

Auditoria de seguridad a Uber



UNIVERSIDAD
Finis Terrae
VINCE IN BONO MALUM

Esteban Motyvay

Noviembre 29, 2017

Universidad Finis Terrae

Tabla de contenidos

1 Introducción

2 Aplicación escogida

3 Plan de Acción

4 Descompilacion

5 Pasos a seguir

6 Pruebas

Introducción

En el presente proyecto se realizara una auditoría de una aplicación Móvil, donde se deberá realizar una investigación de sus tipos de vulnerabilidades que se encuentran dentro de sus códigos, para luego realizar ataques éticos para ver que tan vulnerables es esta. Luego de haber documentado esta auditoría a la aplicación, se deberá reportar estos riesgos a la empresa que se le realizo la auditoría. Para que esta entidad pueda mitigar estos problemas de encontrados.

UBER

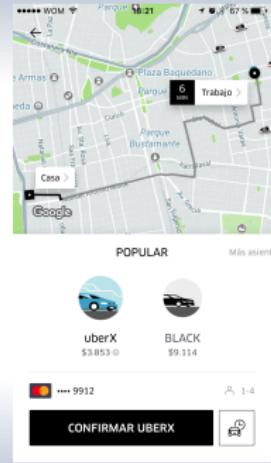
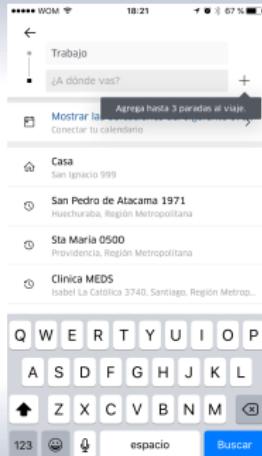
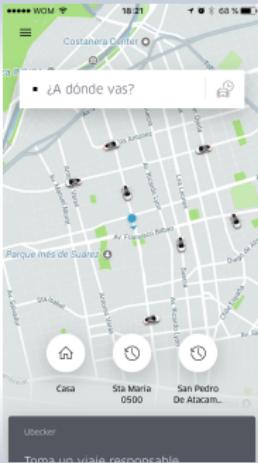
Uber es una compañía norteamericana que está transformando la manera en que las personas se mueven en las ciudades. Contactándose a través de una aplicación, de manera simple, a conductores con usuarios que requieren un servicio de traslado.



U B E R

Aplicación escogida

Uso de aplicación



Objetivos

Objetivo General

- Se deberá realizar una auditoría de seguridad haciendo distintos tipos de ataques éticos a la aplicación Uber, para detectar sus problemas y reportarlos.

Objetivos específicos

- Estudiar aplicación escogida
- Buscar puntos de vulnerabilidad
- Estudiar métodos de ataques a utilizar

Plan de acción

Actividades

- Simulación de pago en Uber con Bin Falsos
- Modificar la ubicación de Uber Drive
- Analizar puertos libres de la aplicación
- Man in the middle a Uber.

Descompilacion

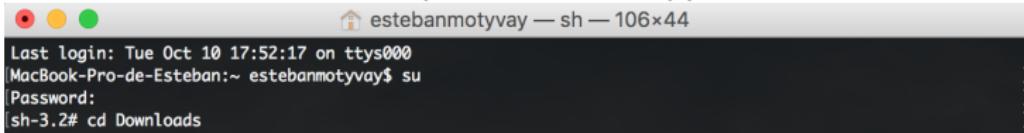
Para realizar la descompilacion de la APK y análisis de Uber, se debió realizar la instalación y actualización de algunos programas:

Programas:

