Healthcare Cybersecurity Community

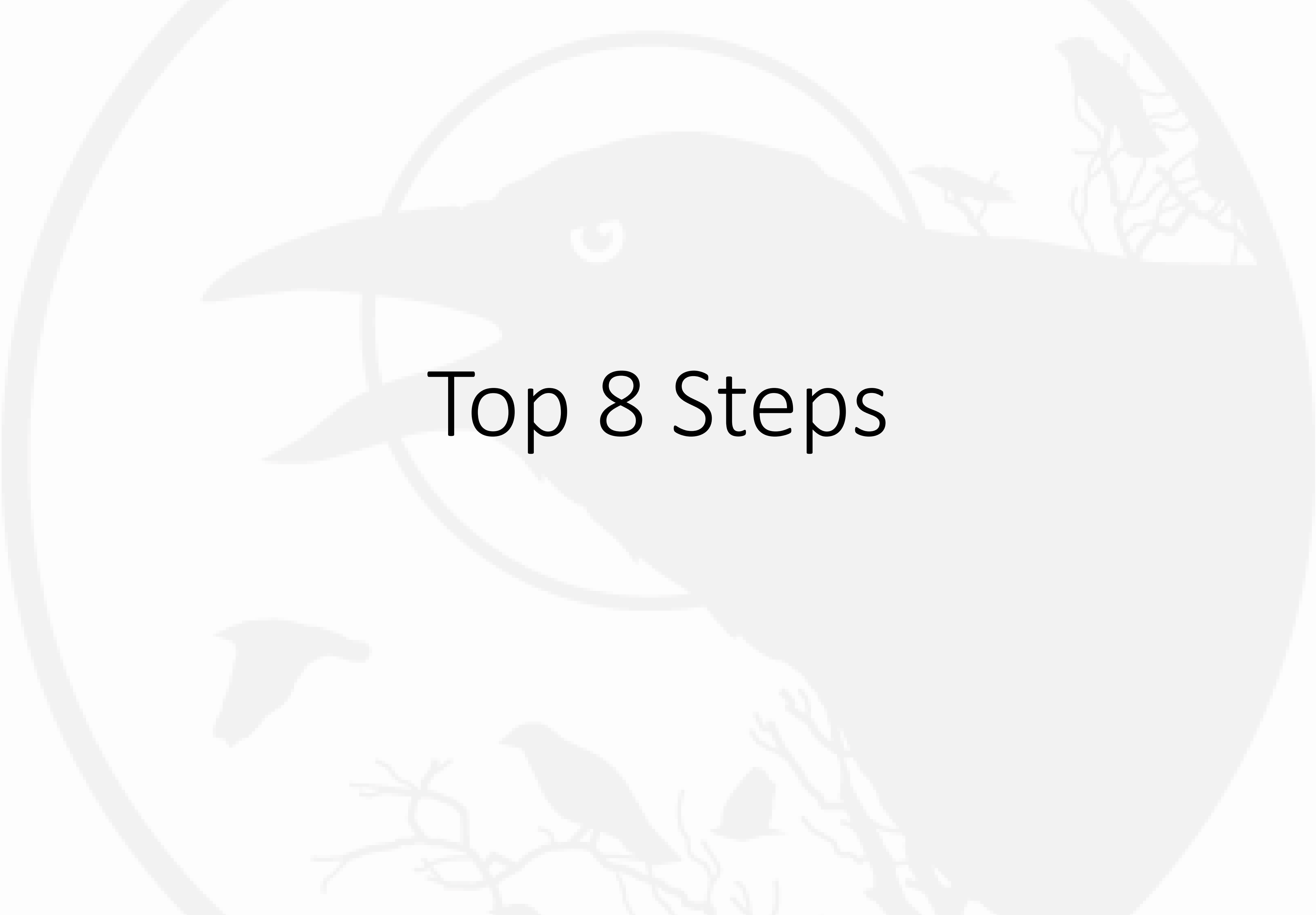
September 22, 2016

HIMSS
transforming health through IT

Top 8 Steps for Mobile - Application Assessment

Christopher Crowley

@CCrowMontance



Top 8 Steps

Top 8 Mobile Device Security Steps

1. Enforce Device Passcode Authentication
2. Monitoring Mobile Device Access and Use
3. Patching Mobile Devices
4. Prohibit Unapproved Third-Party Application Stores
5. Control Physical Access
6. Evaluate Application Security Compliance
7. Prepare an Incident Response Plan for Lost or Stolen Mobile Devices
8. Implement Management and Operational Support

Each of These 8 Steps Are Important

- Each step needs to be:
    - Considered
    - Planned
    - Executed
    - Maintained
- We’ll focus on Application Assessment today
- But there are plenty of other items for your mobile deployment

Application Assessment

Application Assessment

Considerations

Consideration for Application Assessment

- Consider what your objectives are:
  - Maintain access to organization data
  - Detect / Prevent loss of data
  - Detect / Prevent unauthorized modification to data
- Leverage employee assets for work purposes?
- Protect organizationally owned assets?
- Assist employees to protect personal devices?

