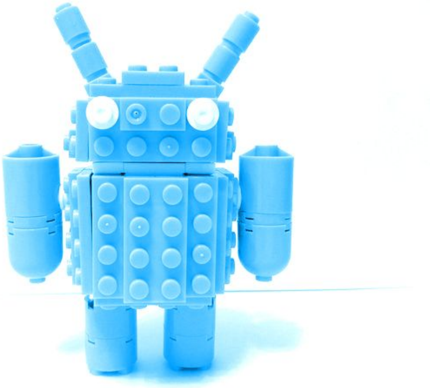
Breaking the bank

Engenharia reversa de aplicativos Android na prática

@ThiagoValverde

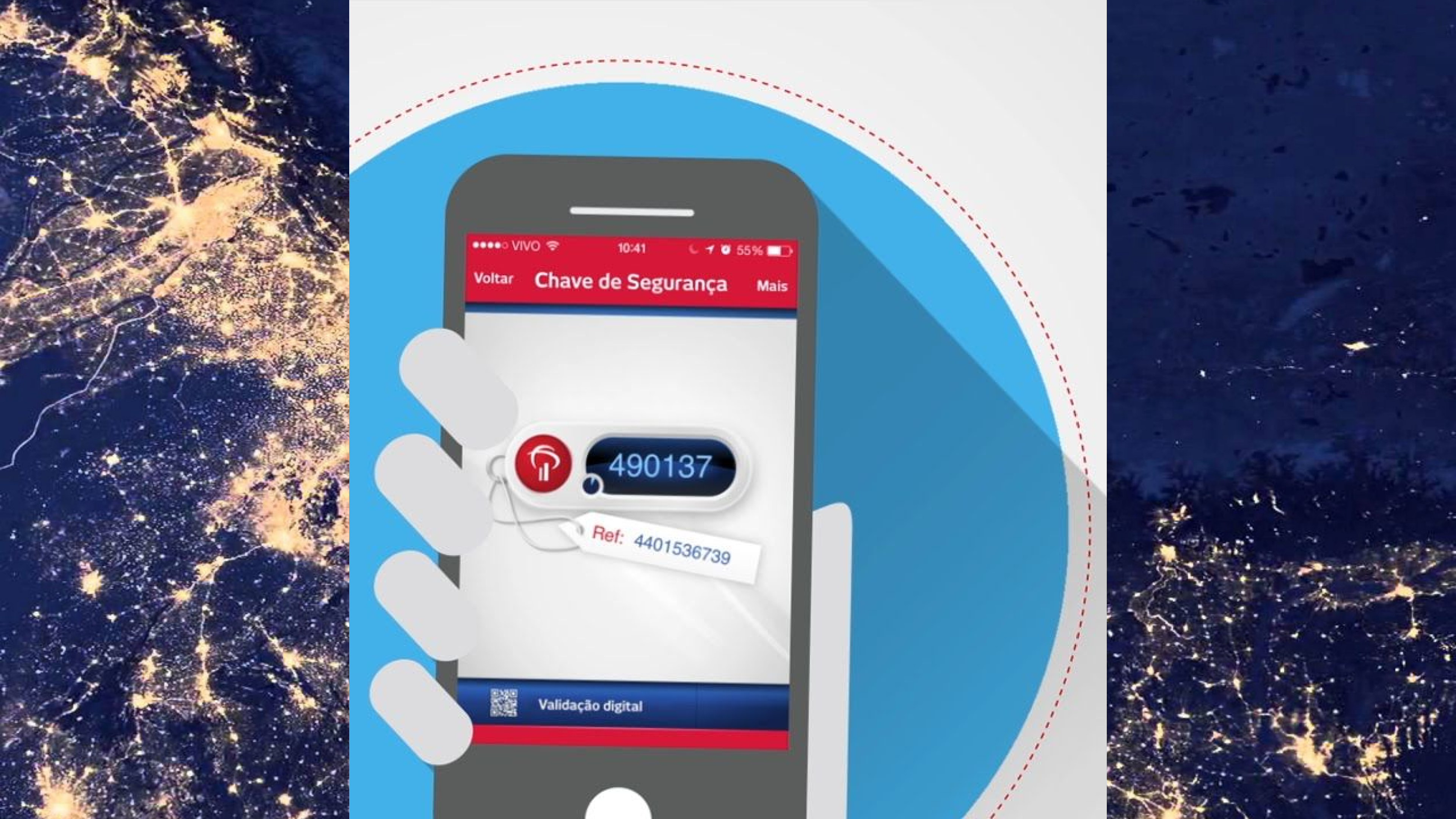


São Bernardo do Campo

UNICAMP

Google

g.co/vrp


●●●●○ VIVO
10:41
55%
Voltar
Chave de Segurança
Mais
490137
Ref: 4401536739
Validação digital

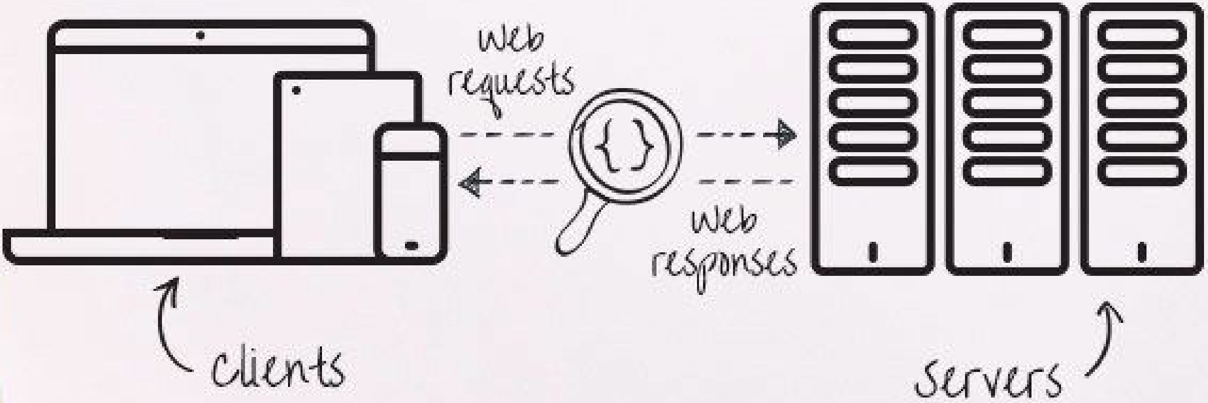
Burp Suite

Fiddler

Charles

mitmproxy

Fiddler

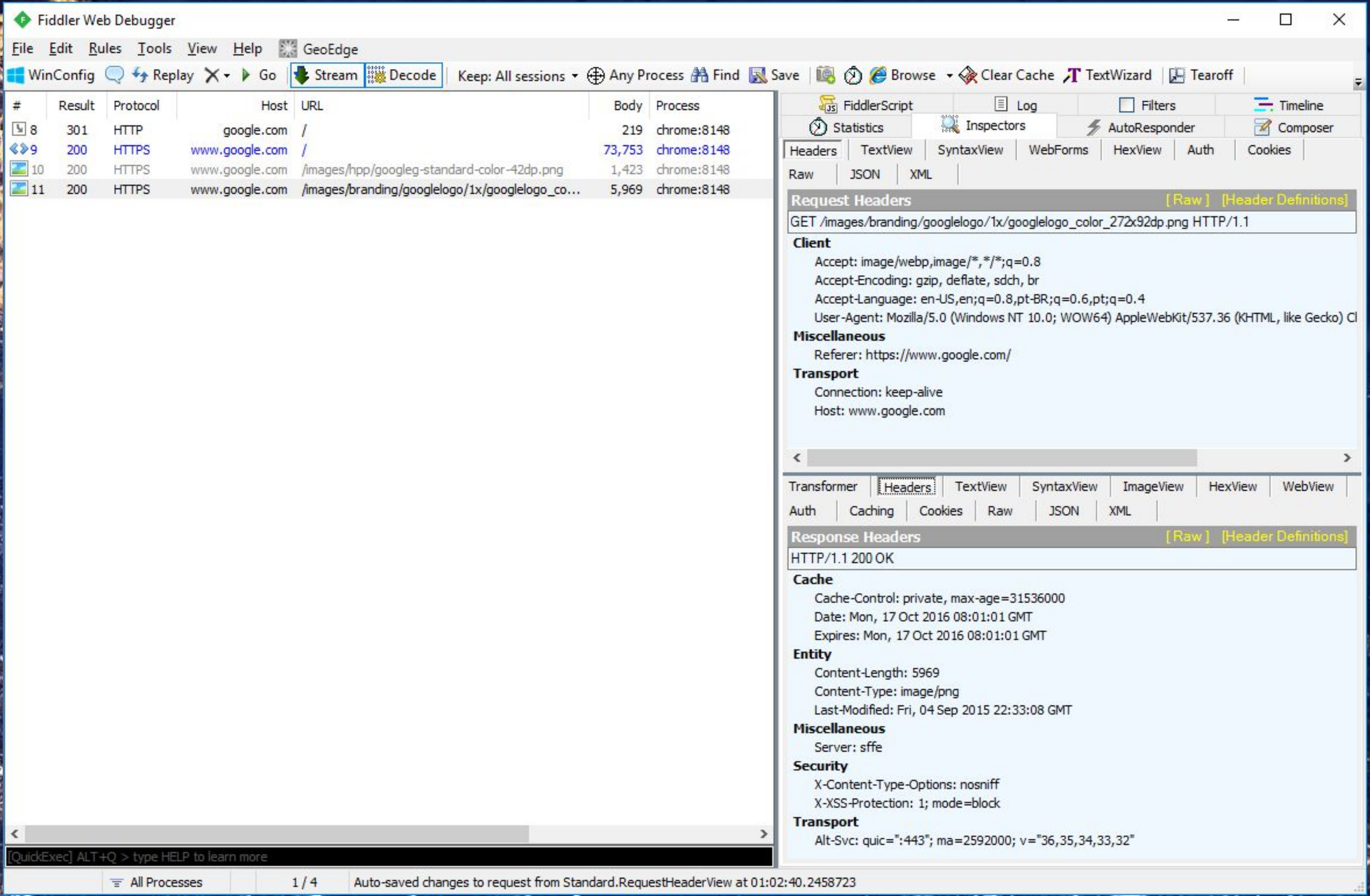


http://www.telerik.com/fiddler

Telerik Fiddler

v4.6.2.3

http://www.telerik.com/fiddler


Fiddler Web Debugger
File Edit Rules Tools View Help GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
FiddlerScript Log Filters Timeline
Statistics Inspectors AutoResponder Composer
Headers TextView SyntaxView WebForms HexView Auth Cookies
Raw JSON XML
Transformer Headers TextView SyntaxView ImageView HexView WebView
Auth Caching Cookies Raw JSON XML
[QuickExec] ALT+Q > type HELP to learn more
All Processes
1 / 4

#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148

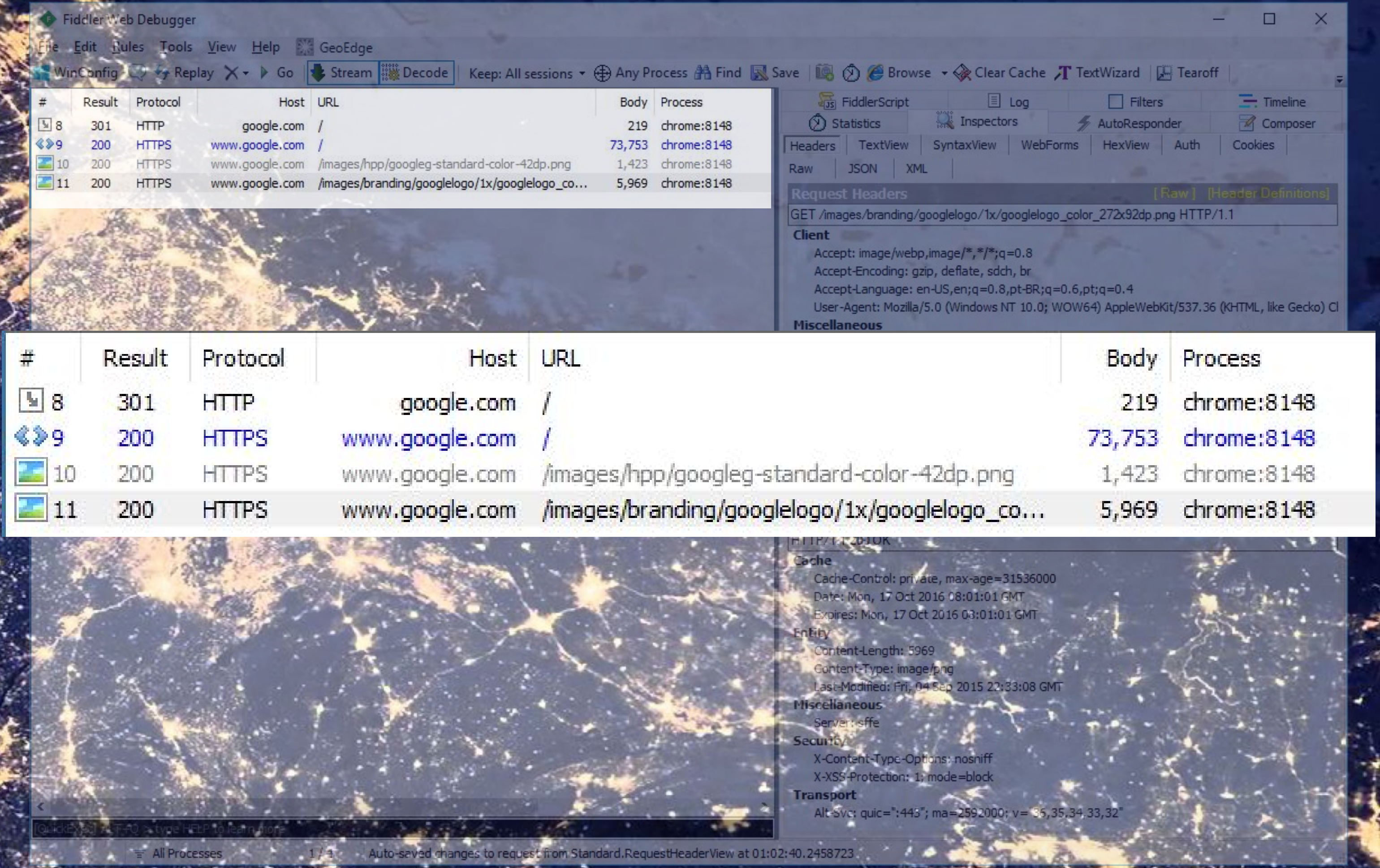
Request Headers [Raw] [Header Definitions]

```
GET /images/branding/googlelogo/1x/googlelogo_color_272x92dp.png HTTP/1.1
Client
    Accept: image/webp,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch, br
    Accept-Language: en-US,en;q=0.8,pt-BR;q=0.6,pt;q=0.4
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Cl
Miscellaneous
    Referer: https://www.google.com/
Transport
    Connection: keep-alive
    Host: www.google.com
```

Response Headers [Raw] [Header Definitions]

```
HTTP/1.1 200 OK
Cache
    Cache-Control: private, max-age=31536000
    Date: Mon, 17 Oct 2016 08:01:01 GMT
    Expires: Mon, 17 Oct 2016 08:01:01 GMT
Entity
    Content-Length: 5969
    Content-Type: image/png
    Last-Modified: Fri, 04 Sep 2015 22:33:08 GMT
Miscellaneous
    Server: sffe
Security
    X-Content-Type-Options: nosniff
    X-XSS-Protection: 1; mode=block
Transport
    Alt-Svc: quic=":443"; ma=2592000; v="36,35,34,33,32"
```

Auto-saved changes to request from Standard.RequestHeaderView at 01:02:40.2458723


Fiddler Web Debugger
File Edit Rules Tools View Help GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
FiddlerScript Log Filters Timeline
Statistics Inspectors AutoResponder Composer
Headers TextView SyntaxView WebForms HexView Auth Cookies
Raw JSON XML
Request Headers [Raw] [Header Definitions]
All Processes 1 / 4

#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148

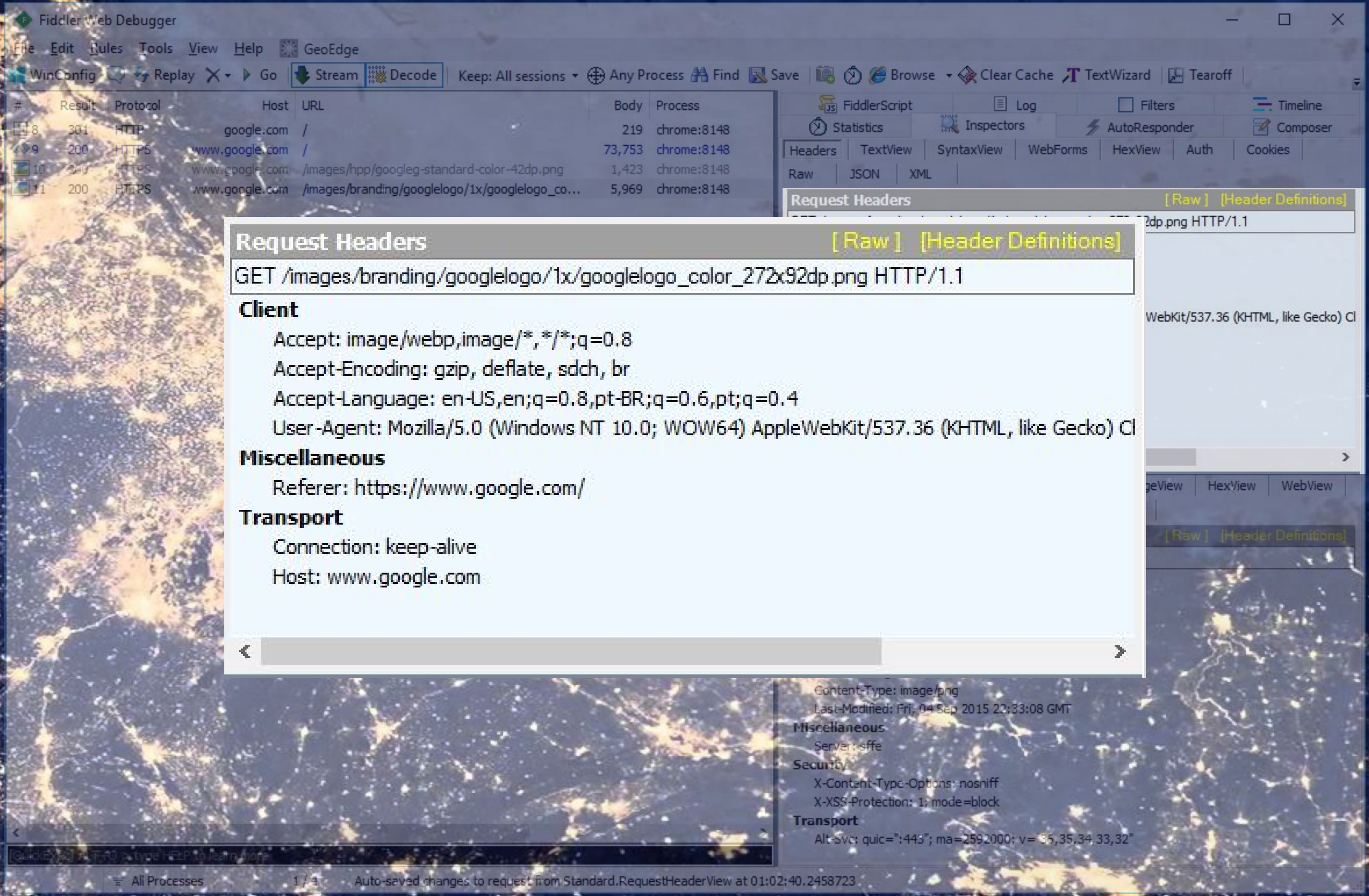
```
GET /images/branding/googlelogo/1x/googlelogo_color_272x92dp.png HTTP/1.1
Client
    Accept: image/webp,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch, br
    Accept-Language: en-US,en;q=0.8,pt-BR;q=0.6,pt;q=0.4
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Cl
Miscellaneous
```

#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148

```
HTTP/1.1 200 OK
Cache
    Cache-Control: private, max-age=31536000
    Date: Mon, 17 Oct 2016 08:01:01 GMT
    Expires: Mon, 17 Oct 2016 08:01:01 GMT
Entity
    Content-Length: 5969
    Content-Type: image/png
    Last-Modified: Fri, 04 Sep 2015 22:33:08 GMT
Miscellaneous
    Server: sffe
Security
    X-Content-Type-Options: nosniff
    X-XSS-Protection: 1; mode=block
Transport
    Alt-Svc: quic=":443"; ma=2592000; v="36,35,34,33,32"
```

```
[QuickExec] ALT+Q > type HELP to learn more
```

Auto-saved changes to request from Standard.RequestHeaderView at 01:02:40.2458723



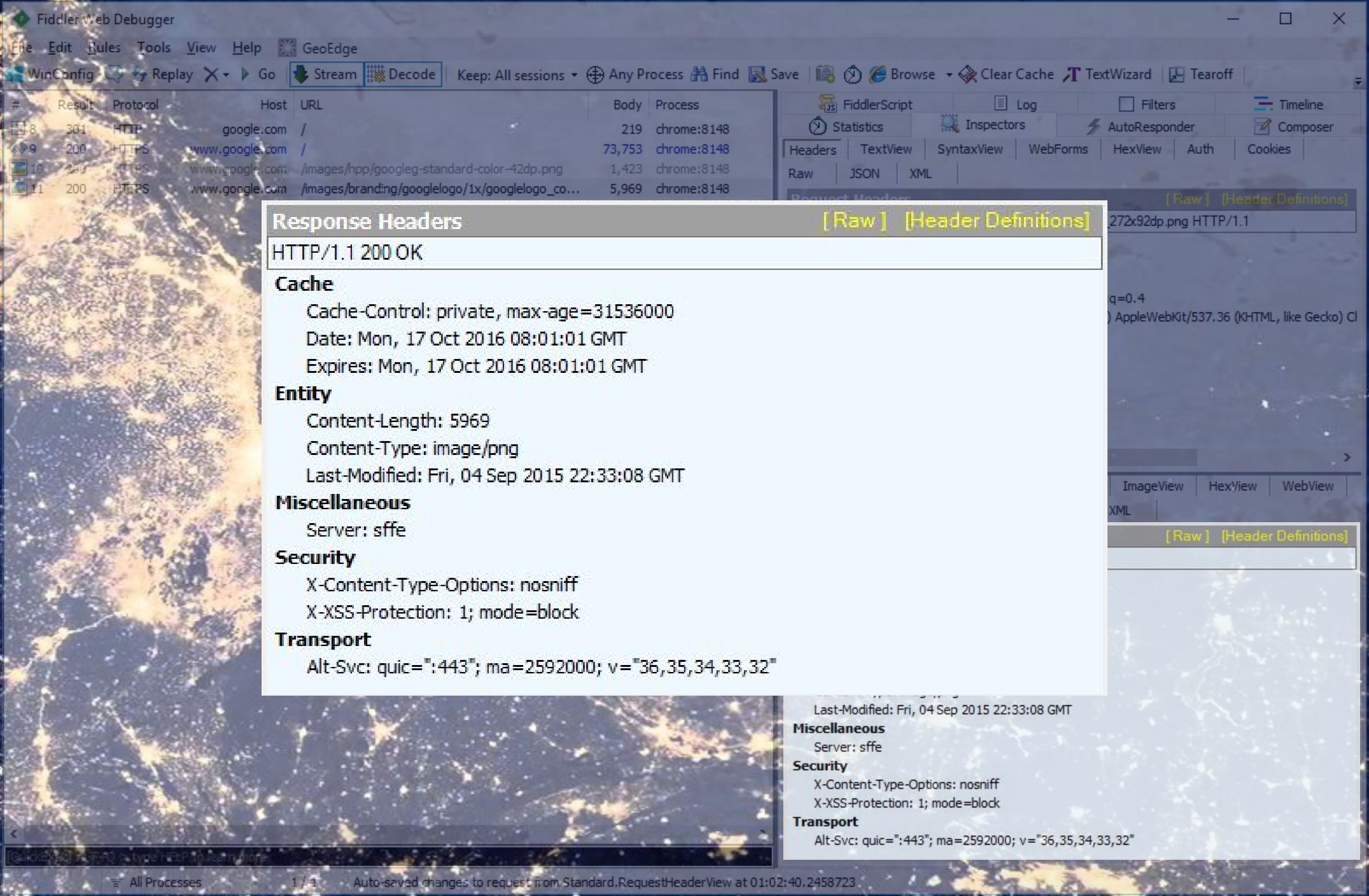
#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148

Request Headers [Raw] [Header Definitions]

```
GET /images/branding/googlelogo/1x/googlelogo_color_272x92dp.png HTTP/1.1
Client
    Accept: image/webp,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch, br
    Accept-Language: en-US,en;q=0.8,pt-BR;q=0.6,pt;q=0.4
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Cl
Miscellaneous
    Referer: https://www.google.com/
Transport
    Connection: keep-alive
    Host: www.google.com
```

```
    Content-Type: image/png
    Last-Modified: Fri, 04 Sep 2015 22:33:08 GMT
Miscellaneous
    Server: sffe
Security
    X-Content-Type-Options: nosniff
    X-XSS-Protection: 1; mode=block
Transport
    Alt-Svc: quic=":443"; ma=2592000; v="36,35,34,33,32"
```

```
All Processes    1 / 4    Auto-saved changes to request from Standard.RequestHeaderView at 01:02:40.2458723
```