- Java SDK y JRE
- Android SDK
- Apktool
- uber.apk

Paso a Paso

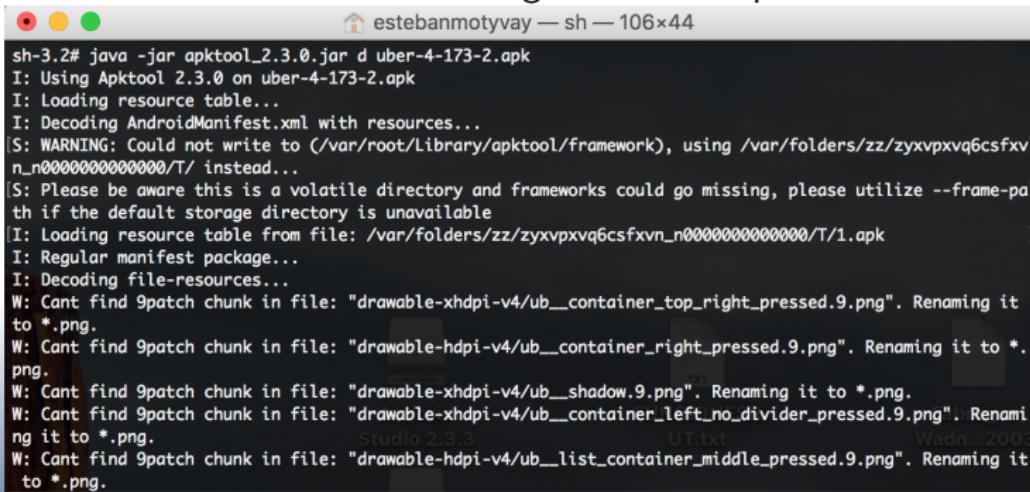
Luego de haber instalado todos los programas necesarios, se debe abrir la terminal, donde se debe iniciar el Super Usuario (su) y se deberá ingresar la Pw correspondiente al super usuario. Luego se inicia todo el proceso de descompilacion de la Apps.



```
estebanmotyvay — sh — 106x44
Last login: Tue Oct 10 17:52:17 on ttys000
MacBook-Pro-de-Esteban:~ estebanmotyvay$ su
Password:
sh-3.2# cd Downloads
```

Paso a Paso

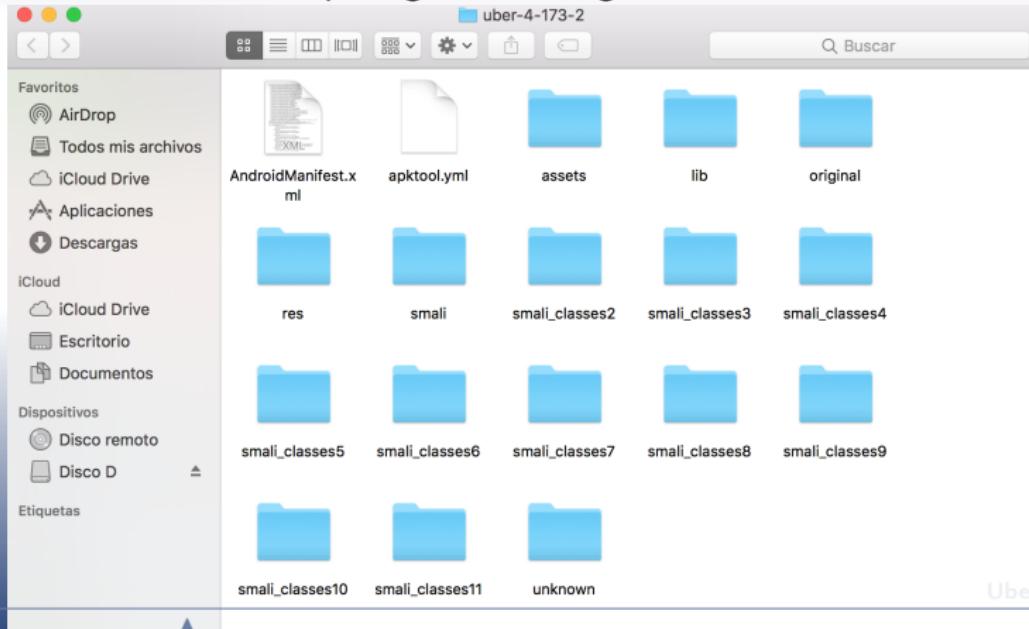
Luego de haber ejecutado el super usuario, se ejecuta la aplicacion Apktool.jar, este se busca por terminal y este se encuentra en descarga. Para poder ejecutarlo se ingresa el comando java -jar d nombredelaapk.apk. La d del comando significa descompilar.



```
estebanmotyvay — sh — 106x44
sh-3.2# java -jar apktool_2.3.0.jar d uber-4-173-2.apk
I: Using Apktool 2.3.0 on uber-4-173-2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
[S: WARNING: Could not write to (/var/root/Library/apktool/framework), using /var/folders/zz/zxyvpxvq6csfxvn_n000000000000/T/ instead...
[S: Please be aware this is a volatile directory and frameworks could go missing, please utilize --framew...
I: Loading resource table from file: /var/folders/zz/zxyvpxvq6csfxvn_n000000000000/T/1.apk
I: Regular manifest package...
I: Decoding file-resources...
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/ub__container_top_right_pressed.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-hdpi-v4/ub__container_right_pressed.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/ub__shadow.9.png". Renaming it to *.png.
W: Cant find 9patch chunk in file: "drawable-xhdpi-v4/ub__container_left_no_divider_pressed.9.png". Renami...
W: Cant find 9patch chunk in file: "drawable-hdpi-v4/ub__list_container_middle_pressed.9.png". Renaming it to *.png.
```

