



UNIVERSIDAD FINIS TERRAE  
FACULTAD DE INGENIERÍA  
ESCUELA DE INGENIERÍA CIVIL

---

# Proyecto Seguridad informatica Auditoria aplicacion Uber

---

*Nombre:*  
Esteban Motyvay  
*Curso:*  
Seguridad Informatica

*Profesor:*  
Maximiliano Vega  
*Fecha entrega:*  
26/10/2017

## 1. Introducción

Desde los inicios de la red de la computacion, se quiso realizar un monitoreo de los paquetes que se envian dentro de una red, siendo una funcion de los Administradores de red de alguna empresa o establecimiento, para poder analizar los paquetes, donde puedan existir tipos de vulnerabilidades dentro de la red de la empresa. Se empezo a implementar seguridad en algunas empresas, para poder detectar y mitigar vulnerabilidades. Con el tiempo empezaron a aparecer empresas para prestar servicios de consultorias de seguridad. Pero lo que no se ha podido lograr a lo largo de la historia es poder mitigar completamente la vulnerabilidad de las redes, debido a que siempre existira un riesgo residual que se debera hacer cargo uno.

¿Que es el riesgo residual?

El riesgo residual se refiere al riesgo remanente luego de realizar un plan de seguridad que disminuyo el riesgo total de un proyecto o sistema. Este riesgo se apalanca mediante la aceptación del mismo o con terceros que asuman este riesgo, generalmente como un seguro. (Ejemplo: Entidades generadoras de certificados SSL).

En el presente proyecto se realizara una auditoria de una aplicacion mobile, donde se debera realizar una investigacion de sus tipos de vulnerabilidades que se encuentran dentro de sus codigos, para luego realizar ataques eticos para ver que tan vulnerables es esta.

Luego de haber documentado esta auditoria a la aplicación, se deberá reportar estos riesgos a la empresa que se le realizo la auditoria. Para que esta entidad pueda mitigar estos problemas de encontrados

## 2. Aplicacion escogida

La aplicacion escogida, es Uber, una de las empresas de transporte mas importante a nivel mundial. Esta empresa se origino en el año 2009 dos amigos Travis Kalanik y Garret M. Camp. Esta empresa cuenta con 6700 empleados, el rubro de esta empresa es el transporte privado.

### Historia

Garret M. Camp, canadiense licenciado en ingeniería, se encontraba en La Ciudad de la Luz junto un amigo lejano, el californiano Travis Kalanik, para asistir a LeWeb, un congreso sobre los negocios del futuro y la innovación. Paradojas del destino, y esperando un taxi que no paraba o nunca llegaba, fue que a las puertas de este evento, unas cuantas maletas, mucha lluvia, y quizá, un poco de mal humor, a este par de amigos se les ocurrió la idea de uno de los negocios más revolucionarios de los últimos años. ¿Qué pasaría si con mi móvil pudiese llamar a un coche para que estuviese en el lugar adecuado en el momento adecuado? Con esta sencilla idea comenzó la verdadera tormenta en las cabezas de estos personajes.



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

Así, ayudan a que las ciudades sean más accesibles, al ofrecer más opciones para los usuarios y más oportunidades de generación de ingresos para socios conductores.

### **3. Objetivos**

#### **3.1. Objetivo general**

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

#### **3.2. Objetivos específicos**

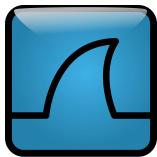
1. Estudiar la aplicación escogida
2. Buscar puntos de vulnerabilidad
3. Estudiar métodos de ataques

## 4. Marco Teórico

A continuación se detallan una serie de términos técnicos necesarios para el total entendimiento del presente proyecto:

### 4.1. Wireshark

Es una herramienta multiplataforma con interfaz grafica para el analisis de red, producto de la evolucion de Ethereal. Incluye la herramienta Tshark en modo consola para capturas, analisis de red, entre otras posibilidades. Este permite ver, aun nivel bajo y detallado, consultar todo lo que esta ocurriendo en la red. Es open source y multiplataforma. Se utiliza a menudo como mejor opcion al momento de auditar redes usualmente redes Ethernet y es compatible con algunas otras. es un analizador de protocolos de red. Permite capturar paquetes de datos desde una red en vivo, o leer los paquetes desde un archivo de captura previamente guardado, o imprimir un formulario descifrado los paquetes o escribir los paquetes en un archivo.



### 4.2. GitHub

Es una plataforma de desarrollo colaborativo para alojar proyectos utilizando el sistema de control de versiones Git. Utilizando el framework Ruby on rails por GitHub. El codigo se almacena de forma publica, aunque existe la opcion de almacenarlo de forma privada, pero para esto se debe crear una cuenta de pago.



### 4.3. Git

Es un software de control de versiones que fue diseñado por Linus Torvalds, pensando en la eficiencia y la confiabilidad del mantenimiento de versiones de aplicaciones cuando estas tienen un gran numero de archivos de código fuente. Git es utilizado para realizar respaldos de copia de seguridad de las versiones de las aplicaciones, para no dañar el código fuente o por si se daña o se borra, se puede realizar una recuperación del repositorio de Git.



