Jornadas “Espacios de Ciberseguridad”

Espionaje y Cibervigilancia

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

NATIONAL CYBERSECURITY INSTITUTE OF SPAIN

Índice

INCIBE - ¿Qué es?

El Instituto Nacional de Ciberseguridad de España (**INCIBE**) es una sociedad dependiente del Ministerio de Industria, Energía y Turismo (**MINETUR**) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (**SETSI**).

INCIBE es la entidad de referencia para el desarrollo de la **ciberseguridad** y de la **confianza digital** de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos (Agenda Digital para España, aprobada en Consejo de Ministros el 15 de Febrero de 2012).

Como **centro de excelencia**, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia , INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

www.incibe.es

INCIBE - ¿Qué es?

Pilares fundamentales sobre los que se apoya la actividad de INCIBE

- **Prestación de servicios** de protección de la privacidad, prevención y reacción a incidentes en ciberseguridad
- **Investigación** generación de inteligencia y mejora de los servicios
- **Coordinación** colaboración con entidades públicas y privadas, nacionales e internacionales

Área de Operaciones

Jornadas “Espacios Ciberseguridad”

Características Jornadas curso 2015-2016

https://www.incibe.es/excelencia/jornadas_incibe/

JORNADAS PARA PROFESORES

Profesores de Bachiller y FP tecnológicos.

Formación para impartir las 8 temáticas de manera autónoma.

Grupos de entre 20 y 30 docentes.

Duración 5h (en una única sesión).

espacioscs_profesores@incibe.es

JORNADAS PARA ALUMNOS

Alumnos de Bachiller y FP tecnológicos.

1 temática por centro (de las 8 posibles).

Grupos de entre 20 y 30 alumnos.

Duración 3h (en una única sesión).

espacioscyberseguridad@incibe.es

MATERIALES ON-LINE (YA DISPONIBLES EN LA PÁGINA WEB DE LAS JORNADAS)

PPT's de las 8 jornadas para alumnos
Vídeos de la impartición de las **8 jornadas íntegras**
Documentación adicional para cada jornada:

- Conocimientos previos de los alumnos.
- Resumen de contenidos y vídeo píldoras de 5min sobre el contenido de cada jornada.
- Material complementario para seguir investigando y aprendiendo sobre cada una de las materias.

Materiales para la impartición de los talleres por parte de los profesores:

- **PPT** presentada en la jornada de **profesores**.
- **Dossier completo** con la explicación detallada de todas las jornadas de alumnos así como los temas generales para la preparación de los entornos de prácticas.

Otras Actuaciones de interés

Si te gusta la ciberseguridad y quieres profundizar en este tema en INCIBE se están desarrollando las siguientes actividades y eventos de ciberseguridad:

- **Formación especializada en ciberseguridad:** MOOC que se desarrollan a través de la plataforma de formación de INCIBE (http://formacion-online.incibe.es) sobre conceptos avanzados en ciberseguridad tales como ciberseguridad industrial, seguridad en dispositivos móviles, programación segura, malware y sistemas TI.

- **Programa de becas:** Programa de becas anual en el que se establecerán diferentes tipologías de becas: formación de cursos especializados y másteres en ciberseguridad, y becas de investigación. Todas las publicaciones de este tipo se realizará a través de la siguiente página https://www.incibe.es/convocatorias/ayudas/.

- **Evento de ciberseguridad – CyberCamp** (http://cybercamp.es).

  CyberCamp es el evento internacional de INCIBE para identificar, atraer y promocionar el talento en ciberseguridad.
  - Identificar trayectorias profesionales de los jóvenes talento.
  - Detectar y promocionar el talento mediante talleres y retos técnicos.
  - Atraer el talento ofreciendo conferencias y charlas de ciberseguridad por profesionales y expertos de primer nivel.

  Y muchas cosas más….
  - Evento para **familias**, contando con actividades de concienciación y difusión de la ciberseguridad para padres, educadores e hijos.
  - Promoción de la **industria** e **investigación** en ciberseguridad.

Índice

Introducción a la ciberseguridad

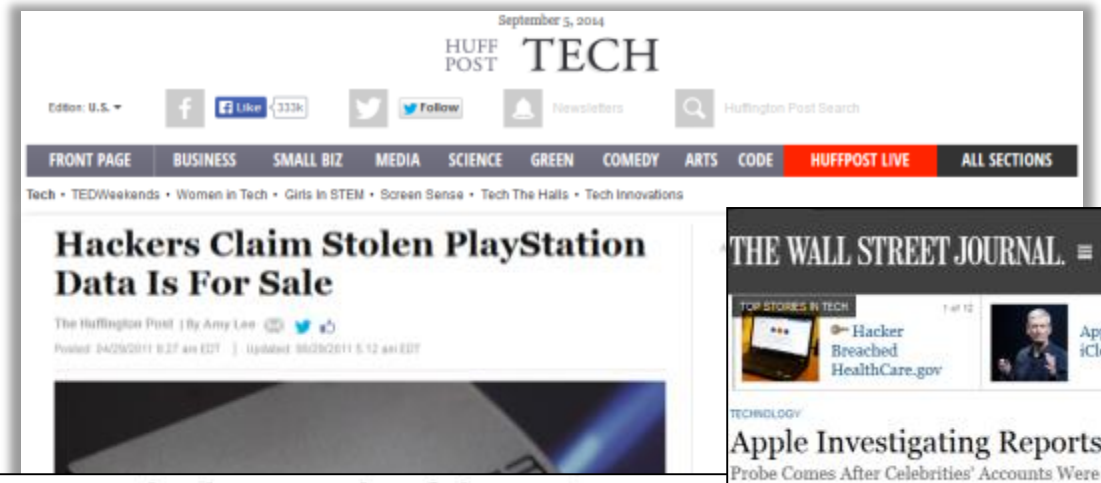
Evolución de las Tecnologías de la Información

- La **información** es uno de los principales activos de una empresa.
- Las empresas almacenan y gestionan la información en los **Sistemas de Información**.
- Para una empresa resulta fundamental proteger sus Sistemas de Información para que su información esté a salvo. Dificultades:
  - El entorno donde las empresas desarrollan sus actividades es cada vez más complejo debido al desarrollo de las tecnologías de información y otros factores del entorno empresarial
  - El perfil de un ciberdelincuente de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar) en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede llegar a ser.

- Es fundamental poner los medios técnicos y organizativos necesarios para garantizar la seguridad de la información. Para lograrlo hay que garantizar la **confidencialidad**, **disponibilidad** e **integridad** de la información.

Introducción a la ciberseguridad

Casos notorios



Introducción a la ciberseguridad

Seguridad de la Información

La seguridad de la información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información:

- La **confidencialidad** es la propiedad de prevenir la divulgación de información a personas no autorizadas.
- La **integridad** es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.
- La **disponibilidad** es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- La **autenticidad**: la información es lo que dice ser o el transmisor de la información es quien dice ser.
- El **no repudio**: Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.

Introducción a la ciberseguridad

Riesgos para los Sistemas de Información

¿Qué son los riesgos en los sistemas de información?

- Las amenazas sobre la información almacenada en un sistema informático.

Ejemplos de riesgos en los sistemas de información

- **Daño físico**: fuego, agua, vandalismo, pérdida de energía y desastres naturales.
- **Acciones humanas**: acción intencional o accidental que pueda atentar contra la productividad.
- **Fallos del equipamiento**: fallos del sistema o dispositivos periféricos.
- **Ataques internos o externos**: hacking, cracking y/o cualquier tipo de ataque.
- **Pérdida de datos**: divulgación de secretos comerciales, fraude, espionaje y robo.
- **Errores en las aplicaciones**: errores de computación, errores de entrada, etc.

Introducción a la ciberseguridad

La figura del HACKER

¿Qué es un hacker?

Experto en seguridad informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

¿Qué tipos de hackers existen en función de los objetivos que tienen?

Black Hat Hackers: Suelen quebrantar la seguridad de un sistema o una red con fines maliciosos.

White Hat Hackers: normalmente son los que penetran la seguridad de los sistemas bajo autorización para encontrar vulnerabilidades. Suelen ser contratados por empresas para mejorar la seguridad de sus propios sistemas.

Gray (Grey) Hat Hackers: Son una mezcla entre los dos anteriores puesto que tienen una ética ambigua. Normalmente su cometido es penetrar en sistemas de forma ilegal para luego informar a la empresa víctima y ofrecer sus servicios para solucionarlo.

Introducción a la ciberseguridad

Clases de ataques

- **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
- **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
- **Modificación:** se trata de modificar la información sin autorización alguna.
- **Fabricación**: se crean productos, tales como páginas web o tarjetas magnéticas falsas.

Introducción a la ciberseguridad

Técnicas de hacking

- **Spoofing:** se suplanta la identidad de un sistema total o parcialmente.
- **Sniffing:** se produce al escuchar una red para ver toda la información transmitida por ésta.
- **Man in the middle:** siendo una mezcla de varias técnicas, consiste en interceptar la comunicación entre dos interlocutores posicionándose en medio de la comunicación y monitorizando y/o alterando la comunicación.
- **Malware:** se introducen programas dañinos en un sistema, como por ejemplo un virus, un keylogger (herramientas que permiten monitorizar las pulsaciones sobre un teclado) o rootkits (herramientas que ocultan la existencia de un intruso en un sistema).
- **Denegación de servicio:** consiste en la interrupción de un servicio sin autorización.
- **Ingeniería social:** se obtiene la información confidencial de una persona u organismo con fines perjudiciales. El Phishing es un ejemplo de la utilización de ingeniería social, que consigue información de la víctima suplantando la identidad de una empresa u organismo por internet. Se trata de una práctica muy habitual en el sector bancario.
- Adicionalmente existen multitud de ataques como **XSS**, **CSRF**, **SQL injection**, etc.

Introducción a la ciberseguridad

Mecanismos de defensa

Ante esta figura, ¿cómo pueden protegerse las compañías con las nuevas tecnologías?

Los principales sistemas y más conocidos son los siguientes:

- **Firewall:** sistemas de restricción de tráfico basado en reglas.

- **Sistemas IDS / IPS:** sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.

- **Honeypot:** equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.

- **SIEM:** sistemas de correlación de eventos y generación de alertas de seguridad.

- **Antimalware:** sistemas de detección de malware informático.

Introducción a la ciberseguridad

Las prácticas del taller se realizan sobre un entorno controlado.

Utilizar las técnicas mostradas en el presente taller sobre un entorno real como Internet, puede ocasionar problemas legales.

Índice

Objetivos del curso

¿Qué vamos a aprender hoy?

- En qué consiste el espionaje y la cibervigilancia.
- La importancia de controlar nuestros datos en internet.
- Cómo obtener información sensible a través de internet.
- Funcionamiento de la Deep Web.
- Técnicas de evasión de restricciones web.
- El riesgo de perdida de la privacidad en internet.

¿Cómo lo vamos a aprender?

1. Teoría.
2. Práctica:
   a. Ejercicios prácticos a lo largo de la presentación usando herramientas públicas en **un entorno controlado**.

Índice

Contexto

La información como valor

- Motivación con fines industriales:
  - Espionaje de compañías competidoras.
  - Conocimiento científico.
  - Posición estratégica de mercado.
  - Información de empleados o candidatos.

- Motivación con fines personales:
  - Suplantación de identidades.
  - Obtener información personal de terceros

- Motivación con fines comerciales:
  - Venta de información personal o empresarial en el mercado negro.

Legalidad y Seguridad en la red

¿Os sentís seguros cuando navegáis por la red?