Paso a Paso

Luego de descompilar la aplicacion, este genera los archivos de la aplicacion donde se encontrara el .XML que sera donde estara el codigo de la aplicacion y otros archivos complementarios para la aplicacion. La aplicacion al descompilar genero los siguientes archivos:



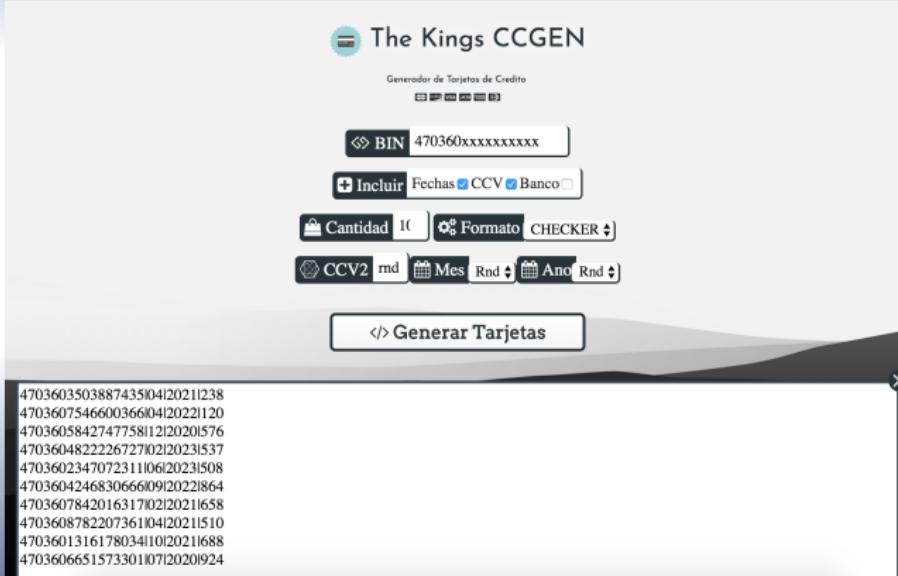
Paso a Paso

Utilizando la aplicación Android Studio, se detecto que esta utilizaba el método de encriptacion de SHA1 y DSA

```
<!-- Signature Algorithms -->
<Algorithm URI="http://www.w3.org/2000/09/xmldsig#dsa-sha1"
    Description="Digital Signature Algorithm with SHA-1 message digest"
    AlgorithmClass="Signature"
    RequirementLevel="REQUIRED"
    JCEName="SHA1withDSA"/>
```

BIN falso

Se realiza la generación de un bin falso dentro de una pagina web. En esto se realiza una investigación de los primeros 4 dígitos del bin que coincidan con un Banco y los siguientes 2 números con las sucursral.