### 4.4. MobSF

Mobile Security Framework es un marco automatizado de pen-testing capaz de realizar análisis estáticos y dinámicos, todo en uno, de aplicación móvil abierta (Android / iOS). Hemos estado dependiendo de múltiples herramientas para llevar a cabo la inversión, la decodificación, la depuración, la revisión de código y la prueba de pluma y este proceso requiere mucho esfuerzo y tiempo. Mobile Security Framework puede utilizarse para un análisis de seguridad eficaz y rápido de las aplicaciones de Android e iOS. Soporta binarios (APK - IPA) y código fuente comprimido.



### 4.5. Apktool

Una herramienta para la ingeniería inversa de terceros, cerrado, aplicaciones binarias de Android. Puede descifrar los recursos de forma casi original y reconstruirlos después de hacer algunas modificaciones. También facilita el trabajo con una aplicación debido al proyecto como la estructura de archivos y la automatización de algunas tareas repetitivas como la construcción de apk, etc.



#### 4.6. Charles

Charles Web Debugging Proxy es una aplicación de servidor proxy de depuración HTTP multiplataforma escrita en Java . Charles Proxy permite al usuario ver HTTP y HTTPS y el tráfico de puerto TCP habilitado al que se accede desde, hacia o a través de la computadora local. Esto incluye solicitudes y respuestas que incluyen encabezados HTTP y metadatos (por ejemplo, cookies, almacenamiento en caché y codificación de información) con funciones dirigidas a ayudar a los desarrolladores a analizar conexiones y mensajes.



## 5. Licencias Aplicación

### Acknowledgements

This application makes use of the following third party libraries:

#### Box

Copyright (c) 2014 Rob Rix

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

#### Braintree

Copyright (c) 2014-2016 Braintree, a division of PayPal, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(a) Licencia 1

(b) Licencia 2

(c) Licencia 3

#### CardIO

Copyright (c) 2013-2016 PayPal Holdings, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

#### Crashlytics

Fabric: Copyright 2015 Twitter, Inc. All Rights Reserved. Use of this software is subject to the terms and conditions of the Fabric Software and Services Agreement located at <https://fabric.io/terms>. Crashlytics Kit: Copyright 2015 Crashlytics, Inc. All Rights Reserved. Use of this software is subject to the terms and conditions of the Crashlytics Terms of Service located at <http://try.crashlytics.com/terms/terms-of-service.pdf> and the Crashlytics Privacy Policy located at <http://try.crashlytics.com/terms/privacy-policy.pdf>. OSS: <http://get.fabric.io/termsopensource.txt>

#### DeviceUtil

Copyright (c) 2013 Inder Kumar Rathore

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

#### DeviceUtil

Copyright (c) 2013 Inder Kumar Rathore

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software; and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

#### Fabric

Fabric: Copyright 2015 Twitter, Inc. All Rights Reserved. Use of this software is subject to the terms and conditions of the Fabric Software and Services Agreement located at <https://fabric.io/terms>. OSS: <http://get.fabric.io/termsopensource.txt>

#### FormatterKit

Copyright (c) 2011 Matt Thompson (<http://mattt.me/>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### Freddy

Copyright (c) 2015 Big Nerd Ranch Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### JWT

Copyright (c) 2013 Karma Mobility, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(a) Licencia 4

### KScrash

Copyright (c) 2012 Karl Stenerud

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in the documentation of any redistributions of the template files themselves (but not in projects built using the templates).

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### LipPhoneNumber

Copyright (c) 2011 The LipPhoneNumber Authors

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

### Lottie

Copyright (c) 2017 Airbnb, Inc.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

(b) Licencia 5

### Lottie

Copyright (c) 2017 Airbnb, Inc.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This project uses portions of code from the Proton framework. Proton is copyright (c) 2012, Bitsift, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
  - Neither the name of the Bitsift, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
- THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

(c) Licencia 6

This project uses portions of code from the Proton framework. Proton is copyright (c) 2012, Bitsift, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Neither the name of the Bitsift, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### Masonry

Copyright (c) 2011-2012 Masonry Team - <https://github.com/Masonry>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT

HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,

WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER

DEALINGS IN THE SOFTWARE.

(a) Licencia 7

### ObjectiveLevelDB

Copyright (c) 2011 Pave Labs

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### PayPal

The PayPalMobile header files and the PayPal iOS SDK Sample App are released under the BSD License.

Copyright (c) 2014-2016 PayPal Holdings, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(b) Licencia 8

### RxBlocking

Copyright © 2015 Krzysztof Zaker All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### RxCocos

Copyright © 2015 Krzysztof Zaker All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(c) Licencia 9

### RxOptional

Copyright (c) 2016 Thane Gill [me@thangill.com](mailto:me@thangill.com)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### RxSwift

Copyright © 2015 Krunoslav Zaher All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(a) Licencia 10

### SnapKit

Copyright (c) 2011 Present SnapKit Team. <https://github.com/SnapKit>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### States-v3

Copyright (c) 2010 Andy Matuschek

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(b) Licencia 11

### Swift YouTube Player

Copyright (C) 2015 Giles Van Grissem.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

### Tune

Copyright (c) 2015 TUNE

Licensed under the Apache License, Version 2.0 (the "License"); you may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

### Thrift

Copyright (c) 2004 Apache Thrift

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

(c) Licencia 12

### leveldb-library

Copyright (c) 2011 The LevelDB Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### Google Maps SDK for iOS

\*This software is based in part on Google Toolbox For Mac:

Copyright © 2006-2013 Google Inc.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This software is based in part on iGLU (http://www.opengl.org/documentation/specs/), an implementation of the OpenGL Utility Library (GLU) (http://www.opengl.org/documentation/specs/). iGLU is based on the GLU source included with Mesa 7.2 (http://mesa3d.sourceforge.net), which in turn derives from the SGI OpenGL Sample Implementations (http://oss.sgi.com/projects/ogl-sample). All code derived from SGI's source is licensed under the SGI Free Software License B version 2.0 (http://oss.sgi.com/projects/FreeB). All other code is licensed under the MIT license (http://www.opensource.org/licenses/mit-license.php).

### XMLDictionary version 1.4, April 16th, 2014

Copyright (C) 2011 Chareud Design

This software is provided "as-is", without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The software may be redistributed in source or binary form, you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

(a) Licencia 13

(b) Licencia 14

## 6. Plan de acción

Que es un plan de acción?

Un plan de acción es una herramienta de planificación de gestión y control de tareas en un proyecto. Este se basa en objetivos planteados que van a ir de manera incremental por cada entrega que se realiza. El plan de acción sirve para coordinar y comprender En el presente trabajo el plan de acción a seguir van a ser variados métodos de acción a realizar, donde a la aplicación se le realizara:

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

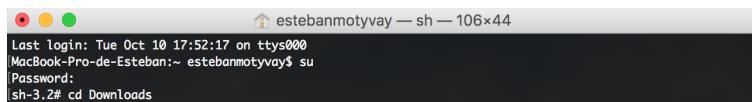
## 7. Desarrollo

### 7.1. Descompilacion

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

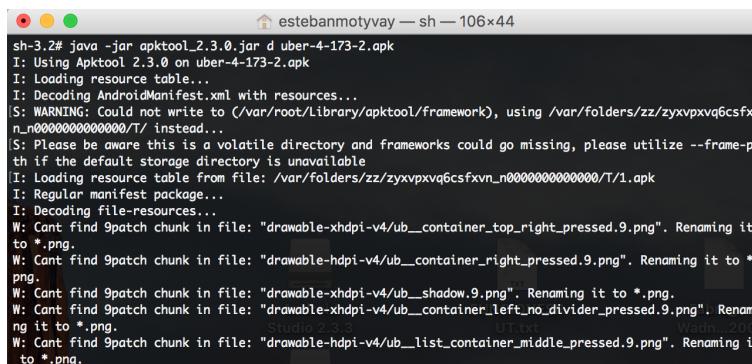
1. Java SDK y JRE
2. Android SDK
3. Apktool
4. uber.apk

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
```

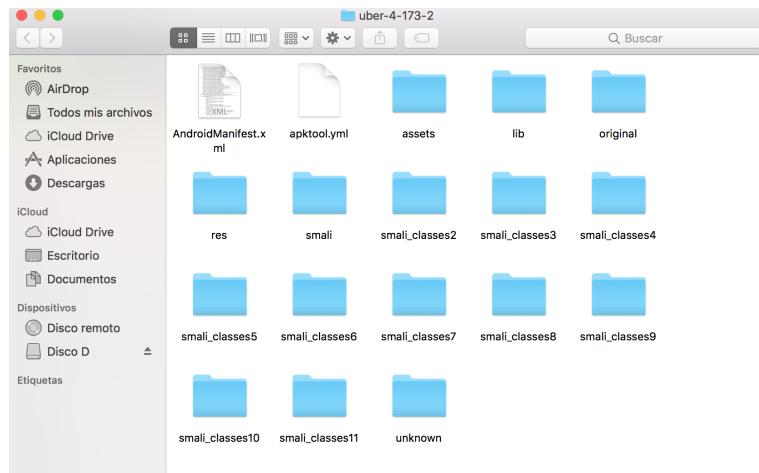
Luego de haber ejecutado el super usuario, se ejecuta la aplicacion Apktool.jar, este se busca por terminal y este se encuentra en descarga. Para poder ejecutarlo se ingresa el comando java -jar d nombredelaapk.apk. La d del comando significa descompilar.



```
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: Can't find 9patch chunk in file: "drawable-xhdpi-v4/ub__container_top_right_pressed.9.png". Renaming it to *.png.
W: Can't find 9patch chunk in file: "drawable-hdpi-v4/ub__container_right_pressed.9.png". Renaming it to *.png.
W: Can't find 9patch chunk in file: "drawable-xhdpi-v4/ub__shadow.9.png". Renaming it to *.png.
W: Can't find 9patch chunk in file: "drawable-xhdpi-v4/ub__container_left_no_divider_pressed.9.png". Renami...
W: Can't find 9patch chunk in file: "drawable-hdpi-v4/ub__list_container_middle_pressed.9.png". Renaming it to *.png.
```

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

Analizado los códigos java y el archivo XLM que fueron generados al realizar ingeniería inversa al Apk, no fue posible detectar a simple vista ciertas fallas. Se requirió ayuda de ciertas aplicaciones de análisis de códigos para detectar vulnerabilidades, detectando que las únicas vulnerabilidades que contenía la aplicación, es mediante los



permisos que se requieren para instalar la aplicacion, como por ejemplo: Activar camara  
Permitir Ubicacion Actual Permitir escribir en SD etc.

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

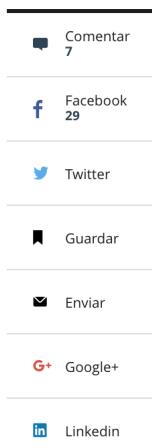
```
<!-- Signature Algorithms -->
<Algorithm URI="http://www.w3.org/2000/09/xmldsig#dsa-sha1"
           Description="Digital Signature Algorithm with SHA-1 message digest"
           AlgorithmClass="Signature"
           RequirementLevel="REQUIRED"
           JCEName="SHA1withDSA"/>
```

Uber al ser una aplicación tan grande y encontrarse ubicada en muchos países, esta cuenta con un nivel de seguridad muy alta en sus app y web. Como anteriormente Uber contó con unas vulnerabilidad, esta fue obligada por la comisión federal de comercio a tener una Auditoria de Seguridad permanente por 20 años.

Por ende, en este proyecto, no se basara en encontrar la vulnerabilidad y tratar de reventar esa vulnerabilidad, lo que se realizara sera tratar de realizar muchos métodos de ataque, y decir que tan segura es esta aplicación y porque.

# Uber será auditada durante 20 años por violar privacidad de usuarios

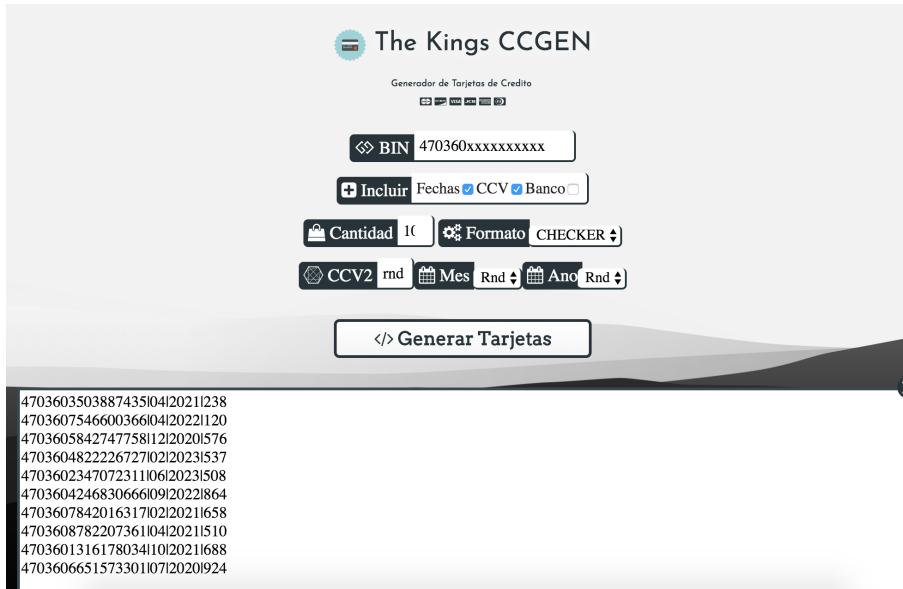
La compañía fue acusada de utilizar un software para monitorear desplazamientos.



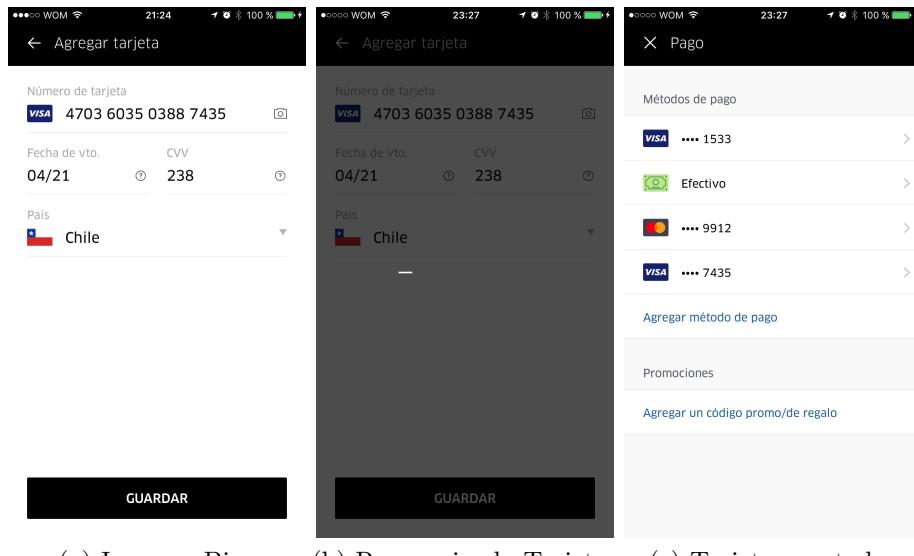
## 8. Pruebas

### 8.1. Bin Falso

Para iniciar las pruebas, se sabe que Uber su método de pago es en base a pago con tarjetas y efectivo, con un porcentaje de 60% y un 40% en efectivo. Por ende, se desea realizar un ingreso de Bin falso, de manera que este pase el sistema de verificación de Bin. Para esto se realizó una investigación sobre el funcionamiento de los Bin y mediante Internet, encontrar cuáles eran los bin falsos que se encontraban en funcionamiento. Que quiere decir que se encuentran en funcionamiento, con el tiempo la gente va investigando sobre las tarjetas de cada país, región, local, etc. Se busca los primeros 6 números de la tarjeta que encuentra accesible, esto funciona de manera que los primeros 4 dígitos de la tarjeta indican el banco, luego de que ya se sabe el banco, se empieza a trabajar en base a ese banco. Se encuentra luego el código de la sucursal que son los siguientes 4 dígitos, pero en este caso se utilizó los primeros 6 dígitos. ¿Por qué? Debido a que se escoge el banco si o si, luego los primeros dos dígitos asigna el rango de las sucursales, dando la posibilidad de encontrar alguna sucursal dentro de 99 posibilidades ya que son los siguientes 2 números que faltan. El resto de los dígitos, se le asigna al programa que los genere mediante números random pero cumpliendo algunos parámetros. Donde los 2 números siguientes vienen siendo los dígitos de control y los últimos 6 dígitos es el número de cuenta. Por ende los últimos 10 dígitos se dejan libre para que el generador se dedique a asignar la sucursal, los dígitos de control y el número de cuenta.



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



Se puede apreciar en las imágenes, que el bin de la tarjeta fue aceptado, por ende se puede realizar un viaje. Lo mas probable que pueda pasar por lo investigado, que se realizara el viaje de manera gratis, para cuando llegue el momento de que Uber realizara el cargo a la tarjeta, este no podrá, se puede dar el caso de que Uber detecte en ese momento que la tarjeta es falsa y bloquee la cuenta, que es lo que le ha pasado a algunos usuarios que han realizado este método y por otro lado se puede dar el caso que queda el pago pendiente el cuenta, hasta realizar un nuevo viaje con otro método de pago o se cargara el pago cuando se registre otra tarjeta.

### 8.1.1. Conclusión

Para concluir esta actividad, al realizar todos los puntos necesarios, se logro llevar a cabo el punto de ingresar un Bin falso, esto quiere decir que ya paso el nivel de vulnerabilidad al ingresar una tarjeta falsa, luego viene el punto de realizar el pedido de un vehículo, para esto, se asigno la tarjeta falsa, luego de esto al realizar el viaje, este no realizo el pago, pero quedo pendiente, luego al querer realizar otro viaje, este daba una alerta de que se debe pagar el viaje anterior con alguna tarjeta o método de pago, para luego realizar el siguiente viaje.

## 8.2. Ubicación Actual

En esta actividad, se desea realizar un cambio en la ubicación de Uber Drive. En que consiste Uber drive, es la aplicación de los chóferes de Uber donde este les muestra un Mapa de donde se encuentran los lugares donde existe la tarifa dinámica, esto quiere decir que en esos lugares donde esta la tarifa dinámica, el valor del viaje se multiplicara por lo indicado por Uber, esto depende de la cantidad de vehículos que anden trabajando y la cantidad de personas que solicitan el vehículo, cuando la demanda es alta, y los vehículos no alcanzan a cubrir todas las necesidades, se realiza la tarifa dinámica. Entonces que se desea realizar en esta actividad, es modificar la ubicación del teléfono de manera que yo no me encuentre en el lugar que debo estar, sino que asigno que mi ubicación se encuentra en el lugar de tarifa dinámica para poder aceptar viajes con un valor mas alto y tener un mayor ingreso a la cuenta. Por ende se instala Cydia.

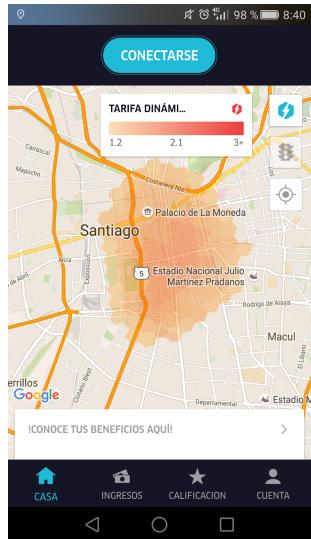


Cydia es una aplicación para iOS, que permite proveer software y demás modificaciones que no están disponibles en la App Store para los usuarios de jailbreak. Funciona a través de repositorios (repos) que son agregados por el propio usuario. Estos ficheros tienen extensión .deb, y pueden ser instalados descargándose de su respectivo sitio web (desde el dispositivo) o copiándolos a la carpeta de Cydia.

Luego se instala Fake GPS, que lo que realiza esta aplicación es asignar como ubicación actual, la ubicación que uno le indique que desea estar, siendo esa tu nueva ubicación actual.



Una vez que se instala Fake GPS, se abre Uber Drive para buscar el lugar que se encuentra con mayor flujo de gente y tarifa dinámica.



Luego de un tiempo, uber instalo un sistema que no se podía abrir la aplicación si es que este detectaba que el dispositivo fue adulterado por Cydia. Uber se volvió una de las aplicaciones mas seguras que existe en el mercado, generando una aplicación casi invulnerable debido a que esta instalo sistema de protección contra equipos adulterados, como por ejemplo en iPhone el sistema Cydia y en el caso de Android el sistema de Rootear el equipo.

### 8.2.1. Conclusión

Para concluir esta actividad, lo que se logro llevar a cabo logro ser realizado en el dispositivo, pero esto no puede ser llevado a cabo en un dispositivo normal, este tiene que tener Root o Jailbreak dependiendo el dispositivo, luego de esto se debe ingresar un Bypass, debido a que Uber utiliza un sistema de seguridad avanzando en que no deja abrir la aplicación si es que el dispositivo se encuentra adulterado, por ende para aceptar viajes que se encuentren en zonas de tarifa dinámica es una muy buena función.

### 8.3. Análisis de puertos

Para esta actividad se realizara una investigación donde se debe analizar el archivo AndroidManifest.xml que este se obtiene cuando se realiza la descompilación de la aplicación. Una vez descompilada se abre el archivo AndroidManifest con un editor de texto. Al analizar, se encuentra la dirección hacia el servidor con la que ellos trabajan.

```
<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"/>
```

Se puede visualizar que la dirección de estos es m.Uber.com . Abrimos Terminal, donde acá se ejecutara NMAP que sera la aplicación con la cual se analizaran los puertos. Para esto se ingresa sudo nmap -O http://m.uber.com y este dará los puertos que se encuentran desbloqueados en el servidor

```
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
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
```

Este arroja que el servidor cuenta con 3 puertos abiertos, que estos son el puerto 21 - 80 - 443. Donde es de FTP - HTTP - HTTPS respectivamente, si estos puertos empezamos a analizar que tipo de ataques se pueden realizar, podemos ver que:

Puerto 21 - ftp:

- Buffer Overflow
- Denegacion de Servicio (DoS)
- Ataque de Fuerza Bruta
- Punto de Acceso

Puerto 80 http:

- Ataque CGI
- Buffer Overflow
- Denegación de Servicio (DoS)
- Recogida de Información
- Punto de Acceso
- Posibilidad de sniffer.

Adicionalmente al realizar el mapeo de Uber, se detecto que este dio 7 IP mas, esto quiere decir que debe haber un servidor Maestro y el resto son para repartir la carga de la cantidad de usuarios que existen.



### 8.3.1. Conclusión

Para concluir esta actividad, se encontro que esta la aplicacion tenia tales puertos abiertos y que se podian realizar los ataques mencionados anteriormente, pero la empresa lo mas probable que tenga los puertos modificados de manera que no sean los que aparecen ahí, debido a que el computador con el que se analiza detecta tal puerto abierto y asume que ese puerto es de http, pero puede ser que la empresa lo modifijo para que sea TCP o algun puerto distinto, por ende no sirve mucho averiguar los puertos si es que los tiene cambiados.

## 8.4. Man in the middle 1

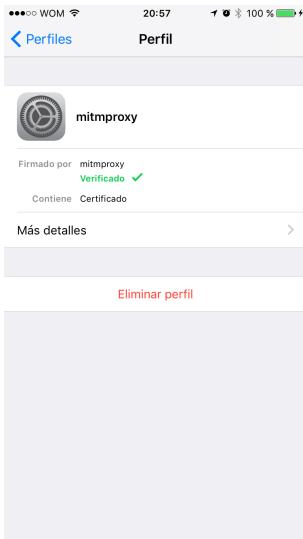
Para realizar esta actividad, se utiliza el programa Wireshark para analizar los paquetes que son enviado. Para esto se instala la aplicación mencionada anteriormente, luego al equipo que se le instala la aplicación, se le conecta un cable de Internet para que a través de la placa de wifi que este tiene, emita señal de Internet por wifi. Una vez realizado esto, de levantar la señal wifi del equipo, debemos conectarnos con el equipo que queremos analizar, en este caso sera con un iPhone. Conectándonos a la señal se comprueba de que el programa esta realmente funcionando con el equipo, e ingresamos a paginas anteriormente testeadas donde se detectaron vulnerabilidades para ver si este cumplía con el mismo resultado. Una vez comprobada que realmente cumple con los resultados, se empieza a realizar la tarea principal de tratar de analizar los paquetes de Uber.

| 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..   | 297.656037              | 192.168.0.106           | 172.217.30.14      | TLSv1.2  | 295    | Client Hello  |
| 1076..   | 297.658017              | 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                         |
| 1076..   | 297.806274              | 104.36.194.175          | 102.168.0.106      | TLSv1.2  | 117    | Change Cipher Spec                                  |
| ▶ 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: CompaqIn_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 0a 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 db 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 00 01 01 | 08 0a 6f be 3f 0f 29 5b | ..!7.... .o.?)[    |          |        |   |
| 0040   | 7a 15 ff f0 c8 4e d6    | 43 38 b0 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..Zs. ....2.8..  |          |        |   |

resultado del man in the middle realizado fue negativo, debido a que se encontró que los paquetes que eran enviados cuando se abría la aplicación, estos paquetes estaban totalmente encriptados.

## 8.5. Man In the middle 2

Para realizar esta actividad, se debe instalar la aplicación de mitmproxy, que sera nuestra aplicación para poder realizar una falsificación de certificado SSL. Luego de haber instalado la aplicación, se deberá realizar la instalación de un dsniff, para poder realizar un ataque de falsificación de la dirección ip y mac para que el equipo victimas se conecte. Una vez instalado empezaremos con la actividad. Se abre mitmproxy y se pasa el certificado de esta apps al iPhone



instalando este certificado en el teléfono, se deberá ingresar al terminal para trabajar con dsniff de manera de forzar la conexión de mi teléfono que pase por el computador con el cual se analizara los paquetes.

una vez forzada, se empieza a recibir los paquetes que son enviados del celular al respectivo servidor de cada aplicación que se está utilizando.

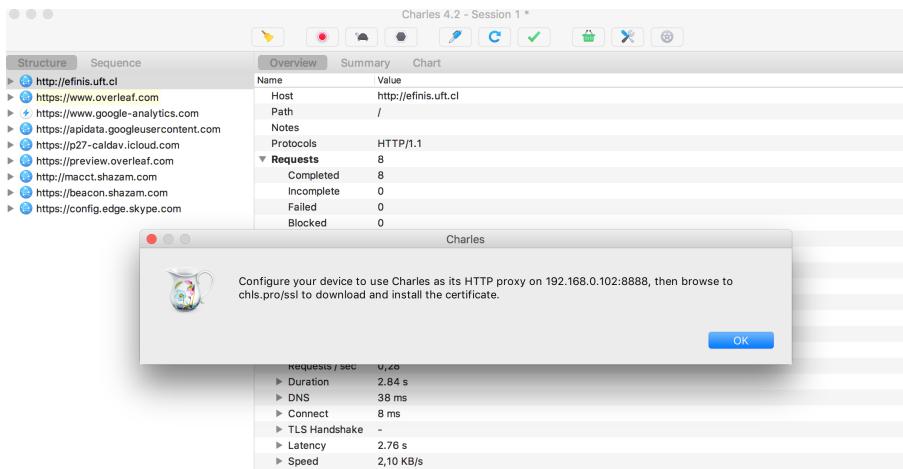
```
Archivo Editar Ver Buscar Terminal Ayuda
token...
  - application/octet-stream 512k 650ms
GET http://audio-ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
token...
  - 206 application/octet-stream 512k 745ms
GET http://audio-ak.spotify.com.edgesuite.net/audio/d4c95b795e5656b56803f00c11f6b34fa80280de?
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]
Warn: 192.168.0.100:65230: Client Handshake failed. The client may not trust the proxy's
certificate for mms.whatsapp.net.
?:help [*:8080]
```

## 8.6. Man in the middle 3

En la tercera actividad de man in the middle se realizó con el programa Charles Proxy, que es una aplicación como Wireshark, pero que se puede instalar por medio de la conexión que se realiza un certificado SSL al teléfono celular. Para iniciar la actividad,



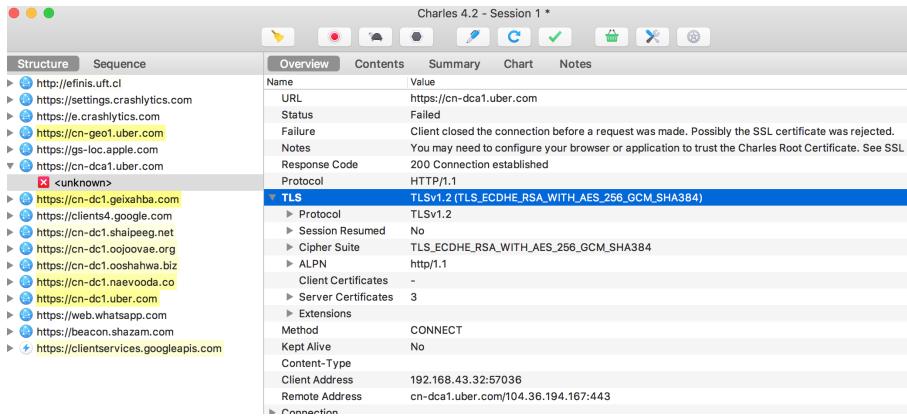
se programa el Proxy que te da la aplicación.



Luego de ingresar el proxy en el celular, este se conecta con la aplicación y se empiezan a recibir paquetes del teléfono.

Al empezar a revisar los paquetes, se puede visualizar que estos vienen protegidos y no permite la visualización del código que se ha enviado.

En conclusión a los 3 man in the middle que se realizaron, recopilando datos de todos los software, se encontró que Uber trabaja con SSL y TLS1.2 siendo una aplicación casi invulnerable a través de un MITM, también se encontró que este utiliza métodos de encriptación. No se logró realizar conexión al servidor, debido a que el servidor realizaba una verificación hacia el iphone para verificar el certificado que este utilizaba para la conexión, y este veía y comprobaba que el certificado no era el correcto, por ende bloqueaba la conexión hacia el servidor.



## 8.7. Man in the middle 4

Para realizar esta actividad, se decidió realizar la misma actividad anteriormente realizada de man in the middle con la aplicación MITMProxy, pero esta vez se utilizará un dispositivo android. Como anteriormente se menciono para iniciar la actividad, en este caso se utilizo un notebook Macbook, el cual se instaló por consola, en que varia en el anteriormente realizado, el anterior se realizó en un Notebook con Sistema operativo Kali Linux y el certificado se encontraba en una carpeta, en este caso, al configurar el Proxy en el celular, se ingreso a la pagina mitm.it donde se descarga el Certificado para el dispositivo que se desee, en este caso se descargo el de Android y luego se instaló.

Una vez realizado todo lo anterior, al haber ejecutado proximidad en consola, este se encuentra “escuchando” de manera que todos los paquetes que son enviados por el dispositivo, estos son interceptados por el notebook. Luego de eso se abre la aplicación a la cual se le está realizando la auditoria, obteniendo los siguientes paquetes.