Application Assessment

Planning

Planning – What is (Un)Acceptable

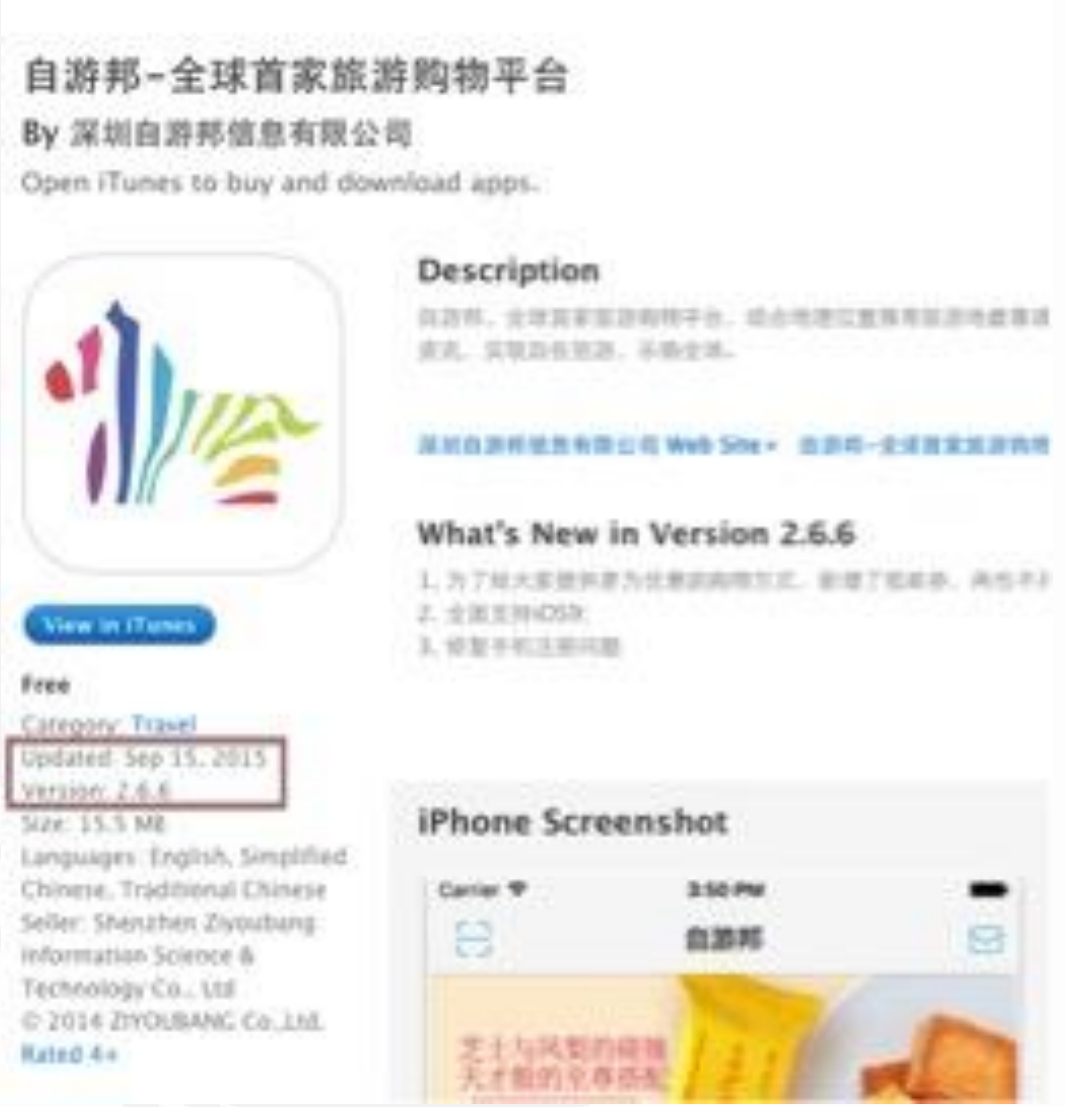
- Two methods for app assessments
  - Thorough inspection of all app capabilities
  - Predetermined “red flags” which would prohibit use of application
    - Example: accesses contacts and copies them off device
    - Example: tracks location and sends off device
    - Example: access to photos / photo stream
    - Example: User login credentials sent in plain text (or logged)

Application Assessment

Execution

Execution of Application Assessment

- Technically involved
- Even Apple and Google miss code included in applications
  - XCode Ghost is an example
  - Malicious library (with C2) included at compile time due to malicious XCode



自游邦-全球首家旅游购物平台

By 深圳自游邦信息有限公司

Open iTunes to buy and download apps.

Description

[illegible]

[illegible] Web Site ▸ [illegible]

What's New in Version 2.6.6

1. [illegible]
2. 全面支持iOS9
3. 修复手机注册问题

Free

Category: Travel

Updated: Sep 15, 2015

Version: 2.6.6

Size: 15.5 MB

Languages: English, Simplified Chinese, Traditional Chinese

Seller: Shenzhen Ziyoubang Information Science & Technology Co., Ltd

© 2014 ZIYOUBANG Co.,Ltd.