Índice

Introducción al espionaje y cibervigilancia

¿Qué es el espionaje informático?

- Obtención encubierta de datos o información confidencial a través de sistemas informáticos.

¿Cuáles son los programas de espionaje más comunes?

- **Adware**

  Programas que recopilan información acerca de los hábitos de navegación del usuario. Se suelen utilizar con fines publicitarios para determinar la conducta de los internautas.

- **Programas de acceso remoto (RAT)**

  Permiten el acceso de una tercera persona a el ordenador para un posterior ataque o alteración de los datos.

- **Troyanos**

  Son programas maliciosos que se presentan al usuario como programas aparentemente inofensivos y ponen en peligro la seguridad del sistema. Estarían englobados también dentro del término RAT puesto que facilitan el control remoto.

Introducción al espionaje y cibervigilancia

¿Cuáles son las técnicas de espionaje más comunes?

- **Virus o gusanos**

  Programas que además de provocar daños en el sistema se propagan a otros equipos haciendo uso de la Red, del correo electrónico, etc.

  Virus

  - El virus es un tipo específico de malware.
  - Es común llamar "virus" al malware, pero en realidad es solo un subconjunto.
  - Su nombre viene por su parecido a los virus reales (infección y propagación).
  - Para su propagación necesitan que cierta interacción por parte del usuario.

  Gusanos

  - Los gusanos (habitualmente llamados worms) son programas maliciosos que se propagan por la red de forma automática.
  - Los gusanos se transmiten explotando vulnerabilidades de los sistemas sin Que el usuario tenga que interactuar con ellos de ninguna manera.

- **Spyware**

  Programas que basan su funcionamiento en registrar todo lo que se realiza en un PC. Se utilizan para obtener información confidencial o conocer cuál es el uso que una persona le está dando a la máquina.

Introducción al espionaje y cibervigilancia

Criptografía

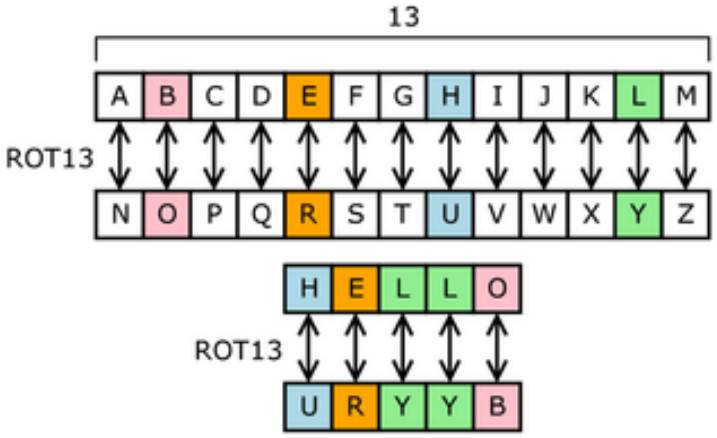
- Hace referencia a las técnicas de alteración de mensajes para evitar la obtención de información por parte de personas no autorizadas.

Evolución del espionaje. Desde la antigüedad…

Rey Sargón I de Acad

Scytale

Cifrado César



- El **objetivo** era ocultar información al pueblo.

Introducción al espionaje y cibervigilancia

Práctica: Descifra el mensaje

- **Objetivo**: descifrar el mensaje codificado con el método Cesar:
  - Realizar un análisis de frecuencias observando que letras se repiten menos, suponiendo que corresponden a las letras menos comunes en castellano (ñ, k…).
  - Si el texto tiene espacios, analizar las palabras más cortas suponiendo que son artículos.
  - Una vez extraída una equivalencia, extraer el desplazamiento para descifrar todo el texto.

Ra ha yhtne qr yn Znapun, qr phlb abzoer ab dhvreb npbeqnezr, ab un zhpub gvrzcb dhr iviín ha uvqnytb qr ybf qr ynamn ra nfgvyyreb, nqnetn nagvthn, ebpía synpb l tnytb pbeerqbe.

Introducción al espionaje y cibervigilancia

Evolución del espionaje. En tiempos de guerra…

- Como técnica de espionaje durante la guerra, disfrazaban a consejeros y guerreros de mercaderes o usaban a exploradores cuya misión era obtener información sobre el enemigo.

- Durante la Revolución francesa, se utilizó a un enano de 60 centímetros de altura como espía al que disfrazaban de bebé e infiltraban entre las líneas enemigas con una falsa mamá.

- Durante la Guerra Civil americana ambos bandos hicieron uso de las redes telegráficas civiles con mensajes transmitidos en código Morse.

A	.-	M	--	Y	-.--	6	-....
B	-...	N	-.	Z	--..	7	--...
C	-.-.	O	---	Ä	.-.-	8	---..
D	-..	P	.--.	Ö	---.	9	----.
E	.	Q	--.-	Ü	..--	.	.-.-.-
F	..-.	R	.-.	Ch	----	,	--..--
G	--.	S	...	0	-----	?	..--..
H	....	T	-	1	.----	!	··—·
I	..	U	..-	2	..---	:	---...
J	.---	V	...-	3	...--	“	.-..-.
K	-.-	W	.--	4	....-	‘	.----.
L	.-..	X	-..-	5	.....	=	-...-

- **Objetivo:** Obtención de información valiosa del enemigo**.**

Introducción al espionaje y cibervigilancia

Evolución del espionaje. La era tecnológica…

- ECHELON es considerada la mayor red de espionaje de la historia con 120 satélites en su poder.
- Rastrea más de 3.000 millones de mensajes al día entre comunicaciones de gobiernos, empresas, ciudadanos, mensajes de radio y satélite, llamadas de teléfono, faxes y correos electrónicos de casi todo el mundo.
- Analiza automáticamente la información y la clasifica para la alianza de inteligencia militar formada por Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda

Introducción al espionaje y cibervigilancia

Países que utilizan el espionaje. China

- Según un informe de la ONU sobre la libertad de expresión y opinión, revela que China es uno de los países que más espía a sus ciudadanos a través de internet junto con Siria, Irán y Vietnam.

- Se comenta, incluso, que autoridades de estos países realizan ataques de phishing para controlar a los ciudadanos, aunque no está probado.

- Es obligatorio realizar un registro de datos personales a quienes quieren crear un blog o web en estos países.

Introducción al espionaje y cibervigilancia

Países que utilizan el espionaje. EEUU

- Espionaje a Irán. Gusano Stuxnet

  Es un malware desarrollado presuntamente por Israel y Estados Unidos diseñado para infectar infraestructuras críticas (en este caso una central nuclear) que infectó a 60.000 equipos en Irán.

- NSA (National Security Agency)

  Es la agencia de inteligencia del Gobierno de los Estados Unidos que se encarga de todo lo relacionado con la seguridad de la información. En ocasiones se ha puesto en entredicho la legalidad de sus prácticas (según varios textos legislativos de carácter nivel nacional e internacional).

Introducción al espionaje y cibervigilancia

Países que utilizan el espionaje. EEUU

- Proyectos filtrados de la NSA:
  - TREASURE MAP
  - MYSTIC
  - PRISM
  - XKEYSCORE
  - BULLRUN
  - Otras prácticas de Ciberespionaje utilizadas por la NSA consistentes en análisis de metadatos, recopilación de SMS o propagación de virus informáticos.

Índice

Métodos de obtención de información

- Buscadores web.
- Herramientas de búsqueda de personas.
- Consulta de dominios.
- Metadatos.
- Repositorios.

Métodos de obtención de información

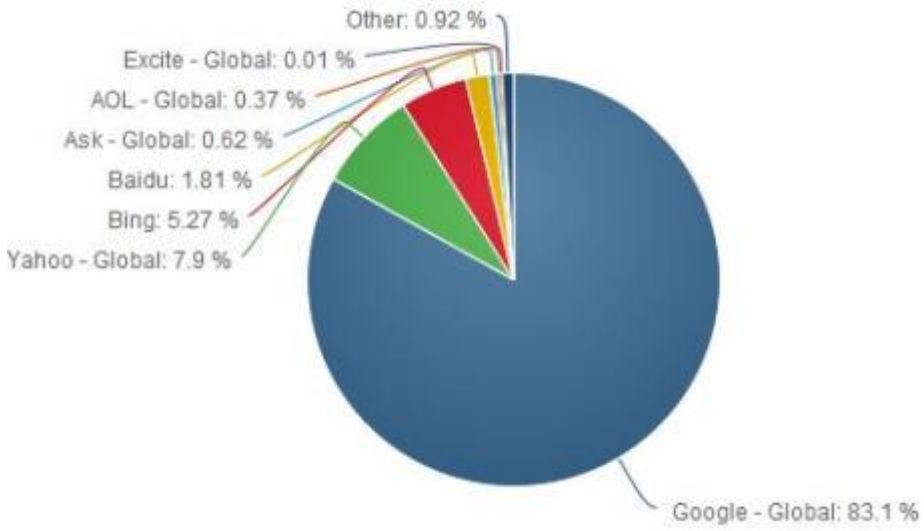
¿Qué es un motor de búsqueda?

- Es un sistema informático que busca archivos almacenados en servidores web.

- Las búsquedas se realizan gracias a los crawlers (arañas web).

- Los crawlers recorren las páginas web recopilando información sobre los contenidos de las mismas.

- Un ejemplo son los buscadores de internet, que pueden buscar en varios servicios.



Métodos de obtención de información

Buscadores web

- Los buscadores web poseen gran cantidad de información almacenada en sus sistemas.

- Los más famosos son:
  - Google
  - Bing
  - Yahoo!
  - Baidu
  - Ask

Métodos de obtención de información

Buscadores web. Robots.txt

- Cada página web decide qué quiere indexar o no utilizando un archivo llamado Robots.txt el cual se encuentra alojado en la raíz de su estructura de carpetas.

- Esta información es muy útil ya que revela directorios ocultos que el administrador no quiere que conozcamos, los cuales pueden contener información confidencial.

Métodos de obtención de información

Buscadores web. Robots.txt

- Ejemplos:

```
User-agent: *
Disallow: /
```

Impide el acceso a todas las URLs para todos los buscadores.

```
User-agent: *
Disallow: /cgi-bin/
Disallow: /tmp/
Disallow: /junk/
Disallow: /folder/
Allow: /folder/file.html
```

Impide el acceso a ciertos directorios.
Permite el acceso a una URL específica dentro de un directorio restringido.

```
User-agent: Googlebot
Allow: /
```

Permite al robot de Google el acceso a todas las URLs.

```
User-agent: *
Disallow: /admin/
Disallow: /*?
Disallow: /*.asp$
```

Impide un directorio y ciertas URLs.

Métodos de obtención de información

Buscadores web. GOOGLE

- Google es el buscador más usado a nivel mundial que nos permite buscar la información que queramos siguiendo unos criterios de búsqueda.

- Para facilitar la tarea de búsqueda, Google permite el uso de unos operadores propios que permiten un filtrado más preciso de la información.

