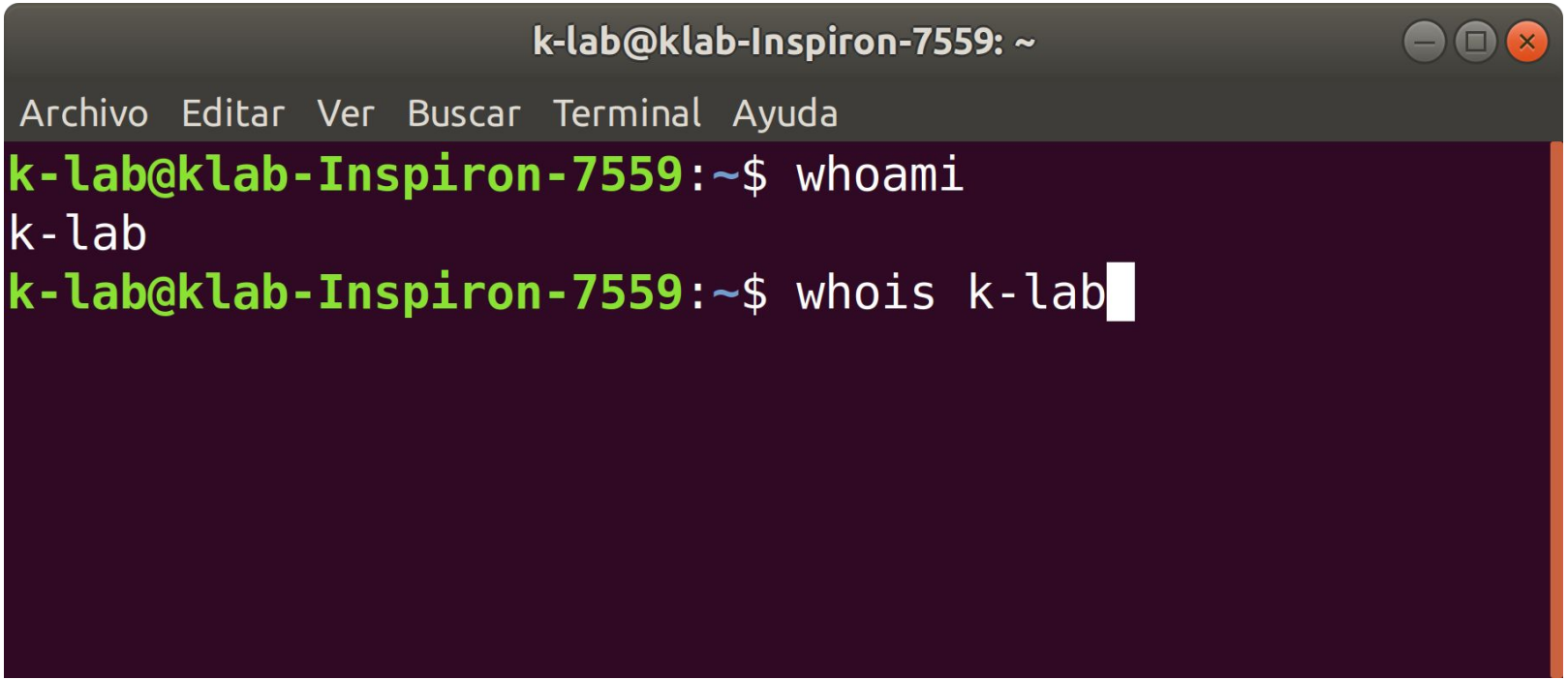
<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Fundación Karisma
Seguridad e intimidad

CoronApp, Medellín me Cuida y CaliValle Corona al laboratorio
¿Cómo se hackea CoronApp sin siquiera intentarlo?

Andres Velásquez
Stéphane Labarthe
FLISOL Bogotá 2020


k-lab@klab-Inspiron-7559: ~
Archivo Editar Ver Buscar Terminal Ayuda
k-lab@klab-Inspiron-7559:~$ whoami
k-lab
k-lab@klab-Inspiron-7559:~$ whois k-lab

“Nada es tan permanente como un programa temporal del gobierno”.

Milton Friedman, economista

K+LAB y los análisis de sitios / apps

Análisis confirma relación de Nation Builder, empresa que ayudó a Trump a llegar a la presidencia, con dos campañas presidenciales en Colombia.