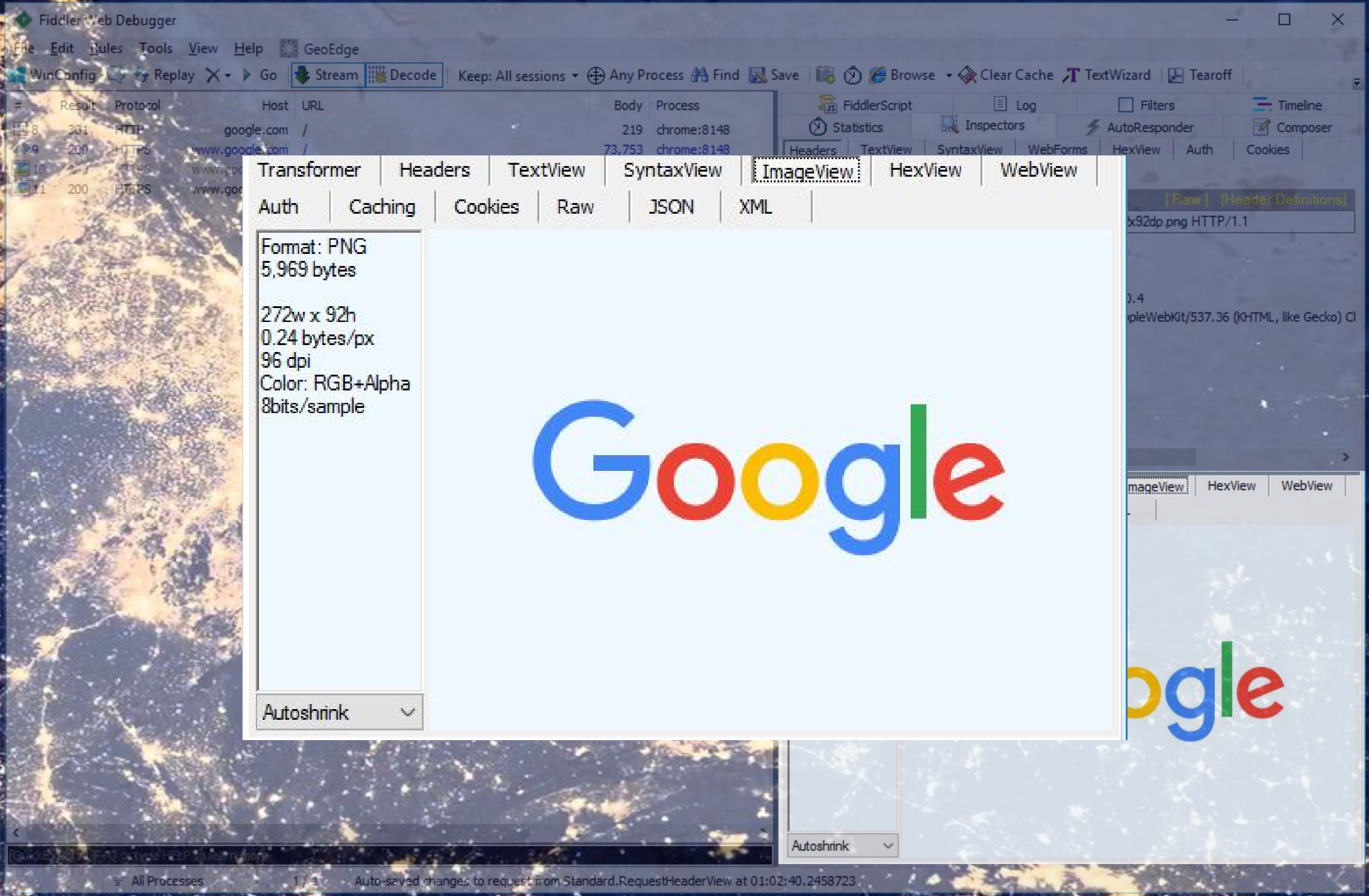

Fiddler Web Debugger
File Edit Rules Tools View Help GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
FiddlerScript Log Filters Timeline
Statistics Inspectors AutoResponder Composer
Headers TextView SyntaxView WebForms HexView Auth Cookies
Raw JSON XML
ImageView HexView WebView
XML
[Raw] [Header Definitions]

#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148

```
Response Headers                                  [ Raw ]  [Header Definitions]
HTTP/1.1 200 OK
Cache
    Cache-Control: private, max-age=31536000
    Date: Mon, 17 Oct 2016 08:01:01 GMT
    Expires: Mon, 17 Oct 2016 08:01:01 GMT
Entity
    Content-Length: 5969
    Content-Type: image/png
    Last-Modified: Fri, 04 Sep 2015 22:33:08 GMT
Miscellaneous
    Server: sffe
Security
    X-Content-Type-Options: nosniff
    X-XSS-Protection: 1; mode=block
Transport
    Alt-Svc: quic=":443"; ma=2592000; v="36,35,34,33,32"
```

```
272x92dp.png HTTP/1.1
q=0.4
) AppleWebKit/537.36 (KHTML, like Gecko) Cl
```

All Processes   1 / 4   Auto-saved changes to request from Standard.RequestHeaderView at 01:02:40.2458723



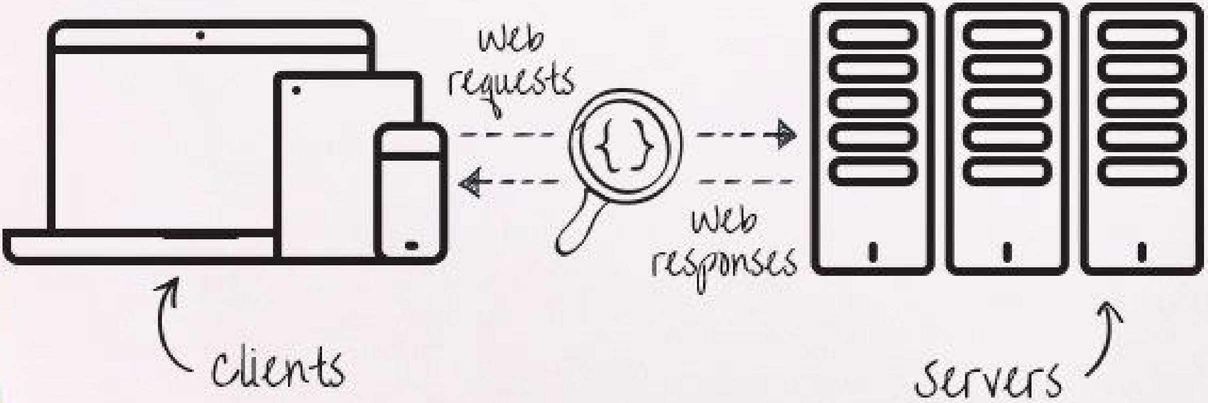
Fiddler Web Debugger
File Edit Rules Tools View Help GeoEdge
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff
FiddlerScript Log Filters Timeline
Statistics Inspectors AutoResponder Composer
Transformer Headers TextView SyntaxView ImageView HexView WebView
Auth Caching Cookies Raw JSON XML
Autoshrink
Google
All Processes

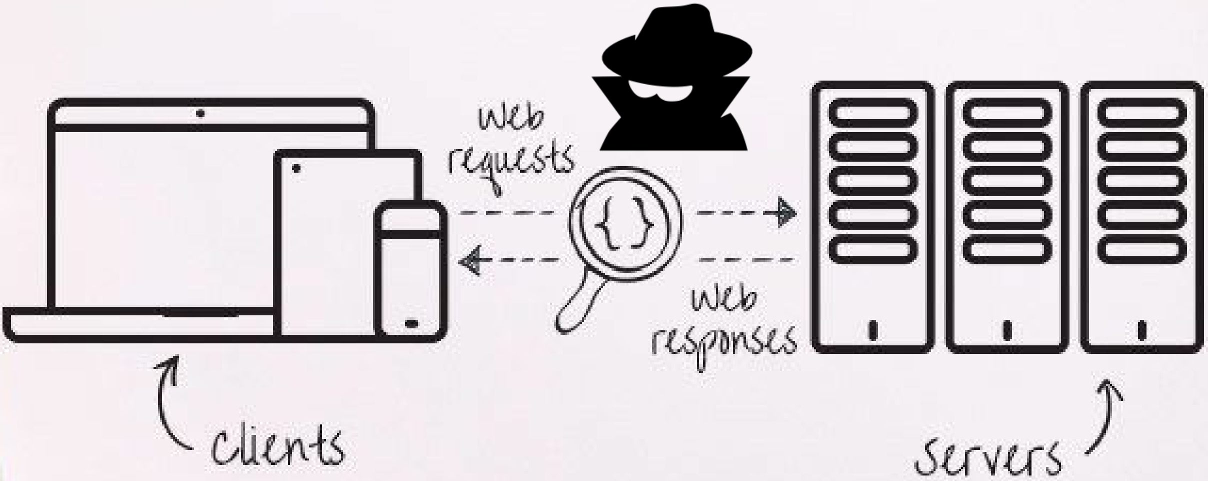
#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.goo			
11	200	HTTPS	www.goo			

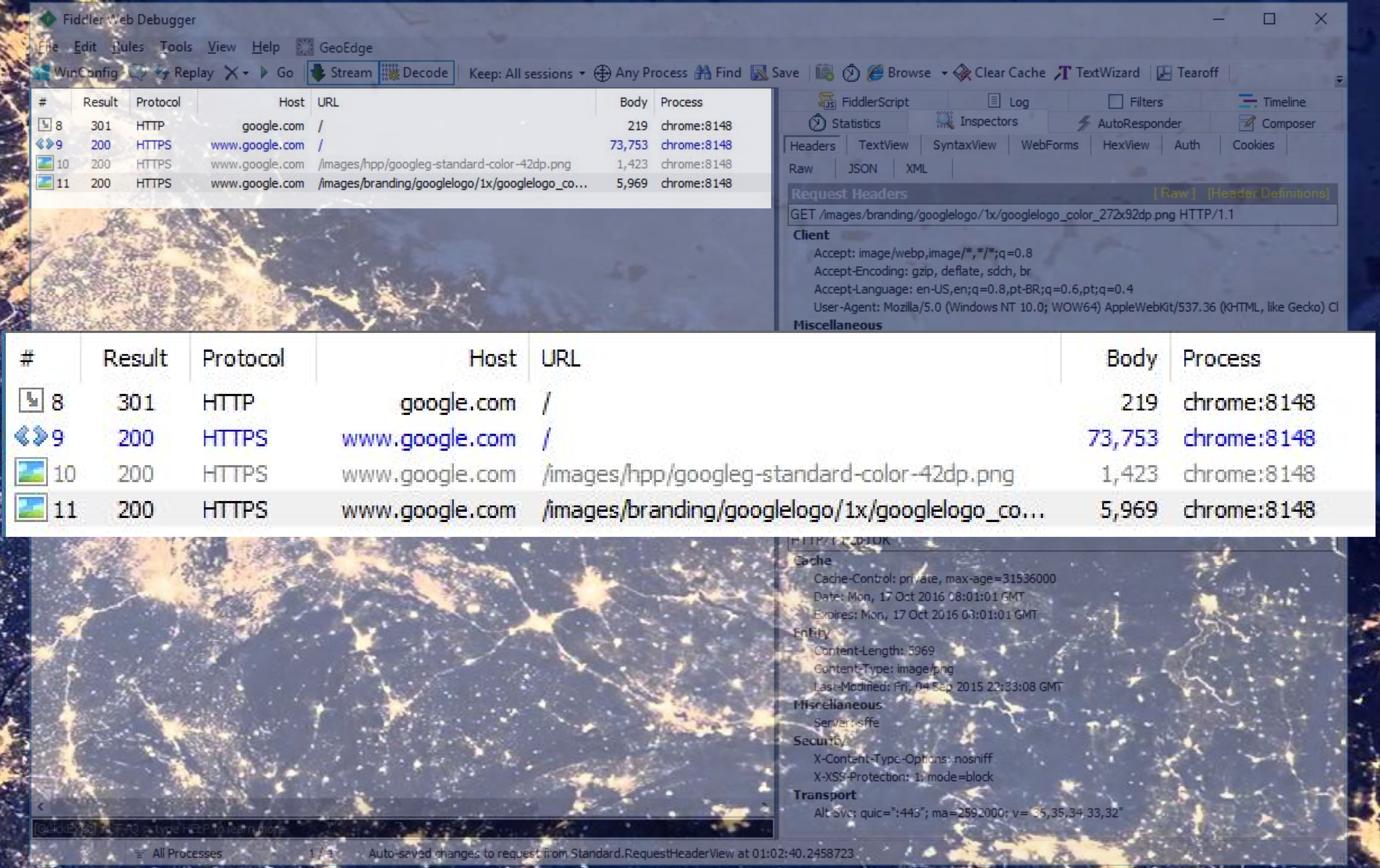
Format: PNG
5,969 bytes

272w x 92h
0.24 bytes/px
96 dpi
Color: RGB+Alpha
8bits/sample

Auto-saved changes to request from Standard.RequestHeaderView at 01:02:40.2458723


web
requests
web
responses
clients
servers


Web requests
{ }
Web responses
clients
servers



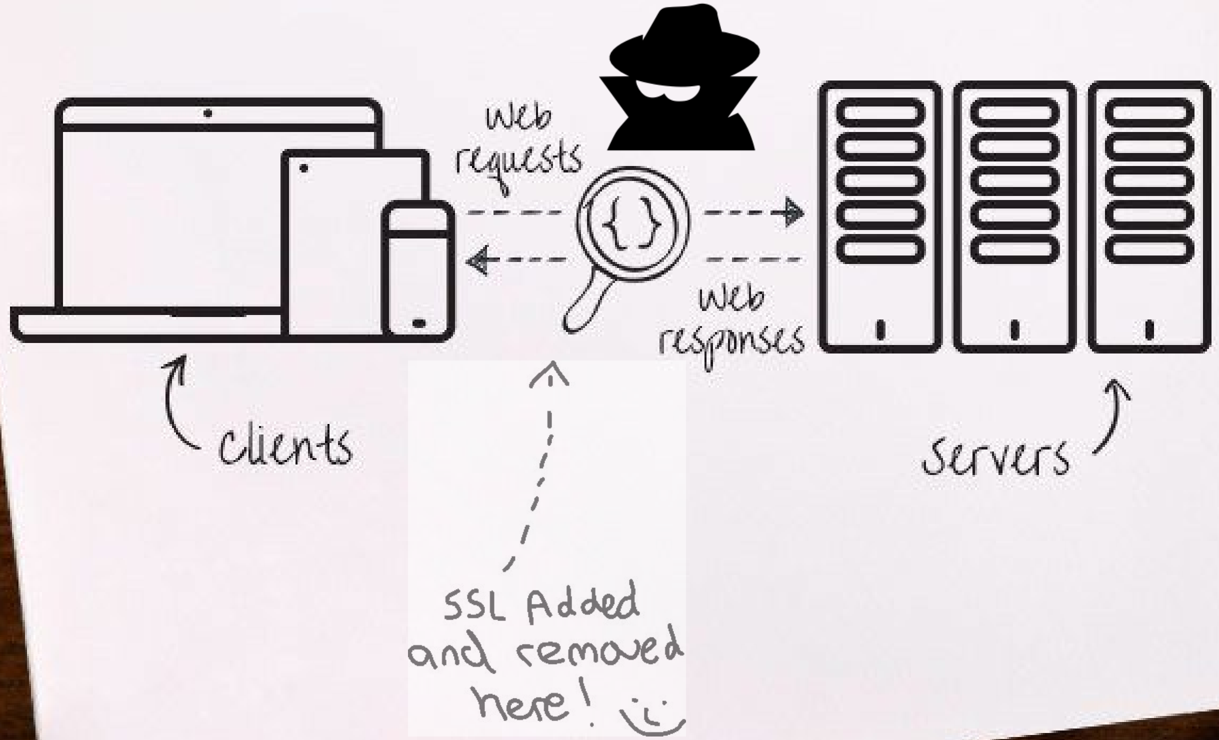
#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148

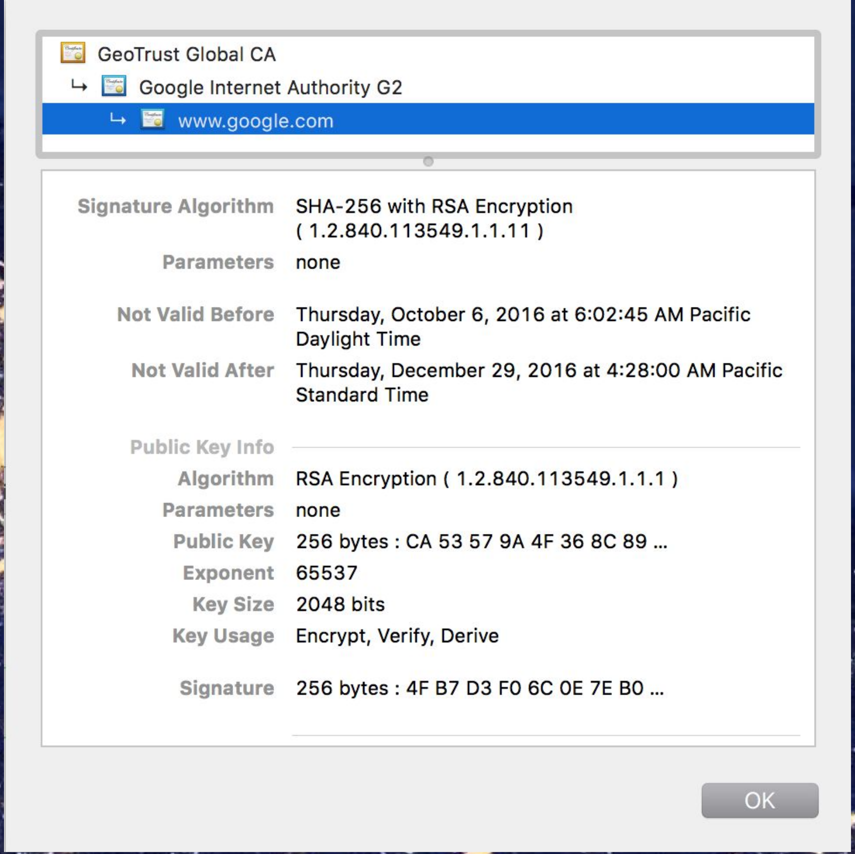
```
GET /images/branding/googlelogo/1x/googlelogo_color_272x92dp.png HTTP/1.1
Client
    Accept: image/webp,image/*,*/*;q=0.8
    Accept-Encoding: gzip, deflate, sdch, br
    Accept-Language: en-US,en;q=0.8,pt-BR;q=0.6,pt;q=0.4
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Cl
Miscellaneous
```

```
HTTP/1.1 200 OK
Cache
    Cache-Control: private, max-age=31536000
    Date: Mon, 17 Oct 2016 08:01:01 GMT
    Expires: Mon, 17 Oct 2016 08:01:01 GMT
Entity
    Content-Length: 5969
    Content-Type: image/png
    Last-Modified: Fri, 04 Sep 2015 22:33:08 GMT
Miscellaneous
    Server: sffe
Security
    X-Content-Type-Options: nosniff
    X-XSS-Protection: 1; mode=block
Transport
    Alt-Svc: quic=":443"; ma=2592000; v="36,35,34,33,32"
```

Auto-saved changes to request from Standard.RequestHeaderView at 01:02:40.2458723

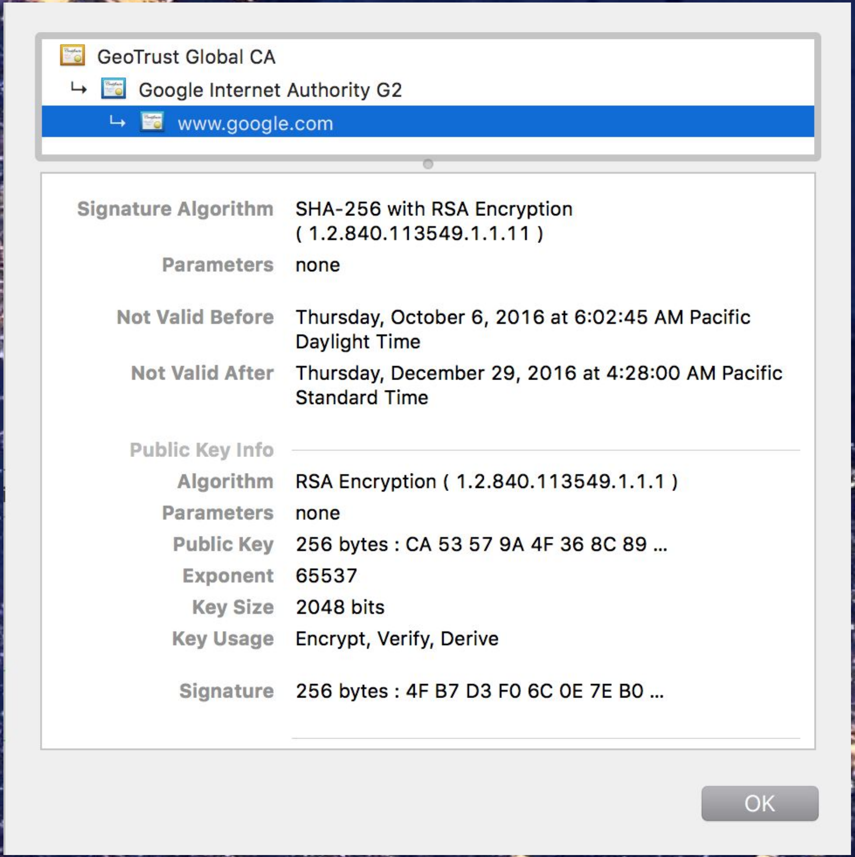
#	Result	Protocol	Host	URL	Body	Process
8	301	HTTP	google.com	/	219	chrome:8148
9	200	HTTPS	www.google.com	/	73,753	chrome:8148
10	200	HTTPS	www.google.com	/images/hpp/googleg-standard-color-42dp.png	1,423	chrome:8148
11	200	HTTPS	www.google.com	/images/branding/googlelogo/1x/googlelogo_co...	5,969	chrome:8148


Web requests
Web responses
clients
servers
SSL Added and removed here! :)



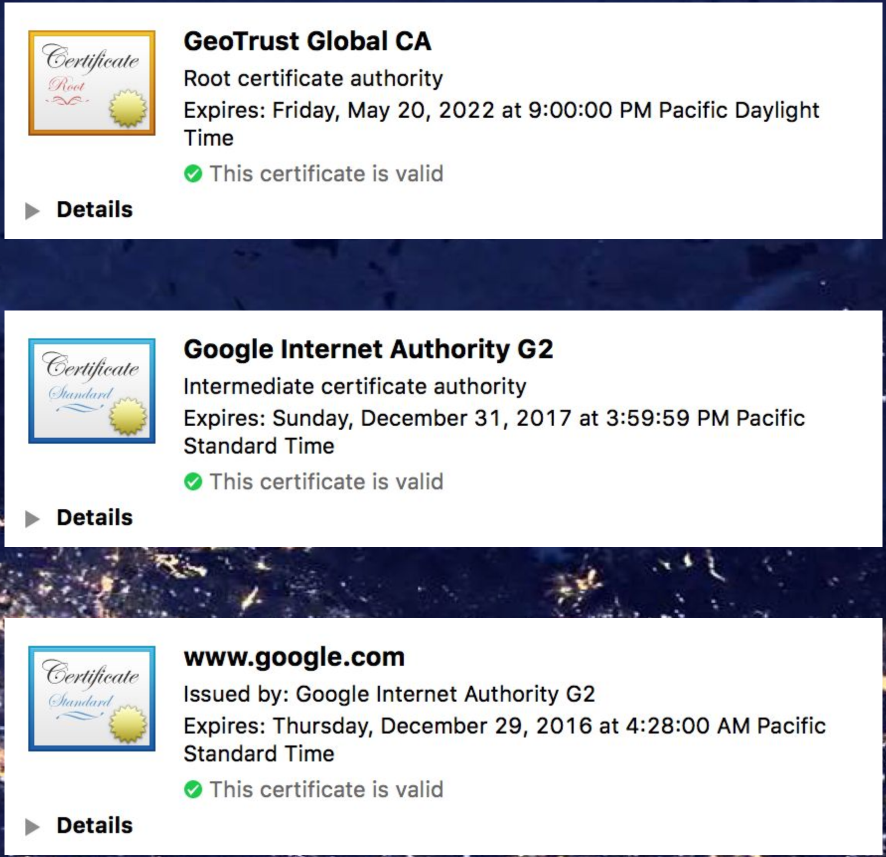
GeoTrust Global CA
↳ Google Internet Authority G2
↳ www.google.com

Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Thursday, October 6, 2016 at 6:02:45 AM Pacific Daylight Time
Not Valid After	Thursday, December 29, 2016 at 4:28:00 AM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : CA 53 57 9A 4F 36 8C 89 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 4F B7 D3 F0 6C 0E 7E B0 ...



GeoTrust Global CA
↳ Google Internet Authority G2
↳ www.google.com

Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Thursday, October 6, 2016 at 6:02:45 AM Pacific Daylight Time
Not Valid After	Thursday, December 29, 2016 at 4:28:00 AM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : CA 53 57 9A 4F 36 8C 89 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 4F B7 D3 F0 6C 0E 7E B0 ...



