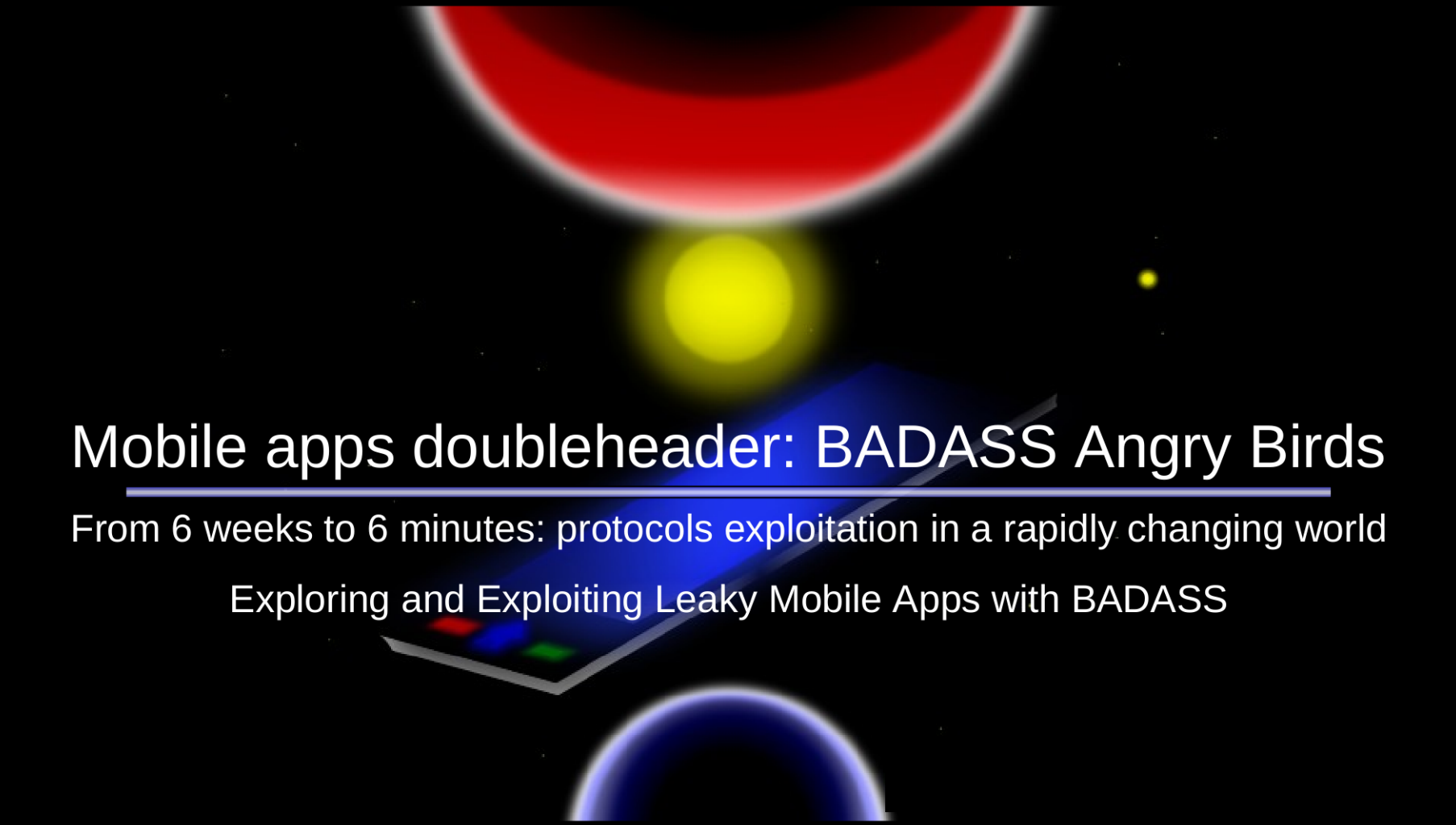


UK SECRET STRAP1 COMINT
S//SI//REL

Mobile apps doubleheader: BADASS Angry Birds

From 6 weeks to 6 minutes: protocols exploitation in a rapidly changing world

Exploring and Exploiting Leaky Mobile Apps with BADASS

GTE/GCHQ

GA5A/CSEC

Coming up…

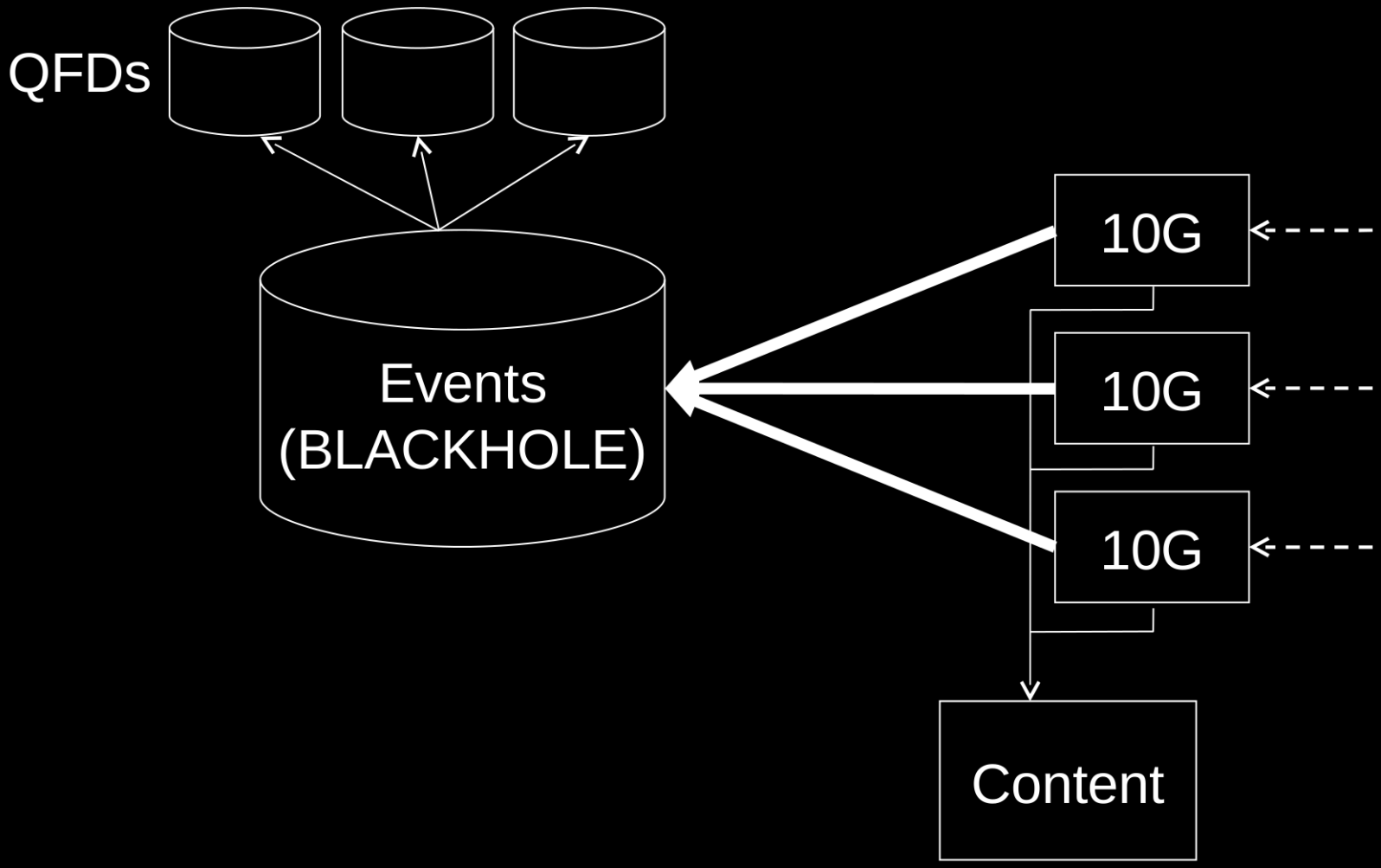
1) **BADASS - From 6 weeks to 6 minutes**: protocols exploitation in a rapidly changing world

2) **We Know How Bad You Are At "Angry Birds"**: Exploring and Exploiting Leaky Mobile Apps with BADASS (OtH)

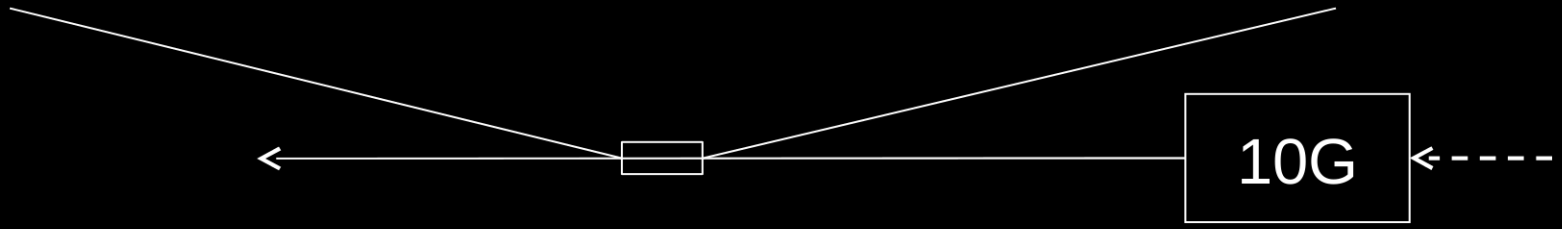
BADASS

- Protocols Exploitation at GCHQ
- Mobile Applications – a challenge
- BADASS - BEGAL Automated Deployment And Survey System
- UNIQUELY CHALLENGED – Rapid deployment
- SEM – more complex extractions