- Operadores más usados:
  - " "
  - -
  - Site
  - Filetype
  - Inurl
  - Intitle
  - Link

Métodos de obtención de información

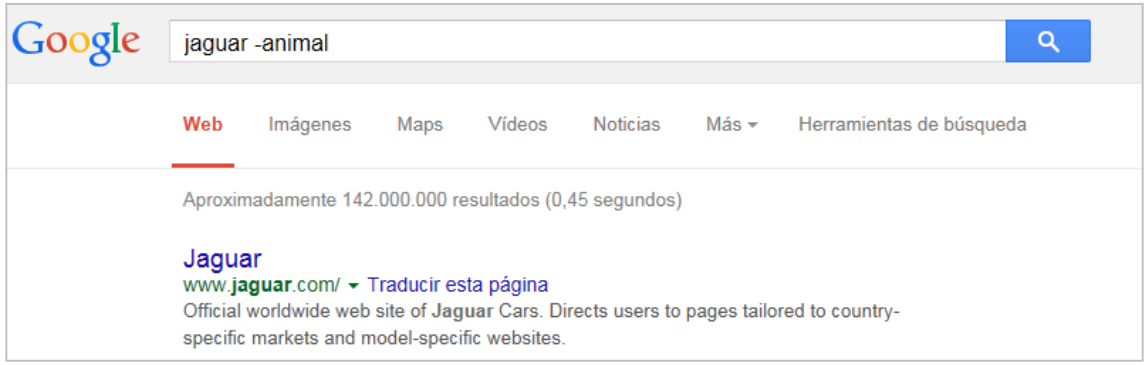
Buscadores web. GOOGLE

- Operador “ ”

  Se utiliza para especificar la búsqueda exacta de la cadena.

- Operador –

  Se utiliza para eliminar palabras en la búsqueda.

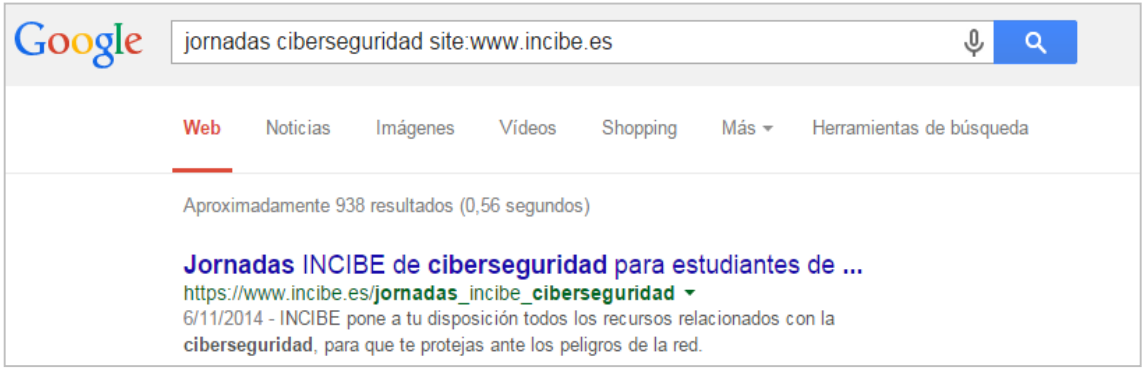


Métodos de obtención de información

Buscadores web. GOOGLE

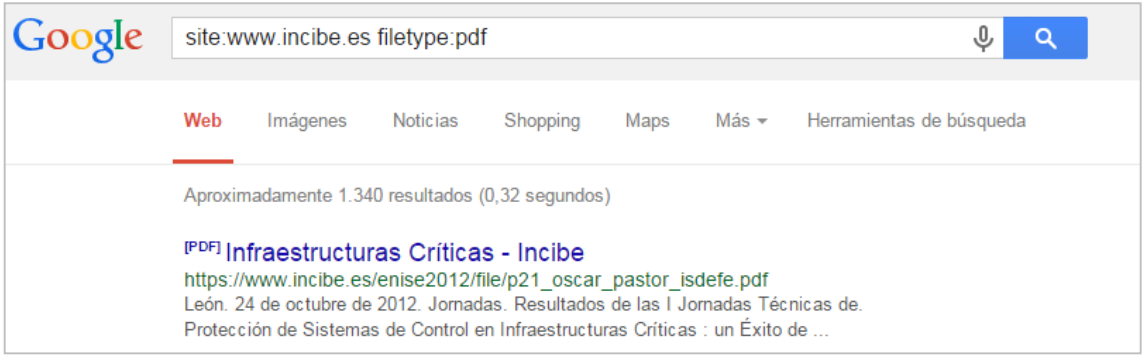
- Operador *site*

  Se utiliza para buscar en un determinado dominio.



- Operador *filetype*

  Se utiliza para especificar un tipo de extensión de archivo.

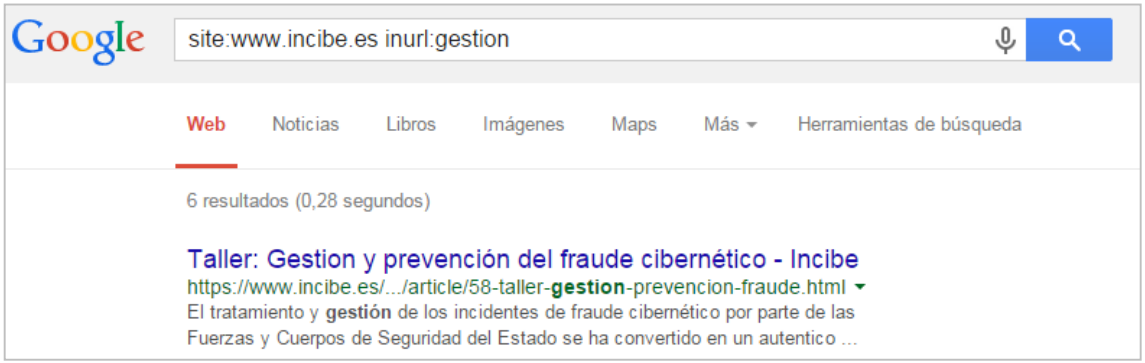


Métodos de obtención de información

Buscadores web. GOOGLE

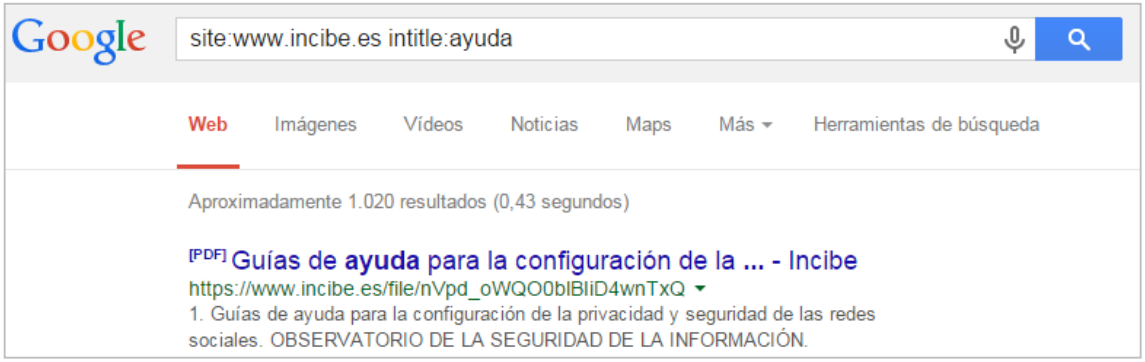
- Operador *inurl*

  Se utiliza para buscar el término en la URL.



- Operador *intitle*

  Se utiliza para buscar páginas con el término en el título.

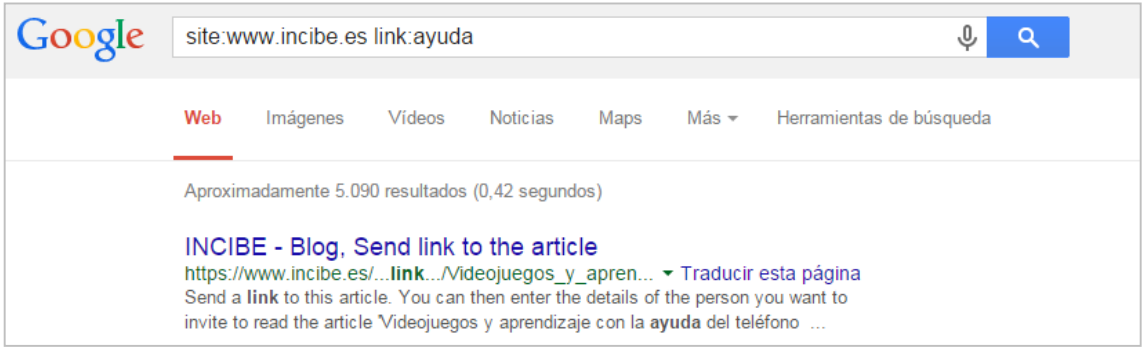


Métodos de obtención de información

Buscadores web. GOOGLE

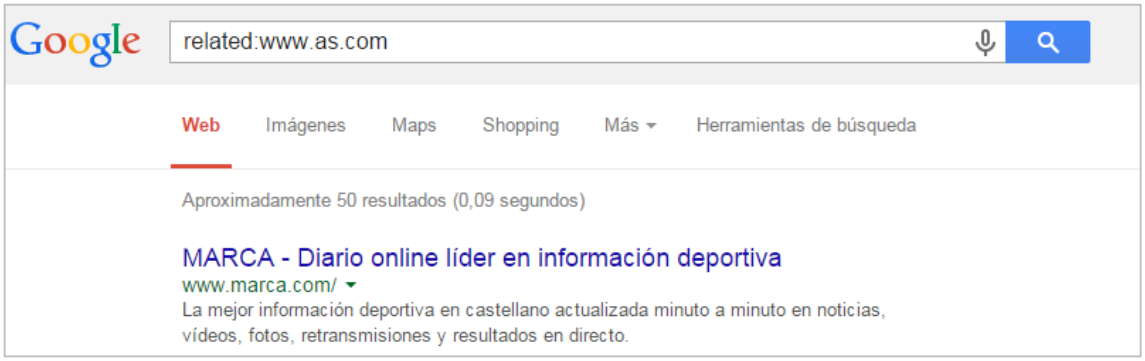
- Operador *link*

  Busca páginas donde aparezca el término dado y que incluyen links en ella.



- Operador *related*

  Se utiliza para mostrar páginas relacionadas.



Métodos de obtención de información

Buscadores web. GOOGLE

Otros comandos de interés…

- Operador *ext*
  Similar al operador filetype. Muestra resultados con la extensión dada.
- Operador *+*
  Solo muestra páginas con el término dado.
- Operador *OR*
  Muestra resultados que incluyan una palabra u otra.
- Operador *Cache*
  Muestra la caché de la página dada. Útil para cuando se elimina contenido.
- Operador *info*
  Muestra información de la página dada.
- Operador intext
  Muestra páginas que en su contenido se encuentre el término dado.

Métodos de obtención de información

Práctica: búsqueda en Google

- ¿Podrías buscar **documentos PDF** en la página de **Incibe** que hablen de **firmas digitales**, pero **no** de certificados digitales?

- ¿Qué cadenas de búsqueda podrías utilizar para buscar páginas de intranet (para empleados) de una empresa en concreto?

Métodos de obtención de información

Buscadores web. GOOGLE DORKS

¿Qué son los Google Dorks?

- Son combinaciones de operadores de búsqueda que se utilizan para extraer información valiosa y concreta desde Google.
- La palabra Dork es despectiva y significa persona inepta.

¿Cómo puedo utilizarlos?

- De forma manual utilizando los operadores vistos anteriormente
- A través de Dorks ya publicados en la web.

