

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/339629744>

Manual de "Supervivencia" Hacker

Presentation · March 2020

DOI: 10.13140/RG.2.2.14621.05601/1

CITATIONS

7

READS

775

1 author:



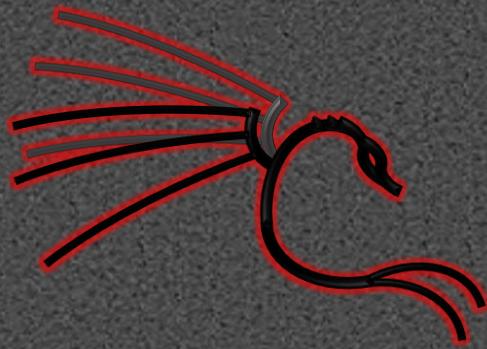
Jose Manuel Redondo

University of Oviedo

126 PUBLICATIONS 339 CITATIONS

SEE PROFILE

José Manuel Redondo López



Manual de Supervivencia Hacker

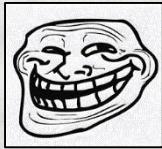
Cómo sobrevivir en la “jungla” de Internet sin (apenas)
conocimientos técnicos



ESCUELA DE INGENIERÍA
INFORMÁTICA

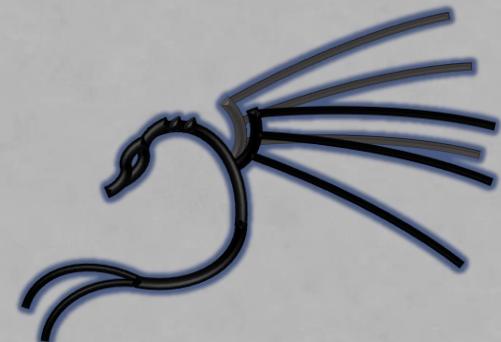
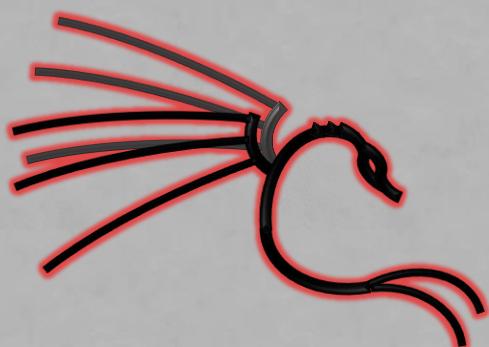


¿Pero, esto que es?

- Probablemente pienses que Internet es oscuro y lleno de terrores
- **¡Tienes razón!** 
- Pero hay una serie de cosas que puedes hacer para estar algo más seguro
 - Y, de paso, hacer que los demás lo estén
 - ¡Y no requiere (casi) conocimientos técnicos!
- **¡Vamos a ver qué son!**

Técnicas de “Defensa”

Como protegerme y/o saber si me ha pasado algo malo



A photograph of a young man with brown hair and a beard, wearing a blue and white plaid shirt. He is standing in a public space, looking over his right shoulder with a slightly surprised or confused expression. In the foreground, there are two women: one woman on the left is blurred, wearing a red sleeveless top; another woman on the right is clearer, wearing a light blue sleeveless top. The background is also blurred, showing other people and what might be a market or street scene.

**CUALQUIER OTRA
COSA**

YO

ACTUALIZACIONES

¡Actualiza por favor!

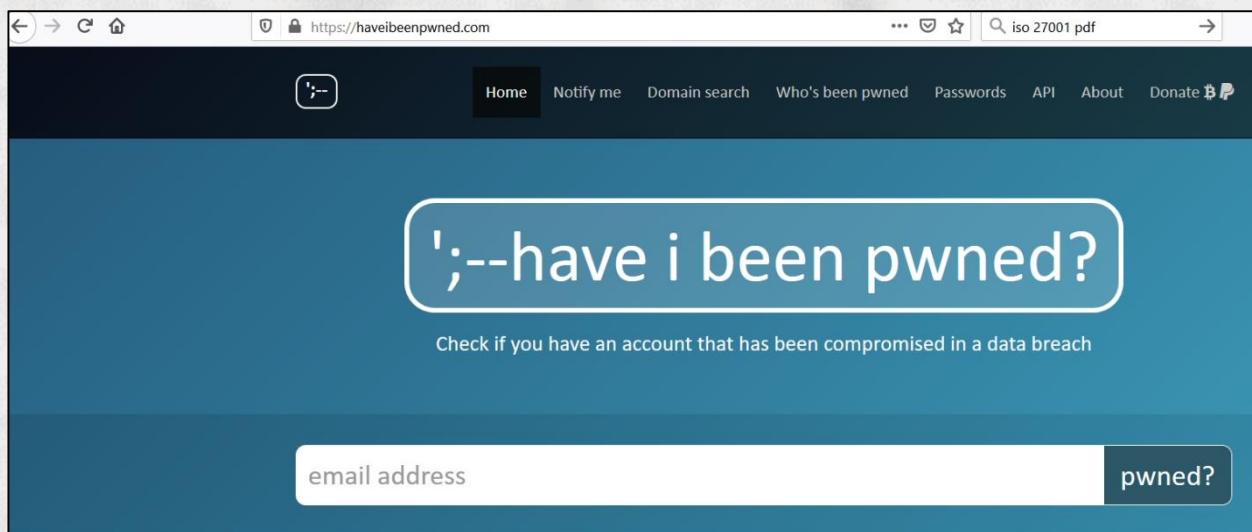
- Aunque lleva tiempo, es imposible medir la importancia de ejecutar programas actualizados para prevenir incidentes de seguridad
- **¡Especialmente navegadores web y sistemas operativos!**
- Sé que lleva tiempo, es una lata y obliga a reiniciar, pero de verdad que es muy importante
 - Es muy frecuente que nuevas vulnerabilidades solo afecten a versiones antiguas de los programas
 - ¡Sal del grupo de afectados! Las actualizaciones son como “vacunas” contra nuevos problemas
 - En Windows además, las actualizaciones también actualizan la base de datos del antivirus integrado

**CUANDO YA TIENES
EL PROBLEMA... Y NO
LO SABES**



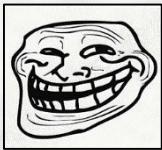
¿Me han robado alguna cuenta?

- Tus cuentas de email podrían haber sido ya comprometidas y no lo sabes
- Habitualmente por robos de datos en sitios web que las tienen guardadas como no deben
- Have I been pwned? (<https://haveibeenpwned.com/>) es un sitio en el que, si le das una cuenta de correo, te dice que contraseñas asociadas han sido robadas



Have I been pwned?

- ¡Genial! ¡Nuestro director no ha sido hackeado!
- ...que se sepa



@uniovi.es pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security [Start using 1Password.com](#)

Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.

Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.

Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

You have been pwned...

- Pero puede devolver que sí...
- Y en ese caso te dice en qué webs se encontraron tus cuentas, cuándo y por qué (el tipo de ataque)
- Y, en ese caso, es posible que tu clave esté circulando por sitios indebidos
- Y que, por tanto, entrarte en la cuenta sea cuestión de tiempo
- ¿Qué hago?

The screenshot shows the homepage of the 'Have I Been Pwned?' website. At the top, there's a navigation bar with links to Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is '';--have i been pwned?'. Below it, a sub-headline says 'Check if you have an account that has been compromised in a data breach'. A search bar contains a blurred email address, and a button next to it says 'pwned?'. The main content area has a red background. It displays the message 'Oh no — pwned!' and 'Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)'. There are buttons for 'Notify me when I get pwned' and 'Donate'. Below this, under 'Breaches you were pwned in', there are two entries: 'Dropbox' and 'last.fm'. Each entry includes a logo, a brief description of the breach, and a 'Compromised data' section. At the bottom, there are four summary statistics: 233 pwned websites, 4,729,225,727 pwned accounts, 54,390 pastes, and 51,474,803 paste accounts.

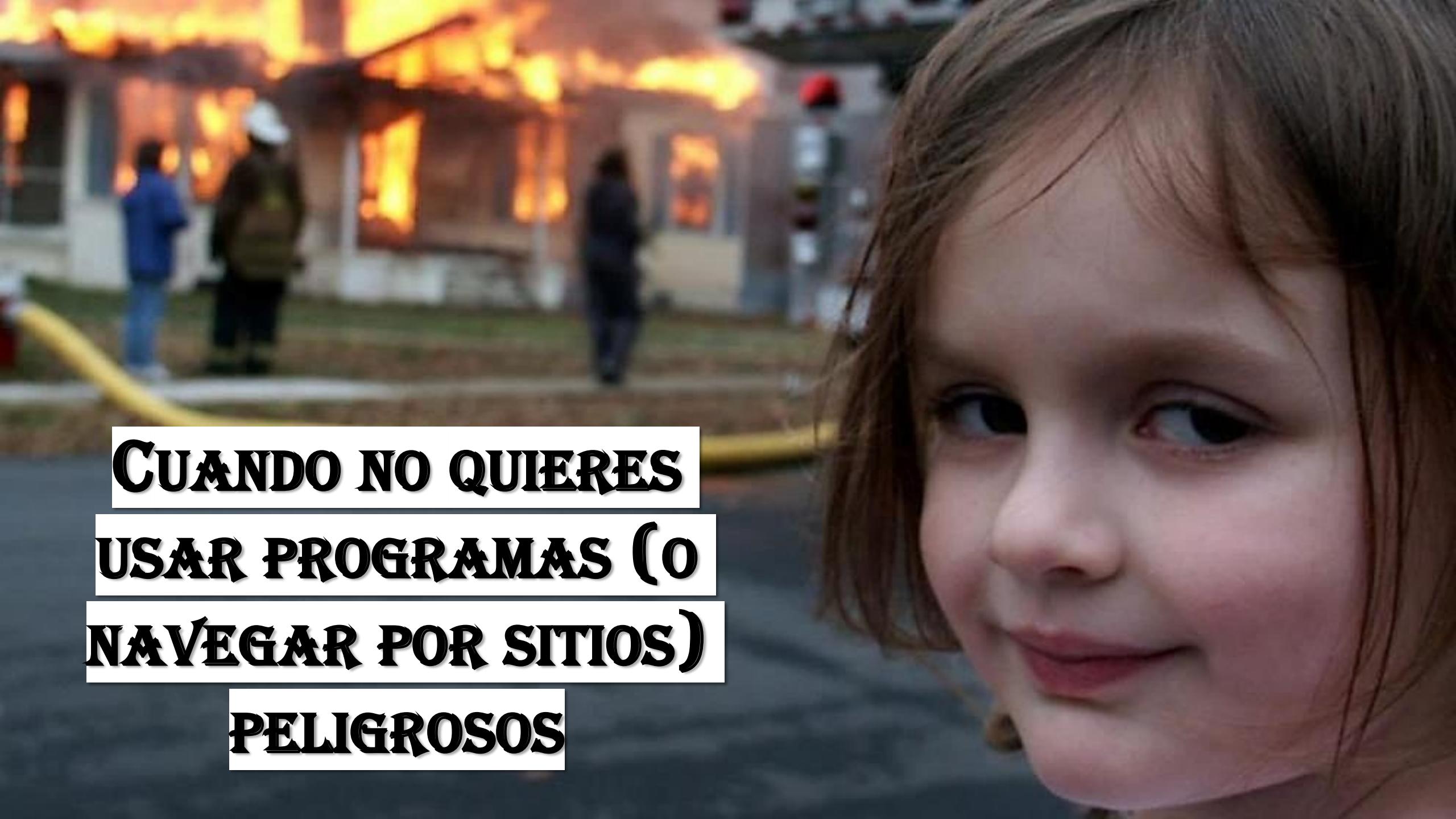
Category	Value
pwned websites	233
pwned accounts	4,729,225,727
pastes	54,390
paste accounts	51,474,803

Gestión de contraseñas

- **No uses la misma clave en todas partes**
 - Pero eso no lo haces, ¿verdad? 
- **Usa una contraseña segura**
 - Larga, que combine mayúsculas, minúsculas, números y otros caracteres (\$, %, &, @, ...)
 - No uses cosas que se puedan relacionar directamente contigo
 - **¿Y como sé si es o no segura?**
 - <https://password.kaspersky.com/es/>
- Activar un **segundo factor de autenticación** (Google Authenticator, etc.), usando el móvil preferentemente
 - Si un servicio lo ofrece, ¡es una forma muy buena de estar más seguro!
 - ¡Busca un tutorial oficial del servicio que lo ofrezca que quieras proteger y sigue sus pasos!



