# XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva


# Privacidad en dispositivos móviles: Memorias de un analista

CCN-CERT
centro criptológico nacional

- David Ventas Sierra
- EXCEM Technologies
- dvs@excem.com / david.ventas@gmail.com

# Índice

1. La seguridad y la privacidad es cosa de todos

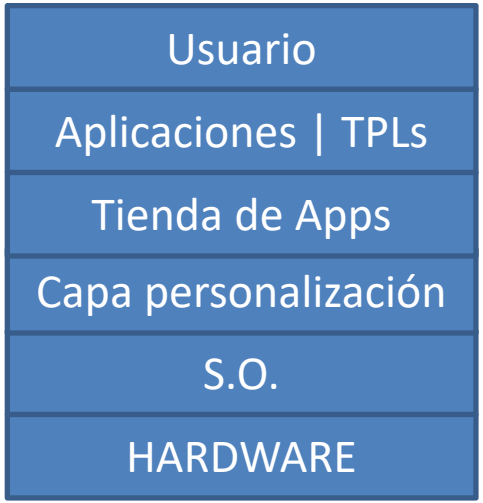
2. Análisis de trafico de red

3. Ejemplos de información

4. Tráfico cifrado

## Esquema de actores implicados

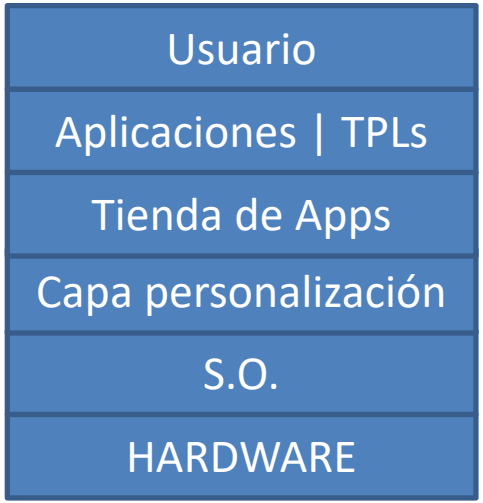
Otra vez la metáfora de la cadena no, por favor.




- Elementos más relevantes implicados en la seguridad y privacidad de los usuarios.
- Existen bugs en el hardware: Drammer (Rowhammer) o GLitchAttack.
- Escaso control de aplicaciones antes de su publicación.
- Aplicaciones con la seguridad más básica imprescindible.