Fuente: *www.exploit-db.com/**google-dorks***

Métodos de obtención de información

Buscadores web. GOOGLE DORKS

- Ejemplo de Dorks:

DATE	Title	Summary
2014-10-14	inurl:logon.html "CSCOE"	Pages containing login portals - Web Server Detection Finds logins portals for Cisco ASA Cl...
2014-10-09	intitle:FRITZ!Box inurl:login.lua	Show open FritzBox-Router with intitle:FRITZ!Box inurl:login.lua ...
2014-10-02	intitle:"virtual office" sonicwall domai...	Network or vulnerability data IP address AD Domain NameLogin entry/method for internal network...
2014-08-09	intitle:"index" intext:"Login to th...	via Priyal Viroja...
2014-04-21	intitle:"Zimbra Web Client Log In"	Open Source Zimbra Webmail Login pages ...
2014-04-21	intitle:"Zimbra Web Client Sign In"	Open Source Zimbra Webmail Login pages ...
2014-04-07	inurl:typo3/install/index.php?mode=	typo3 install logins Bruno Schmid ...
2014-03-31	inurl:"Citrix/XenApp/auth/login.aspx"	Finds login portals for Citrix XenApp. - Andy G - twitter.com/vxhex ...
2014-02-28	intitle:Admin inurl:login.php site:.co.in	dork submitted by M4RKM3N aka Osama Mahmood revels admin login panels of sites :) ...

Métodos de obtención de información

Buscadores web. BING (Microsoft)

- El buscador BING es otro de los grandes buscadores de información que permiten un filtrado de los resultados mediante operadores.

- Los operadores de Google y Bing son similares pero hay ciertas diferencias.

Métodos de obtención de información

Buscadores web. BING (Microsoft)

- filetype
- feed
- contains
- ip
- loc
- prefer
- site
- intitle
- inbody
- inanchor
- hasfeed
- instreamset

Práctica: búsqueda en Bing

- ¿Podrías buscar archivos Excel en la página de **INCIBE**?
- ¿Qué cadenas de búsqueda podrías utilizar para buscar páginas de intranet (para empleados) de una empresa en concreto?

Métodos de obtención de información

Buscadores de dispositivos. SHODAN

- Es un buscador que no busca páginas web como Google o Bing.
- Detecta servidores, cámaras web, impresoras, routers y todo aquello que se conecta a internet.
- Encuentra dispositivos conectados a internet con configuraciones seguridad vulnerables o de fábrica.
- Shodan, al contrario de Google y Bing, solo devuelve un número limitado de entradas a la consulta, ya que para obtener resultados sin limitaciones es necesario pagar una cuota.

Métodos de obtención de información

Buscadores web. SHODAN

Operadores que soporta Shodan en su versión gratuita:

- Country
- City
- Port
- Net
- Hostname

Práctica: búsqueda en Shodan

- ¿Podrías buscar cámaras IP en el buscador de Shodan?
- Si has encontrado alguna cámara web IP conectada. ¿Tiene algún tipo de protección?

Métodos de obtención de información

Herramientas de búsqueda de personas. PeekYou

- Motor de búsqueda de personas que te permite encontrar a cualquier contacto en las diferentes redes sociales de manera rápida y sencilla.
- No se necesita estar registrado.
- Servicio gratuito.

Fuente: *http://www.peekyou.com*

Métodos de obtención de información

Herramientas de búsqueda de personas. Pipl

- Gran motor de búsqueda de personas en redes sociales.
- No se necesita estar registrado.
- Servicio gratuito.

Fuente: *https://**pipl**.com*

Métodos de obtención de información

Herramientas de búsqueda de personas. Páginas blancas

- Versión electrónica de la famosa guía telefónica.
- Base de datos que contiene datos información de nombres con su dirección y teléfonos asociados.
- Servicio gratuito.
- Sin registro
- Existe en multitud de países como por ejemplo:
  - España
  - Argentina
  - Turquía
  - …

PaginasBlancas.es

Fuente: http://blancas.paginasamarillas.es/jsp/home.jsp

Métodos de obtención de información

Práctica: Información personal en Google

- **PASO 1:** Abrir un navegador de internet y entrar en la página de **Google**

  https://www.google.es/

- **PASO 2:** Buscar información vuestra en internet

- **PASO 3:** Utilizar alguna de las herramientas de búsqueda de personas vistas anteriormente.

¿Habéis detectado información personal publicada sin vuestro consentimiento?

Métodos de obtención de información

Consulta de dominios

¿Qué es una consulta de dominio?

- Es un proceso en el que se pregunta al servidor de nombres de dominios (DNS) para obtener información relacionada con el dominio o el host.
- Un host es una computadora conectada a una red que ofrecen servicios de transferencias de archivos, bases de datos, servidores web, etc.

¿Para qué queremos esto?

- Ver si el DNS está resolviendo bien los nombres y las IPs.
  - Saber la dirección IP de un dominio.
  - Saber el nombre del dominio a través de una dirección IP.
- Diagnosticar problemas de configuración que pudieran haber surgido en el DNS.

Métodos de obtención de información

Consulta de dominios

DNS

- El protocolo DNS es el conjunto de reglas que gobierna la traducción entre **direcciones IP** y nombres.
- IP (**Internet Protocol**) es uno de los protocolos fundamentales para el funcionamiento de Internet e identifica con una **dirección** a los elementos de su red.
- Estas direcciones son difíciles de manejar para los humanos (especialmente en IPv6), de forma que en internet existe un sistema de traducción de nombres para identificar clientes y servidores.

- Dirección IPv4 (32 bits): 192.168.1.10
- Dirección IPv6 (128 bits): 2001:0db8:1234:0000:0000:0000:0000:0001

Métodos de obtención de información

Consulta de dominios

DNS. Funcionamiento

- ¿Cómo funciona un DNS?


```
root@EYLab: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@EYLab:~# host www.incibe.es
www.incibe.es has address 195.53.165.153
root@EYLab:~#
```

Métodos de obtención de información

Consulta de dominios

Nslookup

- Es un comando de administración de red incluido en sistemas operativos UNIX y Windows.
- Consulta DNS para obtener el nombre del dominio o la IP de un sitio web.
- Ejemplo:

```
C:\Users>nslookup es.wikipedia.org
Server:
Address:

Non-authoritative answer:
Name:    es.wikipedia.org
Addresses:  2620:0:862:ed1a::1
          91.198.174.192
```

Métodos de obtención de información

Consulta de dominios

Práctica: Nslookup

- **PASO 1:** Abre la consola de comandos de Windows:

  Inicio->Programas->Accesorios->CMD

- **PASO 2:** Escribe el siguiente comando para ver la dirección IP de un sitio web:

  nslookup [sitio web]

- **PASO 3:** Escribe el siguiente comando para ver el host a través de una dirección IP:

  nslookup xxx.xxx.xxx.xxx

¿Ha resuelto la dirección IP?

Métodos de obtención de información

Consulta de dominios

Herramientas automáticas

robtex

Práctica: Robtex

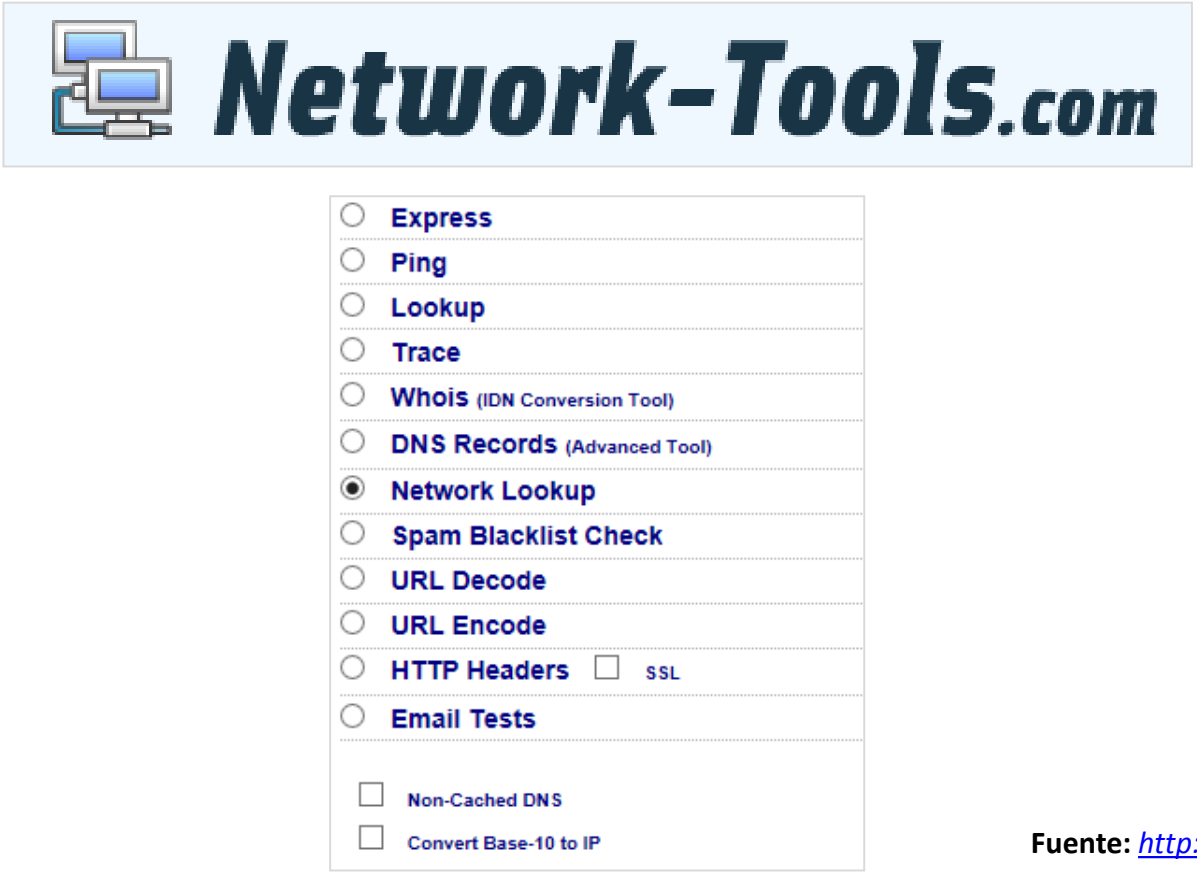
- Comprobar si con esta herramienta automática resuelve la dirección IP
- Ver información relevante

Fuente: *https://www.**robtex**.com/*

Métodos de obtención de información

Consulta de dominios

Herramientas automáticas



Fuente: http://network-tools.com/

Métodos de obtención de información

Metadatos

- Los documentos almacenan información adicional en el propio fichero.
- Esta información puede contener:
  - Usuario creador.
  - Fecha de creación.
  - Fecha de modificación.
  - Software utilizado.

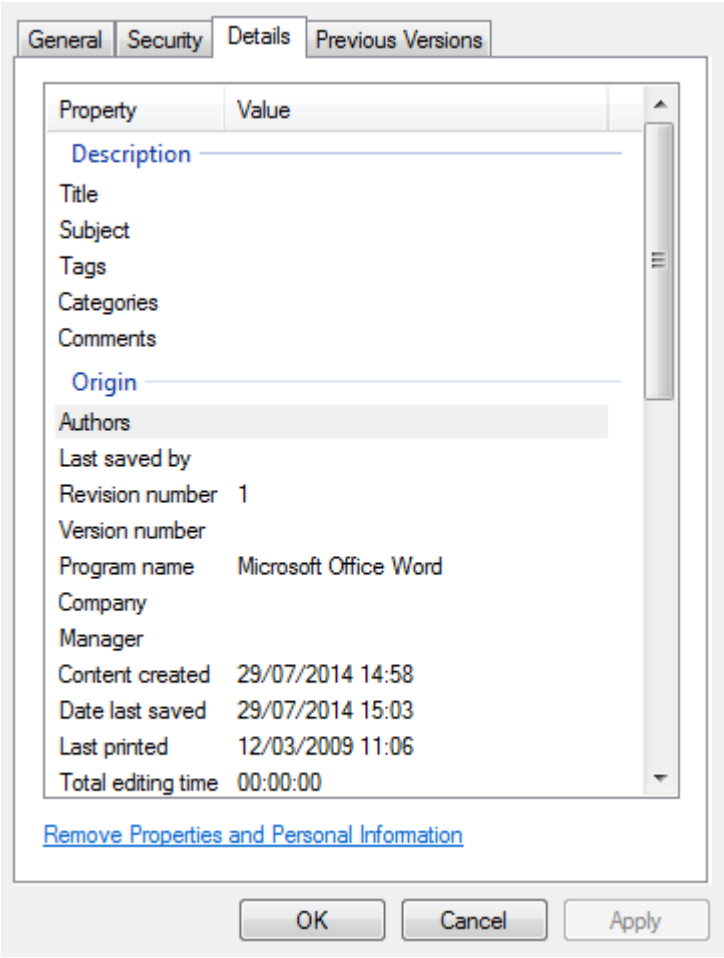
Herramientas

- Exiftool → Para sistemas Linux y Windows.
- Foca Free → Para sistemas Windows.
- Propiedades del fichero.

