



DiY Kit: How to analyze privacy and security on smartphone apps

Pilar Sáenz & Stéphane Labarthe
RightsCon 2018





PLATAFORMAS INSEGURAS,
EL CASO DE
IMEICOLOMBIA.COM.CO

Websites and Apps analysis: strong impact and advocacy potential

La **corresponsabilidad** en acción

La corresponsabilidad es uno de los aspectos más importantes que introduce la nueva política de seguridad digital. Este enfoque reconoce que hay un papel para todos los actores involucrados. El caso de éxito descrito en este documento muestra que es posible el trabajo de diferentes actores para el reporte, solución y seguimiento de problemas de seguridad digital y que el éxito se logra con la disposición de diálogo y cooperación de todas las partes interesadas.



Apps Analysis Methodology

What we look at:

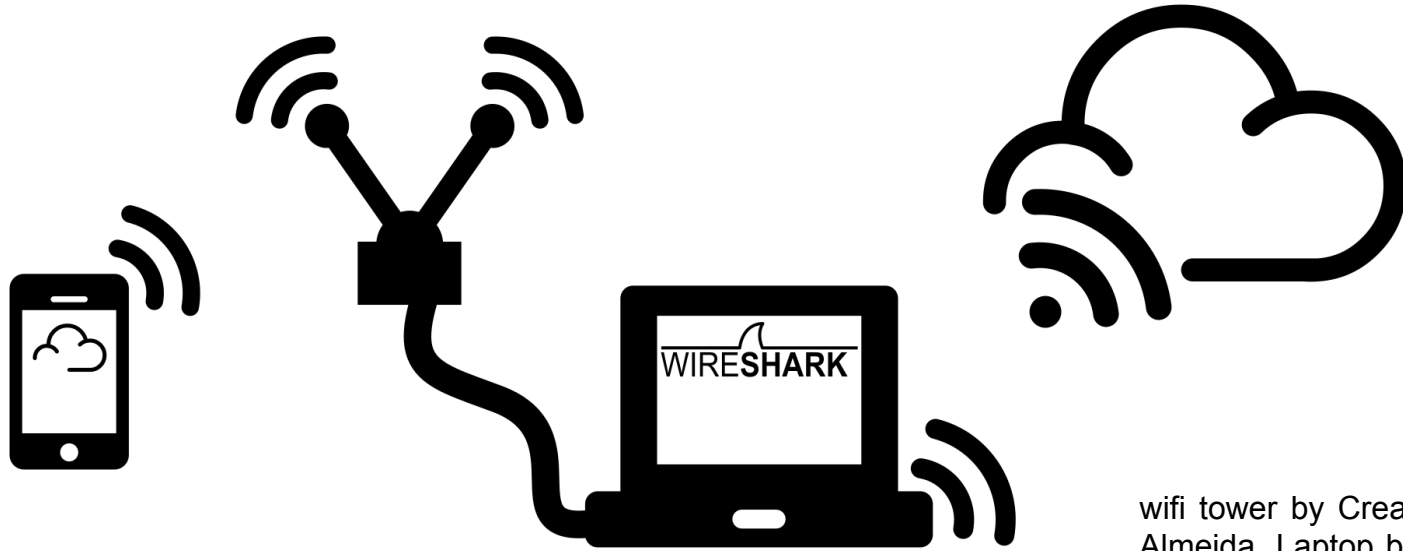
- ✓ Legal information and transparency
 - ✓ Digital security
 - ✓ Tracking
-

Characteristics:

- ✓ Technical analysis
- ✓ Reproducible
- ✓ Use free software
- ✓ No intrusive (legal and ethic)

Let's Open the Black Box

Intercepting HTTP/DNS traffic



wifi tower by Creative Stall, call by Geovani Almeida, Laptop by darwis and cloud wifi by Cristiano Zoucas from the Noun Project

Capturing outbound/inbound packets

Intercepting HTTP-POST and GET... [Sept 2017]



```

▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "aicAuthLogin" = "FUNDACIÓN KARISMA"
    ▶ Form item: "TipoPersona" = "Persona Juridica"
    ▶ Form item: "FormaConsulta" = "Persona Natural"
    ▶ Form item: "RazonSocial" = "Análisis App Dian"
    ▶ Form item: "aicDocumento" = "1015842780"
    ▶ Form item: "aicEscContact" = "Test@karisma.or.co"
    ▶ Form item: "Direccion" = "Callé 59#18"
    ▶ Form item: "Tel" = "738960"
    ▶ Form item: "cmbMake" = "BOGOTÁ, D.C."
    ▶ Form item: "cmbModel" = "BOGOTÁ, D.C."
  
