

XI
JORNADAS
STIC
CCN-CERT

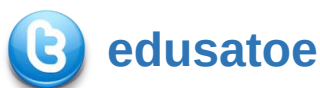
Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Bots de Geolocalización de Usuarios en Telegram

Eduardo Sánchez





Eduardo Sánchez   edusatoe

- Ingeniero Informático
- Doble Máster en Seguridad TIC (Sistemas y Redes; Servicios y Aplicaciones)
- Profesor de Formación Profesional para la Junta de Andalucía
- Profesor de Másters y Postgrados en UCLM y UNEX
- CSO en onBRANDING
- Perito Judicial por la AIF
- Colaborador del blog de Hacking Ético
- Cofundador de la comunidad Hack&Beers
- Cofundador de Hacking Solidario
- Socio fundador de ANPHACKET
- Organizador del congreso Qurtuba Security Congress
- Fundador de las Jornadas de Seguridad Security High School.

**HACK
& BEERS**

ANPHACKET

Qurtuba
SECURITY CONGRESS

**HACKING
SOLIDARIO**

**Security
High School**

on **BRANDING**
siempre on

DISCLAIMER

- Todo lo mostrado a continuación es una **prueba de concepto**.
- **No me hago responsable del mal uso** que se le de a las técnicas de obtención de información mostradas a continuación.
- El uso de balizas digitales sólo está autorizado para las **FFCCSE** o **bajo la autorización de un detective privado** como medida proporcionada al caso en el que se lleve a cabo.

Índice

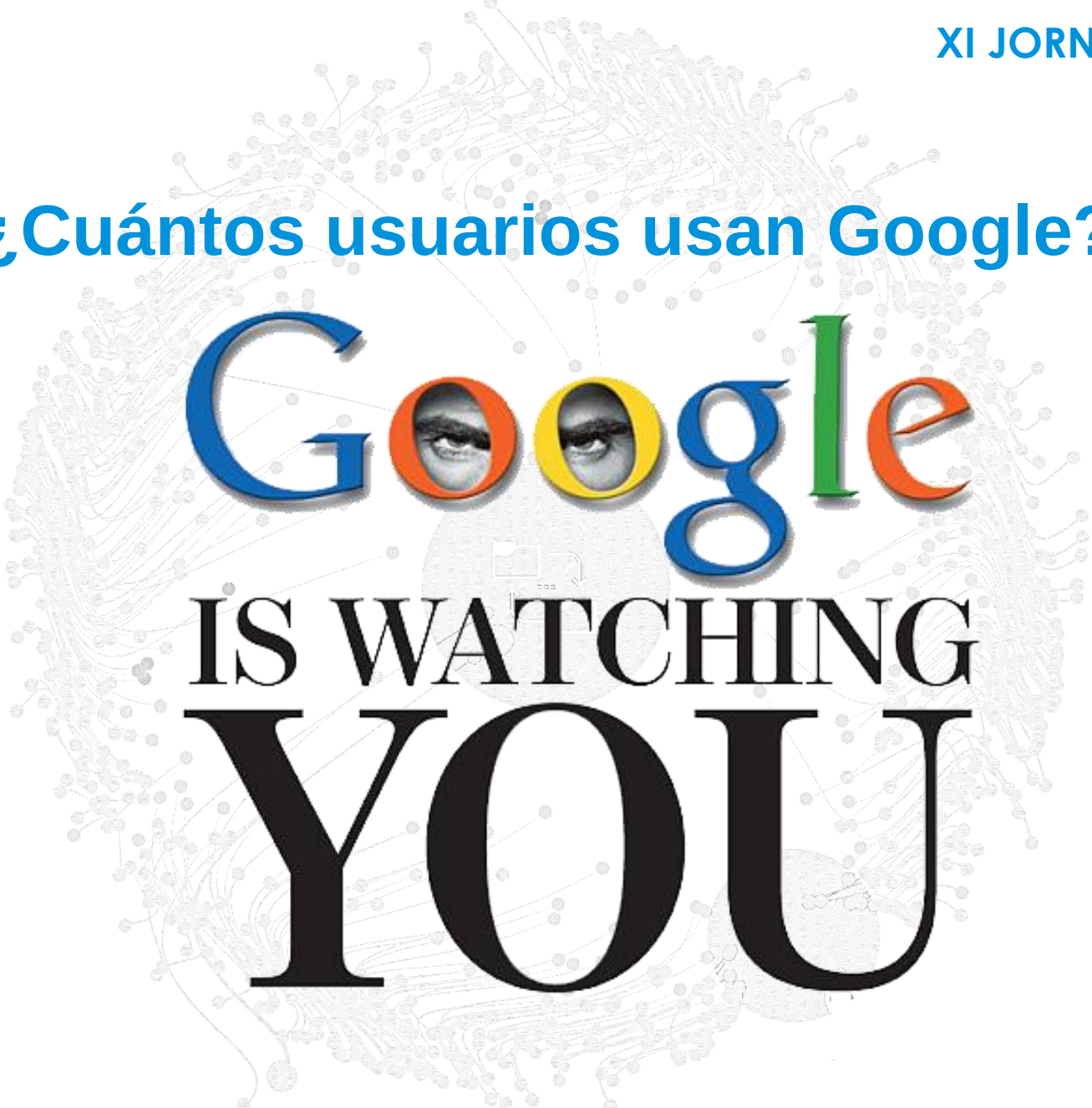
1. ¿Cómo podemos geolocalizar a un usuario?
2. Sistemas de tracking → Balizas.
3. ¿Qué son los Bots?
4. Análisis de Privacidad en RRSS.
5. Herramientas para la creación de Bots.
6. Geolocalización de usuarios de Telegram.

¿Cómo podemos geolocalizar a un usuario?



1. GPS del móvil → Longitud y Latitud.
2. Antenas de telefonía:
 - ✓ Cell ID (CID/BID)
 - ✓ Local Area Code (LAC)
 - ✓ Mobile Country Code (MCC)
 - ✓ Mobile Network Code (MNC/SID)
3. Redes Inalámbricas → MACs de los APs e Intensidad de Señal.
4. Token de tu navegador.
5. Dirección IP.