The Kings CCGEN

Generador de Tarjetas de Crédito

BIN 470360xxxxxxxxxx

Incluir Fechas CCV Banco

Cantidad 10 Formato CHECKER

CCV2 rnd Mes Rnd Ano Rnd

</> Generar Tarjetas

470360350388743504 2021 238
470360754660036604 2022 120
4703605842747758 12 2020 576
470360482222672702 2023 537
4703602347072311 06 2023 508
470360424683066609 2022 864
4703607842016317 02 2021 658
4703608782207361 04 2021 688
470360131617803410 2021 688
4703606651573301 07 2020 924



Ingresando bin

Se realiza la prueba de ingresar el Bin generado a la plataforma de Uber.

21:24 100% •••• WOM

← Agregar tarjeta

Número de tarjeta
VISA 4703 6035 0388 7435

Fecha de vto. CVV
04/21 238

País
Chile

GUARDAR

23:27 100% •••• WOM

← Agregar tarjeta

Número de tarjeta
VISA 4703 6035 0388 7435

Fecha de vto. CVV
04/21 238

País
Chile

GUARDAR

23:27 100% •••• WOM

X Pago

Métodos de pago

- VISA 1533
- Efectivo
- VISA 9912
- VISA 7435

Agregar método de pago

Promociones

Agregar un código promo/de regalo

Ubicación actual

En Uber existe la aplicación Uber Drive que es la aplicación de los choferes de uber, esta trabaja con un mapa, donde este dice el lugar donde se encuentran mas demanda y a la vez si se encuentra con tarifa dinamica. Se realizo la instalacion de Cydia al equipo iphone y se instalo un FakeGps para modificar la ubicación actual del telefono.



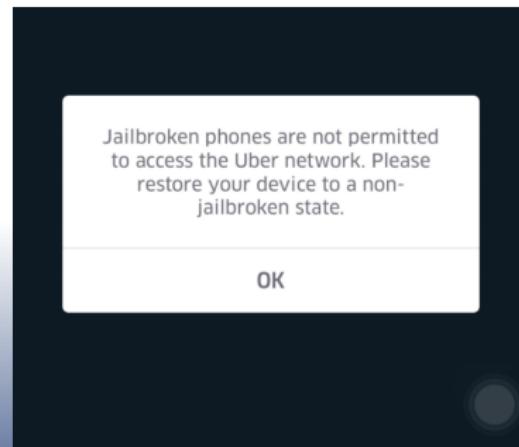
Ubicación Actual

Se realiza la generación de un bin falso dentro de una plataforma web. En esto se realiza una investigación de los primeros 4 dígitos del bin que coincidan con un Banco y los siguientes 2 números con las sucursales.



Resultado Ubicación actual

Luego de ciertos problemas que esta tuvo con sus conductores que realizaban esa actividad para generar mas ingresos. La empresa decidió en que en su aplicación no pueda ser ejecutada si es que el equipo móvil se encontraba alterado, esto transformo a Uber en una de las aplicaciones mas seguras que se encuentran en el mercado.



Análisis de puertos

Se realiza un análisis de puertos a Uber, donde para esto se reviso AndroidManifest.xml buscando la dirección hacia el servidor de la aplicación Uber.

```
<action android:name="android.intent.action.VIEW"/>
<category android:name="android.intent.category.DEFAULT"/>
<category android:name="android.intent.category.BROWSABLE"/>
<data android:host="m.uber.com" android:pathPrefix="/ul/" android:scheme="http"/>
<data android:host="m.uber.com" android:pathPrefix="/ul/" android:scheme="https"/>
```

NMAP

Una vez obtenido la dirección del servidor de Uber, se le realiza un análisis de puerto.

```
Nmap scan report for m.uber.com (104.36.194.160)
Host is up (0.24s latency).
Other addresses for m.uber.com (not scanned): 104.36.194.232 104.36.194.134 104.36.194.159 104.36.194.190 1
04.36.194.234 104.36.194.231 104.36.194.191
Not shown: 997 filtered ports
S://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/ ▾
PORT      STATE SERVICE
21/tcp    open  ftp
          es aplicando el siguiente comando: nmap -sU 21 ...
80/tcp    open  http
443/tcp   open  https
```

Vulnerabilidad de Puertos

Puerto 21 - ftp: Buffer Overflow Denegacion de Servicio (DoS) Ataque de Fuerza Bruta Punto de Acceso

Puerto 80 http: Ataque CGI Buffer Oveflow Denegación de Servicio (DoS)
Recogida de Información Punto de Acceso Posibilidad de sniffer.

