DUDE, WHERE IS MY LAPTOP?

black hat
EUROPE 2013
MARCH 12-15, 2013
AMSTERDAM, NETHERLANDS

VULNEX

WE?

Simón Roses Femerling

- Founder & CEO, VULNEX
- Blog: www.simonroses.com
- Twitter: @simonroses
- Former Microsoft, PwC, @Stake
- DARPA Cyber Fast Track award on software security project
- Black Hat, RSA, OWASP, SOURCE, DeepSec, TECHNET

Curro Márquez

- Director of Intelligence, VULNEX

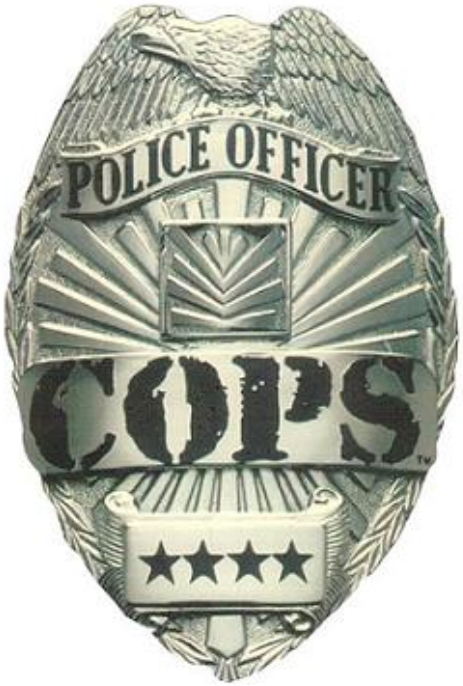
TALK OBJECTIVES

- Examination of Anti-Theft products
- In a mobile world are we safe?
- If stolen, what can they do?

DISCLAIMER

All Anti-Theft solutions are considered safe until proven guilty by a security review.

Neither the authors or VULNEX support in any way the robbery and/or manipulation of electronic devices, nor shall be held liable or responsible for the information herein.



AGENDA

1. Overview
2. Issues & Weaknesses
3. Vulnerabilities & Attacks
4. Conclusions

1. Overview

VULNEX

1. TERMINOLOGY NIGHTMARE: NO ESCAPE!

- BYOx Family

BYOD:	**B**ring **Y**our **O**wn **D**evice
BYOT:	**B**ring **Y**our **O**wn **T**echnology
BYOP:	**B**ring **Y**our **O**wn **P**hone
BYOPC:	**B**ring **Y**our **O**wn **PC**

- Mxx Family

MDM:	**M**obile **D**evice **M**anagement
MAM:	**M**obile **A**pplication **M**anagement
MDP:	**M**obile **D**ata **P**rotection
MDS:	**M**obile **D**ata **S**ecurity

1. PHONES & LAPTOPS CONTAIN YOUR LIFE

- Emails
- Contacts
- Photos
- Social Networks
- Bank Accounts
- Password Managers
- Access to corporate / internal servers
- Apps
- You name it…

1. LOST & STOLEN STATISTICS

- “10,000 mobiles phones stolen per month in London” (that’s 314 phones per day)
  London Metropolitan Police (2013)

- “Lost and stolen cellphones could cost U.S. consumers more than $30 billion this year”
  Lookout (2012)

- “Laptop theft totaled more than $3.5 million dollars in 2005”
  FBI

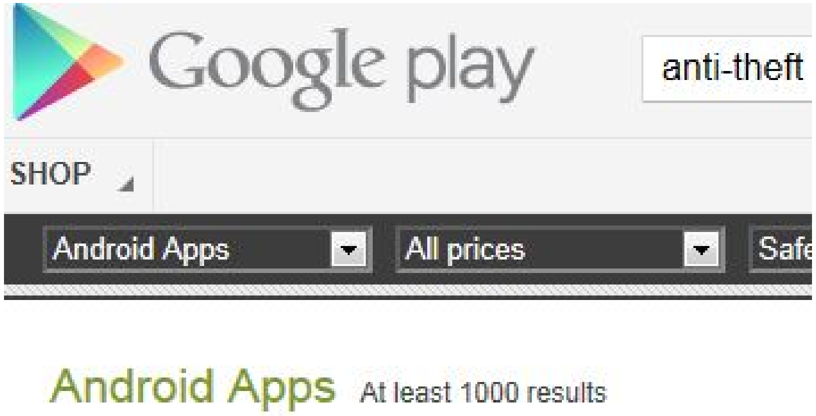
- FBI statistics reveal that 221,009 laptops were reported stolen in 2008 and 2009

- 67,000 phones likely to be lost or stolen during London Olympics
  http://www.venafi.com/67000-phones-likely-to-be-lost-or-stolen-during-london-olympics/

1. ANTI-THEFT FEATURES

- Encrypt & protect information
- Remote Wipe files, directory or system
- Lock screen
- Sound alarm & alert window
- Sent info to C&C:
  - Screenshot
  - Webcam photo
  - Wireless (Access Point) name
  - GPS location
  - IP
- Claim to:
  - Offer strong security
  - Help recovering device

1. SEA OF ANTI-THEFT: PRODUCTS BY NUMBERS



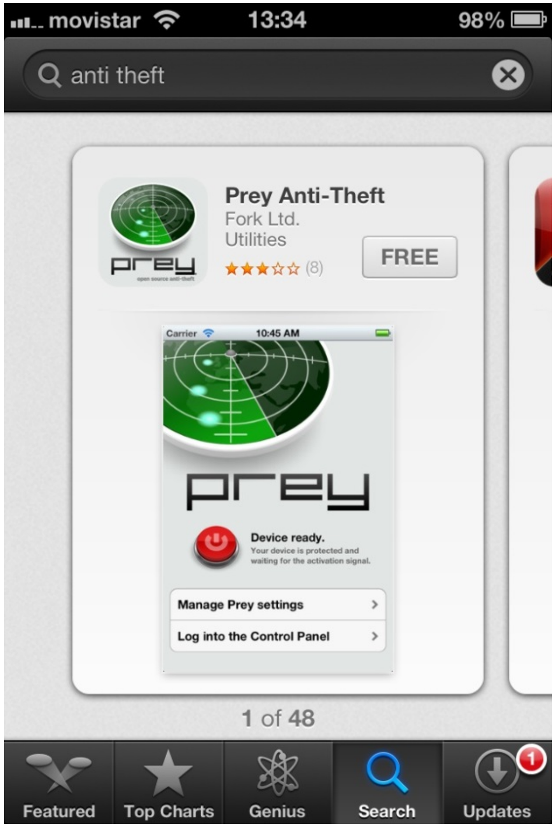
Google play

anti-theft

SHOP

Android Apps | All prices | Safe

Android Apps At least 1000 results



movistar 13:34 98%

anti theft

Prey Anti-Theft
Fork Ltd.
Utilities
★★★☆☆ (8)
FREE

prey

Device ready.
Your device is protected and waiting for the activation signal.