¿Cuántos usuarios usan Google?



Google
IS WATCHING
YOU

Política de Privacidad de Google Location Services

Si permite que un sitio Web obtenga su ubicación a través de este servicio, nosotros recogeremos la información en función de las características de su dispositivo: la información sobre los routers inalámbricos cerca de usted, el ID del móvil de las torres de telefonía más próximas, y la intensidad de tu wifi o la señal de celular. Esta información se utiliza para devolver una ubicación estimada al navegador que la solicita. Además en cada solicitud recopilamos también la dirección IP, el User-Agent y el ID único de su cliente. Esta información se utiliza para diferenciar las solicitudes, no para identificarlo.

Sistemas de Tracking de Usuarios

Rastreo de usuarios a través de los clicks



Grabify IP Logger

<https://grabify.link>

The screenshot shows the Grabify IP Logger website. At the top is a dark navigation bar with the text 'GRABIFY IP LOGGER' and a menu with links: 'TOOLS', 'FEATURES', 'URL'S', 'MY LOGS', 'MY PROFILE', and 'LOGOUT'. Below this is a large teal banner with the word 'GRABIFY' in white. Underneath the banner is the text 'Create or Track URLs'. A blue notification box contains several updates: '- DOMAINS! - Our old domains are making a comeback.', '- NEW - Custom URL's! You can now make custom URL's on your tracking page.', '- Facebook - Like our new facebook page for updates and changes! <https://www.facebook.com/GrabifyLogger/>', and '- Discord - Join our Discord server! <https://discord.gg/gyBQFjv>'. Below the notification is a white input field with the placeholder text 'Enter a valid URL or tracking code...'. Under the input field are two buttons: 'Create URL' and 'Tracking Code'. Below these buttons, it says 'Total Logs: 26,047,481'. A 'DONATION GOAL' section features a progress bar that is approximately 56% full, with a current amount of '\$56.39' and a goal of '\$100'. Below the progress bar is a link to the 'Donation leaderboard'. At the bottom of the donation section, it states 'We need \$43.61 to reach our hosting Donation Goal'. The very bottom of the page shows 'Top Donator: \$50 - Patrizia says: [Waiting on'.

IP Logger

<https://iplogger.org>

IPLogger Services Site help Your IPLoggers Account Contact us English

Please disable your Adblock plugin for IPLogger. Pulsa **F11** para salir del modo de pantalla completa mobile version

IP Logger URL shortener web service with the most detailed click's statistics allowing to track ip address, lookup ip address, check ip location and check any URL for redirects. IP Logger provides many unique visitor counters, including invisible image, IP informers and userbars for your website, blog or forum. If you are wondering how to find ip address of a website or anyone in the internet, you are in the right place! Don't use our services for any unlawful reason, don't perform any illegal or illicit activity using our services or information that may be obtained using our services. If you noticed that someone is abusing IP Logger services, please immediately report it to abuse@iplogger.org

My IP: 178.139.210.105 | Spain/Madrid | Chrome | Windows | VF-ES-NETWORK

subscribe

Paste a link that you want to shorten here shorten

IPLogger URL Shortener - log and track IP addresses

URL Shortener

Enter any URL or link to any image on the internet to shorten it and track IP addresses with detailed logs of all clicks on your short IPLogger link

Enter any URL

Get IPLogger code

Invisible image

Generate invisible IPLogger image, share it via message or publish it on your website or blog and track the IP addresses of all the users who viewed your message. Note that IP grabber presence will not be visible to anyone.