CoronApp
Instituto Nacional de Salud

TODOS POR UN NUEVO PAÍS
PAZ EQUIDAD EDUCACIÓN

UNIDAD PARA LAS VÍCTIMAS

DIAN
Dirección de Impuestos y Aduanas Nacionales

Alcaldía Mayor de Bogotá D.C.
Tullave Plus

Metodología de análisis (sitios webs y apps)

Características:

- ✔ Análisis de la información y técnico
- ✔ Reproductibles: ¡Hagan lo ustedes también!
- ✔ Se usan softwares libres
- ✔ No intrusivo y legal + información previa
- ✔ Mirando: transparencia/información, seguridad digital , privacidad

¡Abramos la caja negra!

¿Porque usar Softwares libres en este contexto?

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

- Transparencia y confianza: código abierto
- Reproductibilidad: programas acesibles a todos sin costo
- Qualidad y eficiencia de las herramientas usadas

¿Que usamos?

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Exodus Privacy: Licencia pública GNU, versión 3.0
ClassyShark3xodus: Licencia Apache 2.0
Wireshark: Licencia pública GNU, versión 2.0
OWASP ZAP: Licencia Apache 2.0
Burp Comunity Edition
Apktool (Herramienta de ingeniería inversa para APKs)
diff (Para ver las diferencias entre las versiones después de ser des compiladas)
ADB (Android Debug)

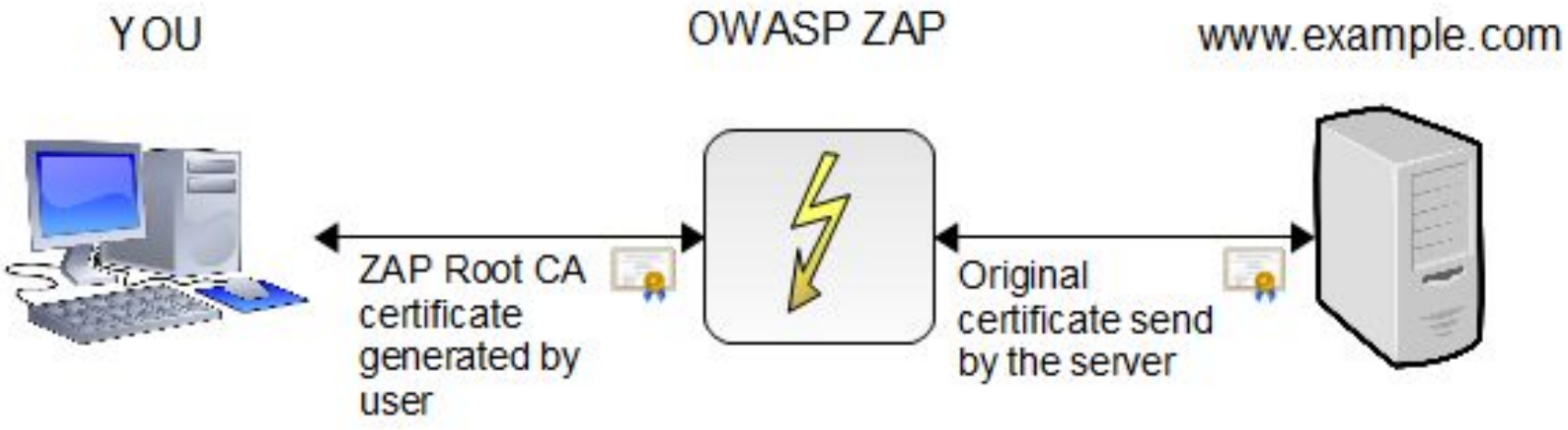
para sitios : **Waterfox + LiveHTTP Headers + CookieManager+**

Análisis estático (sitio web y app)

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Sitios webs	Apps
● dominio y dirección IP (whois) ● certificado ● código fuente (HTML / Javascript) ● cookies	● información del store ● permisos ● rastreadores ● manifiesto Android ● parte accesible del código fuente

Análisis de flujo/paquetes



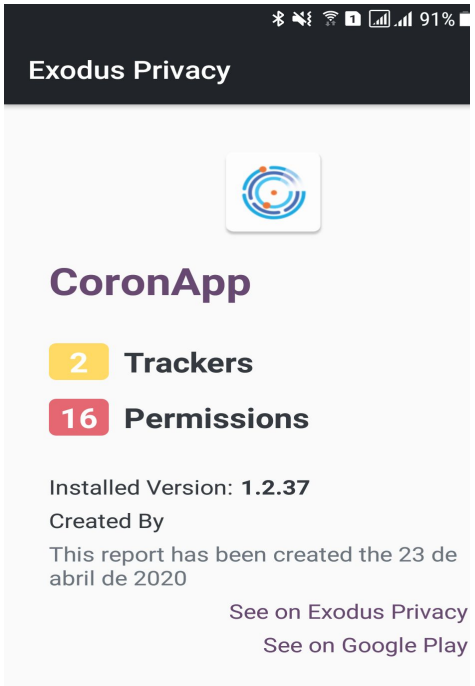
Capturing outbound/inbound packets:
Smartphone Apps : HTTPS, DNS
Website : also HTTPS (with LiveHTTP Headers)

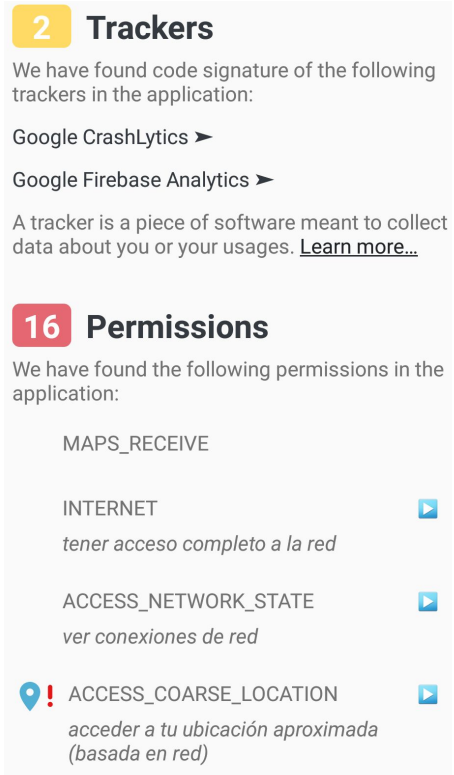
Permisos en las Apps (CaliValleCorona)

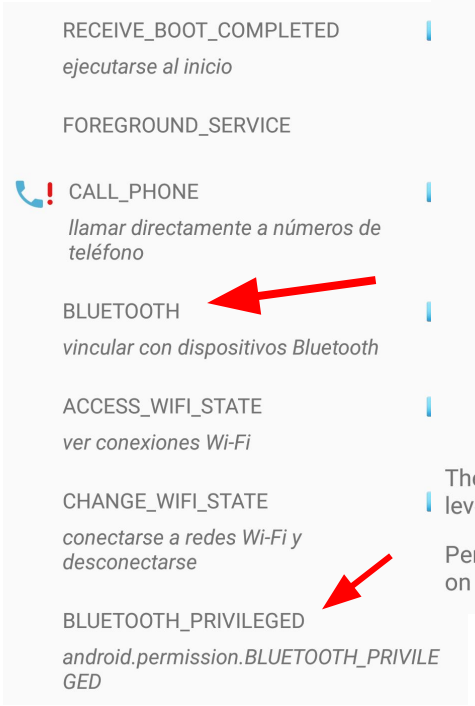
- App permissions: 35
  - com.huawei.permission.external_app_settings.USE_COMPONENT
  - me.everything.badger.permission.BADGE_COUNT_WRITE
  - android.permission.READ_APP_BADGE
  - com.oppo.launcher.permission.READ_SETTINGS
  - com.htc.launcher.permission.UPDATE_SHORTCUT
  - android.permission.READ_PHONE_STATE
  - oppo.permission.OPPO_COMPONENT_SAFE
  - com.sonyericsson.home.permission.BROADCAST_BADGE
  - android.permission.ACCESS_FINE_LOCATION
  - android.permission.GET_TASKS
  - android.permission.ACCESS_NETWORK_STATE
  - com.majeur.launcher.permission.UPDATE_BADGE
  - me.everything.badger.permission.BADGE_COUNT_READ
  - com.sonymobile.home.permission.PROVIDER_INSERT_BADGE
  - android.permission.WRITE_EXTERNAL_STORAGE
  - android.permission.FOREGROUND_SERVICE
  - android.permission.CALL_PHONE
  - android.permission.READ_EXTERNAL_STORAGE
  - com.htc.launcher.permission.READ_SETTINGS
  - com.huawei.android.launcher.permission.CHANGE_BADGE
  - android.permission.ACCESS_COARSE_LOCATION
  - com.sec.android.provider.badge.permission.READ
  - com.huawei.android.launcher.permission.READ_SETTINGS
  - com.google.android.gms.permission.ACTIVITY_RECOGNITION
  - android.permission.INTERNET
  - android.permission.ACCESS_LOCATION_EXTRA_COMMANDS
  - com.anddoes.launcher.permission.UPDATE_COUNT
  - com.sec.android.provider.badge.permission.WRITE
  - android.permission.RECEIVE_BOOT_COMPLETED
  - com.huawei.android.launcher.permission.WRITE_SETTINGS
  - android.permission.ACCESS_BACKGROUND_LOCATION
  - android.permission.ACTIVITY_RECOGNITION
  - android.permission.WAKE_LOCK
  - com.oppo.launcher.permission.WRITE_SETTINGS
  - android.permission.BLUETOOTH

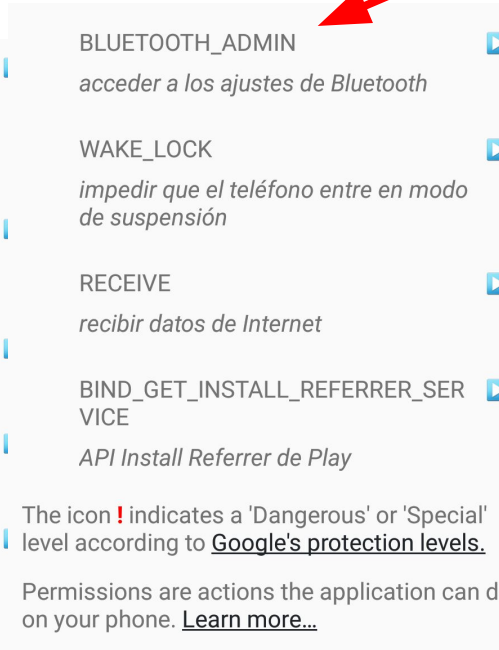
Permisos/tackers CoronApp (Exodus)

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD





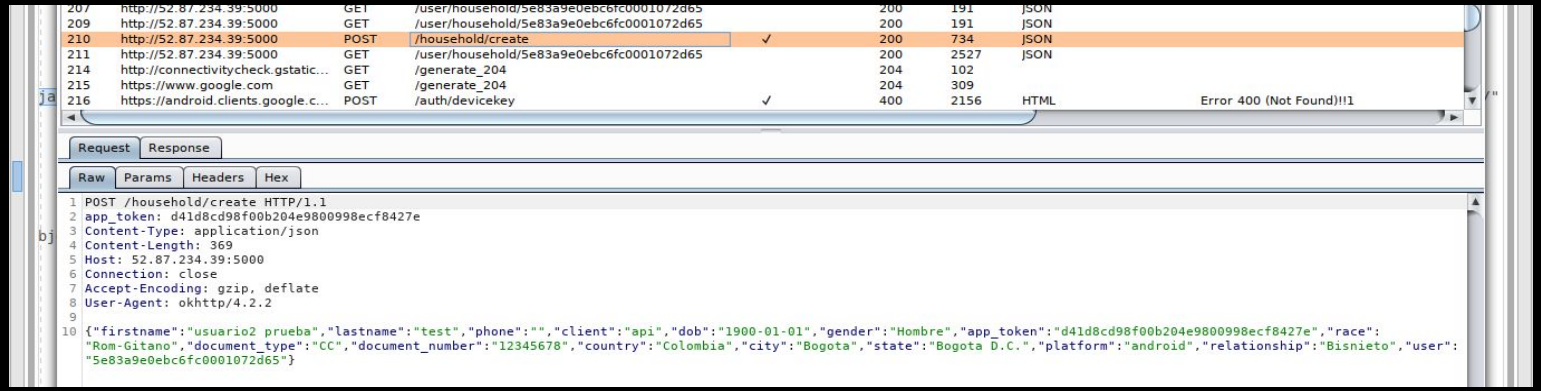




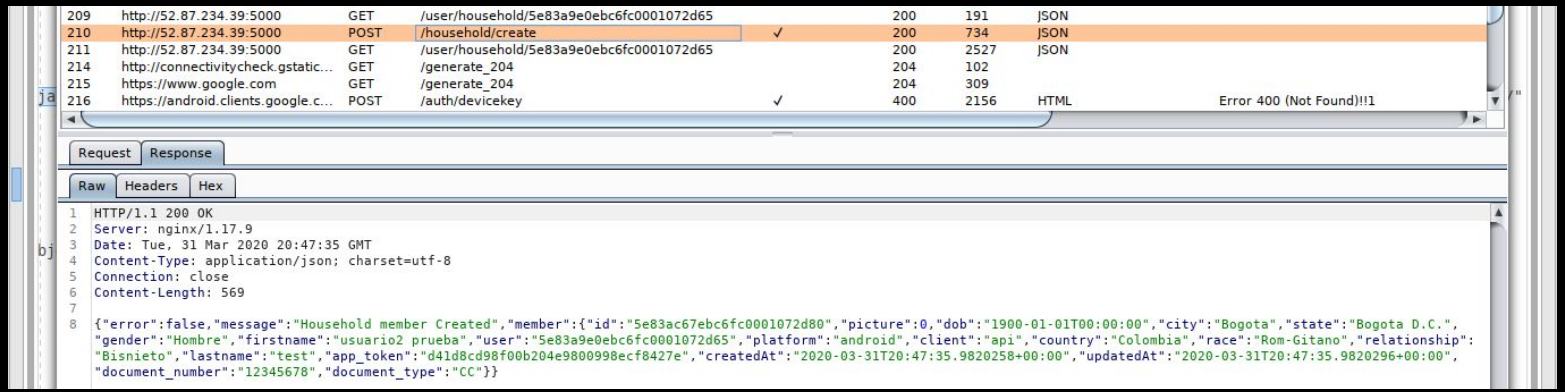
K

Análisis de tráfico en Coronapp - encontrando una vulnerabilidad 1.

request



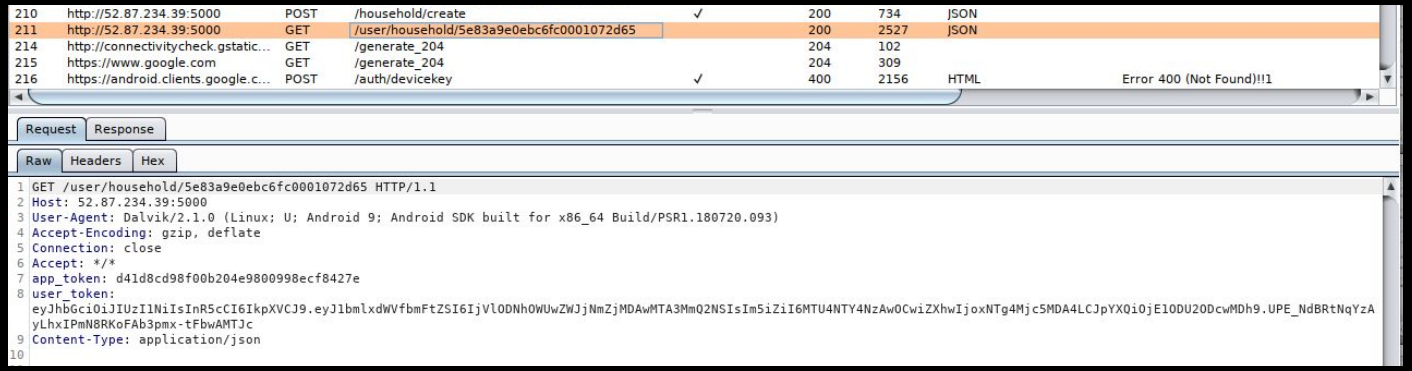
response

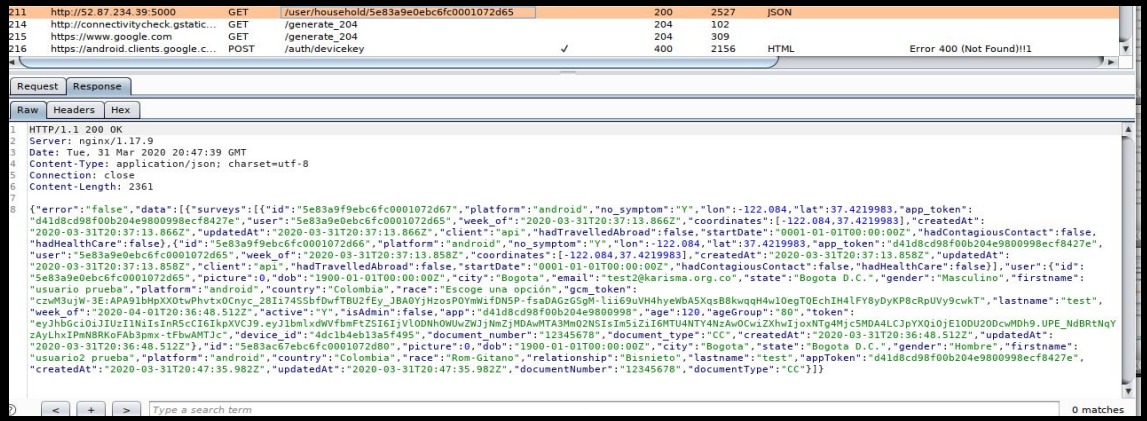


Análisis de tráfico en Coronapp - encontrando una vulnerabilidad. 2.

request

response





Vulnerabilidad Medellin <-> EPM

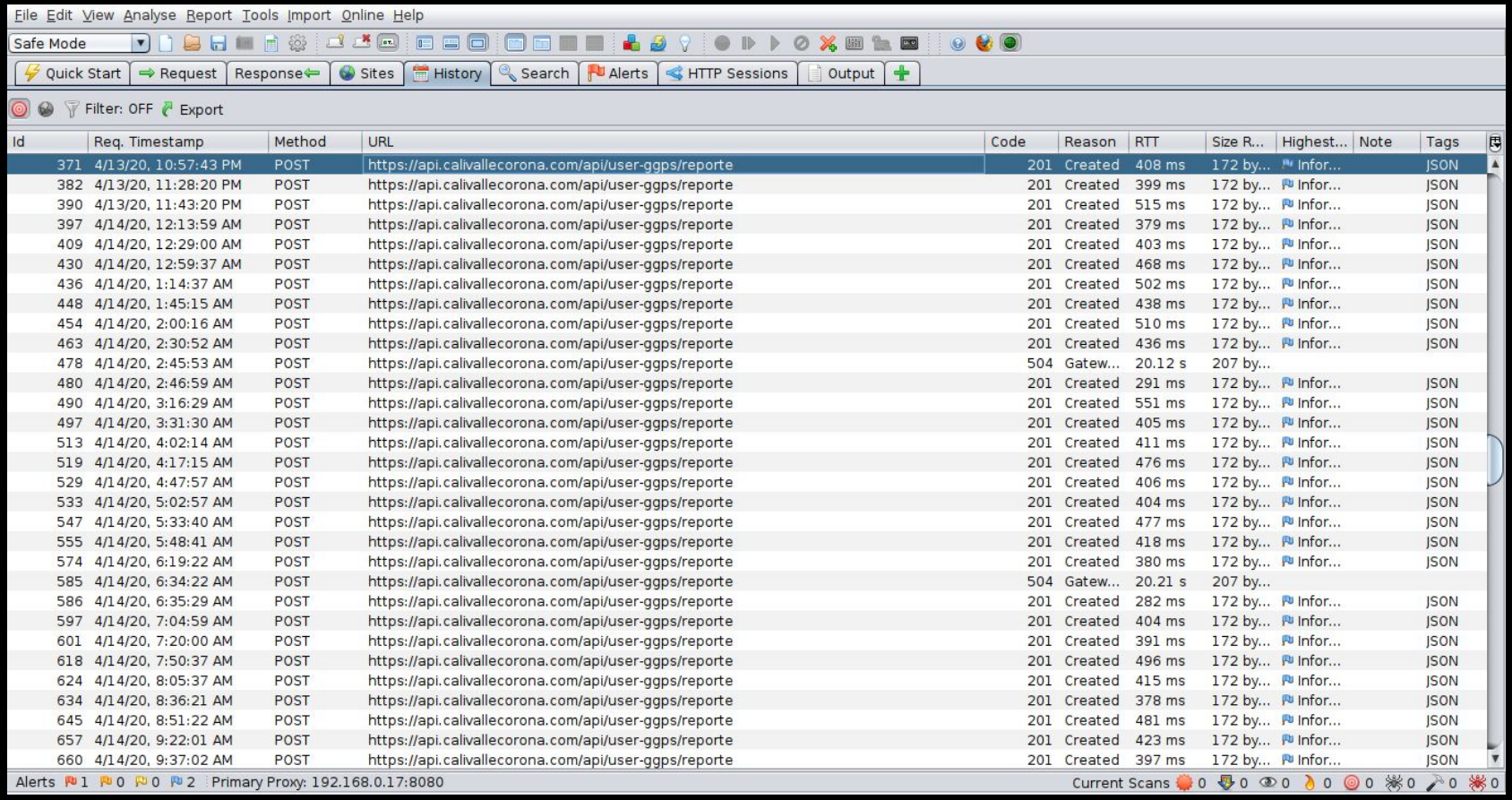
<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

```
GET https://epm.adminfo.net/vsmart/services/epm/index.php/dataDir/?id=44951&_=1586810468367 HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
Origin: https://medellin.gov.co
Connection: keep-alive
Referer: https://medellin.gov.co/medellinmecuida
Host: epm.adminfo.net
```

```
HTTP/1.1 200 OK
Date: Mon, 13 Apr 2020 20:42:33 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1;mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=631138519
X-Permitted-Cross-Domain-Policies: none
Content-Length: 413
Connection: close
Content-Type: application/json; charset=UTF-8
```

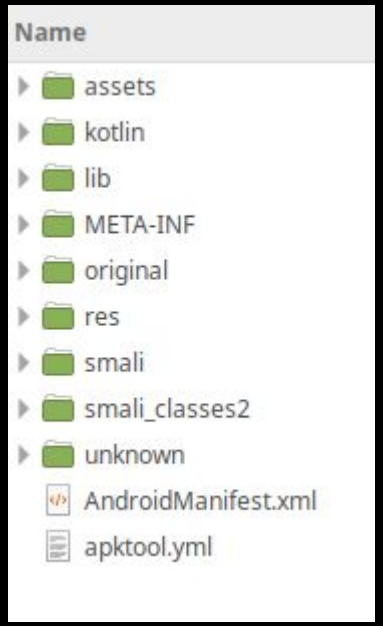
{"identificacion":"4[redacted]","nombre_cliente":"CARDON[redacted]S","cod_ciudad":"1700501001","desc_ciudad":"MEDELLIN",
"cod_dpto":"17005","desc_dpto":"ANTIOQUIA","coordenada_x":"-75.601952","coordenada_y":"6.[redacted]4","direccion":
"CR[redacted]1)","cod_categoria":"1","desc_categoria":"RESIDENCIAL","cod_estrato":"4","desc_estrato":"ESTRATO 4",
"riesgo":"1 Bajo","val_factura":"190253.10"}

Vigilancia intensa de CaliValleCorona



Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size R...	Highest...	Note	Tags
371	4/13/20, 10:57:43 PM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	408 ms	172 by...	Infor...		JSON
382	4/13/20, 11:28:20 PM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	399 ms	172 by...	Infor...		JSON
390	4/13/20, 11:43:20 PM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	515 ms	172 by...	Infor...		JSON
397	4/14/20, 12:13:59 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	379 ms	172 by...	Infor...		JSON
409	4/14/20, 12:29:00 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	403 ms	172 by...	Infor...		JSON
430	4/14/20, 12:59:37 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	468 ms	172 by...	Infor...		JSON
436	4/14/20, 1:14:37 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	502 ms	172 by...	Infor...		JSON
448	4/14/20, 1:45:15 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	438 ms	172 by...	Infor...		JSON
454	4/14/20, 2:00:16 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	510 ms	172 by...	Infor...		JSON
463	4/14/20, 2:30:52 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	436 ms	172 by...	Infor...		JSON
478	4/14/20, 2:45:53 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	504	Gatew...	20.12 s	207 by...			
480	4/14/20, 2:46:59 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	291 ms	172 by...	Infor...		JSON
490	4/14/20, 3:16:29 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	551 ms	172 by...	Infor...		JSON
497	4/14/20, 3:31:30 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	405 ms	172 by...	Infor...		JSON
513	4/14/20, 4:02:14 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	411 ms	172 by...	Infor...		JSON
519	4/14/20, 4:17:15 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	476 ms	172 by...	Infor...		JSON
529	4/14/20, 4:47:57 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	406 ms	172 by...	Infor...		JSON
533	4/14/20, 5:02:57 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	404 ms	172 by...	Infor...		JSON
547	4/14/20, 5:33:40 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	477 ms	172 by...	Infor...		JSON
555	4/14/20, 5:48:41 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	418 ms	172 by...	Infor...		JSON
574	4/14/20, 6:19:22 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	380 ms	172 by...	Infor...		JSON
585	4/14/20, 6:34:22 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	504	Gatew...	20.21 s	207 by...			
586	4/14/20, 6:35:29 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	282 ms	172 by...	Infor...		JSON
597	4/14/20, 7:04:59 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	404 ms	172 by...	Infor...		JSON
601	4/14/20, 7:20:00 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	391 ms	172 by...	Infor...		JSON
618	4/14/20, 7:50:37 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	496 ms	172 by...	Infor...		JSON
624	4/14/20, 8:05:37 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	415 ms	172 by...	Infor...		JSON
634	4/14/20, 8:36:21 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	378 ms	172 by...	Infor...		JSON
645	4/14/20, 8:51:22 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	481 ms	172 by...	Infor...		JSON
657	4/14/20, 9:22:01 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	423 ms	172 by...	Infor...		JSON
660	4/14/20, 9:37:02 AM	POST	https://api.calivallecorona.com/api/user-ggps/reporte	201	Created	397 ms	172 by...	Infor...		JSON

Usando apktool




```
android:screenOrientation="portrait" android:theme="@style/Theme.NoActionBar"/>
        <meta-data android:name="com.google.android.geo.API_KEY" android:value="AIzaSyBap8O4eY3xDn_y_INjrybKkDsp3c6bDEw"/>
        <uses-library android:name="org.apache.http.legacy" android:required="false"/>
        <service android:enabled="true" android:exported="false" android:label="@string/app_name"
android:name="com.hypelabs.hype.HypeService"/>
        <provider android:authorities="co.gov.ins.guardianes.crashlyticsinitprovider" android:exported="false"
android:initOrder="90" android:name="com.crashlytics.android.CrashlyticsInitProvider"/>
        <service android:directBootAware="true" android:exported="false"
android:name="androidx.room.MultiInstanceInvalidationService"/>
        <service android:directBootAware="true" android:exported="false"
android:name="com.google.firebase.components.ComponentDiscoveryService">
            <meta-data
android:name="com.google.firebase.components:com.google.firebase.analytics.connector.internal.AnalyticsConnectorRegistrar"
android:value="com.google.firebase.components.ComponentRegistrar"/>
            <meta-data android:name="com.google.firebase.components:com.google.firebase.iid.Registrar"
android:value="com.google.firebase.components.ComponentRegistrar"/>
        </service>
        <receiver android:exported="true" android:name="com.google.firebase.iid.FirebaseInstanceIdReceiver"
android:permission="com.google.android.c2dm.permission.SEND">
            <intent-filter>
                <action android:name="com.google.android.c2dm.intent.RECEIVE"/>
            </intent-filter>
        </receiver>
```

AP

Top Stories Topics

PRESS RELEASE: Paid content

HypeLabs' Contact-Tracing Technology Focused on Privacy Now Available for Immediate Deployment at No Cost for All Countries

April 14, 2020

CovidApp has already been tested and deployed in some countries in Latin America such as Colombia, the first nation to adopt the system showing the lowest numbers of infected patients in the region and is managing the flattening of the curve.

<K+LAB>
SEGURIDAD DIGITAL Y PRIVACIDAD

Fundación Karisma

¡Gracias!