Pentesting iPhone & iPad Apps

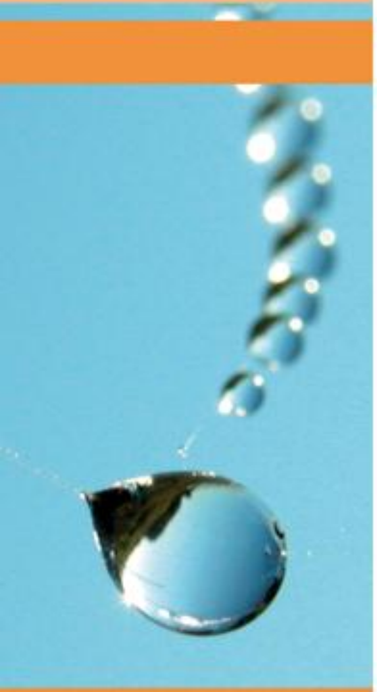
Hack In Paris 2011 – June 17

Photographie © Boris Gribov - Fotolia.com

Who are we?

- Flora Bottaccio
  - ➢ Security Analyst at ADVTOOLS
- Sebastien Andrivet
  - ➢ Director, co-founder of ADVTOOLS

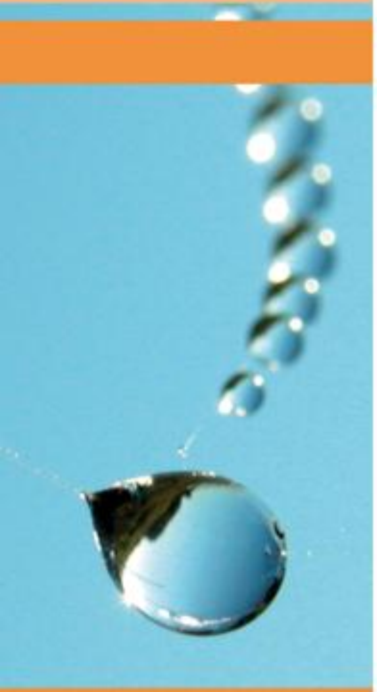
ADVTOOLS SARL



ADVTOOLS

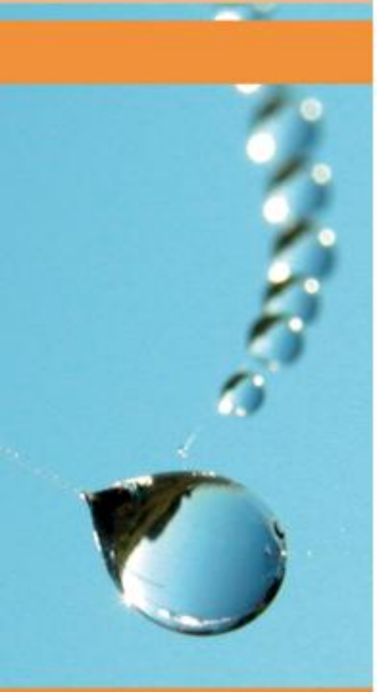
- Swiss company founded in 2002 in Geneva
- Specialized in Information Security & Problems Diagnosis
  - ➢ Pentesting
  - ➢ Security Audits
  - ➢ Forensics
  - ➢ Secure Development

ADV TOOLS SARL



Agenda

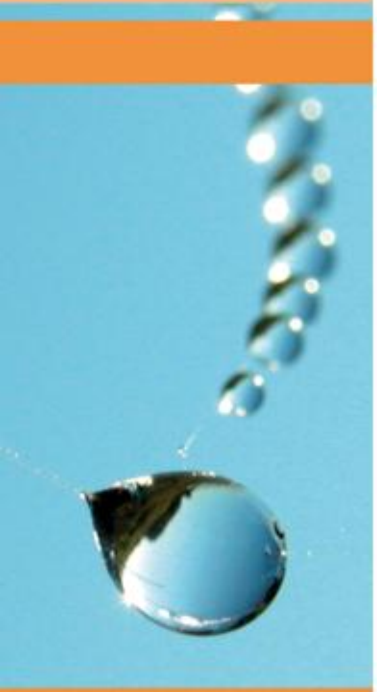
- Overviews
- Previous researches
- iPhone/iPad application pentest
  - Our methodology
- Live demonstrations
- Q&A



iOS Application Types

- Web Applications
  - ➢ HTML + CSS + Javascript
  - ➢ Run inside Safari
- Native Applications:
  - ➢ Written in Objective-C (+ C/C++)
  - ➢ Compiled into CPU code: ARM for actual devices, x86 for iOS Simulator
- MonoTouch, Adobe Flash, …
  - ➢ Written in high-level language
  - ➢ Compiled into CPU code

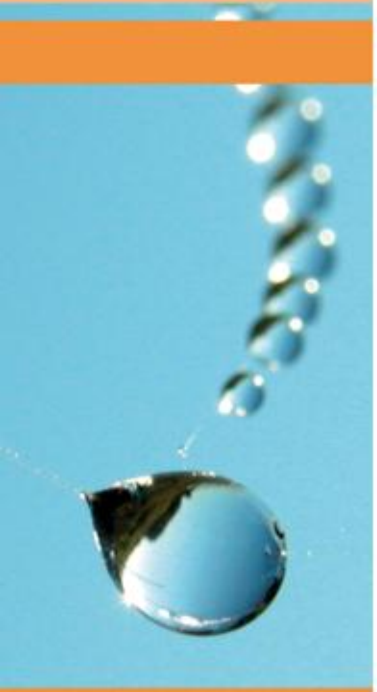
ADV TOOLS SARL



iOS Applications

- Distributed as “.ipa” files
  - in fact simply zip files
- Deployed as “.app” directories
  - like on Mac OS X
- Executable code is:
  - **encrypted** with FairPlay DRM (AES)
  - signed with Apple’s signature
  - decryption with GDB or Crackulous

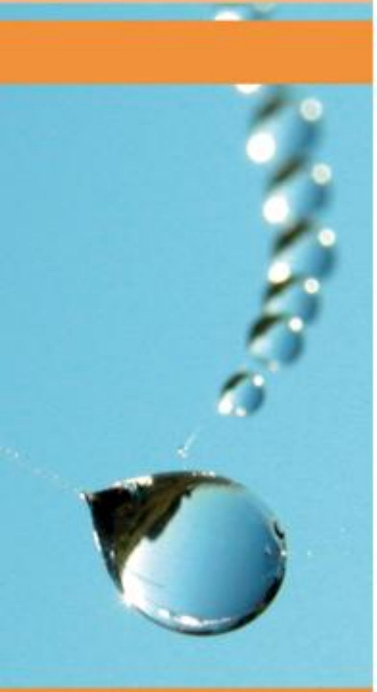
ADV TOOLS SARL



Objective-C

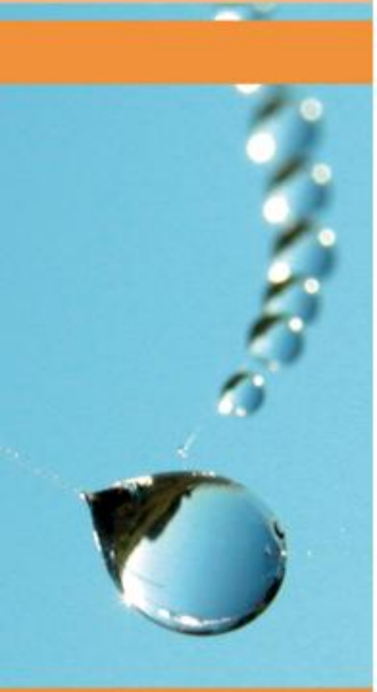
- Objective-C = C + Smalltalk
- Object oriented language
- Created in early 1980s by Stepstone
- Objective-C 2.0 released with Leopard (Mac OS X 10.5)
- Can be mixed with C and C++

ADV TOOLS SARL



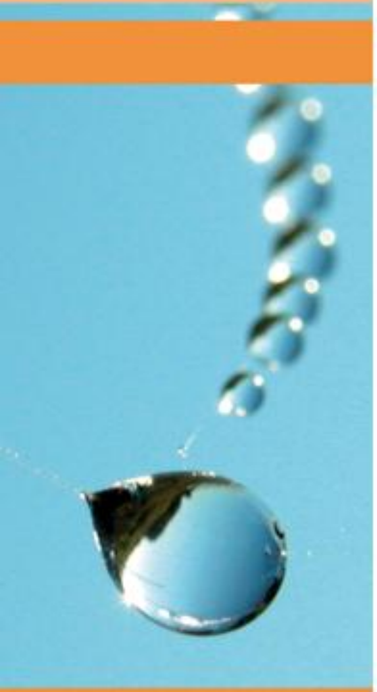
Reverse Engineering

- Not so obvious at first:
  - ARM instruction set
  - Objective-C & objc_msgSend
  - Generated code sometimes strange
  - Few (working) scripts and tools
- Finally not so difficult
- Your best friend:
  - Hex-Rays IDA Pro (Win, Mac, Linux)



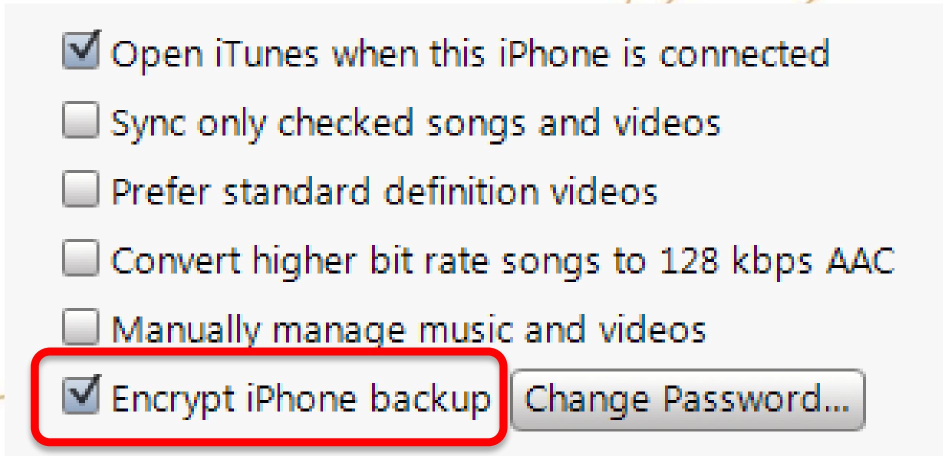
Data storage

- plist files (Property lists)
  - Used and **abused**
  - Binary (depreciated) or XML
- Sqlite 3
  - From time to time
- Keychain
- Binary data files (aka unknown)



iTunes & Backups

- Every time you connect your device to your computer, a backup is made
- Contains almost all data
- By default, **not encrypted**
- To mitigate security problems:



☑ Open iTunes when this iPhone is connected

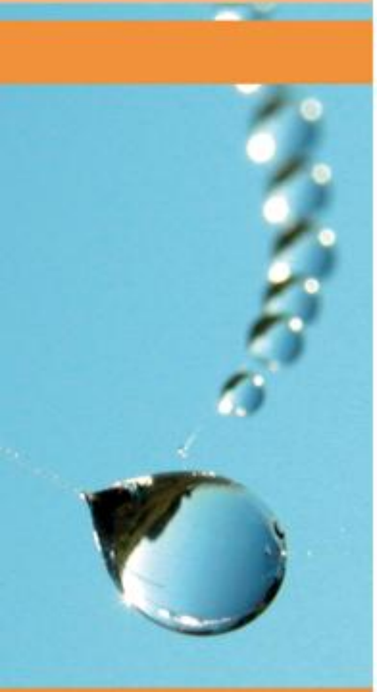
□ Sync only checked songs and videos

□ Prefer standard definition videos

□ Convert higher bit rate songs to 128 kbps AAC

□ Manually manage music and videos

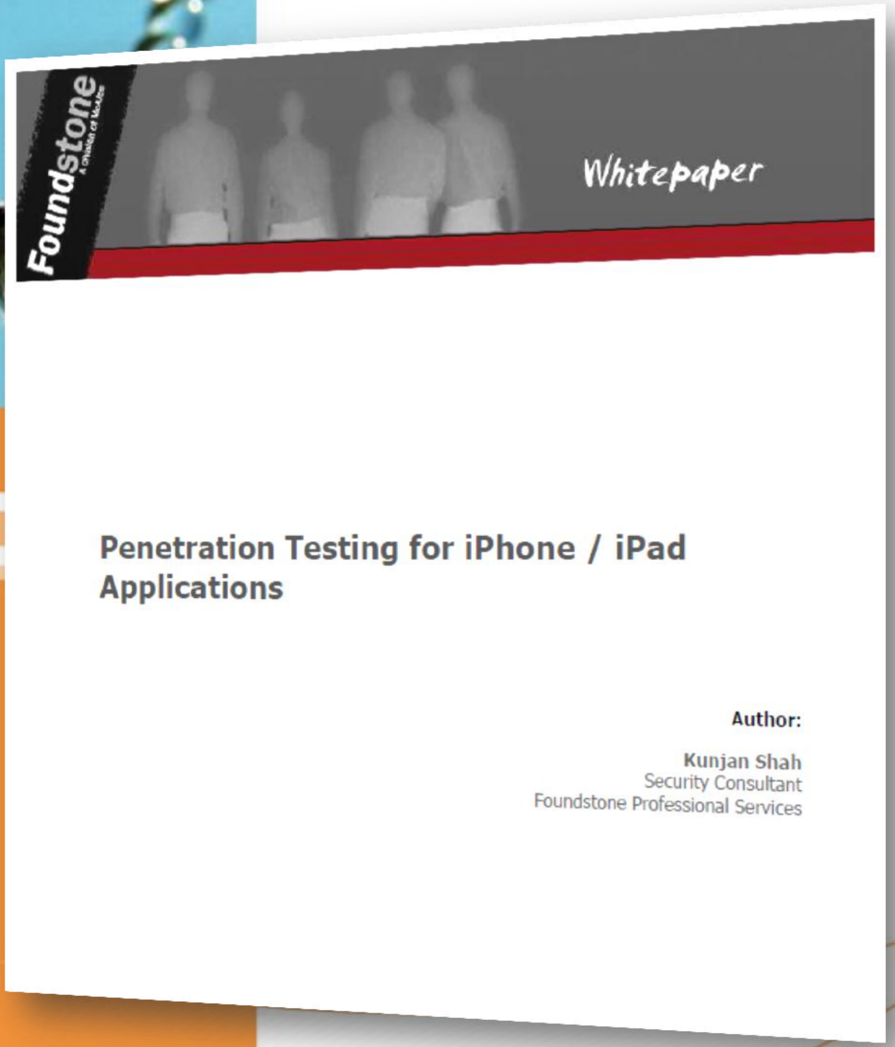
☑ Encrypt iPhone backup



Previous researches

- In general, out of date
- Often inaccurate
- But contain interesting information
- We will give here only some examples

Foundstone (McAfee / Intel)



Foundstone

Whitepaper

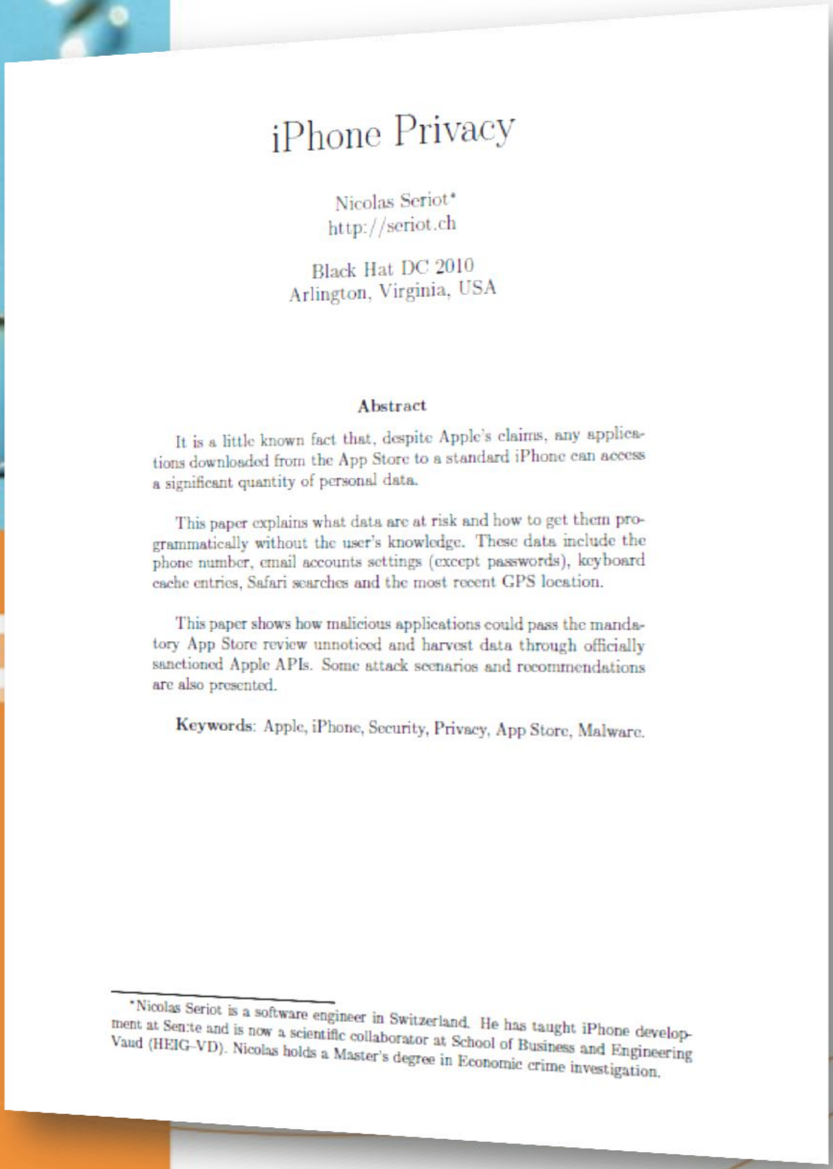
Penetration Testing for iPhone / iPad Applications

Author:

Kunjan Shah
Security Consultant
Foundstone Professional Services

- Disappointing
- Assumes a lot
- In particular, assumes you have the source code
- If you have the sources, you make a code review, not a pentest

Nicolas Seriot



iPhone Privacy

Nicolas Seriot*
http://seriot.ch

Black Hat DC 2010
Arlington, Virginia, USA

Abstract

It is a little known fact that, despite Apple's claims, any applications downloaded from the App Store to a standard iPhone can access a significant quantity of personal data.

This paper explains what data are at risk and how to get them programmatically without the user's knowledge. These data include the phone number, email accounts settings (except passwords), keyboard cache entries, Safari searches and the most recent GPS location.