GCHQ



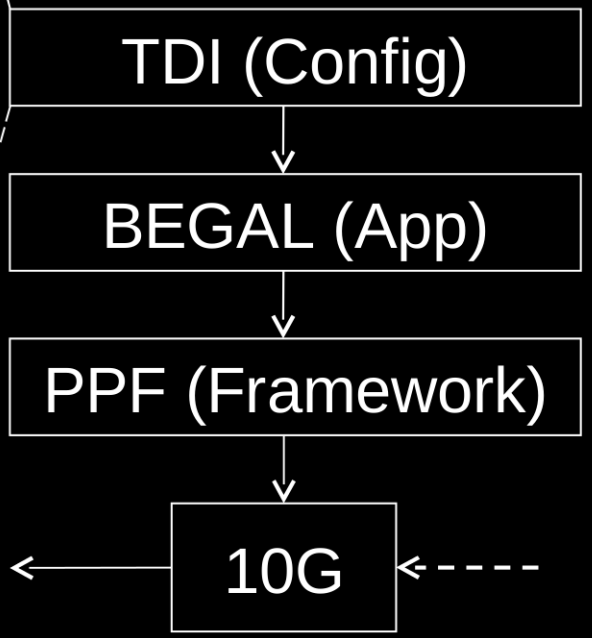
1303138597 6 62824 80 **Google-Prefid-Cookie** 16 **8df8675ed8762cb2** TDI-Scope 7 Machine Route 12 192.168.0.51 HHFP-Hash 8 4909f053 User-Agent 138 **Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; WOW64; Trident/4.0; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.30729)** Host 17 **news.google.co.uk** Geo-IP-Dst 38 37.4192;-122.0574;MOUNTAINVIEW;US;6LLM Event-security-label 6 10007F Stream-security-label 10 400023E0FF Source-Bearer 4 TEST



```
<surveyRule>
  <ruleName>Google-Prefid-Cookie</ruleName>
  <action>
    <actionType>EVENT</actionType>
    <eventFormat>PRESENCE</eventFormat>
    <eventLogicalDestination>presence</eventLogicalDestination>
                                    <presenceEventIdentifierType>Google-Prefid-
Cookie</presenceEventIdentifierType>
    <presenceEventUseSourceIp>true</presenceEventUseSourceIp>
    <presenceEventTIType>TDI</presenceEventTIType>

<presenceEventGenerationType>MACHINE</presenceEventGenerationTy
pe>
  </action>
  <criterionSet>
    <criterion>
      <fspfTasking>
        <selectorType>string</selectorType>
        <selector>; PREF=ID=</selector>
        <bitMask/>
        <caseSensitive>true</caseSensitive>
        <position>-1</position>
        <protocolLayer>APPLICATION_LAYER</protocolLayer>

<numSubsequentPacketsToForward>0</numSubsequentPacketsToForwa
rd>
.....
```



The Good Old Days

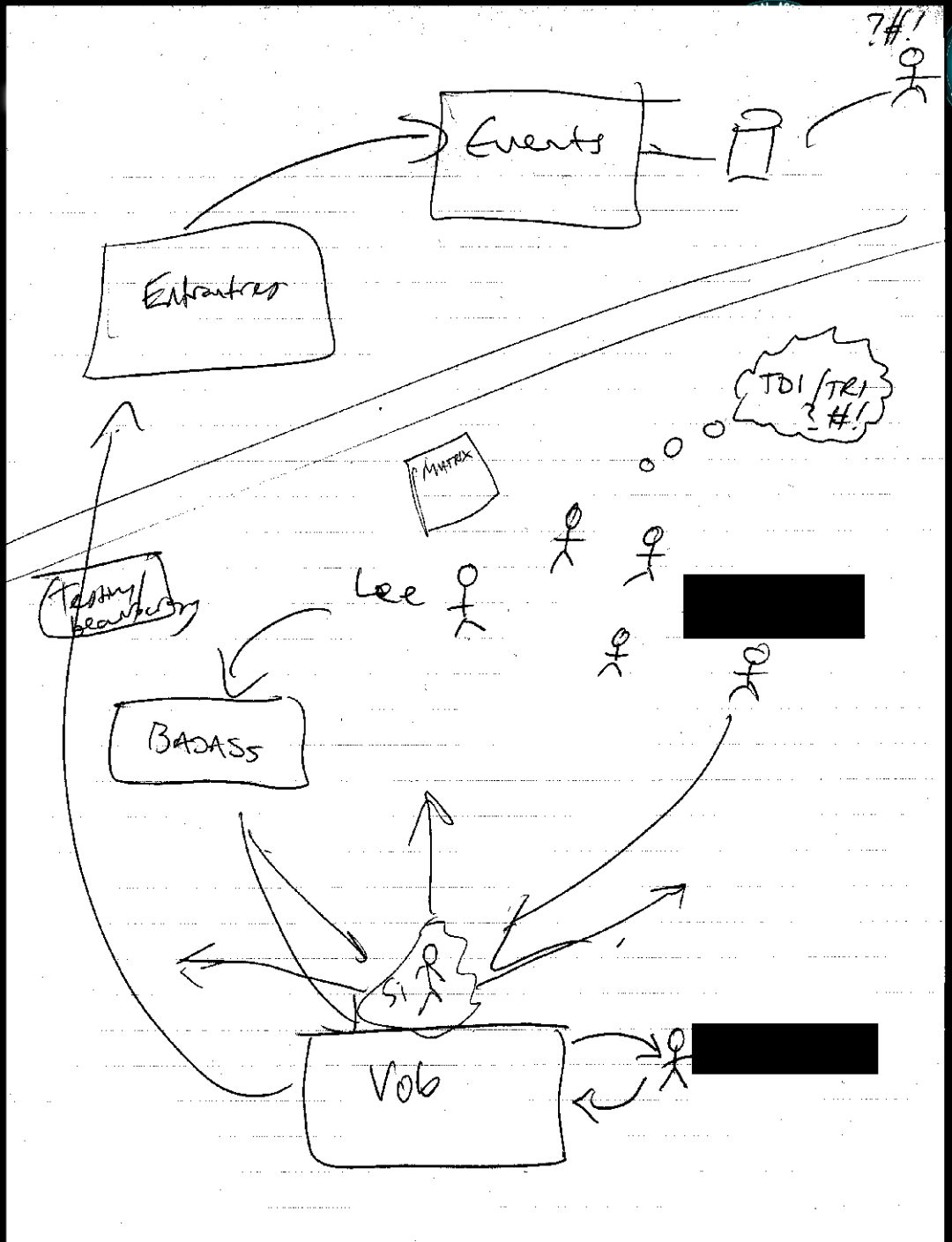
UK TOP SECRET STRAP15 NOPERSON
TOBESTOREDININACCESSIBLEFOLDERINGTESHAREDDRIVE

OPD-GTE

Application:

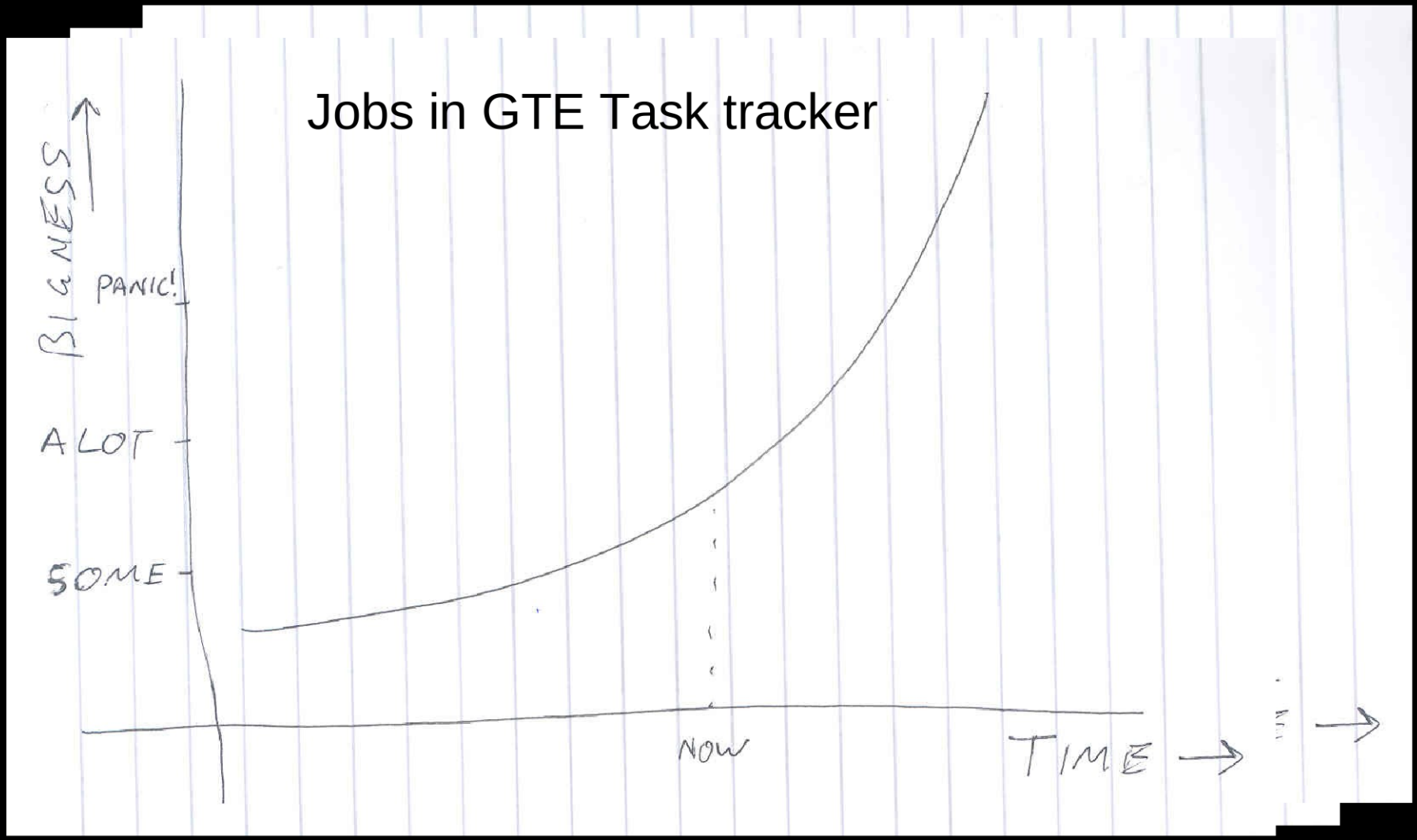
Bebo Mobile Service

New TDI Process 2010



VOB
Datastore (x 2!)
BADASS.
Matrix reports
Spreadsheets
Etc..

