<K+LAB>

Fundación Karisma
Seguridad e intimidad

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

Pilar Sáenz & Stéphane Labarthe
RightsCon 2018

Websites and Apps analysis:

strong impact and advocacy potential

DIAN®
Dirección de Impuestos y Aduanas Nacionales

Apps Analysis Methodology

What we look at:

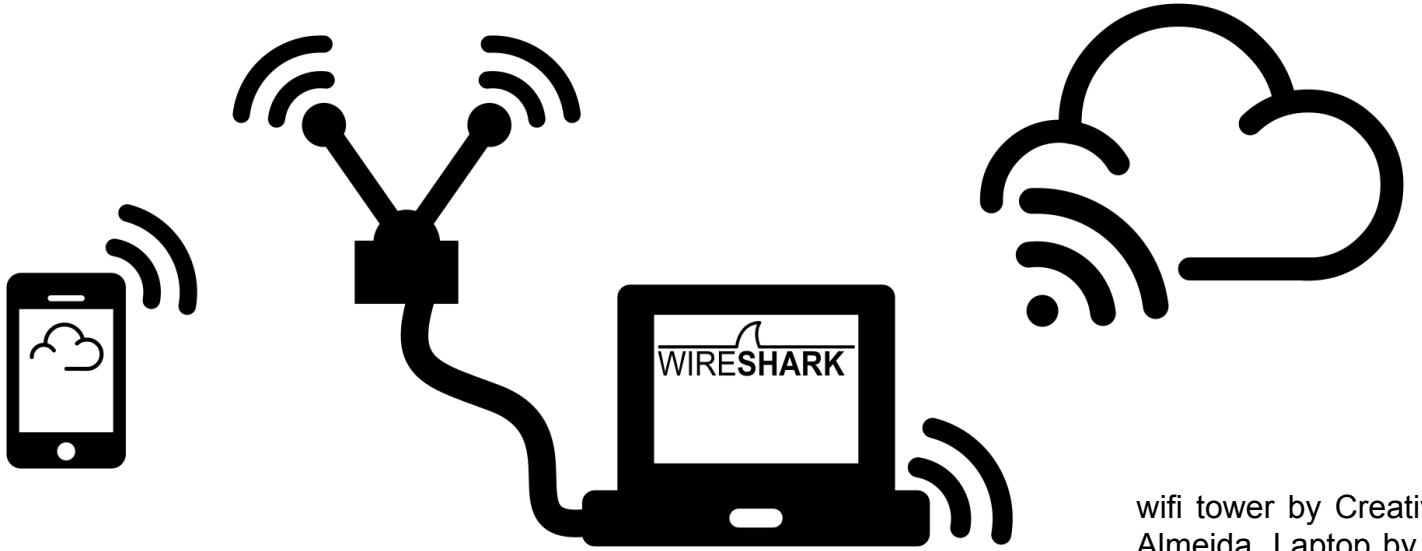
- ✓ Legal information and transparency
- ✓ Digital security
- ✓ Tracking

Characteristics:

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

Let’s Open the Black Box

Intercepting HTTP/DNS traffic



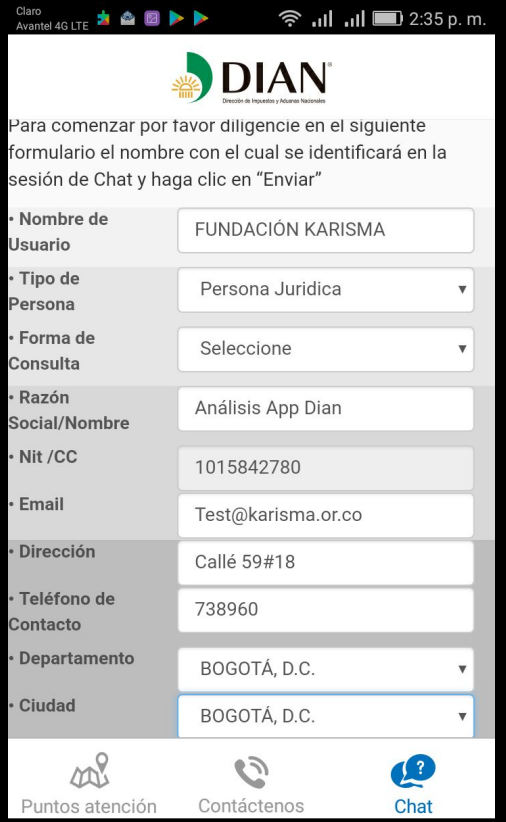
wifi tower by Creative Stall, call by Geovani Almeida, Laptop by darwis and cloud wifi by Cristiano Zoucas from the Noun Project

Capturing outbound/inbound packets

Intercepting HTTP-POST and GET… *[Sept 2017]*

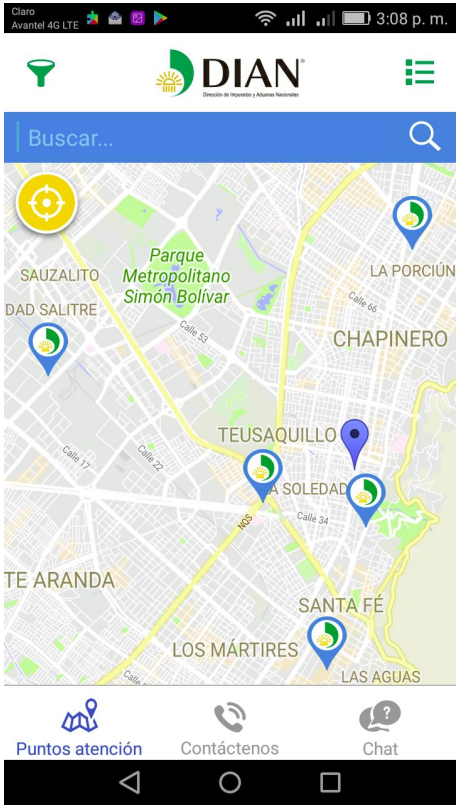

```
▶ Hypertext Transfer Protocol
▼ HTML Form URL Encoded: application/x-www-form-urlenc
  ▶ Form item: "aicAuthLogin" = "FUNDACIÓN KARISMA"
  ▶ Form item: "TipoPersona" = "Persona Juridica"
  ▶ Form item: "FormaConsulta" = "Persona Natural"
  ▶ Form item: "RazonSocial" = "Análisis App Dian"
  ▶ Form 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=B37F9178B88CAA
    ▶ [ [truncated]Expert Info (Chat/Sequence): GET /website/dianchat/htmlclient/htmlclie
      Request Method: GET
    ▼ Request URI [truncated]: /website/dianchat/htmlclient/htmlclient.jsp;jsessionid=B3
        Request URI Path: /website/dianchat/htmlclient/htmlclient.jsp;jsessionid=B37F917
      ▶ Request URI Query [truncated]: htmlclient=true&chathandle=FUNDACI%c3%93N+KARISMA
```



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) [Sept 2017]

Personal information in the (truncated) referer:

http://www.atencionvirtual.com/website/dianchat/htmlclient/htmlclient.jsp;jsessionid[...]& chathandle=**FUNDACIÓN+KARISMA** [...]&customerEmail=**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...

¿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?

<K+LAB>

Fundación Karisma
Seguridad e intimidad

¡Thank you!

mpsaenz@karisma.org.co stephane@karisma.org.co