Get IPLogger code

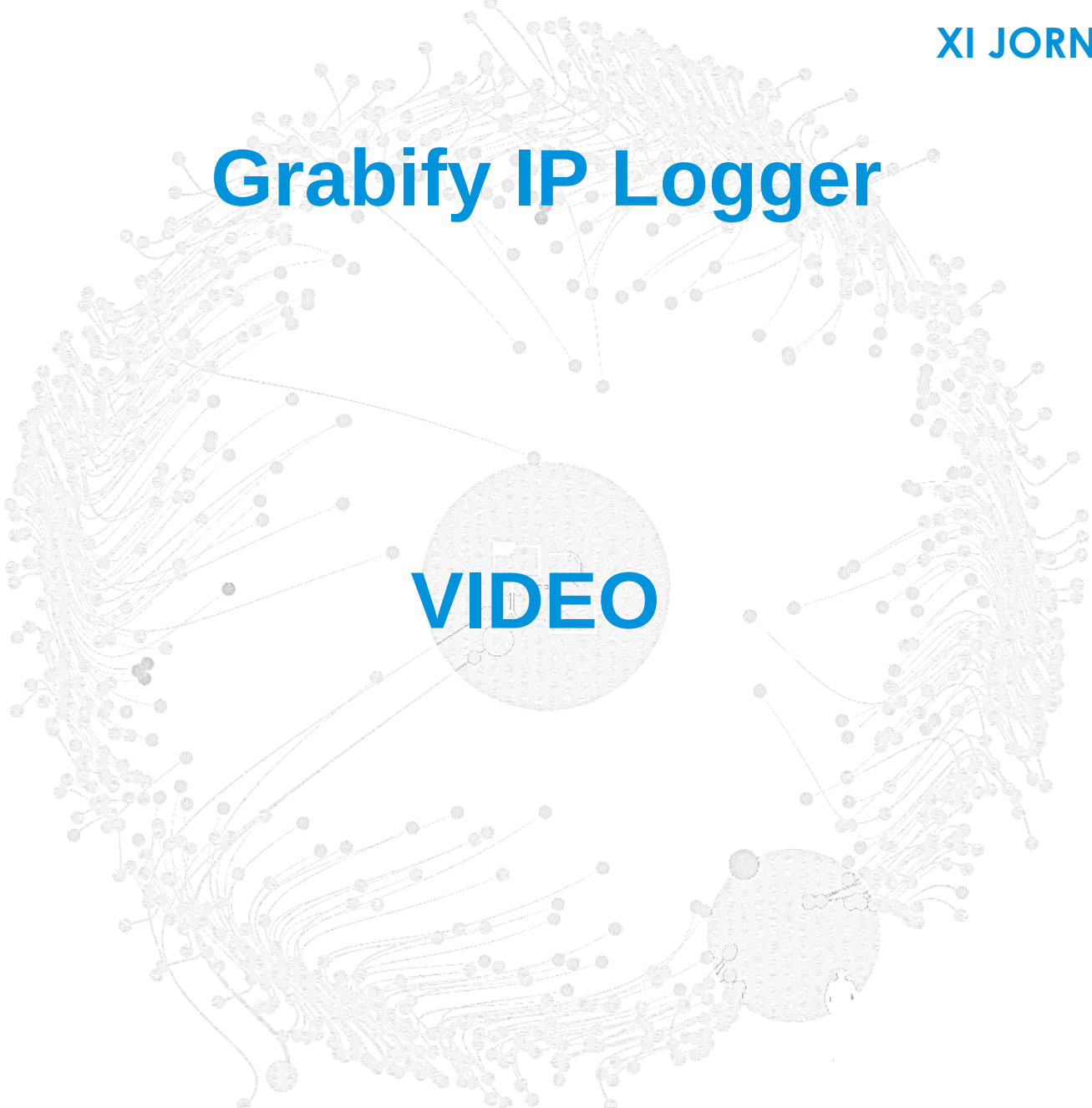
IP Lookup URL Checker

Enter any URL here to check it for redirects, server availability status and location. Enter IP address to get its ISP, country, city and IP geolocation.

Enter any URL or IP address

Get information

Grabify IP Logger



VIDEO

¿Qué son los Bots?

- Los bots son evoluciones de las aplicaciones.
- Suponen el 60% del tráfico de Internet.
- El 35% es tráfico de bots maliciosos.
- Usos de los bots:
 - ✓ Recopilar información.
 - ✓ Identificación de sitios maliciosos o vulnerables.
 - ✓ Arañas/Crawlers para rastreo → SEO positivo y negativo
 - ✓ Spammers: bot que postean publicidad y los enlaces maliciosos.
 - ✓ BotNets para ataques de DDoS.
 - ✓ Otros bots: seguidores de Twitter, rubias de bote...



Comprar Bots

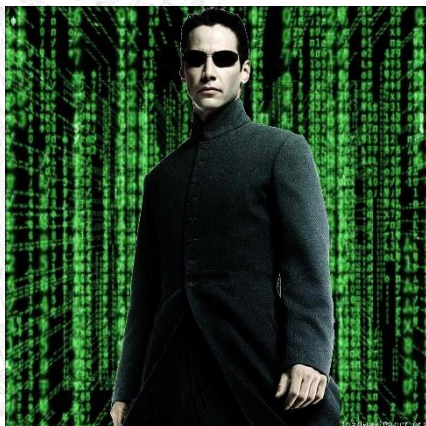
<http://www.compra-seguidores.com/>

1000 Seguidores	2000 Seguidores	5000 Seguidores	10000 Seguidores
9,99€	16,99€	44,99€	84,99€
El precio incluye IVA	El precio incluye IVA	El precio incluye IVA	El precio incluye IVA
Seguidores Mundiales	Seguidores Mundiales	Seguidores Mundiales	Seguidores Mundiales
Menos de 48h (Laborables)	Menos de 48h (Laborables)	Menos de 48h (Laborables)	Menos de 48h (Laborables)
Usuarios Reales	Usuarios Reales	Usuarios Reales	Usuarios Reales
Pago Seguro con PayPal	Pago Seguro con PayPal	Pago Seguro con PayPal	Pago Seguro con PayPal
100% Garantía de Devolución	100% Garantía de Devolución	100% Garantía de Devolución	100% Garantía de Devolución
COMPRAR AHORA	COMPRAR AHORA	COMPRAR AHORA	COMPRAR AHORA