GeoTrust Global CA

Root certificate authority

Expires: Friday, May 20, 2022 at 9:00:00 PM Pacific Daylight Time

✓ This certificate is valid

Google Internet Authority G2

Intermediate certificate authority

Expires: Sunday, December 31, 2017 at 3:59:59 PM Pacific Standard Time

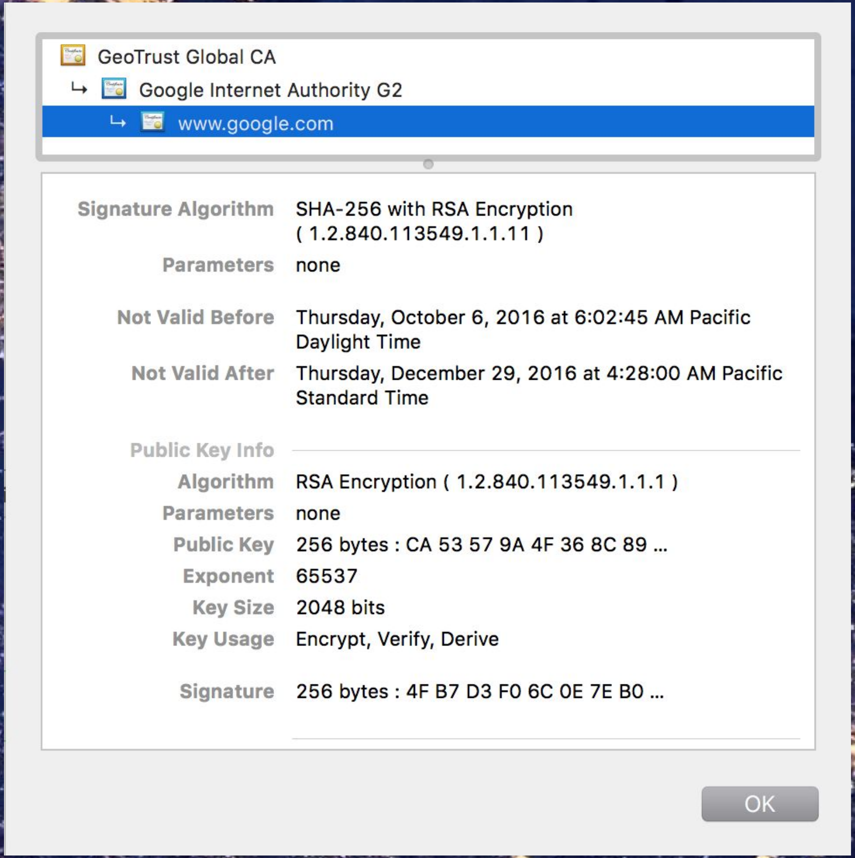
✓ This certificate is valid

www.google.com

Issued by: Google Internet Authority G2

Expires: Thursday, December 29, 2016 at 4:28:00 AM Pacific Standard Time

✓ This certificate is valid



GeoTrust Global CA
↳ Google Internet Authority G2
↳ www.google.com

Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Thursday, October 6, 2016 at 6:02:45 AM Pacific Daylight Time
Not Valid After	Thursday, December 29, 2016 at 4:28:00 AM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : CA 53 57 9A 4F 36 8C 89 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 4F B7 D3 F0 6C 0E 7E B0 ...

Public Key (GeoTrust Global CA)
== DA CC 18 63 30 FD F4 17 …

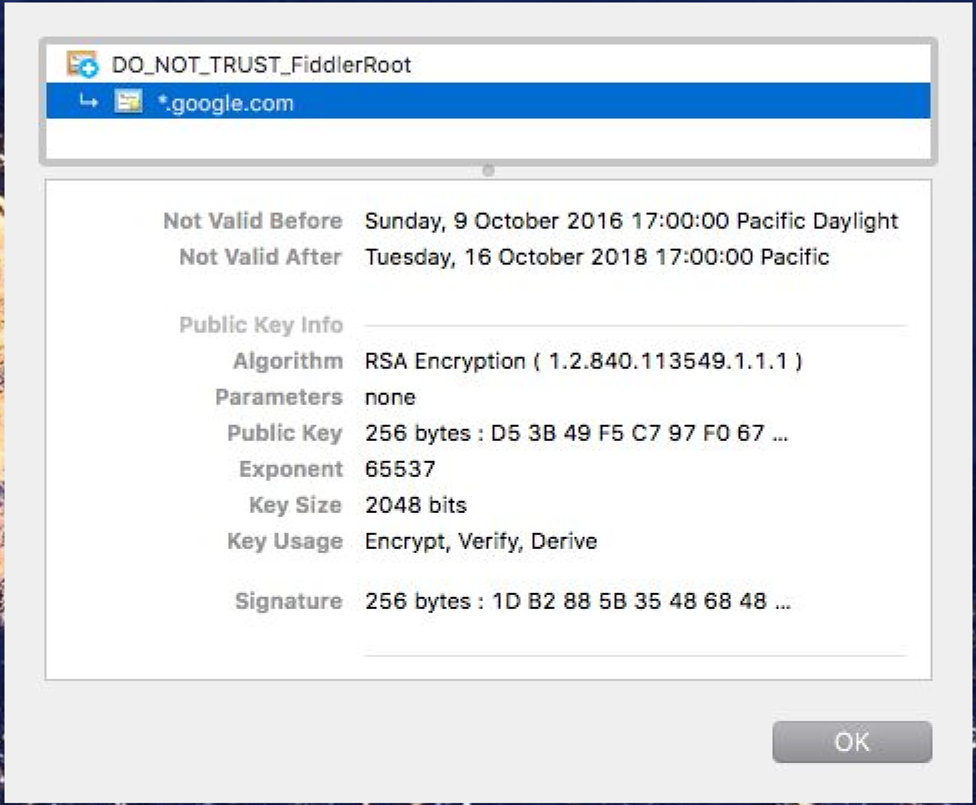
GeoTrust Global CA

Public Key (Google Internet Authority G2)
== 9C 2A 04 77 5C D8 50 91 …

GeoTrust Global CA

Public Key (www.google.com)
== CA 53 57 9A 4F 36 8C 89 …

Google Internet Authority G2



DO_NOT_TRUST_FiddlerRoot

↳ *.google.com

Not Valid Before Sunday, 9 October 2016 17:00:00 Pacific Daylight

Not Valid After Tuesday, 16 October 2018 17:00:00 Pacific

Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Parameters none

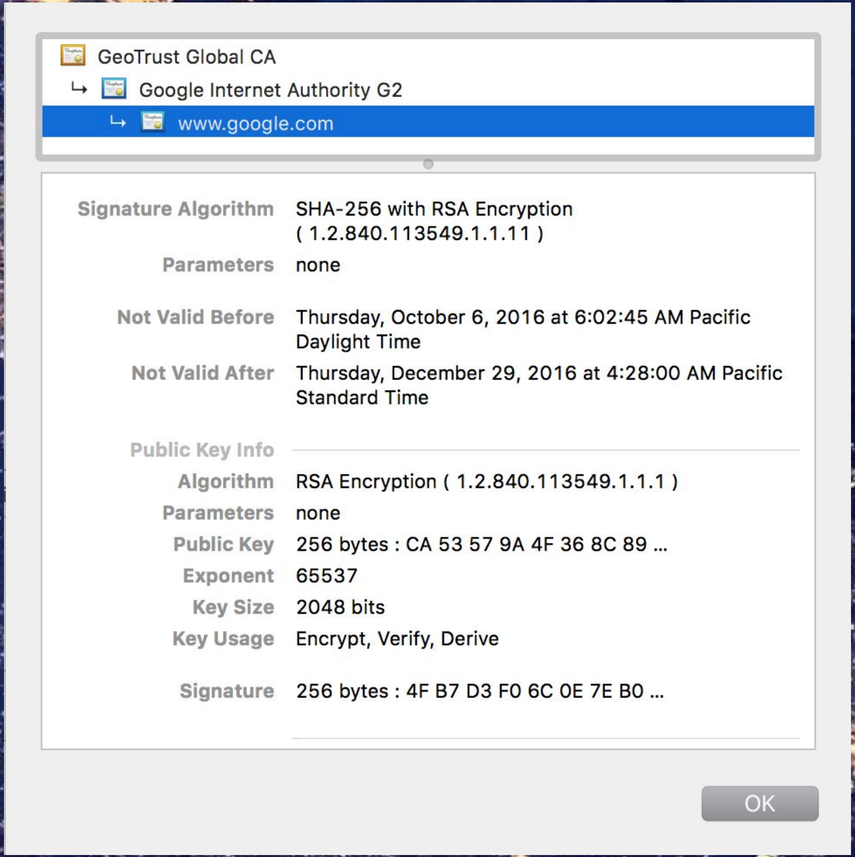
Public Key 256 bytes : D5 3B 49 F5 C7 97 F0 67 ...

Exponent 65537

Key Size 2048 bits

Key Usage Encrypt, Verify, Derive

Signature 256 bytes : 1D B2 88 5B 35 48 68 48 ...



GeoTrust Global CA
↳ Google Internet Authority G2
↳ www.google.com

Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Thursday, October 6, 2016 at 6:02:45 AM Pacific Daylight Time
Not Valid After	Thursday, December 29, 2016 at 4:28:00 AM Pacific Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	256 bytes : CA 53 57 9A 4F 36 8C 89 ...
Exponent	65537
Key Size	2048 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 4F B7 D3 F0 6C 0E 7E B0 ...

Public Key (GeoTrust Global CA)
== DA CC 18 63 30 FD F4 17 …

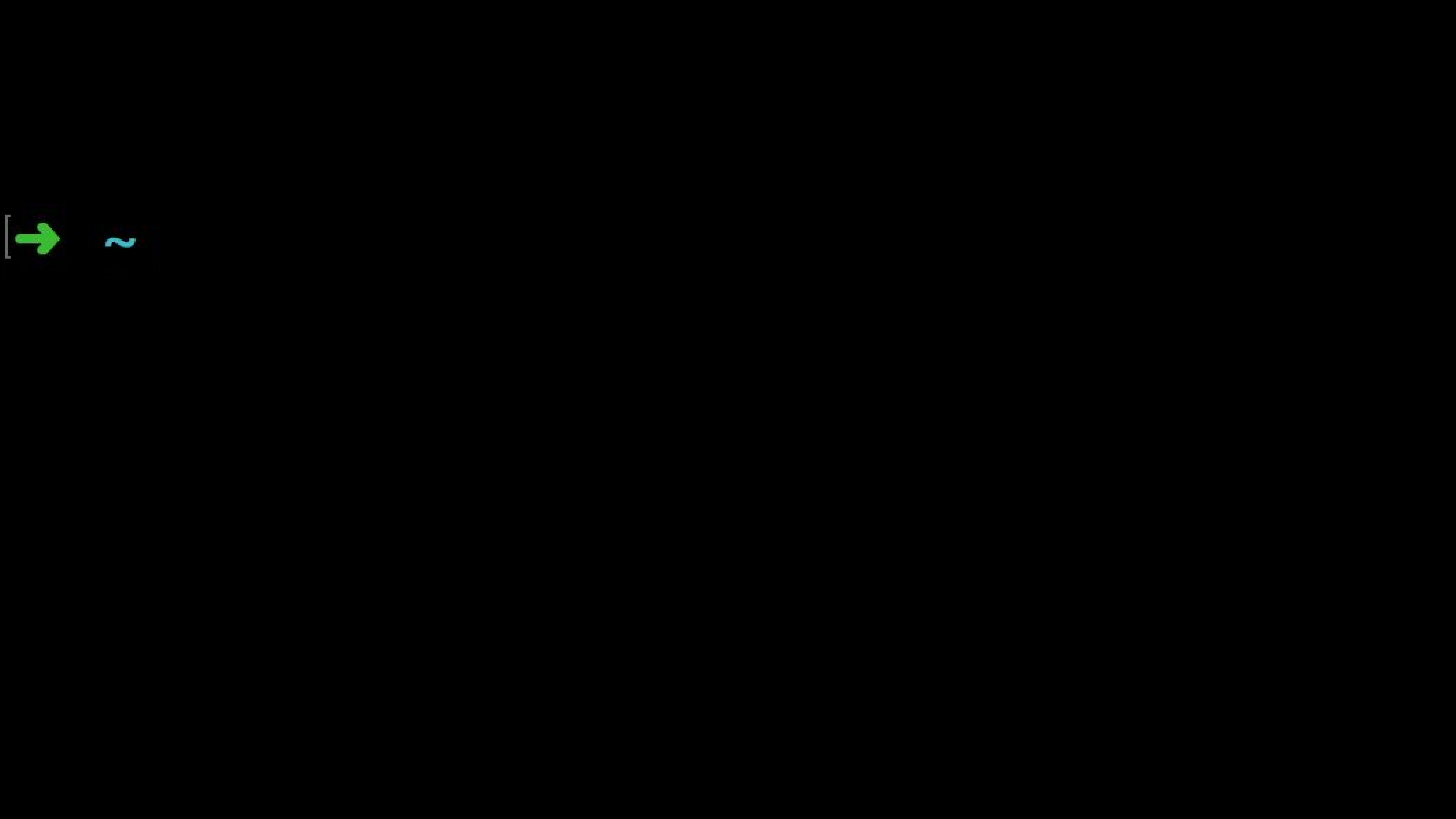
GeoTrust Global CA

Public Key (Google Internet Authority G2)
== 9C 2A 04 77 5C D8 50 91 …

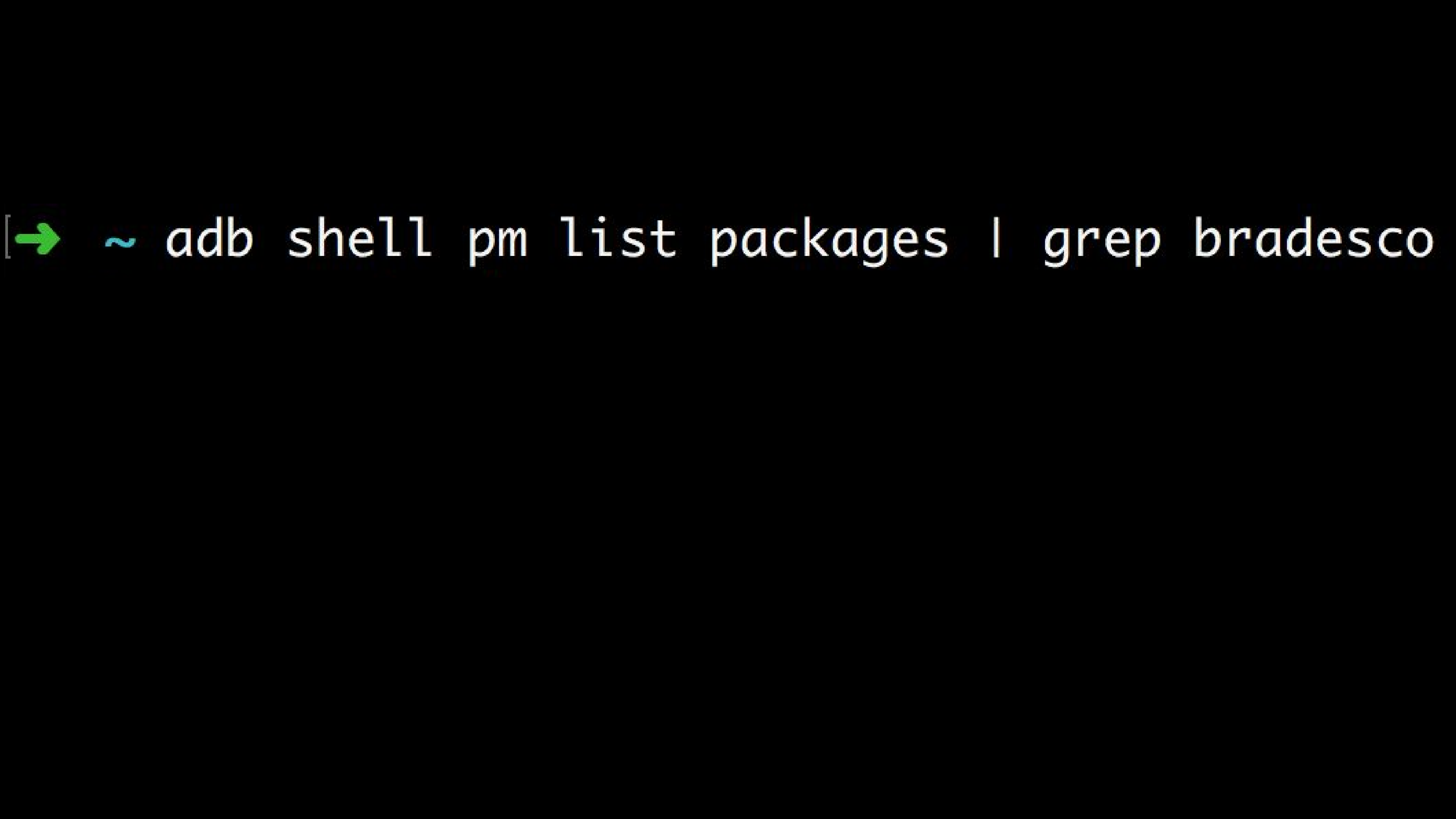
GeoTrust Global CA

Public Key (ww .com)
== CA 53 57 9A 4 C 89 …

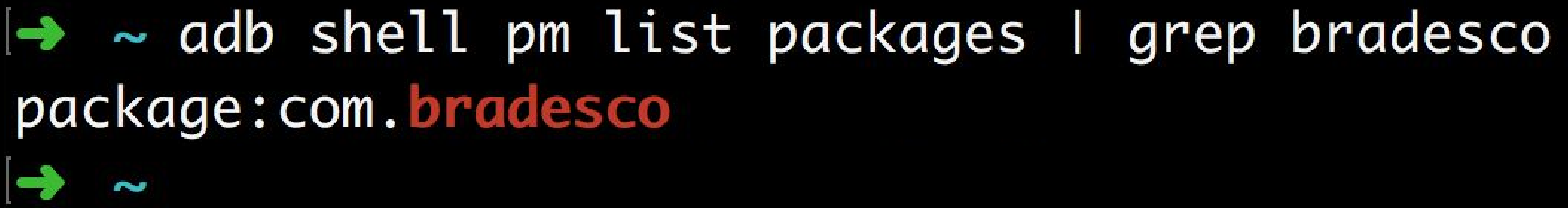
Google Internet Authority G2



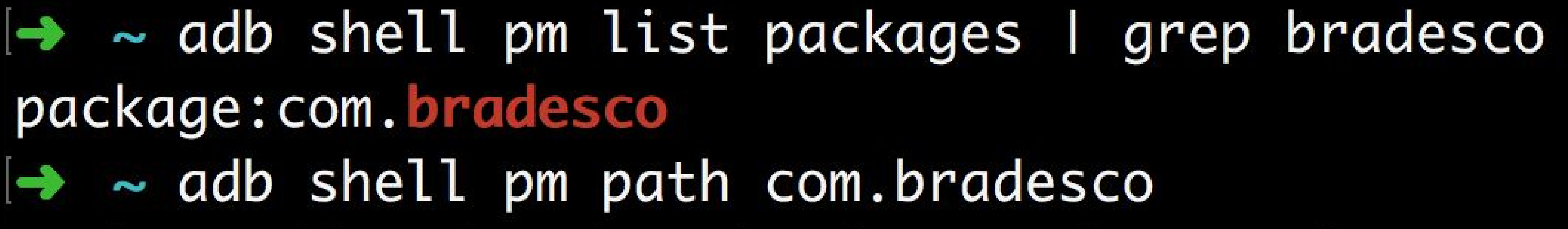
```
➜  ~
```



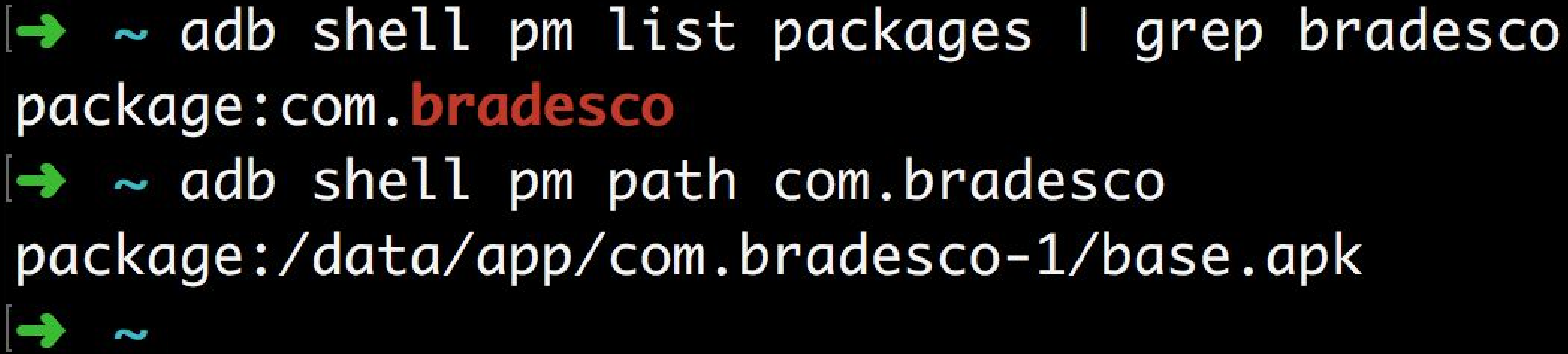
```
[➜  ~ adb shell pm list packages | grep bradesco
```



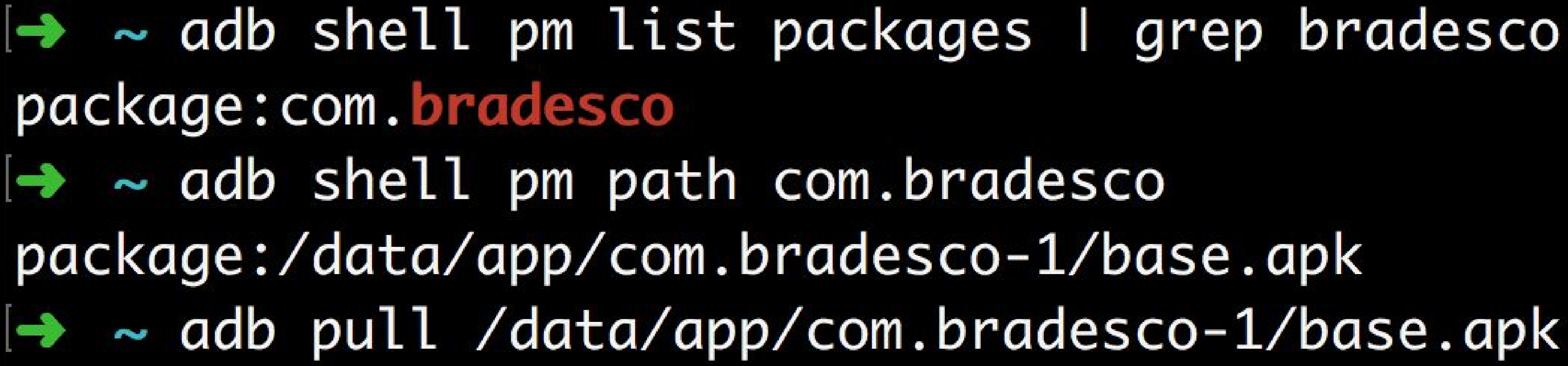
```
➜  ~ adb shell pm list packages | grep bradesco
package:com.bradesco
➜  ~
```



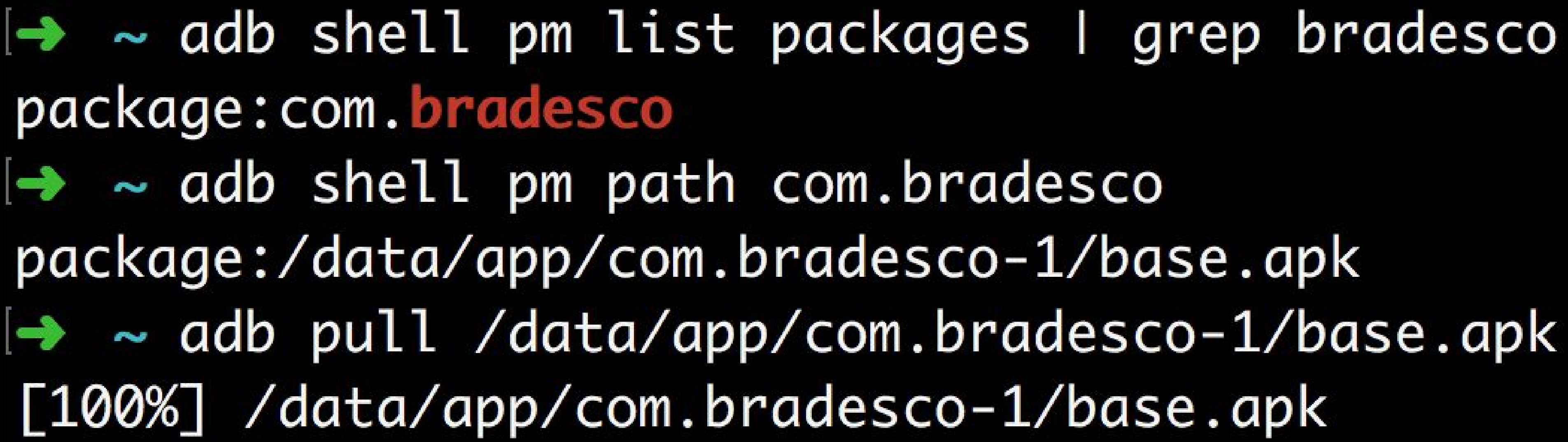
```
➜  ~ adb shell pm list packages | grep bradesco
package:com.bradesco
➜  ~ adb shell pm path com.bradesco
```



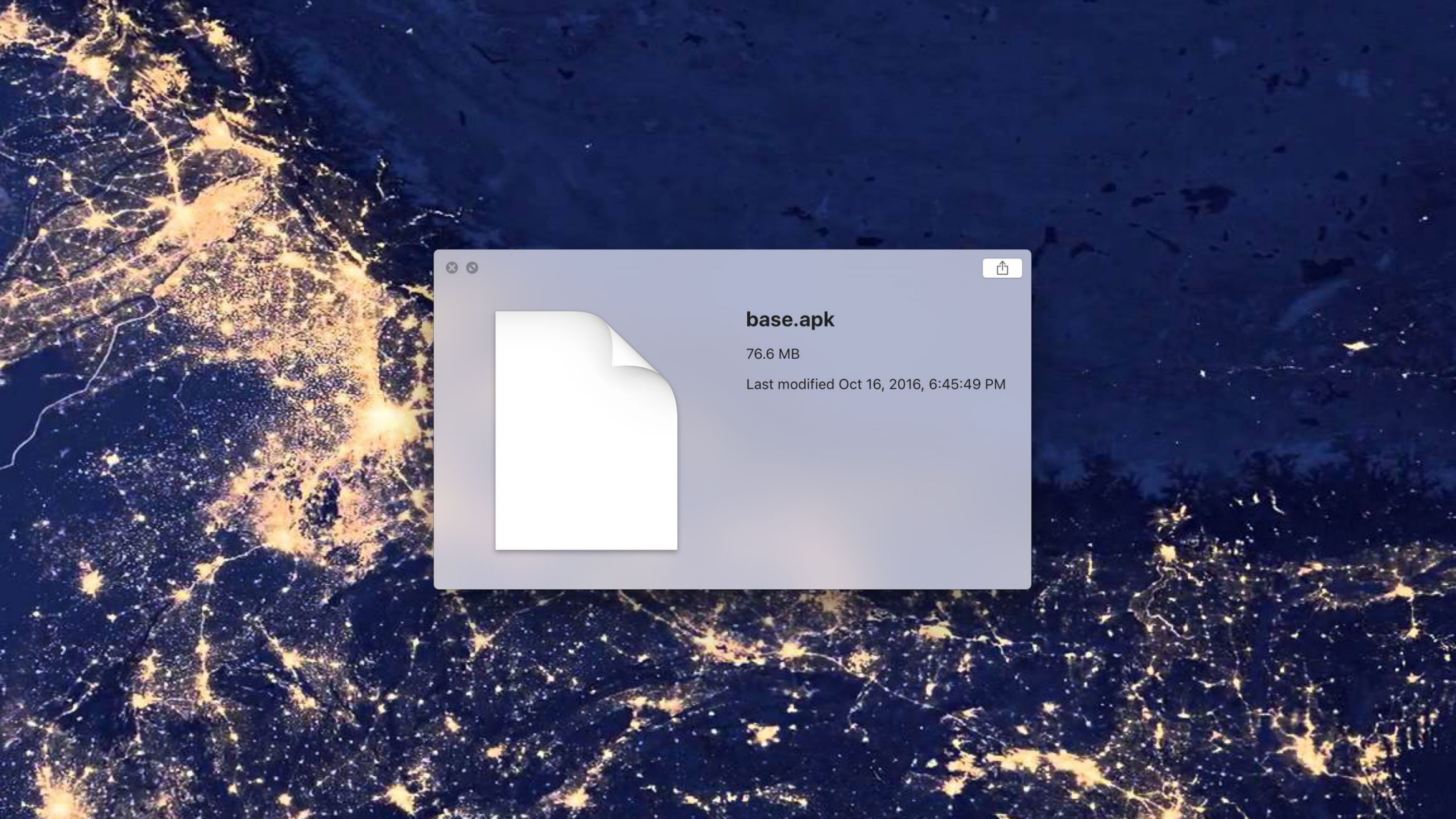
```
➜  ~ adb shell pm list packages | grep bradesco
package:com.bradesco
➜  ~ adb shell pm path com.bradesco
package:/data/app/com.bradesco-1/base.apk
➜  ~
```



```
➜  ~ adb shell pm list packages | grep bradesco
package:com.bradesco
➜  ~ adb shell pm path com.bradesco
package:/data/app/com.bradesco-1/base.apk
➜  ~ adb pull /data/app/com.bradesco-1/base.apk
```



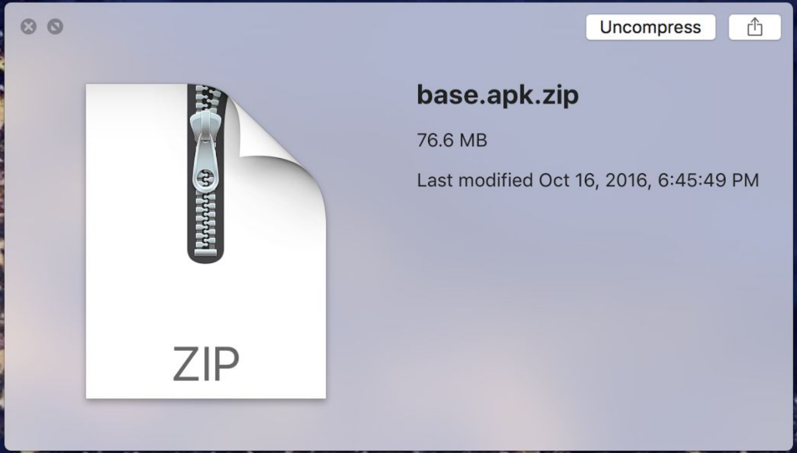
```
➜  ~ adb shell pm list packages | grep bradesco
package:com.bradesco
➜  ~ adb shell pm path com.bradesco
package:/data/app/com.bradesco-1/base.apk
➜  ~ adb pull /data/app/com.bradesco-1/base.apk
[100%] /data/app/com.bradesco-1/base.apk
```



base.apk

76.6 MB

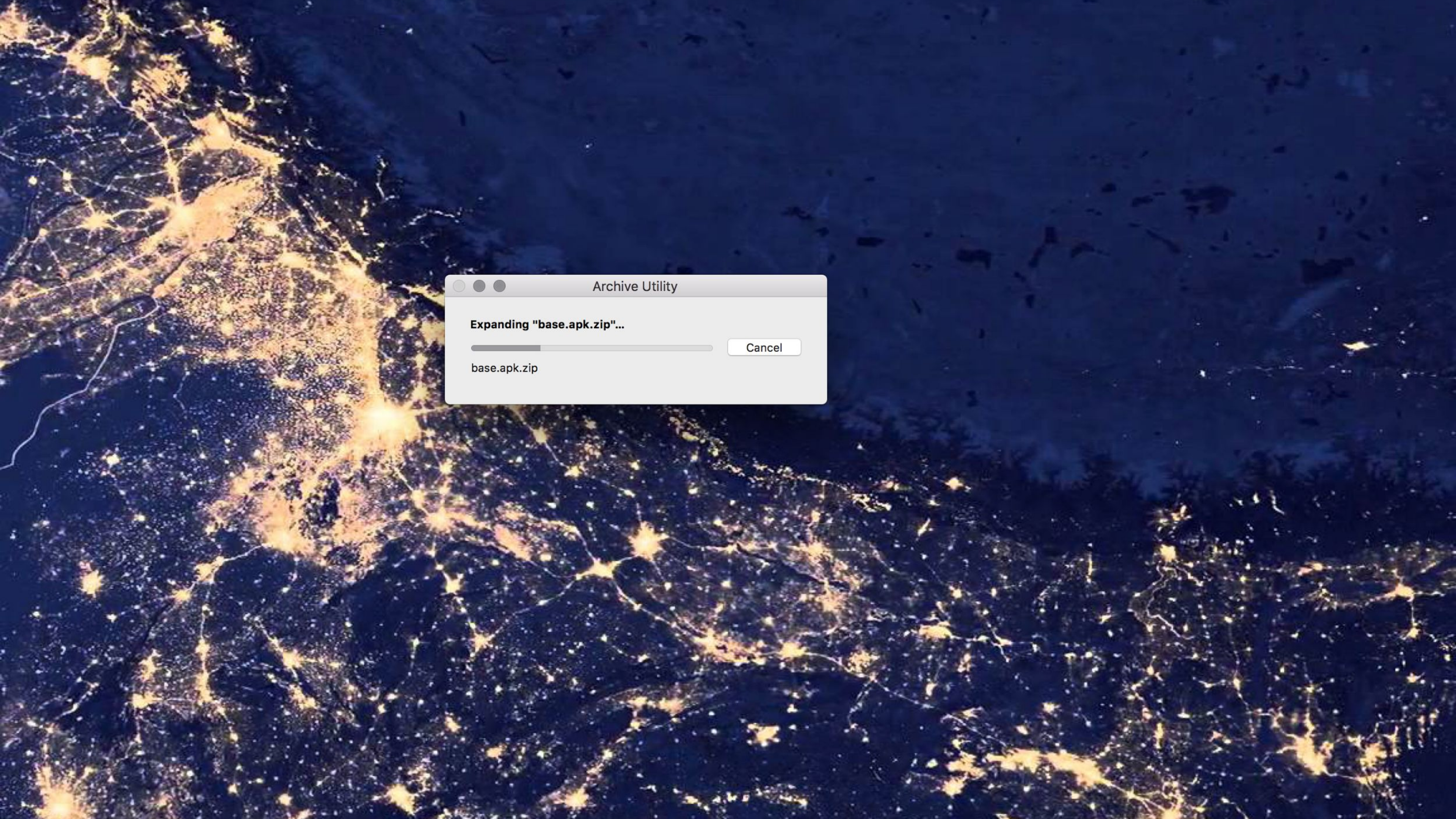
Last modified Oct 16, 2016, 6:45:49 PM



base.apk.zip

76.6 MB

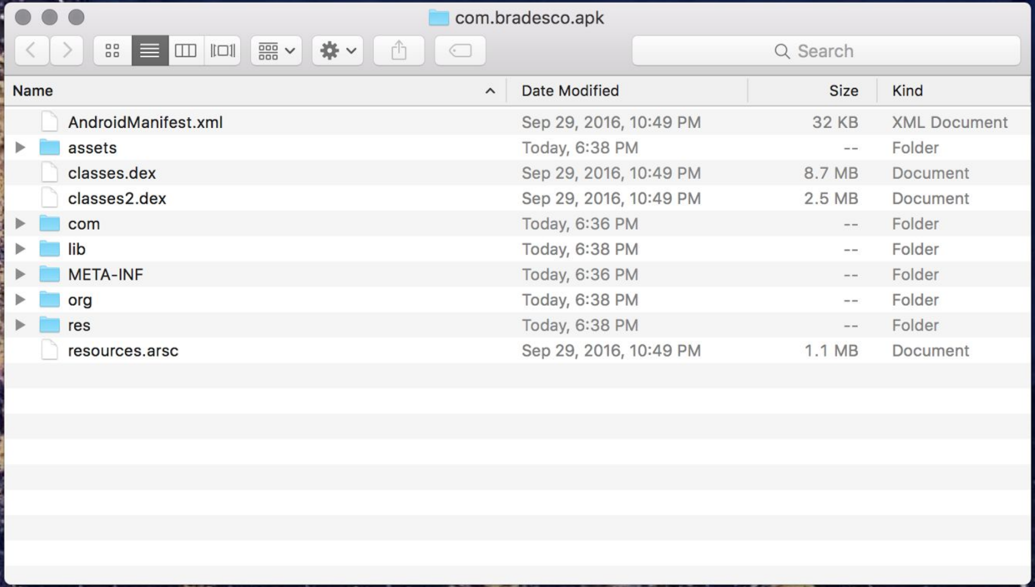
Last modified Oct 16, 2016, 6:45:49 PM



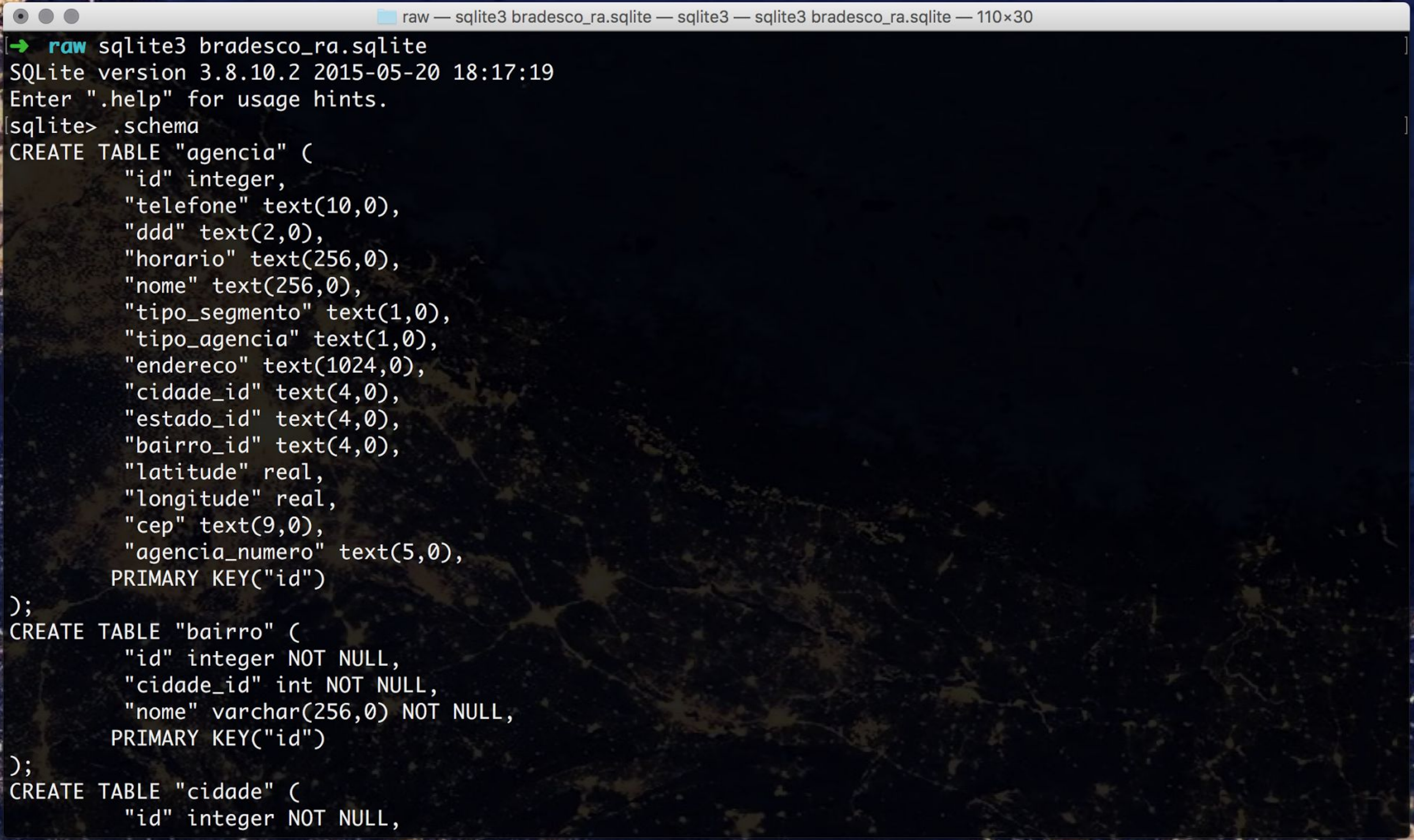
Archive Utility

Expanding "base.apk.zip"...

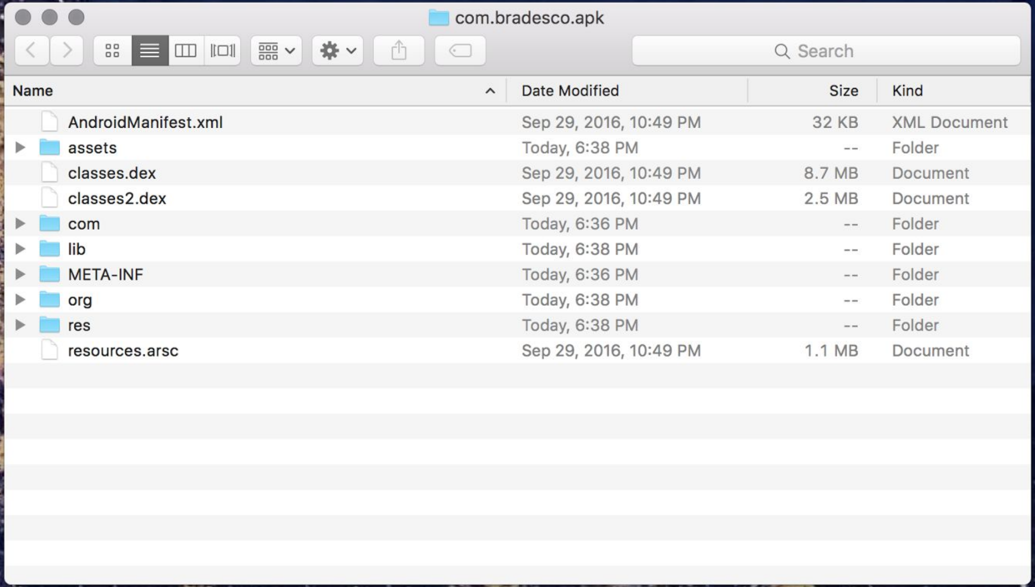
base.apk.zip



Name	Date Modified	Size	Kind
AndroidManifest.xml	Sep 29, 2016, 10:49 PM	32 KB	XML Document
assets	Today, 6:38 PM	--	Folder
classes.dex	Sep 29, 2016, 10:49 PM	8.7 MB	Document
classes2.dex	Sep 29, 2016, 10:49 PM	2.5 MB	Document
com	Today, 6:36 PM	--	Folder
lib	Today, 6:38 PM	--	Folder
META-INF	Today, 6:36 PM	--	Folder
org	Today, 6:38 PM	--	Folder
res	Today, 6:38 PM	--	Folder
resources.arsc	Sep 29, 2016, 10:49 PM	1.1 MB	Document

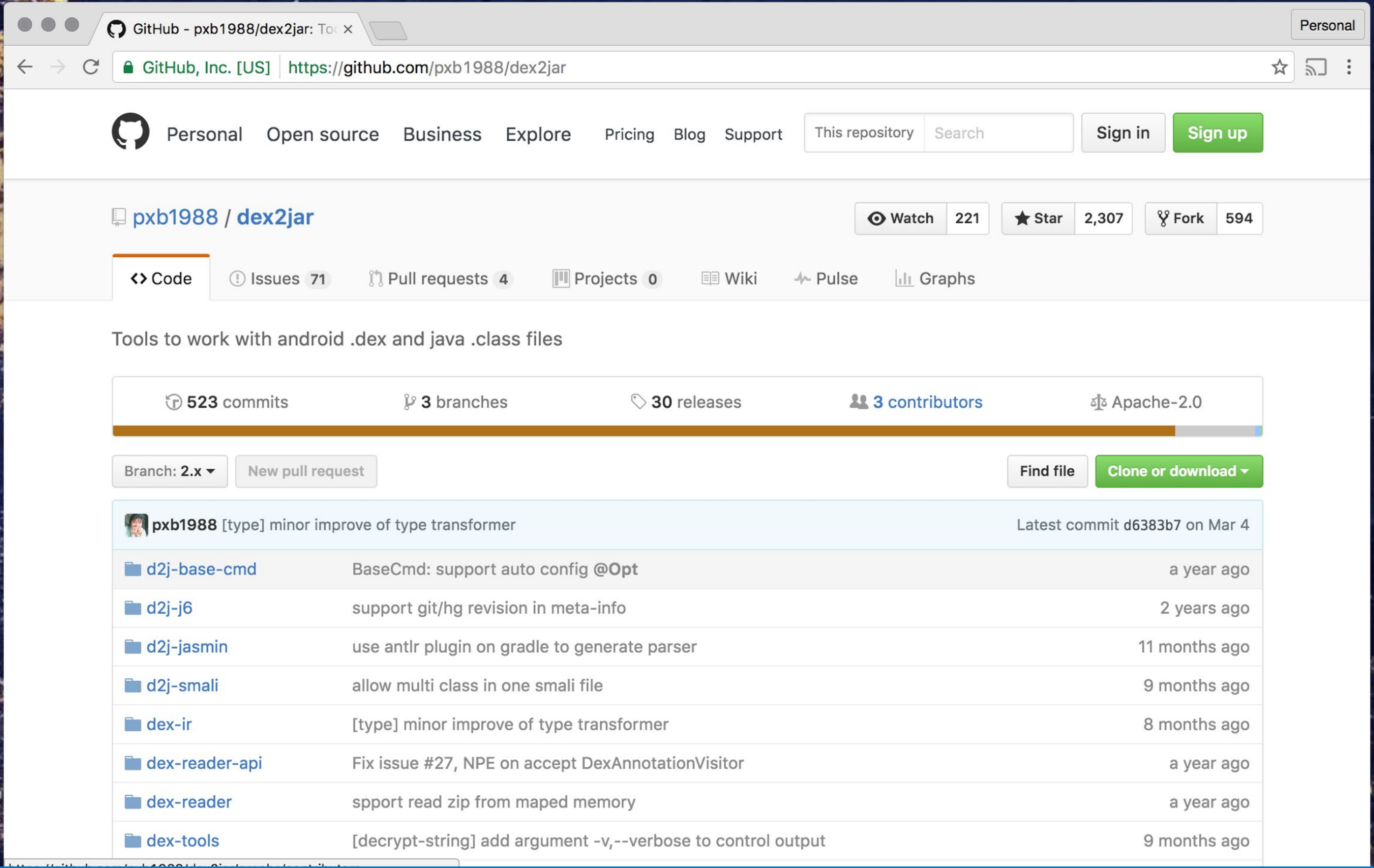

raw — sqlite3 bradesco_ra.sqlite — sqlite3 — sqlite3 bradesco_ra.sqlite — 110×30

```
➜  raw sqlite3 bradesco_ra.sqlite
SQLite version 3.8.10.2 2015-05-20 18:17:19
Enter ".help" for usage hints.
sqlite> .schema
CREATE TABLE "agencia" (
         "id" integer,
         "telefone" text(10,0),
         "ddd" text(2,0),
         "horario" text(256,0),
         "nome" text(256,0),
         "tipo_segmento" text(1,0),
         "tipo_agencia" text(1,0),
         "endereco" text(1024,0),
         "cidade_id" text(4,0),
         "estado_id" text(4,0),
         "bairro_id" text(4,0),
         "latitude" real,
         "longitude" real,
         "cep" text(9,0),
         "agencia_numero" text(5,0),
        PRIMARY KEY("id")
);
CREATE TABLE "bairro" (
         "id" integer NOT NULL,
         "cidade_id" int NOT NULL,
         "nome" varchar(256,0) NOT NULL,
        PRIMARY KEY("id")
);
CREATE TABLE "cidade" (
         "id" integer NOT NULL,
```



com.bradesco.apk

Name	Date Modified	Size	Kind
AndroidManifest.xml	Sep 29, 2016, 10:49 PM	32 KB	XML Document
assets	Today, 6:38 PM	--	Folder
classes.dex	Sep 29, 2016, 10:49 PM	8.7 MB	Document
classes2.dex	Sep 29, 2016, 10:49 PM	2.5 MB	Document
com	Today, 6:36 PM	--	Folder
lib	Today, 6:38 PM	--	Folder
META-INF	Today, 6:36 PM	--	Folder
org	Today, 6:38 PM	--	Folder
res	Today, 6:38 PM	--	Folder
resources.arsc	Sep 29, 2016, 10:49 PM	1.1 MB	Document



pxb1988 / dex2jar

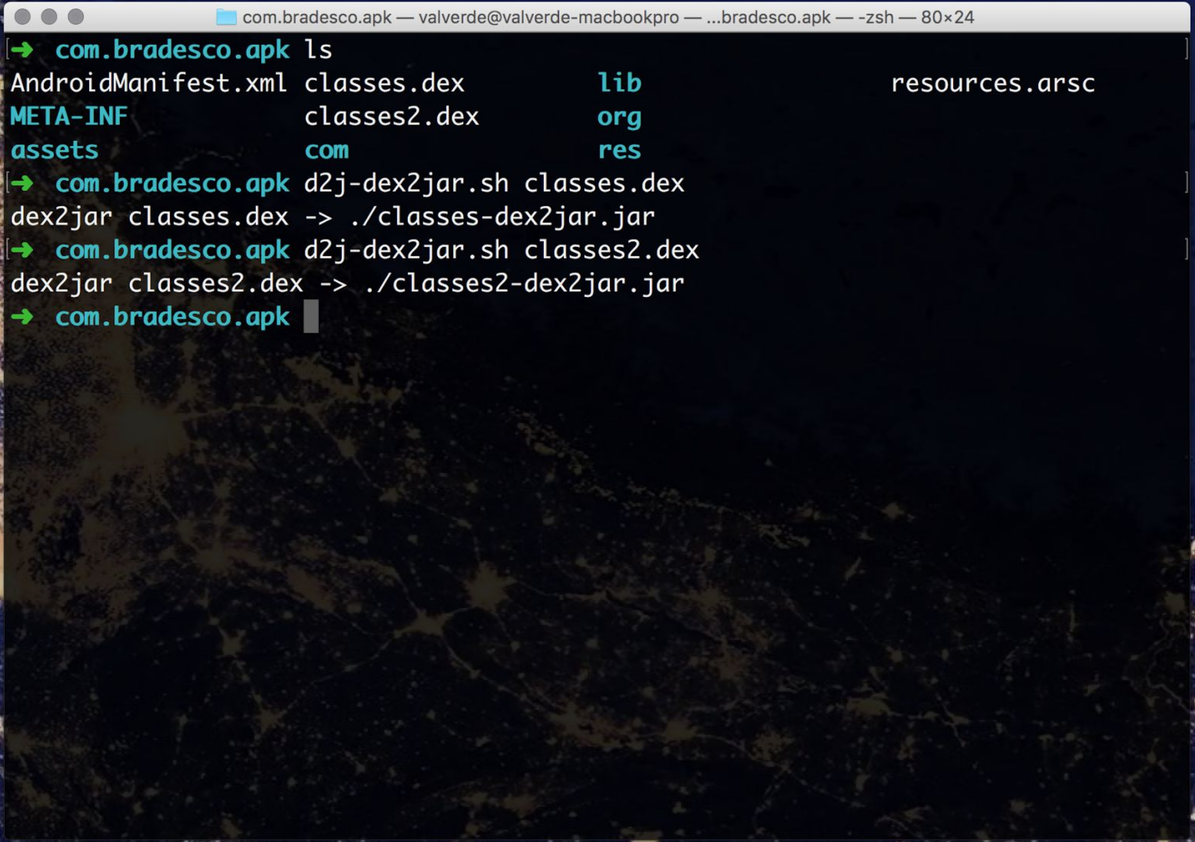
Tools to work with android .dex and java .class files

