa_supplicant.conf
        psk="FBIs Surveillance Van #18"
        psk="Tom Liston Roxorz!"
```

Application Layer - HTTP

- Tools Used:
  - Burp Suite
  - Burp Suite
  - oh yeah Burp Suite!



PortSwigger Web Security

Why Look at the App Layer?

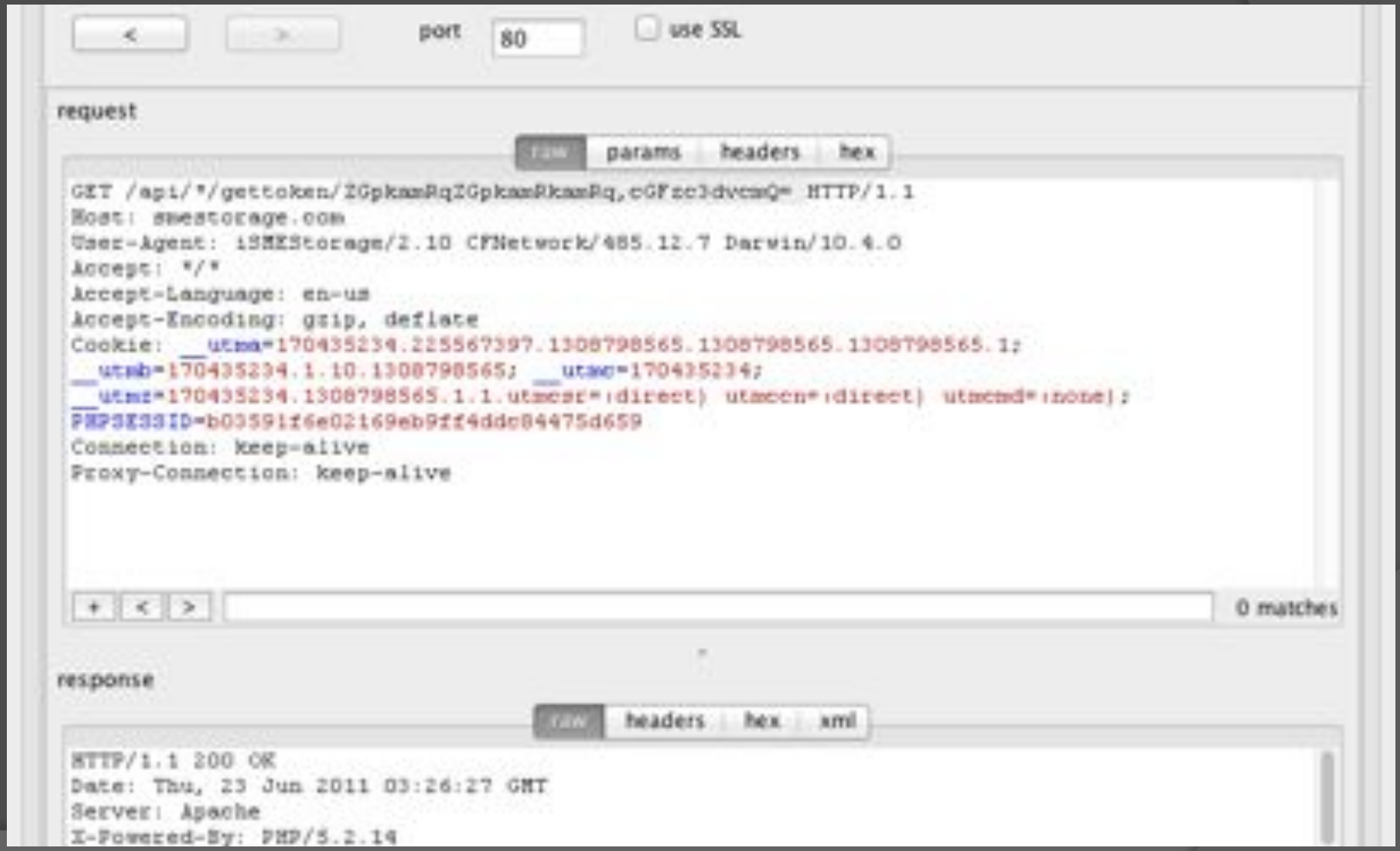
- Very common in mobile platforms
- Many errors are found within the application
  - And how it talks to the back end service
- Able to use many existing tools

Launching Burp Suite

- Memory!

```
Tyrea:Downloads kjohnson$ java -jar burpsuite_pro_v1.4.06.jar
^CTyrea:Downloads kjohnson$ java -Xmx4096M -jar burpsuite_pro_v1.4.06.jar
Deleting temporary files - please wait ... done.
Tyrea:Downloads kjohnson$ java -Xmx4096M -jar burpsuite_pro_v1.4.03.jar
```

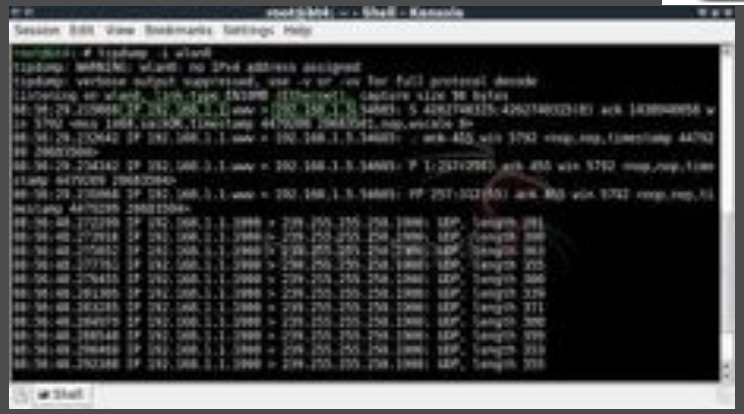
Misunderstanding Encryption



Want Credentials?