Manage Prey settings

Log into the Control Panel

1 of 48

Featured | Top Charts | Genius | Search | Updates

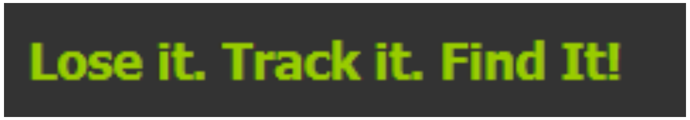
- Antivirus houses have also joined the party…

1. ANTI-THEFT CLAIMS: JUST RELAX

Rest safe.

What we do

We Simplify Enterprise Mobility



Lose it. Track it. Find It!

THE SECURE WORKSPACE

Find your laptop, see who's using it, even what they're wearing!

ANTI-THEFT

Keep your device safe & your safer

2. Issues & Weaknesses

2. PREVIOUS WORK ON THE SUBJECT

- "Deactivate the Rootkit"
  Alfredo Ortega & Anibal Sacco
  http://www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-Ortega-DeactivateRootkit-SLIDES.pdf

- Issues
  - Huge privacy risk (bad/no authentication)
  - Anyone could activate it with enough privileges
  - Anyone can change the configuration
  - Anyone can de-activate it (at least in certain known cases)
  - Whitelisted by AV (potentially undetectable)

2. LACK OF THREAT MODELING (TM)

- How data is protected (Rest / Transit)?
- If stolen can Anti-Theft really:
  - Can data really be wiped?
  - Can device be recovered?
  - Can tampering be detected and stopped ?
  - How resilient are we?
- No understanding of the threats
- ***Because…***

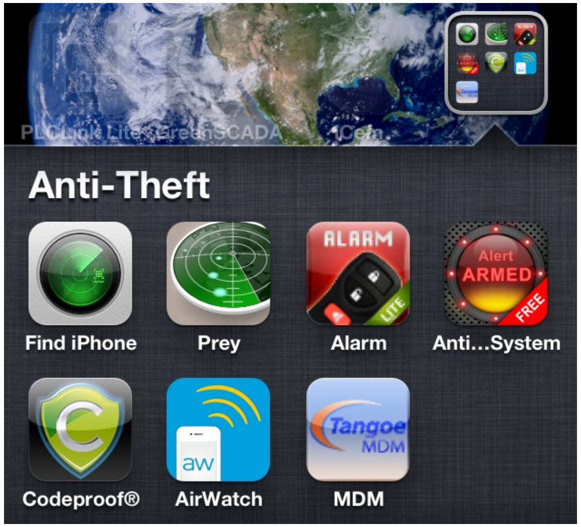
2. NOT ALL THIEVES ARE SO SEXY…

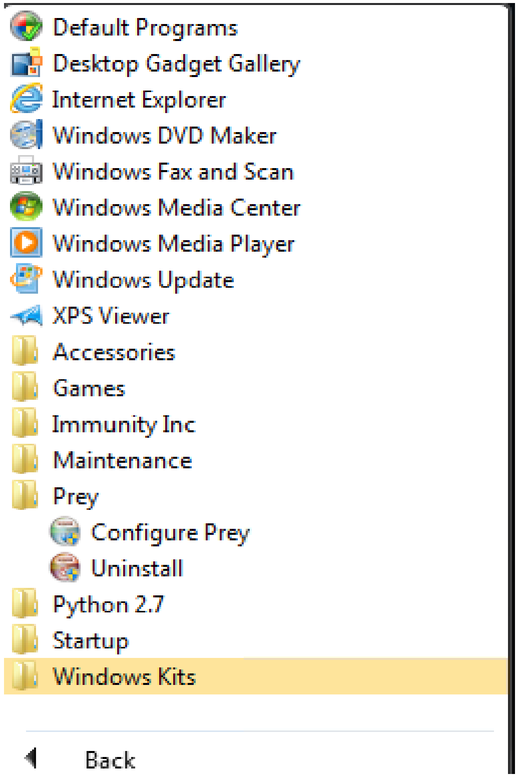
2. THIEF TACTICS

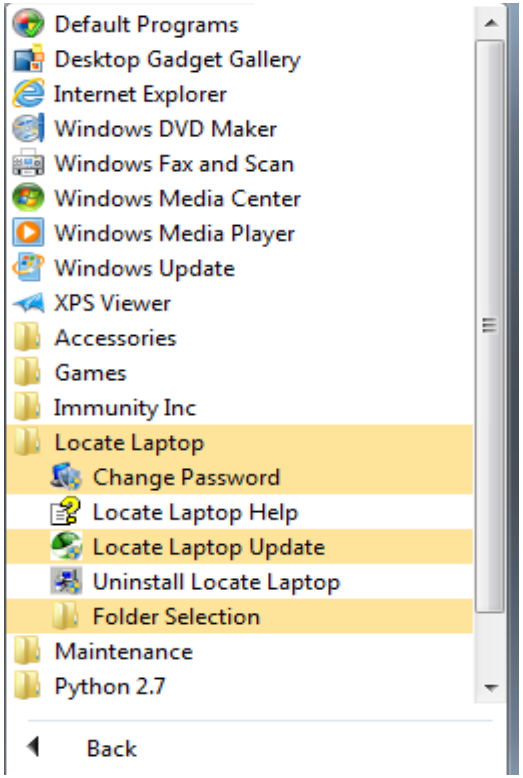
- Network Analysis & Attacks
- System Analysis & Attacks
- Reverse Engineering Apps
  - Android
  - iOS
  - Windows
  - MacOS