# Esquema de actores implicados

Entre todos la mataron…



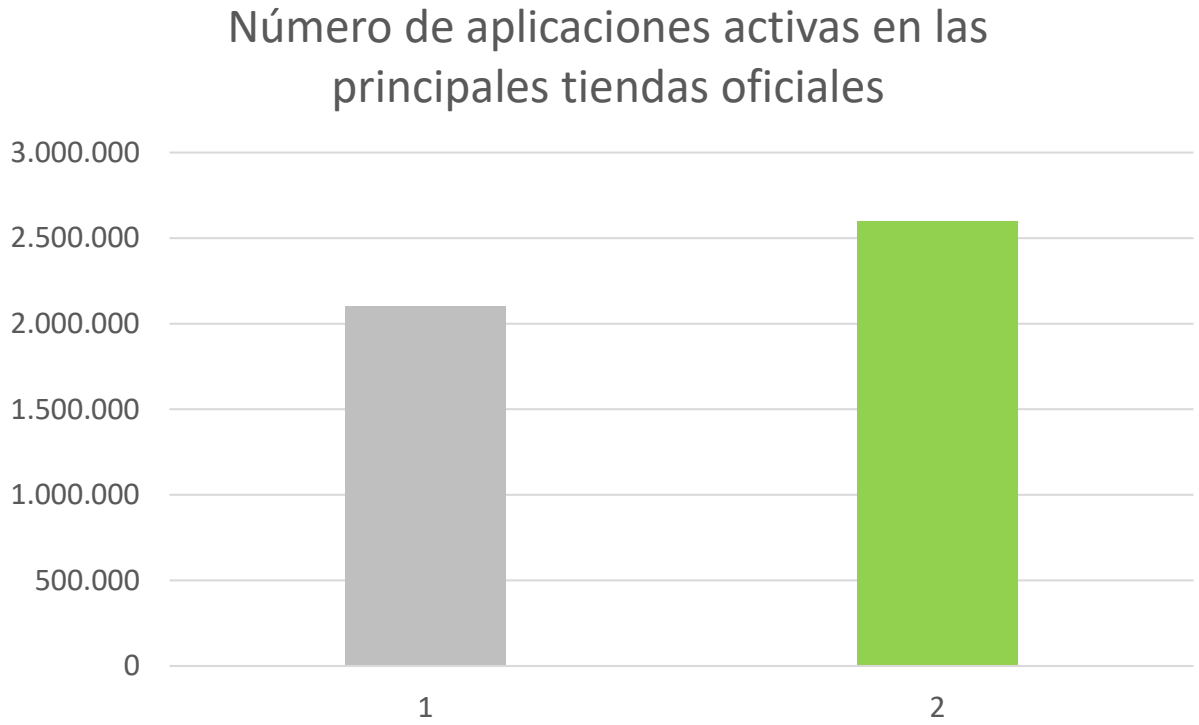

- Las *Third Party Libraries* que implementan como *analytics*, pueden exfiltrar datos.
- Los usuarios desprecian su propia privacidad mediante rr.ss. o prácticas de riesgo.

## Firmware de dispositivos móviles

"Me he comprado un teléfono chino por 90€ que tiene más RAM que mi PC."

- Escándalo Adups: BLU, Lenovo, ZTE, Cubot.
- Caso OnePlus: OxygenOS transmitía datos sensibles.
- Hay estudios en marcha analizando distintos firmwares comerciales.

# Tiendas de aplicaciones




- Apertura App Store: Julio 2008
- Apertura Google Play: Octubre 2008

## Tiendas de aplicaciones

- Mecanismos de control: Google Play Protect y Apple’s App Review Team.

- Aún con todas estas medidas, se han dado casos como el de la botnet WireX y el de XcodeGhost.

## TPL (Third Party Library)

"Cuando un producto es gratuito, en realidad tú eres el producto."

- Representan de media alrededor del 60% del código de una app.
- Usos:
  - Analytics
  - Integración con RR.SS.
  - RestAPI
  - Debugging
- Beneficiarias de una gran parte de los permisos que requiere una app.
- También aportan complejidad y vulnerabilidades a las aplicaciones.

## Aplicaciones desconsideradas con la privacidad

"Vamos a centrarnos en que esto funcione. Ya añadiremos la seguridad…"

- El código de las aplicaciones también es responsable de la privacidad de los usuarios.
- Ejemplo: evolución de WhatsApp desde 2009 hasta 2016.
- Durante nuestra trayectoria hemos visto esa evolución en otras apps como Facebook, MiVodafone, Wallapop…