Métodos de obtención de información

Práctica: Análisis de metadatos

- Crear un documento con una herramienta ofimática.
- Seleccionar el fichero y visualizar sus propiedades.
- En la pestaña “detalles”, analizar los metadatos del fichero.

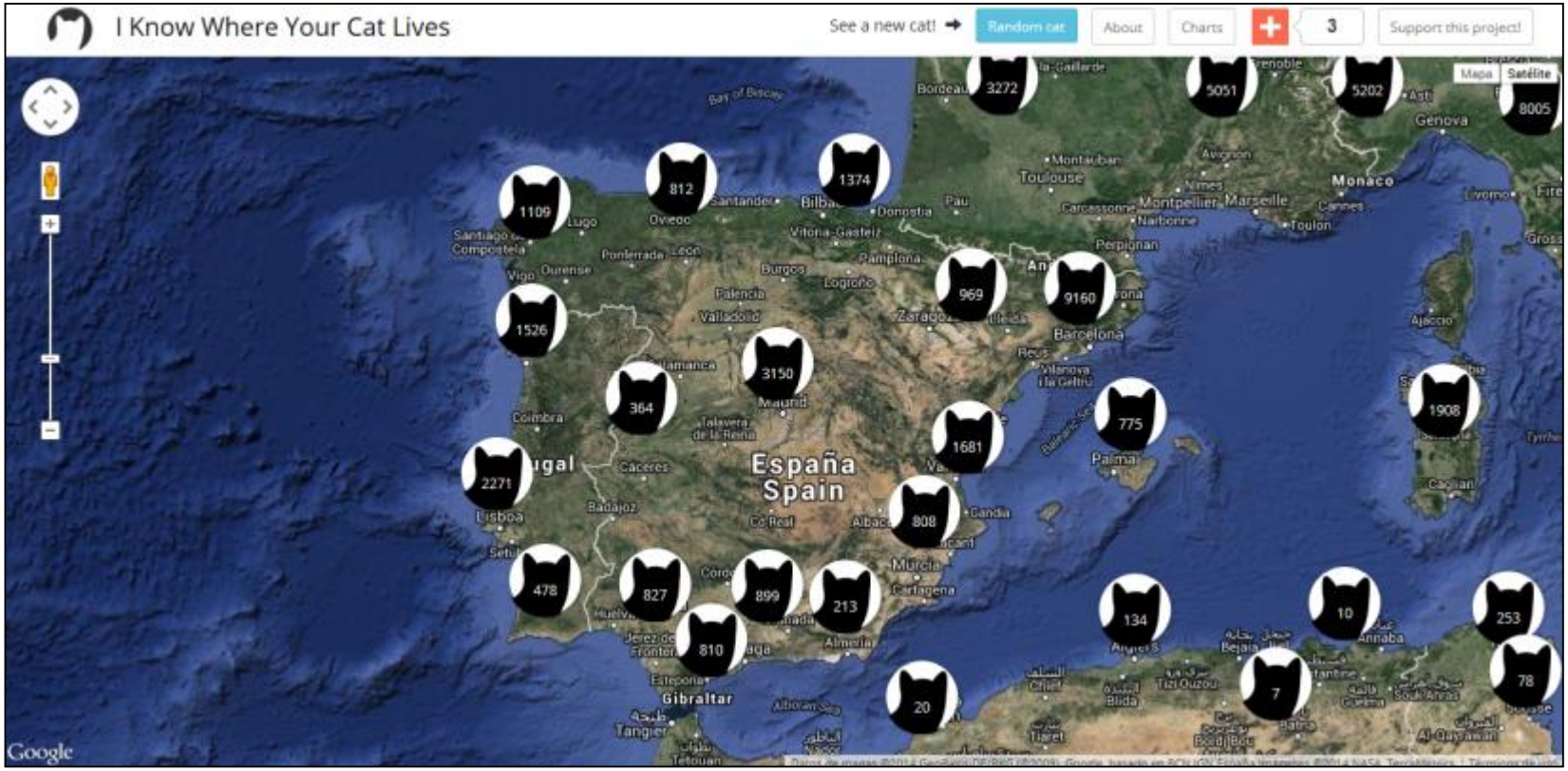


Práctica: Eliminar metadatos

- En la pestaña “detalles” seleccionar la eliminación de propiedades e información personal.
- Verificar la correcta eliminación de los metadatos.

Métodos de obtención de información

Ejemplo: Metadatos incrustadas en imágenes de gatos



Métodos de obtención de información

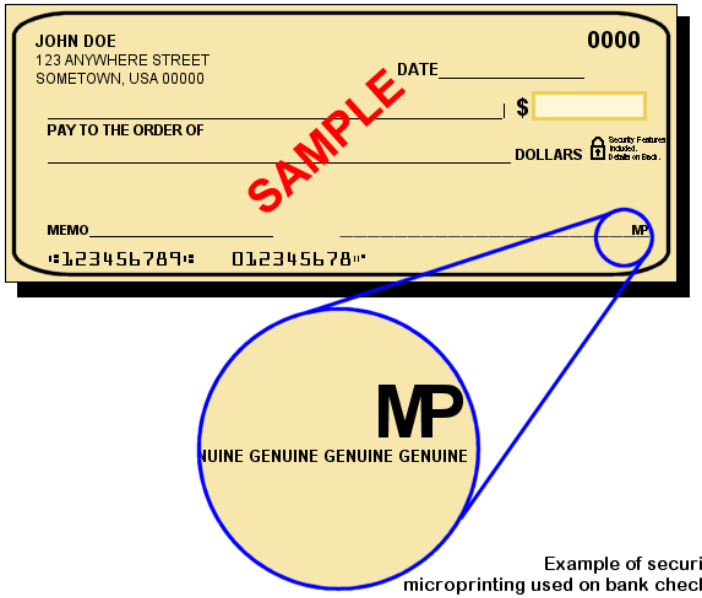
Esteganografía

- Es la ciencia y/o arte de ocultar una información dentro de mensajes u objetos para que no se perciba su existencia.

- La finalidad es establecer un canal encubierto de comunicación para enviar mensajes que pasen inadvertidos para el observador.

Estegoanálisis

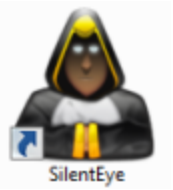
- Es la ciencia que estudia la detección y/o eliminación de información oculta en canales encubiertos.



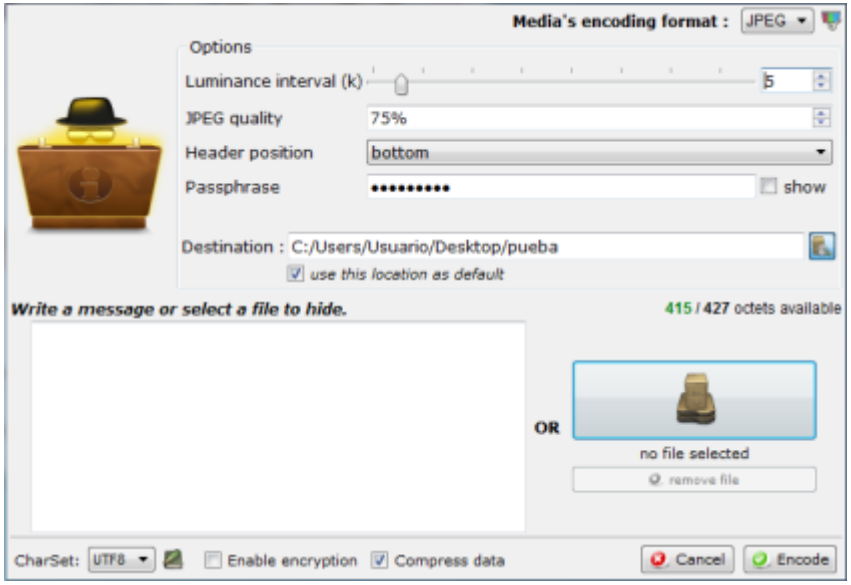
Example of security microprinting used on bank checks

Métodos de obtención de información

Práctica: Incrustar texto oculto en una imagen



- Abrimos el programa SilentEye situado en el escritorio.
- Seleccionamos una imagen y la arrastramos hasta el programa SilentEye.
- Hacemos clic en el botón Encode y utilizaremos la siguiente configuración:
  - Passphrase es la contraseña.
  - Destino es la ruta en la que se guardará la imagen con el texto oculto.
  - Escribimos el texto que queremos ocultar.

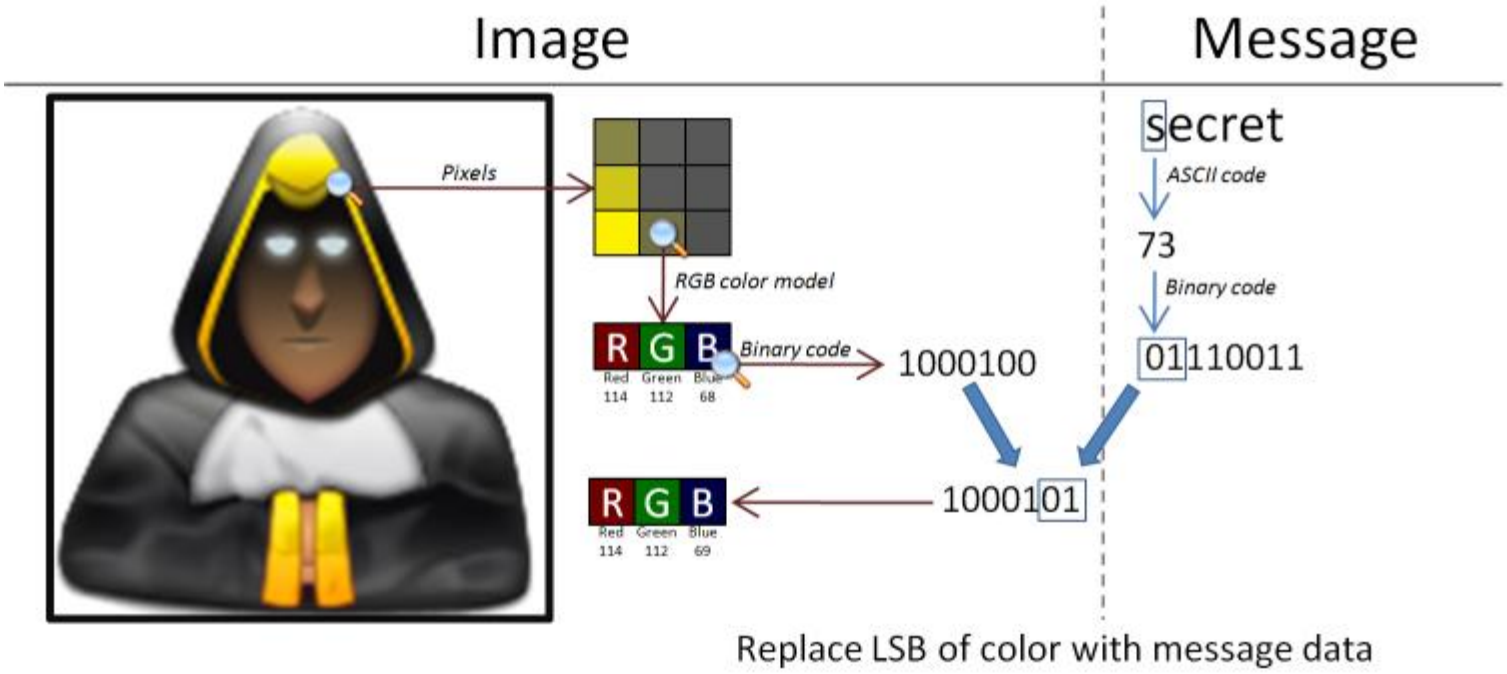


Fuente: *www.silenteye.org*

Métodos de obtención de información

¿Cómo funciona esto?