Transport Layer - TCP

- Tools Used:
  - Wireshark
  - Tcpdump
  - Network Miner

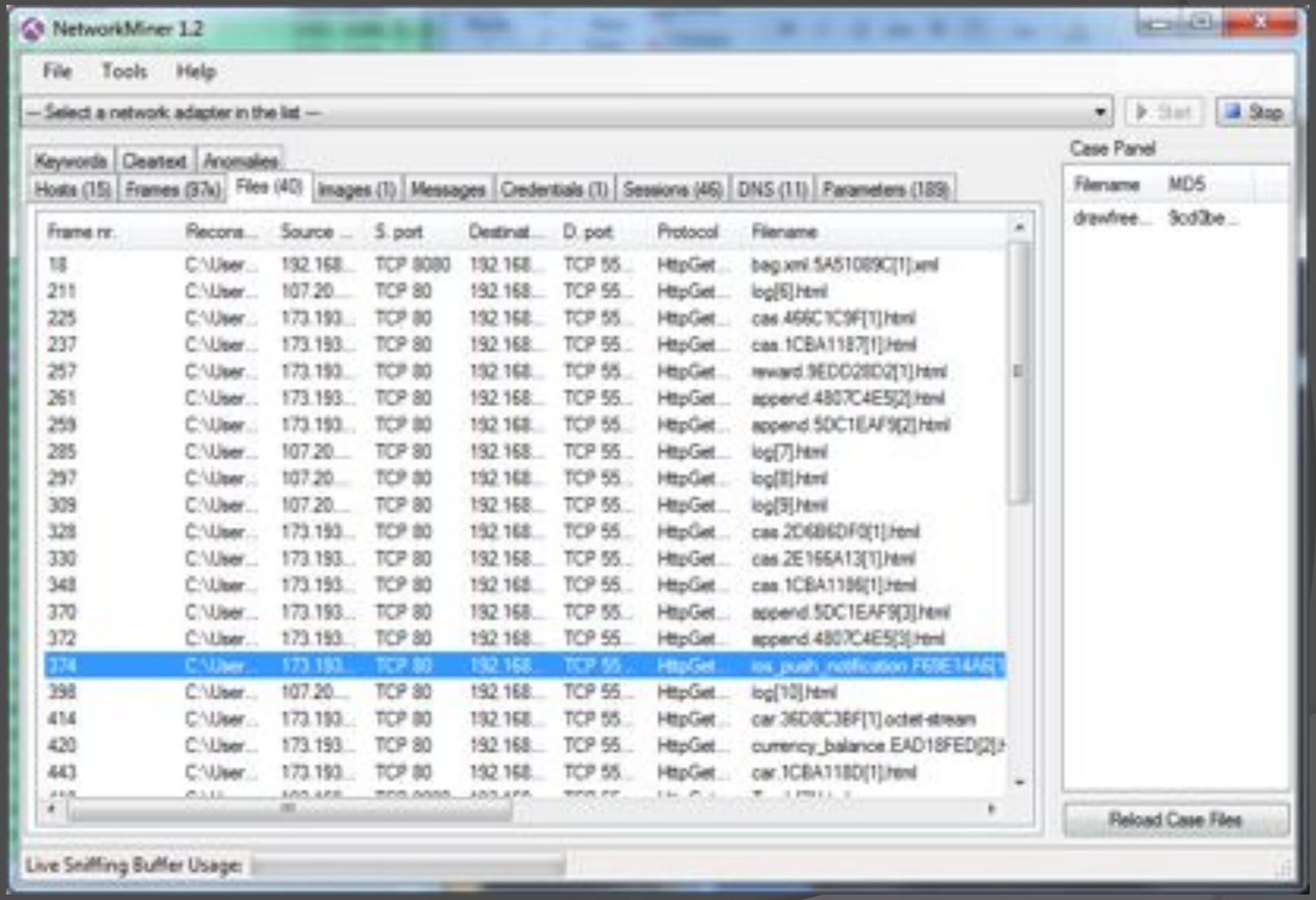


Why look at the transport layer?

- Check to see how network protocols are handled in the app
- Easily look for SSL certificate or other communication issues

NetworkMiner

- Extracts files/images and more
- Can pull out clear txt credentials
- Quickly view parameters


NetworkMiner 1.2
File
Tools
Help
— Select a network adapter in the list —
Start
Stop
Keywords
Cleartext
Anomalies
Hosts (15)
Frames (97k)
Files (40)
Images (1)
Messages
Credentials (1)
Sessions (46)
DNS (11)
Parameters (189)
Frame nr.
Recons...
Source ...
S. port
Destinat...
D. port
Protocol
Filename
18 C:\User... 192.168... TCP 8080 192.168... TCP 55... HttpGet... bag.xml.5A51089C[1].xml
211 C:\User... 107.20... TCP 80 192.168... TCP 55... HttpGet... log[5].html
225 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... cas.466C1C9F[1].html
237 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... cas.1CBA1187[1].html
257 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... reward.9EDD28D2[1].html
261 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... append.4807C4E5[2].html
259 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... append.5DC1EAF9[2].html
285 C:\User... 107.20... TCP 80 192.168... TCP 55... HttpGet... log[7].html
297 C:\User... 107.20... TCP 80 192.168... TCP 55... HttpGet... log[8].html
309 C:\User... 107.20... TCP 80 192.168... TCP 55... HttpGet... log[9].html
328 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... cas.2D6B6DF0[1].html
330 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... cas.2E166A13[1].html
348 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... cas.1CBA1186[1].html
370 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... append.5DC1EAF9[3].html
372 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... append.4807C4E5[3].html
374 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... ios_push_notification F69E14A6[1
398 C:\User... 107.20... TCP 80 192.168... TCP 55... HttpGet... log[10].html
414 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... car.36D8C3BF[1].octet-stream
420 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... currency_balance.EAD18FED[2].h
443 C:\User... 173.193... TCP 80 192.168... TCP 55... HttpGet... car.1CBA118D[1].html
Case Panel
Filename
MD5
drawfree...
9cd3be...
Reload Case Files
Live Sniffing Buffer Usage:

TCP Lab Setup

- Run tcpdump directly on the device

```
tcpdump -w drawfree.pcap -i en0 -nXs 0 host 192.168.1.16
```

- Run Wireshark by sniffing traffic over wireless AP or network hub setup (lots of ways to do this)

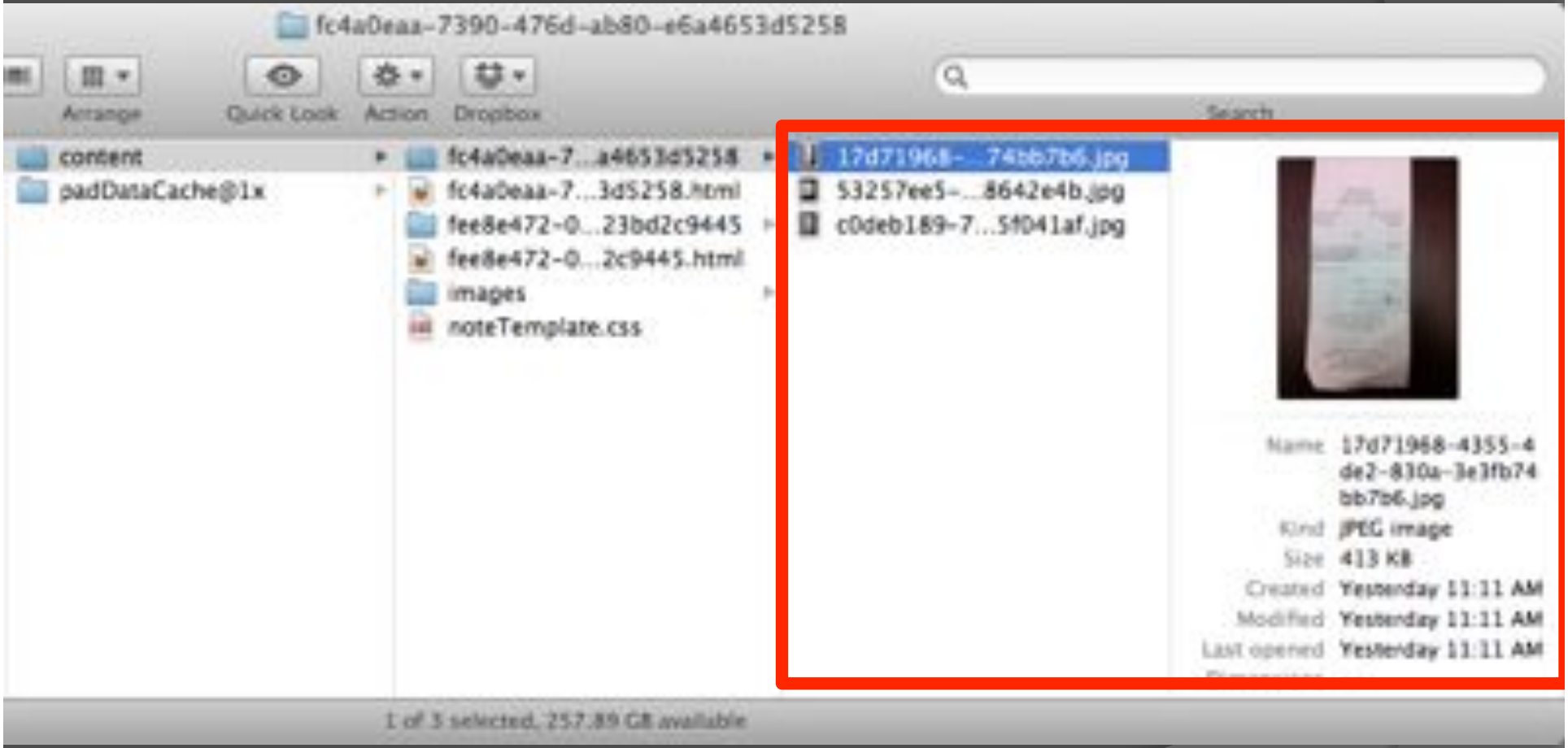
- Import PCAPs into NetworkMiner

App Vulnerabilities

- Several examples that we've found
- Many from the Top 25 downloaded apps

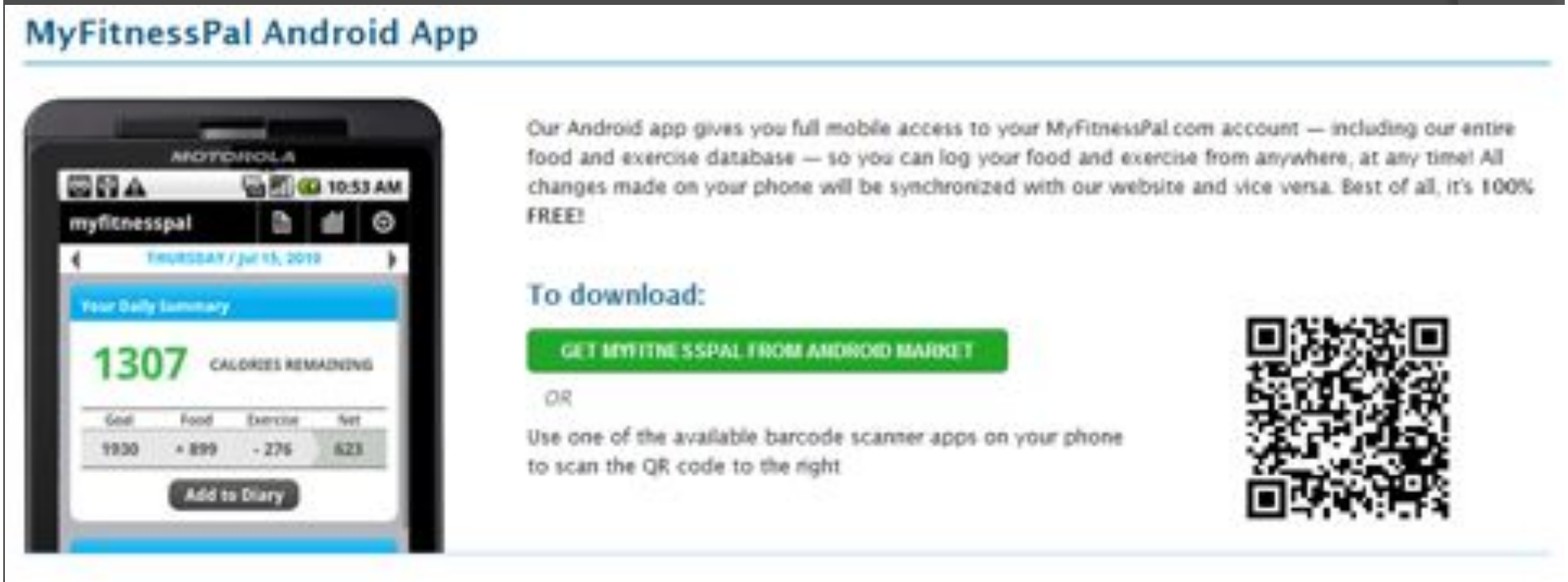
Evernote

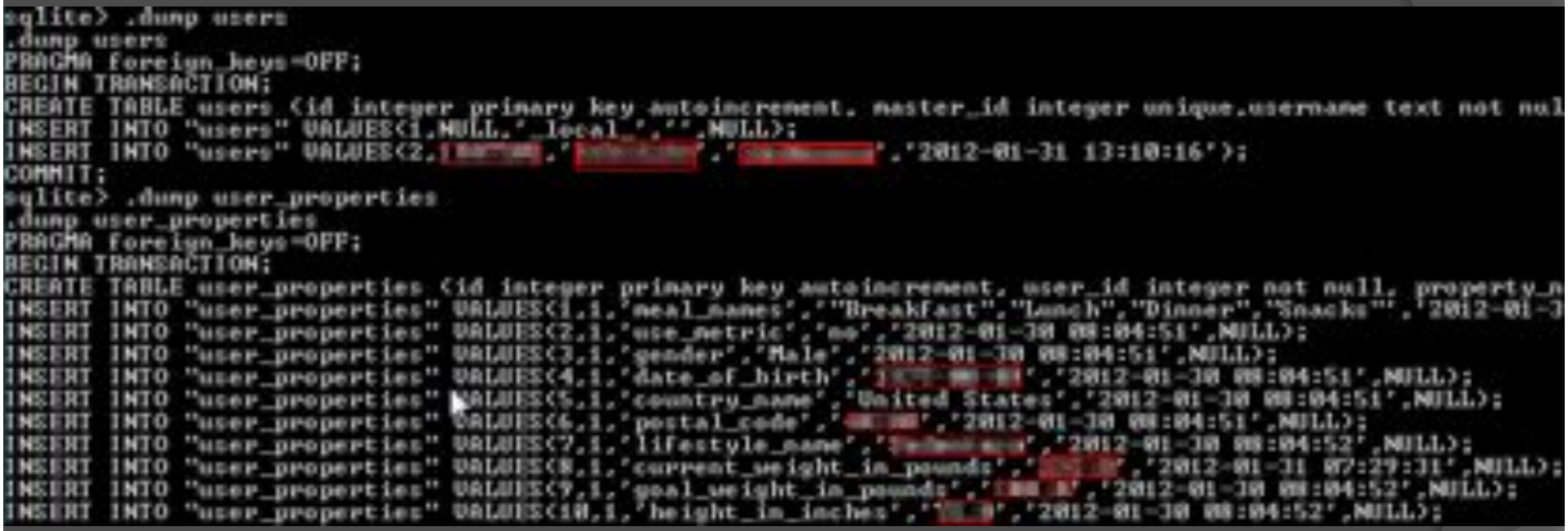
- Notebooks are stored in the cloud
- But…caches some files on the device…
- OWASP M1: Insecure Data Storage


fc4a0eaa-7390-476d-ab80-e6a4653d5258
Arrange
Quick Look
Action
Dropbox
Search
content
padDataCache@1x
fc4a0eaa-7...a4653d5258
fc4a0eaa-7...3d5258.html
fee8e472-0...23bd2c9445
fee8e472-0...2c9445.html
images
noteTemplate.css
17d71968-...74bb7b6.jpg
53257ee5-...8642e4b.jpg
c0deb189-7...5f041af.jpg
Name 17d71968-4355-4de2-830a-3e3fb74bb7b6.jpg
Kind JPEG image
Size 413 KB
Created Yesterday 11:11 AM
Modified Yesterday 11:11 AM
Last opened Yesterday 11:11 AM
1 of 3 selected, 257.89 GB available

MyFitnessPal

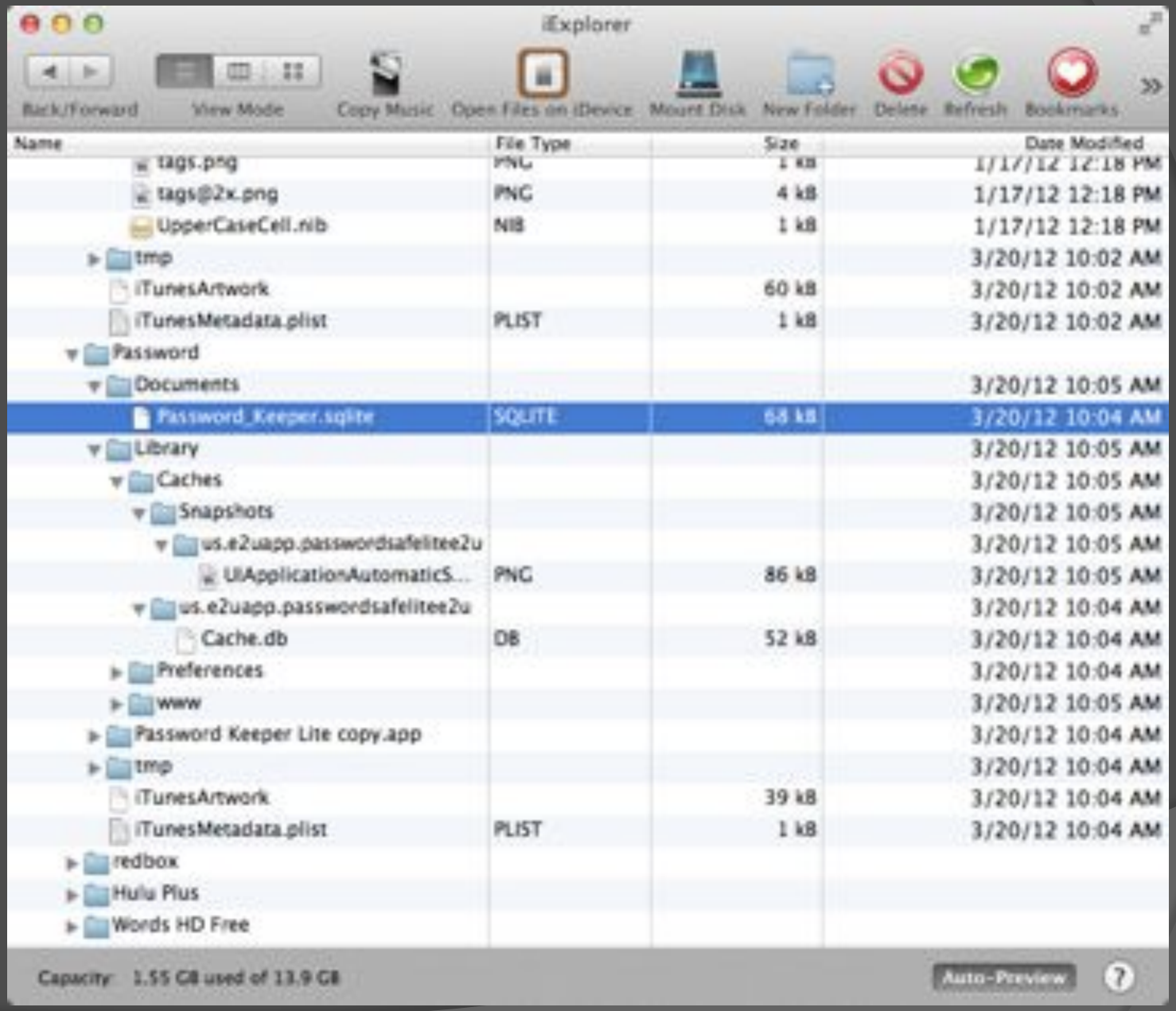
- Android app stores sensitive data on the device (too much data)

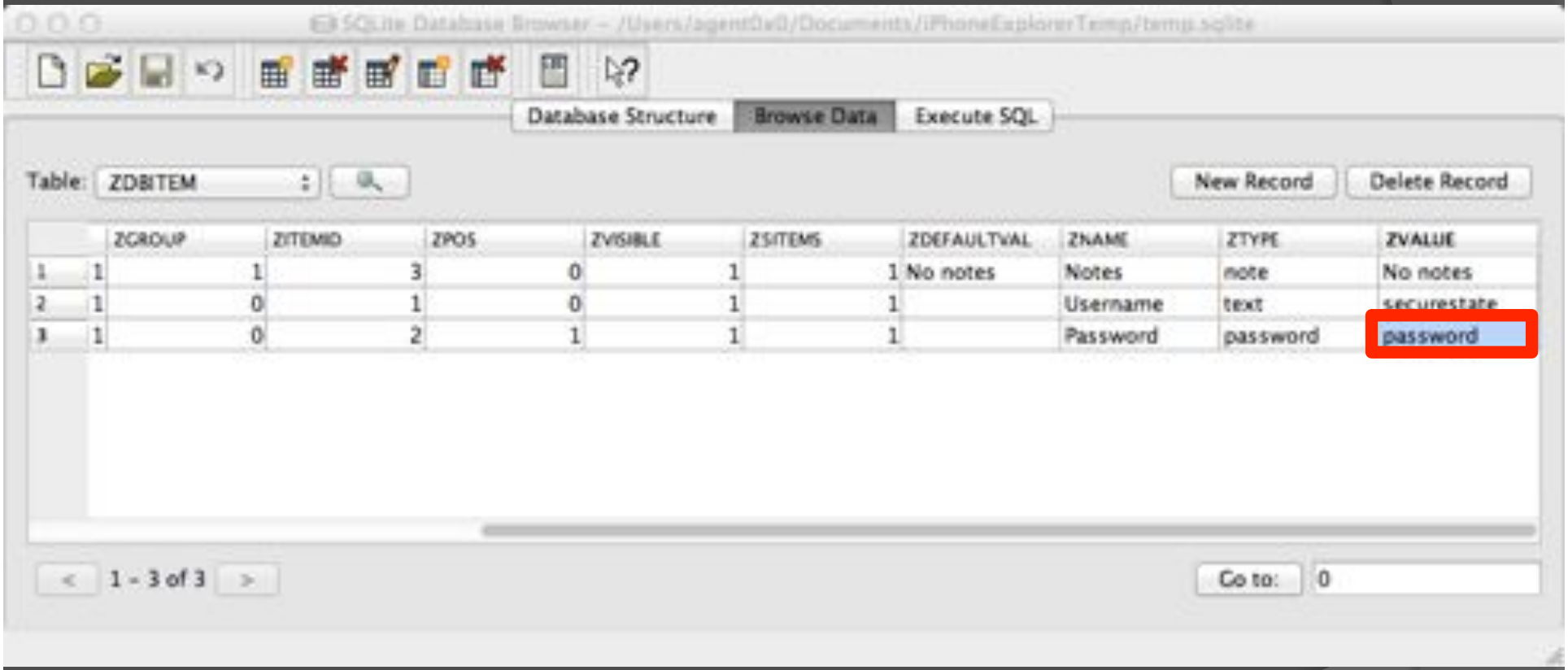


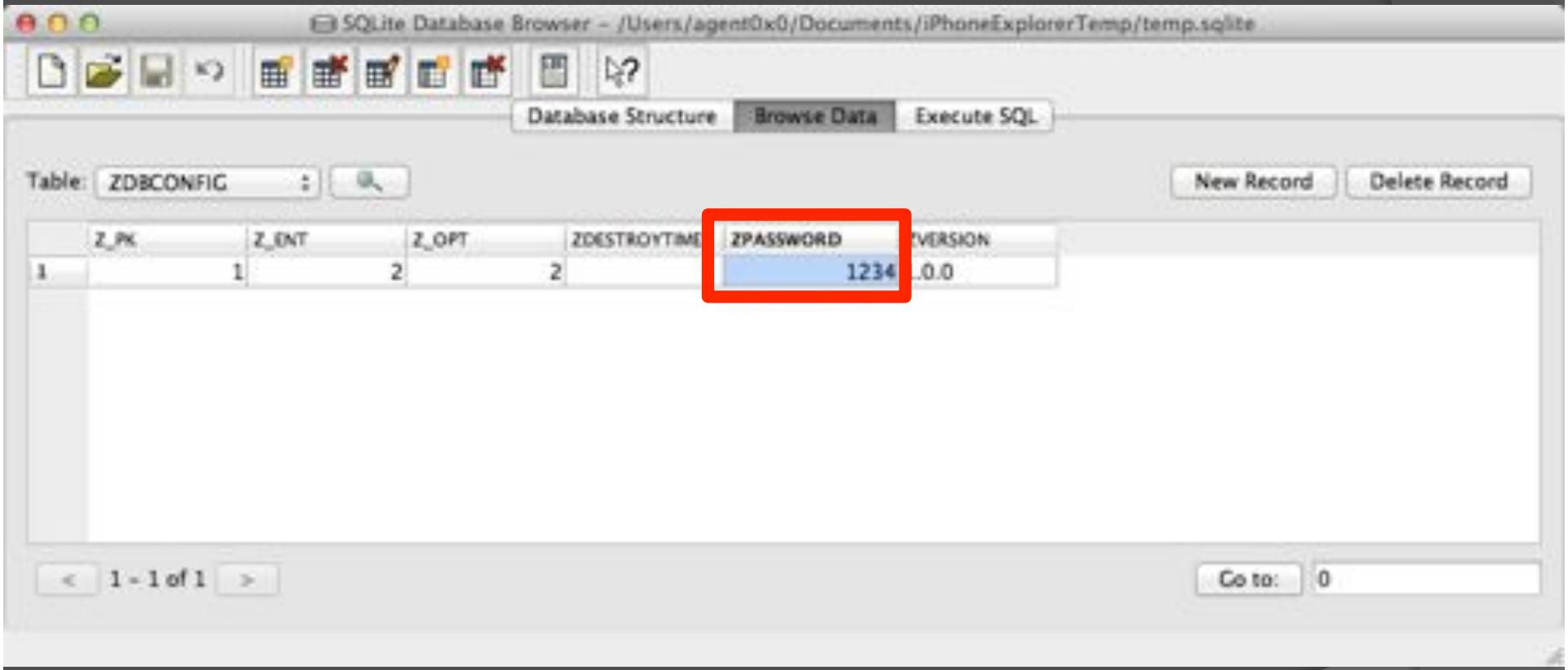

sqlite> .dump users
.dump users
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE users (id integer primary key autoincrement, master_id integer unique,username text not nul
INSERT INTO "users" VALUES(1,NULL,'_local_','',NULL);
INSERT INTO "users" VALUES(2,
,'2012-01-31 13:10:16');
COMMIT;
sqlite> .dump user_properties
.dump user_properties
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE user_properties (id integer primary key autoincrement, user_id integer not null, property_n
INSERT INTO "user_properties" VALUES(1,1,'meal_names','"BreakFast","Lunch","Dinner","Snacks"','2012-01-3
INSERT INTO "user_properties" VALUES(2,1,'use_metric','no','2012-01-30 08:04:51',NULL);
INSERT INTO "user_properties" VALUES(3,1,'gender','Male','2012-01-30 08:04:51',NULL);
INSERT INTO "user_properties" VALUES(4,1,'date_of_birth',
,'2012-01-30 08:04:51',NULL);
INSERT INTO "user_properties" VALUES(5,1,'country_name','United States','2012-01-30 08:04:51',NULL);
INSERT INTO "user_properties" VALUES(6,1,'postal_code',
,'2012-01-30 08:04:51',NULL);
INSERT INTO "user_properties" VALUES(7,1,'lifestyle_name',
,'2012-01-30 08:04:52',NULL);
INSERT INTO "user_properties" VALUES(8,1,'current_weight_in_pounds',
,'2012-01-31 07:29:31',NULL);
INSERT INTO "user_properties" VALUES(9,1,'goal_weight_in_pounds',
,'2012-01-30 08:04:52',NULL);
INSERT INTO "user_properties" VALUES(10,1,'height_in_inches',
,'2012-01-30 08:04:52',NULL);

Password Keeper “Lite”

- PIN and passwords stored in clear-text SQLite database
- So much for the security of your passwords…

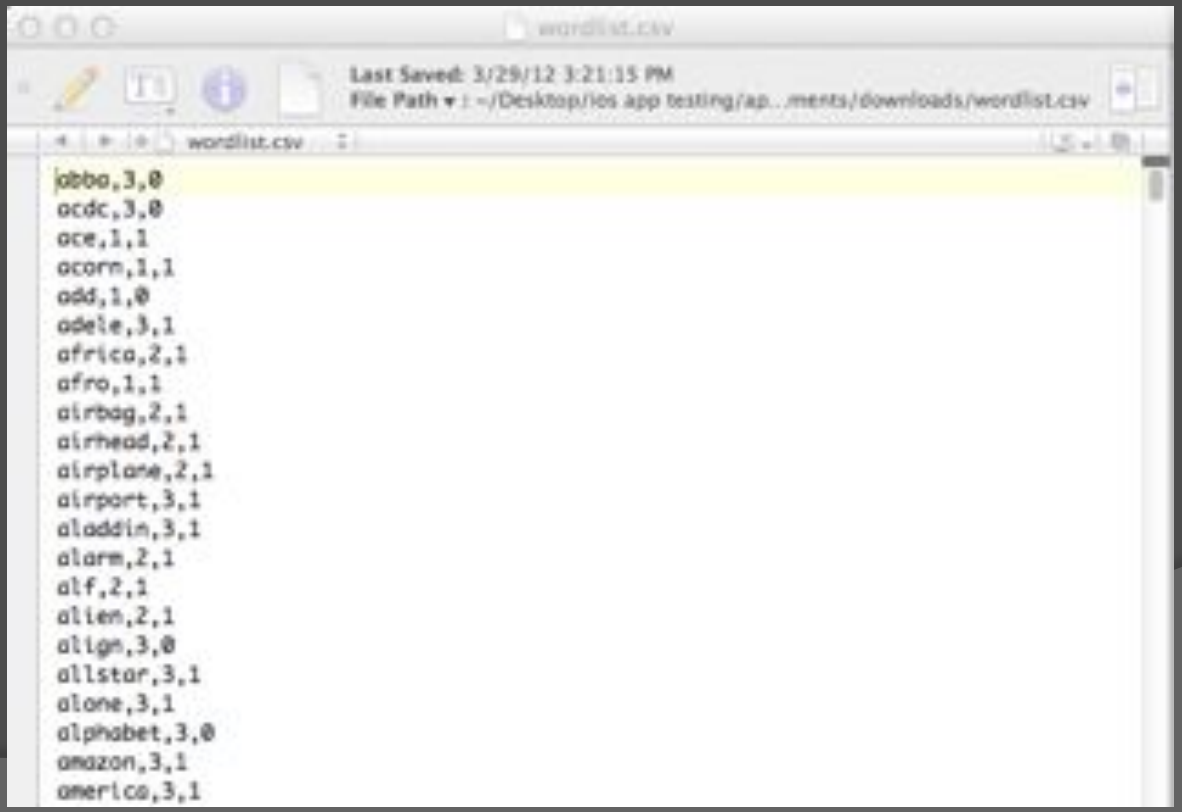

iExplorer
Back/Forward
View Mode
Copy Music
Open Files on iDevice
Mount Disk
New Folder
Delete
Refresh
Bookmarks
Name
File Type
Size
Date Modified
tags.png
PNG
1 kB
1/17/12 12:18 PM
tags@2x.png
PNG
4 kB
1/17/12 12:18 PM
UpperCaseCell.nib
NIB
1 kB
1/17/12 12:18 PM
tmp
3/20/12 10:02 AM
iTunesArtwork
60 kB
3/20/12 10:02 AM
iTunesMetadata.plist
PLIST
1 kB
3/20/12 10:02 AM
Password
Documents
3/20/12 10:05 AM
Password_Keeper.sqlite
SQLITE
68 kB
3/20/12 10:04 AM
Library
3/20/12 10:05 AM
Caches
3/20/12 10:05 AM
Snapshots
3/20/12 10:05 AM
us.e2uapp.passwordsafelitee2u
3/20/12 10:05 AM
UIApplicationAutomaticS...
PNG
86 kB
3/20/12 10:05 AM
us.e2uapp.passwordsafelitee2u
3/20/12 10:04 AM
Cache.db
DB
52 kB
3/20/12 10:04 AM
Preferences
3/20/12 10:04 AM
www
3/20/12 10:05 AM
Password Keeper Lite copy.app
3/20/12 10:04 AM
tmp
3/20/12 10:04 AM
iTunesArtwork
39 kB
3/20/12 10:04 AM
iTunesMetadata.plist
PLIST
1 kB
3/20/12 10:04 AM
redbox
Hulu Plus
Words HD Free
Capacity: 1.55 GB used of 13.9 GB
Auto-Preview


SQLite Database Browser – /Users/agentDa0/Documents/iPhoneExplorerTemp/temp.sqlite
Database Structure
Browse Data
Execute SQL
Table: ZDBITEM
New Record
Delete Record
ZGROUP ZITEMID ZPOS ZVISIBLE ZSITEMS ZDEFAULTVAL ZNAME ZTYPE ZVALUE
1 1 1 3 0 1 1 No notes Notes note No notes
2 1 0 1 0 1 1 Username text securestate
3 1 0 2 1 1 1 Password password password
1 - 3 of 3
Go to: 0


SQLite Database Browser – /Users/agent0x0/Documents/iPhoneExplorerTemp/temp.sqlite
Database Structure
Browse Data
Execute SQL
Table: ZDBCONFIG
New Record
Delete Record
Z_PK
Z_ENT
Z_OPT
ZDESTROYTIME
ZPASSWORD
VERSION
1
1
2
2
1234
1.0.0
1 - 1 of 1
Go to:
0

Draw Something

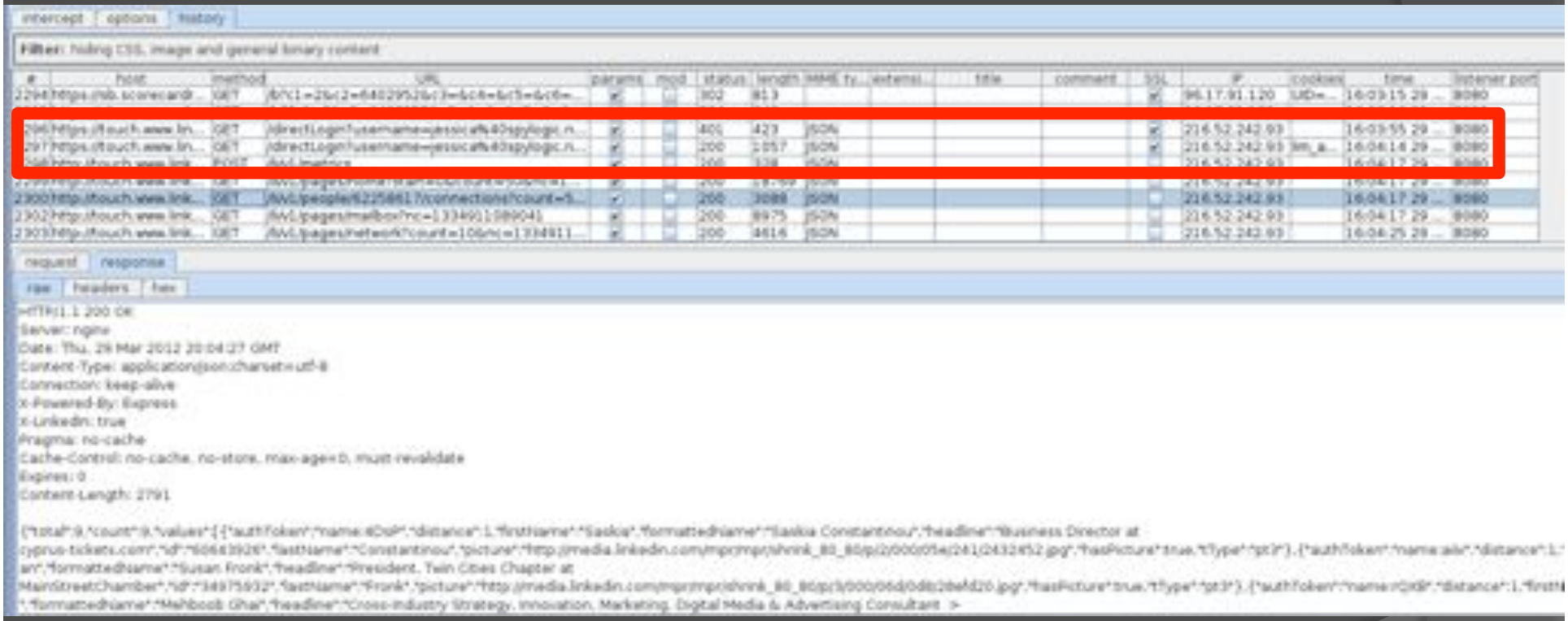
- Word list stored on the device
- Modify to mess with your friends



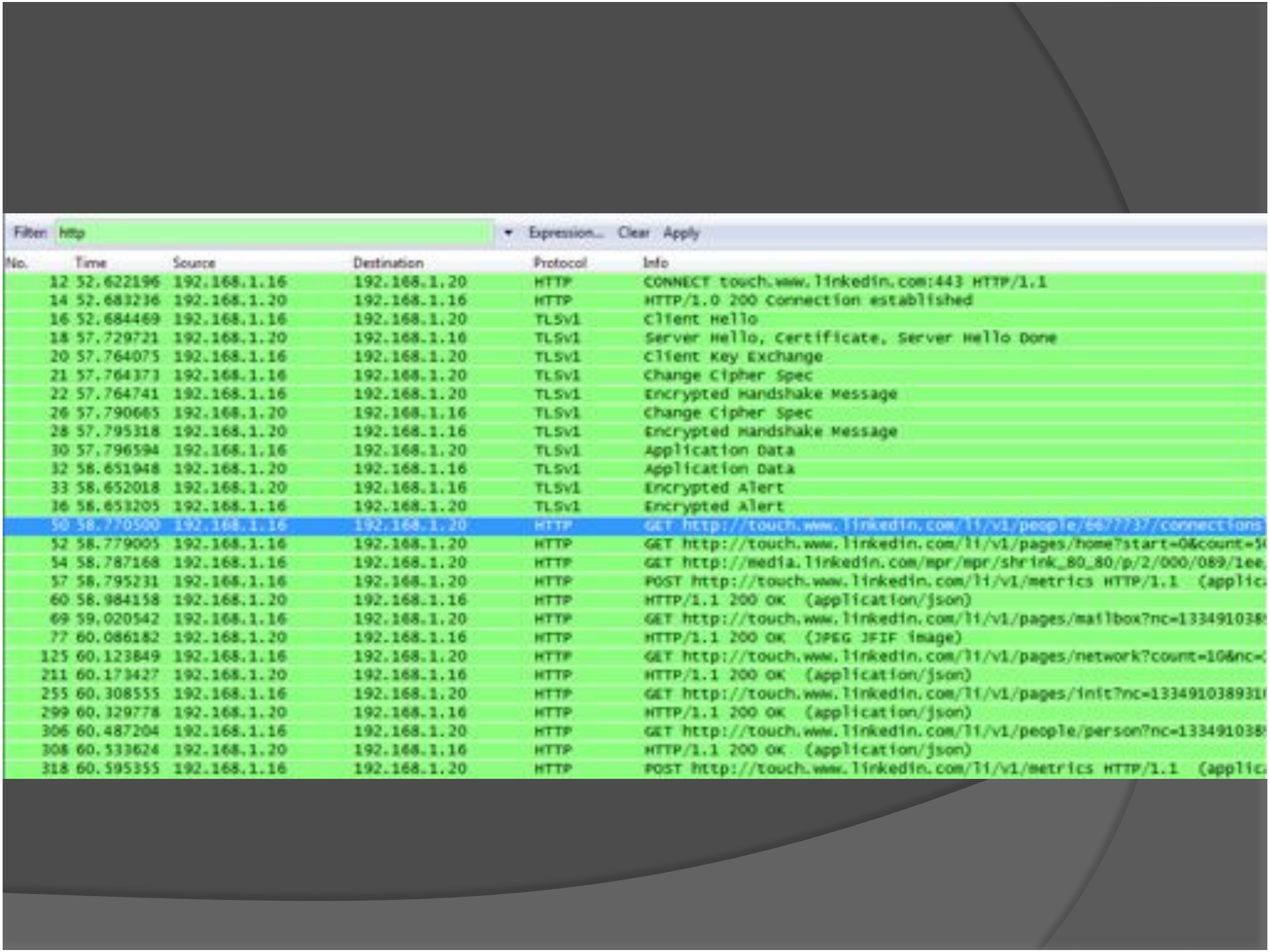
LinkedIn

- SSL only for authentication
- Session tokens and data sent over HTTP
- Lots of apps do this
- M3: Insufficient Transport Layer Protection

Auth over SSL



Data sent over HTTP



Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
12	52.622196	192.168.1.16	192.168.1.20	HTTP	CONNECT touch.www.linkedin.com:443 HTTP/1.1
14	52.683236	192.168.1.20	192.168.1.16	HTTP	HTTP/1.0 200 Connection established
16	52.684469	192.168.1.16	192.168.1.20	TLSv1	Client Hello
18	57.729721	192.168.1.20	192.168.1.16	TLSv1	Server Hello, Certificate, Server Hello Done
20	57.764075	192.168.1.16	192.168.1.20	TLSv1	Client Key Exchange
21	57.764373	192.168.1.16	192.168.1.20	TLSv1	Change Cipher Spec
22	57.764741	192.168.1.16	192.168.1.20	TLSv1	Encrypted Handshake Message
26	57.790665	192.168.1.20	192.168.1.16	TLSv1	Change Cipher Spec
28	57.795318	192.168.1.20	192.168.1.16	TLSv1	Encrypted Handshake Message
30	57.796594	192.168.1.16	192.168.1.20	TLSv1	Application Data
32	58.651948	192.168.1.20	192.168.1.16	TLSv1	Application Data
33	58.652018	192.168.1.20	192.168.1.16	TLSv1	Encrypted Alert
36	58.653205	192.168.1.16	192.168.1.20	TLSv1	Encrypted Alert
50	58.770500	192.168.1.16	192.168.1.20	HTTP	GET http://touch.www.linkedin.com/li/v1/people/6677737/connections
52	58.779005	192.168.1.16	192.168.1.20	HTTP	GET http://touch.www.linkedin.com/li/v1/pages/home?start=0&count=5
54	58.787168	192.168.1.16	192.168.1.20	HTTP	GET http://media.linkedin.com/mpr/mpr/shrink_80_80/p/2/000/089/1ee
57	58.795231	192.168.1.16	192.168.1.20	HTTP	POST http://touch.www.linkedin.com/li/v1/metrics HTTP/1.1 (applic
60	58.984158	192.168.1.20	192.168.1.16	HTTP	HTTP/1.1 200 OK (application/json)
69	59.020542	192.168.1.16	192.168.1.20	HTTP	GET http://touch.www.linkedin.com/li/v1/pages/mailbox?nc=133491038
77	60.086182	192.168.1.20	192.168.1.16	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
125	60.123849	192.168.1.16	192.168.1.20	HTTP	GET http://touch.www.linkedin.com/li/v1/pages/network?count=10&nc=
211	60.173427	192.168.1.20	192.168.1.16	HTTP	HTTP/1.1 200 OK (application/json)
255	60.308555	192.168.1.16	192.168.1.20	HTTP	GET http://touch.www.linkedin.com/li/v1/pages/init?nc=1334910389
299	60.329778	192.168.1.20	192.168.1.16	HTTP	HTTP/1.1 200 OK (application/json)
306	60.487204	192.168.1.16	192.168.1.20	HTTP	GET http://touch.www.linkedin.com/li/v1/people/person?nc=133491038
308	60.533624	192.168.1.20	192.168.1.16	HTTP	HTTP/1.1 200 OK (application/json)
318	60.595355	192.168.1.16	192.168.1.20	HTTP	POST http://touch.www.linkedin.com/li/v1/metrics HTTP/1.1 (applic

Pandora

- Registration over HTTP
- User name/Password and Registration info sent over clear text
- Unfortunately…lots of apps do this


request to http://www.pandora.com:80 [208.85.40.80]
forward
drop
intercept is on
action
raw
params
headers
hex
POST /ipad/register/6CUD747 HTTP/1.1
Host: www.pandora.com
User-Agent: Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Mobile/9A405
Content-Length: 113
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: http://www.pandora.com
Content-Type: application/x-www-form-urlencoded
Referer: http://www.pandora.com/ipad/register/6CUD747
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: v2regbstage=true
Pragma: no-cache
Connection: keep-alive
Proxy-Connection: keep-alive
email=[redacted]y%40gmail.com&password=[redacted]&password_confirm=[redacted]zip=44112&year=1974&gender=male&terms=on

Hard Coded Passwords/Keys

- Major Grocery Chain “Rewards” Android app
- Simple to view the source, extract private key
- OWASP M9: Broken Cryptography
- Do developers really do this?