523 commits | 3 branches | 30 releases | 3 contributors | Apache-2.0

pxb1988 [type] minor improve of type transformer — Latest commit d6383b7 on Mar 4

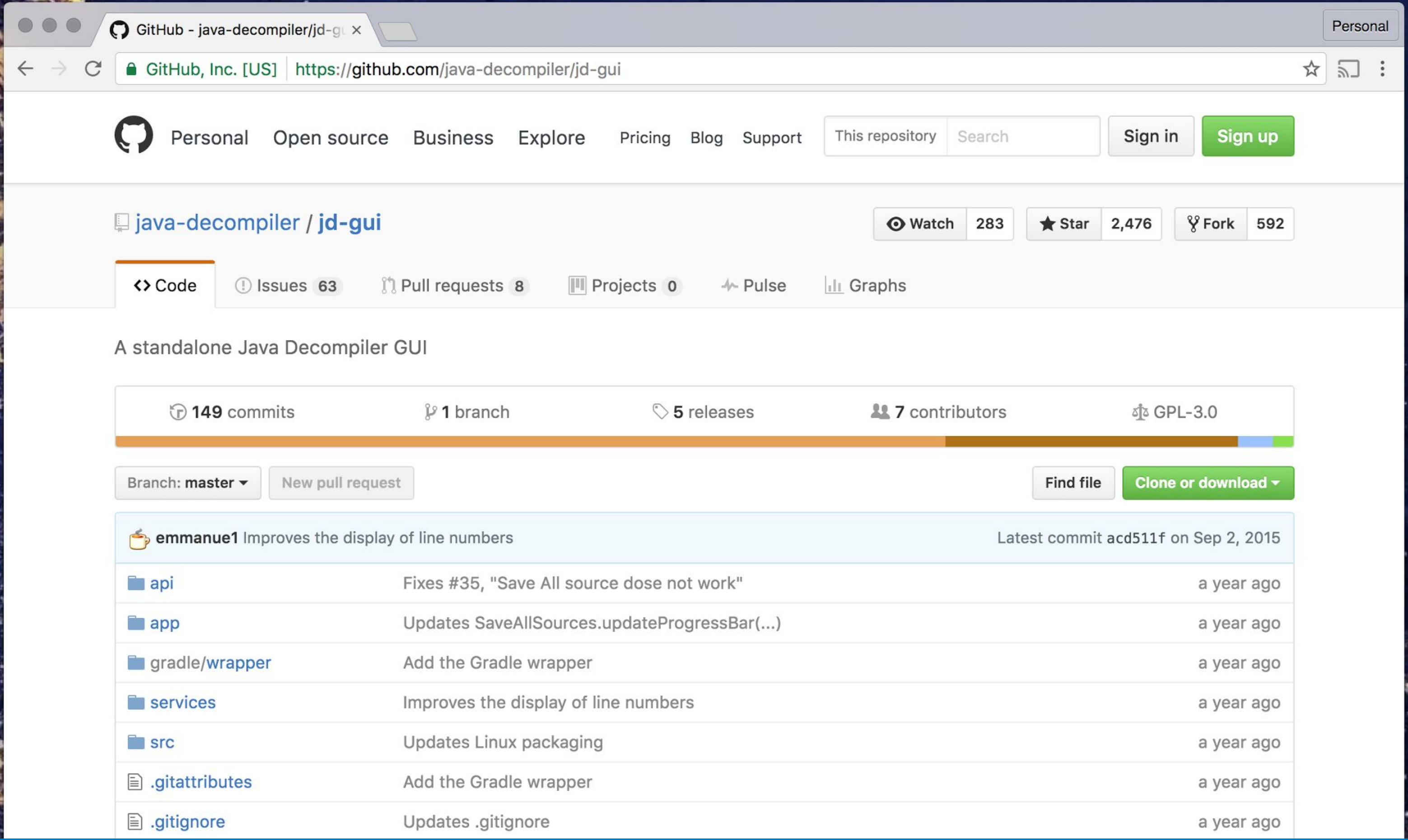
d2j-base-cmd	BaseCmd: support auto config @Opt	a year ago
d2j-j6	support git/hg revision in meta-info	2 years ago
d2j-jasmin	use antlr plugin on gradle to generate parser	11 months ago
d2j-smali	allow multi class in one smali file	9 months ago
dex-ir	[type] minor improve of type transformer	8 months ago
dex-reader-api	Fix issue #27, NPE on accept DexAnnotationVisitor	a year ago
dex-reader	spport read zip from maped memory	a year ago
dex-tools	[decrypt-string] add argument -v,--verbose to control output	9 months ago

https://github.com/pxb1988/dex2jar



com.bradesco.apk — valverde@valverde-macbookpro — ...bradesco.apk — -zsh — 80×24

```
➜  com.bradesco.apk ls
AndroidManifest.xml classes.dex         lib                 resources.arsc
META-INF            classes2.dex        org
assets              com                 res
➜  com.bradesco.apk d2j-dex2jar.sh classes.dex
dex2jar classes.dex -> ./classes-dex2jar.jar
➜  com.bradesco.apk d2j-dex2jar.sh classes2.dex
dex2jar classes2.dex -> ./classes2-dex2jar.jar
➜  com.bradesco.apk
```



java-decompiler / jd-gui

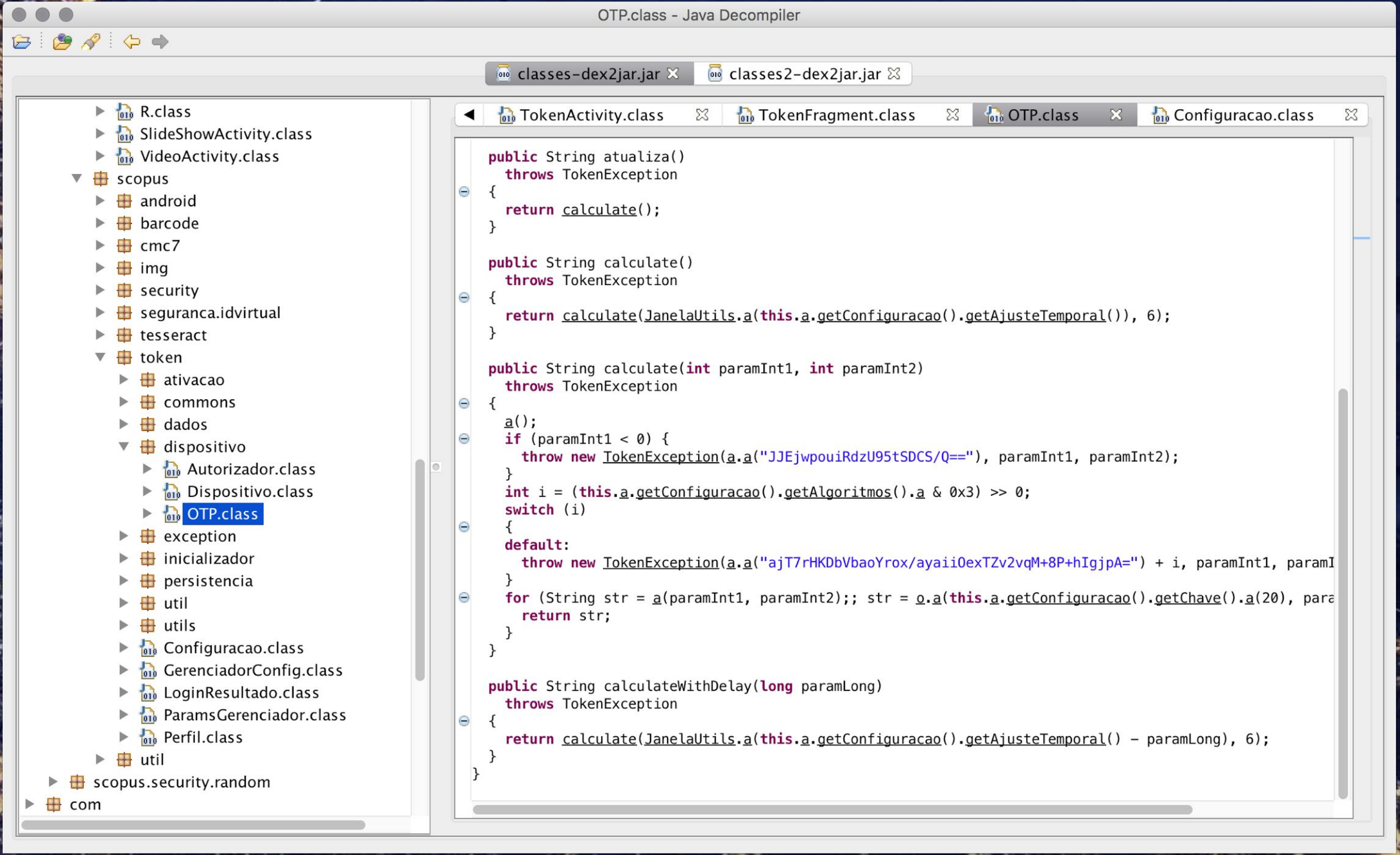
A standalone Java Decompiler GUI

149 commits · 1 branch · 5 releases · 7 contributors · GPL-3.0

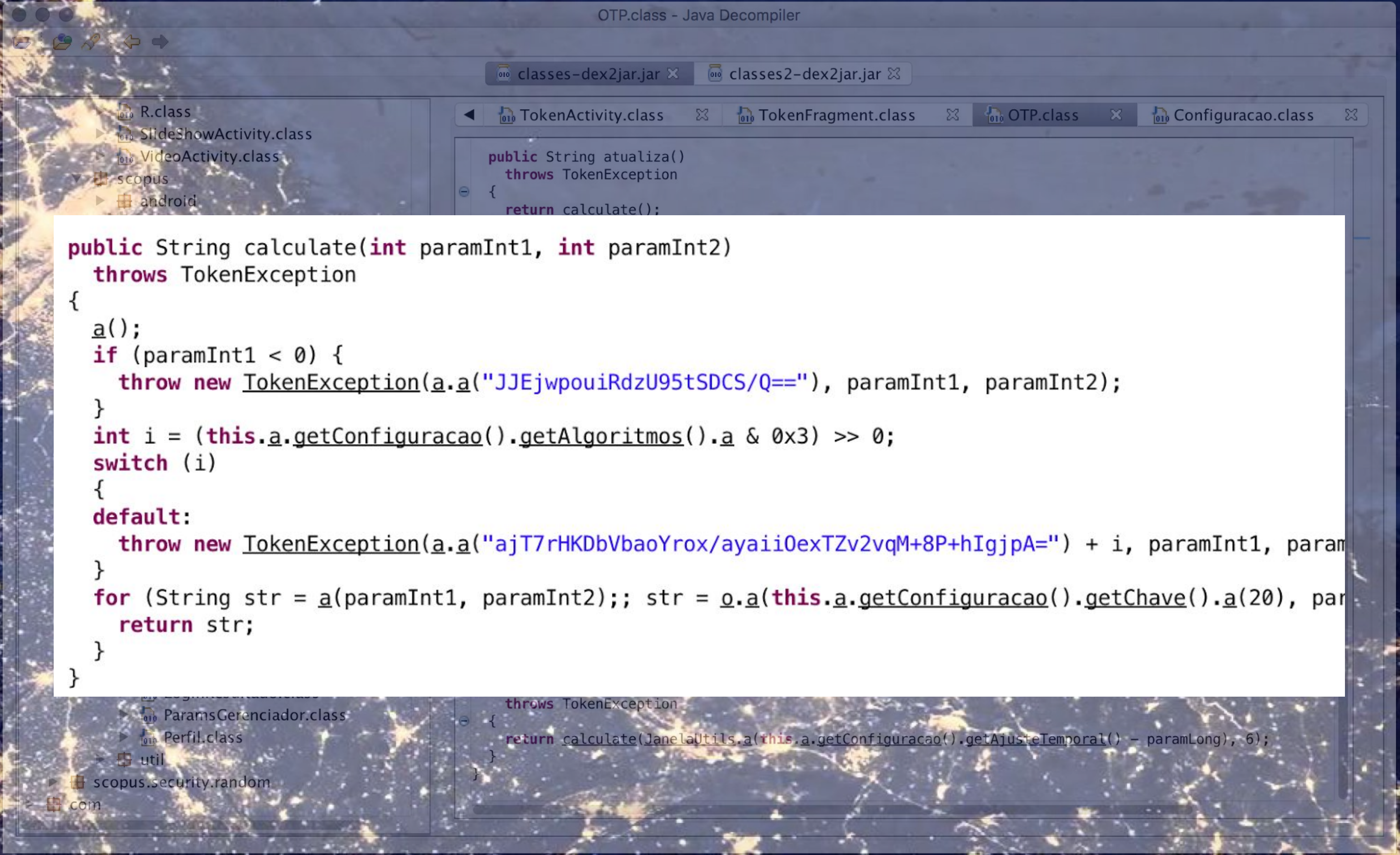
emmanue1 Improves the display of line numbers — Latest commit acd511f on Sep 2, 2015

api	Fixes #35, "Save All source dose not work"	a year ago
app	Updates SaveAllSources.updateProgressBar(...)	a year ago
gradle/wrapper	Add the Gradle wrapper	a year ago
services	Improves the display of line numbers	a year ago
src	Updates Linux packaging	a year ago
.gitattributes	Add the Gradle wrapper	a year ago
.gitignore	Updates .gitignore	a year ago

https://github.com/java-decompiler/jd-gui



```
public String atualiza()
  throws TokenException
{
  return calculate();
}

public String calculate()
  throws TokenException
{
  return calculate(JanelaUtils.a(this.a.getConfiguracao().getAjusteTemporal()), 6);
}

public String calculate(int paramInt1, int paramInt2)
  throws TokenException
{
  a();
  if (paramInt1 < 0) {
    throw new TokenException(a.a("JJEjwpouiRdzU95tSDCS/Q=="), paramInt1, paramInt2);
  }
  int i = (this.a.getConfiguracao().getAlgoritmos().a & 0x3) >> 0;
  switch (i)
  {
  default:
    throw new TokenException(a.a("ajT7rHKDbVbaoYrox/ayaiiOexTZv2vqM+8P+hIgjpA=") + i, paramInt1, paramI
  }
  for (String str = a(paramInt1, paramInt2);; str = o.a(this.a.getConfiguracao().getChave().a(20), para
    return str;
  }
}

public String calculateWithDelay(long paramLong)
  throws TokenException
{
  return calculate(JanelaUtils.a(this.a.getConfiguracao().getAjusteTemporal() - paramLong), 6);
}
}
```

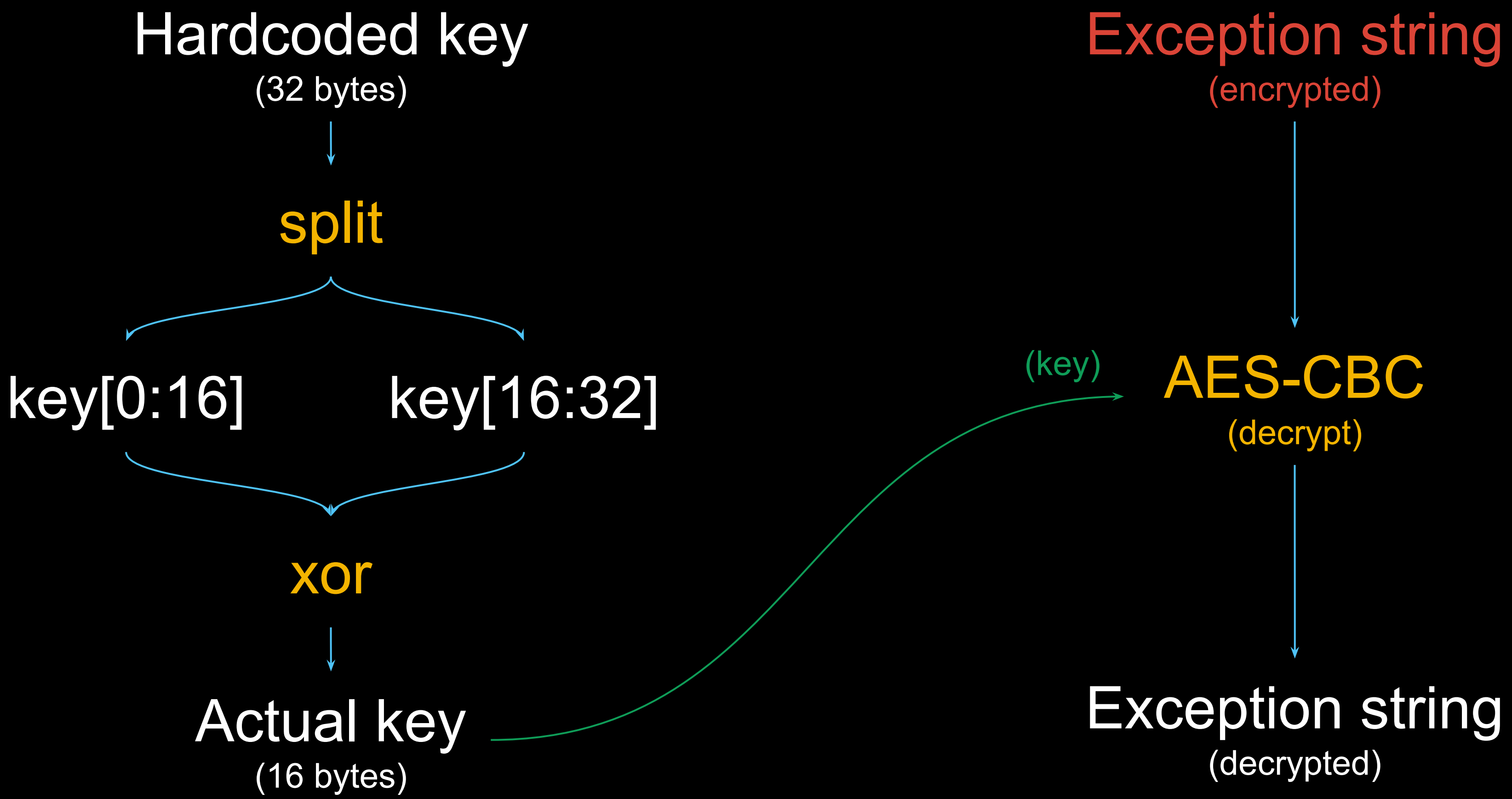


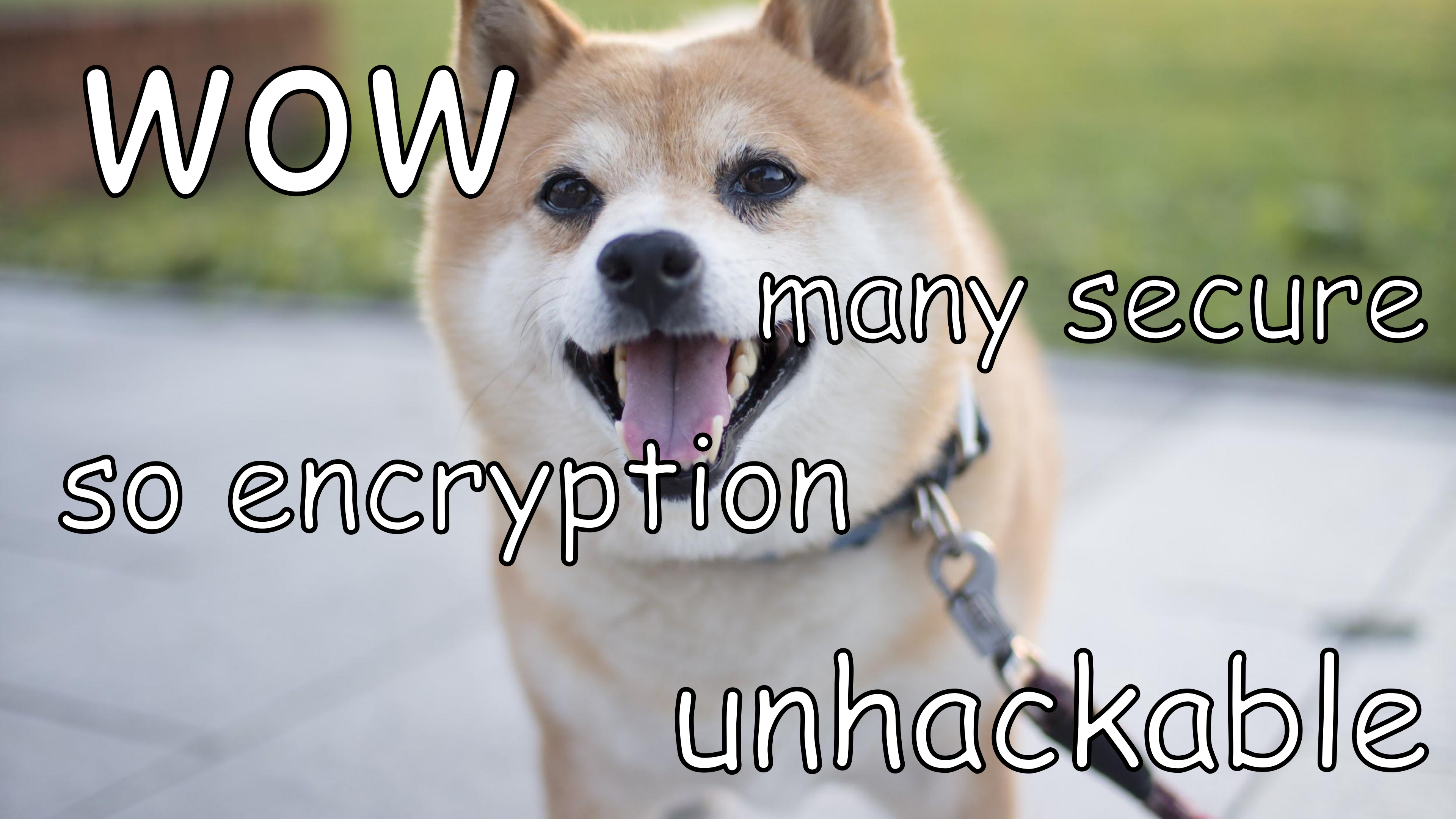
```
public String atualiza()
  throws TokenException
{
  return calculate();
```

```
public String calculate(int paramInt1, int paramInt2)
  throws TokenException
{
  a();
  if (paramInt1 < 0) {
    throw new TokenException(a.a("JJEjwpouiRdzU95tSDCS/Q=="), paramInt1, paramInt2);
  }
  int i = (this.a.getConfiguracao().getAlgoritmos().a & 0x3) >> 0;
  switch (i)
  {
  default:
    throw new TokenException(a.a("ajT7rHKDbVbaoYrox/ayaiiOexTZv2vqM+8P+hIgjpA=") + i, paramInt1, param
  }
  for (String str = a(paramInt1, paramInt2);; str = o.a(this.a.getConfiguracao().getChave().a(20), par
    return str;
  }
}
```