```

```

▼ Hypertext Transfer Protocol
  ▼ [truncated]GET /website/dianchat/htmlclient/htmlclient.jsp;jsessionid=B37F9178B88CA...
    ▶ [ [truncated]Expert Info (Chat/Sequence): GET /website/dianchat/htmlclient/htmlclie...
      Request Method: GET
    ▼ Request URI [truncated]: /website/dianchat/htmlclient/htmlclient.jsp;jsessionid=B37...
      Request URI Path: /website/dianchat/htmlclient/htmlclient.jsp;jsessionid=B37F917...
      ▶ Request URI Query [truncated]: htmlclient=true&chathandle=FUNDACI%3C3%93N+KARISMA
  
```

Claro
Avantel 4G LTE

2:35 p. m.

DIAN
Dirección de Impuestos y Aduanas Nacionales

Para comenzar por favor diligencie en el siguiente formulario el nombre con el cual se identificará en la sesión de Chat y haga clic en "Enviar"

| | |
|----------------------|--------------------|
| Nombre de Usuario | FUNDACIÓN KARISMA |
| Tipo de Persona | Persona Juridica |
| Forma de Consulta | Seleccione |
| Razón Social/Nombre | Análisis App Dian |
| Nit / CC | 1015842780 |
| Email | Test@karisma.or.co |
| Dirección | Callé 59#18 |
| Teléfono de Contacto | 738960 |
| Departamento | BOGOTÁ, D.C. |
| Ciudad | BOGOTÁ, D.C. |

Puntos atención Contáctenos Chat

Where is going my GPS location?

[Sept 2017]



```
▼ Hypertext Transfer Protocol
→ GET /servicio/puntosCercanos/4.6305528/-74.0683867 HTTP/1.1\r\n
  ▶ [Expert Info (Chat/Sequence): GET /servicio/puntosCercanos/4.6305528/-74.0683867 HTT
    Request Method: GET
    Request URI: /servicio/puntosCercanos/4.6305528/-74.0683867
    Request Version: HTTP/1.1
    User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0; ALE-L23 Build/HuaweiALE-L23)\r\n
→ Host: dian.kubo.co\r\n
  Connection: Keep-Alive\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http://dian.kubo.co/servicio/puntosCercanos/4.6305528/-74.0683867]
  [HTTP request 1/2]
  [Response in frame: 450]
  [Next request in frame: 454]
```


A Gift for Google (Get & Referer)

K

[Sept 2017]

```
▶ Internet Protocol Version 4, Src: 10.42.0.228 (10.42.0.228) → Dst: googleapis.l.google.com (216.58.222.234)
▶ Transmission Control Protocol, Src Port: 55977 (55977), Dst Port: http (80), Seq: 1349, Ack: 1, Len: 649
▶ [2 Reassembled TCP Segments (1997 bytes): #550(1348), #551(649)]
▼ Hypertext Transfer Protocol
  ▼ GET /ajax/libs/jquery/1.9.1/jquery.min.js HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /ajax/libs/jquery/1.9.1/jquery.min.js HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ajax/libs/jquery/1.9.1/jquery.min.js
      Request Version: HTTP/1.1
      Host: ajax.googleapis.com\r\n
      Connection: keep-alive\r\n
      User-Agent: Mozilla/5.0 (Linux; Android 6.0; ALE-L23 Build/HuaweiALE-L23; wv) AppleWebKit/537.36 (KHTML,
      Accept: */*\r\n
      → [truncated] Referer: http://www.atencionvirtual.com/website/dianchat/htmlclient/htmlclient.jsp;jsessionid
```

Personal information in the (truncated) referer:

http://www.atencionvirtual.com/website/dianchat/htmlclient/htmlclient.jsp;
jsessionid[...]& chathandle=**FUNDACIÓN+KARISMA** [...]&customer
Email=**test@karisma.org.co** [...]& edu.question=+ **Identificación:+1015842780**
+--+Origen+>>+appMovil[...] **Telefono+de+Contacto+>>+738960+Departamento+>>+**
BOGOTÁ+D.C.

Most changes have been implemented

[May 2018]



Privacy policy, HTTPS, changes in the web server, etc, on its website (also analyzed).



DIAN App doesn't use HTTP/GET to send personal data => Google doesn't have it anymore.



GPS location is not transmitted to external domain.



DIAN App is still sending/receiving personal data with HTTP

Some questions...

K

¿Complementary approach?

Yes, for example:
Exodus Privacy automated analysis
(tracker code in APK file, DNS request)



¿What about HTTPS?

HTTPS Proxy (MitMx, etc.)?
Well...
It is legal?
It is ethical?



Fundación
karisma
Seguridad e
intimidad

¡Thank you!

mpsaenz@karisma.org.co

stephane@karisma.org.co



This presentation has a
[Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)