Man in the middle 1



Wireshark

Man in the middle 1

Se realiza la primera actividad de man in the middle en Wireshark, donde se verifican los paquetes enviados

No.	Time	Source	Destination	Protocol	Length	Info
1075..	297.299495	192.168.0.106	104.36.194.175	TLSv1.2	104	Application Data
1075..	297.421777	104.36.194.175	192.168.0.106	TLSv1.2	1454	Server Hello
1075..	297.424070	104.36.194.175	192.168.0.106	TLSv1.2	1209	Certificate, Server Key Exchange, Server Hello Done
1076..	297.448754	104.36.194.175	192.168.0.106	TLSv1.2	104	Application Data
1076..	297.6568037	192.168.0.106	172.217.30.14	TLSv1.2	295	Client Hello
1076..	297.6568017	192.168.0.106	104.36.194.175	TLSv1.2	141	Client Key Exchange
1076..	297.658048	192.168.0.106	104.36.194.175	TLSv1.2	72	Change Cipher Spec
1076..	297.658070	192.168.0.106	104.36.194.175	TLSv1.2	111	Encrypted Handshake Message
1076..	297.676356	104.36.194.175	192.168.0.106	TLSv1.2	313	Application Data
1076..	297.745851	172.217.30.14	192.168.0.106	TLSv1.2	1454	Server Hello
1076..	297.745856	172.217.30.14	192.168.0.106	TLSv1.2	328	Certificate, Server Key Exchange, Server Hello Done
1076..	297.749898	192.168.0.106	17.188.206.22	TLSv1.2	1254	Application Data [TCP segment of a reassembled PDU]
1076..	297.750190	192.168.0.106	191.232.99.2	TLSv1.2	507	Application Data
1076..	297.806123	192.168.0.106	172.217.30.14	TLSv1.2	141	Client Key Exchange
1076..	297.806219	192.168.0.106	172.217.30.14	TLSv1.2	72	Change Cipher Spec
1076..	297.806262	192.168.0.106	172.217.30.14	TLSv1.2	111	Encrypted Handshake Message
[2026 bytes captured (2026 bytes on wire) (1013 bits captured (1013 bits on wire))						
> Frame 107622: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits) on interface 0						
> Ethernet II, Src: Tp-LinkT_97:62:1e (b0:48:7a:97:62:1e), Dst: CompalIn_fb:45:0a (1c:39:47:fb:45:0a)						
> Internet Protocol Version 4, Src: 172.217.30.14, Dst: 192.168.0.106						
> Transmission Control Protocol, Src Port: 443, Dst Port: 62091, Seq: 4165, Ack: 230, Len: 262						
> [4 Reassembled TCP Segments (3913 bytes): #107619(1037), #107620(1388), #107621(1388), #107622(100)]						
> Secure Sockets Layer						
> Secure Sockets Layer						
0000	1c 39 47 fb 45 0e b0 48	7a 97 62 1e 08 00 45 00	.9G.E..H z.b...E.			
0010	01 3a 7d e9 00 00 32 06	7d bb ac d9 1e 0e c0 a8	.:}...2. }.....			
0020	00 6a 01 bb f2 8b d1 86	05 66 b9 a6 10 ad 80 18	.j..... .f.....			
0030	00 aa 21 37 00 01 01 08	08 aa 6f be 3f 0f 29 5b	.!7.... ..o.?)[
0040	7a 15 ff f0 f0 c8 4e d6	43 38 be b9 30 7d 18 d0	z....N. C8..0)..			
0050	55 83 a2 6a cb 36 11 9c	e8 48 66 a3 6d 7f b8 13	U..J.6.. .Hf.m...			
0060	d4 47 fe 8b 5a 5c 73 fc	ae d9 1b 32 19 38 ab 97	.G..Z.s. ...2.8..			