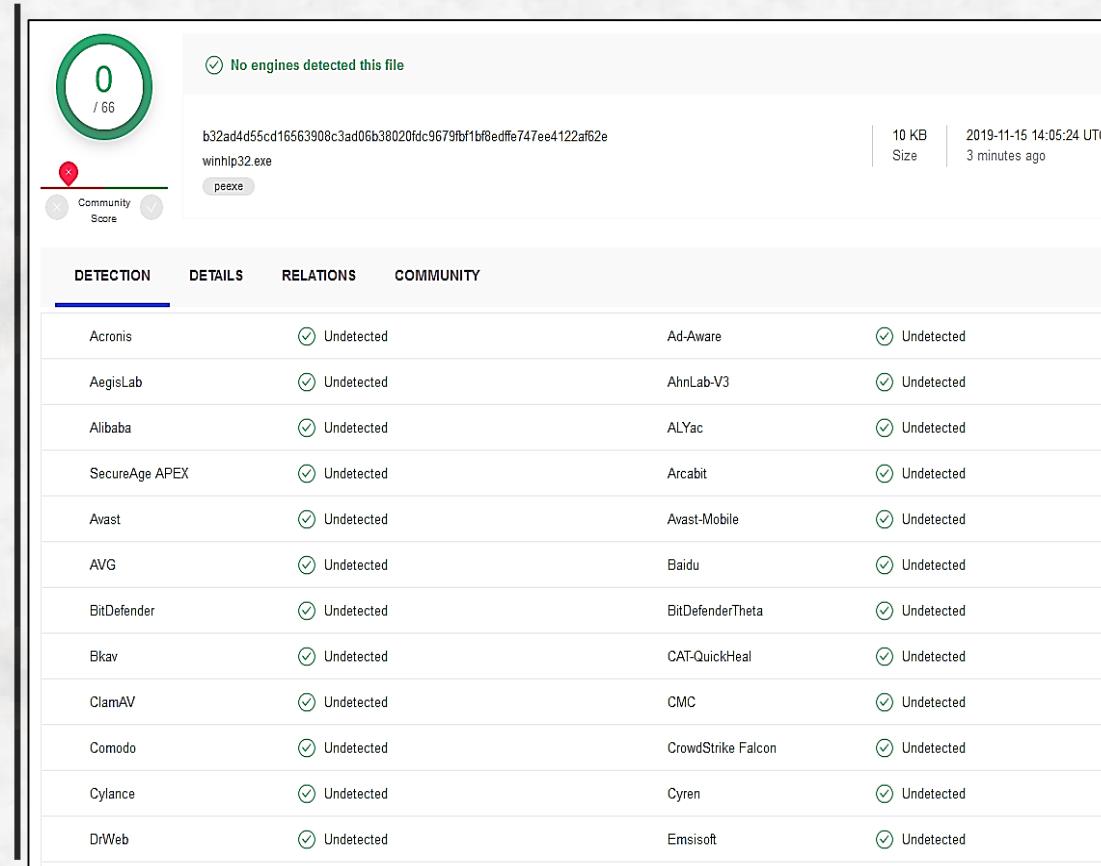
The screenshot shows a password strength check interface. At the top right is a small Spanish flag icon. The main title is "kaspersky SECURE PASSWORD CHECK". Below it is a yellow warning box containing a warning icon and the text: "Kaspersky no guarda ni almacena tus contraseñas" and "No introduzcas tu contraseña real. Este servicio solo tiene fines educativos." A red progress bar at the bottom is mostly red, with a small green section on the right end. To the right of the bar is a red square button with a white asterisk (*). Below the progress bar, a red warning icon points to the text "Contiene palabras muy usadas". Further down, the text "Tu contraseña puede ser descifrada con un ordenador común en" is followed by a large red box containing the text "327 SIGLOS". At the bottom, there is a green navigation bar with a left arrow, a circular icon with dots, and a right arrow. To the right of the navigation bar is the text "En ese tiempo puedes ir y volver a la Luna 1333 veces."



**CUANDO NO QUIERES
USAR PROGRAMAS (o
NAVEGAR POR SITIOS)
PELIGROSOS**

¿Es este programa seguro?

- Como norma general, **bájate siempre programas de sitios oficiales**
- Si aún así tienes dudas, pásale tu antivirus
- Si aún así tienes dudas, pásale 50+ antivirus
 - :O ¿eso se puede hacer? ¡SÍ!
 - Virustotal es un servicio en línea (<https://www.virustotal.com/gui/home/upload>) que analiza cualquier archivo que se le envíe en busca de malware conocido
 - Si pasas sus 50+ antivirus es más probable que el ejecutable no tenga “bichos” ☺
- **¡Los documentos (Office, PDF...) también pueden ser peligrosos!**
¡Mándalos a este servicio también!



The screenshot shows the VirusTotal analysis interface for a file named 'winhlip32.exe'. The main summary indicates a score of 0/66 with a green circle, and a note that 'No engines detected this file'. The file's SHA256 hash is listed as 'b32ad4d55cd16563908c3ad06b38020fdc9679fbf1bf8edfe747ee4122af62e'. The analysis was completed 3 minutes ago at 2019-11-15 14:05:24 UTC, with a file size of 10 KB. Below this, a table lists 50 different antivirus engines, all of which reported the file as 'Undetected'.

Detection Engine	Details	Community
Acronis	Undetected	Ad-Aware
AegisLab	Undetected	AhnLab-V3
Alibaba	Undetected	ALYac
SecureAge APEX	Undetected	Arcabit
Avast	Undetected	Avast-Mobile
AVG	Undetected	Baidu
BitDefender	Undetected	BitDefenderTheta
Bkav	Undetected	CAT-QuickHeal
ClamAV	Undetected	CMC
Comodo	Undetected	CrowdStrike Falcon
Cylance	Undetected	Cyren
DrWeb	Undetected	Emsisoft

¿Es esta web segura?

- Al navegar uno puede tener dudas de si una web es o no segura
- Google Safe Browsing escanea billones de URL para localizar sitios web inseguros
 - Descubre miles de nuevos sitios inseguros todos los días, muchos de los cuales son sitios web legítimos que han sido hackeados
 - Cuando detecta sitios web no seguros, muestra advertencias en la página de búsqueda de Google y en los navegadores web que utilizan esta tecnología
- ¡Pero podemos usarlo para saberlo nosotros mismos sobre sitio que queramos!
 - <https://transparencyreport.google.com/safe-browsing/search>
- ¡Nuestra universidad es segura! ¡bien!

The screenshot shows a search interface for checking website security. At the top, it says "Comprobar el estado de un sitio web". Below that is a search bar containing the URL "www.uniovi.es". To the right of the search bar is a magnifying glass icon. A green horizontal bar labeled "Estado actual" spans most of the width. Below this bar, there is a green checkmark icon followed by the text "No se ha detectado contenido no seguro".

¿Es esta web segura?

- ¡No es suficiente! ¡No me fio de Google!
- Si quieres una segunda opinión puedes, con la comprobación de URL de Virustotal
 - ¡No solo analiza programas!
- Se pone una URL aquí y se mira qué nos dice
 - <https://www.virustotal.com/gui/home/url>

The screenshot shows the Virustotal URL analysis interface. At the top, it displays a green circle with a score of 0 / 71 and the message "No engines detected this URL". Below this, the URL <http://www.uniovi.es/> and the domain www.uniovi.es are shown. To the right, there are status indicators: 200 Status, text/html; charset=UTF-8 Content Type, and 2019-10-26 05:25:36 UTC Date. A "Community Score" is also present. The main area is a table titled "DETECTION DETAILS COMMUNITY" with 15 rows, each listing a different security engine and its result (all are "Clean").

DETECTION	DETAILS	COMMUNITY
ADMINUSLabs	<input checked="" type="checkbox"/> Clean	AegisLab WebGuard <input checked="" type="checkbox"/> Clean
AlienVault	<input checked="" type="checkbox"/> Clean	Antiy-AVL <input checked="" type="checkbox"/> Clean
Avira (no cloud)	<input checked="" type="checkbox"/> Clean	BADWARE.INFO <input checked="" type="checkbox"/> Clean
Baidu-International	<input checked="" type="checkbox"/> Clean	BitDefender <input checked="" type="checkbox"/> Clean
Blueliv	<input checked="" type="checkbox"/> Clean	CLEAN MX <input checked="" type="checkbox"/> Clean
Comodo Site Inspector	<input checked="" type="checkbox"/> Clean	CRDF <input checked="" type="checkbox"/> Clean
CyberCrime	<input checked="" type="checkbox"/> Clean	CyRadar <input checked="" type="checkbox"/> Clean
desenmascara.me	<input checked="" type="checkbox"/> Clean	DNS8 <input checked="" type="checkbox"/> Clean
Dr.Web	<input checked="" type="checkbox"/> Clean	Emsisoft <input checked="" type="checkbox"/> Clean
EonScope	<input checked="" type="checkbox"/> Clean	ESET <input checked="" type="checkbox"/> Clean
ESTsecurity-Threat Inside	<input checked="" type="checkbox"/> Clean	Forcepoint ThreatSeeker <input checked="" type="checkbox"/> Clean
Fortinet	<input checked="" type="checkbox"/> Clean	FraudScore <input checked="" type="checkbox"/> Clean
FraudSense	<input checked="" type="checkbox"/> Clean	G-Data <input checked="" type="checkbox"/> Clean

**CUANDO DECIDES QUE
BASTA YA DE ANUNCIOS
O DE MOLESTIAS AL
NAVEGAR**



¿Cómo puedo navegar con menos riesgo?

© José Manuel
Redondo López

- La gran mayoría de páginas web se financian a través de anuncios
- Esto no sería malo si no fuese porque...
 - Algunos son realmente molestos
 - Otros hacen que navegar sea mucho más lento
 - A veces, incluso son maliciosos
- Hay plugins para bloquearlos, y uno de los más usados es **Adblock Plus**
 - Disponible para Firefox y Chrome
 - Ojo, ¡no te bajes imitaciones o fakes! (mira autor, valoración, nº de descargas...)
- No es el único, pero hace bien su trabajo y es el que uso yo ☺

 **Adblock Plus - bloqueador de anuncios gratis** 

Bloquea los anuncios en YouTube™ y las ventanas emergentes, y combate los programas maliciosos.

[Detalles](#) [Permisos](#)

Get the free ad blocker for Firefox. With almost 500 million downloads to date!

✓ Block annoying ads and popups
✓ Block video ads on sites like YouTube
✓ Speed-up loading time on pages
✓ Reduce risk of "malvertising" infections
✓ Protect your privacy by stopping trackers from following your online activity
✓ Block social media icons tracking

The ad blocker's additional features enable you to easily support your favorite websites by whitelisting them, to add or create your own filters, and to block social media icons tracking.

Adblock Plus supports the Acceptable Ads initiative. Acceptable Ads are shown by default, which helps support websites that rely on advertising revenue but choose to only display nonintrusive ads. This can be disabled at any time for users who wish to block all ads. The initiative allows content producers to receive monetization for their work and helps create an environment of fairness and sustainability for user, advertiser, and creator alike. Learn more

By downloading and installing this extension, you agree to our [Terms of Use](#) and our [Privacy Policy](#).

Permitir actualizaciones automáticas Predeterminado Activado Desactivar

Ejecutar en ventana privada Permitir No permitir
Cuando está activada, la extensión tendrá acceso a todo lo que haces mientras navegas de forma privada. [Descubre más](#)

Autor [Adblock Plus](#)

Versión 3.8

¿Cómo puedo navegar con menos riesgo?

© José Manuel
Redondo López

- Navegar es un problema no solo por los anuncios, también **por los contenidos**
- Muchas webs usan un lenguaje de programación llamado Javascript para mostrar elementos
 - Tiene usos 100% legítimos
 - Pero también puede usarse para saber qué webs visitas, engañarte, mostrar anuncios, contenidos falsos o maliciosos...
 - Puede hacer que navegar sea más lento
- Un plugin que bloquea esto es Noscript
 - Para Firefox y para Chrome
 - Bloquea también otros ataques

The screenshot shows the configuration page for the NoScript extension. At the top, there's a header with the NoScript logo, a toggle switch, and three dots. Below the header, a paragraph explains that NoScript provides maximum protection by only allowing active content from domains you trust. It highlights its award-winning status and its ability to mitigate vulnerabilities like Spectre and Meltdown.