Rated 4+

iPhone Screenshot

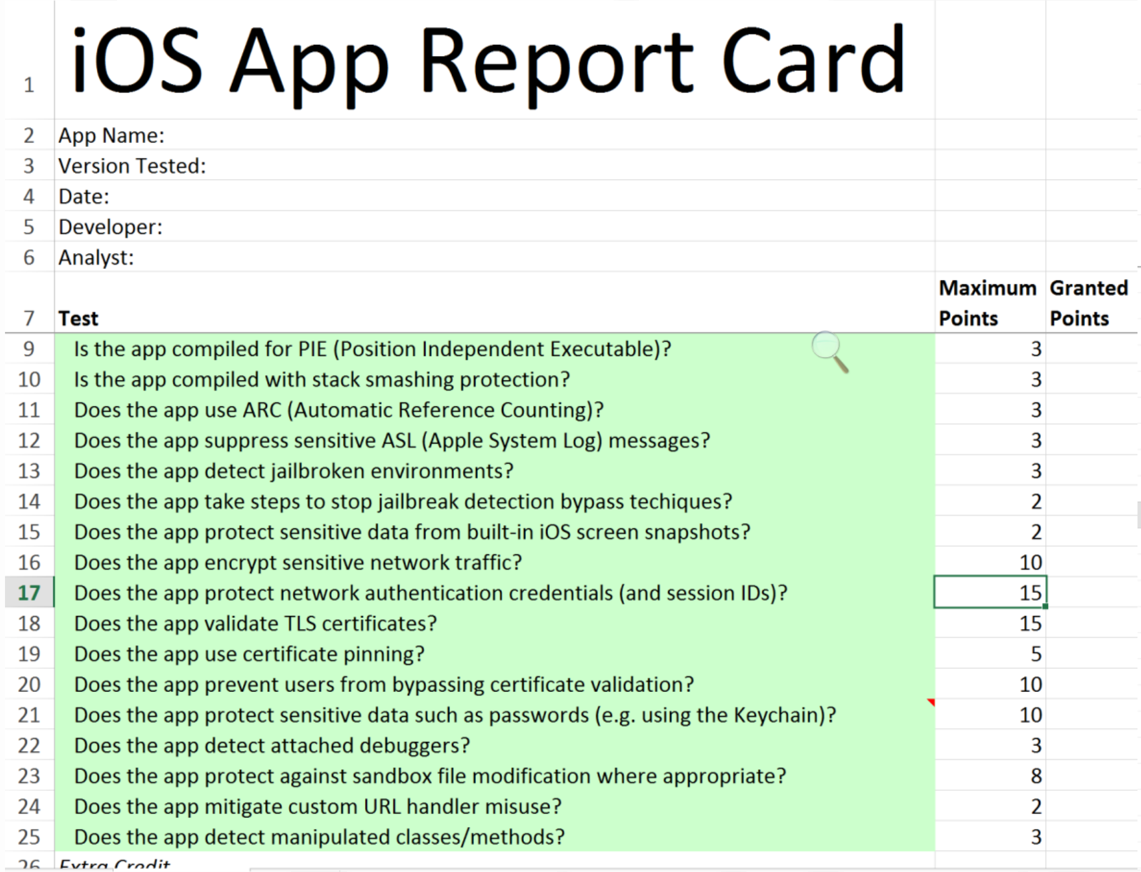
image from: https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html

Methodology Helps Overcome Limitations

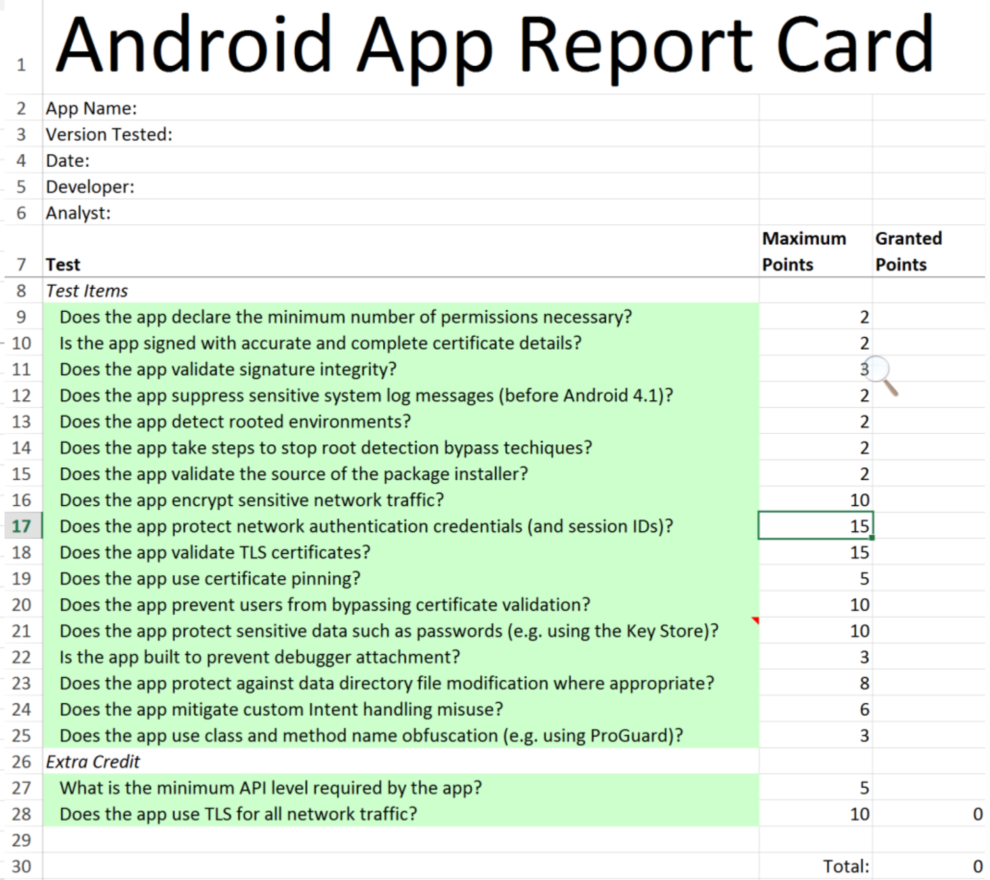
- Having a repeatable methodology is helpful to minimize the effort, as well as help the assessor to be sure that important facets aren’t overlooked
- It also helps to train the assessor