Man in the middle 2



Man in the middle 2

Se realiza la segunda actividad de man in the middle en MitmProxy y DSniff. En este punto se debe ingresar el Certificado dado por la aplicación, que se guardara como perfil de iphone



Man in the middle 2

Se visualiza la captura de paquetes que esta teniendo la aplicación forzando la conexión del iPhone al notebook.

```
Archivo Editar Ver Buscar Terminal Ayuda
    token...
    - 206 application/octet-stream 512k 650ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 512k 745ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 512k 626ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 512k 758ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 512k 597ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 512k 667ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 512k 695ms
GET http://audio.ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
    token...
    - 206 application/octet-stream 291k 389ms
>> GET http://init-p01st.push.apple.com/bag
    - 200 application/x-apple-plist 7k 143ms
[20/20] [showhost]                                         ?:help [*:8080]
Warn: 192.168.0.100:65230: Client Handshake failed. The client may not trust the proxy's
certificate for mms.whatsapp.net.
```

Man in the middle 3



Man in the middle 3

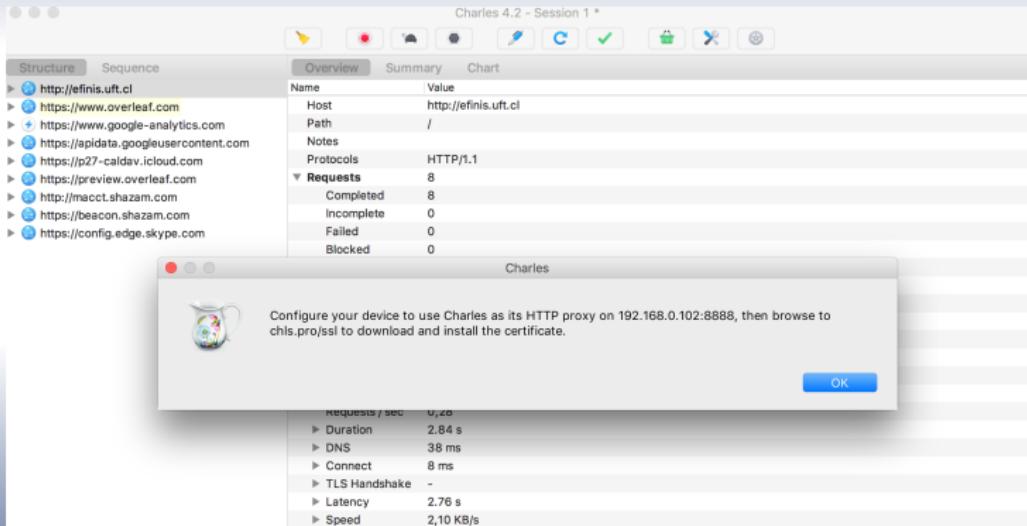
En el tercer Mitm se utilizo la aplicación Charles Proxy que es una aplicación tipo Wireshark pero que se puede implementar certificado SSL.

Donde se debió instalar un Perfil al iphone para poder controlar y manejar sus paquetes.



Man in the middle 3

Se puede visualizar que al empezar a hacer el enlace en el iPhone, esta pidiendo que se conecte por Proxy.



The screenshot shows the Charles 4.2 proxy tool interface. The main window displays a list of network requests under the 'Structure' tab. The requests listed include:

- http://efinis.uff.cl
- https://www.overleaf.com
- https://www.google-analytics.com
- https://apidata.googleusercontent.com
- https://p27-caldav.icloud.com
- https://preview.overleaf.com
- http://macct.shazam.com
- https://beacon.shazam.com
- https://config.edge.skype.com

The 'Overview' tab is selected, showing summary statistics:

Name	Value
Host	http://efinis.uff.cl
Path	/
Notes	
Protocols	HTTP/1.1
Requests	8
Completed	8
Incomplete	0
Failed	0
Blocked	0

A modal dialog box titled 'Charles' is displayed, instructing the user to configure their device to use Charles as its HTTP proxy on 192.168.0.102:8888, then browse to chls.pro/ssl to download and install the certificate. The 'OK' button is at the bottom right of the dialog.