- Utilizando el algoritmo de sustitución LSB (Least Significant Byte)

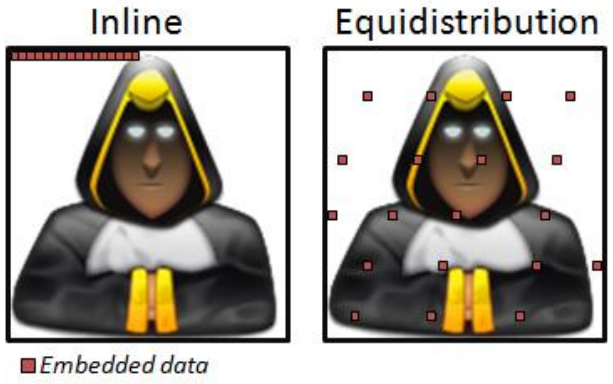


Fuente: [www.**silenteye**.org](http://www.silenteye.org)

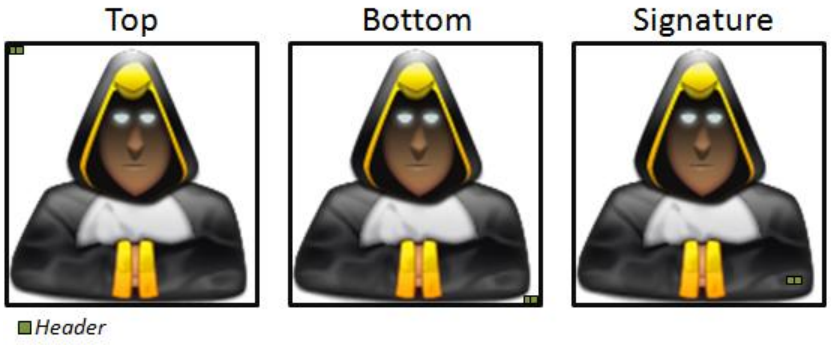
Métodos de obtención de información

¿Cómo funciona esto?

- Utilizando modelos de distribución



- Configurando las cabeceras



Fuente: *www.silenteye.org*

Métodos de obtención de información

Repositorios

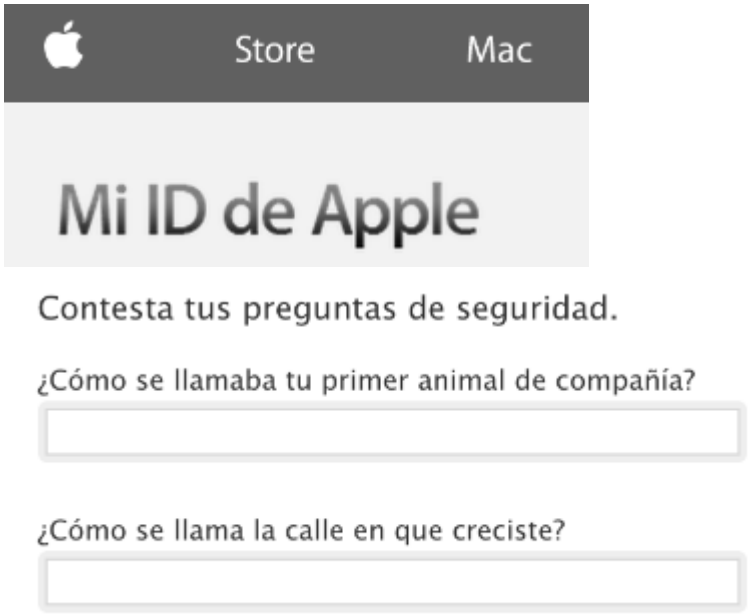
- Un repositorio es un sitio centralizado donde se almacena y mantiene información digital.
- Normalmente se encuentra en la forma de bases de datos o archivos informáticos.
- Los repositorios más conocidos son:
- Pastebin

- Reddit

Métodos de obtención de información

Práctica: Obtención de información en redes sociales

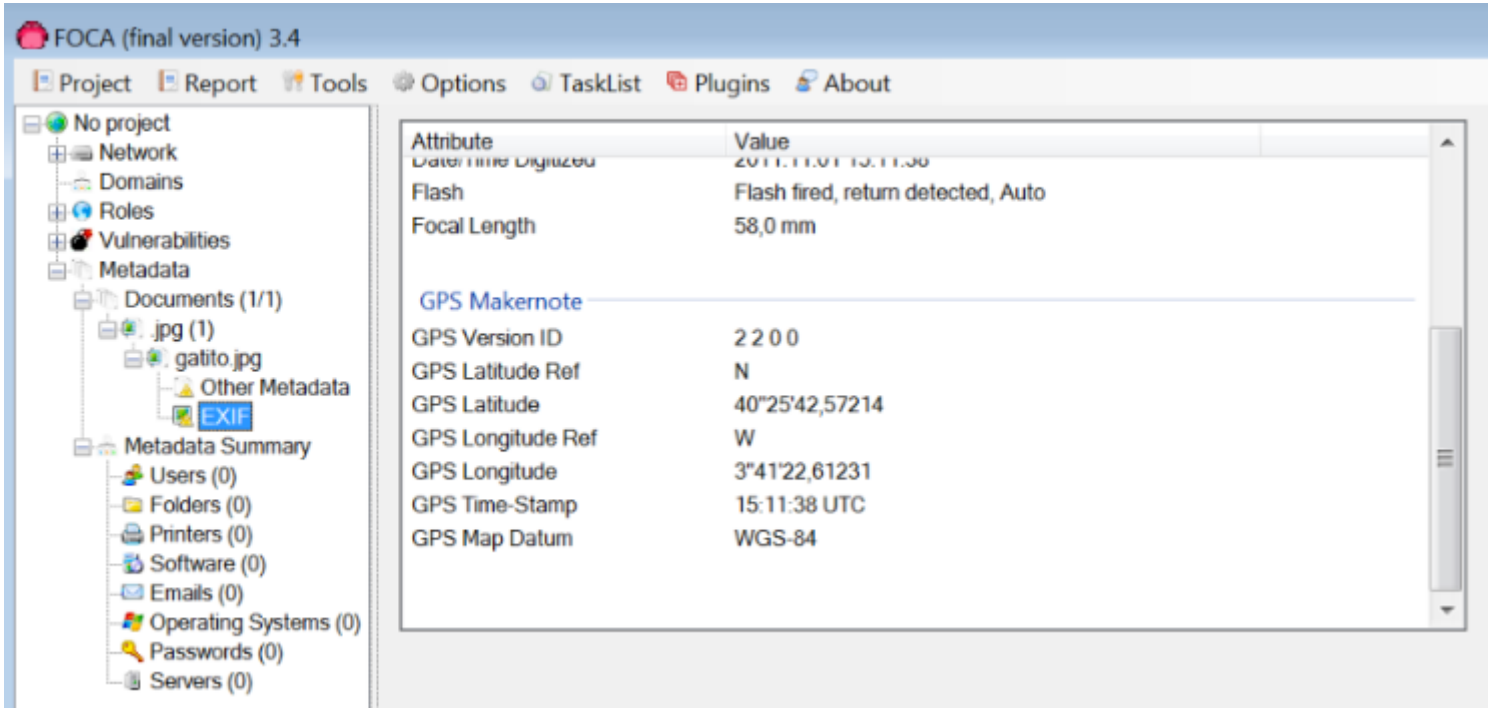
- El objetivo de este ejercicio será obtener las respuestas a las preguntas de seguridad de la cuenta Apple de John Cinebi



Métodos de obtención de información

Práctica: Obtención de información en redes sociales

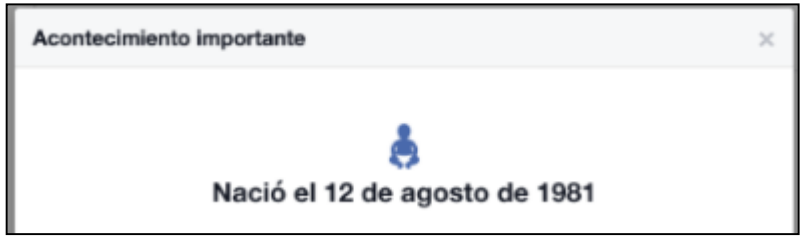
- Para ello, puedes utilizar la información pública de sus redes sociales (Twitter, Facebook, Google+…)
- Necesitarás las herramientas Foca Free y GeoSetter.



Métodos de obtención de información

Práctica - Solución: Obtención de información en redes sociales

- Lo primero que solicita Apple es la fecha de nacimiento del propietario de la cuenta. Esta información se puede obtener fácilmente de Facebook:

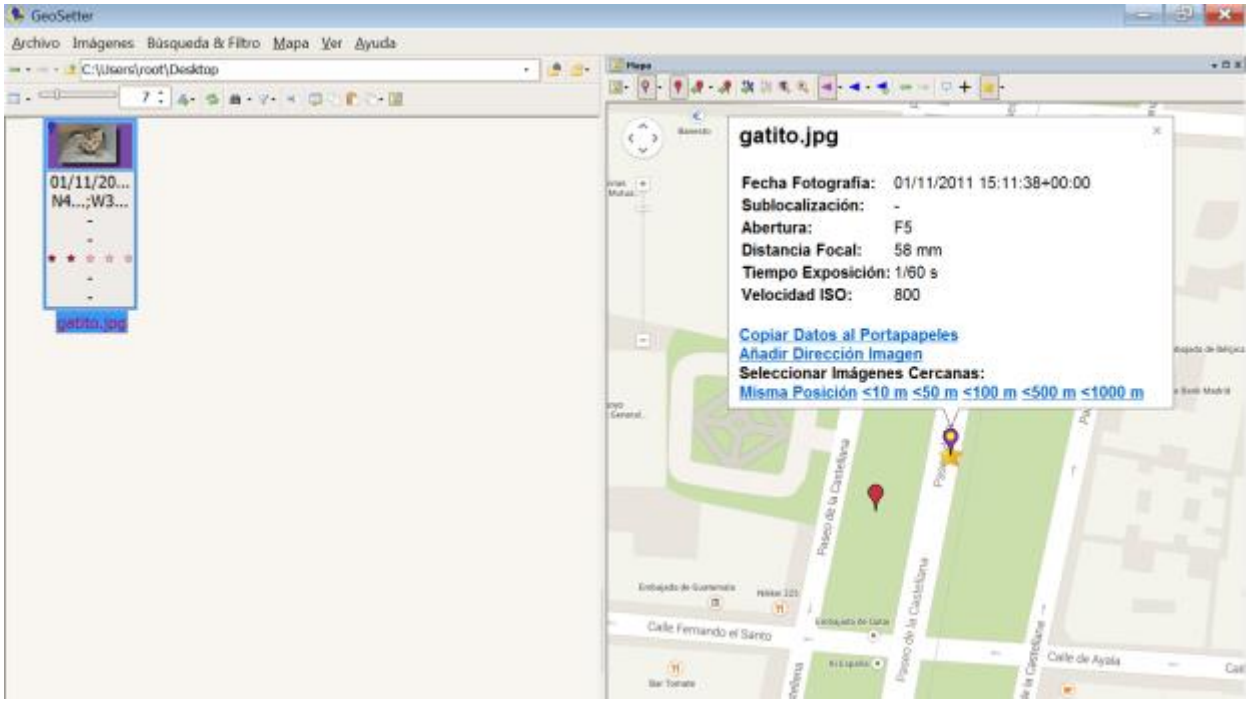


- El nombre del animal de compañía de John Cinebi (Lucas) está publicado en Twitter:

Métodos de obtención de información

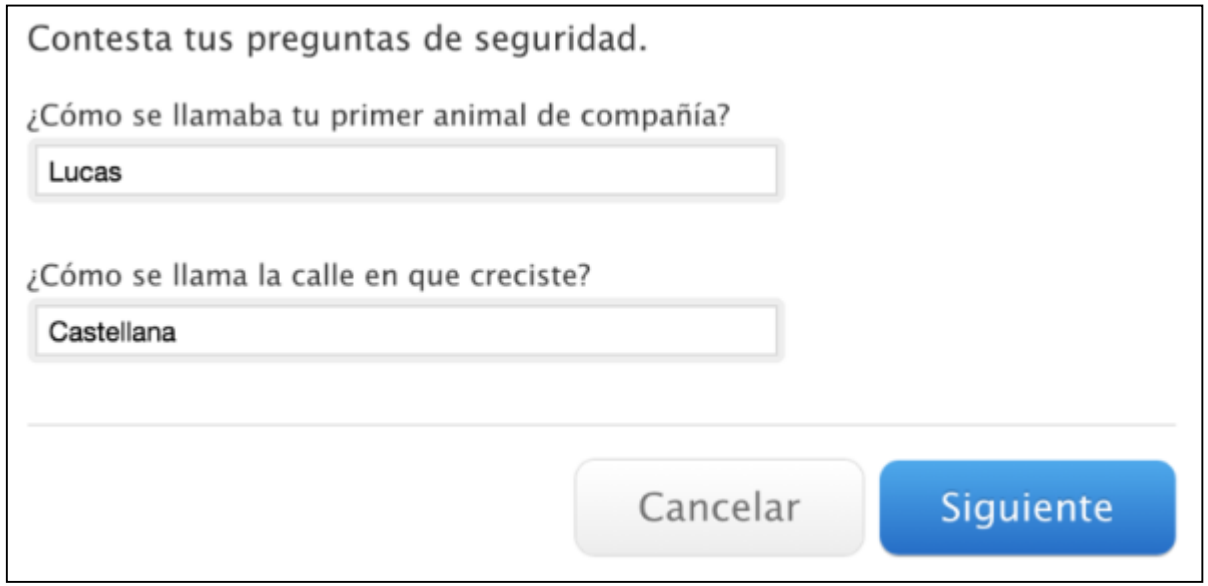
Práctica - Solución: Obtención de información en redes sociales

- La última pregunta es el nombre de la calle en la que vive John Cinebi. Esta información está disponible en los metadatos de la foto publicada en Dropbox. Para extraerla, se puede utilizar la herramienta GeoSetter:



Métodos de obtención de información

Práctica - Solución: Obtención de información en redes sociales



Métodos de obtención de información

Caso con gran repercusión: Celebgate

APPLE ACTÚA ANTE EL CELBGATE

Por BERENICE ÁRCEGA SARMIENTO 05 DE SEPTIEMBRE DE 2014

La compañía ha presentado una nueva alerta de seguridad para evitar las filtraciones de fotos y demás información privada.

Dicha alerta permitirá tomar acción inmediata de las siguientes formas: ya sea cambiando la contraseña para recuperar el control de la misma, o bien alertando al equipo de seguridad de Apple. Además, al respecto de las investigaciones llevadas a cabo por Apple para determinar el método de hackeo, se ha llegado a la conclusión, tras más de 40 horas de trabajo, que el ataque se produjo mediante el empleo de nombres de usuario, contraseñas y preguntas de seguridad de las famosas, una práctica que se ha convertido en algo frecuente.

Índice

Deep Web

¿Qué es la deep web?

- Es todo el contenido de internet que no está indexado por los motores de búsqueda.
- La mayor parte de la información encontrada en la deep web está generada dinámicamente para que los motores de búsqueda no puedan hallarla.

Esta red es utilizada para cometer actos delictivos (mafias, pederastas, mercado negro, etc.). Debido a ello, se recomienda un acceso responsable a la misma.

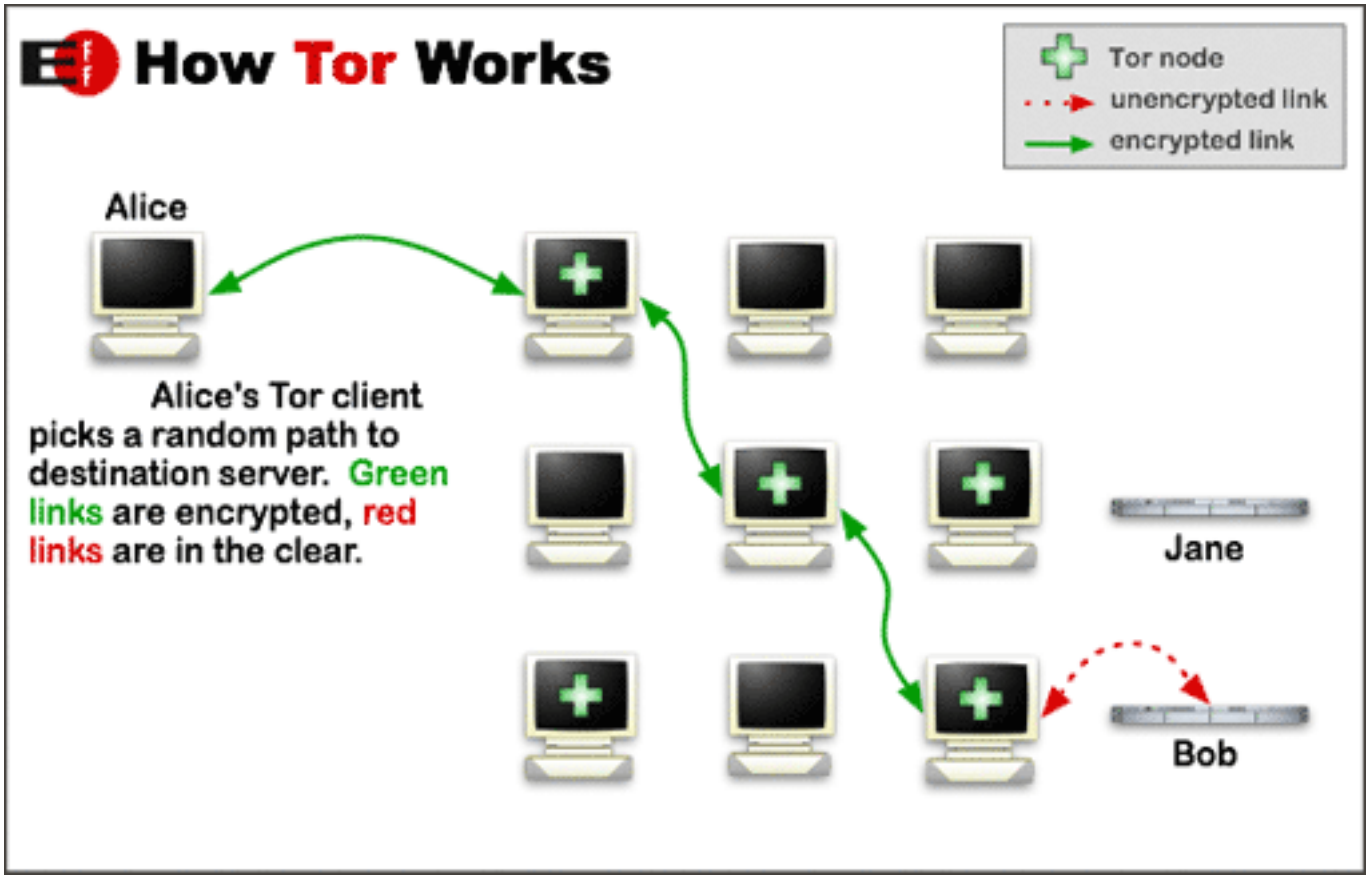
Deep Web

¿Qué significa TOR?

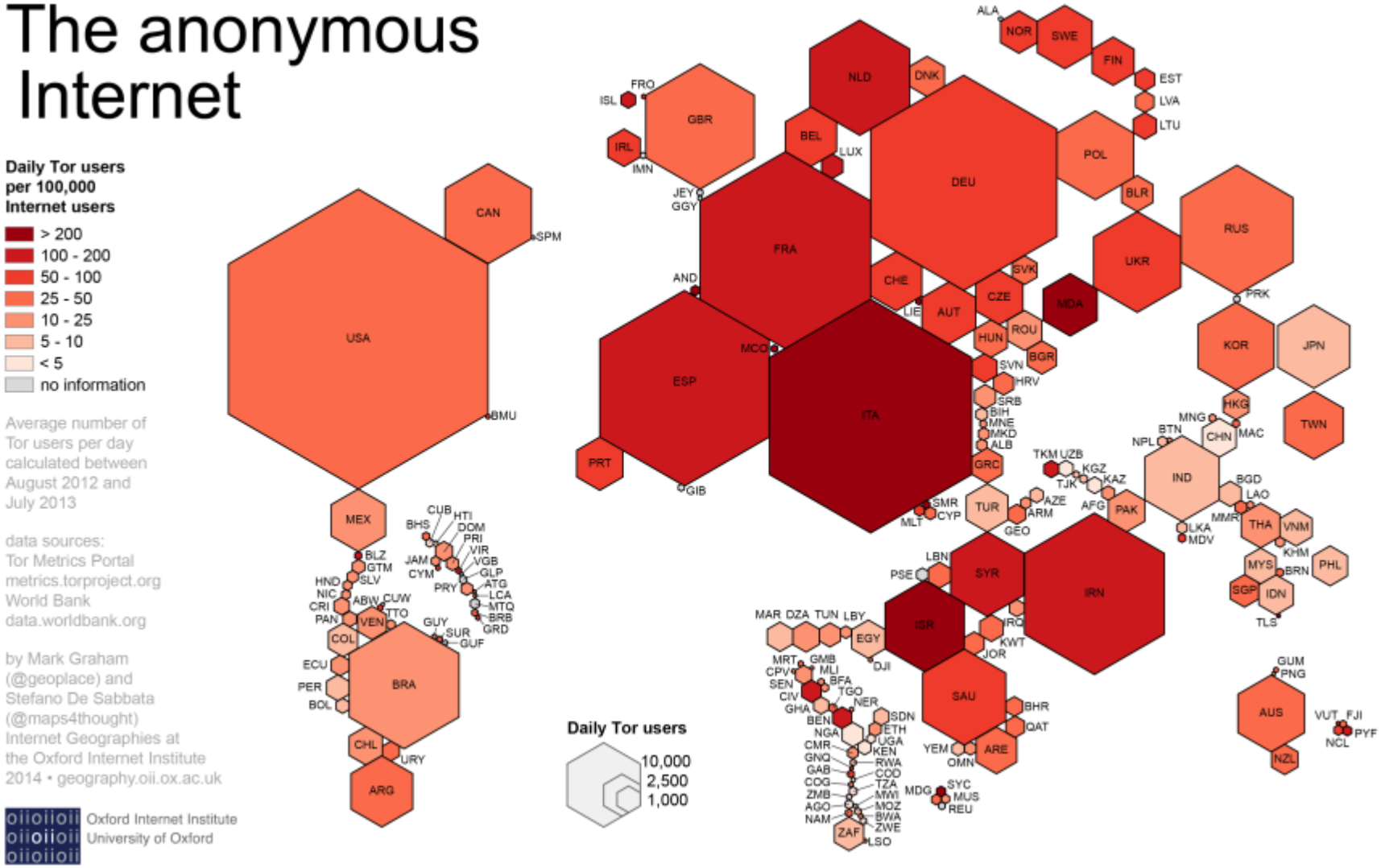
- The Onion Router, abreviado como Tor, cuyas principales características son:
  - Es una red de comunicaciones distribuida superpuesta sobre internet.
  - Su principal característica es el anonimato (IP anónima).
  - Mantiene la integridad de la información.
  - La información que viaja sigue el principio de confidencialidad.
  - Es utilizada para navegar de forma anónima y evadir restricciones. En países como China es uno de las pocas posibilidades de navegación sin restricciones.