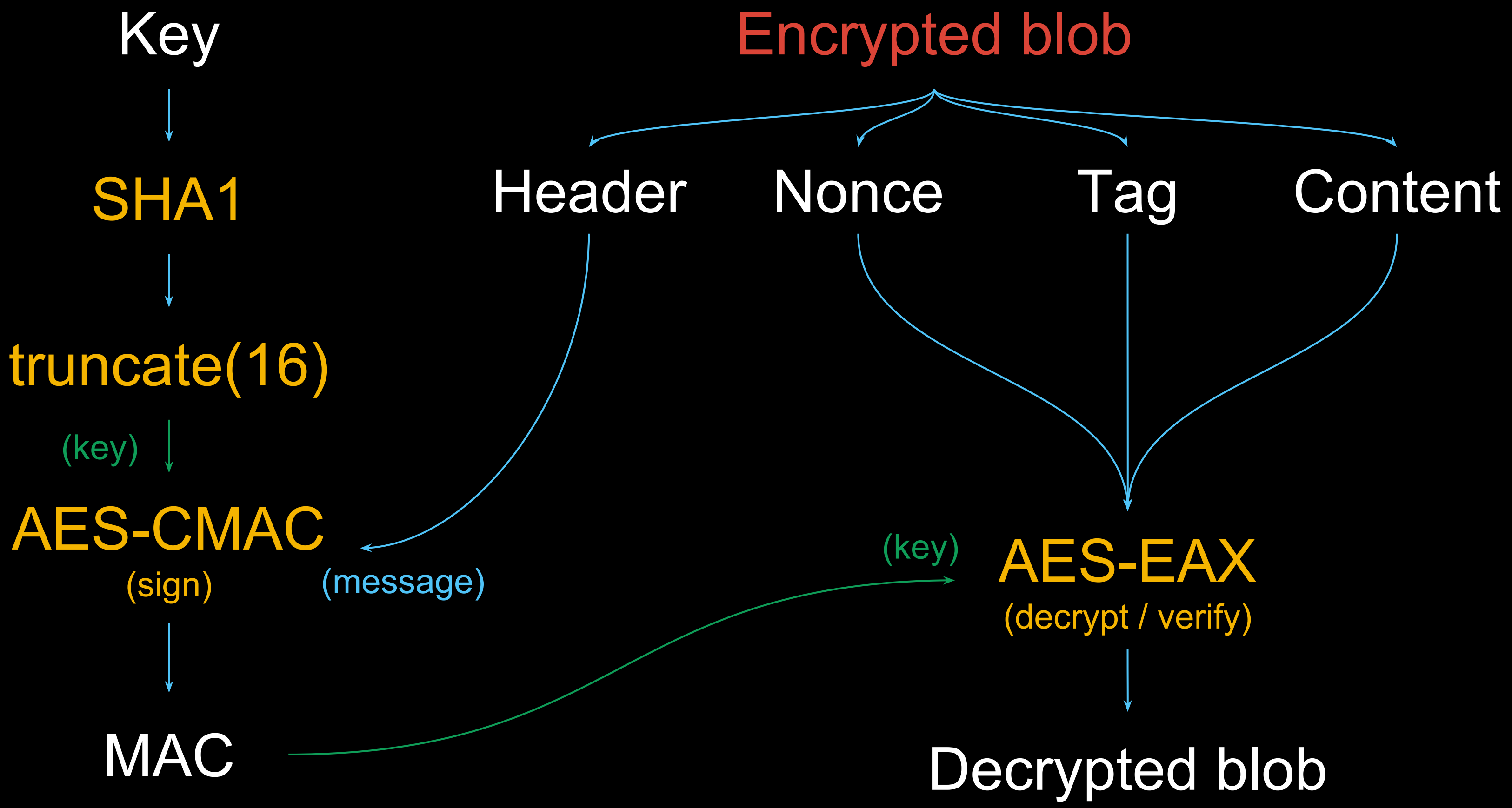
```
  throws TokenException
{
  return calculate(JanelaUtils.a(this.a.getConfiguracao().getAjusteTemporal() - paramLong), 6);
}
}
```

decrypt(exception_string)




wow
many secure
so encryption
unhackable

decrypt(key, blob)



Key

SHA1

truncate(16)

(key)

AES-CMAC

(sign)

(message)

MAC

Encrypted blob

Header

Nonce

Tag

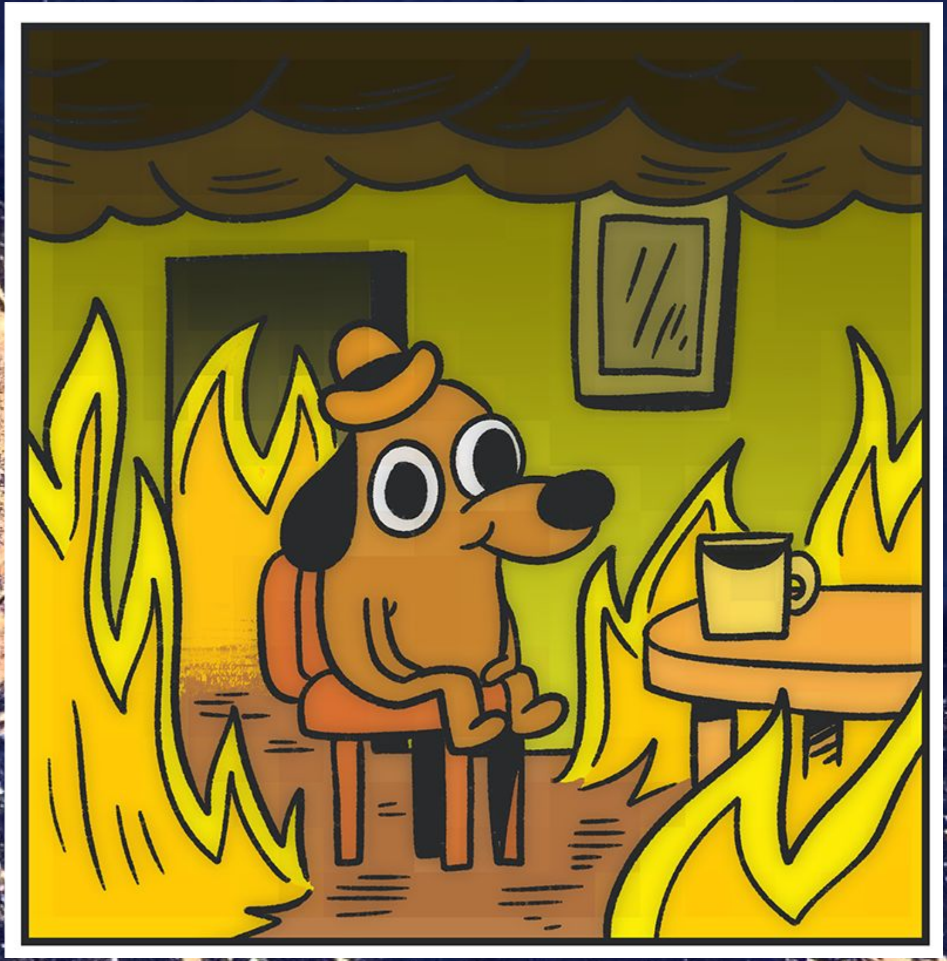
Content

(key)

AES-EAX

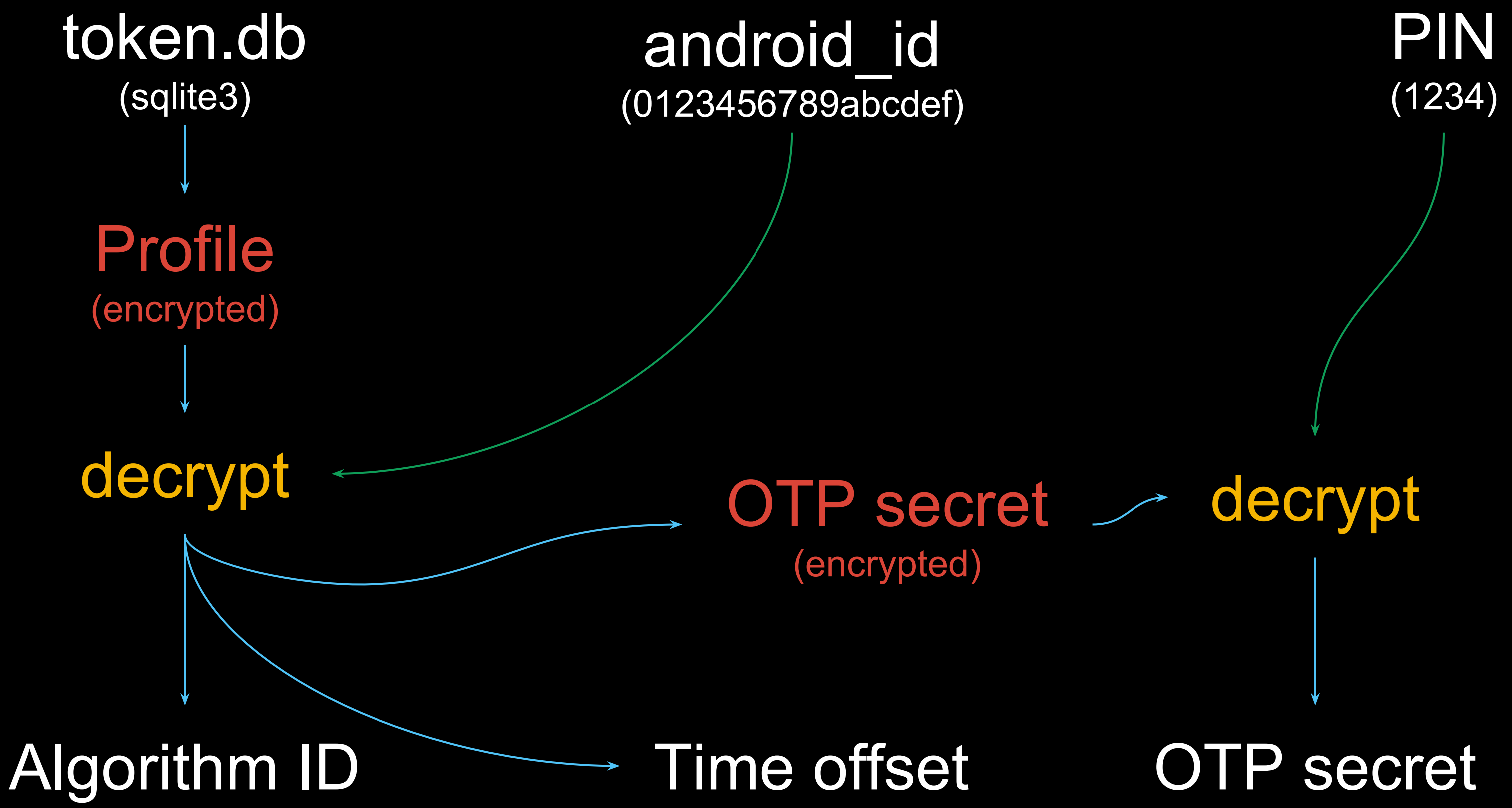
(decrypt / verify)

Decrypted blob

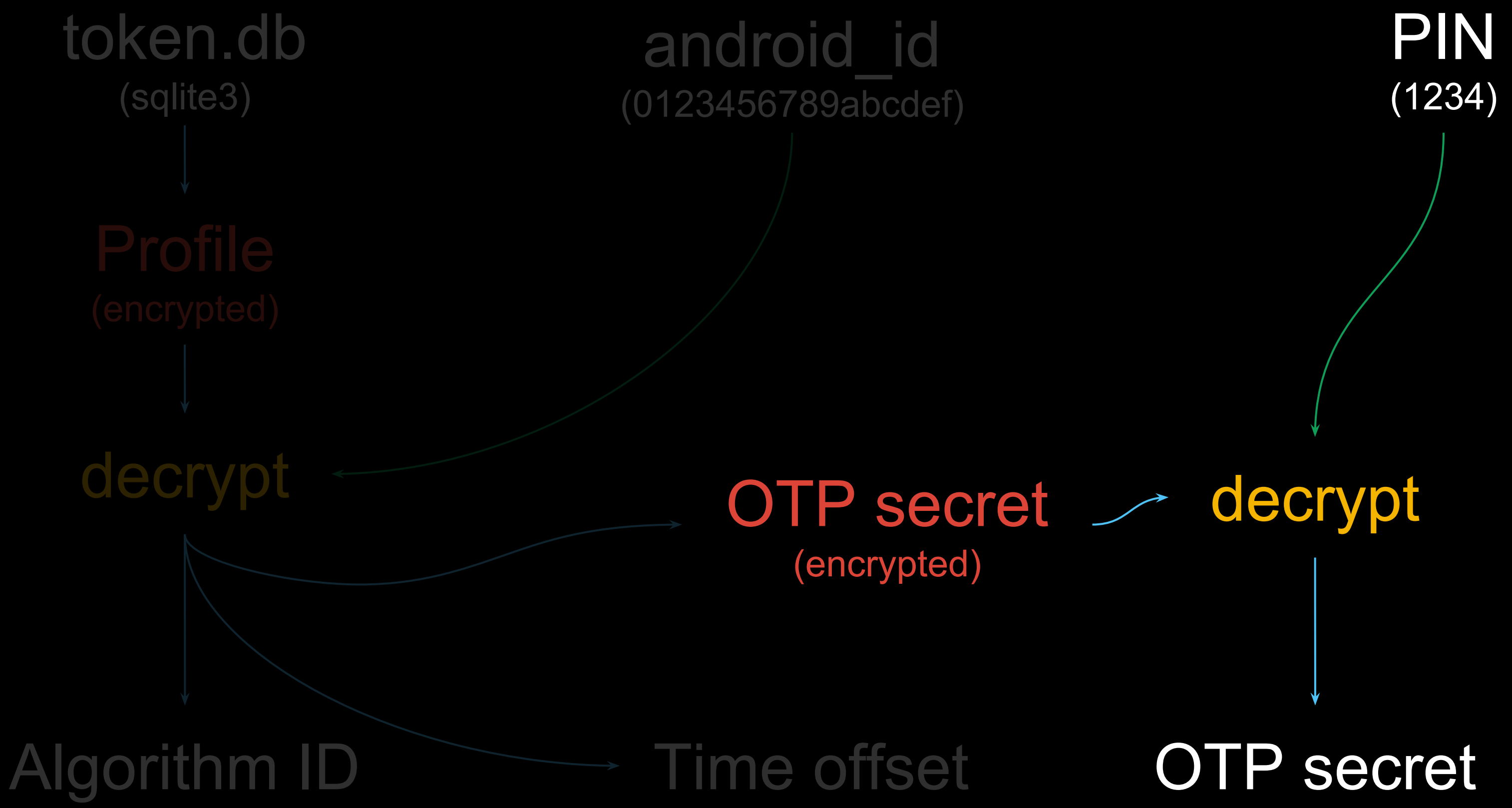


Comic by KC Green (https://thenib.com/this-is-not-fine)

get_otp_secret(db, android_id, pin)



get_otp_secret(db, android_id, pin)



token.db
(sqlite3)

android_id
(0123456789abcdef)

PIN
(1234)

Profile
(encrypted)

decrypt

OTP secret
(encrypted)

decrypt

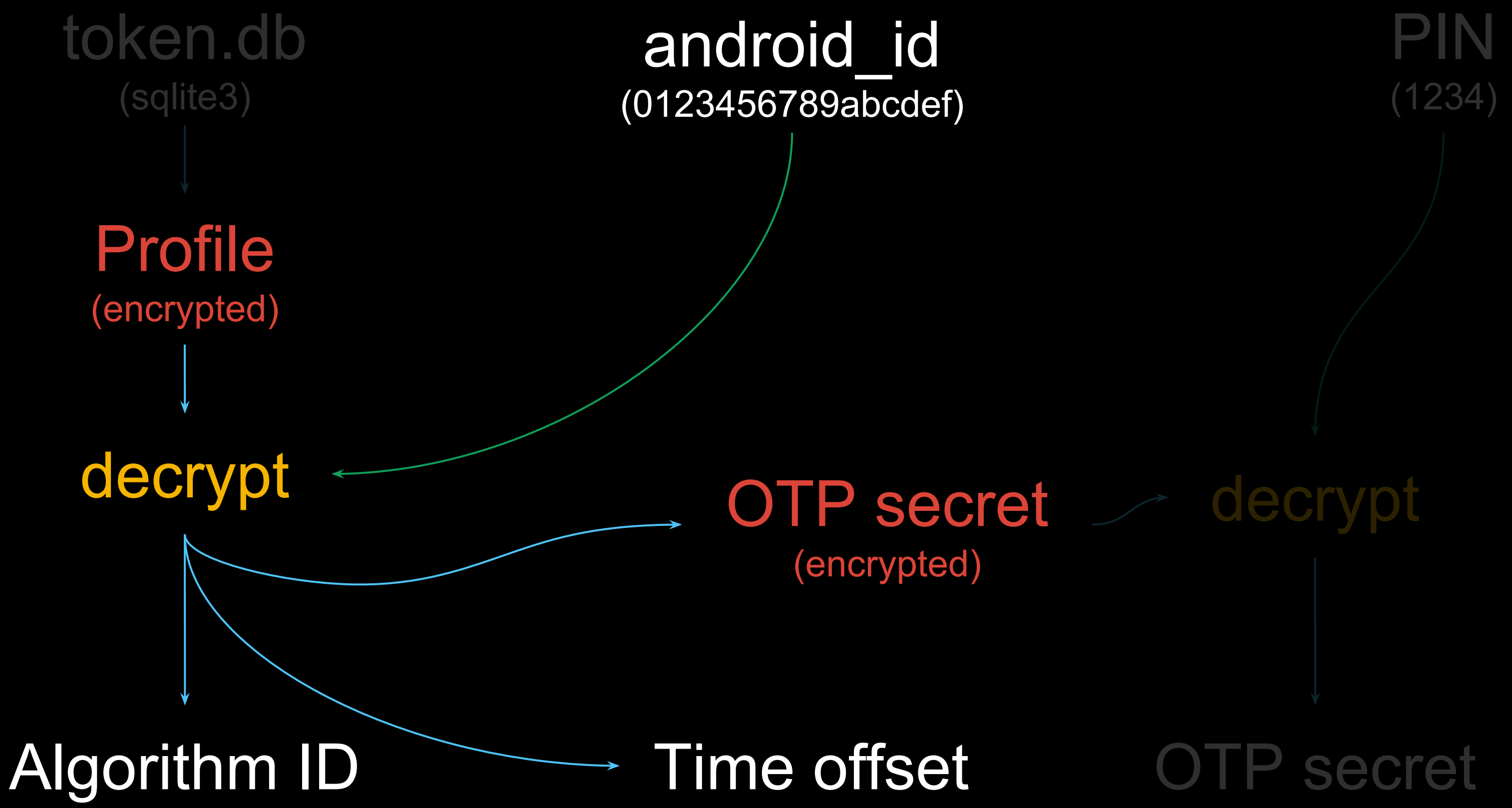
Algorithm ID

Time offset

OTP secret

Comic by KC Green (https://thenib.com/this-is-not-fine)

get_otp_secret(db, android_id, pin)



token.db
(sqlite3)

android_id
(0123456789abcdef)

PIN
(1234)

Profile
(encrypted)

decrypt

OTP secret
(encrypted)

decrypt

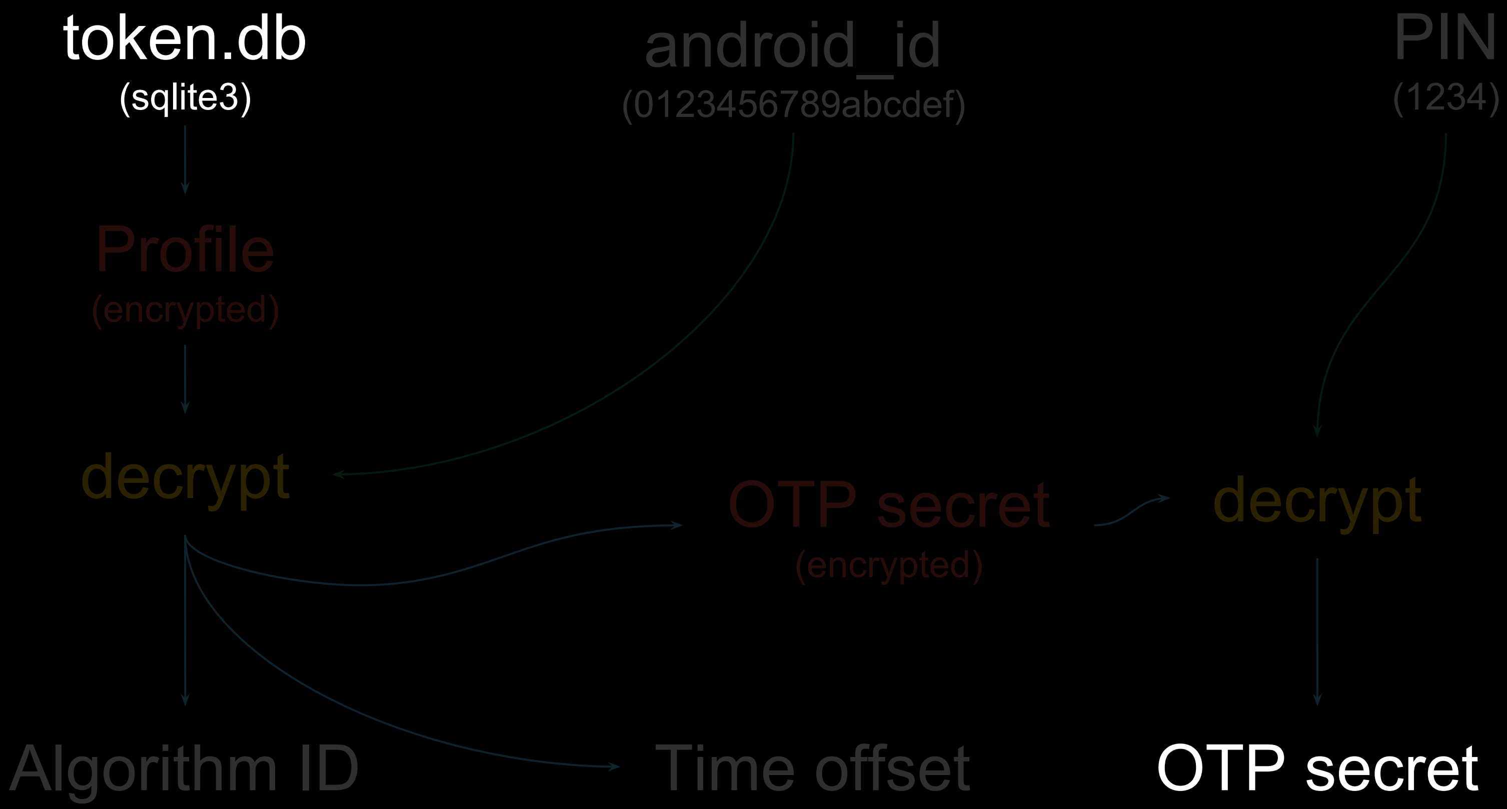
Algorithm ID

Time offset

OTP secret

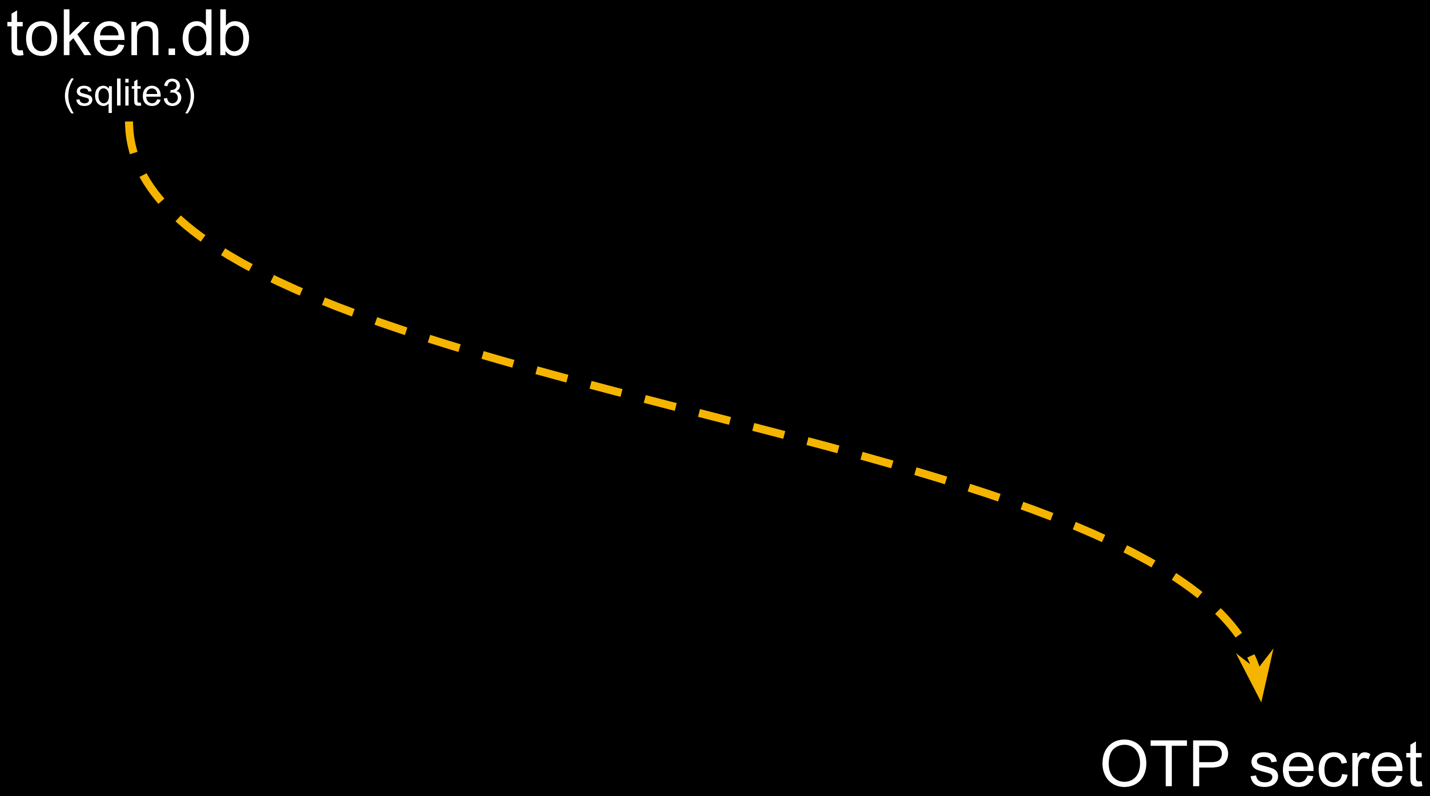
Comic by KC Green (https://thenib.com/this-is-not-fine)

get_otp_secret(db, android_id, pin)