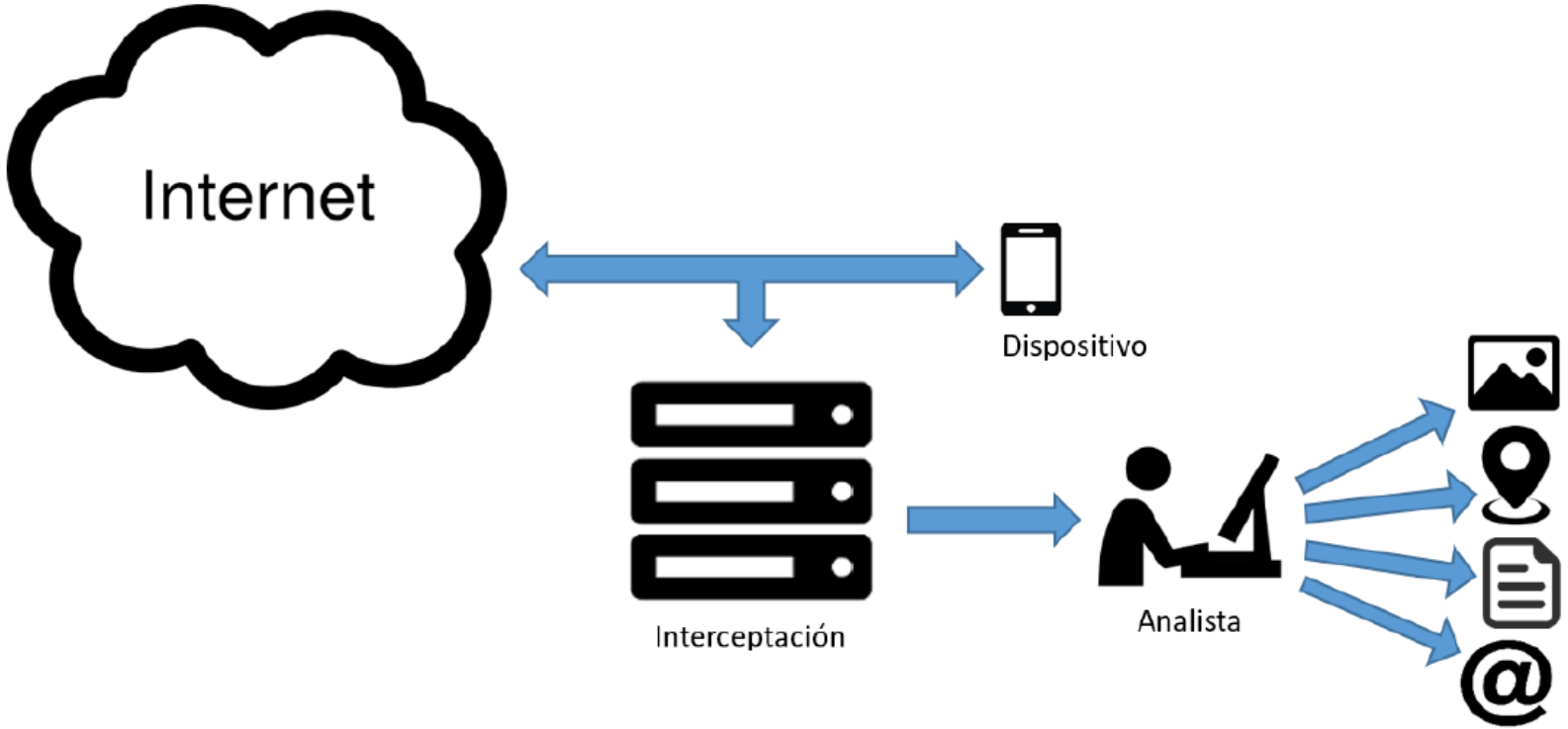
# El papel del usuario

Los usuarios siguen manteniendo actividades de riesgo como:

- La descarga de aplicaciones de tiendas no oficiales.
- El rooteo de terminales.
- Otorgar permisos innecesarios a aplicaciones.
- Utilización de páginas no seguras. Compras, conversores online…

# Análisis de tráfico

"Son solo 1700 hosts más y termino."