Below the paragraph are tabs for "Detalles", "Permisos", and "Notas de la versión". The "Permisos" tab is selected. It contains sections for "Winner of the 'PC World - World Class Award'" and "It protects your 'trust boundaries'". There's also a note about its preemptive approach preventing exploitation of security vulnerabilities.

Under the "Permisos" tab, there's a "FAQ" link (<https://noscript.net/faq>) and a "Forum" link (<https://noscript.net/forum>). A "A Basic NoScript 10 Guide" section is also present.

At the bottom of the main content area, there's a message from the developer asking for contributions: "El desarrollador de este complemento solicita que ayudes a continuar su desarrollo haciendo una pequeña contribución." To the right of this message is a "Colaborar" button with a heart icon.

Below the main content, there are two sections with radio buttons:

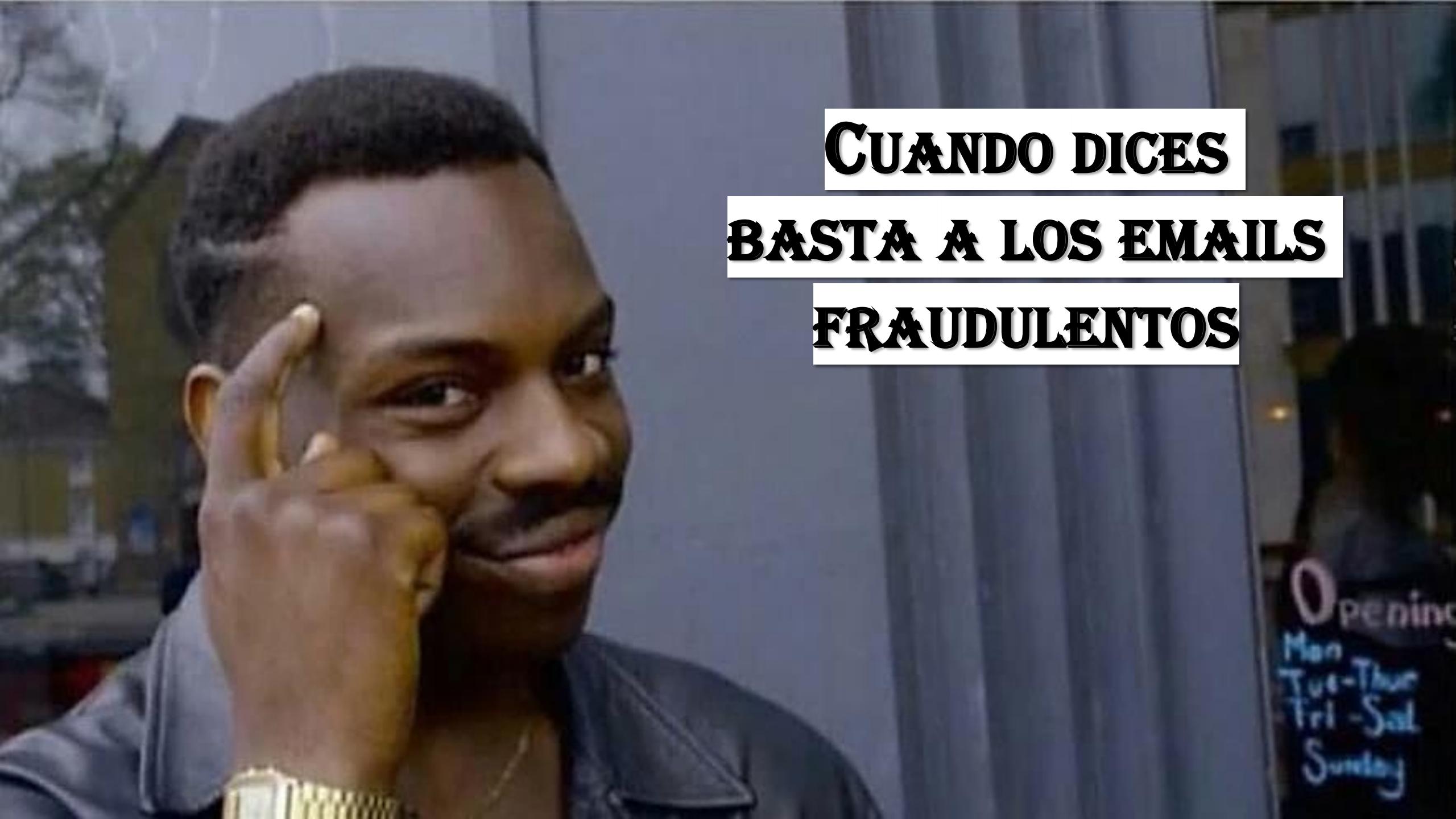
- "Permitir actualizaciones automáticas": Predeterminado Activado Desactivar
- "Ejecutar en ventana privada": Permitir No permitir

At the very bottom, there are "Autor" and "Giorgio Maone" fields.

¿Cómo puedo navegar con menos riesgo?

- Pero hay que “entrenarlo”
 - Al ir a una página, se cargan muchas otras secundarias mediante scripts
 - El plugin lista todas y bloquea la mayoría
 - Como consecuencia, seguramente la página se vea mal o falten trozos
 - Así que miramos la lista haciendo clic en su icono y empezamos a desbloquear las que suenan menos “sospechosas”
 - Hasta que veamos el contenido de la página que queremos ver
 - El plugin **recuerda** esta selección para siempre
 - ¡Solo hay que hacerlo 1 vez por página!

X	C	Q	S!	!	!	!	!
🚫	🚫	🚫	🔒	...	youtube.com		
🚫	🚫	🚫	🔒	...	gstatic.com		
🚫	🚫	🚫	🔒	...	ytimg.com		
🚫	🚫	🚫	🚫	...	adslzone.net		
🚫	🚫	🚫	🚫	...	ad-delivery.net		
🚫	🚫	🚫	🚫	...	addthis.com		
🚫	🚫	🚫	🚫	...	addthisedge.com		
🚫	🚫	🚫	🚫	...	btserve.com		
🚫	🚫	🚫	🚫	...	cdnjquery.com		
🚫	🚫	🚫	🚫	...	consensu.org		
🚫	🚫	🚫	🚫	...	disqus.com		
🚫	🚫	🚫	🚫	...	disquscdn.com		
🚫	🚫	🚫	🚫	...	disqusservice.com		
🚫	🚫	🚫	🚫	...	doubleclick.net		
🚫	🚫	🚫	🚫	...	facebook.com		
🚫	🚫	🚫	🚫	...	facebook.net		
🚫	🚫	🚫	google-analytics.com		
🚫	🚫	🚫	google.com		
🚫	🚫	🚫	google.es		
🚫	🚫	🚫	googletagmanager.com		
🚫	🚫	🚫	googletagservices.com		
🚫	🚫	🚫	gstatic.com		
🚫	🚫	🚫	marfeel.com		
🚫	🚫	🚫	marfeelcache.com		
🚫	🚫	🚫	moatads.com		
🚫	🚫	🚫	moonmail.io		
🚫	🚫	🚫	onesignal.com		
🚫	🚫	🚫	re2sync.com		

A black and white photograph of a man in a dark suit and tie, holding a briefcase. He is looking slightly to the right with a thoughtful expression, his right hand resting against his chin. The background is a blurred indoor setting.

CUANDO DICES
BASTA A LOS EMAILS
FRAUDULENTOS

¿Me puedo fiar de los emails que me llegan?

- Los correos falsos son una plaga, y tenemos que aprender a defendernos
- Hay que practicar estos 10 “mandamientos”
 1. **Nunca te fíes del nombre del remitente:** mira el email
 - Aún así podría falsificarse,
 - Hay virus que mandan emails en nombre de usuarios cuyas máquinas están infectadas
 - ¿Es de alguien famoso? Elimínalo (salvo que tu también lo seas y le conozcas ☺)
 2. **Mira, pero no cliques:** Si acercas el ratón a un enlace/botón verás en la barra de abajo del navegador la dirección a la que apunta
 - Si no es la misma que la del enlace que ves, es muy mala señal (¡no clickes!)
 3. **Errores gramaticales obvios:** Spam casi con 100% de probabilidad
 4. **Cómo te saluda:** Si el saludo es generalista (“Querido cliente”), mala señal
 5. **Te pide información personal:** Una empresa/banco **NUNCA** te va a pedir información privada (cuentas bancarias, claves, nombres de usuario, nºs de tarjetas de crédito...) por email
 - ¡El email es un medio inseguro!

¿Me puedo fiar de los emails que me llegan?

6. **¿Es algo urgente?** Mala señal
 - Si te piden algo comprometedor para ya, es para que lo hagas sin pensar
7. **Mira la firma del email:** Un emisor real suele firmar los emails de forma correcta
 - Si no lo hace, tampoco quiere decir nada...
8. **¡OJO CON LOS ADJUNTOS!:** La mayoría de emails maliciosos intentan que abras el adjunto porque ahí está lo que hace daño
 - ¿Facturas? ¿Multas? ¿Problemas con cartas/paquetes? ¿Documentos del banco?... **NO LO ABRAS** y compruébalo por teléfono con la empresa real
9. **Sospecha:** Observa y ante el mínimo indicio de algo raro, no te fíes
 - ¿Te pide cometer un delito? Elimínalo
 - ¿Te pide ayuda con una transferencia bancaria? Elimínalo
 - ¿Te pide confirmar una transacción pero tu no la recuerdas? Elimínalo y vete a la página oficial
 - ¿Tienes algo a la venta y quiere comprarlo, pero vive en el extranjero y te cuenta una película? Timo, elimínalo
 - ¿Se muestra interesado en ti porque ha visto una foto tuya en un perfil público? Timo típico, elimínalo
 - ...
10. **Si tienes dudas,** consulta con un experto
 - O bórralo, mejor prevenir que lamentar ☺

Amazon Update <AmazonUpdate@efficaciousrbays.xyz>
to me ▾

⚠ Why is this message in Spam? It's similar to messages that were detected by our spam filters. Learn more

amazon.com Prime
The Amazon Marketplace

-SHOPPER/MEMBER:4726

-DATE-OF-NOTICE: 12/22/2015

Hello Shopper [REDACTED] @gmail.com! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with \$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this \$100 reward, simply go below to get your coupon card and then just use it during checkout on your next purchase. That's all there is to it!

[Please visit here now to get your reward](#)

***DON'T WAIT! The Link Above Expires on 12/28!

Jpmorgan Chase <H.J.Bongartz@t-online.de>
3/30/2019 12:13 PM

To: smrfs@emailonline.chase.com

The picture can't be displayed.

Chase : Important notification regarding your chase bank debit/credit/ATM/Prepaid Card.

Dear Customer

As part of our security commitment to safeguard your online banking transactions and activities, this notification is to confirm that you or an authorized party used your account information's for online transactions using your chase debit/credit card details.

To view and confirm this transaction, kindly click the button below

[View all Transactions](#)

Chase Card Services
Email Operations Team

MARK ZUCKERBERG
WINNING AMOUNT

Reply-To: MARK ZUCKERBERG

WINNING AMOUNT

My name is Mark Zuckerberg, A philanthropist the founder and CEO of the social-network's youngest billionaires and Chairman of the Mark Zuckerberg Charitable Foundation. I believe strongly in giving while living! I had one idea that never changed help people and i have decided to secretly give (\$1,500,000.00) to randomly select you should count yourself as the lucky individual. Your email address was chosen at your earliest convenience, so I know your email address is valid. (mzuckerberg) to know more about me: https://en.wikipedia.org/wiki/Mark_Zuckerberg/ or you can

Regards,
MARK ZUCKERBERG

PayPal

Check your recent activity and update your informations

Hello PayPal User,

Check your recent activity by logging in now. We have detected different logins to your account from different country

Ip logging :	country:	Statement Date:
95.108.142.138	Russia	28 November 2016

What you do?

Open your account by clicking the "login" button, and remember to update your information after logging in. We will give you 3 days to update your information or we will suspend your account forever.