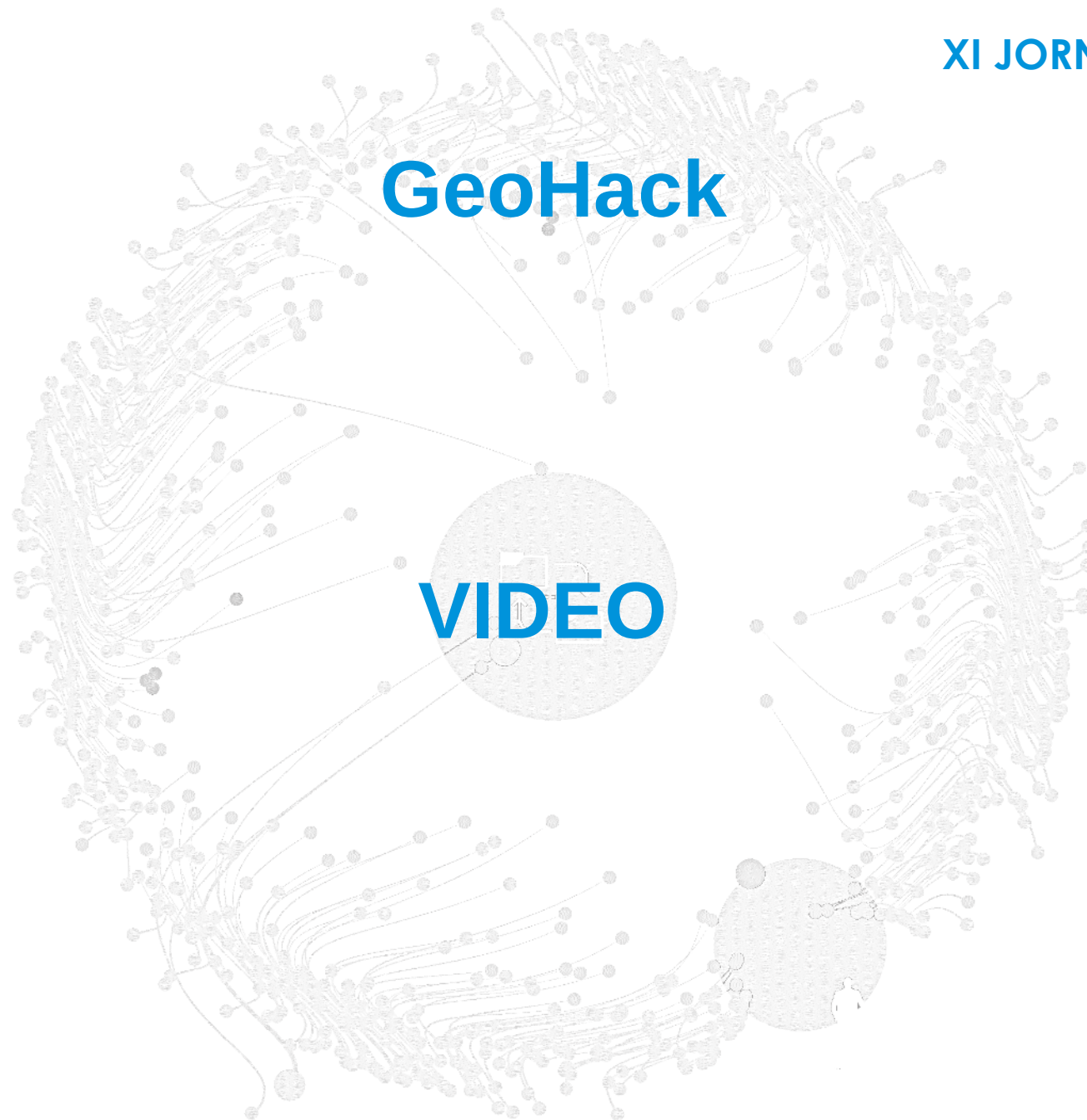
GeoHack

Descubrimiento de Vulnerabilidades con Bots

<https://geohack.kedarastudios.com/>



By @goldrak @interh4ck

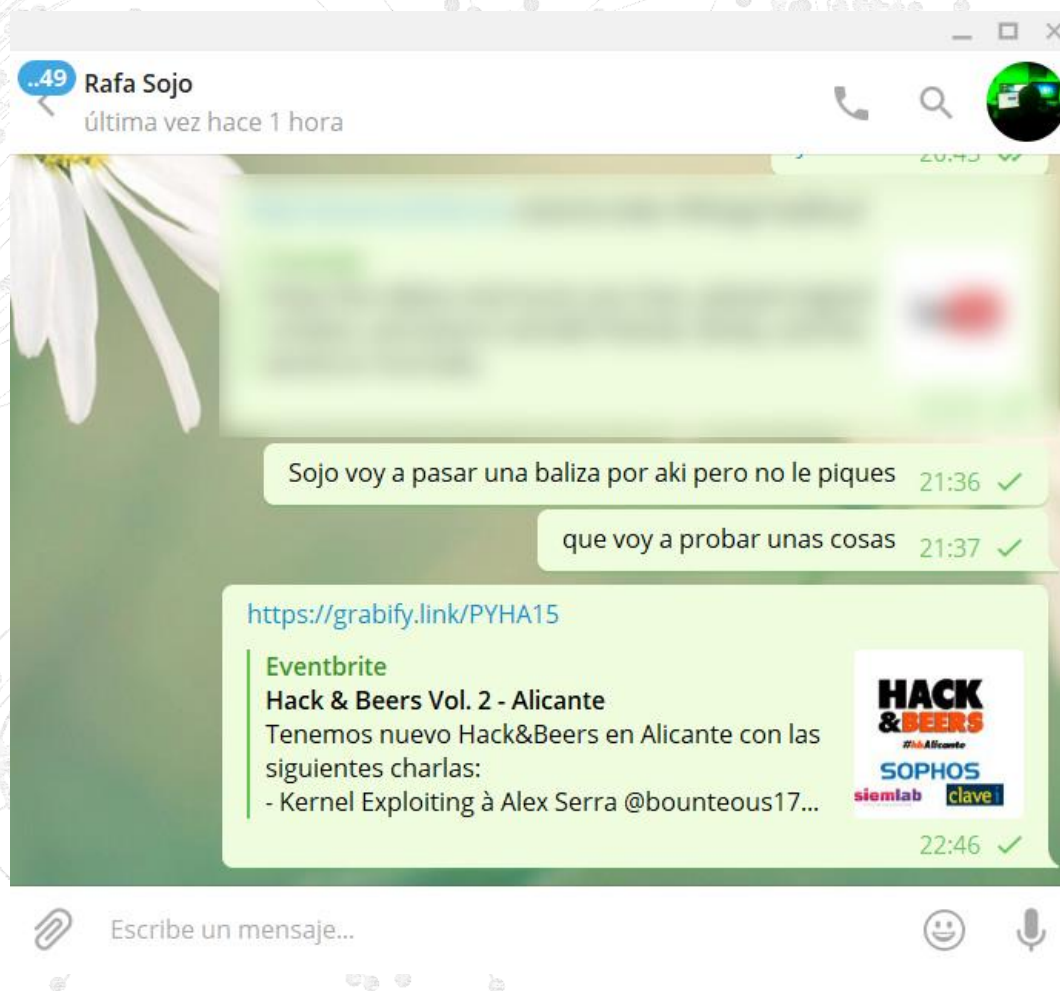


Análisis de Privacidad en Redes Sociales





Análisis de Privacidad en Telegram



Análisis de Privacidad en Twitter

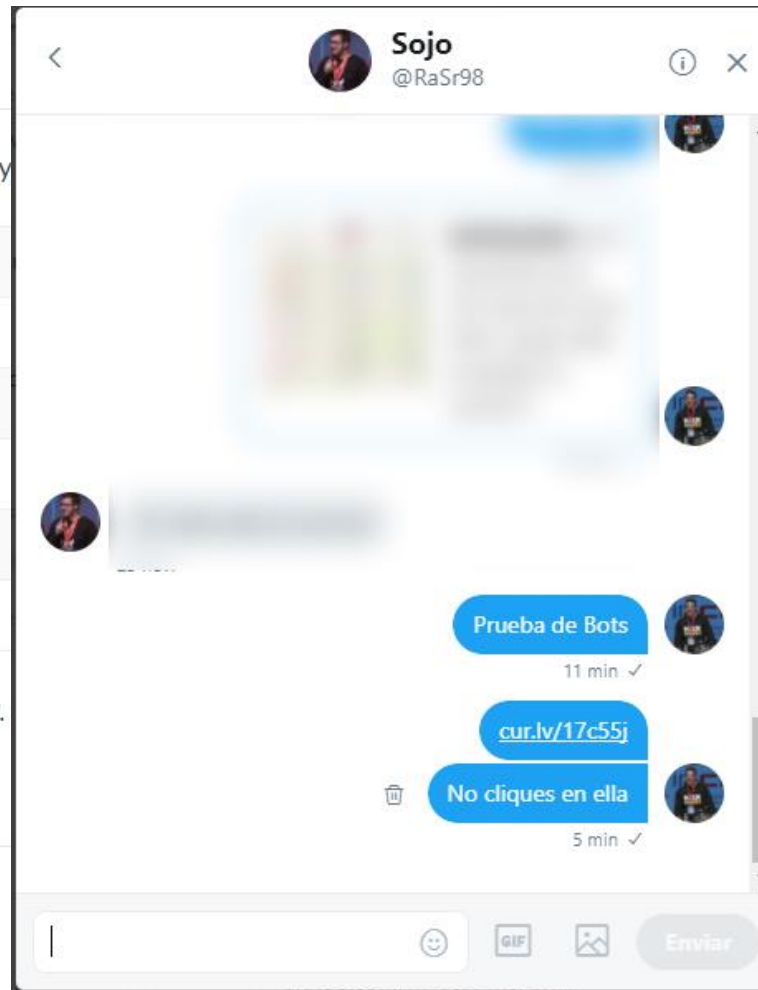
LINK SHORTENERS

Here are a list of link shorteners that you can use to help disguise y further

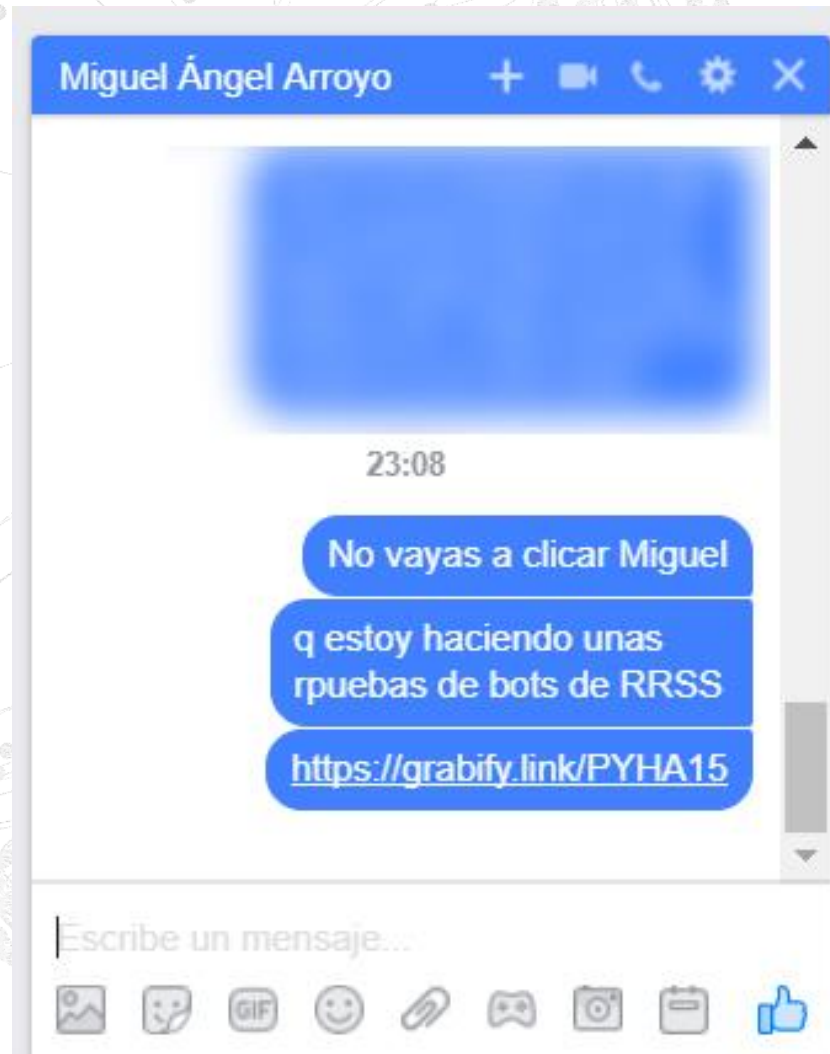
cur.lv	http://cur.lv/17c55j
shortest	http://ceesty.com/wyc4vx
adf.ly	http://yamechanic.com/BvKW
bit.ly *	
biturl.io	Loading...
rurl.co	Loading...

We do not have any affiliations with any of these link shorteners services provided.

*Some shortners may have bots show up in the logs such as bit.ly.



Análisis de Privacidad en Facebook





Análisis de Privacidad en LinkedIn

Manuel Camacho

Móvil • Hace 4 horas



Hoy

Buenas noches compi, no pinches en el link que estoy haciendo una prueba con BOTs

<https://grabify.link/PYHA15>

23:19

Leído 

Escribe un mensaje o adjunta un archivo

Análisis de Privacidad en Whatsapp





Análisis de Privacidad en Skype



Resultados del Análisis con Grabify

GRABIFY IP LOGGER

TOOLS ▾ LOGIN REGISTER

RESULTS: 10

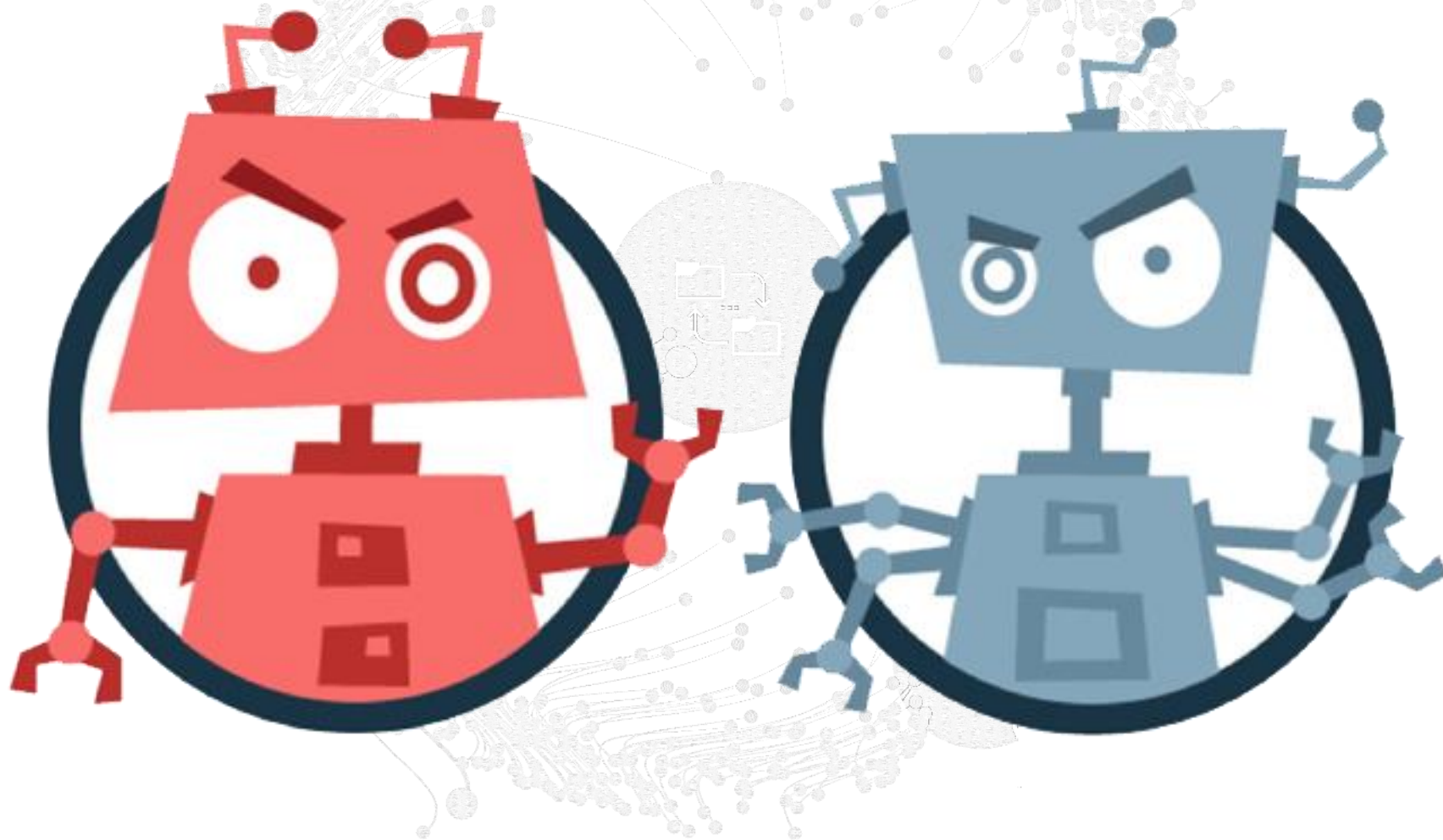
Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Pages: 1

Hide Bots ☐

Date/Time	IP Address	Country	User Agent (Hover or tap for more information)	Referring URL	Host Name	ISP
2017-11-26 21:46:57	149.154.167.170	United Kingdom	Bot: TelegramBot (like TwitterBot) 	no referrer	149.154.167.170	D2 Vishnevoe
2017-11-26 21:52:25	199.16.157.183	United States, San Francisco	Bot: Twitterbot/1.0 	no referrer	199.16.157.183	Twitter
2017-11-26 22:08:56	173.252.86.214	United States, Menlo Park	Bot: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)	no referrer	173.252.86.214	Facebook
2017-11-26 22:08:59	173.252.100.209	United States, Menlo Park	Bot: facebookexternalhit/1.1 	no referrer	173.252.100.209	Facebook
2017-11-26 22:09:01	173.252.121.114	United States, Menlo Park	Bot: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)	no referrer	173.252.121.114	Facebook
2017-11-26 22:09:04	173.252.98.215	United States, Menlo Park	Bot: facebookexternalhit/1.1 (+http://www.facebook.com/externalhit_uatext.php)	no referrer	173.252.98.215	Facebook
2017-11-26 22:19:53	108.174.2.205	United States, Mountain View	Bot: LinkedInBot/1.0 (compatible; Mozilla/5.0; Jakarta Commons-HttpClient/3.1 +http://www.linkedin.com) 	no referrer	108-174-2-205.fwd.linkedin.com	LinkedIn Corporation
2017-11-26 22:28:14	31.4.197.145	Spain, Málaga	WhatsApp/2.17.395 A 	no referrer	31-4-197-145.red-acceso.airtel.net	Vodafone Spain
2017-11-26 22:39:29	199.16.157.182	United States, San Francisco	Bot: Twitterbot/1.0 	no referrer	199.16.157.182	Twitter
2017-11-26 22:42:18	104.45.18.178	Netherlands, Amsterdam	Bot: Mozilla/5.0 (Windows NT 6.1; WOW64) SkypeUriPreview Preview/0.5 	no referrer	104.45.18.178	

Herramientas para la Creación de Bots

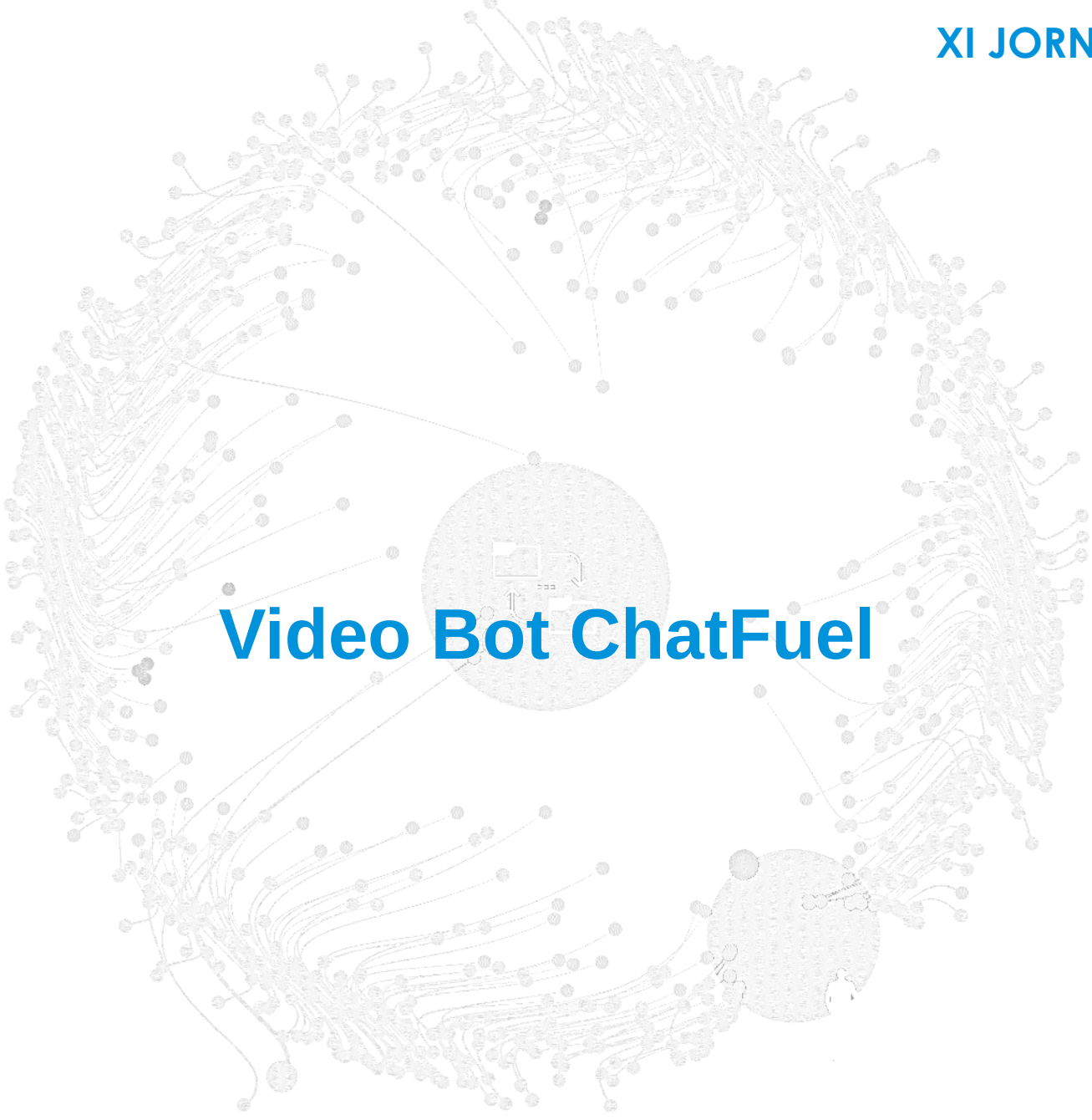


Herramientas para la Creación de Bots

RECETA 1

1. Crear Bot con BotFather **/newbot**
2. Asignar identificador y nombre al Bot.
3. Copiar **token** del Bot.
4. Añadir nuevo Bot a Chatfuel **/addbot**
5. Abrir Bot y crear la funcionalidad.