Deep Web

¿Cómo funciona?



Deep Web


The anonymous Internet
Daily Tor users per 100,000 Internet users
> 200
100 - 200
50 - 100
25 - 50
10 - 25
5 - 10
< 5
no information
Average number of Tor users per day calculated between August 2012 and July 2013
data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org
by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk
Oxford Internet Institute
University of Oxford
Daily Tor users
10,000
2,500
1,000

Deep Web

Algunos casos con gran repercusión

Fuente : http://www.as.com ; http://www.cuatro.com

Deep Web

Esta práctica se realiza sobre un entorno controlado. Se desaconseja su realización en un entorno real.

Práctica: Navegación anónima con TOR

- **PASO 1:** Abrir un navegador de internet y entrar en la siguiente página web:

  http://whatismyipaddress.com/

- **PASO 2:** Apunta la dirección IP en un archivo de texto. IP Pública

- **PASO 3:** Abrir el navegador TOR Browser situado en el escritorio y entrar otra vez en la página web:

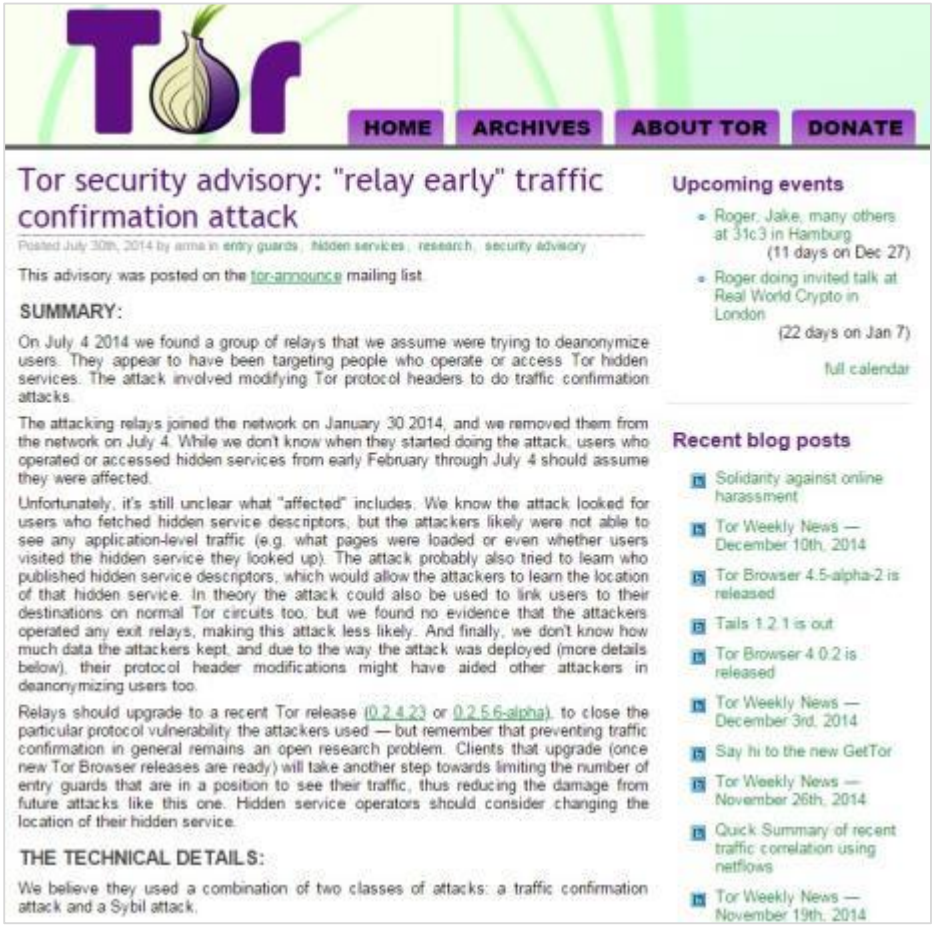
  http://whatismyipaddress.com/

¿Qué ocurre con la nueva IP?

Deep Web

El fin del anonimato…

- Ataque dirigido a TOR en Julio 2014
- Objetivo: Desmantelar el anonimato de los usuarios conectados en la red



Tor

HOME ARCHIVES ABOUT TOR DONATE

Tor security advisory: "relay early" traffic confirmation attack

Posted July 30th, 2014 by arma in entry guards, hidden services, research, security advisory

This advisory was posted on the tor-announce mailing list.

SUMMARY:

On July 4 2014 we found a group of relays that we assume were trying to deanonymize users. They appear to have been targeting people who operate or access Tor hidden services. The attack involved modifying Tor protocol headers to do traffic confirmation attacks.

The attacking relays joined the network on January 30 2014, and we removed them from the network on July 4. While we don't know when they started doing the attack, users who operated or accessed hidden services from early February through July 4 should assume they were affected.

Unfortunately, it's still unclear what "affected" includes. We know the attack looked for users who fetched hidden service descriptors, but the attackers likely were not able to see any application-level traffic (e.g. what pages were loaded or even whether users visited the hidden service they looked up). The attack probably also tried to learn who published hidden service descriptors, which would allow the attackers to learn the location of that hidden service. In theory the attack could also be used to link users to their destinations on normal Tor circuits too, but we found no evidence that the attackers operated any exit relays, making this attack less likely. And finally, we don't know how much data the attackers kept, and due to the way the attack was deployed (more details below), their protocol header modifications might have aided other attackers in deanonymizing users too.

Relays should upgrade to a recent Tor release (0.2.4.23 or 0.2.5.6-alpha), to close the particular protocol vulnerability the attackers used — but remember that preventing traffic confirmation in general remains an open research problem. Clients that upgrade (once new Tor Browser releases are ready) will take another step towards limiting the number of entry guards that are in a position to see their traffic, thus reducing the damage from future attacks like this one. Hidden service operators should consider changing the location of their hidden service.

THE TECHNICAL DETAILS:

We believe they used a combination of two classes of attacks: a traffic confirmation attack and a Sybil attack.

Upcoming events

- Roger, Jake, many others at 31c3 in Hamburg (11 days on Dec 27)
- Roger doing invited talk at Real World Crypto in London (22 days on Jan 7)

full calendar

Recent blog posts

- Solidarity against online harassment
- Tor Weekly News — December 10th, 2014
- Tor Browser 4.5-alpha-2 is released
- Tails 1.2.1 is out
- Tor Browser 4.0.2 is released
- Tor Weekly News — December 3rd, 2014
- Say hi to the new GetTor
- Tor Weekly News — November 26th, 2014
- Quick Summary of recent traffic correlation using netflows
- Tor Weekly News — November 19th, 2014

Índice

Evasión de restricciones

- A la hora de navegar por internet, un factor importante a tener en cuenta es el anonimato.

- Web proxy
  - Proxify
  - HideMyAss

- Archive.org

- Google translate

- VPN

- Tor

Fuentes: *https://**proxify**.com* ; *https://www.**hidemyass**.com* ; ***https://translate.google.com/*** ; *www.**hotspotshield**.com/*

Índice

Resumen

¿Qué hemos visto en esta jornada?

- Qué es la cibervigilancia y el espionaje.
- Un poco de historia. El espionaje a través de los tiempos.
- Qué métodos existen para obtener información a través de internet
  - Buscadores web y de personas
  - Herramientas de dominios
  - Información oculta en archivos → METADATOS
  - Contenedores de información online → REPOSITORIOS
- Qué es la red TOR y Deep Web con ejemplos prácticos.
- Métodos de evasión de restricciones en la web

Ejercicios realizados sobre un entorno controlado.
Se desaconseja su realización en un entorno real.

Resumen

Cuestiones

1. ¿Qué método de cifrado sustituye cada letra del alfabeto por una equivalente tras aplicar un desplazamiento en el mismo?

2. ¿Qué son los metadatos? ¿Qué tipo de información pueden contener?

3. ¿Por qué es importante controlar nuestra información publicada en internet? ¿Cómo puede afectar internet a nuestra privacidad?

4. ¿Qué es la Deep Web? ¿Y la red TOR?

5. ¿Qué métodos de evasión de restricciones en la web conoces?

Resumen

Respuestas

1. El método de cifrado César.
2. En el propio fichero del documento hay almacenada información adicional como: usuario creador, fecha de creación, fecha de modificación, software utilizado, etc. Esta información adicional son los metadatos.
3. Es importante para no perder nuestra privacidad en internet y estar más seguros al navegar por la red. Si no adoptamos las medidas adecuadas podemos poner a dominio público nuestra información personal como páginas consultadas, información confidencial, mostrar dónde estamos, fecha de creación y de modificación de un documento, etc.
4. La Deep Web es el contenido de internet que no está indexado por los motores de búsqueda, de esta manera no se puede hallar utilizando un buscador. Debido a sus características, la emplean muchos ciberdelincuentes. La red TOR es una red de comunicaciones distribuida superpuesta sobre internet que mantiene el anonimato y la integridad de la información.
5. Existen varios métodos como el empleo de algún Webproxy (Proxify, HideMyAss), utilizar una VPN, usar TOR, consultar páginas como Archive.org o emplear Google Translate para acceder a páginas.

Índice

Gracias

por tu atención

Contáctanos

Contacto (más información y dudas sobre las jornadas):

espaciosciberseguridad@incibe.es

En las redes sociales:

@incibe
@certsi
@osiseguridad
@CyberCampES

Oficina de Seguridad del internauta
(Pienso luego clico)

INCIBE
OSIseguridad

Oficina de Seguridad del internauta
CyberCamp

Pág. INCIBE
Grupo INCIBE

Oficina de Seguridad del internauta

En la sede:
Avenida José Aguado, 41 - Edificio INCIBE
24005 León
Tlf. 987 877 189

En los sitios web:
www.incibe.es
www.osi.es
www.cybercamp.es