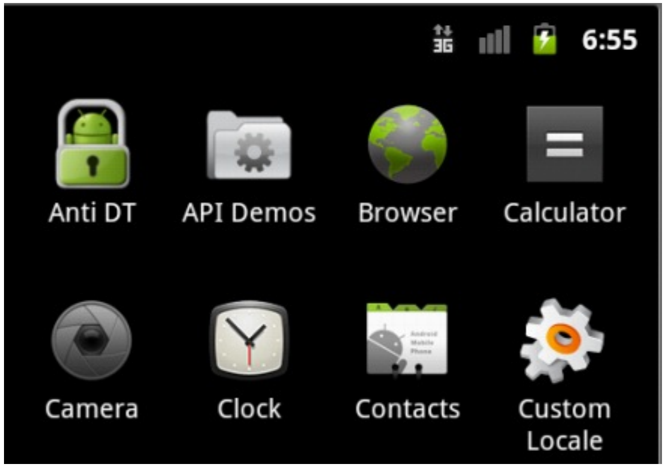
3. Vulnerabilities & Attacks

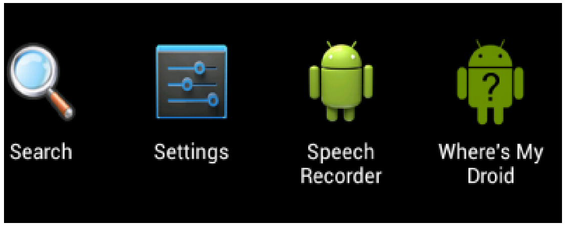
4. HIDE IN PLAIN SIGHT… RIGHT!

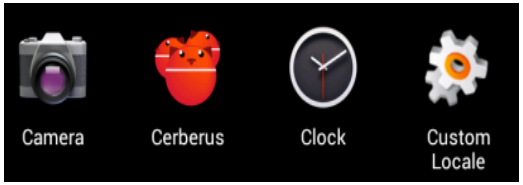












3. ALL KIND OF INFORMATION DISCLOSURE

Thief: snooping the network

Emails

Person Names

Passwords

GPS coordinates

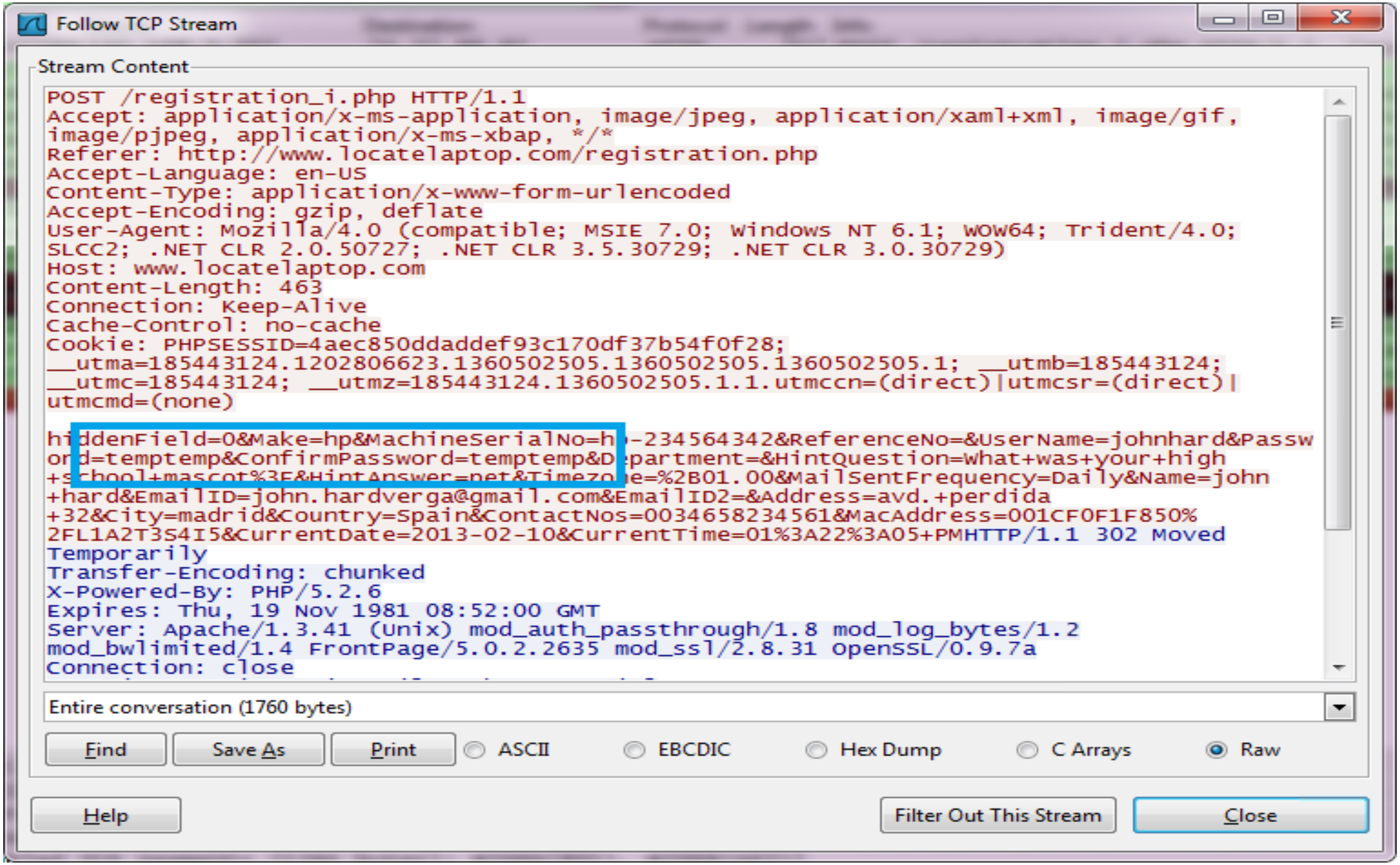
OS version

Phone Numbers

Device ID

Application Internals

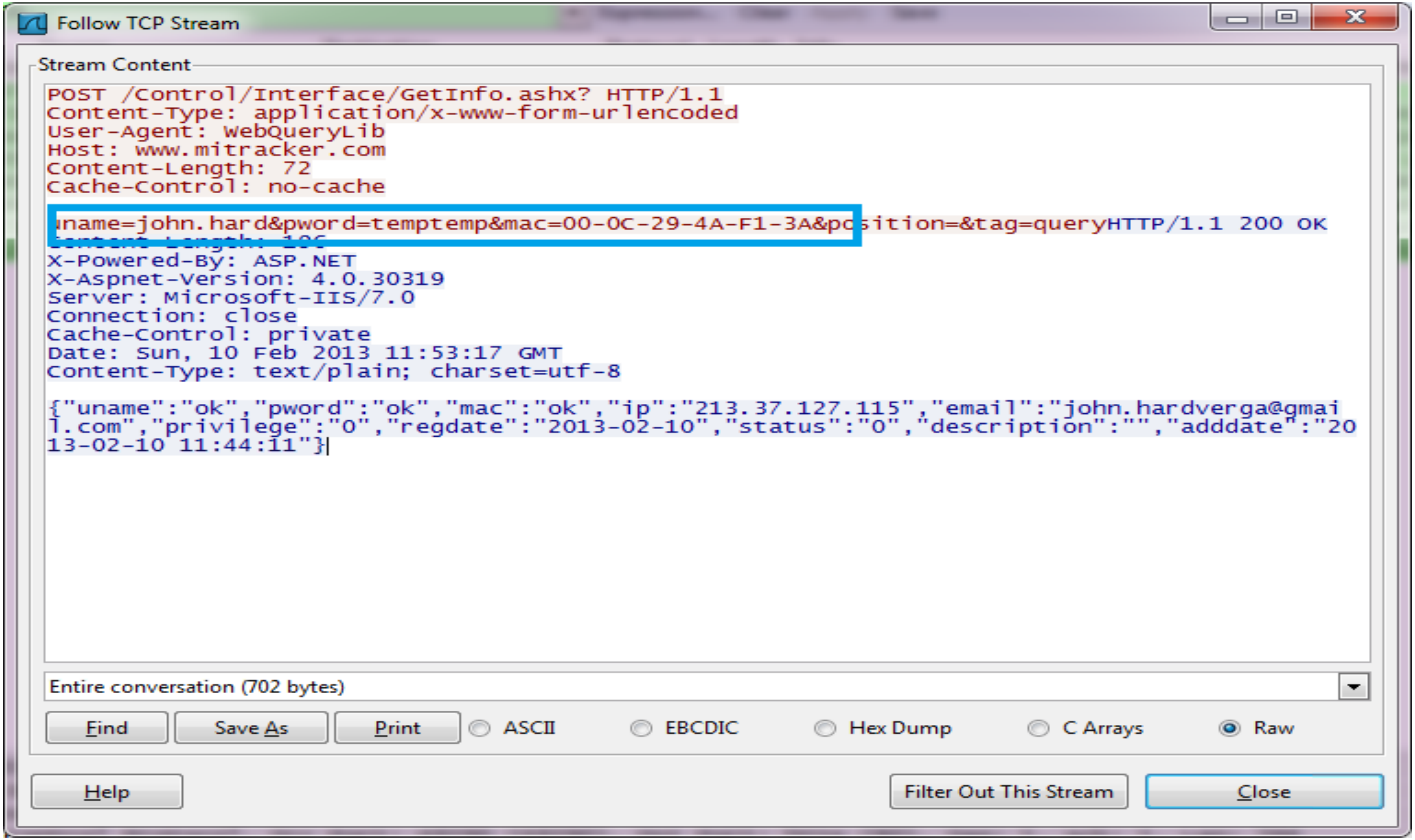
3. CLEAR TEXT SECRETS (IN TRANSIT): LOCATEMYLAPTOP (WINDOWS)



```
POST /registration_i.php HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif,
image/pjpeg, application/x-ms-xbap, */*
Referer: http://www.locatelaptop.com/registration.php
Accept-Language: en-US
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Host: www.locatelaptop.com
Content-Length: 463
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=4aec850ddaddef93c170df37b54f0f28;
__utma=185443124.1202806623.1360502505.1360502505.1360502505.1; __utmb=185443124;
__utmc=185443124; __utmz=185443124.1360502505.1.1.utmccn=(direct)|utmcsr=(direct)|
utmcmd=(none)

hiddenField=0&Make=hp&MachineSerialNo=hp-234564342&ReferenceNo=&UserName=johnhard&Passw
ord=temptemp&ConfirmPassword=temptemp&Department=&HintQuestion=What+was+your+high
+school+mascot%3F&HintAnswer=pet&Timezone=%2B01.00&MailSentFrequency=Daily&Name=john
+hard&EmailID=john.hardverga@gmail.com&EmailID2=&Address=avd.+perdida
+32&City=madrid&Country=Spain&ContactNos=0034658234561&MacAddress=001CF0F1F850%
2FL1A2T3S4I5&CurrentDate=2013-02-10&CurrentTime=01%3A22%3A05+PMHTTP/1.1 302 Moved
Temporarily
Transfer-Encoding: chunked
X-Powered-By: PHP/5.2.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Apache/1.3.41 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2
mod_bwlimited/1.4 FrontPage/5.0.2.2635 mod_ssl/2.8.31 OpenSSL/0.9.7a
Connection: close
```

VULNEX

3. CLEAR TEXT SECRETS (IN TRANSIT): MITRACKER (WINDOWS)

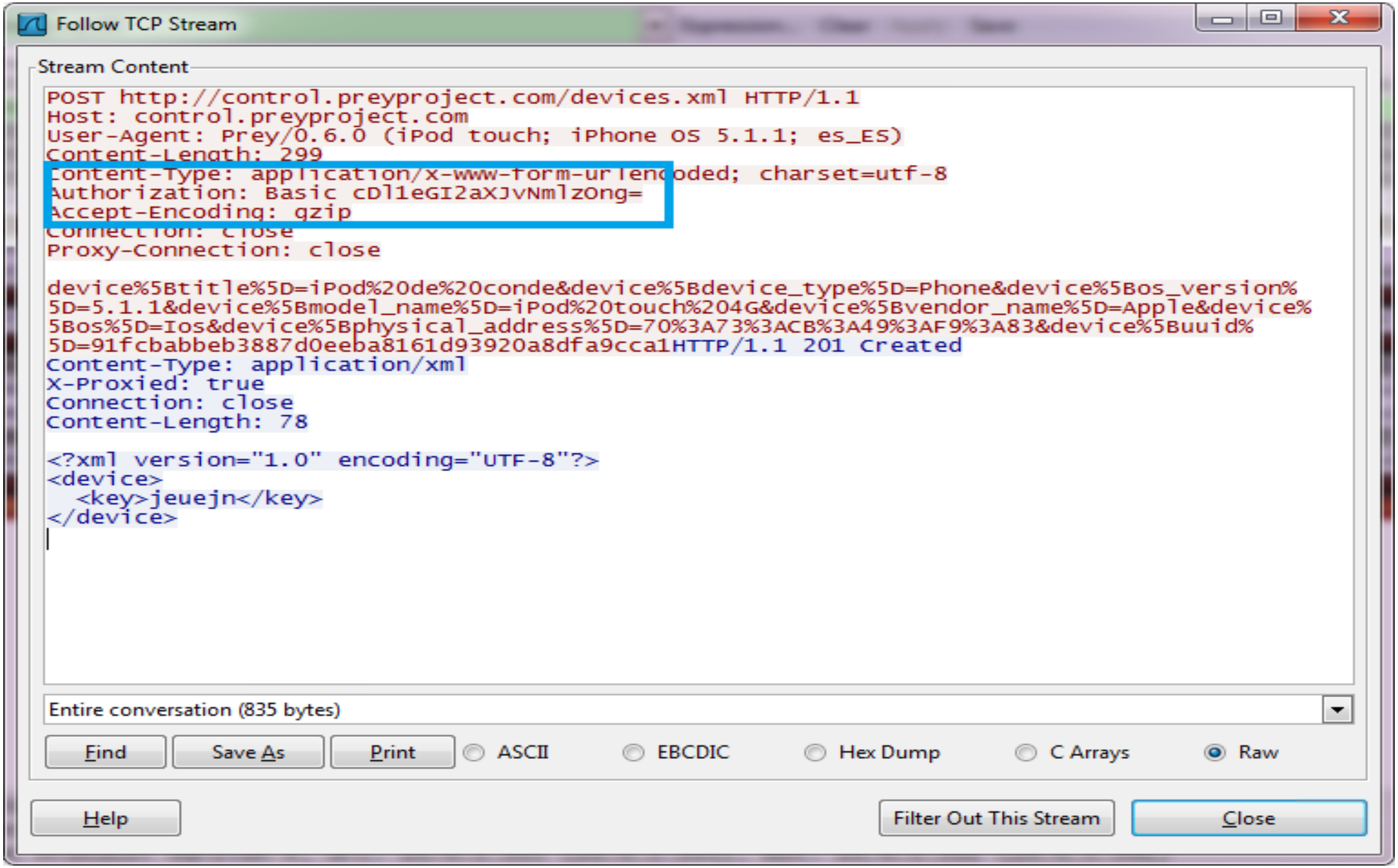


```
POST /Control/Interface/GetInfo.ashx? HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: WebQueryLib
Host: www.mitracker.com
Content-Length: 72
Cache-Control: no-cache

uname=john.hard&pword=temptemp&mac=00-0C-29-4A-F1-3A&position=&tag=queryHTTP/1.1 200 OK
Content-Length: 106
X-Powered-By: ASP.NET
X-Aspnet-Version: 4.0.30319
Server: Microsoft-IIS/7.0
Connection: close
Cache-Control: private
Date: Sun, 10 Feb 2013 11:53:17 GMT
Content-Type: text/plain; charset=utf-8

{"uname":"ok","pword":"ok","mac":"ok","ip":"213.37.127.115","email":"john.hardverga@gmai
l.com","privilege":"0","regdate":"2013-02-10","status":"0","description":"","adddate":"20
13-02-10 11:44:11"}
```

Entire conversation (702 bytes)

○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

3. CLEAR TEXT SECRETS (IN TRANSIT): PREY (IOS)



```
POST http://control.preyproject.com/devices.xml HTTP/1.1
Host: control.preyproject.com
User-Agent: Prey/0.6.0 (iPod touch; iPhone OS 5.1.1; es_ES)
Content-Length: 299
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Authorization: Basic cDl1eGI2aXJvNmlzOng=
Accept-Encoding: gzip
Connection: close
Proxy-Connection: close

device%5Btitle%5D=iPod%20de%20conde&device%5Bdevice_type%5D=Phone&device%5Bos_version%
5D=5.1.1&device%5Bmodel_name%5D=iPod%20touch%204G&device%5Bvendor_name%5D=Apple&device%
5Bos%5D=Ios&device%5Bphysical_address%5D=70%3A73%3ACB%3A49%3AF9%3A83&device%5Buuid%
5D=91fcbabbeb3887d0eeba8161d93920a8dfa9cca1HTTP/1.1 201 Created
Content-Type: application/xml
X-Proxied: true
Connection: close
Content-Length: 78

<?xml version="1.0" encoding="UTF-8"?>
<device>
  <key>jeuejn</key>
</device>
```

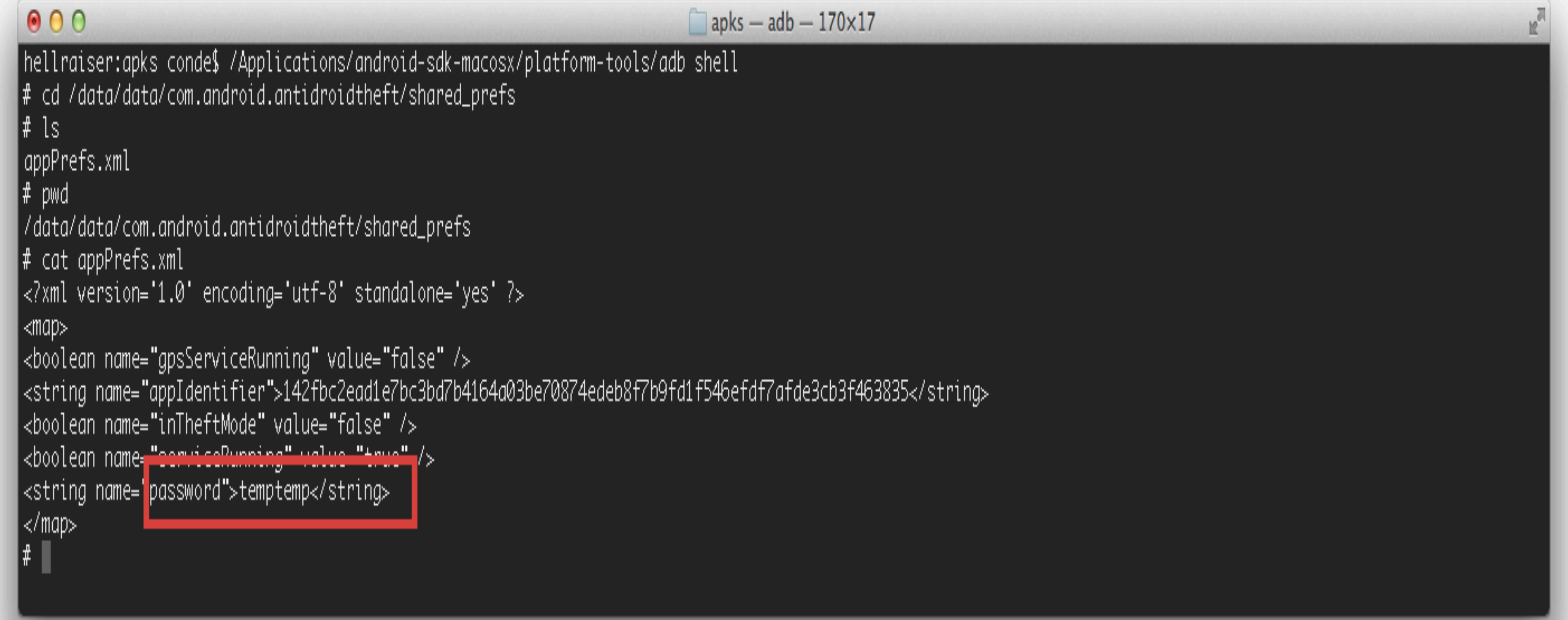
Entire conversation (835 bytes)