Comic by KC Green (https://thenib.com/this-is-not-fine)

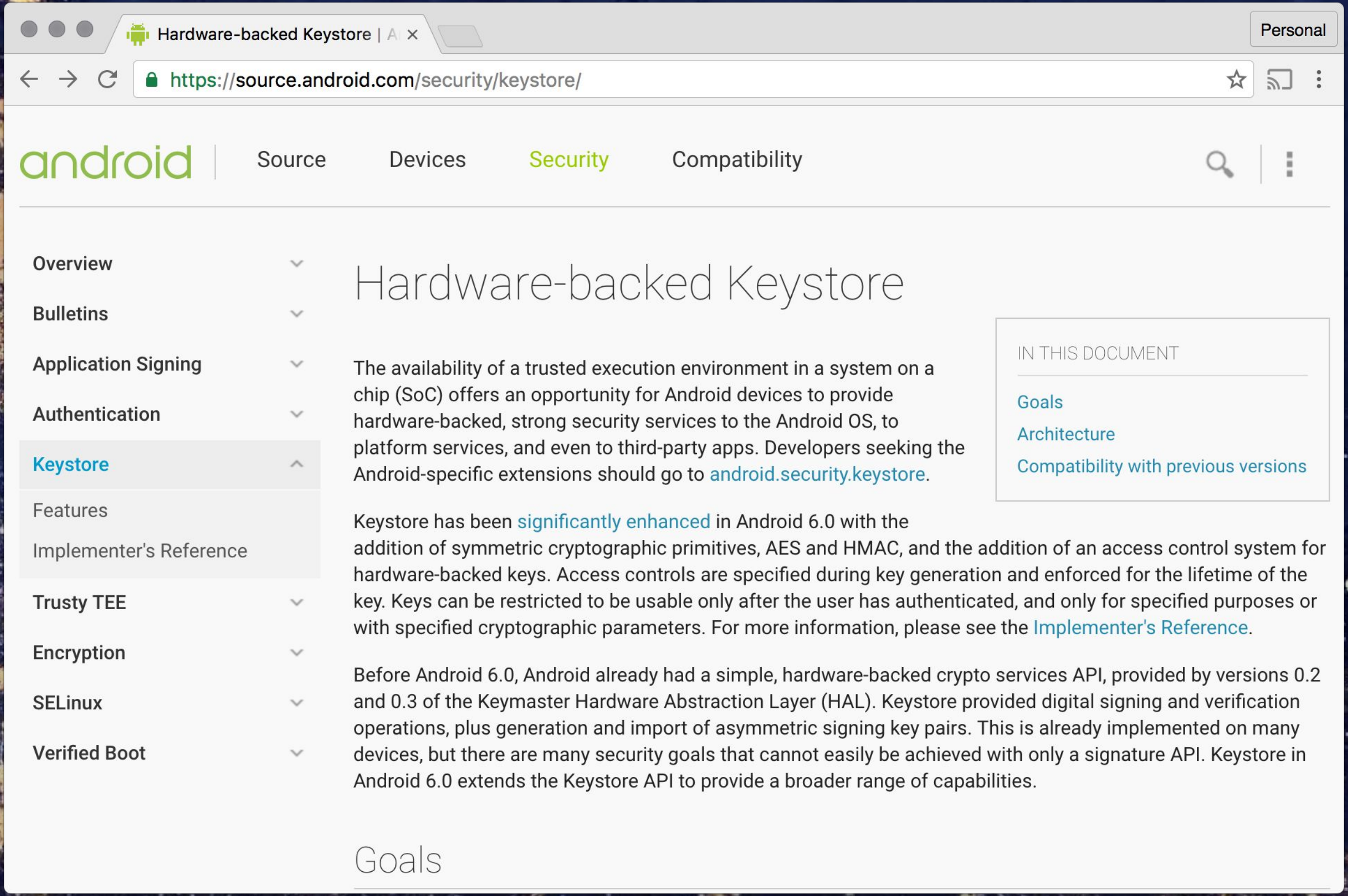
get_otp_secret(db, android_id, pin)



token.db

(sqlite3)

OTP secret



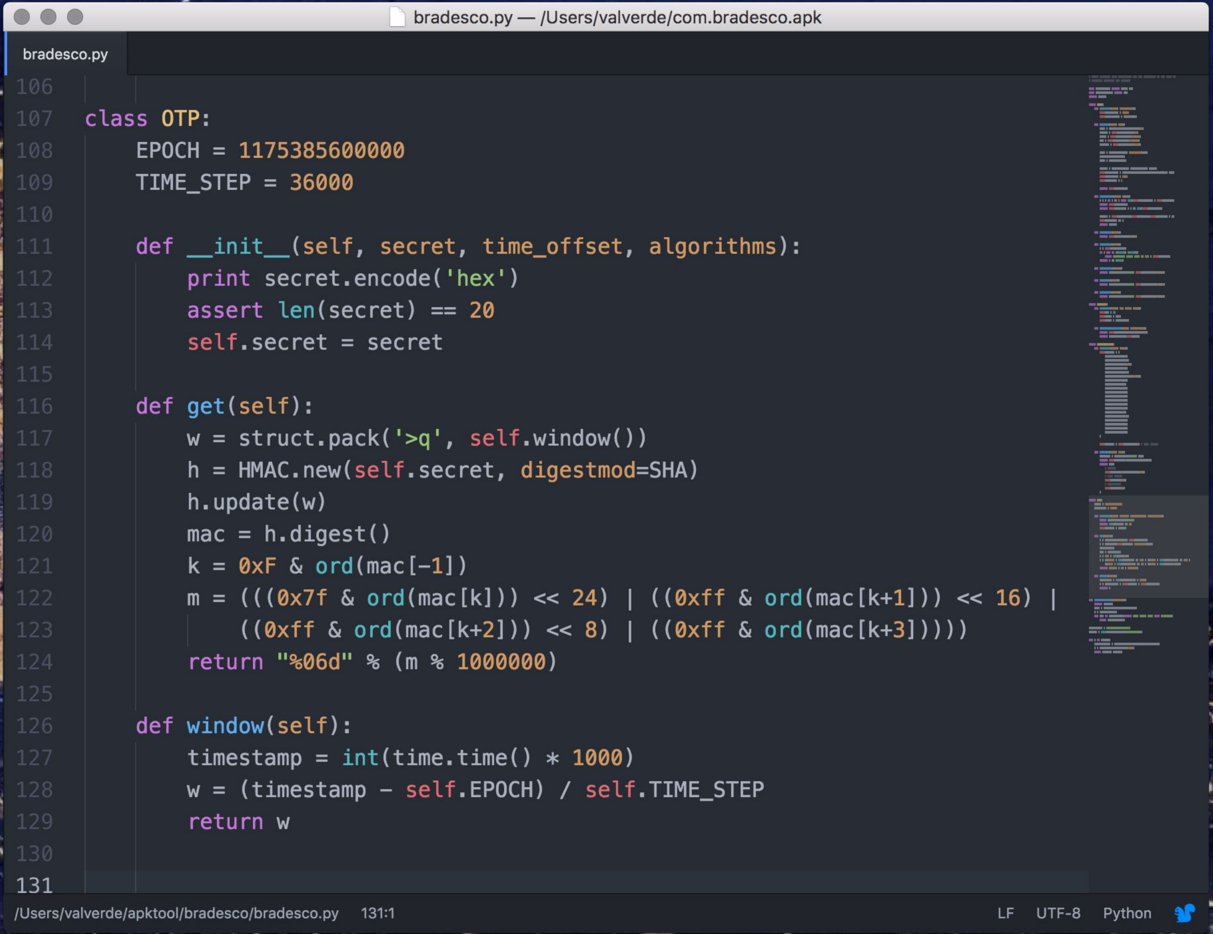
Hardware-backed Keystore

The availability of a trusted execution environment in a system on a chip (SoC) offers an opportunity for Android devices to provide hardware-backed, strong security services to the Android OS, to platform services, and even to third-party apps. Developers seeking the Android-specific extensions should go to android.security.keystore.

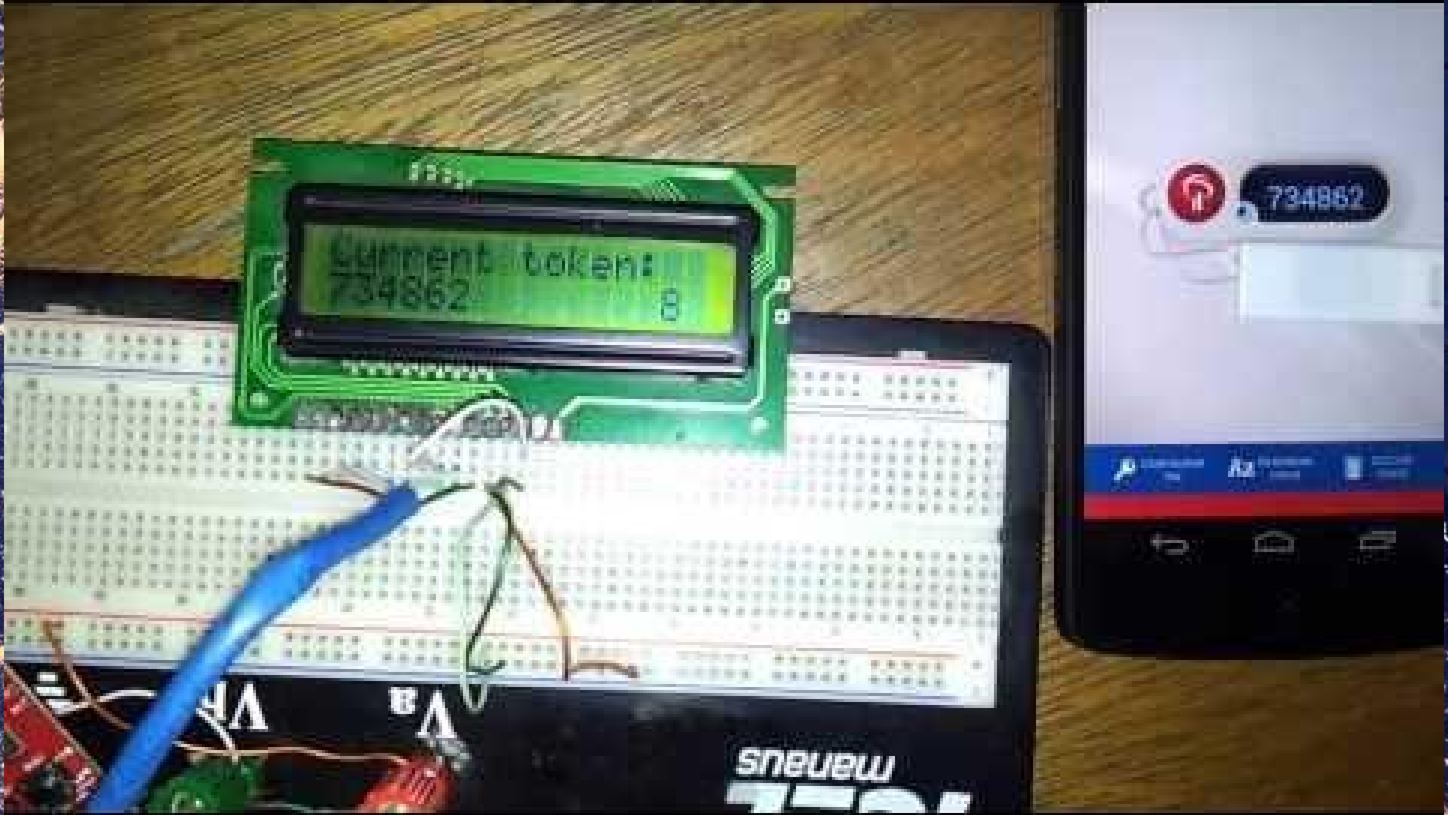
Keystore has been significantly enhanced in Android 6.0 with the addition of symmetric cryptographic primitives, AES and HMAC, and the addition of an access control system for hardware-backed keys. Access controls are specified during key generation and enforced for the lifetime of the key. Keys can be restricted to be usable only after the user has authenticated, and only for specified purposes or with specified cryptographic parameters. For more information, please see the Implementer's Reference.

Before Android 6.0, Android already had a simple, hardware-backed crypto services API, provided by versions 0.2 and 0.3 of the Keymaster Hardware Abstraction Layer (HAL). Keystore provided digital signing and verification operations, plus generation and import of asymmetric signing key pairs. This is already implemented on many devices, but there are many security goals that cannot easily be achieved with only a signature API. Keystore in Android 6.0 extends the Keystore API to provide a broader range of capabilities.

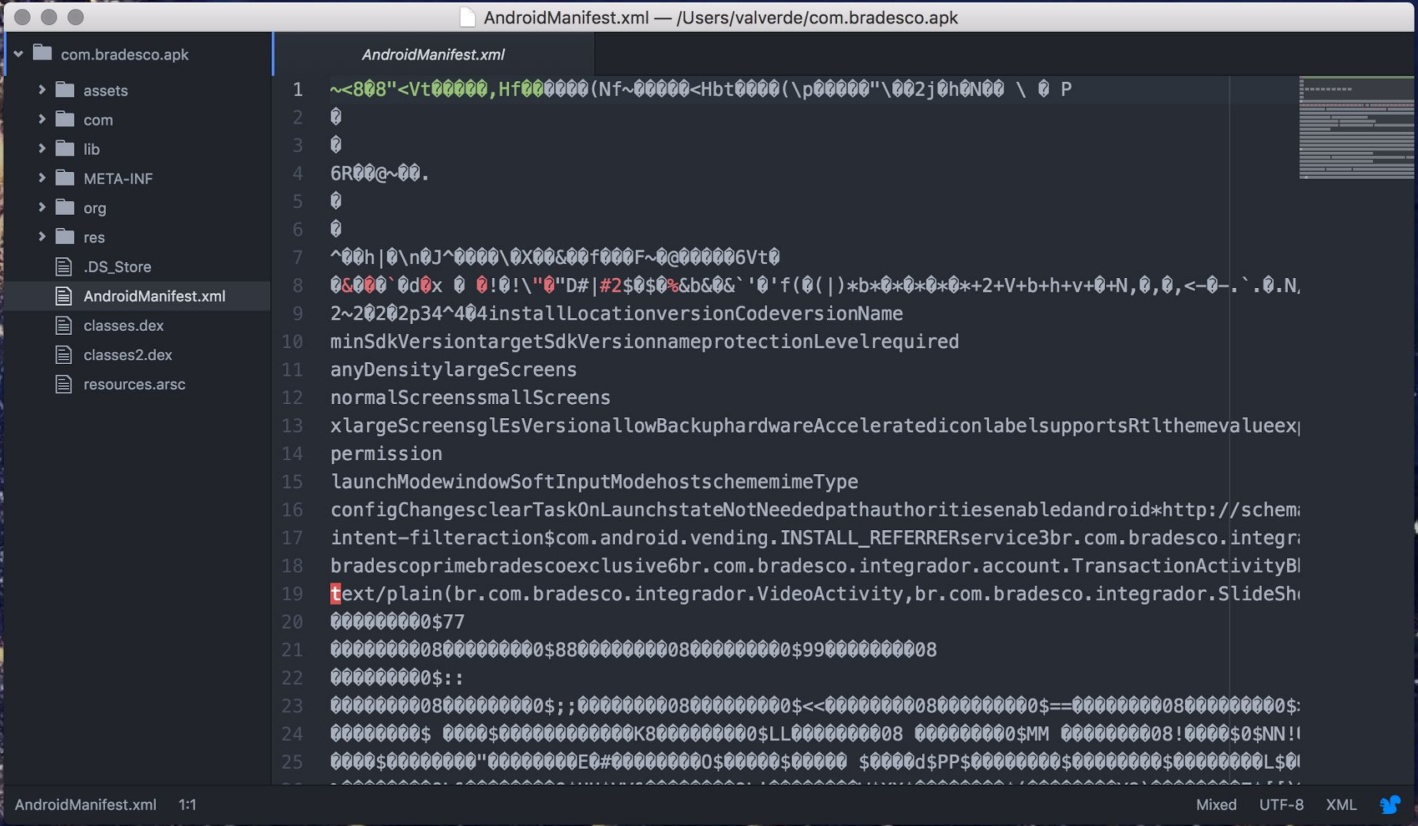
Goals


bradesco.py — /Users/valverde/com.bradesco.apk
bradesco.py
/Users/valverde/apktool/bradesco/bradesco.py
131:1
LF
UTF-8
Python

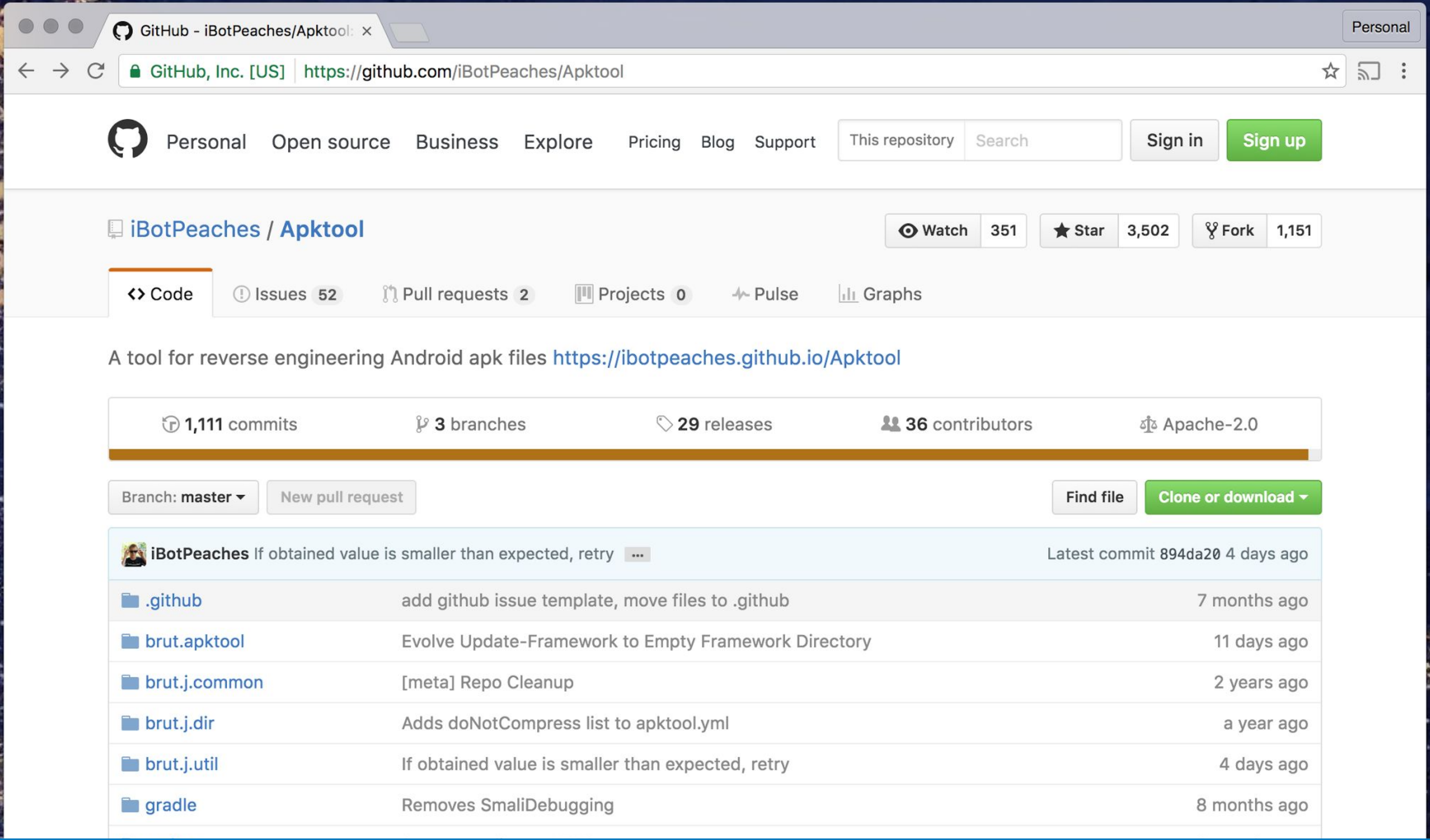
```python
class OTP:
    EPOCH = 1175385600000
    TIME_STEP = 36000

    def __init__(self, secret, time_offset, algorithms):
        print secret.encode('hex')
        assert len(secret) == 20
        self.secret = secret

    def get(self):
        w = struct.pack('>q', self.window())
        h = HMAC.new(self.secret, digestmod=SHA)
        h.update(w)
        mac = h.digest()
        k = 0xF & ord(mac[-1])
        m = (((0x7f & ord(mac[k])) << 24) | ((0xff & ord(mac[k+1])) << 16) |
            ((0xff & ord(mac[k+2])) << 8) | ((0xff & ord(mac[k+3]))))
        return "%06d" % (m % 1000000)

    def window(self):
        timestamp = int(time.time() * 1000)
        w = (timestamp - self.EPOCH) / self.TIME_STEP
        return w
```


Current token:
734862 8
734862

WATCH_DOGE
SUCH MANY HACKING_ WOW



```
~<8�8"<Vt�����,Hf������(Nf~�����<Hbt����(\p�����"\��2j�h�N�� \ � P
�
�
6R��@~��.
�
�
^��h|�\n�J^����\�X��&��f���F~�@������6Vt�
�&���`�d�x � �!�!\"�"D#|#2$�$�%&b&�&`'�'f(�(|)*b*�*�*�*�*+2+V+b+h+v+�+N,�,�,<-�-.`.�.N,
2~2�2�2p34^4�4installLocationversionCodeversionName
minSdkVersiontargetSdkVersionnameprotectionLevelrequired
anyDensitylargeScreens
normalScreenssmallScreens
xlargeScreensglEsVersionallowBackuphardwareAcceleratediconlabelsupportsRtlthemevalueex
permission
launchModewindowSoftInputModehostschememimeType
configChangesclearTaskOnLaunchstateNotNeededpathauthoritiesenabledandroid*http://schem
intent-filteraction$com.android.vending.INSTALL_REFERRERservice3br.com.bradesco.integr
bradescoprimebradescoexclusive6br.com.bradesco.integrador.account.TransactionActivityB
text/plain(br.com.bradesco.integrador.VideoActivity,br.com.bradesco.integrador.SlideSh
���������0$77
���������08���������0$88����������08���������0$99����������08
���������0$::
���������08����������0$;;���������08����������0$<<���������08����������0$==���������08����������0$
��������$ ����$������������K8����������0$LL���������08 ���������0$MM ���������08!����$0$NN!
����$���������"���������E�#���������O$������$������ $����d$PP$���������$���������$���������L$�
```



iBotPeaches / Apktool

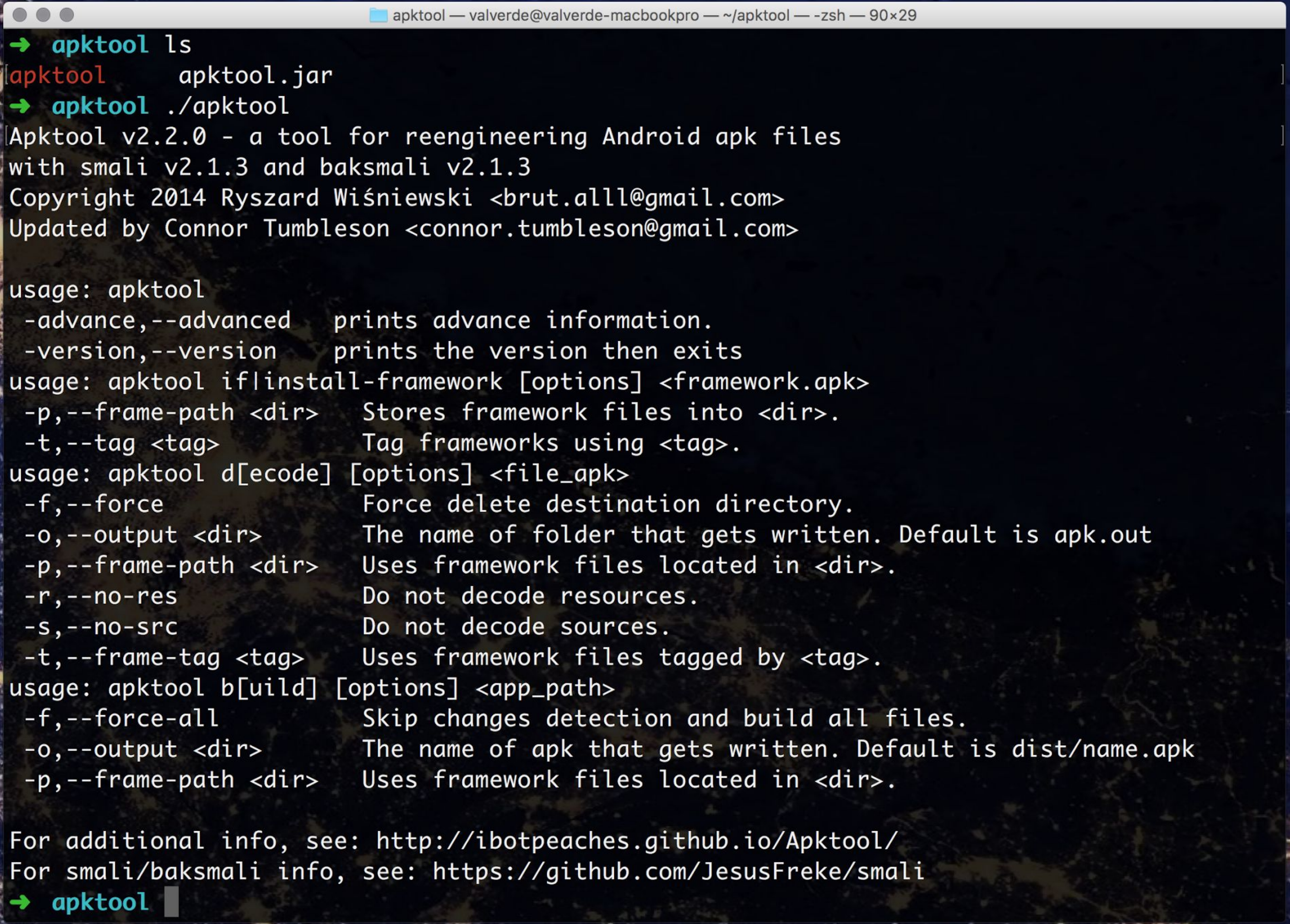
A tool for reverse engineering Android apk files https://ibotpeaches.github.io/Apktool

1,111 commits · 3 branches · 29 releases · 36 contributors · Apache-2.0

iBotPeaches If obtained value is smaller than expected, retry … Latest commit 894da20 4 days ago

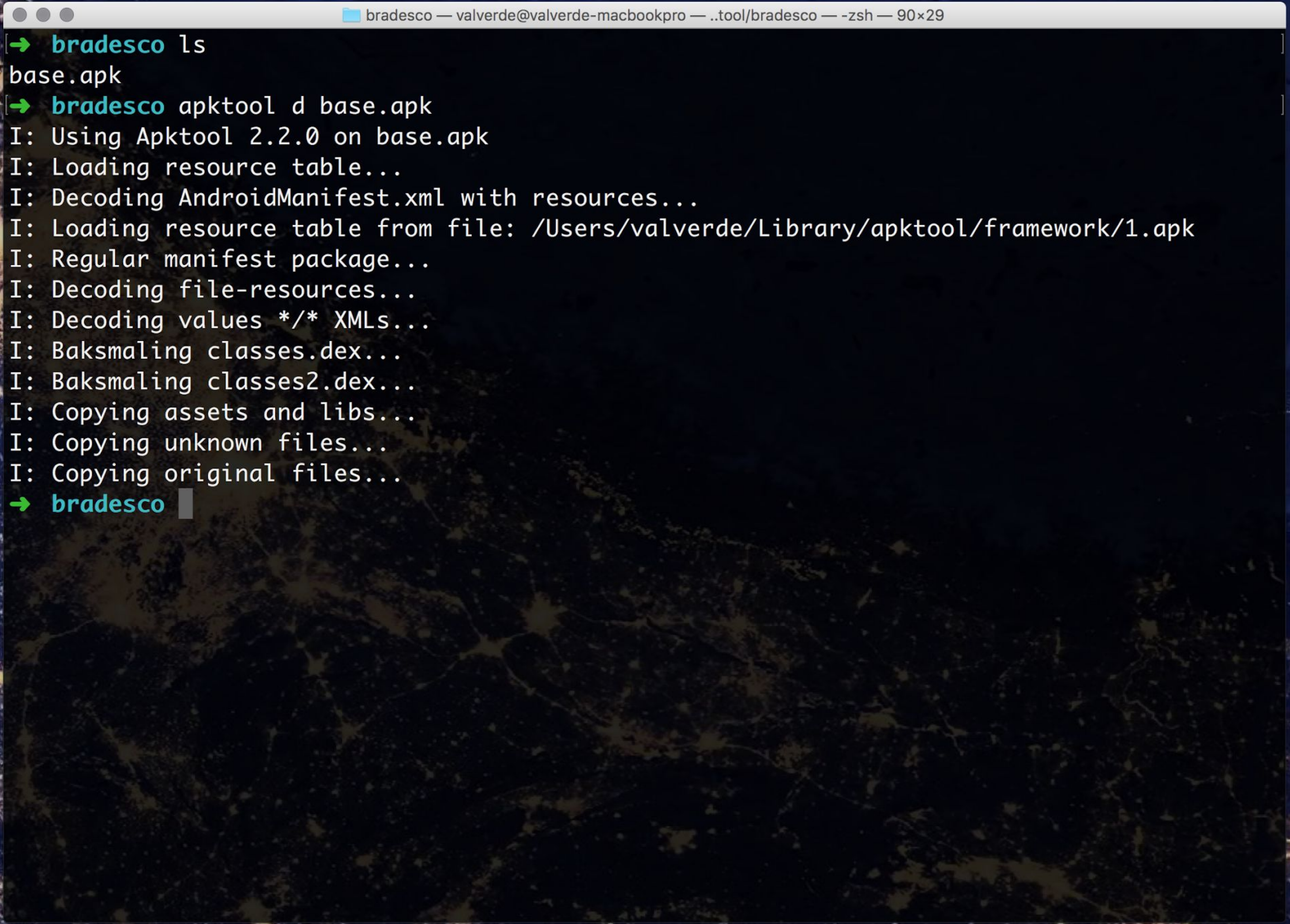
.github	add github issue template, move files to .github	7 months ago
brut.apktool	Evolve Update-Framework to Empty Framework Directory	11 days ago
brut.j.common	[meta] Repo Cleanup	2 years ago
brut.j.dir	Adds doNotCompress list to apktool.yml	a year ago
brut.j.util	If obtained value is smaller than expected, retry	4 days ago
gradle	Removes SmaliDebugging	8 months ago

https://github.com/iBotPeaches/Apktool



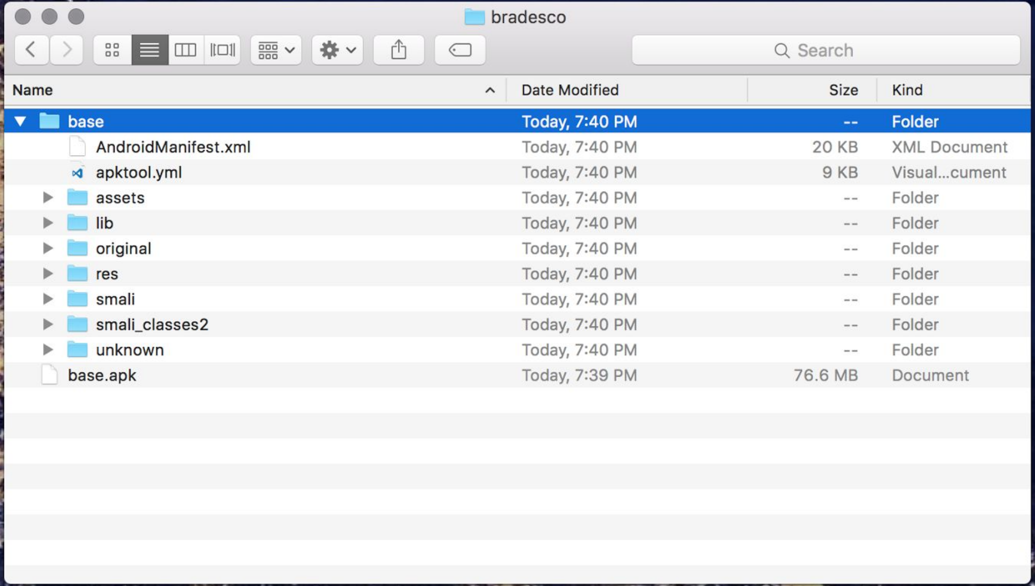
apktool — valverde@valverde-macbookpro — ~/apktool — -zsh — 90×29

```
➜  apktool ls
apktool      apktool.jar
➜  apktool ./apktool
Apktool v2.2.0 - a tool for reengineering Android apk files
with smali v2.1.3 and baksmali v2.1.3
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   prints advance information.
 -version,--version    prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Stores framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. Default is apk.out
 -p,--frame-path <dir>   Uses framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
 -p,--frame-path <dir>   Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
➜  apktool
```

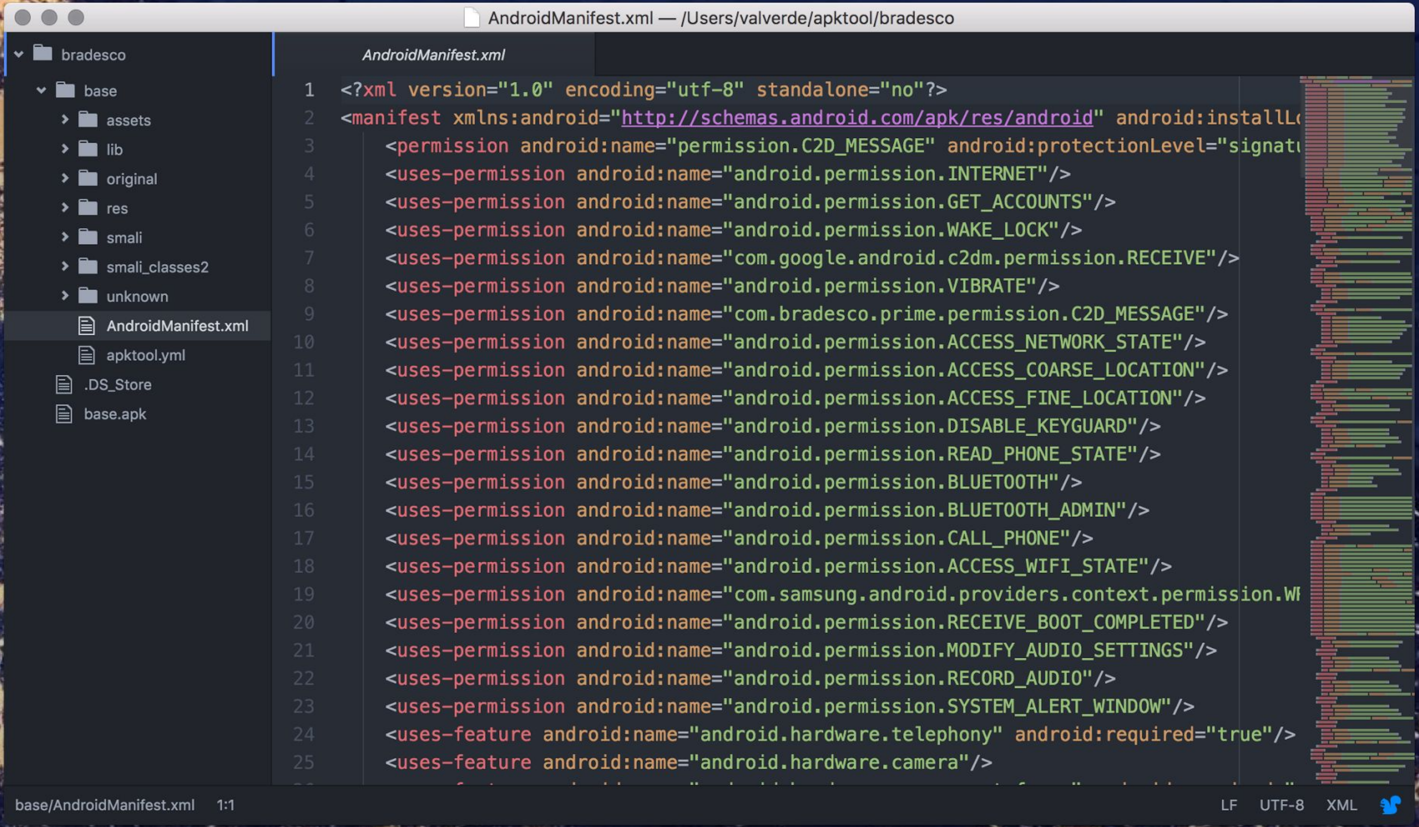


bradesco — valverde@valverde-macbookpro — ..tool/bradesco — -zsh — 90×29

```
➜  bradesco ls
base.apk
➜  bradesco apktool d base.apk
I: Using Apktool 2.2.0 on base.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/valverde/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Baksmaling classes2.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
➜  bradesco 
```

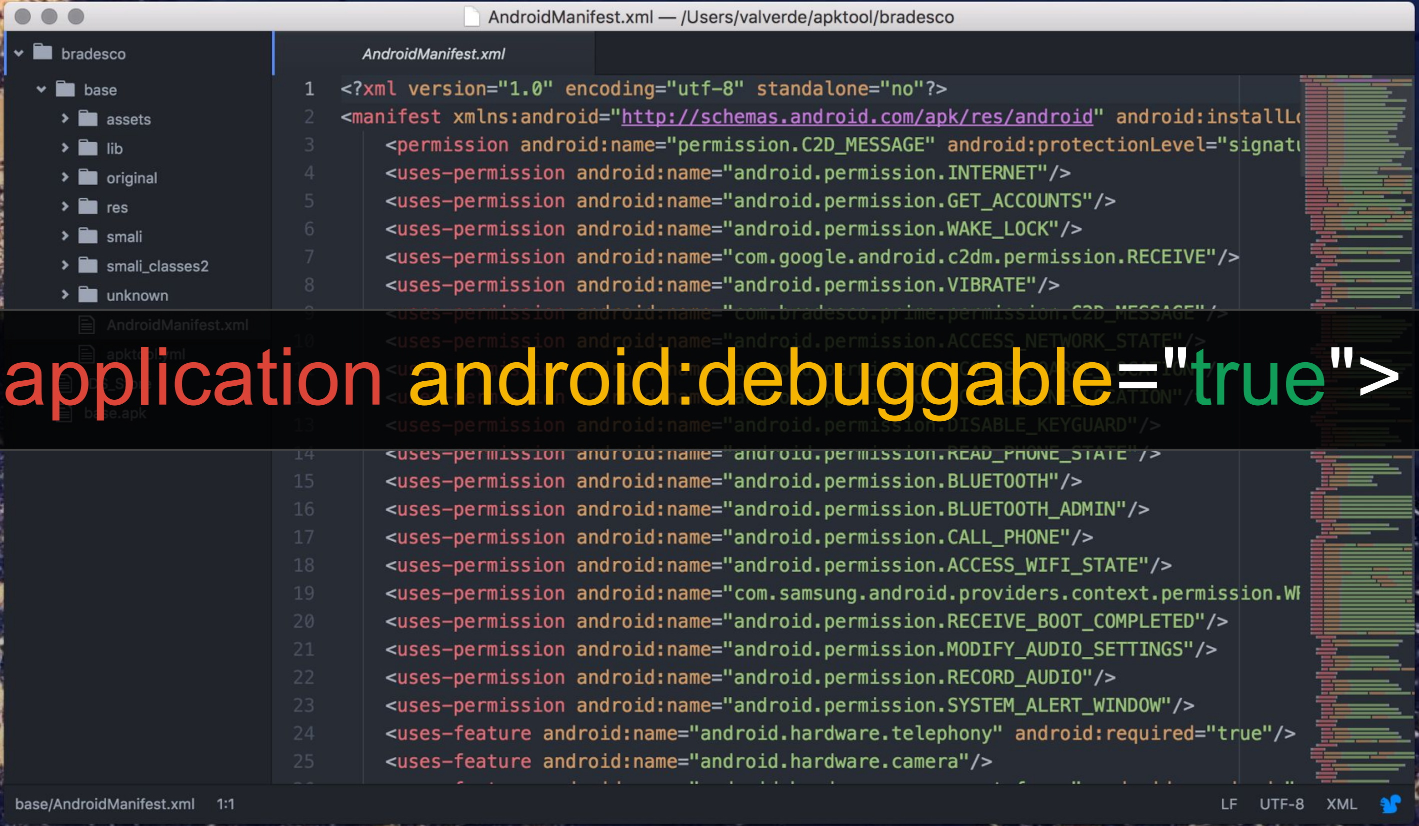


Name	Date Modified	Size	Kind
base	Today, 7:40 PM	--	Folder
AndroidManifest.xml	Today, 7:40 PM	20 KB	XML Document
apktool.yml	Today, 7:40 PM	9 KB	Visual...cument
assets	Today, 7:40 PM	--	Folder
lib	Today, 7:40 PM	--	Folder
original	Today, 7:40 PM	--	Folder
res	Today, 7:40 PM	--	Folder
smali	Today, 7:40 PM	--	Folder
smali_classes2	Today, 7:40 PM	--	Folder
unknown	Today, 7:40 PM	--	Folder
base.apk	Today, 7:39 PM	76.6 MB	Document

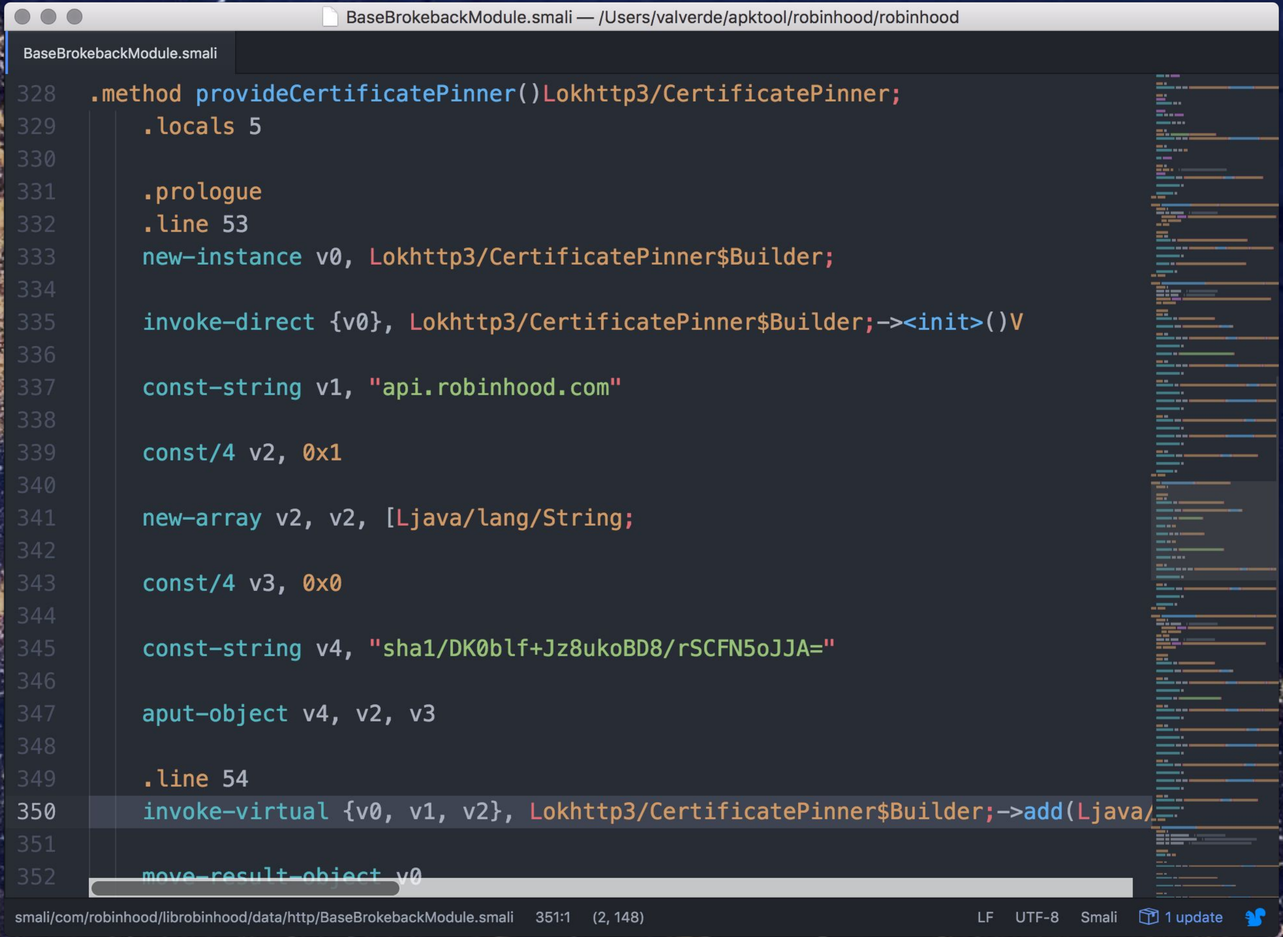


```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:installL
    <permission android:name="permission.C2D_MESSAGE" android:protectionLevel="signat
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="com.bradesco.prime.permission.C2D_MESSAGE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="com.samsung.android.providers.context.permission.W
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-feature android:name="android.hardware.telephony" android:required="true"/>
    <uses-feature android:name="android.hardware.camera"/>
```

<application android:debuggable="true">



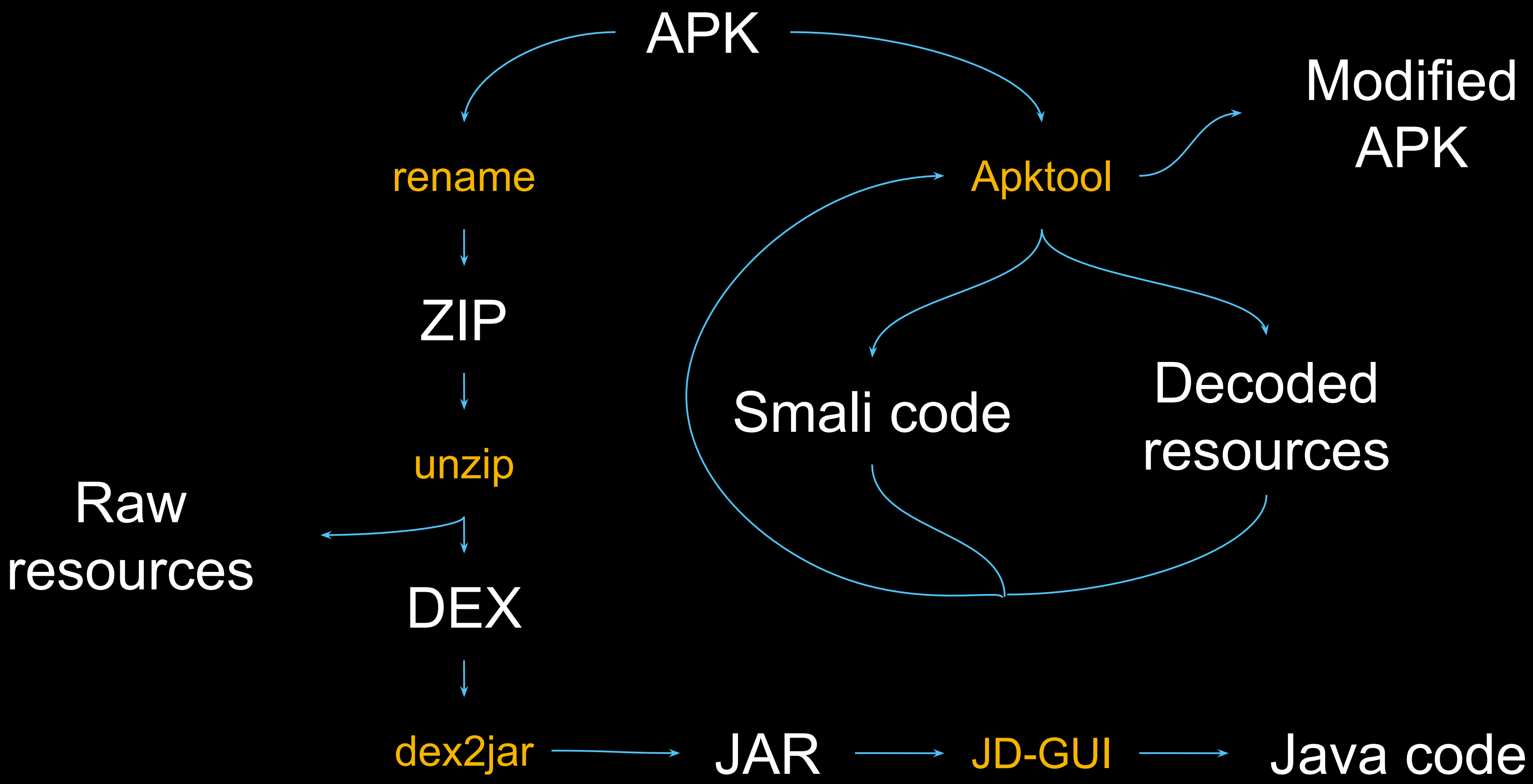
```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:installL
    <permission android:name="permission.C2D_MESSAGE" android:protectionLevel="signatu
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="com.bradesco.prime.permission.C2D_MESSAGE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="com.samsung.android.providers.context.permission.WI
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-feature android:name="android.hardware.telephony" android:required="true"/>
    <uses-feature android:name="android.hardware.camera"/>
```



BaseBrokebackModule.smali — /Users/valverde/apktool/robinhood/robinhood
BaseBrokebackModule.smali

```
.method provideCertificatePinner()Lokhttp3/CertificatePinner;
    .locals 5

    .prologue
    .line 53
    new-instance v0, Lokhttp3/CertificatePinner$Builder;

    invoke-direct {v0}, Lokhttp3/CertificatePinner$Builder;-><init>()V

    const-string v1, "api.robinhood.com"

    const/4 v2, 0x1

    new-array v2, v2, [Ljava/lang/String;

    const/4 v3, 0x0

    const-string v4, "sha1/DK0blf+Jz8ukoBD8/rSCFN5oJJA="

    aput-object v4, v2, v3

    .line 54
    invoke-virtual {v0, v1, v2}, Lokhttp3/CertificatePinner$Builder;->add(Ljava/

    move-result-object v0
```

smali/com/robinhood/librobinhood/data/http/BaseBrokebackModule.smali 351:1 (2, 148)
LF UTF-8 Smali 1 update


APK
rename
ZIP
unzip
Raw resources
DEX
dex2jar
JAR
JD-GUI
Java code
Apktool
Modified APK
Smali code
Decoded resources

Q&A