If you receive this email in the SPAM folder, click on "Not Spam" button to fix it.

[Login and update your informations](#)

Naomi Surugaba [azlin@moa.gov.my]
Inbox
Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,

I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.

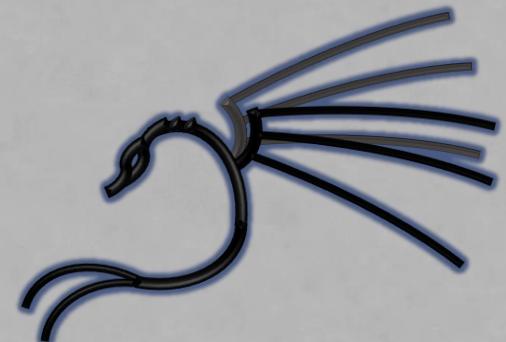
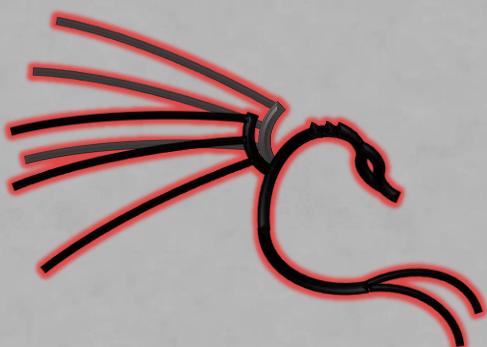
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli. Meanwhile before the incident, my late Father came to Cotonou Benin Republic with the sum of USD4, 200,000.00 (US\$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.

I am here seeking for an avenue to transfer the fund to you in only you're reliable and trustworthy person to invest the fund. I am here in Benin Republic because of the death of my parent's and I want you to help me transfer the fund into your bank account for investment purpose.

Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent's. Reply to my alternative email: missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated. Remain blessed,
Miss Naomi Surugaba.

Técnicas de “Ataque”

Realmente no ☺, pero verás las web con “ojos de hacker”



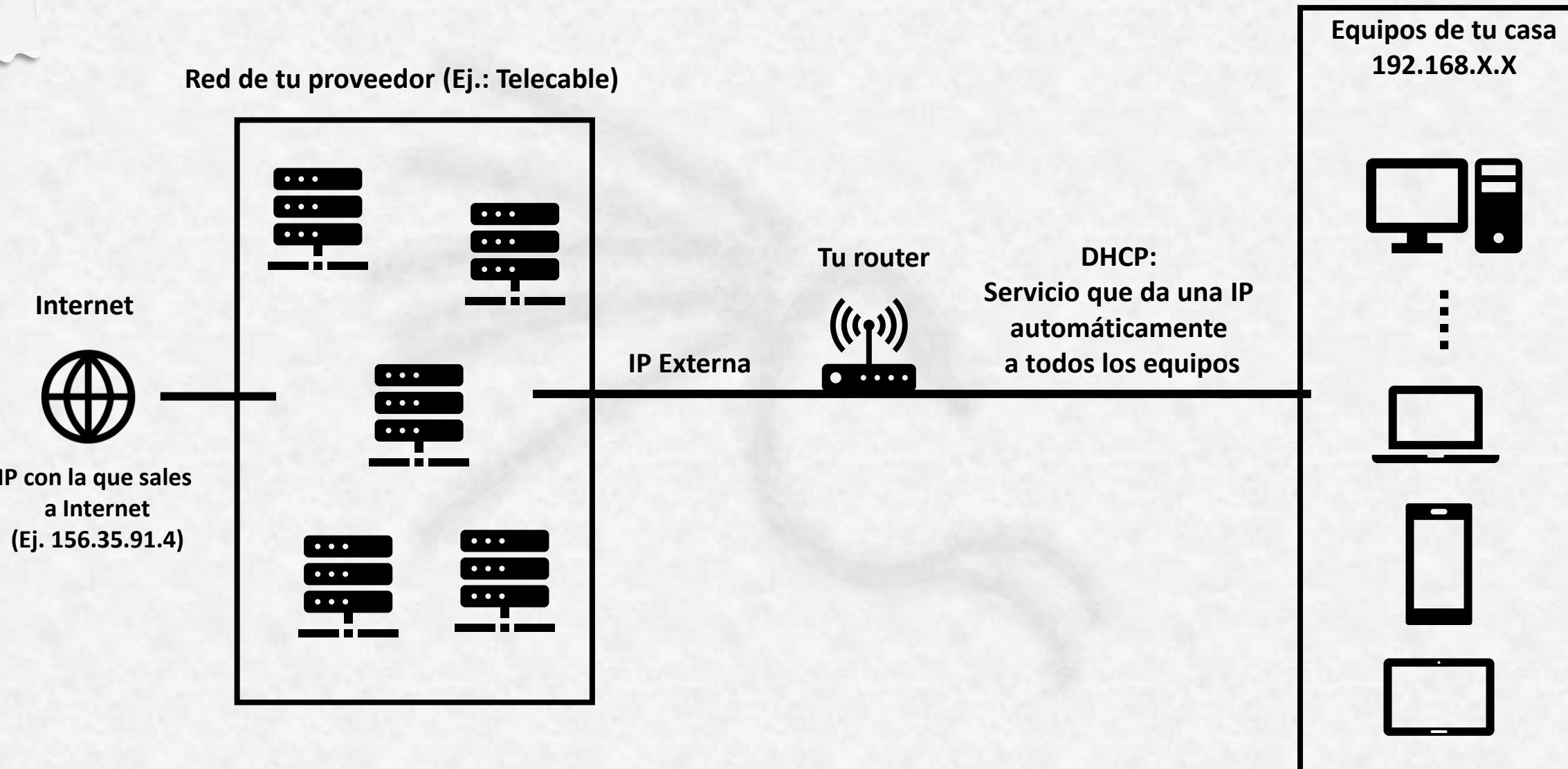
IP y DNS

- Para entender el resto de esta presentación tienes que saber una serie de cosas
 - Toda máquina en Internet del mundo tiene una **IP única** (como el DNI)
 - Tradicionalmente es un conjunto de nºs, típicamente 4 entre 0 y 255 (Ej.: 192.168.34.1)
 - Como recordar esto es imposible para todas las máquinas, se usa en su lugar un nombre simbólico
 - Ej.: www.ingenieriainformatica.uniovi.es
 - Y el **servicio DNS** se encarga de que, cada vez que tu pones un nombre de una web, automáticamente se obtenga la IP correspondiente y se vaya al sitio correcto
 - Navegar por Internet implica que se hacen estas traducciones automáticamente sin que te enteres ☺

Internet en casa: como se suele instalar

- En una empresa o institución, las cosas son más o menos así
- Pero en un hogar, la cosa es ligeramente diferente
 - Te dan un aparato (router) al que conectas cualquier cosa capaz de usar Internet (PC, teléfono, Tablet, TV, Playstation, XBox, Switch...)
 - Este router le da a cada aparato una IP privada, que solo vale para los equipos de tu casa
 - Cuando uno quiere “salir afuera”, traduce esa IP a la IP única que has contratado para salir a Internet
 - Quizá tu proveedor haga más traducciones intermedias...pero tú no lo sabes ☺
 - De esta forma tú contratas una IP pero puedes conectar N dispositivos a Internet con ella
 - Sin embargo, para el exterior, todos tus equipos tienen la misma IP
 - Pero el router no es tonto y sabe a quien mandar las respuestas que le llegan a cada uno por separado
 - Esta traducción se llama NAT (por si lo has visto en algún sitio)

Internet en casa: como se suele instalar



Sobre lo que vamos a ver a continuación...

- Averiguar información pública de una web en sí no es delito
 - Es saber mirar mejor lo que recibes en el navegador
- Pero lo que hagas con esa información, **sí puede serlo (y penal, es decir, cárcel)**
 - Acceder a sistemas/datos sin consentimiento del propietario
 - Divulgar la información comprometedora que has encontrado
 - ...
- Por tanto, **NO hagas estas cosas sin autorización previa y por escrito de los propietarios**
 - O salvo que el sistema sea tuyo o de un familiar que te autorice a examinarlo
- Es mejor que tú encuentres un problema con buena fe antes que un criminal...
 - ...pero **sólo si cuentas con la debida autorización (o es tuyo)**
 - Porque, de no hacerlo, y de acuerdo a la ley vigente, **tú eres el criminal ☹ (¡aunque tu intención sea la mejor de todas!)**

¡Me dijiste que me harías famosa en Internet!



Y ahora todo el mundo sabe dónde están tus dispositivos...



Shodan

- Shodan (<http://www.shodanhq.com/>) es un motor de búsqueda capaz de encontrar dispositivos en Internet: routers, servidores, cámaras, semáforos, impresoras...
 - Revela qué tipo de servicio/aparato es, su versión, etc.
 - Información que se puede usar para encontrar problemas relacionados con los mismos o si representan un peligro, ya que tienen software al que se puede acceder, y por lo tanto atacar
- Localizarlos es legal, entrar en ellos NO
- ¿Qué puedo hacer con esto entonces?
 - Si tienes equipos propios / un familiar con una empresa / alguien que te deja hacerlo, pídele su IP o la URL de su web
 - Mira si encuentras dispositivos expuestos asociados a la misma, pero no entres en ellos
 - Avísale, no vaya a ser que haya algo que no debería estar público
- Más información:
 - <https://danielmiessler.com/study/shodan/>
 - <https://hacking-etico.com/2016/02/12/4979/>

The search engine for **Webcams**
Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Shodan Developers Book View All... apache

SHODAN

Explore Enterprise Access Contact Us

New to Shodan? Login or Register

Explore the Internet of Things

Monitor Network Security

See the Big Picture

Get a Competitive Advantage

56% of Fortune 100

Shodan is used around the world by

TOTAL RESULTS: 14,301,988

RELATED TAGS: web servers

TOP COUNTRIES:

Country	Count
United States	4,755,632
Mexico	1,234,983
China	1,051,604
Germany	1,044,601
Japan	896,419

TOP SERVICES:

Service	Count
HTTP	7,055,884
HTTPS	5,376,265
HTTP (8080)	629,781
8081	263,495
HTTP (81)	174,230

72.29.75.120 static.heartline.cam
Heartline.com
Added on 2017-12-04 15:19:36 GMT
United States, Orlando
Details

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache
Last-Modified: Wed, 29 Jul 2015 05:29:09 GMT
ETag: "6f-528849e438500"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

<html><head><meta HTTP-Equiv="refresh" Content="0;URL=/cgi-bin/def...

SerranoArt
66.39.58.227
serranoart.com
pair Networks
Added on 2017-12-04 15:19:36 GMT
United States, Pittsburgh
Technology: S
Details

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache/2.4.29
Last-Modified: Wed, 02 Jan 2018 19:02:16 GMT
ETag: "241d-442c1ea6d2400"
Accept-Ranges: bytes
Content-Length: 9245
Content-Type: text/html

Google Hacking

- Capacidad de hacer ciertas búsquedas manualmente en el buscador Google cuyo objetivo es detectar vulnerabilidades, problemas de configuración o información que pueda conducir a un ataque
- Hay un montón de consultas predefinidas que cubren diferentes tipos de ataques / procedimientos de recopilación de información en la Google Hacking Database:
<https://www.exploit-db.com/google-hacking-database>
- El procedimiento es:
 - Elegir una categoría de búsqueda y una búsqueda dentro de la misma
 - Realizar la consulta sobre un objetivo concreto que te autorice a ello (añade site:<URL o IP de tu objetivo> al final) y ver si se devuelve algo comprometedor
- ¿Y qué hago si encuentro algo que afecta a un familiar o amigo? Como en Shodan, avísale
 - Hacer una búsqueda en Google no es delito, usarla para entrar a un sistema, SÍ
- **Más ejemplos:**
 - <https://wifibit.com/google-hacking/>
 - <https://ciberpatrulla.com/osint-con-google/>

Google Hacking Database

Show 15

Date Added ▾

2020-01-17	intitle:"WS02 Management Console"
2020-01-10	intitle:"webview login" alcatel lucent
2020-01-09	intitle:"LABVANTAGE Logon"
2020-01-09	site:"fogli/domaadmin.cgi"
2020-01-09	inurl:"8080/login.jsp?os_destination=."
2020-01-09	intitle:"index of" "wp-security-audit-log"
2020-01-09	intext:"powered by codoforum" inurl:"user/login"
2020-01-06	inurl:"index.php?enter=guest"
2020-01-06	intitle:"Zabbix" intext:"username" intext:"password" inurl:"/zabbix/index.php"

Google Hacking Database

Show 15

Date Added Dork

2019-09-24	site:*/server-status intext:'Apache server status for'
2019-09-02	inurl:iisstart.htm intitle:'IIS7'
2019-08-30	inurl:phpmyadmin/change_log.php -github -gitlab
2019-08-12	inurl:WebPortal?banking
2019-07-31	intitle:'Apache2 Ubuntu Default Page: It works'
2019-07-31	intitle:'IIS Windows Server' -inurl:'IIS Windows Server'
2019-07-29	inurl:server-status + "Server MPM,"
2019-06-24	inurl:phpinfo.php intext:build 2600
2019-06-17	inurl:OrganizationChart.cc
2019-06-17	intext:'Brought to you by eVetSites'
2019-06-06	intext:'Powered by GetSimple' -site:get-simple.info
2019-05-20	inurl:icm01.php

Category	Author
Filey	Begin typing...
Footholds	
Files Containing Usernames	
Sensitive Directories	
Web Server Detection	
Vulnerable Files	
Vulnerable Servers	
Error Messages	
Category	Author
Various Online Devices	Afie
Pages Containing Login Portals	Bruno Schmid
Pages Containing Login Portals	Reza Abasi
Pages Containing Login Portals	Reza Abasi
Pages Containing Login Portals	Reza Abasi
Files Containing Juicy Info	Reza Abasi
Pages Containing Login Portals	Prasanth
Various Online Devices	Reza Abasi
Pages Containing Login Portals	Reza Abasi

intitle:"Apache2 Ubuntu Default Page: It works"	
GHDB-ID: 5311	Author: REZA ABASI
Published: 2019-07-31	Google Dork Description: intitle:"Apache2 Ubuntu Default Page: It works"
←	Google Search: intitle:"Apache2 Ubuntu Default Page: It works"
web server detection: intitle:"Apache2 Ubuntu Default Page: It works"	
Reza Abasi(Turku)	

intitle:"Apache2 Ubuntu Default Page: It works" 

Aproximadamente 27.000 resultados (0,40 segundos)

Traducir esta página

Apache2 Ubuntu Default Page: It works Annex02!

Apache2 Ubuntu Default Page: It works Annex02! It works! This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

Traducir esta página

Apache2 Ubuntu Default Page: It works * PROXY *****

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page ...

Traducir esta página

Apache2 Ubuntu Default Page: It works

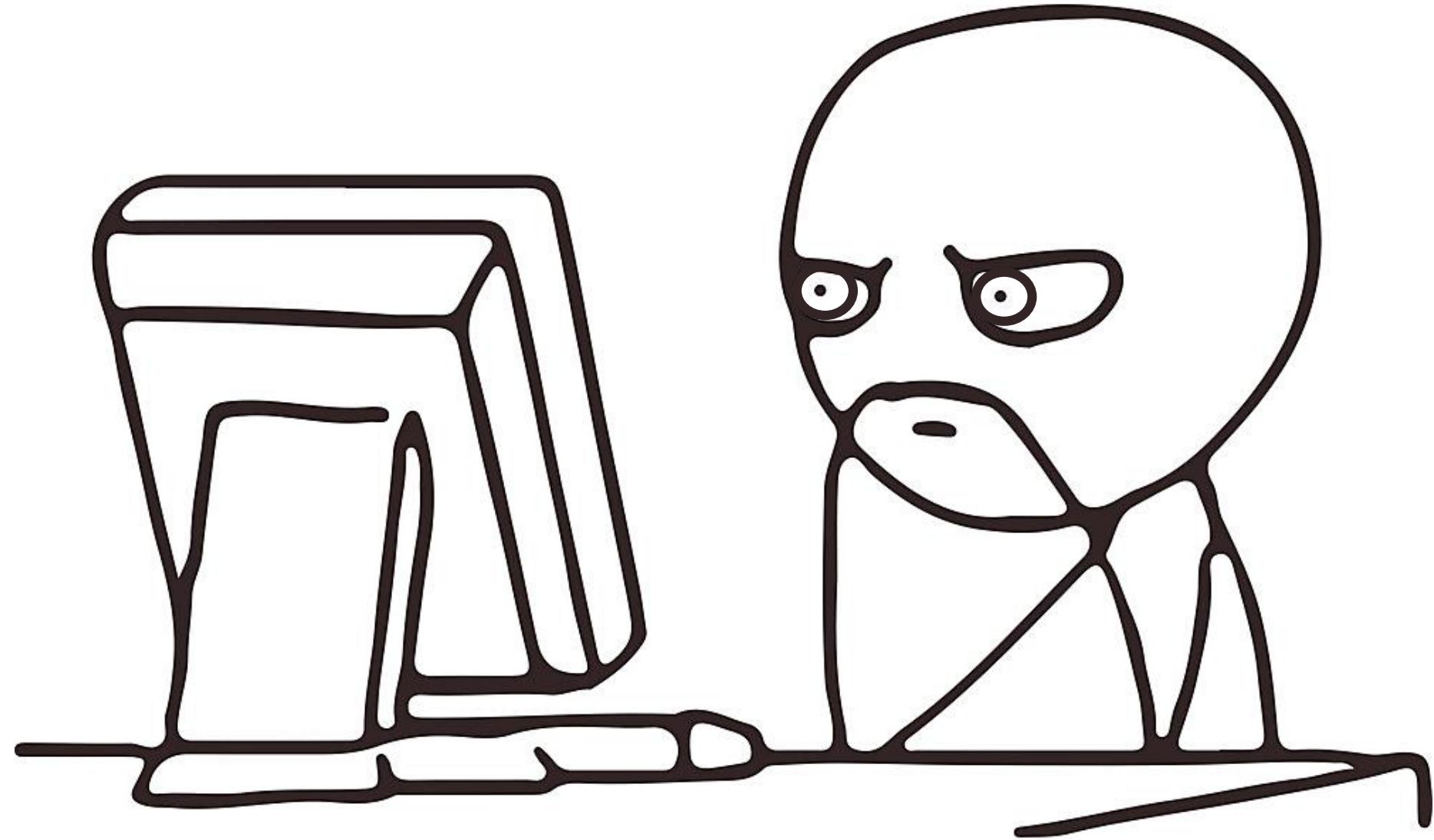
Apache2 Ubuntu Default Page: It works. It works! XXXX This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

Traducir esta página

Apache2 Ubuntu Default Page: It works

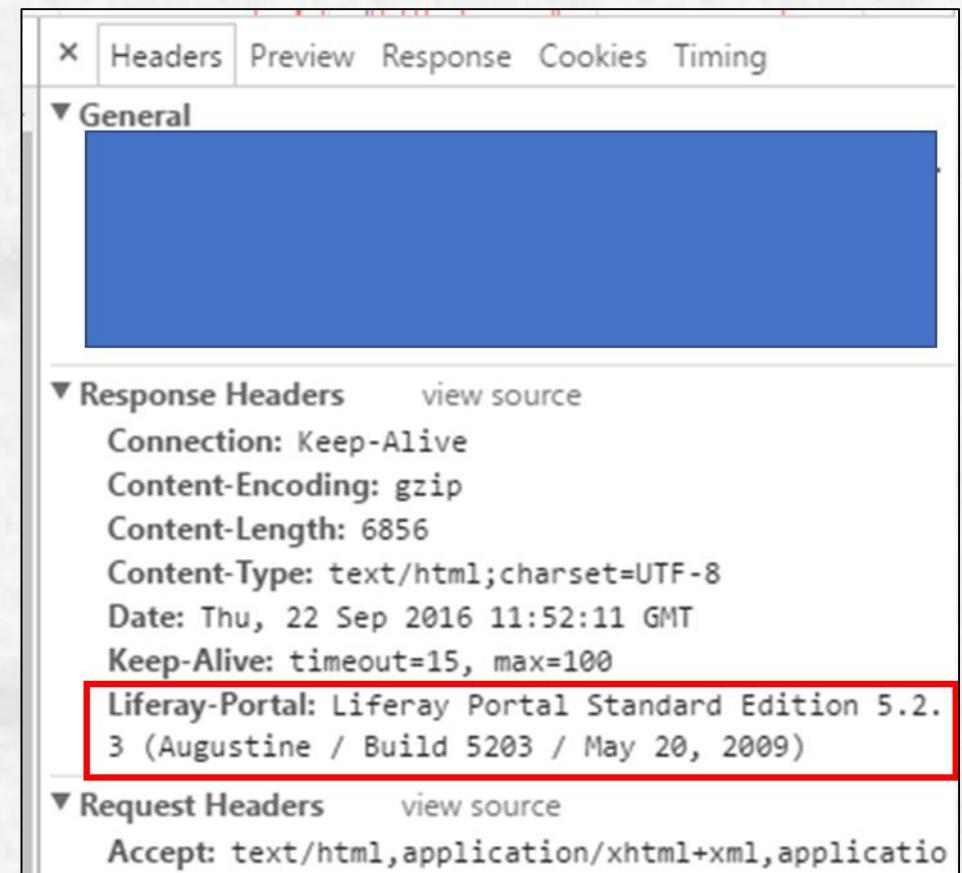
it works !

Pero...¿qué ven mis ojos de elfo?



Información de las webs y CVEs

- Cuando nos conectamos a cualquier web, junto con la página nos llegan cabeceras
- Se pueden ver con las **herramientas del desarrollador** del navegador
- A veces delatan productos usados para hacer las webs y sus versiones
- Esta información que se puede usar en un repositorio de vulnerabilidades para saber cuáles tienen
- El ejemplo delata un producto llamado Liferay, incluida su versión
 - https://www.cvedetails.com/vulnerability-list/vendor_id-2114/product_id-12592/version_id-109268/Liferay-Portal-5.2.3.html



¿Cómo veo esta información?

The screenshot illustrates the process of viewing network traffic information in Firefox. It shows the following steps:

- Firefox Menu:** A red box highlights the "Desarrollador web" option under the "Más" section of the Firefox menu.
- Developer Tools Sidebar:** A red box highlights the "Inspector" option in the sidebar menu.
- Developer Tools Network Tab:** The main window displays the Network tab of the developer tools. A red arrow points from the "Red" tab in the sidebar to the "Red" tab in the main toolbar. The table below shows several requests for "main.css" files.

Estado	Método	Archivo	Causa	Tipo	Transferido	Tamaño
200	GET	main.css?browserId=firefox&themeld=	stylesheet	css	cacheado	240,21 KB
200	GET	main.css?browserId=firefox&themeld=	stylesheet	css	cacheado	240,21 KB
200	GET	main.css?browserId=firefox&themeld=	stylesheet	css	cacheado	240,21 KB
200	GET	main.css?browserId=firefox&themeld=	stylesheet	css	cacheado	240,21 KB
200	GET	main.css?browserId=firefox&themeld=	stylesheet	css	cacheado	133,92 KB
200	GET	main.css?browserId=firefox&themeld=	stylesheet	text/css; charset=UTF-8		133,92 KB
- Network Requests Table:** The table shows the following details:
 - Estado: 200 (Success)
 - Método: GET
 - Archivo: main.css?browserId=firefox&themeld=
 - Causa: stylesheet
 - Tipo: css
 - Transferido: cacheado
 - Tamaño: 240,21 KB / 133,92 KB
- Network Headers:** A red box highlights the "Cabeceras" tab in the sidebar, which lists the request headers:
 - Cache-Control: max-age=31536000, public
 - Connection: Keep-Alive
 - Content-Encoding: gzip
 - Content-Length: 37040
 - Content-Type: text/css
 - Date: Fri, 28 Feb 2020 09:27:09 GMT
 - ETag: "19ba08f1"
 - filter-class: com.liferay.portal.servlet.filters.header.HeaderFilter
 - Keep-Alive: timeout=15, max=98

Información de las webs y CVEs

- ¿Hay webs que listan los problemas de seguridad de todos los productos conocidos?
 - Sí, ¡y es legal!
- Se usan para saber cuándo toca actualizar el software si presenta problemas serios
 - Pero también se puede usar para descubrir si usas software inseguro
- ¿Qué hago si localizo algo así en la web de un familiar / amigo / alguien que me autoriza a hacer esto?
 - Ya sabes, avísale para que (normalmente) lo actualice...
 - **¡Pero actualizar algo puede romper una web!** Mejor pídeselo a un experto...

Liferay » Portal » 5.2.3 Community : Security Vulnerabilities

Cpe Name:cpe:/a:liferay:portal/5.2.3::community

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level
1	CVE-2011-1571			Exec Code	2011-05-07	2011-05-31	9.3	None
2	CVE-2011-1504	79		XSS	2011-05-07	2011-05-31	3.5	None
3	CVE-2011-1503	200		+Info	2011-05-07	2011-05-31	3.5	None

Unspecified vulnerability in the XSL Content portlet in Liferay Portal Community Edition (CE) 5.x and 6.x before 6.0.6 GA, when Apache Tomcat or Oracle GlassFish Server 3.1.2 before 3.1.2.1 processes an XML file via unknown vectors.

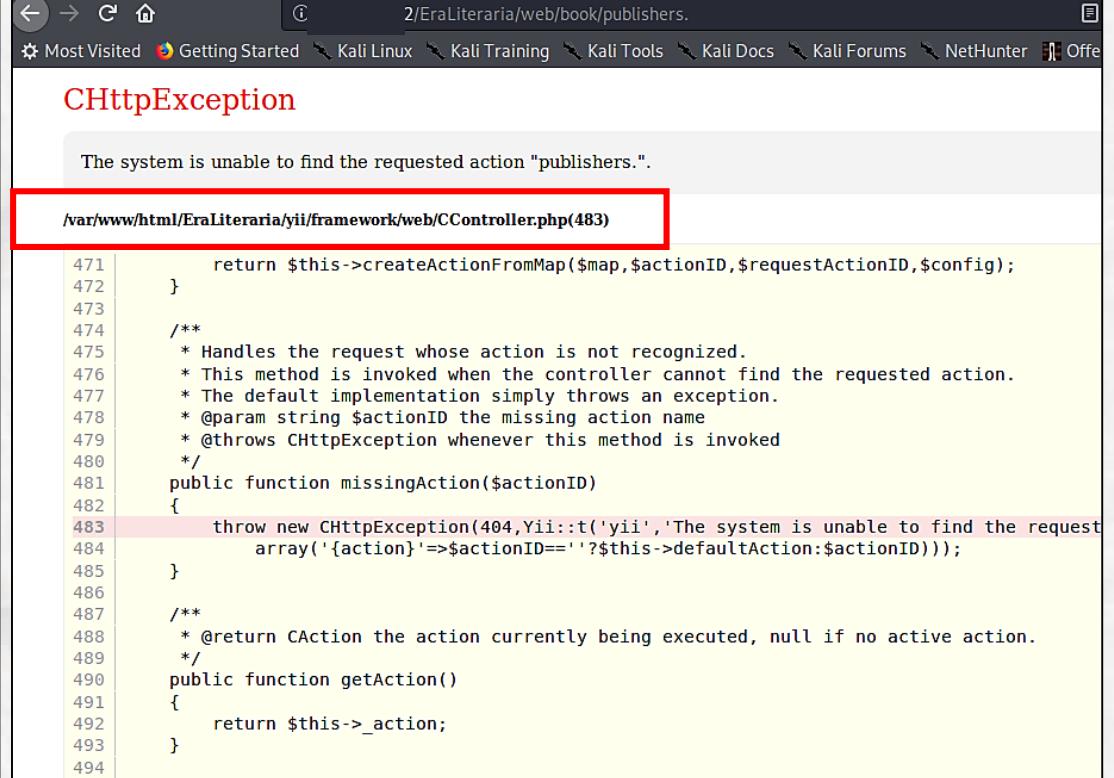
Cross-site scripting (XSS) vulnerability in Liferay Portal Community Edition (CE) 5.x and 6.x before 6.0.6 GA allows remote authenticated users to inject arbitrary web script code into other users' browser via a crafted URL.

The XSL Content portlet in Liferay Portal Community Edition (CE) 5.x and 6.x before 6.0.6 GA, when Apache Tomcat or Oracle GlassFish Server 3.1.2 before 3.1.2.1 processes an XML file via a file:/// URL.

Total number of vulnerabilities : 3 Page : 1 (This Page)

Errores como fuentes de información

- A veces, navegando “mal” apostar se obtiene información de los errores causados
- Por ejemplo, añadiendo un carácter extraño “.” a la URL
- Y esto nos revela el código de la aplicación y que está usando algo llamado **Yii**
 - Que tiene vulnerabilidades:
https://www.cvedetails.com/product/38868/Yiiframework-YII.html?vendor_id=13516

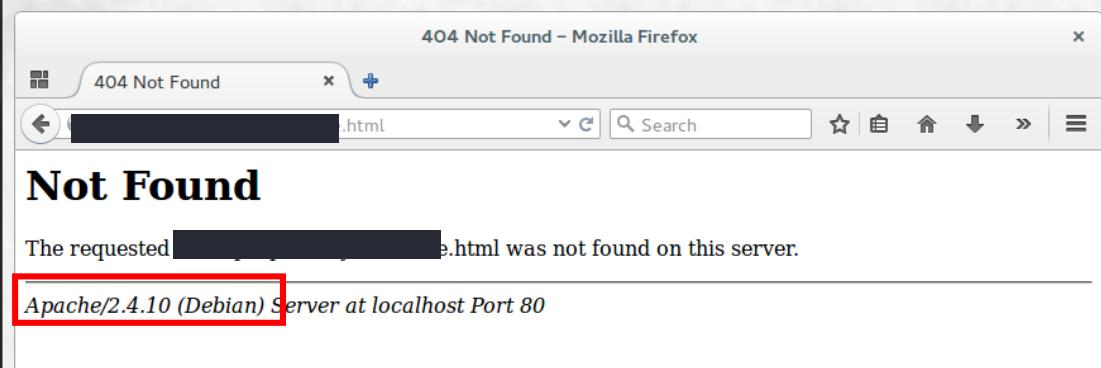


The screenshot shows a web browser window with the URL `2/EraLiteraria/web/book/publishers.`. The page displays a red **CHttpException** message: "The system is unable to find the requested action "publishers.". Below the message, the source code of the `/var/www/html/EraLiteraria/yii/framework/web/CController.php` file is shown, specifically line 483 which contains the error message. The code is as follows:

```
471     return $this->createActionFromMap($map,$actionID,$requestActionID,$config);
472 }
473 /**
474 * Handles the request whose action is not recognized.
475 * This method is invoked when the controller cannot find the requested action.
476 * The default implementation simply throws an exception.
477 * @param string $actionID the missing action name
478 * @throws CHttpException whenever this method is invoked
479 */
480 public function missingAction($actionID)
481 {
482     throw new CHttpException(404,Yii::t('yii','The system is unable to find the request
483         array('{action}'=>$actionID=='?'$this->defaultAction:$actionID));
484 }
485 /**
486 * @return CAction the action currently being executed, null if no active action.
487 */
488 public function getAction()
489 {
490     return $this->_action;
491 }
492 }
493 }
494 }
```

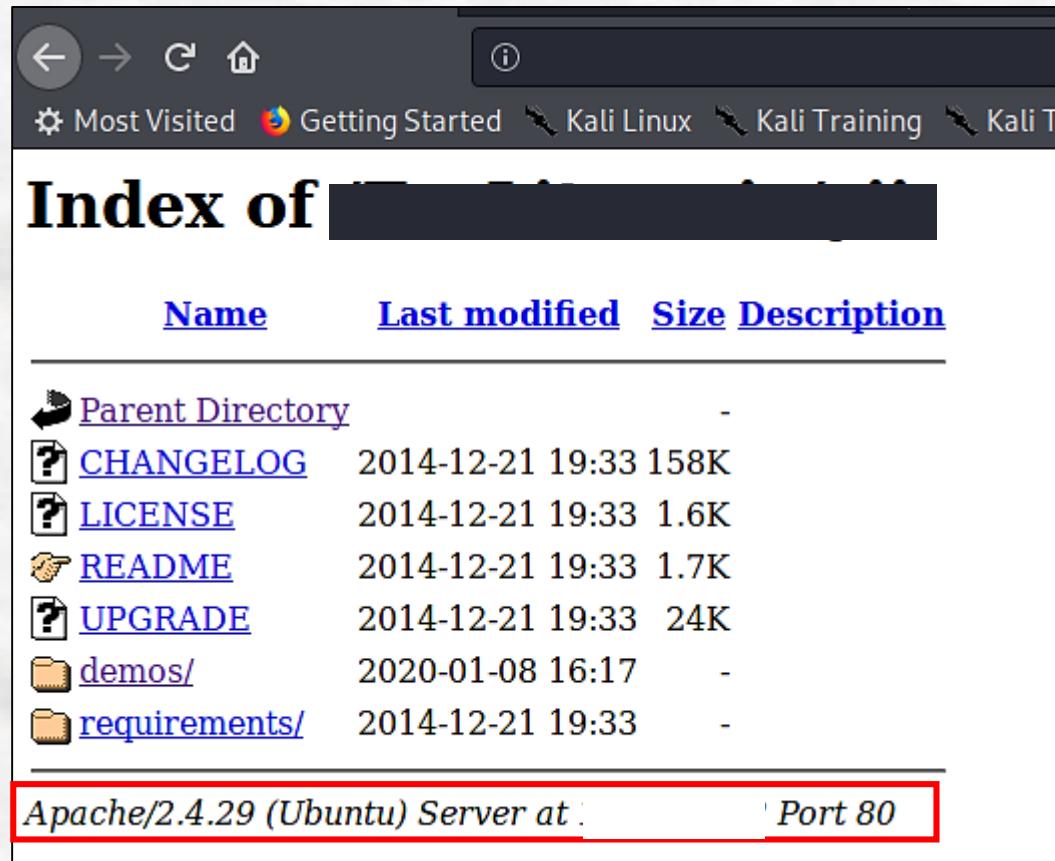
Errores como fuentes de información

- Otra forma típica de hacerlo es intentar navegar a páginas que no existen
- A veces, los errores 404 pueden dar sorpresas en forma de información de productos usados
- Y con ella, repetimos el proceso anterior
- ¡Toda información de productos usados debería ser eliminada de una web!



Errores como fuentes de información

- Otro error es el 403, cuando se accede a una ruta no permitida, como /
 - Muchas veces se redirecciona a una página genérica
 - Pero, a veces se genera un **listado de directorios**
 - Esto lista todos los contenidos la web, sean visibles o no
 - Documentos (con versiones de programas), ficheros ocultos potencialmente descargables...es decir, problemas
 - **¡Este es un error gravísimo que debe eliminarse a toda costa!**



The screenshot shows a web browser window with a dark theme. At the top, there are navigation icons (back, forward, search, etc.) and a toolbar with links like "Most Visited", "Getting Started", "Kali Linux", "Kali Training", and "Kali T". Below the toolbar, the title "Index of" is visible, followed by a partially obscured path. The main content is a table listing files and directories:

Name	Last modified	Size	Description
Parent Directory		-	
CHANGELOG	2014-12-21 19:33	158K	
LICENSE	2014-12-21 19:33	1.6K	
README	2014-12-21 19:33	1.7K	
UPGRADE	2014-12-21 19:33	24K	
demos/	2020-01-08 16:17	-	
requirements/	2014-12-21 19:33	-	

At the bottom of the page, a red border highlights the footer text: "Apache/2.4.29 (Ubuntu) Server at : Port 80".

El fichero robots.txt

- Muchas webs tienen uno, porque se utiliza para indicar a los motores de búsqueda que no indexen las entradas indicadas bajo la palabra clave Disallow
- Estos archivos siempre son accesibles usando este patrón de URL: <http://<La URL>/robots.txt>
- El problema es que este archivo es público, accesible y ¡por lo tanto declara la existencia de estos contenidos “ocultos” a cualquiera!
- Demasiada información -> ya sabéis lo que pasa y lo que hay que hacer, ¿no? ☺

```
User-agent: *
Disallow: /cp/bio
Disallow: /cp/top
Disallow: /news
Disallow: /blogtop
Disallow: /blogbio
Disallow: /bh
Disallow: /cp
Disallow: /showblog
Disallow: /index.php
Disallow: /index2.php
Disallow: /jump.php
Disallow: /past-technology-news
Disallow: /klip
Disallow: /?go=
Disallow: /?option=
Disallow: /?q=
Disallow: /?t=
Disallow: /?webmenu=
Disallow: /%22
Disallow: /c/a/Choosing%20
```

Los metadatos

- Son datos que se añaden a un archivo, pero no como parte de su contenido
- Mucha gente ignora que existen
 - No sabe que muchos programas colocan automáticamente metadatos en los archivos que generan
 - ¡Sin consentimiento!
- Hay una web que analiza los metadatos de documentos individuales y otros tipos de archivos: **Metashield Analyzer**
 - <https://www.elevenpaths.com/es/labstools/metashield-analyzer/index.html>
- Esta web acepta cualquier archivo de una serie de tipos y extrae sus metadatos para ver si hay algo útil o sospechoso en ellos

Analyze your files with Metashield Clean-up Online.

To analyze the metadata in a file, choose the file below and click on "Analyze". Once you accept the Terms and Conditions of Use for Metashield Clean-up Online services a screen will appear with the summary of metadata found.

...228123_10217037728028503_8850651055466217472_n.jpg Select Analyze

Metadata found in 67228123_10217037728028503_8850651055466217472_n.jpg

- ColorPalette
- IccProfileClass
- IccProfileConnectionSpace
- IccProfileCopyright
- IccProfileCreationDate
- IccProfileCreator
- IccProfileFlags
- IccProfileSignature
- IccProfileVersion
- OriginalTransmissionReference
- Software
 - Values
 - Apple Computer, Inc.
- Categories
- 67228123_10217037728028503_8850651055466217472_n.jpg
- SpecialInstructions
- TransmissionReference

**¡Donde está el que me
envía ese email!**

Que yo lo vea...

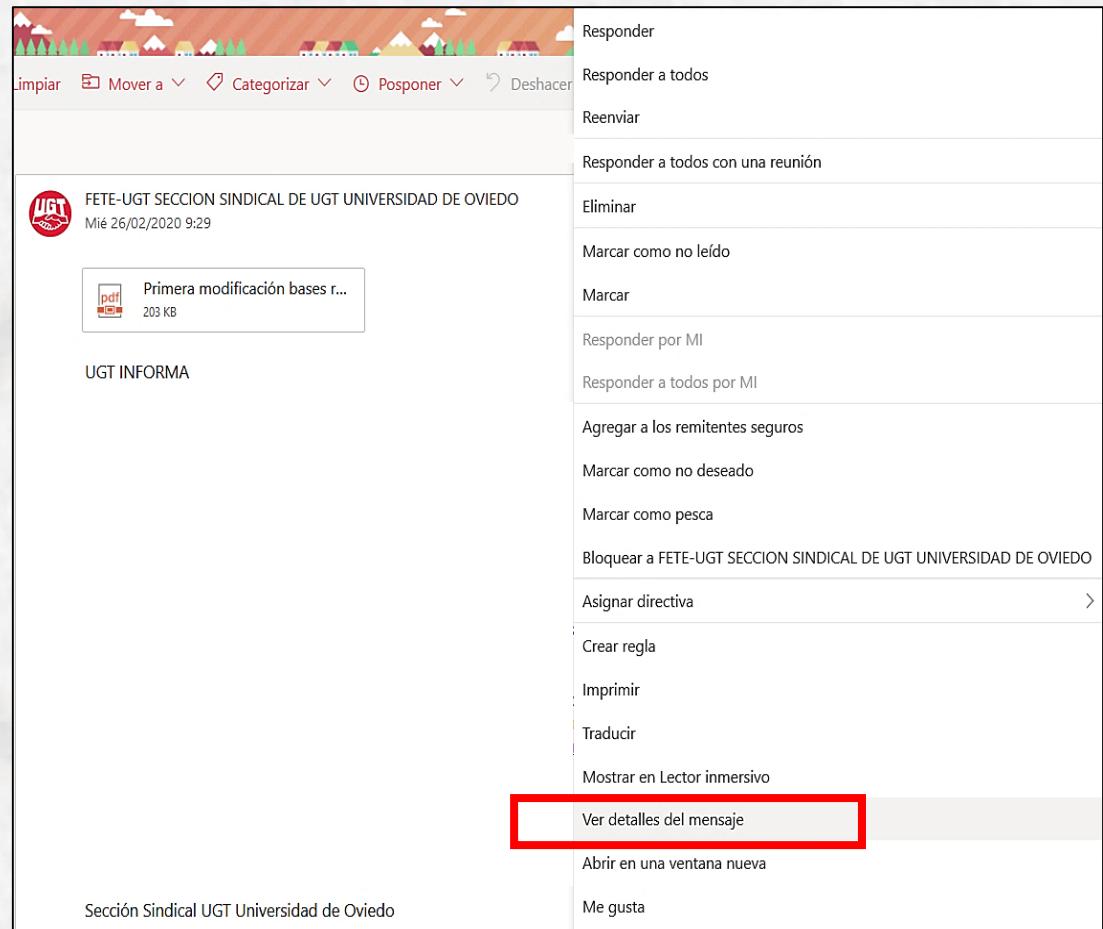


¿De dónde viene un email?

- El email sigue siendo uno de los medios de comunicación electrónica más usados hoy en día
 - Y se sigue usando para fines poco lícitos o para amenazar a personas ☹
- La cuestión es, ¿podemos saber quién es el emisor incluso aunque la cuenta de email sea falsa?
 - No, pero nos podemos acercar en determinados casos...
 - ...y sin ser expertos en informática 
- Esta técnica puede funcionar mejor o peor según casos, pero se puede usar para desenmascarar a alguien que hace lo que no debe
 - Y para aportar más datos a la policía si hay que denunciar
 - Y, lo más importante, no implica hacer nada ilegal ☺

¿De dónde viene un email?

- El truco consiste en acceder a una parte de todo email que habitualmente no se ve
- **Son sus cabeceras e información de control**
- En cada proveedor de correo la opción para verlas cambia (“*Ver detalles*”, “*Ver cabeceras del mensaje*”...)
- En Outlook web está aquí (“*Ver detalles del mensaje*”)



¿De dónde viene un email?

- Al hacer esto sale un montón de texto, la mayoría del cual no entenderemos
- Pero el importante es uno: **Received: from**
 - Cuando envías un correo “rebota” por un montón de máquinas intermedias
 - Estas máquinas se encargan de que llegue a su destino “viajando” por distintas partes del mundo
 - Se añade un **Received: from** por cada una de las que pasa
 - Y se muestra la IP de la misma (normalmente)

Detalles de mensaje

```
Received-SPF: Pass (protection.outlook.com: domain of uniovi.es designates
156.35.      as permitted sender) receiver=protection.outlook.com;
client-ip=156.35      ; helo=      .uniovi.es;
Received: from |      .uniovi.es (156.35.      ) by
protection.outlook.com (10.15.      ) with Microsoft SMTP
Server (version=TLS1_0, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id
15.20.2772.14 via Frontend Transport; Wed, 26 Feb 2020 08:29:34 +0000
Received: from |      .uniovi.es (172.22.      ) by
|      .uniovi.es
(172.22.      ) with Microsoft SMTP Server (TLS) id 14.3.468.0; Wed, 26 Feb
2020 09:28:03 +0100
Received: from |      .uniovi.es (172.22.      ) by
|      .uniovi.es (172.22.      ) with Microsoft SMTP Server (TLS) id
15.0.1395.4; Wed, 26 Feb 2020 09:27:57 +0100
Received: from |      uniovi.es (172.22.      ) by
|      .uniovi.es (172.22.      ) with Microsoft SMTP Server (TLS) id
15.0.1395.4 via Frontend Transport; Wed, 26 Feb 2020 09:27:56 +0100
Received: from |      protection.outlook.com (104.47.      )
by |      .uniovi.es (156.35.      ) with Microsoft SMTP Server (TLS) id
14.3.468.0; Wed, 26 Feb 2020 09:27:57 +0100
Received: from |      .prod.outlook.com (20.179.      ) by
|      .prod.outlook.com (52.133.      ) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
```

¿De dónde viene un email?

- Y de esta forma, podemos bajar la “cadena” de Received: from hasta llegar a la primera de ellas
- ¡Es la primera máquina en la cadena de máquinas que nos envió el mensaje!
- Ahora tenemos su IP, **¿qué podemos hacer con ella?**

Detalles de mensaje

```
15.0.1395.4·Wed, 26 Feb 2020 09:27:57 +0100
Received: from .uniovi.es (172.22. ) by
| .uniovi.es (172.22. ) with Microsoft SMTP Server (TLS) id
15.0.1395.4 via Frontend Transport; Wed, 26 Feb 2020 09:27:56 +0100
Received: from .protection.outlook.com (104.47. ) by
by .uniovi.es (156.35. ) with Microsoft SMTP Server (TLS) id
14.3.468.0·Wed, 26 Feb 2020 09:27:57 +0100
Received: from .prod.outlook.com (20.179. ) by
| prod.outlook.com (52.133. ) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.2750.21; Wed, 26 Feb 2020 08:27:55 +0000
```

¿De dónde viene un email?

- Pues geolocalizarla en el mundo, ya que hay servicios que lo hacen
 - Como <https://www.iplocation.net/>
- Estos servicios localizan de forma más o menos precisa en función de si es una IP pública o pertenece a un proveedor de Internet
- No es la panacea...¡Pero merece la pena probar! ☺

The screenshot shows the homepage of iplocation.net. At the top, there's a navigation bar with links for 'MY IP', 'HIDE IP', 'CHANGE IP', 'VPN', 'PROXY', 'GAMES', 'DDOS', 'WEB', and 'SEARCH'. Below the navigation is a search bar with the placeholder 'Where is Geolocation of an IP Address?'. A message indicates 'Your public IP Address is 156.35.' with a link to 'Hide IP with VPN'. A 'IP Location Finder' section contains an input field with '20.179.' and a red 'IP Lookup' button. To the right, a note says 'Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.' Below this is a link to 'Report a problem.' At the bottom, it says 'Is the data shown below not accurate enough? Please read [geolocation accuracy](#) info to learn why.' and 'Geolocation data from IP2Location (Product: DB6, updated on 2020-2-1)'. On the right side, there are sections for 'ADVERTISING', 'DOMAIN', 'POPULAR', and 'RECENT' with various links.

¿De dónde viene un email?

- El servicio nos da las coordenadas del sitio donde cree que está la máquina que envió el mensaje
 - Latitud y Longitud
- Con ellas podemos geolocalizar cualquier parte del mundo
- ¿Qué programa conoces que te deje hacer eso?
 - ¡Google Earth!

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2020-2-1)

IP Address	Country	Region	City
20.179	United States of America 	Washington	Redmond
ISP	Organization	Latitude	Longitude
Microsoft Corporation	Not Available	47.6829	-122.1209

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
20.179.	United States 	Washington	Redmond
ISP	Organization	Latitude	Longitude
Not Available	Microsoft Corporation (microsoft.com)	47.6740	-122.1215

Geolocation data from [DB-IP](#) (Product: Full, 2020-2-1)

IP Address	Country	Region	City
20.179.	United States 	New Jersey	Newark
ISP	Organization	Latitude	Longitude
Microsoft Corporation	Microsoft Corporation	40.7357	-74.1724

▼ Buscar

47.689°,-122.1209°

Buscar

por ejemplo: Restaurantes

Obtener indicaciones Historial

A 47°41'20.4"N 122°07'15.2"W
16430 NE 99th St, Redmond, WA 98052, EE. UU.
★★★☆☆

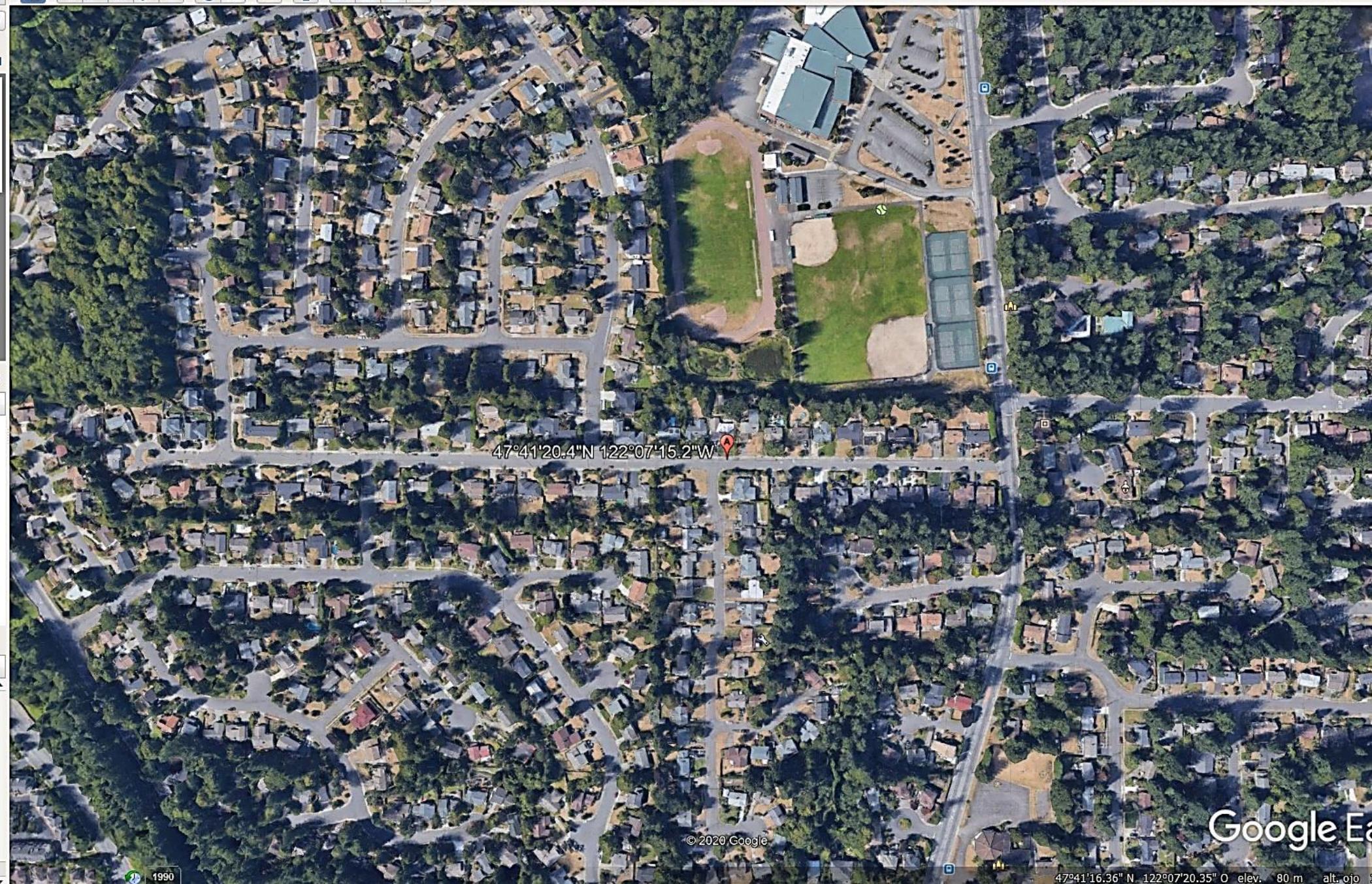
▼ Sitios

- Mis sitios
- Tour de lugares destacados
 - Asegúrate de que la capa de edificios 3D está activada.
- Sitios temporales



▼ Capas

- Base de datos principal
 - Anuncios
 - Fronteras y etiquetas
 - Lugares
 - Fotografías
 - Carreteras
 - Edificios 3D
 - Océanos
 - Tiempo
 - Galería
 - Concienciación global
 - Más



© 2020 Google

1990

47°41'16.36" N 122°07'20.35" O elev. 80 m alt. ojo

Google Earth

¿De dónde viene un email?

- ¿Un correo de UGT emitido desde Washington? Eso no suena creíble...
- Porque es la IP del primer servidor de correo que inició la transferencia, no del emisor ☺
 - En este caso es un servidor de la nube de Microsoft, que está en Washington
- Pero si seguimos bajando podríamos encontrarnos con otro dato interesante x-originating-ip
- ¿Qué pasa si geolocalizamos ahora esta IP de la misma forma?

```
Authentication-Results-Original: uniovi.es; dkim=none (message not signed)
header.d=none;uniovi.es; dmarc=none action=none header.from=uniovi.es;
x-originating-ip: [156.35. ]  
x-ms-publictraffictype: Email
```

¿De dónde viene un email?

- Los datos devueltos ahora son mucho más creíbles y precisos:
 - España
 - Asturias
 - Oviedo
 - Universidad de Oviedo
 - Y una latitud y longitud...
- Google Earth y ... ¡hola! ☺
 - NOTA: La oficina de UGT está en el campus del Milán, y me devuelve una localización algo por encima de ella
 - ¡Es aproximado! (pero muy útil)

Geolocation data from IP2Location (Product: DB6, updated on 2020-2-1)

IP Address	Country	Region	City
156.35.	Spain 	Asturias, Principado de	Oviedo
ISP	Organization	Latitude	Longitude
Universidad de Oviedo	Not Available	43.3603	-5.8448

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
156.35.	Not Available	Not Available	Not Available
ISP	Organization	Latitude	Longitude
Entidad Pública Empresarial Red.es	Universidad de Oviedo (uniovi.es)	0.0000	0.0000

Geolocation data from DB-IP (Product: Full, 2020-2-1)

IP Address	Country	Region	City
156.35.	Spain 	Asturias	Oviedo
ISP	Organization	Latitude	Longitude
Entidad Pública Empresarial Red.es	Uniovi	43.363	-5.84396

▼ Buscar

43.3693°, -5.8448°

Buscar

por ejemplo: Restaurantes

Obtener indicaciones Historial

A 43°22'09.5"N 5°50'41.3"W
33011 Oviedo, Asturias
★★★☆☆

▼ Sitios

- Mis sitios
- Tour de lugares destacados

Asegúrate de que la capa de edificios 3D está activada.

- Sitios temporales



▼ Capas

- Base de datos principal
- Anuncios
- Fronteras y etiquetas
- Lugares
- Fotografías
- Carreteras
- Edificios 3D
- Océanos
- Tiempo
- Galería
- Concienciación global
- Más



¿De dónde viene un email?

- La localización es aproximada / por código postal
 - Si sale desde una IP pública de un centro, empresa o institución, probablemente te dará el nombre
 - ¿Cuánta gente conoces que usa la Wifi en el Carrefour de los Prados?
 - Si sale desde una instalación típica de casa, te dará el código postal de la zona en la que se encuentra y (seguramente) su proveedor
 - ¿Cuánta gente conoces en ese distrito que tiene Telecable contratado?
 - Si te envían varios emails desde diferentes sitios, tendrás geolocalizaciones aproximadas de por dónde se mueve el emisor
 - ¿Cuánta gente conoces que vive en la zona de Llamaquique y de vez en cuando va a la zona de Viesques el fin de semana?
 - ¿Y que además va por el Carrefour de los Prados?
 - ¿Y que tiene Telecable contratado?

¿De dónde viene un email?

- Pongamos que el contenido del email es un delito
- Si manda imágenes, conviene mirar su metadatos
 - Porque pueden contener el tipo de dispositivo que hizo la foto
 - Ahora entendéis por qué los metadatos son útiles también ☺
- ¿Cuánta gente conoces de tu entorno que...?
 - Va por el Carrefour de los Prados
 - Vive en la zona de Llamaquique y va a Viesques los fines de semana
 - Tiene Telecable contratado
 - ...y usa un IPhone X?
- La policía sabe todo esto y puede cruzar datos con su base de datos de personas
- ¿Problem? 

¿Y si lo envío desde el móvil? Red 4G

- Mensaje enviado desde una red 4G (Telecable) desde dentro del parque San Francisco

Detalles de mensaje

X-MIS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <
MIME-Version: 1.0
X-MS-Exchange-Organization-MessageDirectionality: Originating
X-MS-Exchange-Organization-AuthSource: .prod.outlook.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [188.171.100.10]
X-MS-Exchange-Organization-Network-Message-Id:
1333c61d-ef24-4a72-9dc8-08d7bb960f8b

Country	Capital	Madrid
State/Province		Principality of Asturias
District/County		Centro
City		Oviedo
Zip Code		33007
Latitude & Longitude of City		43.36300, -5.85347



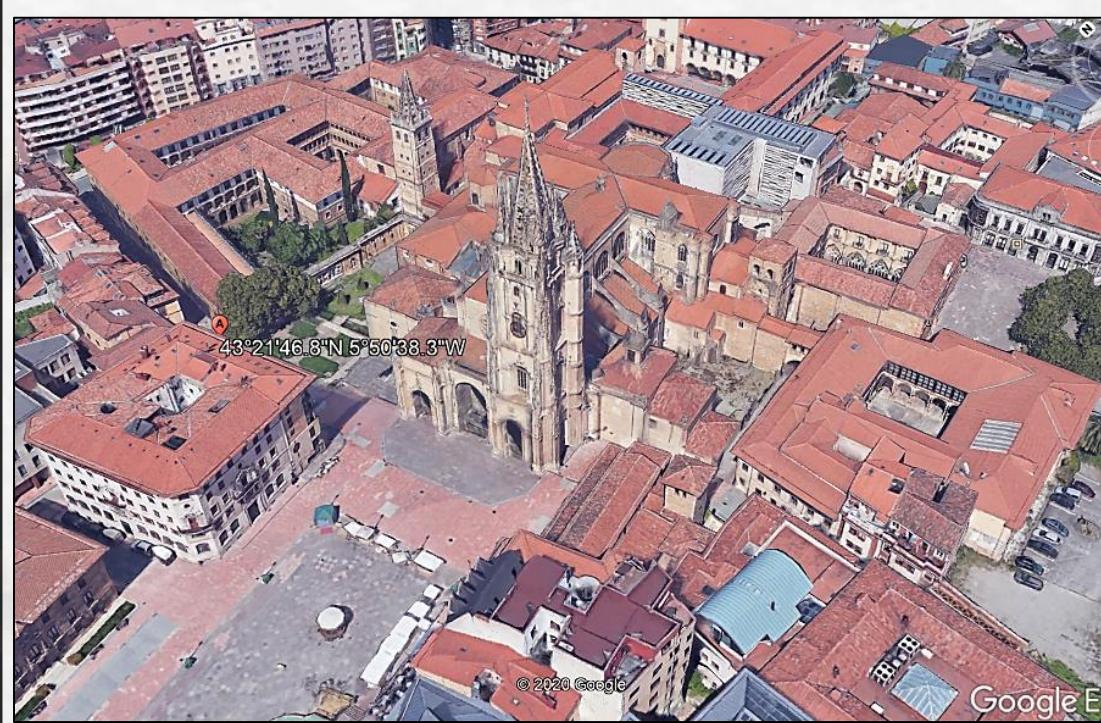
¿Y si lo envío desde el móvil? Red Wifi

- Mensaje enviado desde la Facultad de Psicología (usando Uniovi Wifi)

Detalles de mensaje

X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <@email.android.com>
MIME-Version: 1.0
X-MS-Exchange-Organization-MessageDirectionality: Originating
X-MS-Exchange-Organization-AuthSource: .prod.outlook.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [156.35.]
X-MS-Exchange-Organization-Network-Message-Id:
5b5e228e-2ae5-4d3a-98f0-08d7bb96dd14

District/County	Casco Antiguo
City	Oviedo
Zip Code	33003
Latitude & Longitude of City	43.36300, -5.84396
Geoname ID	3114711
Is EU?	true



Y, ante esto, ¿Qué hacer?

© José Manuel
Redondo López

- Ser gente decente y legal ☺
 - Porque es lo que se debe hacer ☺
 - Y porque, en caso de no serlo, localizar a alguien es técnicamente posible
 - Nosotros de forma aproximada, la policía de forma definitiva ☺
 - Y en ese caso, tener que responder ante la justicia
- ¿Y con el Whatsapp / Telegram?
 - ¿Puede la policía pedir los datos de las IPs de los emisores bajo orden judicial?
 - Ellos tienen medios que nosotros no
 - Y ya veis lo que pasa en cuanto tienes una IP...
 - ¡Hasta el infinito y más allá! ☺



ESCUELA DE INGENIERÍA
INFORMÁTICA

José Manuel Redondo López