```
estebanmotyvay — mitmproxy — 80x24
>> 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 impide 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&sd़=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 Dónde abrirá una página preguntando para qué tipo de Certificado.

[1/6] ?help [*:8080]
```

Luego de recibir los paquetes, se empiezan a revisar , con el fin de encontrar algún tipo de información que se encuentre en texto plano o códigos de ejecución que sean enviados.

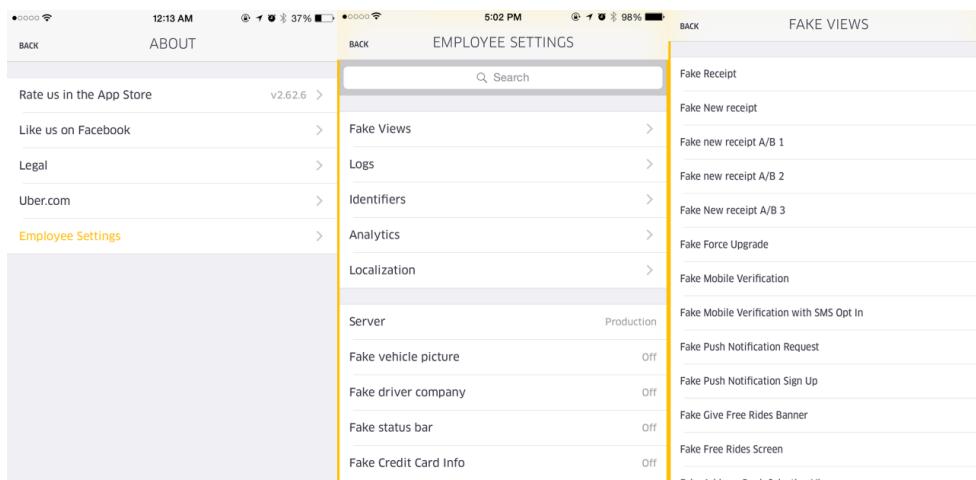
Al analizar los datos, se encontró que todos los datos que son enviados, estos están cifrados de manera que no puedan ser legibles, lo que se encontró que puede llamar la atención es que asigna números de usuario, que al poder ser modificados lo mas probable es que se puedan obtener los datos de otros usuarios.

### 8.7.1. Conclusión

Para concluir esta actividad, una vez realizado todos los puntos se logró llevar a cabo un avance más grande que los Man in the middle anteriores, debido a que en este se obtuvieron un poco más de datos, que pueden ser interpretados, pero habían demasiado que estaban encriptados, se encontró un solo post, que no se encontraba encriptado, que eran los números de usuario y de tracking.

## 8.8. Anexo - Man in the middle año 2015

En el año 2015 a Uber se le realizo un Man in the middle hacia su aplicación, para saber que era lo que esta enviaba al servidor y que era lo que enviaba como respuesta el servidor de Uber a la aplicacion. El Hacker que realizo esta actividad, con nombre Natham (un desarrollador de aplicacion) , pero logro encontrar partes de codigo que se enviaban donde el cambio una opcion que se encontraba en Booleano, donde pudo cambiar un False por un True y no causo mucha diferencia, pero ingresando a una parte del menu, se encontro un nuevo menu que accedia al menu de desarrollador.



Logrando que este desarrollador de aplicacion que estaba indagando en la aplicacion, noto que ahora tiene la herramienta de desarrollador de Uber, donde tiene acceso a todos los datos que se pueden modificar en la aplicacion.

## 9. Entregables

| Entregable       | Fecha      |
|------------------|------------|
| Entregable 1     | 27/09/2017 |
| Entregable 2     | 11/10/2017 |
| Entregable 3     | 25/10/2017 |
| Entregable 4     | 2/11/2017  |
| Entregable 5     | 15/11/2017 |
| Entregable Final | 29/11/2017 |

Cuadro 1: Tabla de entregables.