Mobile Applications – Some Stats



Why?

Many different platforms (iOS, Android, WP7, Blackberry)

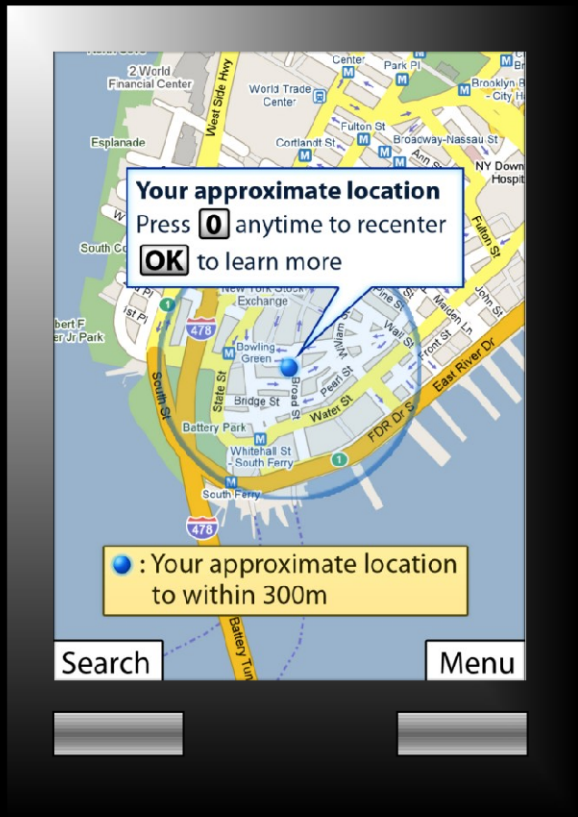
App store business model – everyone is writing software

Much greater diversity of software

(Basket) Case Studies

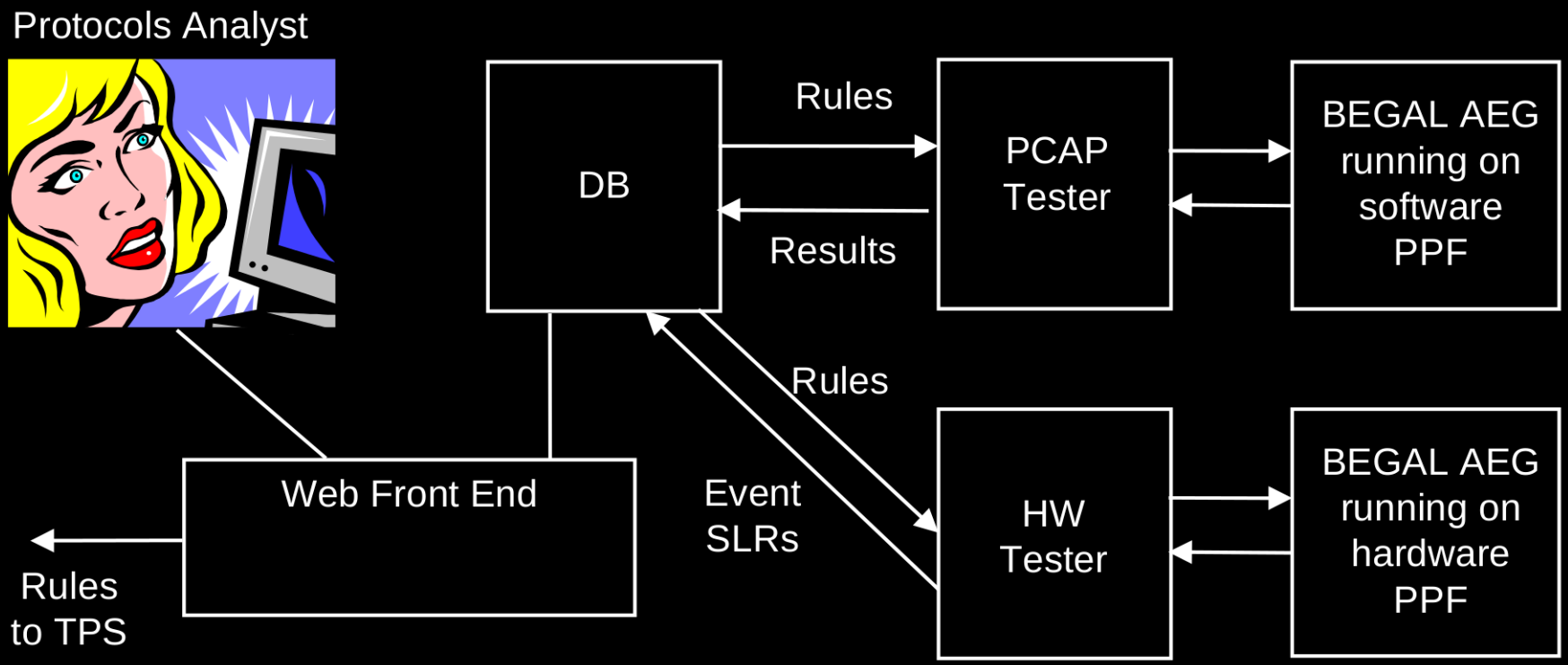
GMM – 18 months from analysis to deployment

TDIs – typical time from rule completion to deployment ~ 3 months



Intro to BADASS

BEGAL Automated Development / Deployment And Something Something



[redacted]_Googlemobilemaps-000e-Body

Back to list | Copy this rule

Rule Properties show

Rule text

Edit XML/YAML

Testing status: Produced an invalid result in the FKB pcap test, and testing has been suspended

Testing Progress (GTE): Rule Check | DKB PCAP | FKB PCAP | FKB Soak [redacted]

Deployment status: DEPLOYED

Deployment Progress (TPS): Submission | HB Priority | Deploy — deployed in heartbeats:

Version definition hide

XML | YAML

```
<surveyRule>
  <ruleName>M_Googlemobilemaps-000e-Body</ruleName>
  <action>
    <actionType>EVENT</actionType>
    <eventFormat>PRESENCE</eventFormat>
    <eventLogicalDestination>presence</eventLogicalDestination>
    <presenceEventIdentifierType>M_Googlemobilemaps-000e-Body</presenc
    <presenceEventUseSourceIp>true</presenceEventUseSourceIp>
    <presenceEventTIType>TDI</presenceEventTIType>
    <presenceEventGenerationType>MACHINE</presenceEventGenerationType>
  </action>
  <criterionSet>
    <criterion>
      <fspfTasking>
        <selectorType>string</selectorType>
        <selector>/glm/mmap</selector>
        <bitMask/>
        <caseSensitive>true</caseSensitive>
        <position>-1</position>
        <protocolLayer>APPLICATION_LAYER</protocolLayer>
```

Logs: show

Packet Dump

hide

Hexdump | ASCII

download as pcap

Packet #1

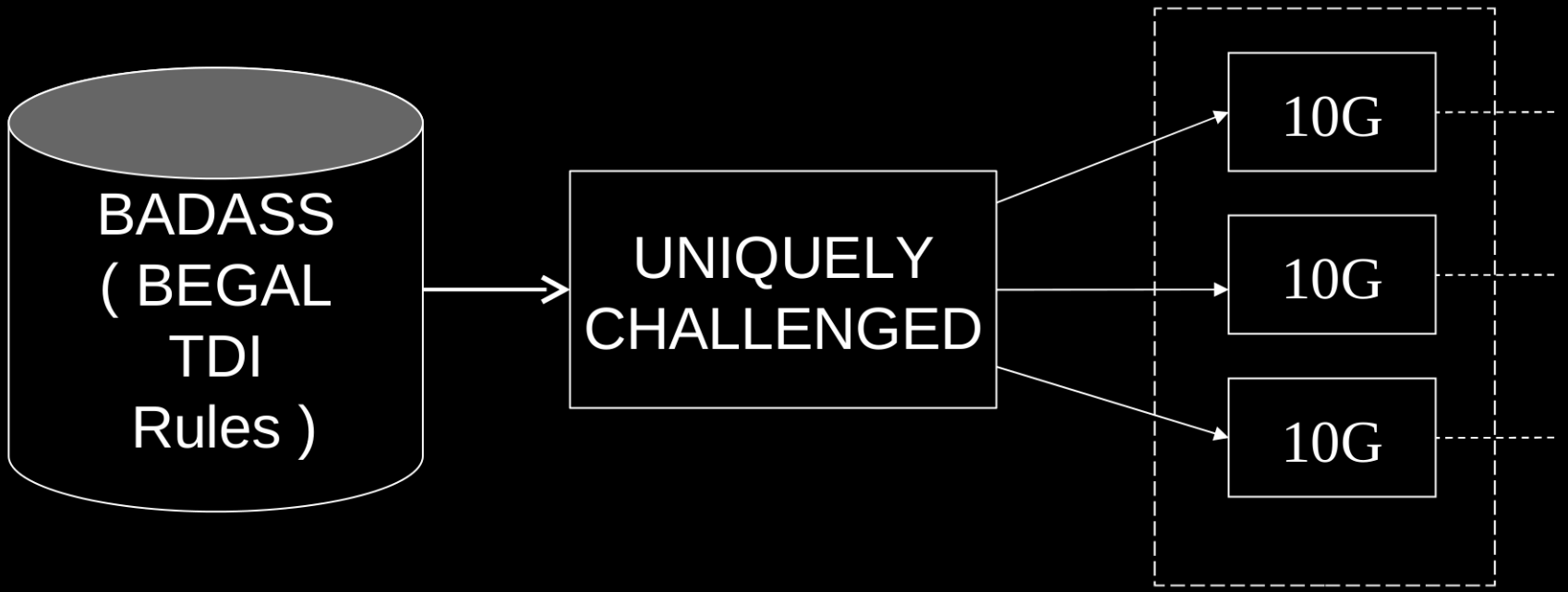
Timestamp: 2011-04-12 16:25:11

```
Network layer; protocol=TCP srcip=[redacted] destip=[redacted] fragoff=0
0000: 4500 0177 8258 4000  4006 4859 0a40 add5   E..w.X@.@.HY.@..
0010: d155 e564                                  .U.d
Transport layer; srcport=50323 destport=80
0014: c493 0050 9ad1 405b  56d8 dc5d 8018 7d78   ...P..@[V..]..}x
0024: abf7 0000 0101 080a  ffff c224 2ee0 c3b2   ...........$....
Application layer
0034: 504f 5354 202f 676c  6d2f 6d6d 6170 2048   POST /glm/mmap H  5:APPLICATION|ANY|FWD|1|C|/glm/mmap
0044: 5454 502f 312e 310d  0a43 6f6e 7465 6e74   TTP/1.1..Content
0054: 2d54 7970 653a 2061  7070 6c69 6361 7469   -Type: applicati
0064: 6f6e 2f62 696e 6172  790d 0a43 6f6e 7465   on/binary..Conte
0074: 6e74 2d4c 656e 6774  683a 2036 3530 0d0a   nt-Length: 650..
0084: 486f 7374 3a20 6d6f  6269 6c65 6d61 7073   Host: mobilemaps
0094: 2e63 6c69 656e 7473  2e67 6f6f 676c 652e   .clients.google.
00a4: 636f 6d0d 0a43 6f6e  6e65 6374 696f 6e3a   com..Connection:
00b4: 204b 6565 702d 416c  6976 650d 0a55 7365    Keep-Alive..Use  C:APPLICATION|ANY|TAG|0|I|\nUser-Agent:
00c4: 722d 4167 656e 743a  204d 6f7a 696c 6c61   r-Agent: Mozilla
00d4: 2f35 2e30 2028 4c69  6e75 783b 2055 3b20   /5.0 (Linux; U;
00e4: 416e 6472 6f69 6420  322e 312d 7570 6461   Android 2.1-upda
00f4: 7465 313b 2065 6e2d  6762 3b20 4854 4320   te1; en-gb; HTC
0104: 4465 7369 7265 2042  7569 6c64 2f45 5245   Desire Build/ERE
0114: 3237 2920 4170 706c  6557 6562 4b69 742f   27) AppleWebKit/
0124: 3533 302e 3137 2028  4b48 544d 4c2c 206c   530.17 (KHTML, l
0134: 696b 6520 4765 636b  6f29 2056 6572 7369   ike Gecko) Versi
0144: 6f6e 2f34 2e30 204d  6f62 696c 6520 5361   on/4.0 Mobile Sa
0154: 6661 7269 2f35 3330  2e31 3720 2862 7261   fari/530.17 (bra
0164: 766f 2045 5245 3237  293b 2067 7a69 700d   vo ERE27); gzip.  F:APPLICATION|ANY|TAG|0|C|\r\n\r\n|ffffffff
0174: 0a0d 0a                                    ...
```

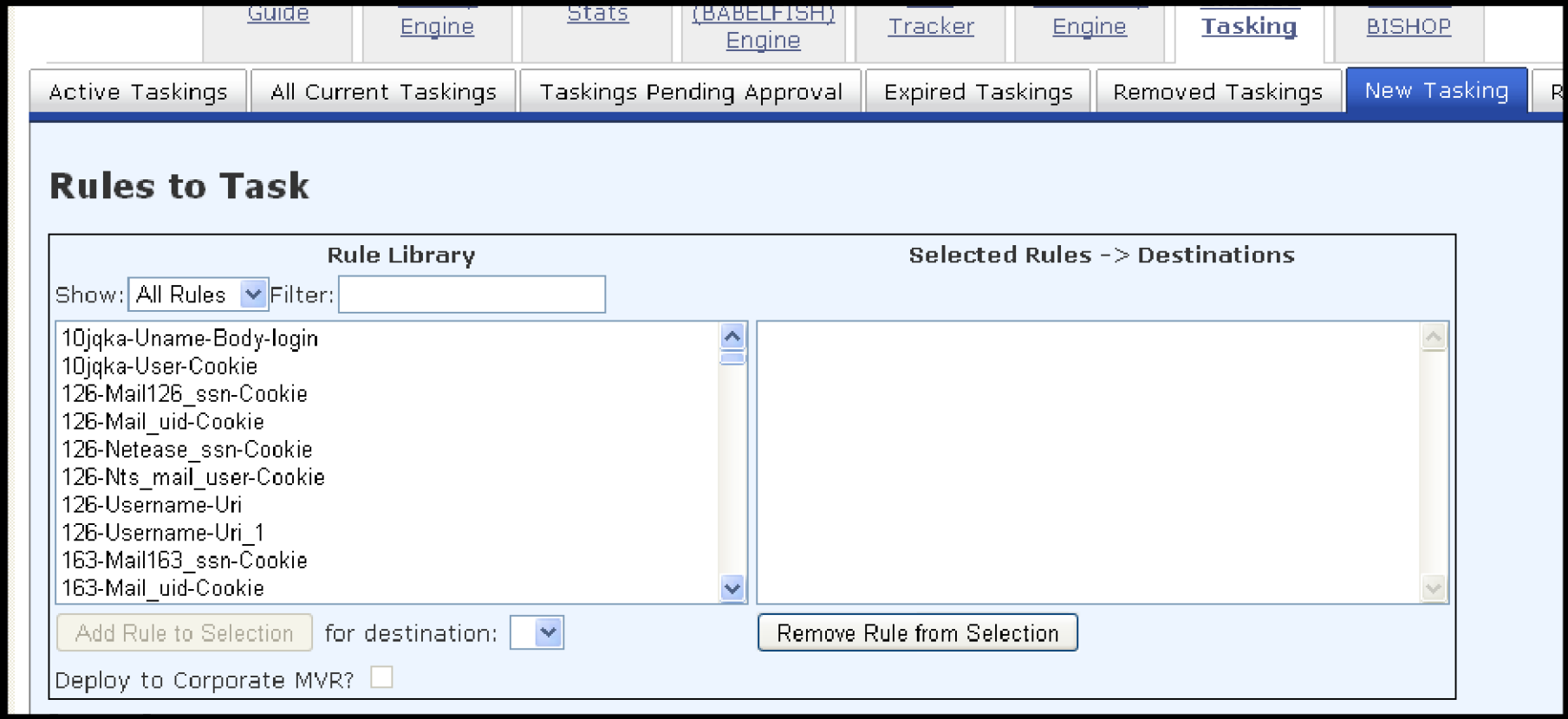
Things worth mentioning

- Testing – increased confidence in rules produced by GTE
- Training – can use web interface to educate, and to prevent common mistakes
- Deduping effort – knowledge of what has already been done
- Became corporate TDI repo through back door
- Devolved management of protocols – no one person has to oversee all of them

UNIQUELY CHALLENGED



UNIQUELY CHALLENGED



UNIQUELY CHALLENGED

One person has complete oversight of a technology from analysis to deployment – important for rapidly changing protocols

SEM – the future

Developed by ICTR at GCHQ

Complex events - More than just TDIs

Social interactions

Geo

Network Events

SEM

Rule Filters

Browse the current rules using [n]one or more filters

Rule Descriptor	Descriptor Value
item_class	identity-present
item_service	Facebook
any	

Go

Results

- Actor|Direct|Facebook|identity-present|email|login_x-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|login_x-Set-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|lxe-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|lxe-Set-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|mobile-email-Method-Body [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|mobile-m_user-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|reg_fb_gate-Set-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|email|reg_fb_ref-Set-Cookie [edit] [create like] [YAML edit] [YAML create like]
- Actor|Direct|Facebook|identity-present|uid-c_user|c_user-Cookie [edit] [create like] [YAML edit] [YAML create like]

```
_orignal_tdi_rule:  Facebook-ID-HTTP-Cookie-c_user
_orignal_tdi_type:  Facebook-CUser-Cookie
_rule_creator:  sjcarro
_rule_editor:  kbbaldw
_rule_status:  locked
data_stream:  HTTP-Request
extract:
  - context:  Cookie
    pattern:  '(?:^|[ ;])c_user=([^ ;]+)'
extraction:  Direct
item_attribution:  Actor
item_class:  identity-present
item_scope:  User
item_service:  Facebook
item_tech_context:  c_user-Cookie
item_type:  uid-c_user
item_universe:  service
rule:  Actor|Direct|Facebook|identity-present|uid-c_user|c_user-Cookie
```

Over to Marty…

Coming up…

- Quick Overview: Ads and Analytics in the Mobile Realm
- Ads (Mobclix, AdMob, Mydas)
- Analytics (Dataflurry)
- Updates to Android IDs
- Windows Phone 7 User and Device IDs
- ~~Ab~~using BADASS for Fun and Profit

Ads and Analytics in the Mobile Realm

Q: Why bother looking at mobile ads and analytics?

A: Developers use them to make money!

Ads and analytics support the developer with:

- App Development
- User Experience
- App Marketing

Ads and Analytics in the Mobile Realm

Ads are used as a means of generating revenue for a developer

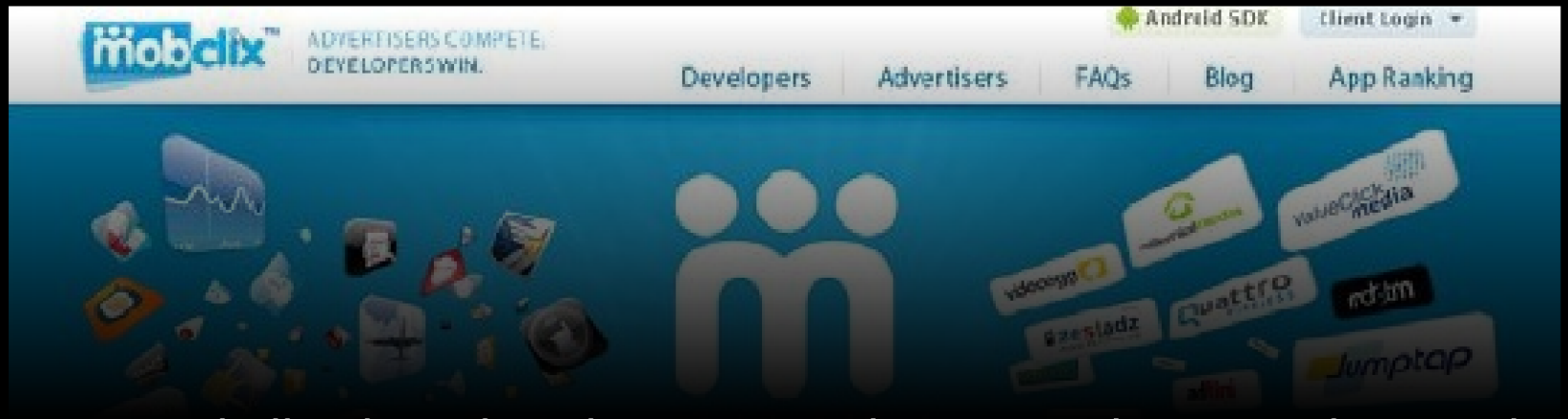
- Advertisers need information about the device/user to properly target ads
- Unlikely to see ads in an app that charges
- Many developers are releasing dual versions of apps: ad-supported and paid

Ads and Analytics in the Mobile Realm

Analytics are used as a means of generating usage metrics for a developer

- "Anonymous usage statistics"
- Present in both paid and free apps
- Developer is presented with aggregate data for an app

Ads: Mobclix



WSJ: Mobclix, the ad exchange, matches more than 25 ad networks with some 15,000 apps seeking advertisers. The Palo Alto, Calif., company collects phone IDs, encodes them (to obscure the number), and assigns them to interest categories based on what apps people download and how much time they spend using an app, among other factors. By tracking a phone's location, Mobclix also makes a "best guess" of where a person lives, says Mr. Gurbuxani, the Mobclix executive. Mobclix then matches that location with spending and demographic data from Nielsen Co.

Ads: Mobclix

```
GET /?p=android
&i={GUID}
&s=320x50 (ad size)
&av=1.4.2
&u={IMEI}
&andid={Android ID}
&v=2.3.0
&ct=null
&dm={Phone Name}
&hwdm={Phone HW Model}
&sv={OS Version}&ua={User-Agent}
&o=0&ap=0
&ll=51.903699%2C-2.078062
&l=en_GB HTTP/1.1
Cookie:
User-Agent: …
Host: ads.mobclix.com
Connection: Keep-Alive
```

Ads: Mobclix

```
GET /?p={platform}
&i={GUID}
&s=320x50 (ad size)
&av=1.4.2
&u={IMEI}
&andid={Android ID}
&v=2.3.0
&ct=null
&dm={Phone Name}
&hwdm={Phone HW Model}
&sv={OS Version}
&ua={User-Agent}
&o=0
&ap=0
&ll=51.903699%2C-2.078062
&l=en_GB HTTP/1.1
Cookie:
User-Agent: …
Host: ads.mobclix.com
Connection: Keep-Alive
```

- GET request indicates platform and the device identifier
  - the order of the p argument in the GET can vary between platforms
- ll is lat,long; not always present
- Uses multiple URLs for activities:
  - Ads: ads.mobclix.com
  - Analytics: data.mobclix.com/post/sendData
  - Feedback: data.mobclix.com/post/feedback
  - Config: data.mobclix.com/post/config

Cross-Platform Ads: Mobclix

```
GET /?p={platform}
&i={GUID}
&s=320x50 (ad size)
&av=1.4.2
&u={IMEI}
&andid={Android ID}
&v=2.3.0
&ct=null
&dm={Phone Name}
&hwdm={Phone HW Model}
&sv={OS Version}
&ua={User-Agent}
&o=0
&ap=0
&ll=51.903699%2C-2.078062
&l=en_GB HTTP/1.1
Cookie:
User-Agent: …
Host: ads.mobclix.com
Connection: Keep-Alive
```

Argument	iPhone	Android	WP7*
{platform}	iphone	android	?
{u}	UDID	AndID, or IMEI when {andid} is set	?
{andid}	N/A	AndID	N/A

*: WP7 Mobclix SDK still in beta

Cross-Platform Ads: AdMob

```
GET /p/i/e2/9b/e29b1e7503a5b24b3e693ece2c887173.png HTTP/1.1
Host: mm.admob.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW
iPhone1,2; en_us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-
20090617)
X-Admob-Isu: 7355c9d9f7d1033e0fe3ee13513366ad69170013
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: uuid=81a66cc2cf3f554e02f089c04d8d4fcb;
admobuu=486177273327484712647443760381 26
Connection: keep-alive
```

The isu can appear both as an argument in a POST or in the X-ADMOB-ISU HTTP header extension. The value itself is 32-40 bytes long.

Hosts using this value consistently: r.admob.com, mm.admob.com, mmv.admob.com, and a.admob.com

Cross-Platform Ads: AdMob

```
GET /p/i/e2/9b/e29b1e7503a5b24b3e693ece2c887173.png HTTP/1.1
Host: mm.admob.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; HW
iPhone1,2; en_us) AppleWebKit/525.18.1 (KHTML, like Gecko) (AdMob-iSDK-
20090617)
X-Admob-Isu: 7355c9d9f7d1033e0fe3ee13513366ad69170013
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Cookie: uuid=81a66cc2cf3f554e02f089c04d8d4fcb;
admobuu=486177273327484712647443760381 26
Connection: keep-alive
```

The platform can be identified by the User-Agent string:

- iPhone: AdMob-iSDK-20yymmdd
- Android: AdMob-ANDROID-20yymmdd
- WP7: possibly AdMob-WINDOWSPHONE7-20yymmdd; observed 20yymmdd-WINDOWSPHONE7-AldaritSuperAds

Cross-Platform Ads: AdMob

```
POST /ad_source.php HTTP/1.1
Accept: */*
Content-Length: 277
Accept-Encoding: identi
Content-Type: applicati
User-Agent: {User-agent
Host: r.admob.com
Connection: Keep-Alive
Cache-Control: no-cache
...rt=0
&u={User-Agent}
&isu={isu}
&ex=1
&client_sdk=1
&l=en
&f=jsonp
&z=1304518478
&s=a14d248b5738462
&v=20101123-WINDOWSPHONE7-AldaritSuperAds
```

Argument	iPhone	Android	WP7
{isu}*	iPhone UDID, or MD5 hash of the int val of the UDID	MD5 hash of the int val of the Android ID	SHA1 hash of the int val of the Device ID

*: isu can appear both as an argument in a POST or in the X-ADMOB-ISU HTTP header extension

Cross-Platform Ads: Mydas

```
GET /getAd.php5?
sdkapid=35447
&auid={Phone IMEI}
&ua={User-Agent}
&mmisdk=3.6.3-10.10.26.
&kw={keywords for app}
&mode=live
&adtype=MMBannerAdTop
HTTP/1.1
```

Argument	iPhone	Android	WP7
{auid}	?	IMEI	Base64-encoded integer value of Device ID
HTTP Host	?	androidsdk.ads.mp.mydas.mobi	ads.mp.mydas.mobi

```
Host: androidsdk.ads.mp.mydas.mobi
Accept-Encoding: gzip
Accept-Language: en-GB, en-US
```

Analytics: Dataflurry

Analytics firm Flurry estimates that 250,000 Motorola Droid phones were sold in the United States during the phone's first week in stores.

Analytics: Dataflurry

Managing User Privacy Expectations

Although some users may be concerned about their privacy, all data is gathered anonymously. On Pinch Media's own website, the company states that when Pinch Analytics is installed within an application, the following information is sent back on each application run:

- A hardware identifier not connectable to any personal information
- The model of the phone (HTC, Samsung, LG, Droid 2, and so on) and operating system (2.1, 2.2, and so on)
- The application's name and version
- The result of a check to see if the device has been jailbroken
- The result of a check to see if the application has been stolen and the developer hasn't been paid
- The length of time the application was run
- The user's location (if the user explicitly agrees to share it)

Analytics: Dataflurry

- The gender and age of the user (if the application uses Facebook Connect)

None of this information can identify the individual. No names, phone numbers, email addresses, or anything else considered personally identifiable information is ever collected. The information sent from applications, when it arrives at the servers, is quickly converted to aggregated reports—unprocessed data is processed as quickly as possible. The aggregated reports show counts and averages, not anything user specific. For instance, a developer can see the following information:

- The number of distinct users who've accessed the application
- The average length of time the application was used
- The percentage of phones using each operating system
- The percentage of each model of phone (3G, 3GS, and so on)
- A breakdown of user locations by country, state, and major metropolitan area (for example, 20,000 in USA, 700 in New York state, 500 in New York City)
- The percentage of users of each gender
- The percentage of users by "age bucket" (21–29, 30–39, and so on)

Analytics: Dataflurry Example

```
POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close

.........O?.n..IPF9LEEU8YW9ICKDSIUQ..2.0.74..BBPIN574646979....O?......O?......device.m
odel..Blackberry8900..device.manufacturer..Research In
Motion..device.os.version..5.2.0.31..runtime.total.memory..169452204..storage.available.
.524280..audio.encodings.,encoding=audio/amr encoding=pcm
encoding=gsm..microedition.commports..USB1..microedition.configuration..CLDC-
1.1..microedition.encoding..ISO8859_1..microedition.global.version..1.0..microedition.lo
cale..en-
GB..microedition.platform..BlackBerry8900/5.0.0.411..microedition.profiles..MIDP-
2.1..wireless.messaging.sms.smsc.
+441234567890..wireless.messaging.mms.mmsc.&http://mms.mycarrier.co.uk/servlets/mms..jav
ax.bluetooth.LocalDevice..true.)javax.microedition.content.ContentHandler..true.)
javax.microedition.global.ResourceManager..true.&javax.microedition.io.SocketConnection.
.true.)javax.microedition.io.file.FileConnection..true.
$javax.microedition.location.Location..true.-
javax.microedition.media.control.VideoControl..true..javax.microedition.media.control.Re
cordControl..true.,javax.microedition.payment.TransactionModule..false..javax.microediti
on.pim.PIM..true.
$javax.microedition.sip.SipConnection..false.*javax.microedition.sip.SipServerConnection
..false..javax.obex.Operation..true.*javax.wireless.messaging.MessageConnection..true.
$javax.wireless.messaging.TextMessage..true.)
javax.wireless.messaging.MultipartMessage..true.
```

POST always calls aar.do or aar.donull
Host is always data.flurry.com

Analytics: Dataflurry Example (Device Identifier)

```
POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close

.........O?.n..IPF9LEEU8YW9ICKDSIUQ..2.0.74..BBPIN574646979....O?......O?......device.m
odel..Bla
Motion..de                                                                    lable.
.524280..a
encoding=(
1.1..micr                                                                     ion.lo
cale..en-
GB..micro
2.1..wire
+4412345671                                                                   s..jav
ax.blueto
javax.mic                                                                     ction.
.true.)jav
$javax.mi
javax.mic                                                                     rol.Re
cordContr                                                                     oediti
on.pim.PI
$javax.mi                                                                     ection
..false..                                                                     rue.
$javax.wireless.messaging.TextMessage..true.)
javax.wireless.messaging.MultipartMessage..true.
```

- BlackBerry: BBPIN574646979 ➔ 22406AC3
- Android: AND{AndroidID, 16 hex bytes}
- iPhone: IPHONE{iPhoneUDID, 40 hex bytes}
- Symbian: ID{SomeIDNumber, 8-10 digit int}
- IMSI: IMSI{IMSI}
- IMEI: IMEI{IMEI, 15 digit int}

Analytics: Dataflurry Example (Device Metadata)

```
POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close

.........O?.n..IPF9LEEU8YW9ICKDSIUQ..2.0.74..BBPIN574646979....O?......O?......device.m
odel..Blackberry8900..device.manufacturer..Research In
Motion..device.os.version..5.2.0.31..runtime.total.memory..169452204..storage.available.
.524280..audio.encodings.,encoding=audio/amr encoding=pcm
encodi
1.1..m                                                                          lo
cale..(
GB..mi
2.1..w
+44123                                                                          av
ax.blu
javax.                                                                          n.
.true.
$javax
javax.                                                                          Re
cordCo                                                                          ti
on.pim
$javax                                                                          on
..false..javax.obex.Operation..true.*javax.wireless.messaging.MessageConnection..true.
$javax.wireless.messaging.TextMessage..true.)
javax.wireless.messaging.MultipartMessage..true.
```

Handset is RIM BlackBerry 8900 with OS 5.2.0.31

device.model Blackberry8900

device.manufacturer Research In Motion

device.os.version 5.2.0.31

runtime.total.memory 169452204

storage.available 524280

Analytics: Dataflurry Example (Device Metadata)

```
POST http://data.flurry.com/aar.donull HTTP/1.1
Host: data.flurry.com
Proxy-Connection: keep-alive
Content-Type: application/octet-stream
Content-Length: 1395
Connection: close
```

Phone Number and Carrier Information

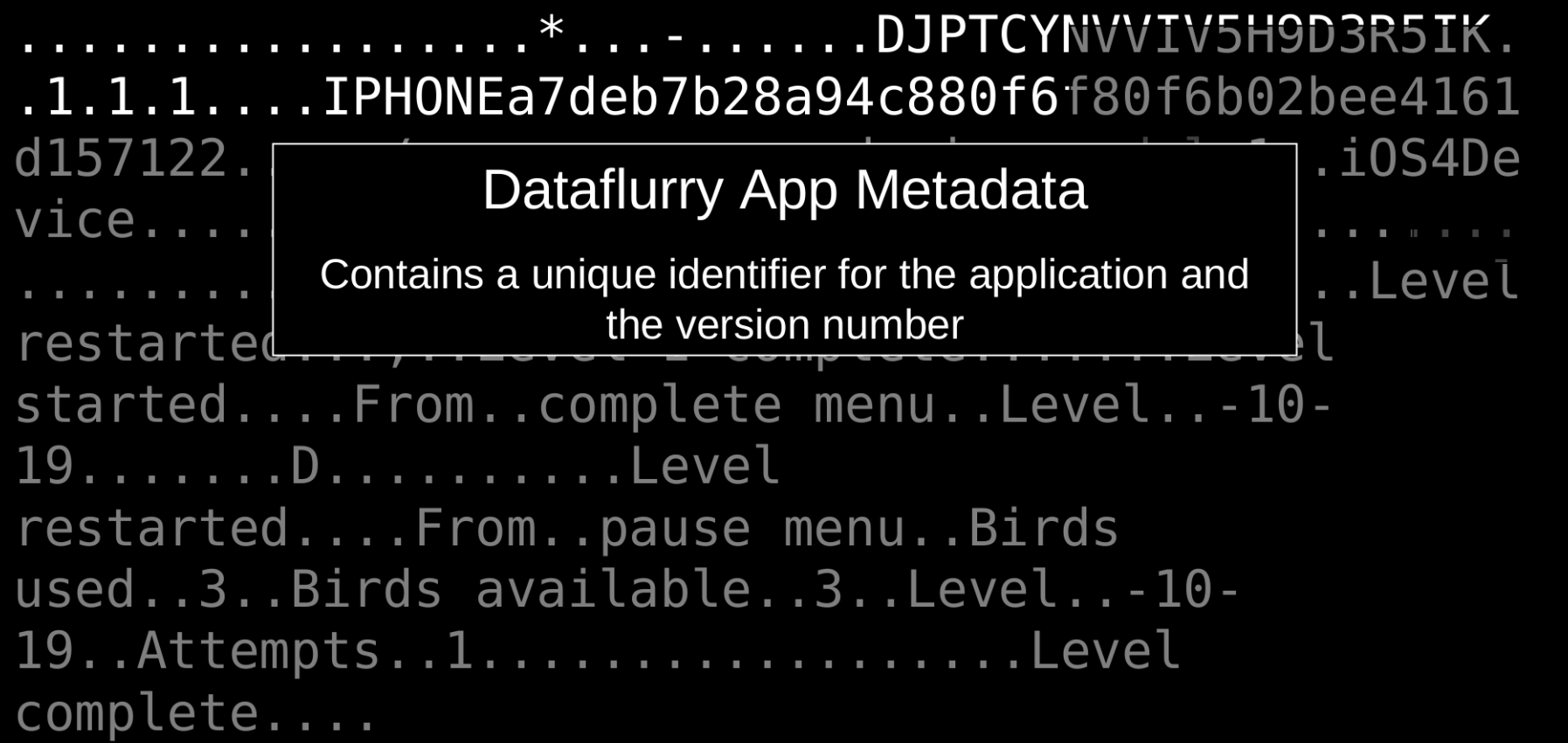
wireless.messaging.sms.smsc +441234567890

wireless.messaging.mms.mmsc

http://mms.mycarrier.co.uk/servlets/mms

```
cale..en-
GB..microedition.platform..BlackBerry8900/5.0.0.411..microedition.profiles..MIDP-
2.1..wireless.messaging.sms.smsc.
+441234567890..wireless.messaging.mms.mmsc.&http://mms.mycarrier.co.uk/servlets/mms..jav
ax.bluetooth.LocalDevice..true.)javax.microedition.content.ContentHandler..true.)
javax.microedition.global.ResourceManager..true.&javax.microedition.io.SocketConnection.
.true.)javax.microedition.io.file.FileConnection..true.
$javax.microedition.location.Location..true.-
javax.microedition.media.control.VideoControl..true..javax.microedition.media.control.Re
cordControl..true.,javax.microedition.payment.TransactionModule..false..javax.microediti
on.pim.PIM..true.
$javax.microedition.sip.SipConnection..false.*javax.microedition.sip.SipServerConnection
..false..javax.obex.Operation..true.*javax.wireless.messaging.MessageConnection..true.
$javax.wireless.messaging.TextMessage..true.)
javax.wireless.messaging.MultipartMessage..true.
```

Analytics: Dataflurry Breakdown



Dataflurry App Metadata

Contains a unique identifier for the application and the version number

Analytics: Dataflurry Breakdown

.....*...-.....DJPTCYNVVIV5H9D3R5IK.
.1.1.1....IPHONEa7deb7b28a94c880f6f80f6b02bee4161
d157122...-./.....-.....device.model.1..iOS4De
vice.....1.1.1...-.wVH.....VG.....
.....Level
restarte
started.
19.....
restarted....From..pause menu..Birds
used..3..Birds available..3..Level..-10-
19..Attempts..1.....Level
complete....

Dataflurry Device Metadata

Contains a unique identifier for the handset and properties of the handset

Analytics: Dataflurry Breakdown

Analytics: Dataflurry Device Metadata

Device Hardware

- device.model
- device.manufacturer

Phone Information

- wireless.messaging.sms.smsc
- wireless.messaging.mms.mmsc
- IMSI
- IMEI

OS Information

- build.brand
- build.id
- device.os.version
- version.release

Cell Network Metadata

- network.mcc
- network.mnc
- network.lac
- network.cellid
- com.sonyericsson.net.cellid
- com.sonyericsson.net.lac
- com.sonyericsson.net.mcc
- com.sonyericsson.net.mnc
- CellID
- cellid
- LAC
- Lac
- lac
- MCC
- Mcc
- mcc
- MNC
- Mnc
- mnc
- com.nokia.mid.countrycode
- com.nokia.mid.cellid
- com.nokia.mid.networkid
- com.nokia.network.access

Analytics: Dataflurry Device Metadata

- device.model
- device.manufacturer
- device.os.version
- device.software.version
- build.brand
- build.id
- version.release
- runtime.total.memory
- storage.available.size
- audio.encodings
- microedition.commports
- microedition.configuration
- microedition.encoding
- microedition.global.version
- microedition.locale
- microedition.platform
- microedition.profiles
- wireless.messaging.sms.smsc
- wireless.messaging.mms.mmsc
- javax.bluetooth.LocalDevice
- javax.microedition.content.ContentHandler
- javax.microedition.global.ResourceManager
- javax.microedition.io.SocketConnection
- javax.microedition.io.file.FileConnection
- javax.microedition.location.Location
- javax.microedition.media.control.VideoControl
- javax.microedition.media.control.RecordControl
- javax.microedition.payment.TransactionModule
- javax.microedition.pim.PIM
- javax.microedition.sip.SipConnection
- javax.microedition.sip.SipServerConnection
- javax.obex.Operation
- javax.wireless.messaging.MessageConnection
- javax.wireless.messaging.TextMessage
- javax.wireless.messaging.MultipartMessage
- pur.date
- rel.date
- pur.price
- store.id
- bluetooth.api.version
- fileconn.dir.memorycard
- fileconn.dir.photos.file
- fileconn.dir.photos.name
- fileconn.dir.private.file
- fileconn.dir.videos.file
- fileconn.dir.photos.name
- fileconn.dir.tones
- fileconn.dir.tones.name
- microedition.chapi.version
- microedition.io.file.FileConnection.version
- microedition.jtwi.version
- microedition.m3g.version
- microedition.pim.version
- microedition.location.version
- supports.audio.capture
- supports.mixing
- supports.recording
- supports.video.capture
- video.snapshot.encodings
- microedition.media.version
- streamable.contents
- video.encodings
- com.sonyericsson.net.cellid
- com.sonyericsson.net.lac
- com.sonyericsson.net.mcc
- com.sonyericsson.net.mnc
- microedition.timezone
- microedition.hostname
- IMEI
- IMSI
- network.mcc
- network.mnc
- network.lac
- network.cellid
- CellID
- Cellid
- cellId
- LAC
- lac
- Lac
- MCC
- Mcc
- mcc
- MNC
- Mnc
- mnc
- commports.maxbaudrate
- com.nokia.mid.countrycode
- com.nokia.mid.cellid
- com.nokia.mid.networkid
- com.nokia.network.access
- version.release
- country.code
- default.timezone
- storage.available

Mobile Gateway HTTP Headers and Data Aggregators: DataFlurry

```
POST /aar.do HTTP/1.0
Connection: Keep-Alive
User-Agent: SonyEricssonS500i/R8BA Profile/MIDP-2.0 Configuration/CLDC-1.1
UNTRUSTED/1.0
Host: data.flurry.com
Accept: */*
Accept-Charset: utf-8, iso-8859-1
Content-Type: application/octet-stream
Content-Length: 2327
Via: infoX WAP Gateway V300R001, Huawei Technologies
x-up-calling-line-id: +44
x-forwarded-for:
x-huawei-IMSI:

.........%......KHFP142N4PHQBQ8R7XEH..1.5.0..IMEIIMEI 35808401-728365-6-
65 ...!.
$5....%...*....microedition.platform..SonyEricssonS500i/R8BA024....1.5.0...%.
.N(.....;0........onChatMessageSent...(..onChatNewSession...Q.
```

Analytics: Other Methods & Providers

Many apps send a beacon out when the app is started

- Can be first- or third-party
- Typicaly includes phone ID; can include IMEI, geo, etc.
- Examples: Qriously, Com2Us, Fluentmobile, Papayamobile

BB App World will geolocate users using MCC and MNC to determine what content to show in the app store

Android ID Changes

Typically, Android IDs have followed the format below:

ANDROID_ID															
2	0	0	Hex encoded IMEI (inc. check digit)												
2	2	MEID?													
3	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Seeing Android IDs starting to use the full 64-bits and decent distribution

Special case: **9774d56d682e549c** is a non-unique Android ID (related to a Froyo release bug)

Windows Phone 7 Device IDs

App descriptions in the Marketplace will indicate whether a given app will use the account identifier or the phone identifier, both or neither.

Device IDs are 20-byte values (40-byte hex strings) represented in the following ways:

- A1A2A3A4A5B1B2B3B4B5C1C2C3C4C5D1D2D3D4D5 is the usual ASCII representation, typically in upper-case
- A1A2A3A4-A5B1B2B3-B4B5C1C2-C3C4C5D1-D2D3D4D5
- A1-A2-A3-A4-A5-B1-B2-B3-B4-B5-C1-C2-C3-C4-C5-D1-D2-D3-D4-D5
- Base64 encoding the integer value of the identifier. The resulting string looks like oaKjpKWxsrO0tcHCw8TF0dLT1NU=
- Long number string (i.e. 1962122536433201191792182411891841901332040148215211 8)

Windows Phone 7 App IDs

All traffic from a Win7 handset appears to carry the GUID associated with the app in the HTTP Referer field.

```
POST /Service/ServiceElleStyleTag.svc HTTP/1.1
Accept: */*
Referer: file:///Applications/Install/BB7CD1F6-BCDA-DF11-A844-
00237DE2DB9E/Install/
Content-Length: 243
Accept-Encoding: identity
Content-Type: text/xml; charset=utf-8
SOAPAction: "urn:ServiceElleStyleTag/GetPlaces
User-Agent: NativeHost
Host: styletag.elle.fr
Connection: Keep-Alive
Cache-Control: no-cache

<s:Envelope
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetPlacesIn
Area><centerLat>51.899262428283691</centerLat><centerLong>-
2.0722637176513672</centerLong><take>10</take><skip>0</skip></GetPlacesI
nArea></s:Body></s:Envelope>
```

If the Referer field is formatted in this way only for WP7 apps, it may be possible to use this as a mobile TDI against the Live account

Windows Phone 7 MSN Ads

Apps that use MSN's Mobile Ad service associate with the handset's Live account instead of the handset itself.

```
GET /v3/Delivery/Placement?
pubid=break001wp7
&pid=USM3PB
&adm=1
&cfmt=text,image&sft=jpeg,png,gif&w=480&h=80
&fmt=json
&cltp=app
&dim=le
&nct=1&lc=en-GB&idtp=anid
&uid=63388195C29A61B3EA2E62EEFFFFFFFF HTTP/1.1
Accept: */*
Referer: file:///Applications/Install/D1CD2DCB-7CD5-DF11-A844-
0237DE2DB9E/Install/
Accept-Encoding: identity
User-Agent: NativeHost (or occasionally, User-Agent: Windows Phone Ad
Client (Xna)/5.1.0.0)
Host: mobileads.msn.com
Connection: Keep-Alive
```

Windows Phone 7 Marketplace

The WP7 Marketplace also associates with the handset's Live account, and can include enough metadata to indicate that the account is active on a handset.

```
GET /v3.2/en-GB/apps?
orderBy=downloadRank
&cost=paid&chunkSize=10
&clientType=WinMobile%207.0
&store=Zest
&store=O2OGB
&store=HTC HTTP/1.1
User-Agent: ZDM/4.0; Windows Mobile 7.0;
Host: catalog.zune.net (or origin-catalog.zune.net)
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ANON=A=63388195C29A61B3EA2E62EEFFFFFFFF&E=b1
NAP=V=1.9&E=ac2&C=WbPWets1RmtLDSMaoaSy121N44id48LnRE
EVrcQ0q8wd6Ds0g&W=1
```

The "store" arguments can help identify the handset manufacturer and the carrier

This is the ANON cookie value for the Live account associated with the handset

~~A~~busing BADASS for Fun and Profit

Medialytics traffic from Android uses MD5 sum of the Android ID string
Example: 200142d4dfcd56a9 = DEA9F697DEB0CBBB8433018A0B723BF9

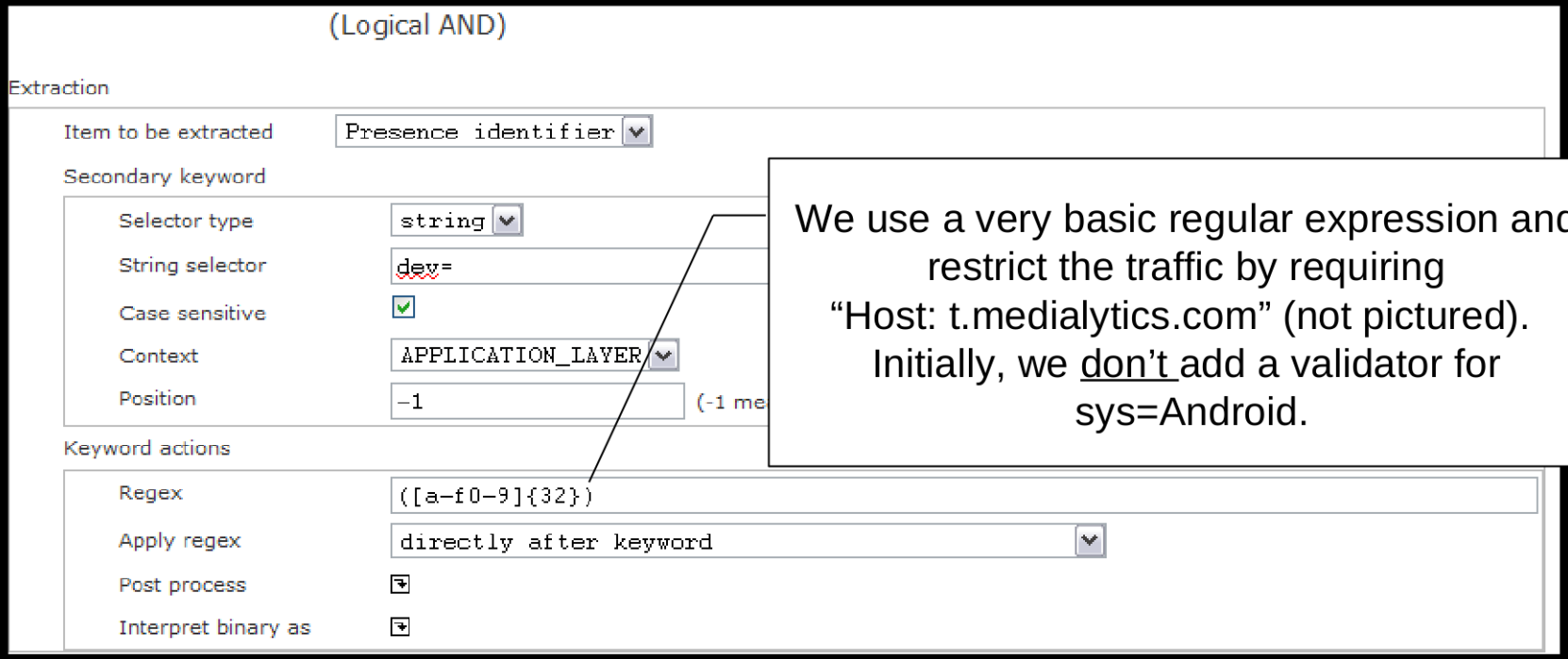
```
POST /event HTTP/1.1
Content-Length: 543
Content-Type: application/x-www-form-urlencoded
Host: t.medialytics.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

v=2.0&b=0&tok=CAFEBABE
&sys=Android
&sysv=2.3.3
&dev=dea9f697deb0cbbb8433018a0b723bf9
&model=google+Nexus+One
&app=77327b6f00e7aa0f452d9d3ac3e2d1618e0f3aaa
&appv=2.5.3-BB70302
&data=...
```

Odds are that they're using something similar for iPhones….

~~Ab~~using BADASS for Fun and Profit

We can use the FKB PCAP testing step as a launching point for a fishing expedition…



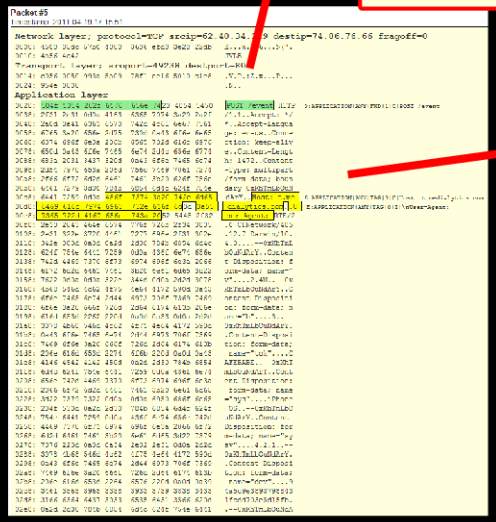
We use a very basic regular expression and restrict the traffic by requiring "Host: t.medialytics.com" (not pictured). Initially, we don't add a validator for sys=Android.

This should give us traffic for Android, iPhone and any other platform they're using MD5 sums against.

~~Abusing~~ BADASS for Fun and Profit

BADASS can show us packet dumps of traffic that completely matched the rule, and traffic that matched on the selector but failed on the rule.

```
Application layer
0028: 504f 5354 202f 6576  656e 7420 4854 5450   POST /event HTTP  0:APPLICATION|ANY|FWD|1|C|POST /event
0038: 2f31 2e31 0d0a 4163  6365 7074 3a20 2a2f   /1.1..Accept: */
```



Green indicates the selector hitting in the packet payload.

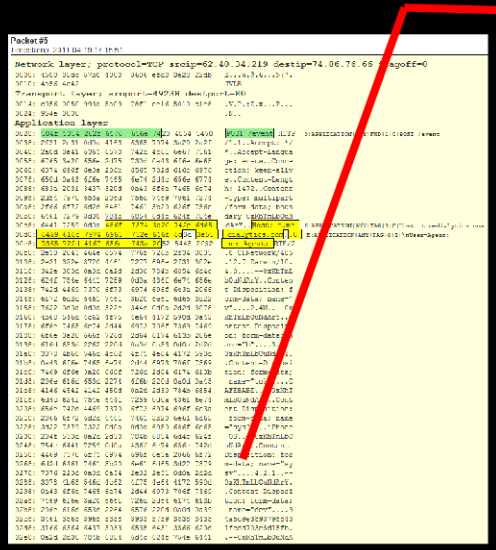
```
00b8: 6461 7279 3d30 784b  6854 6d4c 624f 754e   dary=0xKhTmLbOuN
00c8: 6441 7259 0d0a 486f  7374 3a20 742e 6d65   dArY..Host: t.me
00d8: 6469 616c 7974 6963  732e 636f 6d0d 0a55   dialytics.com..U
00e8: 7365 722d 4167 656e  743a 2052 5445 2f32   ser-Agent: RTE/2
00f8: 2e30 2043 464e 6574  776f 726b 2f34 3835   .0 CFNetwork/485
```

Yellow indicates where part of the rule hit. In this case, it's the "Host: t.medialytics.com" validator and where a User-Agent extractor hit in the traffic.

The lack of other highlighted regions indicates that there was no hit on the "dev" presence identifier…

~~Abusing~~ BADASS for Fun and Profit

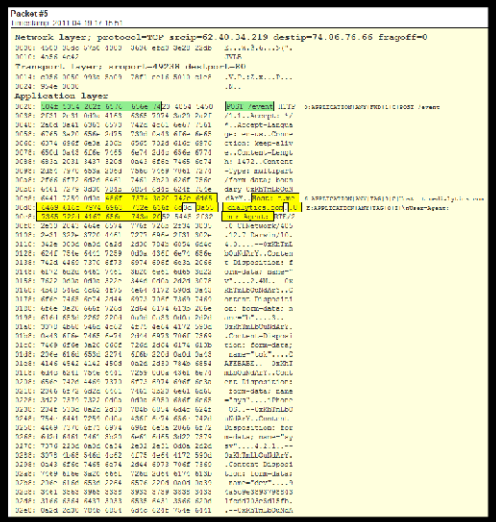
… but that doesn't mean that the dev identifier isn't there! It's just formatted differently.



```
01f8: 6d4c 624f 754e 6441  7259 0d0a 436f 6e74   mLbOuNdArY..Cont
0208: 656e 742d 4469 7370  6f73 6974 696f 6e3a   ent-Disposition:
0218: 2066 6f72 6d2d 6461  7461 3b20 6e61 6d65    form-data; name
0228: 3d22 7379 7322 0d0a  0d0a 6950 686f 6e65   ="sys"....iPhone
0238: 204f 530d 0a2d 2d30  784b 6854 6d4c 624f    OS..--0xKhTmLbO
0248: 754e 6441 7259 0d0a  436f 6e74 656e 742d   uNdArY..Content-
0258: 4469 7370 6f73 6974  696f 6e3a 2066 6f72   Disposition: for
0268: 6d2d 6461 7461 3b20  6e61 6d65 3d22 7379   m-data; name="sy
0278: 7376 220d 0a0d 0a34  2e32 2e31 0d0a 2d2d   sv"....4.2.1..--
0288: 3078 4b68 546d 4c62  4f75 4e64 4172 590d   0xKhTmLbOuNdArY.
0298: 0a43 6f6e 7465 6e74  2d44 6973 706f 7369   .Content-Disposi
02a8: 7469 6f6e 3a20 666f  726d 2d64 6174 613b   tion: form-data;
02b8: 206e 616d 653d 2264  6576 220d 0a0d 0a39    name="dev"....9
02c8: 3461 3563 3965 3338  3933 3739 3838 3433   4a5c9e3893798843
02d8: 3166 6364 6437 3033  6535 6431 3566 620d   1fcdd703e5d15fb.
02e8: 0a2d 2d30 784b 6854  6d4c 624f 754e 6441   .--0xKhTmLbOuNdA
```

~~Ab~~using BADASS for Fun and Profit

Using the FKB PCAP test in this manner has shown us that:



1. Medialytic traffic can appear as form-data
2. Our theory about iPhone traffic having a similar structure holds
3. iPhone traffic is using the MD5 sum against the UUID
4. We can create a rule against the iPhone variant with ease (“sys=iPhone OS” vs. “sys=Android”)

and most importantly:

1. **Creativity, iterative testing, domain knowledge, and the right tools can help us target multiple platforms in a very short time period.**

To bring us full-circle…

AdMob

Dataflurry
(Flurry/Pinch Media)

MobClix

Medialytics
(Medialets)