```
<string name="user_token" />
<string name="[redacted]private">3h1ut1ns0v3</string>
```

Why yes, they do!

iOS/Android authentication and security

2

Here is what I am trying to do and can anyone provide some best practice advice for authentication and security?

Each user will have their own private database on the cloud. He will have his local couchdb on iOS/Android. My iOS/Android app will replicate between mobile and the cloud. Users can also access their data on the cloud from the web. I am using CouchDB authentication and there is no middle tier. When a user sign up for a new account, I will create a new database in the cloud with his account name. I compared Iris Couch and Cloudant and and chose Iris Couch because Cloudant doesn't give me admin privilege to achieve this.

My questions:

1. Is it a good idea or possible for the iOS/Android/Web client to have admin privilege to create a new database when they sign up for a new user account? I could hard code the admin username and password on the iOS/Android clients but that feels very wrong. For the web client, I won't have the option to hard code the admin password at all. Alternatively, I can setup a new machine in the cloud to monitor _users database changes and create new databases accordingly.
2. Shall I use the user's credential to replicate between mobile and cloud?
3. I am using Iris Couch for hosting. What is the best way to integrate Facebook authentication into my authentication model? I saw this plugin but does it require my own hosting and making changes to the server?

https://github.com/sander/CouchDB-Facebook-Authentication

Out of curiosity, I also look at Cloudant hosting. But it doesn't look like I can create CouchDB users and support my database-per-user model. I don't have admin access to _user database.

Privacy Issues

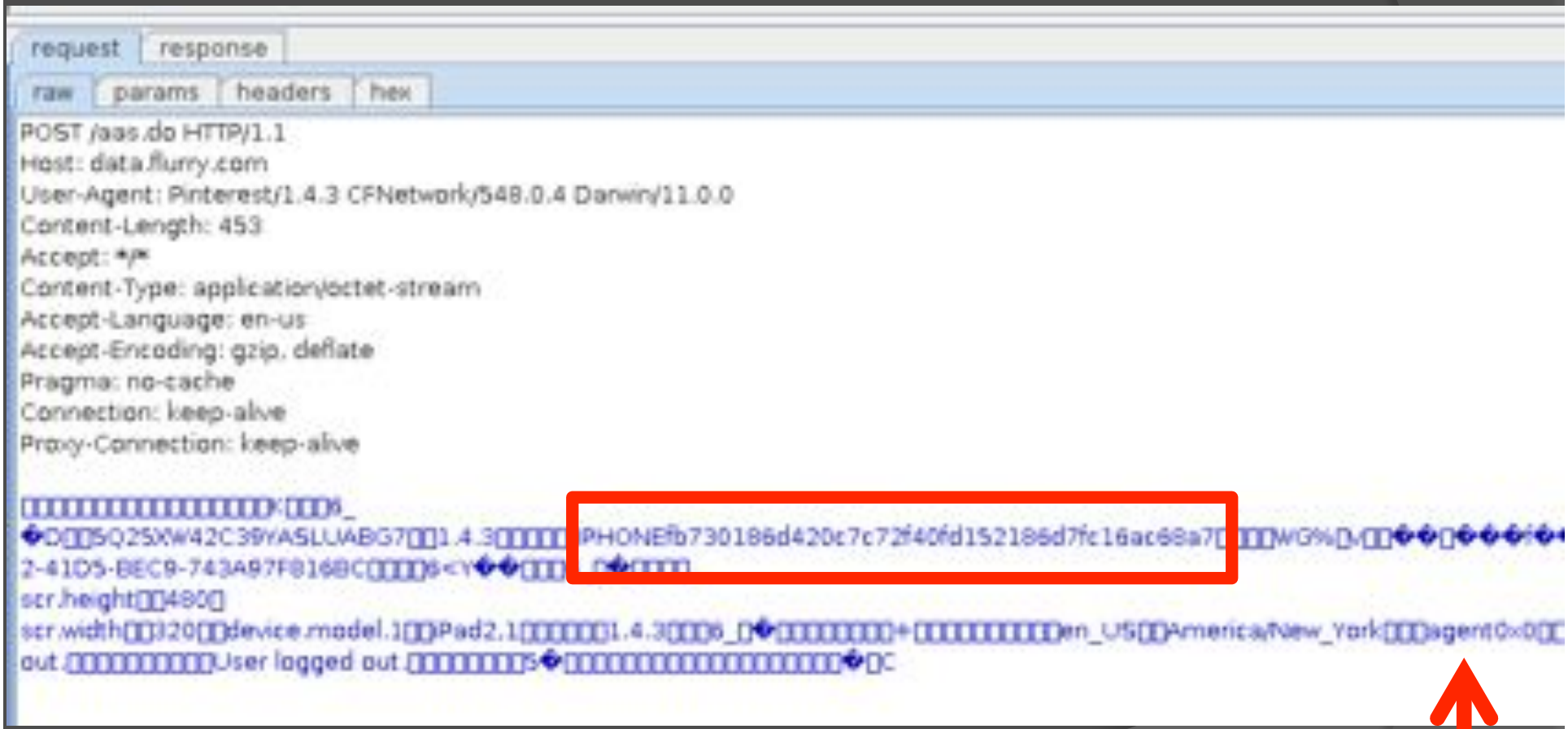
- Example: Draw Something App (Top 25)
- UDID and more sent to the following third-party ad providers:
  - appads.com
  - mydas.mobi
  - greystripe.com
  - tapjoyads.com

What is UDID?

- Alpha-numeric string that uniquely identifies an Apple device


iPhone Configuration Utility
Add
Share
Export
LIBRARY
Devices
Applications
Provisioning Profiles
Configuration Profiles
DEVICES
Summary
Configuration Profiles
Provisioning Profiles
Applications
Console
Device
Name: securestate's iPad
Capacity: 13.86 GB
Software Version: 5.0.1 (9A405)
Identifier: fb730186d420c7c72f40fd152186d7fc16ac68a7
IMEI: Unknown
MEID: Unknown
Bluetooth MAC Address:
Last Connected: March 29, 2012 12:35 PM
Contact
Phone Number:
Name:
Email Address:
Certificate

Pinterest and Flurry.com



Amid Privacy Concerns, Apple Has Started Rejecting Apps That Access UDIDs

KIM-MAI CUTLER

Saturday, March 24th, 2012 — 26 Comments

Amid extra scrutiny from Congress around privacy issues, Apple this week has started rejecting apps that access UDIDs, or identification numbers that are unique to every iPhone and iPad.

Apple had already given **developers a heads-up about the change more than six months ago** when it said in some iOS documentation that it was going to deprecate UDIDs. But it looks like Apple is moving ahead of schedule with pressure from lawmakers and the media. It can take more than a year to deprecate features because developers need time to adjust and change their apps. A few weeks ago, **some of the bigger mobile-social developers told me that Apple had reached out and warned them to move away from UDIDs.**

Conclusions

- Mobile devices are critically common
- Most people use them without thinking of security
- Developers seem to be repeating the past
- We need to secure this area

Contact Us

- John Sawyer
- Tom Eston
  - Twitter: @agent0x0
  - teston@securestate.com
- Kevin Johnson
  - Twitter: @secureideas
  - kjohnson@secureideas.net