SANS SEC575 - Application Report Cards

- https://github.com/joswr1ght/MobileAppReportCard.git



1	iOS App Report Card		
2	App Name:		
3	Version Tested:		
4	Date:		
5	Developer:		
6	Analyst:		
7	**Test**	**Maximum Points**	**Granted Points**
9	Is the app compiled for PIE (Position Independent Executable)?	3	
10	Is the app compiled with stack smashing protection?	3	
11	Does the app use ARC (Automatic Reference Counting)?	3	
12	Does the app suppress sensitive ASL (Apple System Log) messages?	3	
13	Does the app detect jailbroken environments?	3	
14	Does the app take steps to stop jailbreak detection bypass techiques?	2	
15	Does the app protect sensitive data from built-in iOS screen snapshots?	2	
16	Does the app encrypt sensitive network traffic?	10	
17	Does the app protect network authentication credentials (and session IDs)?	15	
18	Does the app validate TLS certificates?	15	
19	Does the app use certificate pinning?	5	
20	Does the app prevent users from bypassing certificate validation?	10	
21	Does the app protect sensitive data such as passwords (e.g. using the Keychain)?	10	
22	Does the app detect attached debuggers?	3	
23	Does the app protect against sandbox file modification where appropriate?	8	
24	Does the app mitigate custom URL handler misuse?	2	
25	Does the app detect manipulated classes/methods?	3	
26	*Extra Credit*		



1	Android App Report Card		
2	App Name:		
3	Version Tested:		
4	Date:		
5	Developer:		
6	Analyst:		
7	**Test**	**Maximum Points**	**Granted Points**
8	*Test Items*		
9	Does the app declare the minimum number of permissions necessary?	2	
10	Is the app signed with accurate and complete certificate details?	2	
11	Does the app validate signature integrity?	3	
12	Does the app suppress sensitive system log messages (before Android 4.1)?	2	
13	Does the app detect rooted environments?	2	
14	Does the app take steps to stop root detection bypass techiques?	2	
15	Does the app validate the source of the package installer?	2	
16	Does the app encrypt sensitive network traffic?	10	
17	Does the app protect network authentication credentials (and session IDs)?	15	
18	Does the app validate TLS certificates?	15	
19	Does the app use certificate pinning?	5	
20	Does the app prevent users from bypassing certificate validation?	10	
21	Does the app protect sensitive data such as passwords (e.g. using the Key Store)?	10	
22	Is the app built to prevent debugger attachment?	3	
23	Does the app protect against data directory file modification where appropriate?	8	
24	Does the app mitigate custom Intent handling misuse?	6	
25	Does the app use class and method name obfuscation (e.g. using ProGuard)?	3	
26	*Extra Credit*		
27	What is the minimum API level required by the app?	5	
28	Does the app use TLS for all network traffic?	10	0
29			
30		Total:	0

Application Report Cards

- Report Cards address:
  - Permissions
  - Executable deficiencies
  - Local data storage and protection:
    - Confidentiality
    - Integrity
  - Protection of network communication
  - Inter-process communication

Assessment Legal Preface

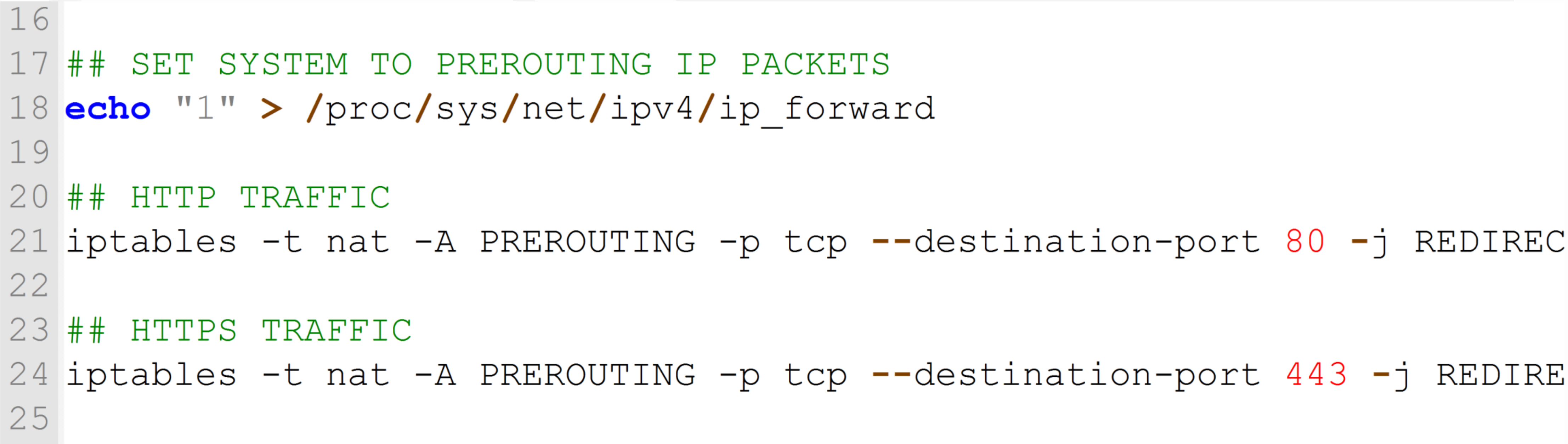
- Consult your legal counsel
- However, the notion is that assessing an application (which was legally obtained) for suitability of interoperation within your network is legal
- Do so for networks only where you have written permission to perform this type of analysis

Methodology – Network

- Easiest to perform without specialized tools
- Put the mobile device on a network, and monitor the communication through a laptop
- Challenge – TLS protected communication
- Challenge – interpreting hidden or obfuscated data
- Challenge – application has a trigger condition which isn’t met in your testing, obscuring some undesirable but present behavior

Methodology – Network

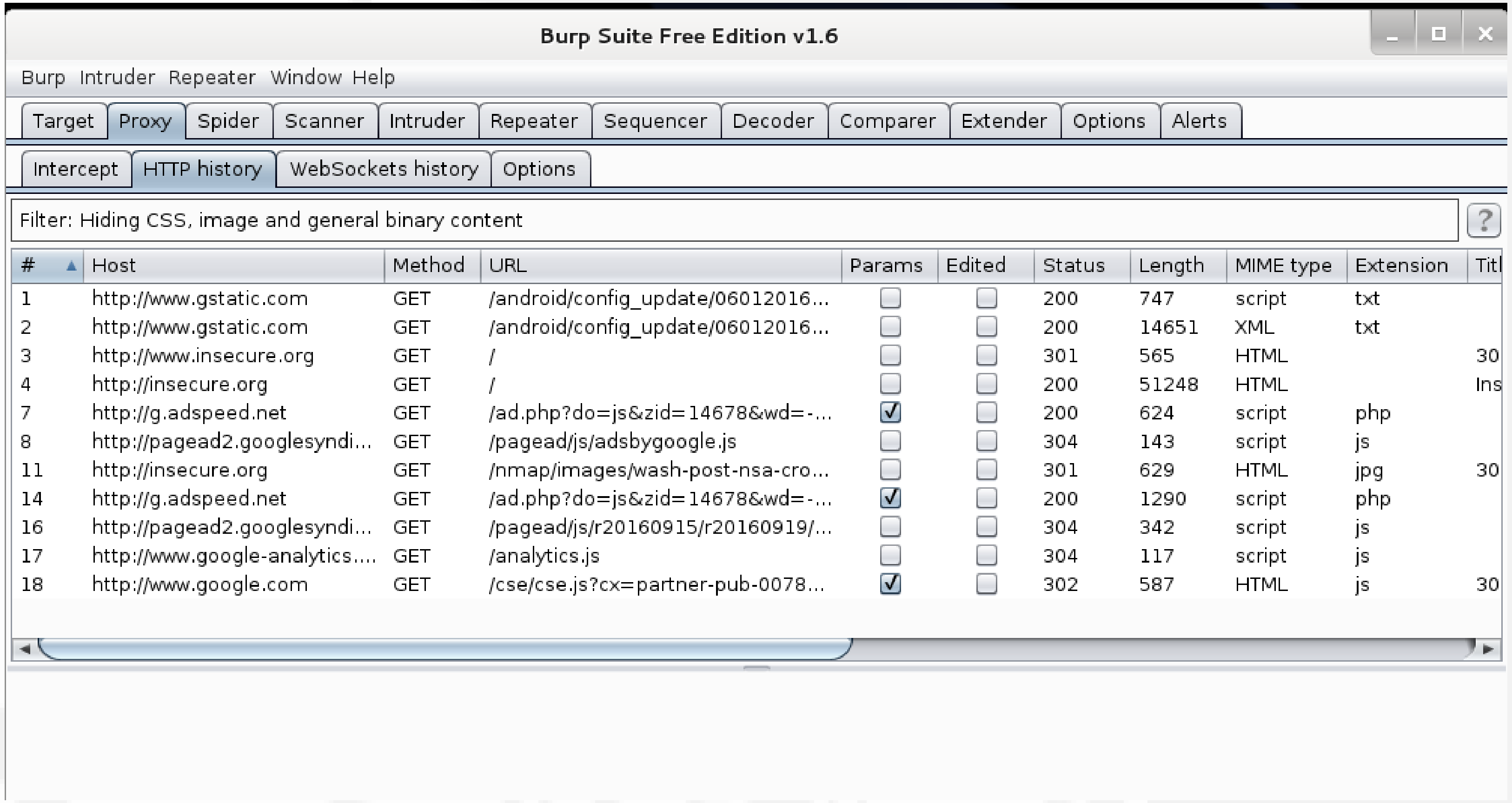
- Transparent firewall rules can direct traffic into a proxy
- Or device can be configured to use a proxy



```

## SET SYSTEM TO PREROUTING IP PACKETS
echo "1" > /proc/sys/net/ipv4/ip_forward

## HTTP TRAFFIC
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIREC

## HTTPS TRAFFIC
iptables -t nat -A PREROUTING -p tcp --destination-port 443 -j REDIRE

```

Methodology – Network

- Proxy is transparently viewing (and can modify) the content


Burp Suite Free Edition v1.6
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
?

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Titl
1	http://www.gstatic.com	GET	/android/config_update/06012016...	□	□	200	747	script	txt	
2	http://www.gstatic.com	GET	/android/config_update/06012016...	□	□	200	14651	XML	txt	
3	http://www.insecure.org	GET	/	□	□	301	565	HTML		30
4	http://insecure.org	GET	/	□	□	200	51248	HTML		Ins
7	http://g.adspeed.net	GET	/ad.php?do=js&zid=14678&wd=-...	☑	□	200	624	script	php	
8	http://pagead2.googlesyndi...	GET	/pagead/js/adsbygoogle.js	□	□	304	143	script	js	
11	http://insecure.org	GET	/nmap/images/wash-post-nsa-cro...	□	□	301	629	HTML	jpg	30
14	http://g.adspeed.net	GET	/ad.php?do=js&zid=14678&wd=-...	☑	□	200	1290	script	php	
16	http://pagead2.googlesyndi...	GET	/pagead/js/r20160915/r20160919/...	□	□	304	342	script	js	
17	http://www.google-analytics....	GET	/analytics.js	□	□	304	117	script	js	
18	http://www.google.com	GET	/cse/cse.js?cx=partner-pub-0078...	☑	□	302	587	HTML	js	30

Methodology – Network

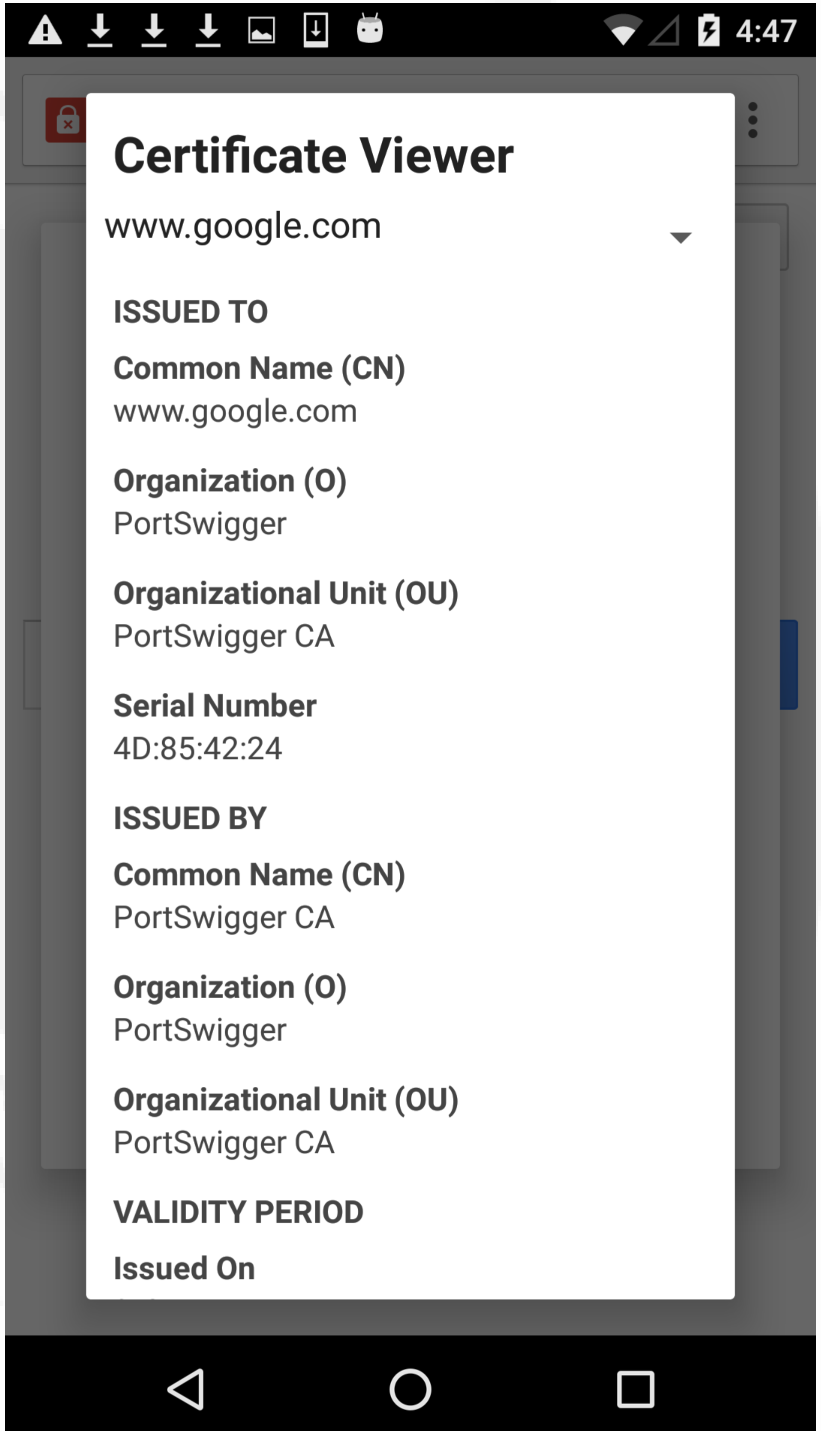
- How to deal with TLS?
- Easiest way is to include proxy’s certificate
- Burp serves up a .der format file, so convert it

```
openssl x509 -inform der -outform pem -in cacert.der -out cacert.pem
python -m SimpleHTTPServer 9090
```

- Browse to system, collect cert (http://172.16.42.42:9090/)
- Install Cert: Settings – Security – “Install from Storage”
- Select “cacert.pem”

Methodology – Network

- Get "man in the middle"
- Here the cert issuer for www.google.com is my Burp Suite CA – "PortSwigger CA"
- Apps vary on how they deal with this depending on how they're programmed



Certificate Viewer

www.google.com

ISSUED TO

Common Name (CN)
www.google.com

Organization (O)
PortSwigger

Organizational Unit (OU)
PortSwigger CA

Serial Number
4D:85:42:24

ISSUED BY

Common Name (CN)
PortSwigger CA

Organization (O)
PortSwigger

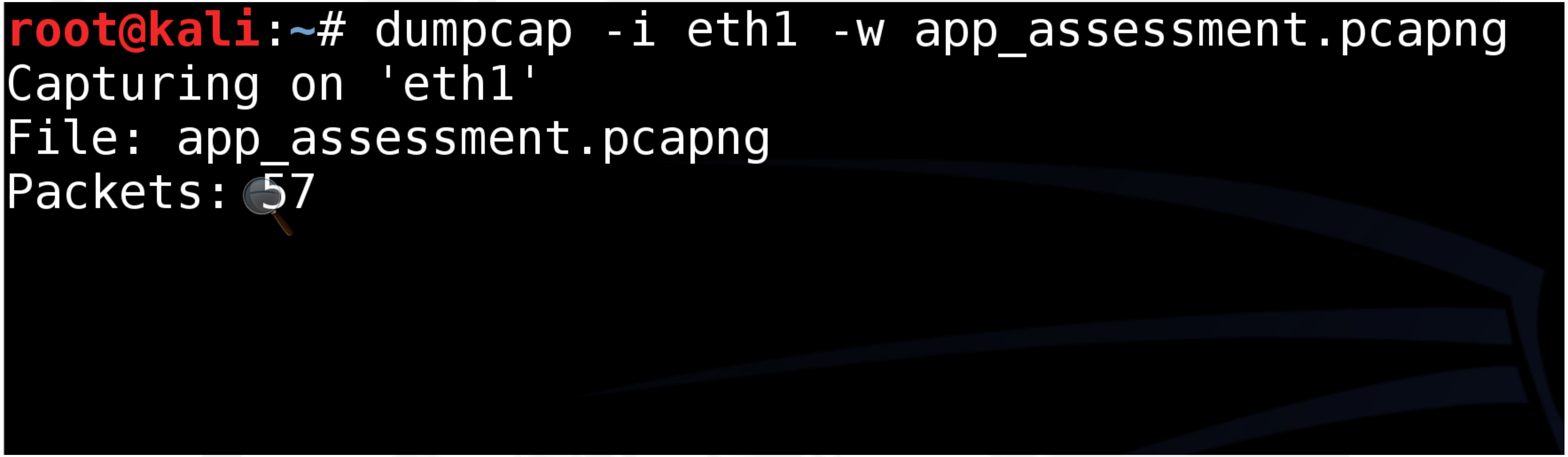
Organizational Unit (OU)
PortSwigger CA

VALIDITY PERIOD

Issued On

Methodology – Network

- Additionally, full packet capture (PCAP) via tcpdump, dumpcap, wireshark, etc. during assessment



```
root@kali:~# dumpcap -i eth1 -w app_assessment.pcapng
Capturing on 'eth1'
File: app_assessment.pcapng
Packets: 57
```

Methodology – Code Assessment

- By reviewing the code, there is an opportunity to see more than the behavior of the app during your observation
- You can see all of the things the application is programmed to do
- This is more complex than evaluation of network
- Requires tools to assist with the code assessment

Acquire Application to Assess

- Android – a couple of options
  - Install app, use ES FileExplorer to backup apk
  - Tool like RealAPK Leecher to pull from Play store
- iOS
  - Must have a jailbroken phone to extract application, but network/behavioral assessment can be done without jailbroken phone
  - Jailbroken phone: collect executable from within the install directory
  - Decrypt with gdb or rasticrac

Methodology – Inter-process Communication

- Android – use of “intents”
- Android components:
  - Activities
  - Services
  - Content Providers
  - Broadcast Receiver

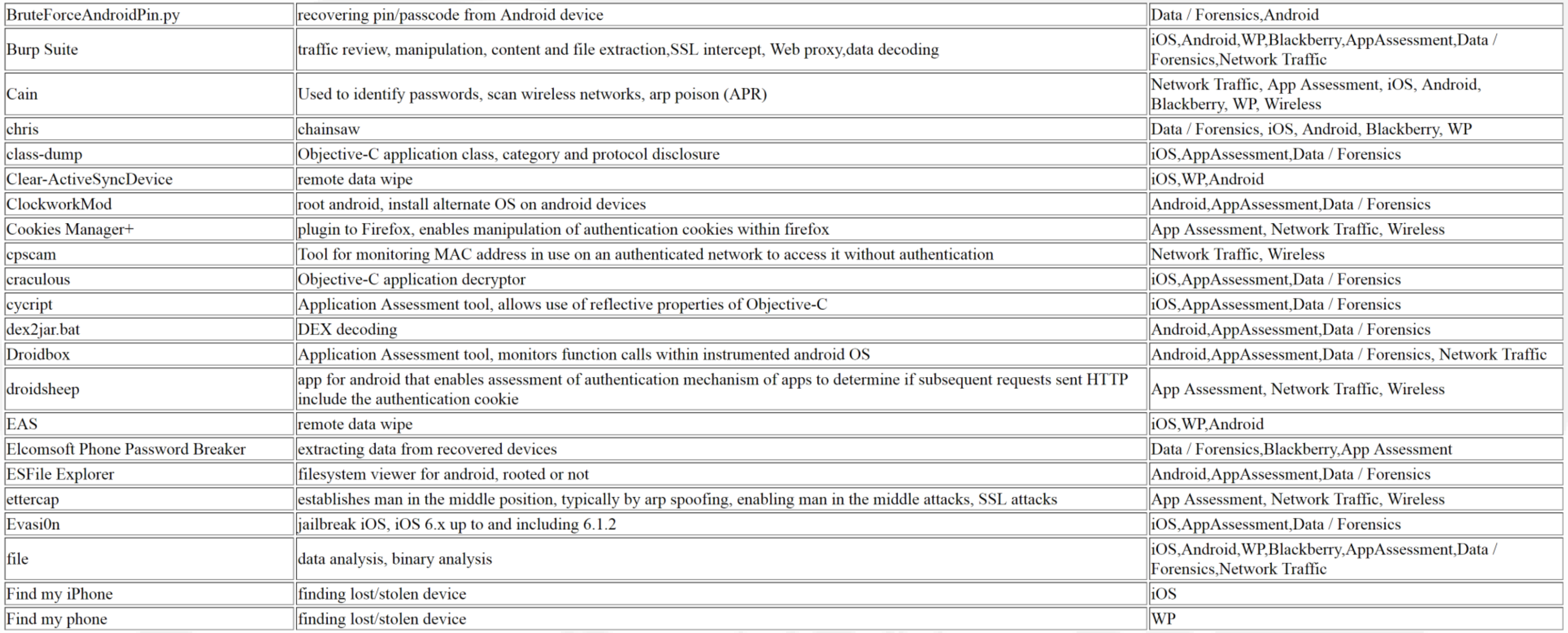
- iOS – chroot (sandbox) with minor exceptions for data sharing between apps
  - Document provider (shares with other apps)
  - Document picker (can import)
  - Action extension
  - Custom keyboard
- Also, URL handlers such as “twitter://”

Methodology – Inter-process Communication

- Assessing the IPC is involved in both platforms
- Drozer is very helpful for this on Android
- iOS no automated tool yet to help with exploration of IPC
  - Concern of action extension for exposure of app to active content returned into application context
- Challenge is time, and exploring potential content provided

Methodology – Tools

- You need a bunch of tools to be able to do this work
- Frequently still involve extensive manual work



BruteForceAndroidPin.py	recovering pin/passcode from Android device	Data / Forensics,Android
Burp Suite	traffic review, manipulation, content and file extraction,SSL intercept, Web proxy,data decoding	iOS,Android,WP,Blackberry,AppAssessment,Data / Forensics,Network Traffic
Cain	Used to identify passwords, scan wireless networks, arp poison (APR)	Network Traffic, App Assessment, iOS, Android, Blackberry, WP, Wireless
chris	chainsaw	Data / Forensics, iOS, Android, Blackberry, WP
class-dump	Objective-C application class, category and protocol disclosure	iOS,AppAssessment,Data / Forensics
Clear-ActiveSyncDevice	remote data wipe	iOS,WP,Android
ClockworkMod	root android, install alternate OS on android devices	Android,AppAssessment,Data / Forensics
Cookies Manager+	plugin to Firefox, enables manipulation of authentication cookies within firefox	App Assessment, Network Traffic, Wireless
cpscam	Tool for monitoring MAC address in use on an authenticated network to access it without authentication	Network Traffic, Wireless
craculous	Objective-C application decryptor	iOS,AppAssessment,Data / Forensics
cycript	Application Assessment tool, allows use of reflective properties of Objective-C	iOS,AppAssessment,Data / Forensics
dex2jar.bat	DEX decoding	Android,AppAssessment,Data / Forensics
Droidbox	Application Assessment tool, monitors function calls within instrumented android OS	Android,AppAssessment,Data / Forensics, Network Traffic
droidsheep	app for android that enables assessment of authentication mechanism of apps to determine if subsequent requests sent HTTP include the authentication cookie	App Assessment, Network Traffic, Wireless
EAS	remote data wipe	iOS,WP,Android
Elcomsoft Phone Password Breaker	extracting data from recovered devices	Data / Forensics,Blackberry,App Assessment
ESFile Explorer	filesystem viewer for android, rooted or not	Android,AppAssessment,Data / Forensics
ettercap	establishes man in the middle position, typically by arp spoofing, enabling man in the middle attacks, SSL attacks	App Assessment, Network Traffic, Wireless
Evasi0n	jailbreak iOS, iOS 6.x up to and including 6.1.2	iOS,AppAssessment,Data / Forensics
file	data analysis, binary analysis	iOS,Android,WP,Blackberry,AppAssessment,Data / Forensics,Network Traffic
Find my iPhone	finding lost/stolen device	iOS
Find my phone	finding lost/stolen device	WP

Methodology – Distributions

- There are some pre-built distributions which give you an environment to work from
  - MobiSec (SecureIdeas)
  - Androlab (androl4b)
  - Santoku Linux (from NowSecure)
  - Kali Linux
- Give you the benefit of the tools already set up
- Probably doesn’t have everything you need, but a good start