Chatfuel



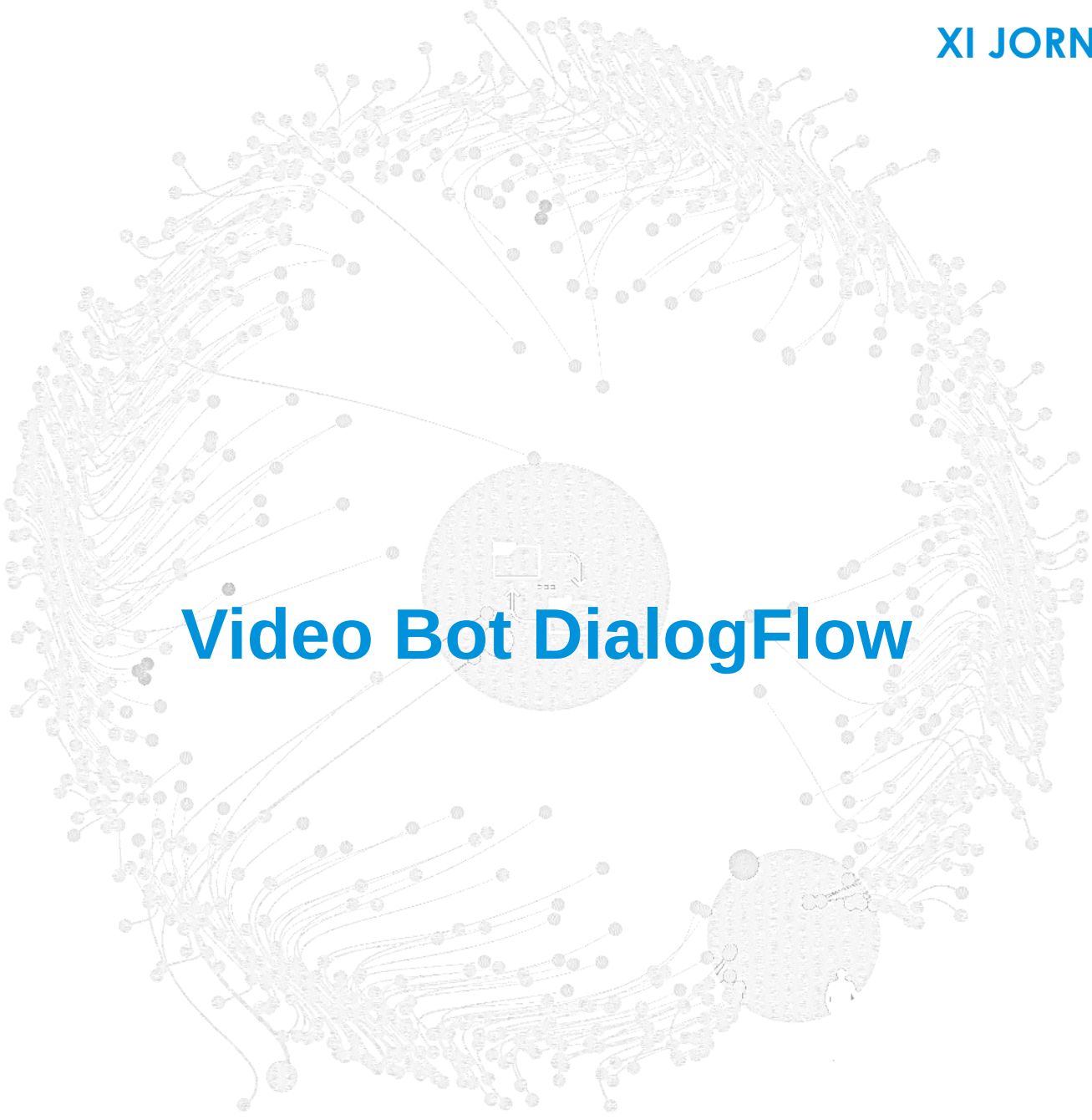
Video Bot ChatFuel

Herramientas para la Creación de Bots

RECETA 2

1. Crear Bot con BotFather **/newbot**
2. Asignar identificador y nombre al Bot.
3. Copiar **token** del Bot.
4. Crear un **agente** en Dialogflow
5. Integración de nuestro agente con Telegram (añadir token)
6. Añadir **contextos y acciones** al Bot





Video Bot DialogFlow

¿Cómo identificamos a los usuarios de Telegram?



Herramientas para la Creación de Bots

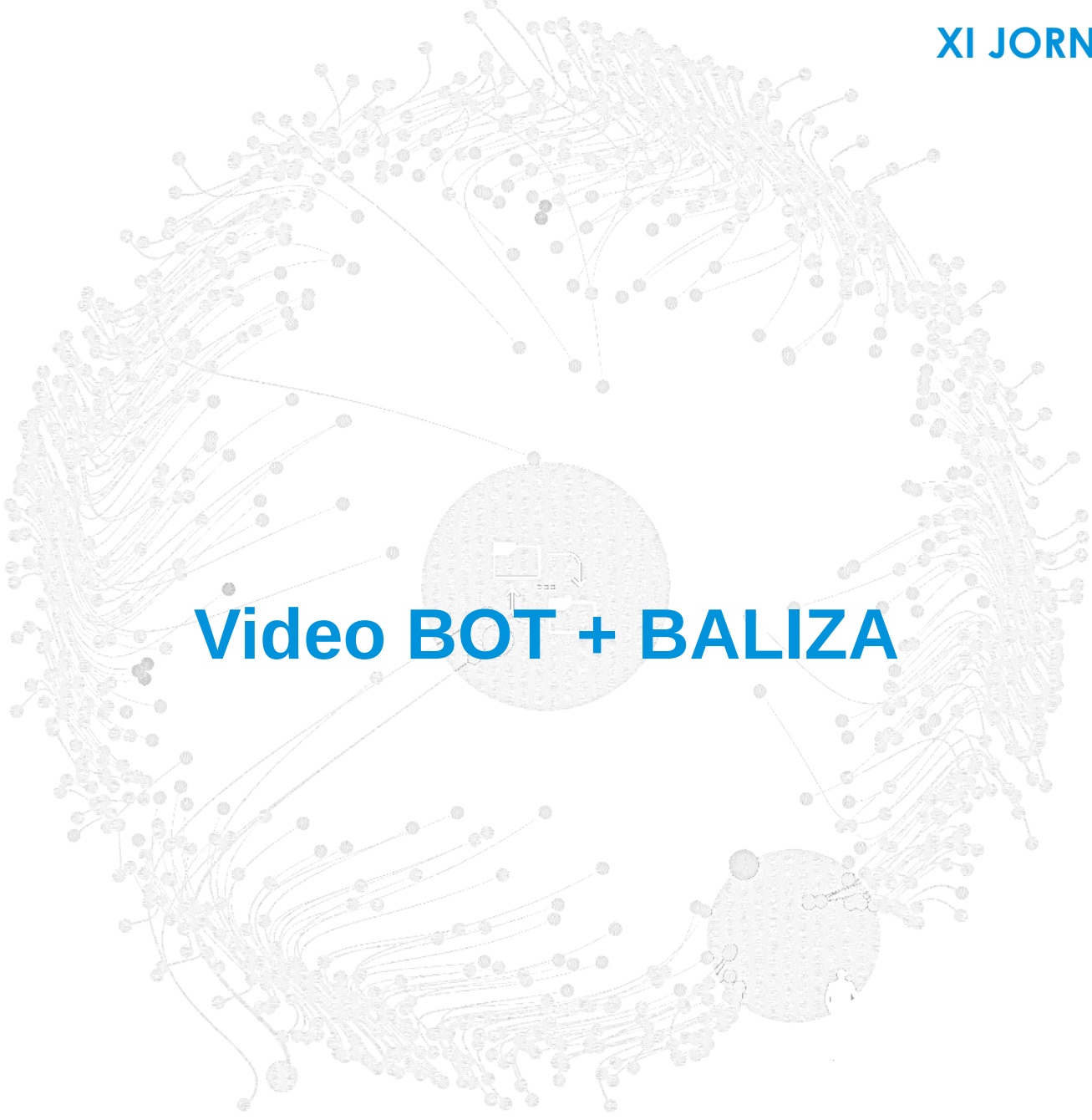
RECETA 3

BOT

+

BALIZA





Video BOT + BALIZA



Video AGRADECIMIENTOS