## ¿Para qué sirve el análisis de tráfico?

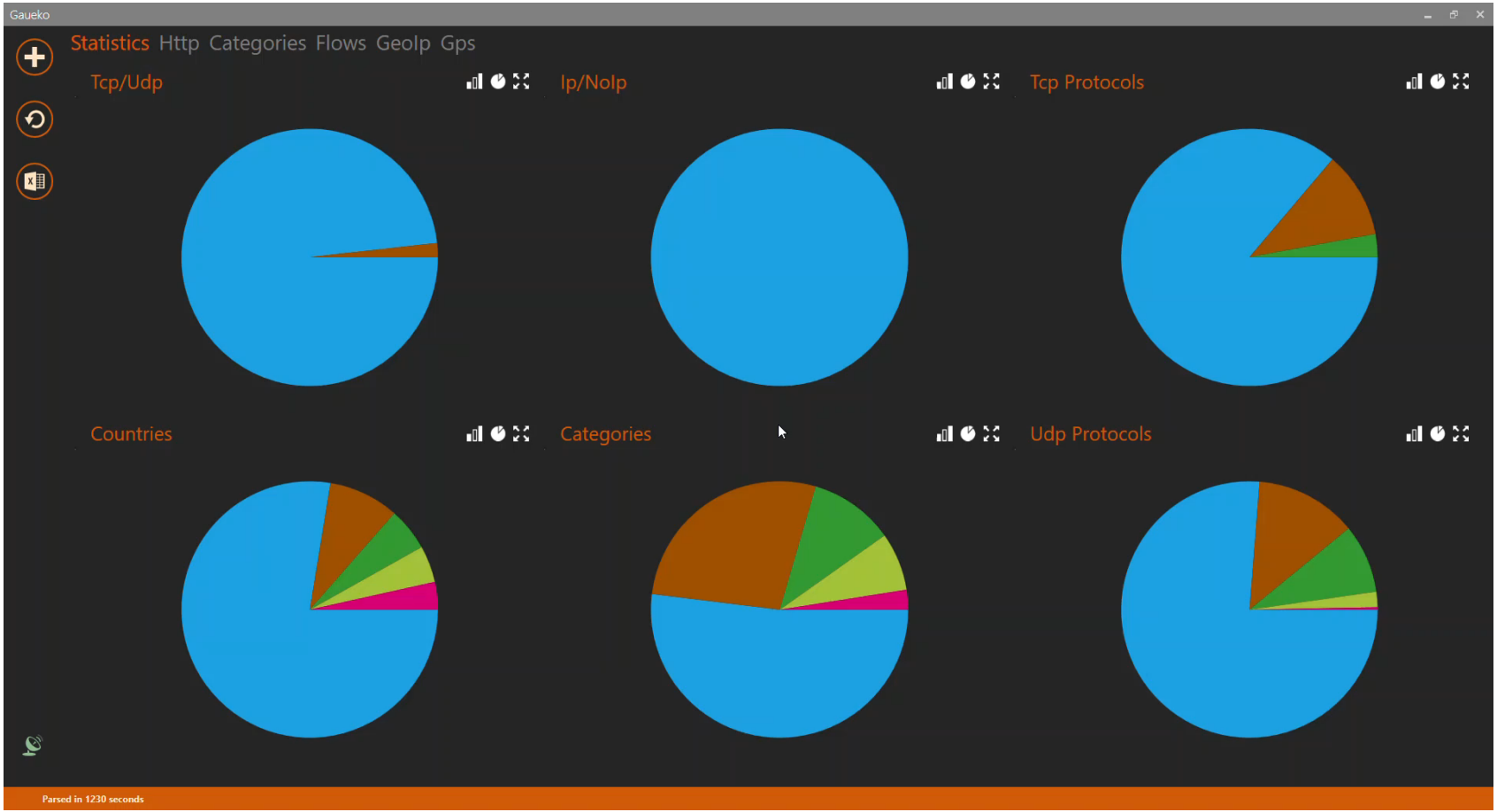
En el caso de un analista del bando “de los buenos”:

- Obtención de evidencias legales.
- *Fingerprinting* del objetivo. Hábitos en internet.
- Hábitos y rutinas en el mundo real.
- Extracción de datos personales.
- OSINT.
- Información variada que puede ser de utilidad para las unidades que llevan a cabo las investigaciones.

# Herramienta PitBull

No confundir con el “cantante”…

- Analizador / clasificador de tráfico de red.
- Diseñado para capturas de tamaño medio a grande. Probado hasta con ficheros de 40 GB.
- Permite obtener una “fotografía” general del tráfico en pocos minutos, con los datos más relevantes.
- Es posible agrupar elementos, examinar flujos en detalle, exportar resultados a xls, abrir fragmentos de tráfico en otra instancia de PitBull o en otras aplicaciones como Wireshark y un amplio etcétera.


Gaueko
Statistics Http Categories Flows GeoIp Gps
Tcp/Udp
Ip/NoIp
Tcp Protocols
Countries
Categories
Udp Protocols
Parsed in 1230 seconds

# Ejemplos de fugas de datos

Miguitas de pan…

- Numerosas aplicaciones o sus TPLs aún filtran información que, más o menos grave, probablemente el usuario no estaría conforme con que se compartiera.

- A continuación algunos ejemplos:

# Ejemplos de fugas de datos

## Localizaciones

```
POST /ut/v2 HTTP/1.1
Content-Type: application/json
Accept: application/json
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; HUAWEI G7-L01 Build/HuaweiG7-L01) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/39.0.0.0 Mobile Safari/537.36
Host: mediation.adnxs.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 4705
{"tags":[{"id":9767645,"primary_size":{"width":300,"height":250},"sizes":[{"width":300,"height":
250},{"width":320,"height":250}],"allow_smaller_sizes":false,"allowed_media_types":
[1,4],"prebid":false,"disable_psa":true,"require_asset_url":false}],"user":{"gender":
0,"language":"es"},"device":{"make":"HUAWEI","model":"HUAWEI G7-L01","useragent":"Mozilla\/5.0
(Linux; Android 5.1.1; HUAWEI G7-L01 Build\/HuaweiG7-L01) AppleWebKit\/537.36 (KHTML, like Gecko)
Version\/4.0 Chrome\/39.0.0.0 Mobile Safari\/537.36","mnc":1,"mcc":214,"carrier":"vodafone
ES","connectiontype":2,"geo":{"lat":43.      ,"lng":-2.      ,"loc_age":569494,"loc_precision":
18},"devtime":1530312026671,"limit_ad_tracking":false,"device_id":{"aaid":"77      )3c8-4bea-
a3e1-7      ","os":"android"},"app":
{"appid":"com.anuntis.fotocasa"},"sdkver":"ansdk4.7","sdk":
{"source":"ansdk","version":"4.7"},"supply_type":"mobile_app","keywords":[{"key":"kw_es-sch-
transaction","value":["Alquiler"]},{"key":"kw_es-sch-city_zone_id","value":["0"]},{"key":"kw_es-
sch-rooms_max","value":["0"]},{"key":"kw_es-sch-county_id","value":["427"]},{"key":"kw_es-sch-
site","value":["fotocasa"]},{"key":"kw_es-sch-region_level1_id","value":["18"]},{"key":"kw_es-
sch-region_level1","value":["Pa..s Vasco"]},{"key":"kw_es-sch-mts2_max","value":["0"]},
```

Tráfico generado por Adnxs, una TPL probablemente en Fotocasa.

# Ejemplos de fugas de datos

## Listados de Apps instaladas o en uso

```
POST /v3/event/collection_apps HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 6.0.1; SM-G920F Build/MMB29K; wv) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/68.0.3440.70 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: api.pingstart.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 920
```

```
platform=android&osv=6.0.1&publisher_id=5679&apps=org.francho.android.zgzbus
%2Ccom.mcdonalds.android%2Ccom.icare.iweight%2Ccom.camerasideas.instashot
%2Cimoblife.toolbox.full%2Ccom.whatsapp%2Ccom.picsart.studio
%2Ccom.appstar.callrecorder%2Ccom.zerodesktop.appdetox.qualitytime
%2Ccolor.dev.com.magenta%2Ccom.andrwq.recorder%2Ccom.instagram.android
%2Ccom.melodis.midomiMusicIdentifier.freemium%2Ccom.anuntis.segundamano
%2Ccom.google.android.instantapps.supervisor
%2Cdevian.tubemate.v3%2Ccom.snaptube.premium%2Ccom.twitter.android
%2Ccom.mokaware.modonoche%2Ccoches.net%2Ccom.facebook.katana%2Ccom.facebook.orca
%2Ccom.google.android.apps.translate%2Ccom.ui.LapseItPro%2Ccom.alensw.PicFolder
%2Ccom.orange.miorange%2Ccom.colectivosvip.cluballen
%2C&dpi=640.0&brand=samsung&app_versioncode=10323&versioncode=1.0.4&root=1&app_name=co
m.snaptube.premium&aid=cab          3&gaid=2      e-6f8e-     -a2b4-
c1          2&model=SM-G920F&HTTP/1.1 200 OK
```

Tráfico probablemente generado por una TPL de Snaptube.

# Ejemplos de fugas de datos

## Datos del terminal

```
GET /v1/protect/search?avr=7.0&title=
)&androidID=51              14 imei=3584              &event=CONTENT_GP&advertisin
gID=2      3-e56b-    -a5e3-
c          e imsi=21403&v=4.34.0.10409&u=dc8c26bdd2134cf2bf8a8a68a5121b2c133c1943&ch
=tube_uptd_as&networkCountryIso=ES&region=ES&locale=es_ES&lang=es&pn=com.snaptube.pr
emium&f=phoenix2&net=WIFI&random_id=10&vc=10409 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G930F Build/NRD90M; wv) AppleWebKit/
537.36 (KHTML, like Gecko) Version/4.0 Chrome/69.0.3497.100 Mobile Safari/537.36
Host: api.ad.snappea.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

Análisis del tráfico generado por la aplicación Snaptube.

# Ejemplos de fugas de datos

## Datos de la navegación