At the bottom of the Charles window, performance metrics are shown:

Request/sec	0,28
Duration	2.84 s
DNS	38 ms
Connect	8 ms
TLS Handshake	-
Latency	2.76 s
Speed	2,10 KB/s

Man in the middle 3

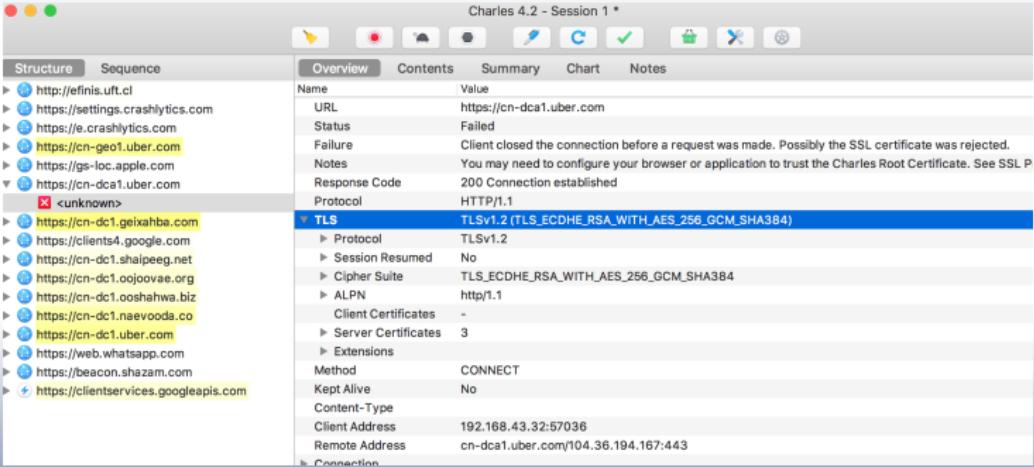
Una vez realizado todas las actividades, se empieza a capturar los paquetes del iphone de la aplicación Uber, donde se podrá ver las transferencia de datos.

- ▶ <https://settings.crashlytics.com>
 - ▶ <https://cn-geo1.uber.com>
 - ▶ <https://cn-dca1.uber.com>
 - ▶ <https://cn-dc1.geixahba.com>
 - ▶ <https://cn-dc1.shapieeg.net>
 - ▶ <https://clients4.google.com>
 - ▶ <https://cn-dc1.oojoovae.org>
 - ▶ <https://cn-dc1.ooshahwa.biz>
 - ▶ <https://cn-dc1.naevooda.co>
 - ▶ <https://cn-dc1.uber.com>

▼  <https://cn-geo1.uber.com>

Man in the middle 3

Finalmente en el resultado obtenido, se puede ver que tiene los datos encriptados.



The screenshot shows the Charles 4.2 interface with the 'Session 1' tab selected. In the left sidebar, there's a list of requests. One request to <https://cn-dca1.uber.com> is highlighted. On the right, the 'Overview' tab is active, displaying detailed information about this request. The 'TLS' section is expanded, showing the protocol used is **TLSv1.2 (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)**. Other details include the cipher suite **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**, ALPN as **http/1.1**, and three server certificates. The method is **CONNECT** and the content type is **Kept Alive**.

Name	Value
URL	https://cn-dca1.uber.com
Status	Failed
Failure	Client closed the connection before a request was made. Possibly the SSL certificate was rejected.
Notes	You may need to configure your browser or application to trust the Charles Root Certificate. See SSL P
Response Code	200 Connection established
Protocol	HTTP/1.1

TLS	
Protocol	TLSv1.2
Session Resumed	No
Cipher Suite	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ALPN	http/1.1
Client Certificates	-
Server Certificates	3
Extensions	

Method	CONNECT
Kept Alive	No
Content-Type	
Client Address	192.168.43.32:57036
Remote Address	cn-dca1.uber.com[104.36.194.167]:443