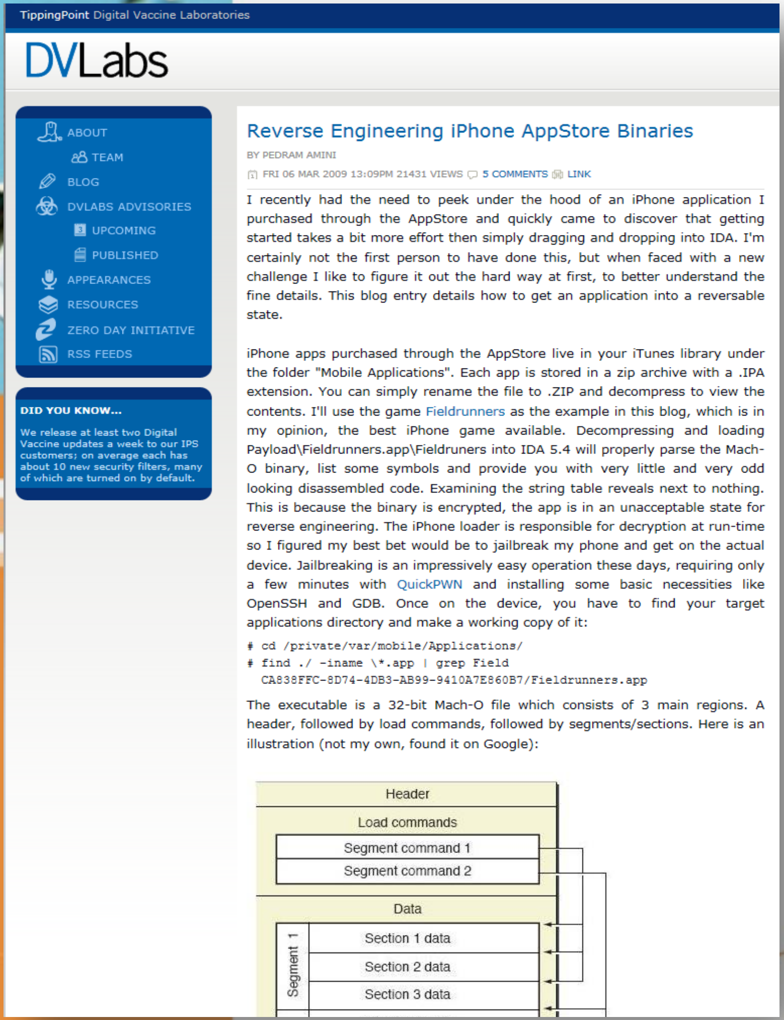
This paper shows how malicious applications could pass the mandatory App Store review unnoticed and harvest data through officially sanctioned Apple APIs. Some attack scenarios and recommendations are also presented.

Keywords: Apple, iPhone, Security, Privacy, App Store, Malware.

*Nicolas Seriot is a software engineer in Switzerland. He has taught iPhone development at Sen:te and is now a scientific collaborator at School of Business and Engineering Vaud (HEIG-VD). Nicolas holds a Master's degree in Economic crime investigation.

- Not exactly on the same subject (about privacy)
- **Excellent** source of info
- However, a little out of date (everything is quickly out of date with Apple devices)

DVLabs (TippingPoint / HP)



TippingPoint Digital Vaccine Laboratories

DVLabs

- ABOUT
  - TEAM
- BLOG
- DVLABS ADVISORIES
  - UPCOMING
  - PUBLISHED
- APPEARANCES
- RESOURCES
- ZERO DAY INITIATIVE
- RSS FEEDS

DID YOU KNOW...

We release at least two Digital Vaccine updates a week to our IPS customers; on average each has about 10 new security filters, many of which are turned on by default.

Reverse Engineering iPhone AppStore Binaries

BY PEDRAM AMINI

FRI 06 MAR 2009 13:09PM 21431 VIEWS 5 COMMENTS LINK

I recently had the need to peek under the hood of an iPhone application I purchased through the AppStore and quickly came to discover that getting started takes a bit more effort then simply dragging and dropping into IDA. I'm certainly not the first person to have done this, but when faced with a new challenge I like to figure it out the hard way at first, to better understand the fine details. This blog entry details how to get an application into a reversable state.

iPhone apps purchased through the AppStore live in your iTunes library under the folder "Mobile Applications". Each app is stored in a zip archive with a .IPA extension. You can simply rename the file to .ZIP and decompress to view the contents. I'll use the game Fieldrunners as the example in this blog, which is in my opinion, the best iPhone game available. Decompressing and loading Payload\Fieldrunners.app\Fieldruners into IDA 5.4 will properly parse the Mach-O binary, list some symbols and provide you with very little and very odd looking disassembled code. Examining the string table reveals next to nothing. This is because the binary is encrypted, the app is in an unacceptable state for reverse engineering. The iPhone loader is responsible for decryption at run-time so I figured my best bet would be to jailbreak my phone and get on the actual device. Jailbreaking is an impressively easy operation these days, requiring only a few minutes with QuickPWN and installing some basic necessities like OpenSSH and GDB. Once on the device, you have to find your target applications directory and make a working copy of it:

```
# cd /private/var/mobile/Applications/
# find ./ -iname \*.app | grep Field
  CA838FFC-8D74-4DB3-AB99-9410A7E860B7/Fieldrunners.app
```

The executable is a 32-bit Mach-O file which consists of 3 main regions. A header, followed by load commands, followed by segments/sections. Here is an illustration (not my own, found it on Google):

- Our starting point for decryption of apps
- Old (2009), some assumptions no more valid

ARTeam

ARTeam
the international bank of knowledge

Pri

PATCHING APPLICATIONS FROM APPLE'S APPSTORE WITH ADDITIONAL PROTECTION

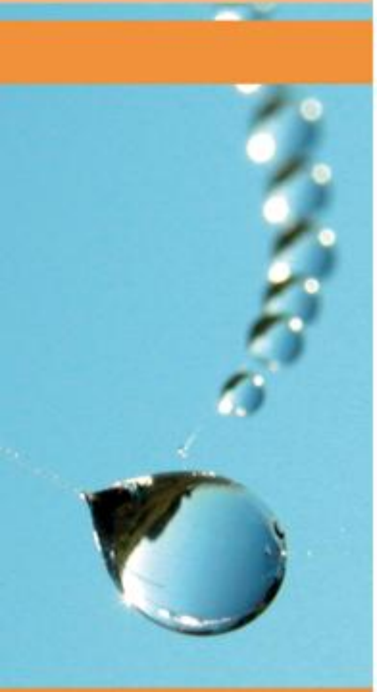
ADV TOOLS SARL

- About cracking, not pentesting
- **Brilliant**
- But very old now (2008 & 2009)

Previous Researches

- Some interesting documents available
- Nothing specifically about pentesting iOS application and that is realistic and useable
- This is one of the reasons we make this presentation today

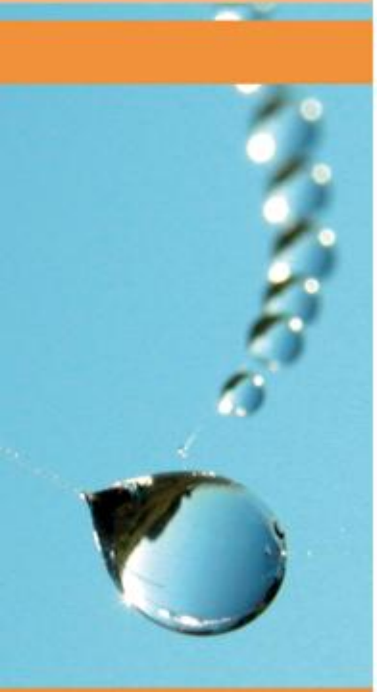
ADV TOOLS SARL



Pentesting iOS Applications

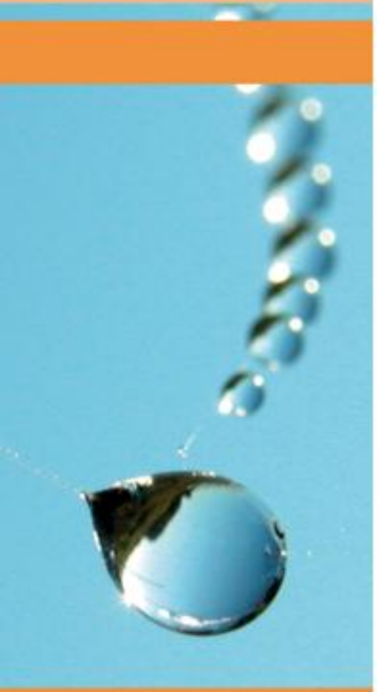
- **Step 1**: Preparing a device
- **Step 2**: Preparing a workstation
- **Step 3**: Preparing a network
- **Step 4**: Pentesting
- **Step 5**: Report

ADV TOOLS SARL



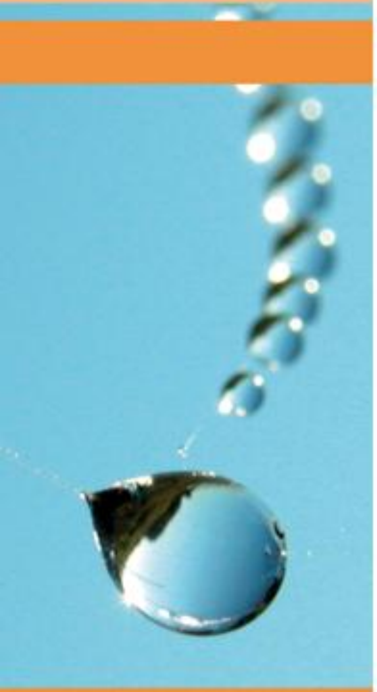
Step 1: Device

- Dedicated iPhone or iPad
- Jailbreak
  - ➢ Avoid iPad 2 for the moment
- Install tools



Tools

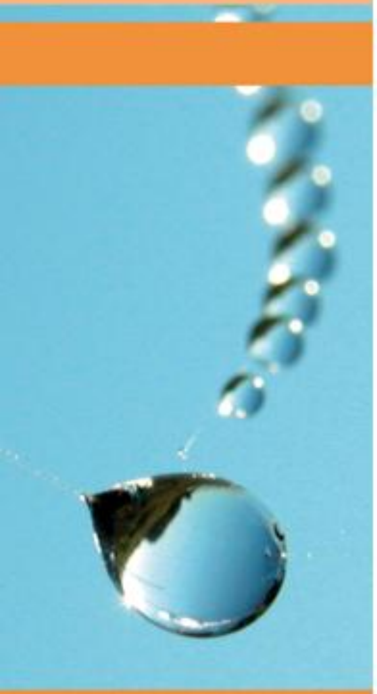
- Cydia
- APT 0.7 Strict
- adv-cmds
- Darwin CC Tools
- GNU Debugger
- inetutils
- lsof
- MobileTerminal
- netcat
- network-cmds
- nmap
- OpenSSH
- tcpdump
- top
- wget
- Crackulous



Default Passwords

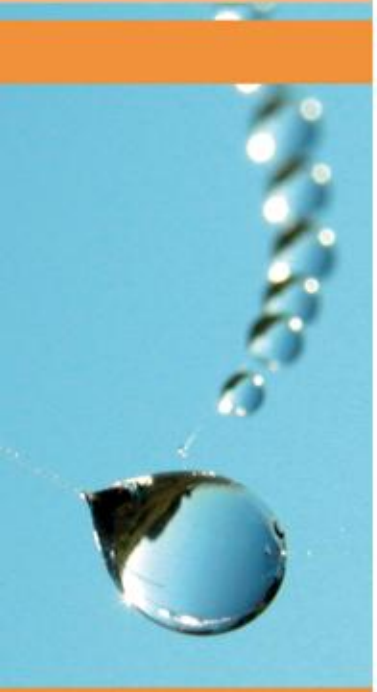
- By default, there are two users:
  - root
  - mobile
- Passwords = alpine
- **Be sure to change them:**
  - passwd
  - passwd mobile

Step 2 : Workstation



- Windows:
  - OK
- Mac OS X (Snow Leopard)
  - Better
- Linux, FreeBSD, …
  - Good luck!
  - Possible but you will need a Windows to run some tools (virtual machine…)

ADV TOOLS SARL



Some Tools

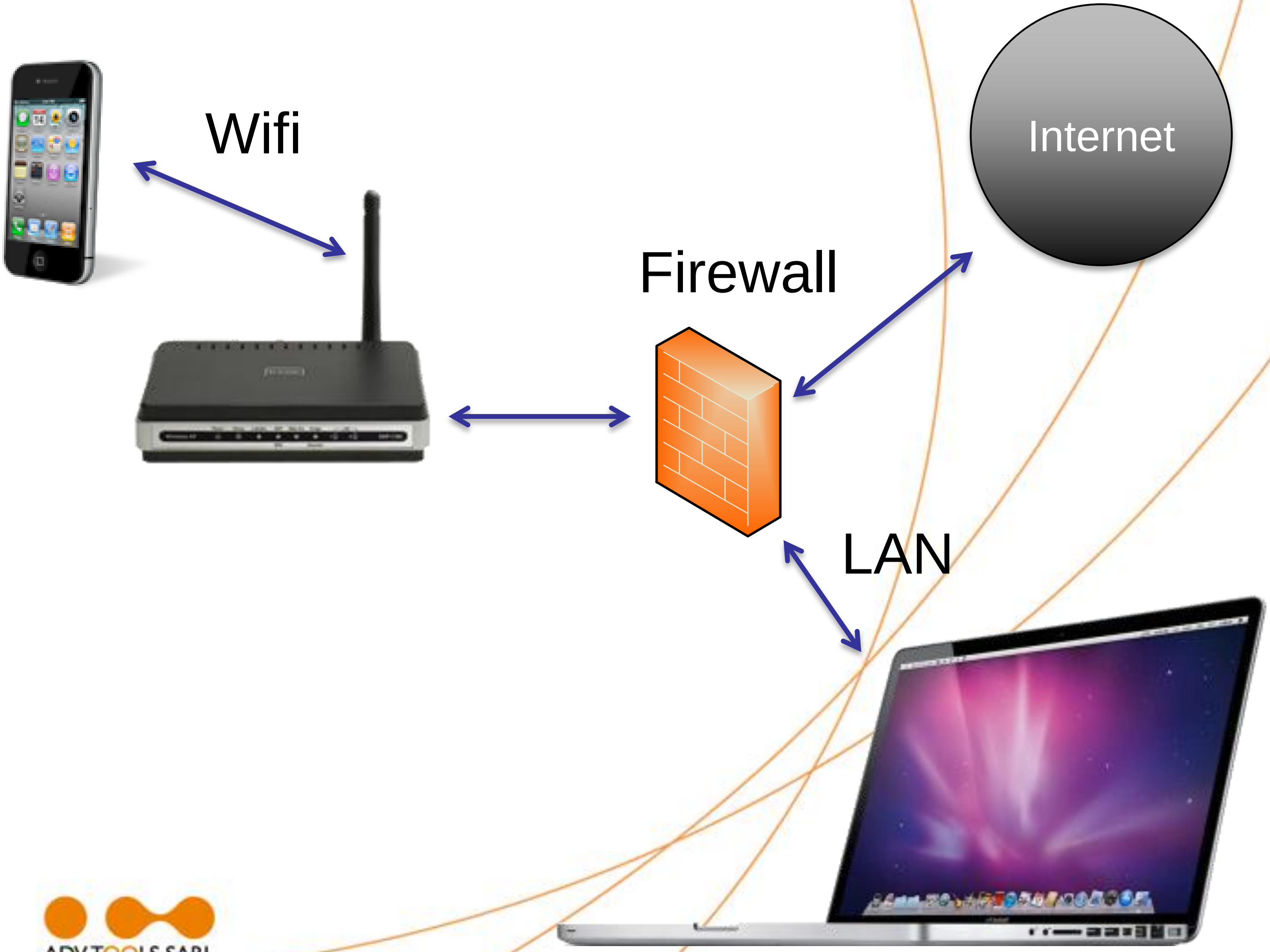
- Windows:
  - SecureCRT or Putty, WinSCP
  - plist Editor for Windows
- Mac OS X:
  - ssh, SecureCRT, Cyberduck
  - XCode
- Windows / Mac:
  - SQLite Database Browser
  - Apple iPhone Configuration Utility
  - Wireshark
  - Burp / Webscarab / …
  - IDA Pro (+ ARM decompiler)

Our Tools

- **ADVsock2pipe**
  - Remote network captures (Windows)
- **ADVinterceptor 2.0**
  - Communications interception
  - DNS & Web Servers
- Will be released in June, 2011
- GPLv3

ADV TOOLS SARL

Step 3: Network



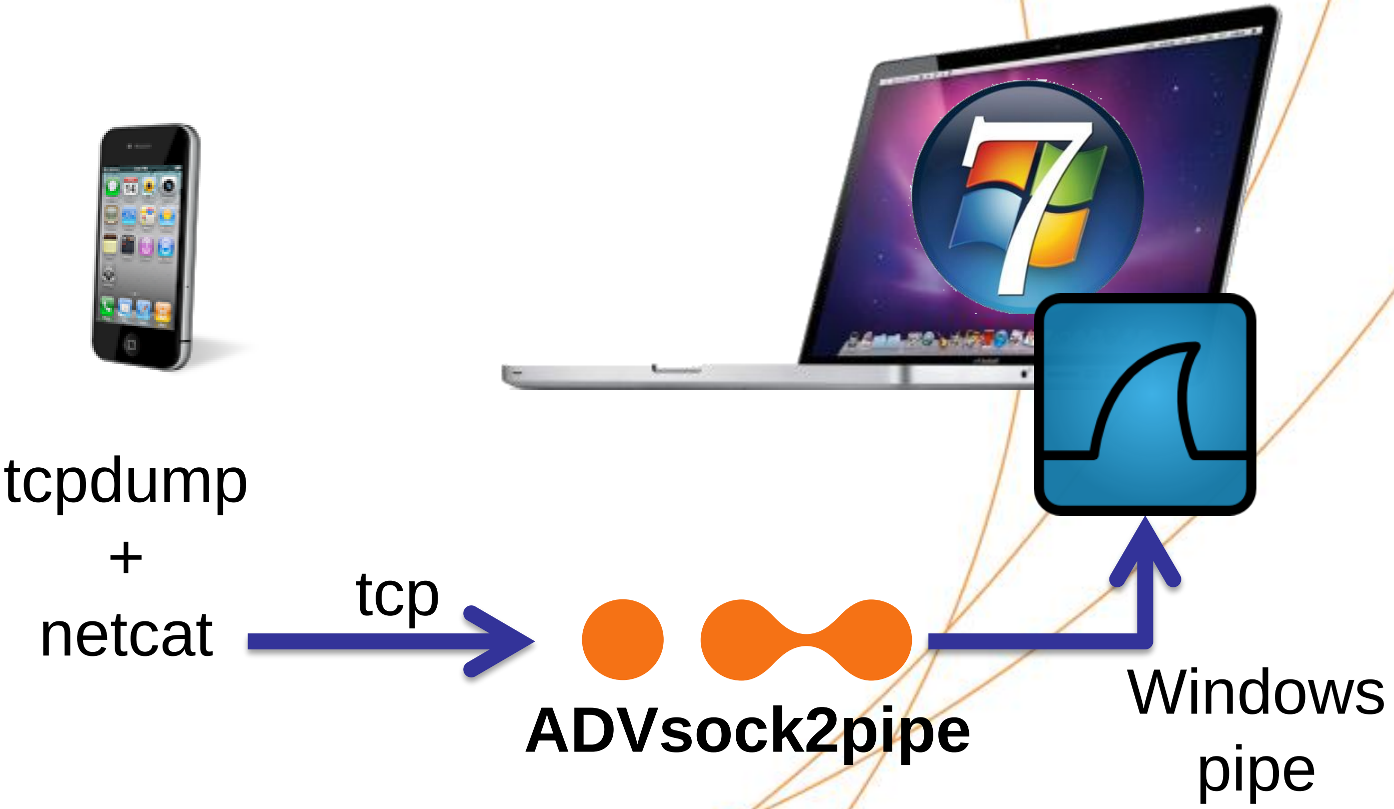
ADV TOOLS SARL

Step 4: Pentesting

- **Step A**: Install app. from iTunes
- **Step B**: Reconnaissance (passive)
  - B.1: Network capture
  - B.2: Interception
  - B.3: Artifacts
  - B.4: Decrypt + Reverse engineering
- **Step C**: Attack (active)
  - C.1: Interception + tampering

ADV TOOLS SARL

B.1: Network Capture



tcpdump
+
netcat

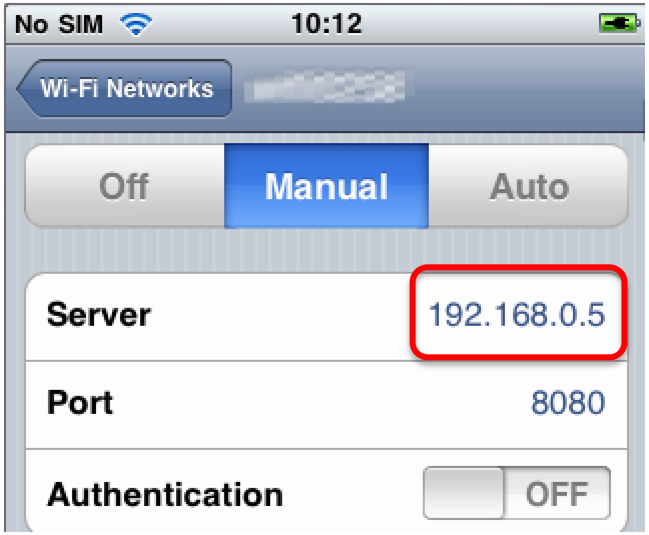
tcp

ADVsock2pipe

Windows
pipe

ADV TOOLS SARL

B.2: Interception
Proxy method



No SIM 10:12

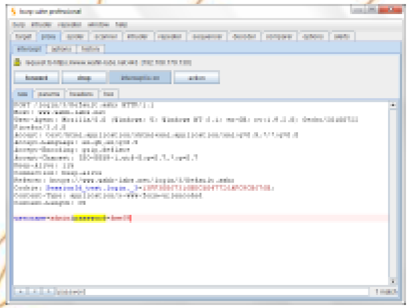
Wi-Fi Networks

Server 192.168.0.5

Port 8080

Authentication OFF

Proxy →

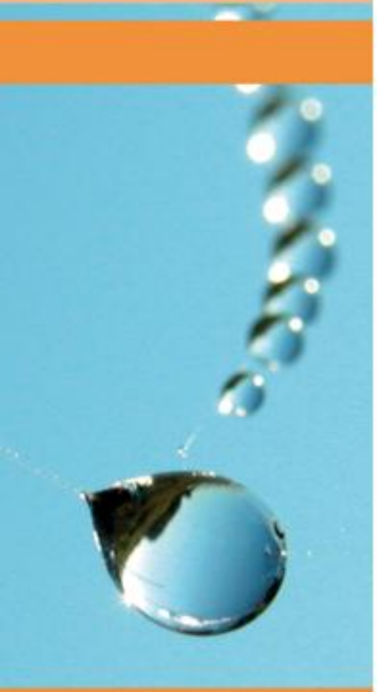


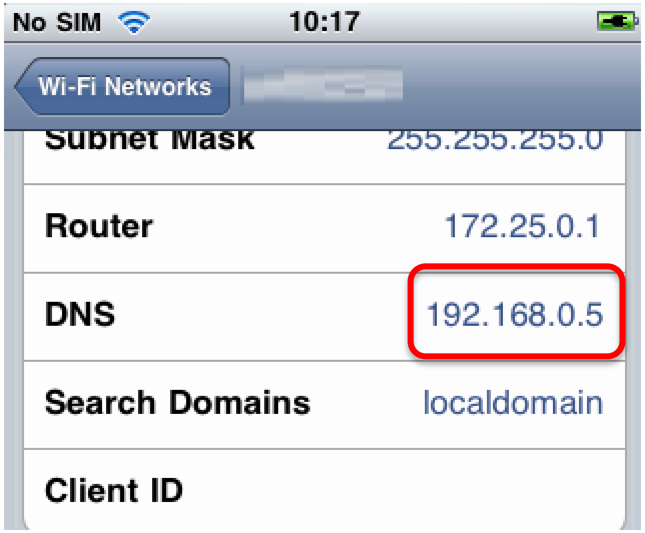
Burp Suite Pro
WebScarab
…

ADV TOOLS SARL

B.2: Interception

ADVinterceptor

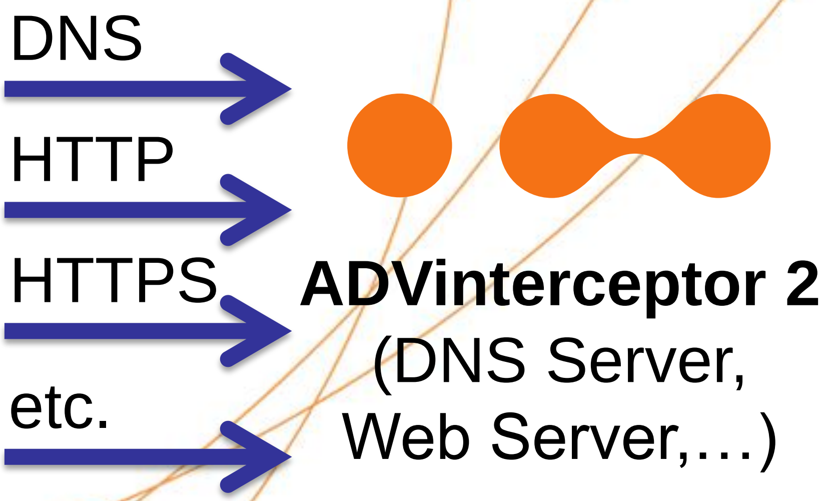




No SIM 10:17

Wi-Fi Networks [redacted]

Subnet Mask	255.255.255.0
Router	172.25.0.1
DNS	192.168.0.5
Search Domains	localdomain
Client ID	



DNS

HTTP

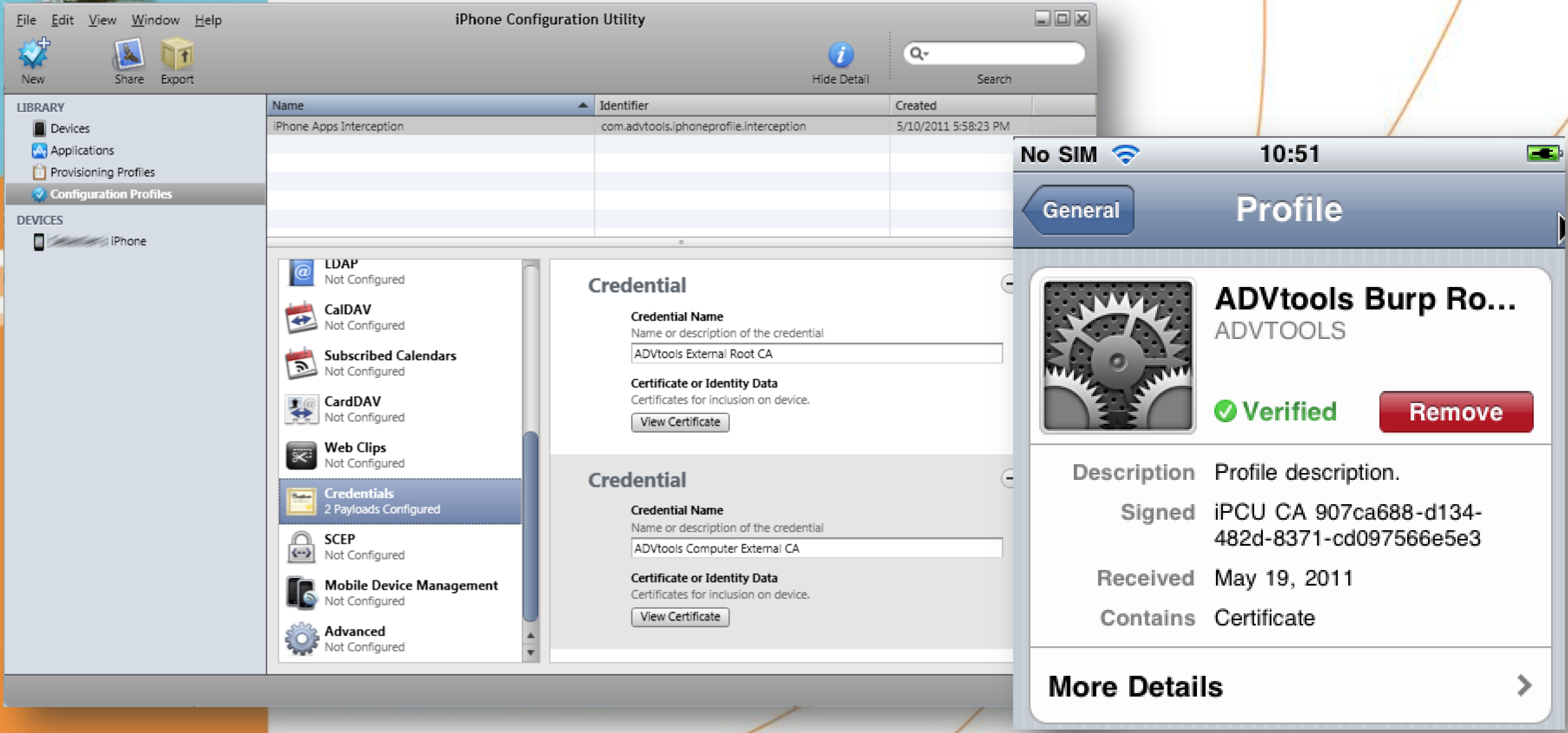
HTTPS

etc.

ADVinterceptor 2
(DNS Server,
Web Server,…)

Inject SSL Certificates

- Root from Burp or ADVinterceptor
- Use Apple iPhone Configuration



Name	Identifier	Created
iPhone Apps Interception	com.advtools.iphoneprofile.interception	5/10/2011 5:58:23 PM

Credential

Credential Name
Name or description of the credential
ADVtools External Root CA

Certificate or Identity Data
Certificates for inclusion on device.
View Certificate

Credential

Credential Name
Name or description of the credential
ADVtools Computer External CA

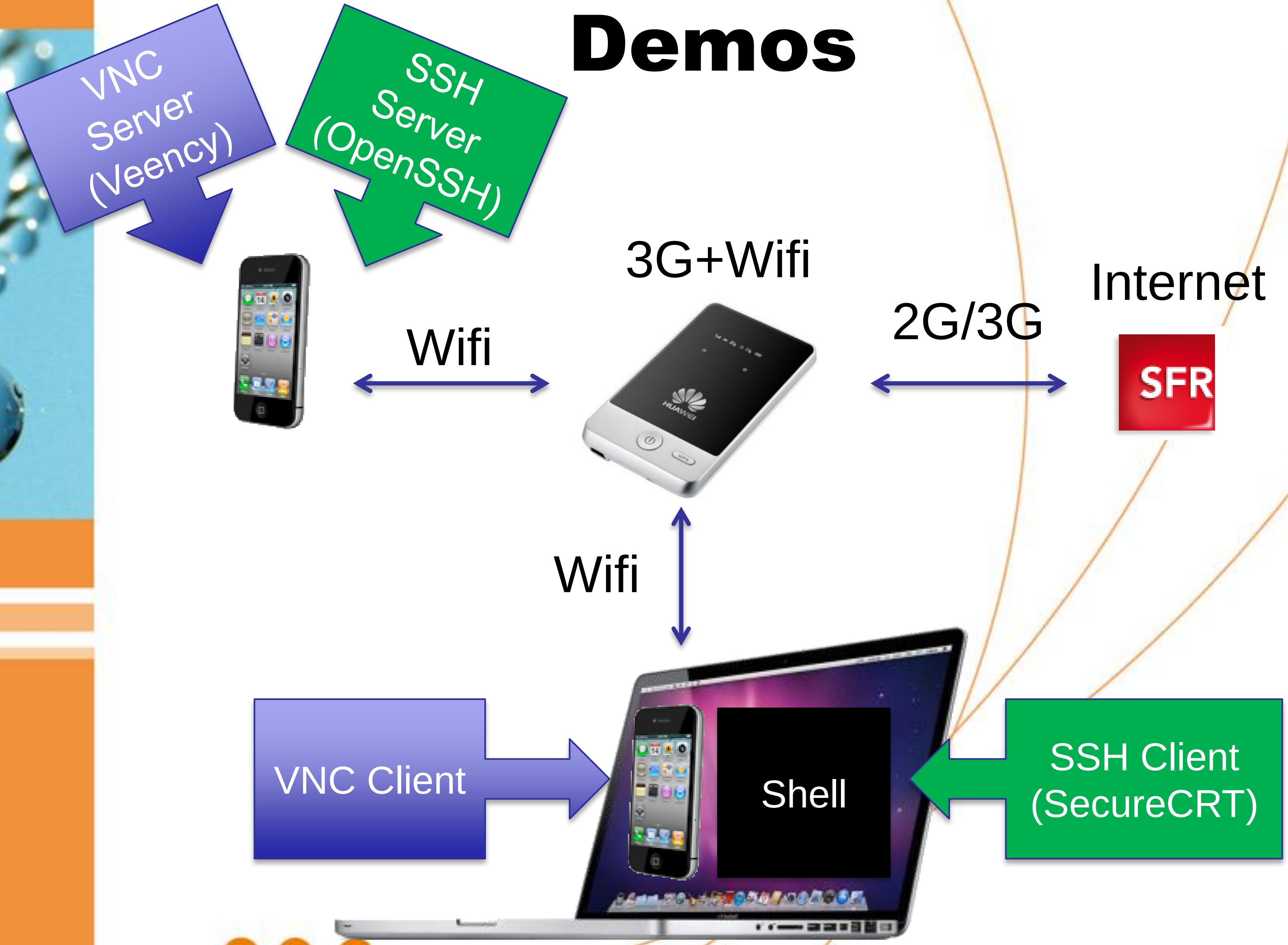
Certificate or Identity Data
Certificates for inclusion on device.
View Certificate

ADVtools Burp Ro...
ADVTOOLS
✓ Verified
Remove

Description Profile description.
Signed iPCU CA 907ca688-d134-482d-8371-cd097566e5e3
Received May 19, 2011
Contains Certificate

More Details ›

Demos



VNC Server (Veency)

SSH Server (OpenSSH)

3G+Wifi

Internet

Wifi

2G/3G

Wifi

VNC Client

Shell

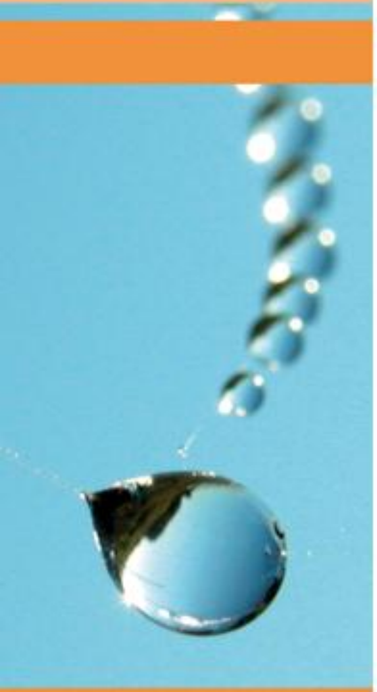
SSH Client (SecureCRT)

ADVTOOLS SARL

Windows 7 on Mac Book

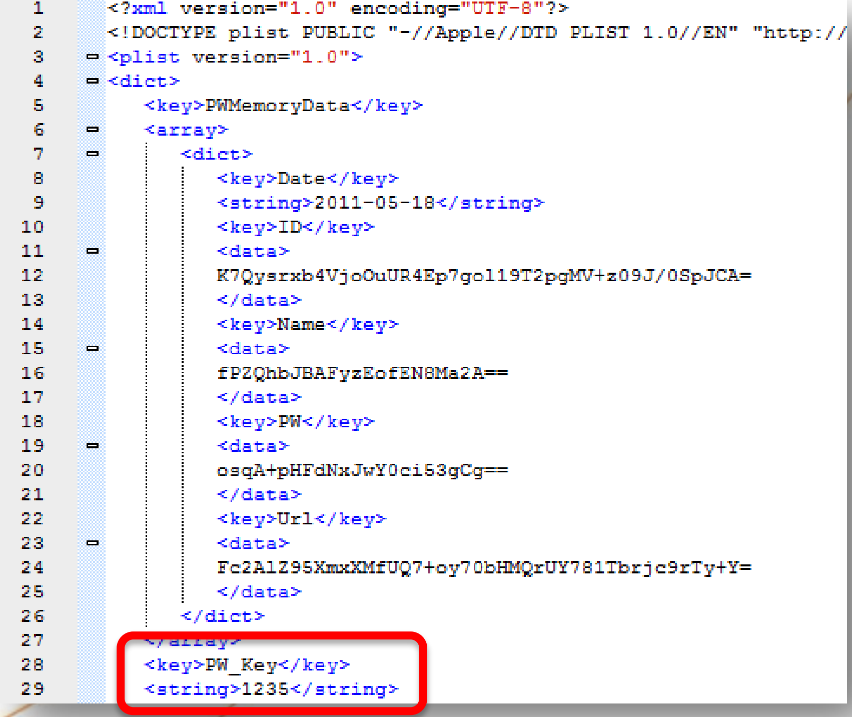
Demos

- Goal is to illustrate the previous points, not to make a complete pentest
- This is also to show the catastrophic level of security of some iOS apps



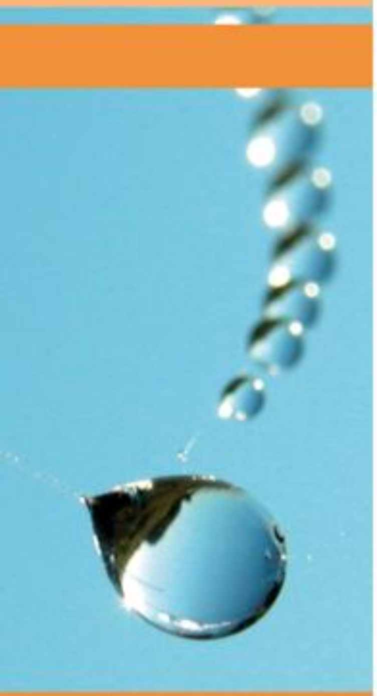
Demo # 1

- An application that stores "securely" password
- Data are encrypted… except the password



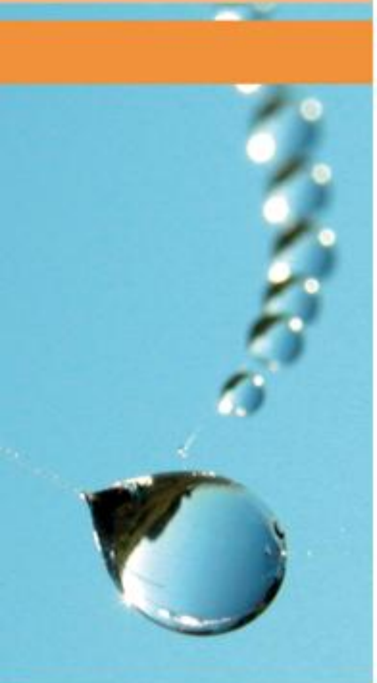
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
<plist version="1.0">
<dict>
    <key>PWMemoryData</key>
    <array>
        <dict>
            <key>Date</key>
            <string>2011-05-18</string>
            <key>ID</key>
            <data>
            K7Qysrxb4VjoOuUR4Ep7gol19T2pgMV+z09J/0SpJCA=
            </data>
            <key>Name</key>
            <data>
            fPZQhbJBAFyzEofEN8Ma2A==
            </data>
            <key>PW</key>
            <data>
            osqA+pHFdNxJwY0ci53gCg==
            </data>
            <key>Url</key>
            <data>
            Fc2A1Z95XmxXMfUQ7+oy70bHMQrUY781Tbrjc9rTy+Y=
            </data>
        </dict>
    </array>
    <key>PW_Key</key>
    <string>1235</string>
```

ADV TOOLS SARL



Demo # 2

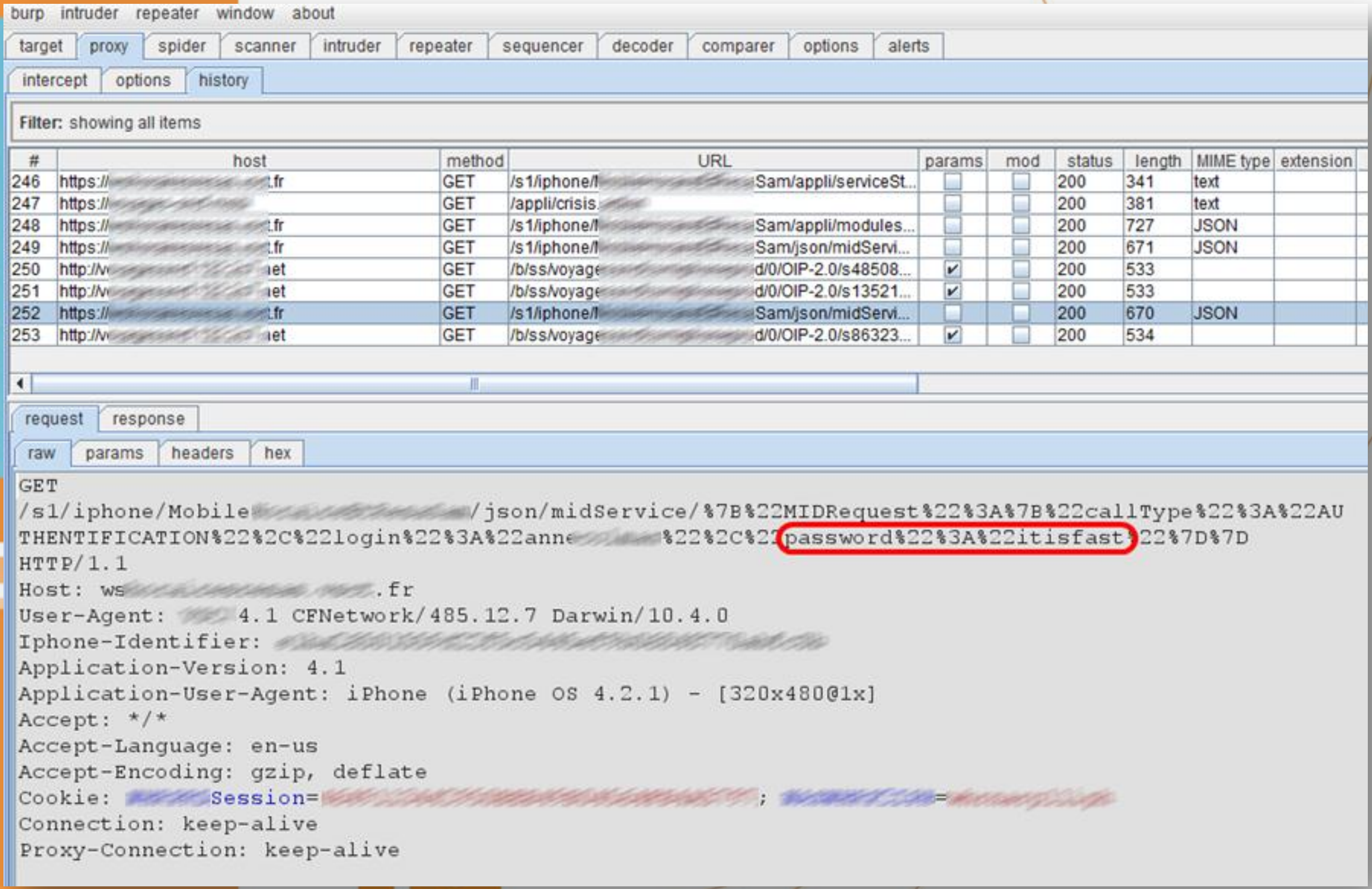
- Network capture with
  - tcpdump
  - netcap
  - ADVsock2pipe
  - Wireshark



Demo # 3

- French application (passengers)
- Interception with proxy method & Burp
- Password in clear inside the SSL tunnel: not really a problem
- Password also in clear in a file (Property List): not good

ADV TOOLS SARL

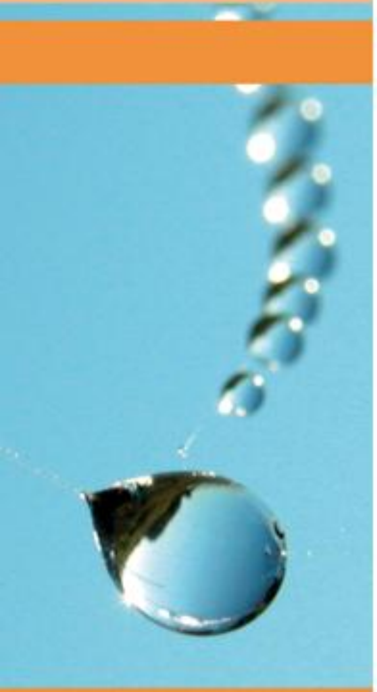

burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
request response
raw params headers hex

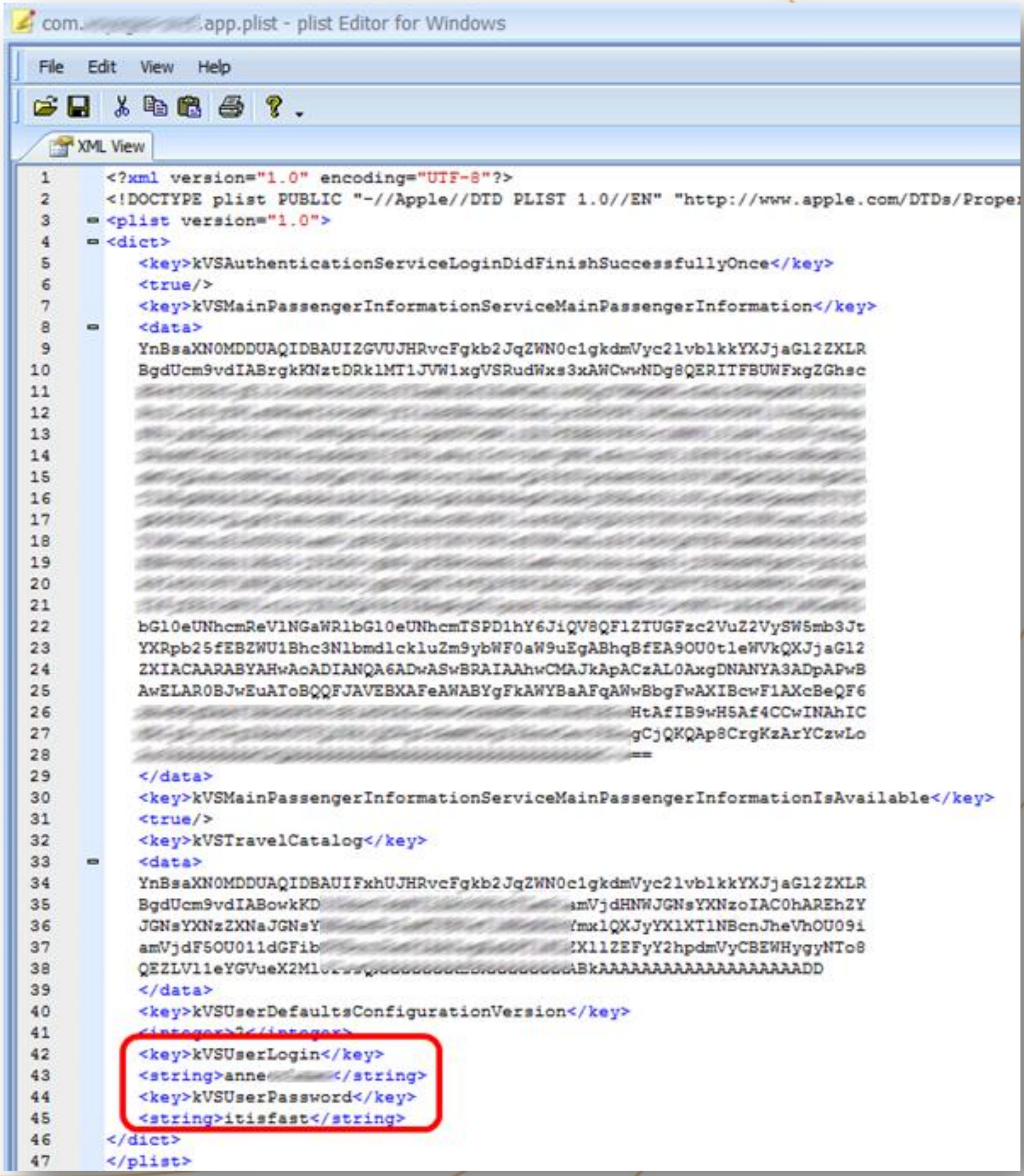
Filter: showing all items

#	host	method	URL	params	mod	status	length	MIME type	extension
246	https://[redacted].fr	GET	/s1/iphone/[redacted]Sam/appli/serviceSt...	□	□	200	341	text	
247	https://[redacted]	GET	/appli/crisis.[redacted]	□	□	200	381	text	
248	https://[redacted].fr	GET	/s1/iphone/[redacted]Sam/appli/modules...	□	□	200	727	JSON	
249	https://[redacted].fr	GET	/s1/iphone/[redacted]Sam/json/midServi...	□	□	200	671	JSON	
250	http://w[redacted]et	GET	/b/ss/voyage[redacted]d/0/OIP-2.0/s48508...	☑	□	200	533		
251	http://w[redacted]et	GET	/b/ss/voyage[redacted]d/0/OIP-2.0/s13521...	☑	□	200	533		
252	https://[redacted].fr	GET	/s1/iphone/[redacted]Sam/json/midServi...	□	□	200	670	JSON	
253	http://w[redacted]et	GET	/b/ss/voyage[redacted]d/0/OIP-2.0/s86323...	☑	□	200	534		

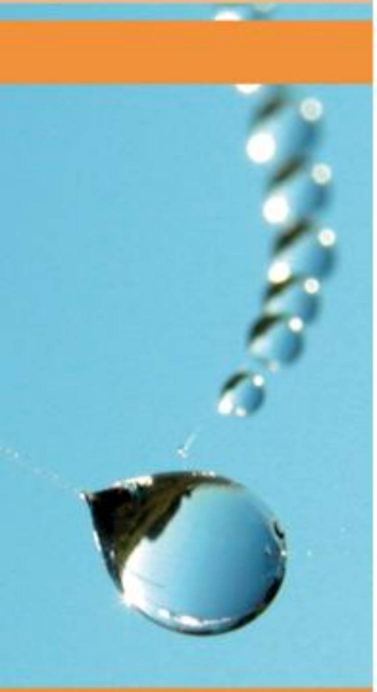
```
GET
/s1/iphone/Mobile[redacted]/json/midService/%7B%22MIDRequest%22%3A%7B%22callType%22%3A%22AU
THENTIFICATION%22%2C%22login%22%3A%22anne[redacted]%22%2C%22password%22%3A%22itisfast%22%7D%7D
HTTP/1.1
Host: ws[redacted].fr
User-Agent: [redacted] 4.1 CFNetwork/485.12.7 Darwin/10.4.0
Iphone-Identifier: [redacted]
Application-Version: 4.1
Application-User-Agent: iPhone (iPhone OS 4.2.1) - [320x480@1x]
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: [redacted]Session=[redacted]; [redacted]=[redacted]
Connection: keep-alive
Proxy-Connection: keep-alive
```

ADV TOOLS SARL





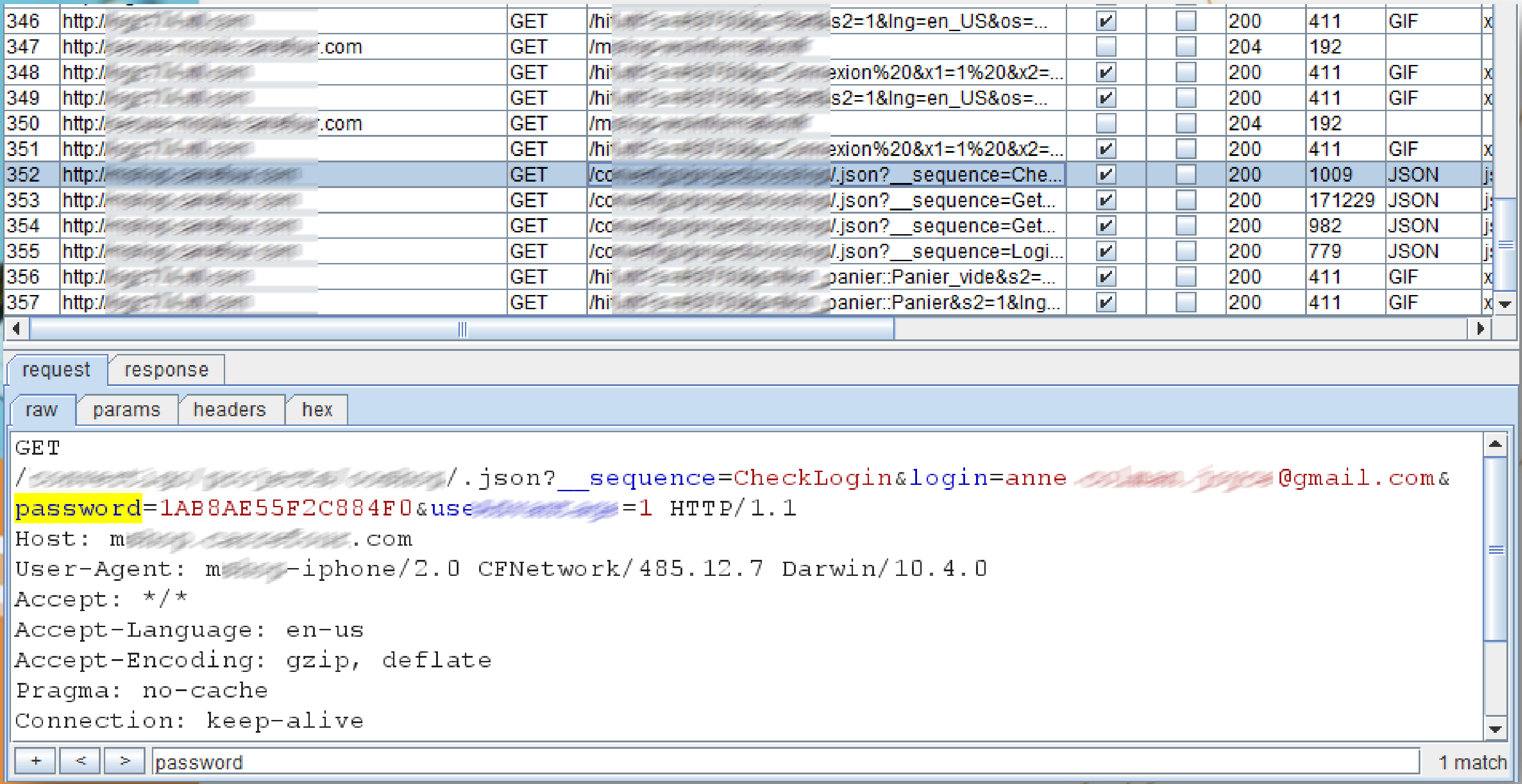
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/Proper
<plist version="1.0">
<dict>
    <key>kVSAuthenticationServiceLoginDidFinishSuccessfullyOnce</key>
    <true/>
    <key>kVSMainPassengerInformationServiceMainPassengerInformation</key>
    <data>
    YnBsaXN0MDDUAQIDBAUIZGVUJHRvcFgkb2JqZWN0c1gkdmVyc2lvblkkYXJjaGl2ZXLR
    BgdUcm9vdIABrgkKNztDRklMT1JVW1xgVSRudWxs3xAWCwwNDg8QERITFBUWFxgZGhsc
    [redacted]
    bGl0eUNhcmReVlNGaWRlbGl0eUNhcmTSPD1hY6JiQV8QFlZTUGFzc2VuZ2VySW5mb3Jt
    YXRpb25fEBZWU1Bhc3NlbmdlckluZm9ybWF0aW9uEgABhqBfEA9OU0tleWVkQXJjaGl2
    ZXIACAARABYAHwAoADIANQA6ADwASwBRAIAAhwCMAJkApACzAL0AxgDNANYA3ADpAPwB
    AwELAR0BJwEuAToBQQFJAVEBXAFeAWABYgFkAWYBaAFqAWwBbgFwAXIBcwF1AXcBeQF6
    [redacted]HtAfIB9wH5Af4CCwINAhIC
    gCjQKQAp8CrgKzArYCzwLo
    ==
    </data>
    <key>kVSMainPassengerInformationServiceMainPassengerInformationIsAvailable</key>
    <true/>
    <key>kVSTravelCatalog</key>
    <data>
    YnBsaXN0MDDUAQIDBAUIFxhUJHRvcFgkb2JqZWN0c1gkdmVyc2lvblkkYXJjaGl2ZXLR
    BgdUcm9vdIABowkKD[redacted]amVjdHNWJGNsYXNzoIAC0hAREhZY
    JGNsYXNzZXNaJGNsY[redacted]YmxlQXJyYXlXT1NBcnJheVhOU09i
    amVjdF5OU011dGFib[redacted]ZX11ZEFyY2hpdmVyCBEWHygyNTo8
    QEZLV11eYGVueX2M1[redacted]ABkAAAAAAAAAAAAAAAAAAADD
    </data>
    <key>kVSUserDefaultsConfigurationVersion</key>
    <integer>2</integer>
    <key>kVSUserLogin</key>
    <string>anne[redacted]</string>
    <key>kVSUserPassword</key>
    <string>itisfast</string>
</dict>
</plist>
```



Demo # 4

- French retailer
- Interception with
  - ADVinterceptor + Burp
- No SSL
- First message (CheckLogin)
  - Password “encrypted” with CRC64
- Second message (Login)
  - Password in clear!

ADV TOOLS SARL



346	http://[redacted]	GET	/hi[redacted]s2=1&lng=en_US&os=...	☑	□	200	411	GIF	x
347	http://[redacted].com	GET	/m[redacted]	□	□	204	192		
348	http://[redacted]	GET	/hi[redacted]exion%20&x1=1%20&x2=...	☑	□	200	411	GIF	x
349	http://[redacted]	GET	/hi[redacted]s2=1&lng=en_US&os=...	☑	□	200	411	GIF	x
350	http://[redacted].com	GET	/m[redacted]	□	□	204	192		
351	http://[redacted]	GET	/hi[redacted]exion%20&x1=1%20&x2=...	☑	□	200	411	GIF	x
352	http://[redacted]	GET	/co[redacted]/.json?__sequence=Che...	☑	□	200	1009	JSON	j
353	http://[redacted]	GET	/co[redacted]/.json?__sequence=Get...	☑	□	200	171229	JSON	j
354	http://[redacted]	GET	/co[redacted]/.json?__sequence=Get...	☑	□	200	982	JSON	j
355	http://[redacted]	GET	/co[redacted]/.json?__sequence=Logi...	☑	□	200	779	JSON	j
356	http://[redacted]	GET	/hi[redacted]panier::Panier_vide&s2=...	☑	□	200	411	GIF	x
357	http://[redacted]	GET	/hi[redacted]panier::Panier&s2=1&lng...	☑	□	200	411	GIF	x

```
GET
/[redacted]/.json?__sequence=CheckLogin&login=anne [redacted]@gmail.com&
password=1AB8AE55F2C884F0&use[redacted]=1 HTTP/1.1
Host: m[redacted].com
User-Agent: m[redacted]-iphone/2.0 CFNetwork/485.12.7 Darwin/10.4.0
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Pragma: no-cache
Connection: keep-alive
```

Thank you

To contact us:

flora@advtools.com

sebastien@advtools.com

www.advtools.com

ADV TOOLS SARL