VULNEX

3. PHYSICAL ACCESS TO DEVICE

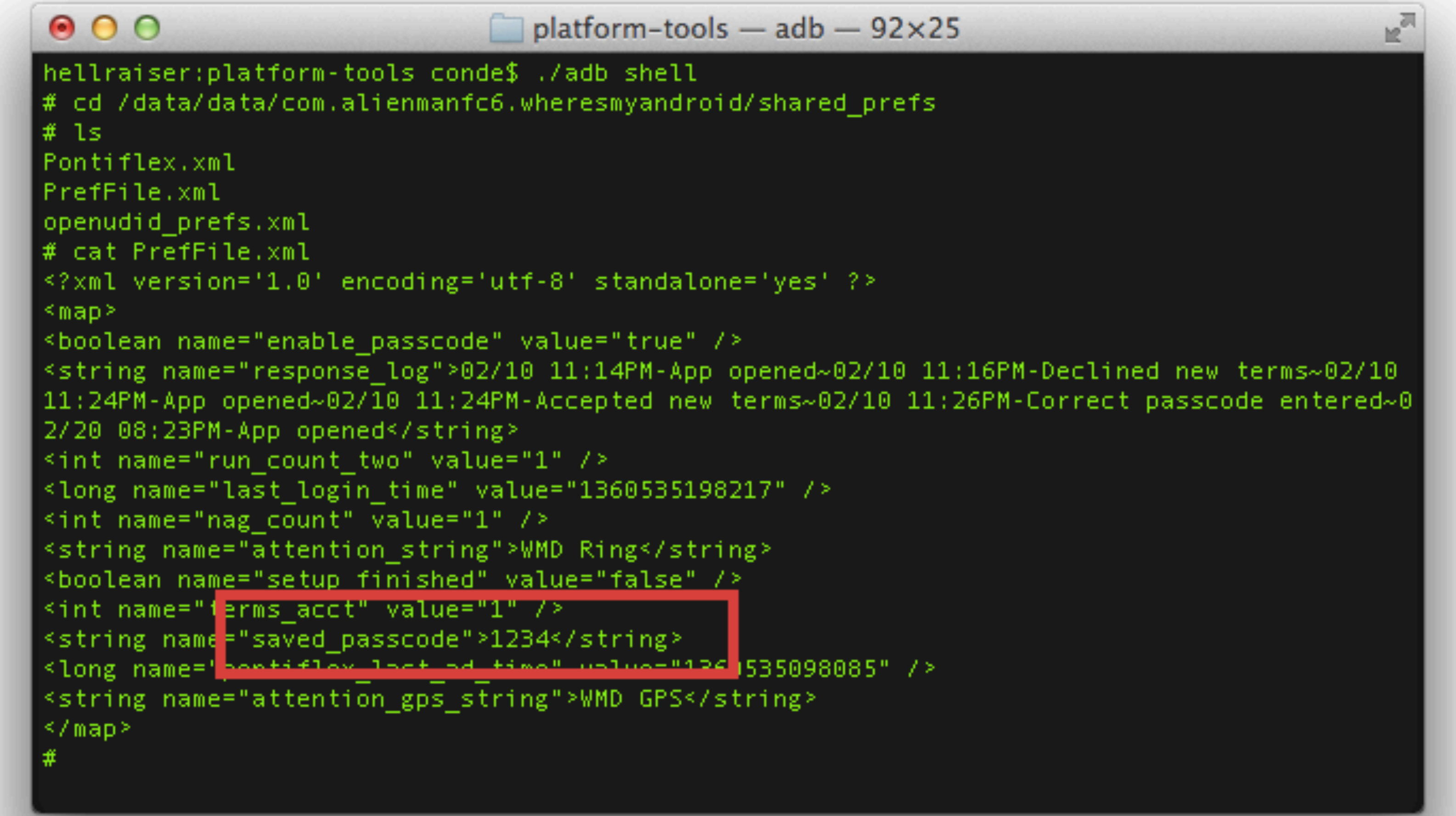
- Thief
  - Shield device in a Faraday box / bag
  - Break device security
    - Recovery modes
    - Android
      - Maybe already rooted?
      - USB debugging
    - Passcode bypass
    - Forensic LIVE CD
    - Jailbreak tools

3. CLEAR TEXT SECRETS (AT REST): ANTIDROIDTHEFT (ANDROID)



```
hellraiser:apks conde$ /Applications/android-sdk-macosx/platform-tools/adb shell
# cd /data/data/com.android.antidroidtheft/shared_prefs
# ls
appPrefs.xml
# pwd
/data/data/com.android.antidroidtheft/shared_prefs
# cat appPrefs.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="gpsServiceRunning" value="false" />
<string name="appIdentifier">142fbc2ead1e7bc3bd7b4164a03be70874edeb8f7b9fd1f546efdf7afde3cb3f463835</string>
<boolean name="inTheftMode" value="false" />
<boolean name="serviceRunning" value="true" />
<string name="password">temptemp</string>
</map>
#
```

3. CLEAR TEXT SECRETS (AT REST): WHERE’S MY DROID (ANDROID)



```
hellraiser:platform-tools conde$ ./adb shell
# cd /data/data/com.alienmanfc6.wheresmyandroid/shared_prefs
# ls
Pontiflex.xml
PrefFile.xml
openudid_prefs.xml
# cat PrefFile.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="enable_passcode" value="true" />
<string name="response_log">02/10 11:14PM-App opened~02/10 11:16PM-Declined new terms~02/10
11:24PM-App opened~02/10 11:24PM-Accepted new terms~02/10 11:26PM-Correct passcode entered~0
2/20 08:23PM-App opened</string>
<int name="run_count_two" value="1" />
<long name="last_login_time" value="1360535198217" />
<int name="nag_count" value="1" />
<string name="attention_string">WMD Ring</string>
<boolean name="setup_finished" value="false" />
<int name="terms_acct" value="1" />
<string name="saved_passcode">1234</string>
<long name="pontiflex_last_ad_time" value="1360535098085" />
<string name="attention_gps_string">WMD GPS</string>
</map>
#
```

3. ANTI-THEFT CRYPTO FAILS

- No crypto at all…
- Weak cryptographic algorithms
  - MD5 no salt
  - SHA1
- No use of crypto hardware

3. LOCK DOWN BYPASS: PREY

- DEMO

3. SECURE WIPE (AND RECOVERY) I

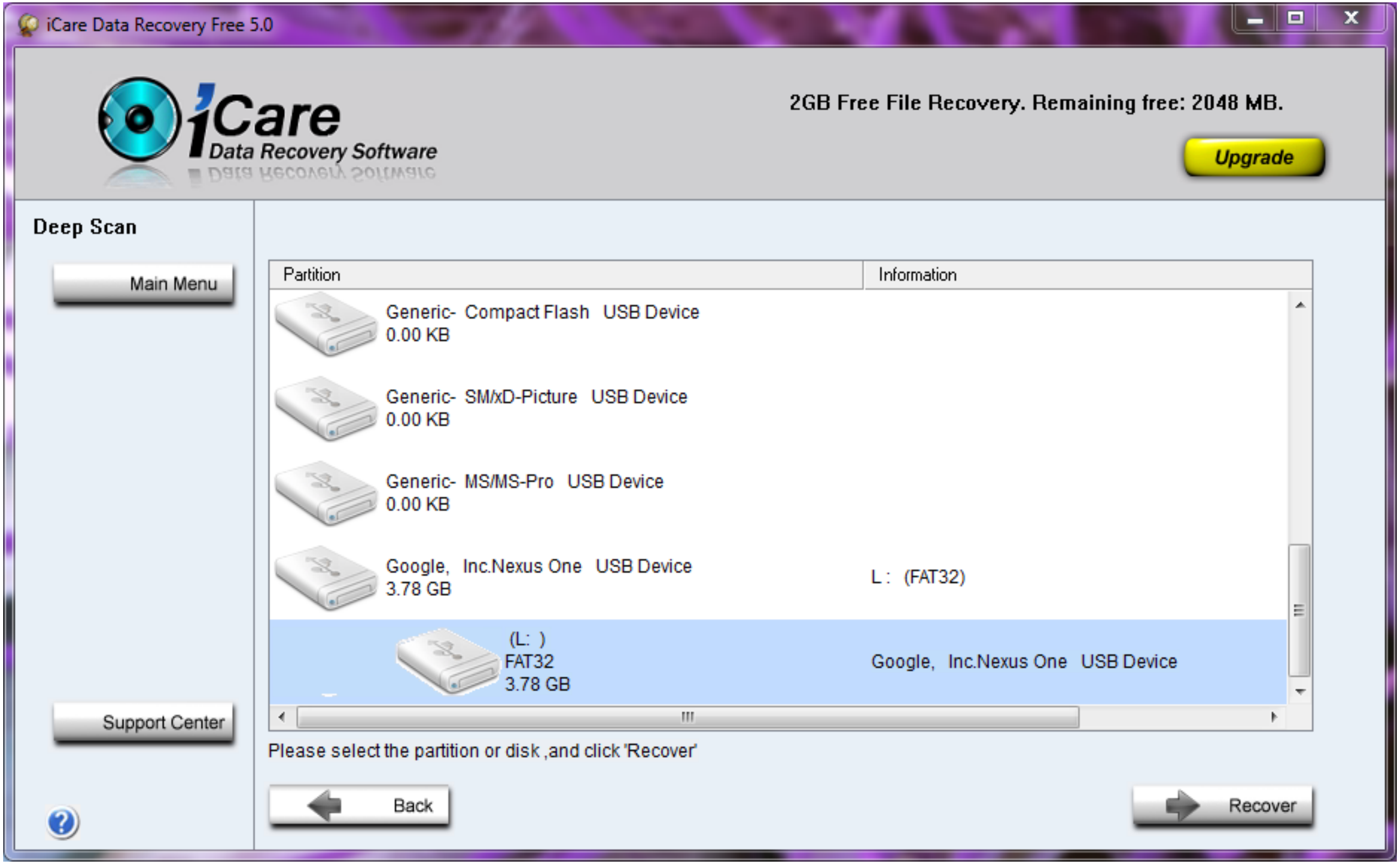
- Apps do not have secure delete capabilities, relies on a delete() call from OS

- SD Cards many times do not get deleted
  - Some Apps not configured by default

3. SECURE WIPE (AND RECOVERY) II

- Thief: Remove SD Card as soon device is stolen!
- Use forensic tools to recovered Data if device wiped
  - Windows: Use any LIVE CD/DVD forensic
  - Android
    - Open Source Android Forensics Toolkit http://sourceforge.net/projects/osaftoolkit/
    - iCare Recovery Android http://www.icare-recovery.com/free/android-data-recovery-freeware.html
  - iPhone
    - Iphone Analyzer http://sourceforge.net/projects/iphoneanalyzer/
    - iOS Forensic research http://www.iosresearch.org/

3. SECURE WIPE (AND RECOVERY) III



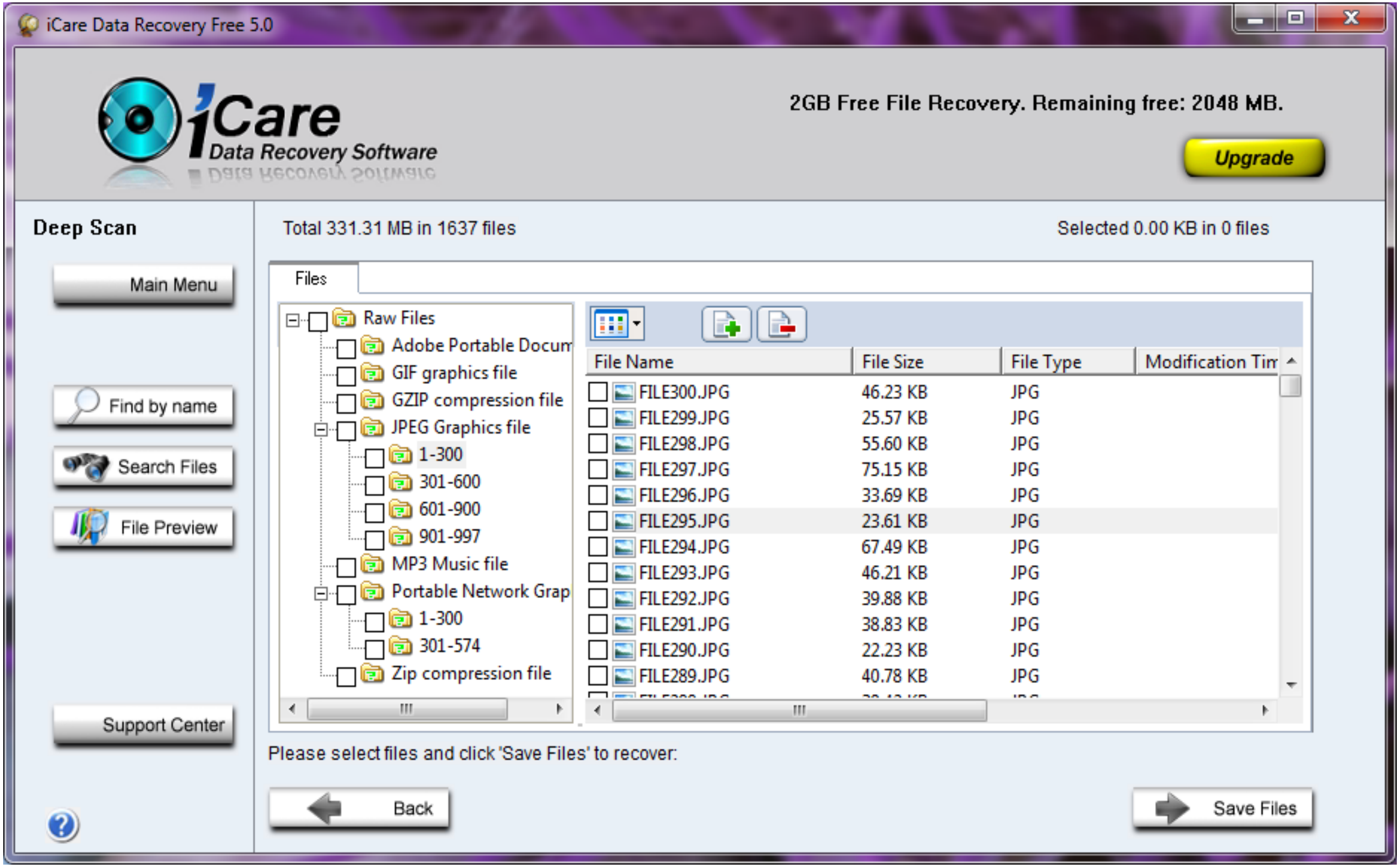
2GB Free File Recovery. Remaining free: 2048 MB.

Deep Scan

Partition	Information
Generic- Compact Flash USB Device 0.00 KB	
Generic- SM/xD-Picture USB Device 0.00 KB	
Generic- MS/MS-Pro USB Device 0.00 KB	
Google, Inc.Nexus One USB Device 3.78 GB	L : (FAT32)
(L:) FAT32 3.78 GB	Google, Inc.Nexus One USB Device

Please select the partition or disk ,and click 'Recover'

3. SECURE WIPE (AND RECOVERY) IV



2GB Free File Recovery. Remaining free: 2048 MB.

Total 331.31 MB in 1637 files

Selected 0.00 KB in 0 files

File Name	File Size	File Type	Modification Tim
□ FILE300.JPG	46.23 KB	JPG	
□ FILE299.JPG	25.57 KB	JPG	
□ FILE298.JPG	55.60 KB	JPG	
□ FILE297.JPG	75.15 KB	JPG	
□ FILE296.JPG	33.69 KB	JPG	
□ FILE295.JPG	23.61 KB	JPG	
□ FILE294.JPG	67.49 KB	JPG	
□ FILE293.JPG	46.21 KB	JPG	
□ FILE292.JPG	39.88 KB	JPG	
□ FILE291.JPG	38.83 KB	JPG	
□ FILE290.JPG	22.23 KB	JPG	
□ FILE289.JPG	40.78 KB	JPG	

Please select files and click 'Save Files' to recover:

3. JHV DEFUSER I

- “John Hard Vegas, Anti-Theft defuser”

- Features:
  - Fingerprint Anti-Theft
  - Steal credentials
  - Disable Anti-Theft

3. JHV DEFUSER II

- Current Anti-Theft apps defused (* Windows only):
  - Prey
  - LaptopLock
  - Bak2u / Phoenix
  - Snuko
  - LocateLaptop

- *More to come and other platforms…*

3. JHV DEFUSER III

- DEMO

3. INSERT ROOTKIT TO STOLEN DEVICE – SUBVERTING ANTI-THEFT

1. Stolen device

2. Shield device
3. Tamper device
4. Install Rootkit
5. Enable Anti-Theft and return device

6. User happy again ☺

VULNEX

3. THIEF CRAFT

- Disable Anti-Theft remote if possible
- Mute sound on device
- Remove SD Card
- Shield it
- Break device security
- Collect user data
- Recover deleted data

3. AVOID BEING…

4. Conclusions

4. RISKS SUMMARY

- Clear Text Secrets
  - At-Rest: Mobile Top 10 2012-M1 Insecure Data Storage
  - In-Transit: Mobile Top 10 2012 - M3 Insufficient Transport Layer Protection
- Poor Cryptographic Algorithm
  - CWE-327: Use of a Broken or Risky Cryptographic Algorithm
- Insecure Development Practices
  - Shipped with Debug
  - No data validation
  - NO SSL certification checks
- Privacy Violations
- Wiped data can be recovered (most of the time)
- Lack of Resilient & Security Defenses
- Easily defeated

4. THE UGLY TRUTH

- Anti-Theft products need to improve their security

- Some products need to change their claims

4. USER SECURITY

- Keep up on updates
- Enforce security defenses (usual suspects)
  - Firewall
  - Anti-virus
- Beware of public networks
- If Anti-Theft app installed, make sure it does what it claims!

4. ANTI-THEFT VENDORS

- Understand your threats!
- Build **secure software,** not **security software**
- Protect user data effectively

4. BE SAFE IF YOU CAN

4. Q&A

- Please fill out the Black Hat feedback form
- Thanks!