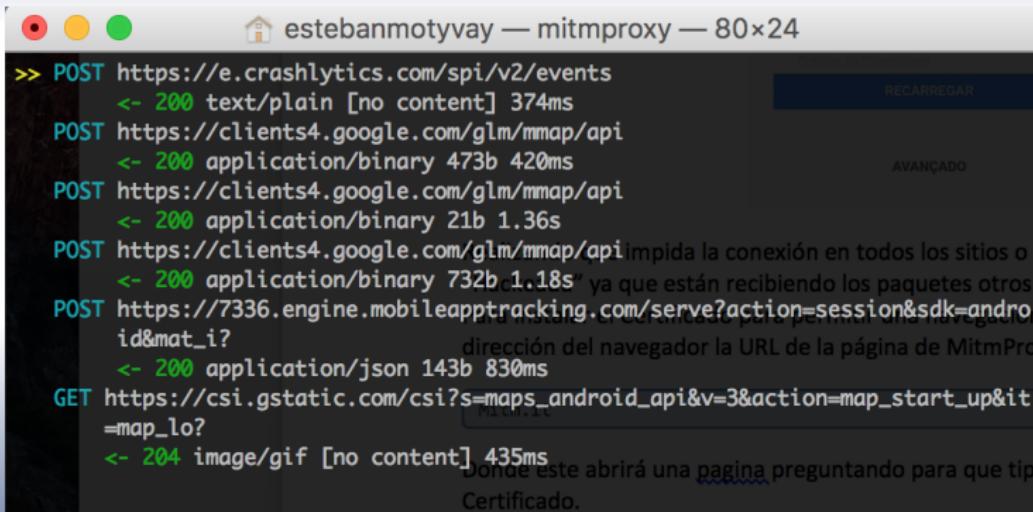


Man in the middle 4



Man in the middle 4

En el cuarto mitm se volvió a utilizar mitmproxy, pero ahora en este caso se utilizo un dispositivo android con los certificados, generando que en esta actividad se recibieran mas paquetes que los que llegaron anteriormente.



The screenshot shows the mitmproxy browser interface. At the top, there are three circular status indicators (red, yellow, green) followed by the title "estebanmotyvay — mitmproxy — 80x24". Below the title, the main area displays a list of network requests:

- >> POST https://e.crashlytics.com/spl/v2/events
 <- 200 text/plain [no content] 374ms
- POST https://clients4.google.com/glm/mmap/api
 <- 200 application/binary 473b 420ms
- POST https://clients4.google.com/glm/mmap/api
 <- 200 application/binary 21b 1.36s
- POST https://clients4.google.com/glm/mmap/api impida la conexión en todos los sitios o
 <- 200 application/binary 732b 1.18s" ya que están recibiendo los paquetes otros
- POST https://7336.engine.mobileapptracking.com/serve?action=session&sdk=andro
 id&mat_i? dirección del navegador la URL de la página de MitmPro
 <- 200 application/json 143b 830ms
- GET https://csi.gstatic.com/csi?s=maps_android_api&v=3&action=map_start_up&it
 =map_lo?
 <- 204 image/gif [no content] 435ms

A tooltip at the bottom right of the interface reads: "Dónde este abrirá una página preguntando para que tipo de Certificado."

Man in the middle 4

Los datos obtenidos que no se encontraban encriptados eran los que se encuentran en este punto.

Request

Response

Detail

Content-Type:

application/json

Date:

Tue, 29 Nov 2017 00:47:09 GMT

Server:

nginx

Vary:

Accept-Encoding: 2-CV...ay.doe

X-Log-ID:

11d663bf085ba3fb82f0224cc770c05-20171129-7336

X-Mat-Responder:

p-pacmon02-1b.use01

X-Powered-By:

MakaMakaMaka

Content-Length:

143

Connection:

keep-alive

[decoded gzip] JSON

Captura de pantalla - 05.28

{

```
"log_id": "11d663bf085ba3fb82f0224cc770c05-20171129-7336",
"site_event_type": "open",
"success": true,
"tracking_id": "21268f90dc32ffa93282f473c76648b2"
```

}

[5/6]

Captura de pantalla - 05.21 [*:8080]

Conclusión

En conclusión general del proyecto que se llevo a cabo, realizando distintas pruebas para encontrar alguna vulnerabilidad, pero Uber al ser una empresa tan grande, esta conlleva a que esta sea muy segura, por ende lo que se trato de comprobar era la seguridad de uber protegiendo sus datos. Uber al estar en constante auditoría de seguridad por empresas, esta cada día trata de que sea mas segura. Y con el desarrollo que se trato de hacer no se logro encontrar ninguna vulnerabilidad.