```
POST /api/v1/track HTTP/1.1
Accept: application/json
User-Agent: Android SPT Tracker 5.1.0_playservices_11_0_1 1401 -
sdrn:schibsted:client:net.infojobs.mobile.android:            InfoJobs (HUAWEI,CLT-
L29,kirin970,27)
Content-Type: application/json
Content-Length: 2330
Host: collector.schibsted.io
Connection: Keep-Alive
Accept-Encoding: gzip
{"device":
{"environmentId":"14bd4fd6-2e5b-4dbe-                ","hardware":"kirin970","jweIds"
:"
                                                                                    ,
"manufacturer":"HUAWEI","model":"CLT-L29","networkConnectivity":{"networks":
[{"networkState":"connected","networkType":"wifi"}],"@type":"NetworkConnectivity"},"os
Version":"4.4.103+","product":"CLT-
L29","release":"8.1.0","sdkVersion":"27","@type":"Device"},"location":
{"accuracy":"2000.0","latitude":"41.                ","longitude":"-0.                ',
"timestamp":1539          ,"@type":"GeoCoordinates"},"object":{"category":"Todas las
categor..as","filters":
{"contractLength":"","contractType":"","education":"","experience":"","jobSector":"Tod
as las categor..as","locality":"","occupationalCategory":"Todas las
categor..as","query":"media jornada","region":'          "},"items":
[{"category":"Comercial y ventas > Comercial","name":
```

Análisis de tráfico dirigido a Schibsted relacionado con Infojobs.

# Ejemplos de fugas de datos

## Datos personales

```
GET /o/3/
TkRjd01ESTJ
                                                    _U5GxRRg HTTP/1.1
Host: link.es.expediamail.com
Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: es-es
Connection: keep-alive
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8
(KHTML, like Gecko) Mobile/14G60

HTTP/1.1 200
Content-Type: image/gif
X-Application-Context: application:deployed:8080
Content-Length: 43
Connection: keep-alive

GIF89a.............!.......,...........D..;
```


Píxel incluido en una newsletter de Expedia.

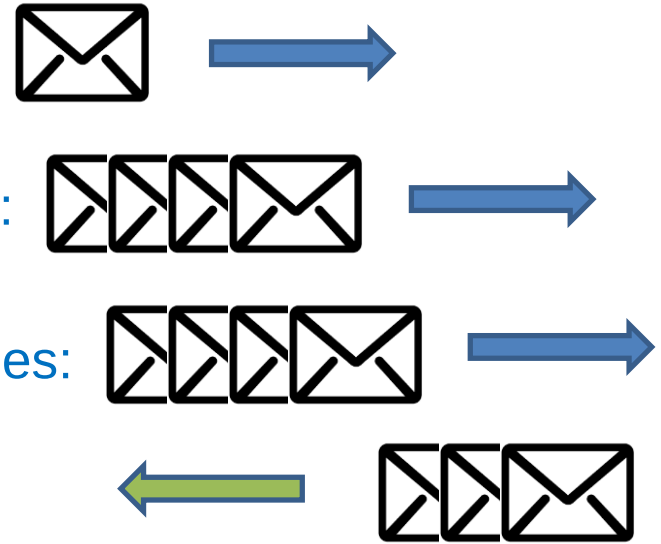
## *Fingerprinting* de tráfico cifrado

"Pero… con el TOR ese mi privacidad está garantizada, ¿no?"

- El *fingerprinting* de tráfico de red es una técnica en pleno desarrollo.
- Consiste en averiguar cuál es el servidor web o servidor de aplicación al que se dirige el tráfico cifrado.
- Se establecen conjuntos de datos limitados para los servidores que se quieren identificar.
- Actualmente se emplea *machine learning* para esta tarea.

# *Fingerprinting* de tráfico cifrado

- La evolución de la técnica ha sido constante:
- Paquete a paquete:
- Ráfagas de paquetes:
- Ráfagas bidireccionales:



# Estudios mencionados

- Adaptive Encrypted Traffic Fingerprinting With Bi-Directional Dependence
  Khaled Al-Naami, Swarup Chandra, Ahmad Mustafa, Latifur Khan, Zhiqiang Lin, Kevin Hamlen, and Bhavani Thuraisingham, Computer Science Department - The University of Texas at Dallas

- Understanding Third-party Libraries in Mobile App Analysis
  Haoyu Wang and Yao Guo, School of Computer Science - Beijing University of Posts and Telecommunications

# XII Jornadas STIC CCN-CERT

## Ciberseguridad, hacia una respuesta y disuasión efectiva


- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional