Las Huellas informáticas

ÍNDICE

El rastro informático: "Todo deja huella"

1.- Introducción

Internet en nuestras vidas es una herramienta necesaria para nuestro día a día, actualmente cualquier persona es capaz de conectarse a la red. Por esto mismo, es necesario conocer más sobre ella; muchas personas creen que al conectarse a Internet, como están detrás de una pantalla, creen que son totalmente anónimas y pueden hacer y decir todo lo que les plazca, sin el peligro de ser descubiertas.

Así pues, mi trabajo de investigación consiste en esto. Quiero mostrar cómo poder navegar en la red sin dejar ningún tipo de rastro y saber qué acciones quedan marcadas y de qué manera.

Para empezar a hablar sobre qué es el rastro informático y cuáles son las huellas que vamos dejando una vez que nos conectamos, habría que saber qué es Internet y cómo se estructura.

[1]Se puede pensar que Internet pertenece a alguien o tiene su paradero físico en algún lugar concreto, pero esto no es así. Internet no lo posee nadie ya que es una colección de redes de todos los tamaños y clases. Estas redes se conectan unas a otras de muchas maneras diferentes para formar una única identidad que conocemos como Internet. De hecho, de esto viene su nombre, Internet se llama así dado que su fin era la interconexión de distintas redes (inter-net)

2.- Estructura de Internet

La estructura de Internet se basa en una jerarquía de redes.

Todo ordenador que se conecta a Internet es parte de una red. Por ejemplo, puede que uses un modem o una conexión ADSL para conectar con tu proveedora de servicios de Internet **ISP**. Cuando te conectas a tu ISP, te vuelves parte de su red. La ISP entonces puede que se conecte con una red más grande y se vuelva parte de la otra red. Internet es simplemente una red de redes.

ISP (Internet service provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cablemódem, GSM, dial-up, etcétera.

Internet se estructura utilizando el **protocolo Ipv4** (Internet Protocol Version 4) a través de **direcciones IP** que identifican a cada usuario.

Ahora bien, una vez escuchados los conceptos en los que se va a basar este trabajo; tendríamos que tener una idea bastante clara de lo que son.

La definición más importante que tenemos que tener en cuenta es la de dirección IP.

Dirección IP es una etiqueta para asignar un número de conexión a todos los usuarios que se conectan a la red.

Hay varios tipos de conexiones IP, hay direcciones IP *privadas* o *públicas* y *dinámicas* o *fijas.*

2.1.- Direcciones Ipv4 e Ipv6

Estas direcciones IP se empezaron asignando con el protocolo Ipv4, que usa direcciones de 32 bits; esto quiere decir que el número de direcciones que puede crear son $(2^{32} = 4\,294\,967\,296)$ direcciones IP únicas.

Como no se esperaba que Internet evolucionara tan rápido, ni que el protocolo Ipv4 tuviera tanto éxito, han empezado a escasear este tipo de direcciones, y limitar el crecimiento y el uso de Internet, sobretodo en India y China. Por esto se ha creado el protocolo Ipv6, que se está empezando a implementar poco a poco.

Este **protocolo Ipv6**, nos ofrece el mismo tipo de direcciones que el Ipv4 pero extiende muchísimo el límite admitiendo 340 sextillones de direcciones $(2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456\,)$

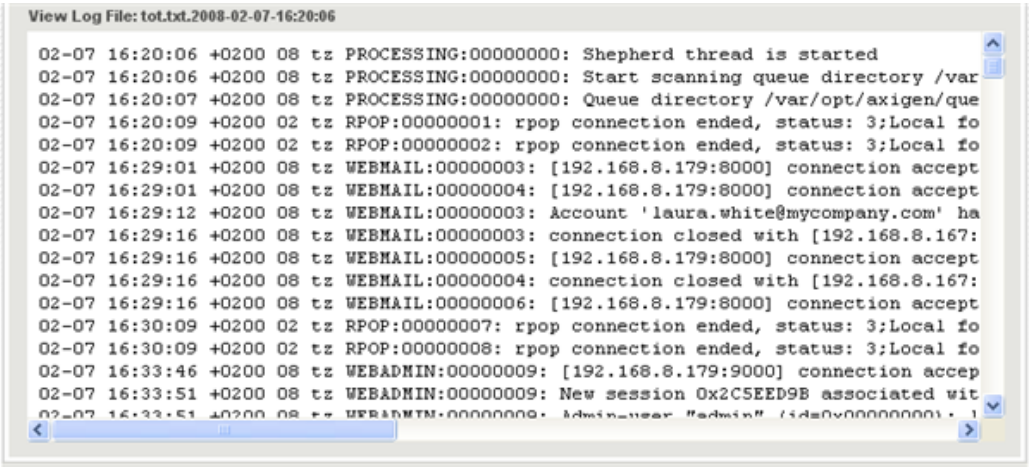
2.2.- Archivos log

Cuando hemos introducido los conceptos de direcciones IP y los protocolos que las crean hemos de saber también qué son los archivos log.

La palabra log viene del inglés, que significa bitácora.

Cada servidor tiene un archivo log que debe ir guardando para tener un recuento de todas las conexiones que se han ido produciendo en cada momento por si se comete algún tipo de infracción cibernética o por si se necesita en otro momento para cualquier otro fin.

Estos archivos reflejan qué, cómo, cuándo y dónde se produce un evento para un dispositivo o particular.



Una vez definidos los conceptos de archivos log, direcciones IP y tocados por encima los conceptos de Ipv4 e Ipv6 querremos saber cómo se estructura Internet.

Internet se creó por el desarrollo masivo de redes **LAN o WAN**, este tipo de redes eran sencillas y unían ordenadores de empresas o particulares.

Este tipo de redes siguen existiendo en la actualidad para distintos fines, pero sin duda fueron las que preceden a la red a la que todos estamos conectados, Internet.

Internet funciona con la estrategia **Cliente/Servidor**, lo que significa que en la Red hay ordenadores 'Servidores' que dan una información concreta en el momento que se solicite, y por otro lado están los ordenadores que piden dicha información, los llamados 'Clientes'.

2.3.- Protocolo TCP/IP

Existe una gran variedad de "lenguajes" que usan los ordenadores para comunicarse por Internet. Estos lenguajes se llaman Protocolos.
Se ha establecido que en Internet, toda la información ha de ser transmitida mediante el **Protocolo TCP/IP**.
TCP/IP son las siglas de "Transfer Control Protocol / Internet Protocol esto significa que este protocolo se encarga de trasferir paquetes de información. Cuando un ordenador quiere mandar otro un fichero de datos, lo primero que hace es partirlo en trozos pequeños (de unos 4kb) y posteriormente enviar cada trozo por separado.

Nada más conectarnos a Internet aparece nuestro navegador predeterminado y preferido. Un web browser o navegador es una aplicación que opera a través de Internet, interpretando archivos y sitios web desarrollados a menudo en código HTML que contienen información y contenido en hipertexto de todas las partes del mundo.

HTML es un tipo de código muy extendido en la utilización de Internet ya que permite crear fácilmente contenido de hipertexto.

Los navegadores de Internet más conocidos son: Mozilla Firefox, Google Chrome, Safari (navegador únicamente creado para dispositivos IOS), Internet Explorer, Opera…

Todos estos navegadores tienen una opción incluida que se identifica como "navegación privada o anónima". Esta navegación tiene la funcionalidad de no recopilar las distintas páginas web a las que nos hemos ido conectando en nuestro historial de búsqueda.

Con esto puede parecer sencillo, ya que pone “navegación privada” y te da la sensación de que estas como más seguro, tu información está más protegida por así decirlo, pero esto, es totalmente mentira.

Que tu información no quede recopilada en tu historial de búsqueda no significa que esta información ya se haya borrado, es más, cuando un usuario se conecta a Internet con esta opción habilitada, esto queda grabado en los archivos log de los que hemos hablado antes de las páginas a las que te has ido conectando: lo que permite, con un poco de entendimiento del código HTML y el acceso a estos archivos, saber qué persona se ha conectado a esa página web, sabiendo que ese usuario no quiere que se quede guardado que ha estado en la misma. Así que, en definitiva, al querer esconderte, lo único que estás haciendo es exponerte mucho más ante cualquier administrador de páginas o antes las mismas autoridades que espían lo que has estado investigando o viendo. Pero de este tema hablaremos un poquito más adelante.

3.- 7 rastros importantes

Ahora vamos a dar una vuelta a todos los rastros, señales o huellas que vamos dejando por las cuales se nos puede identificar fácilmente, no solo quién somos sino desde donde nos conectamos y a qué hora exacta lo hacemos.

Hay 7 rastros importantes que vamos dejando, según dijo 8Fabrizio (Mejía Madrid) hace ya unos años:

3.1.- El historial de audio

Google te escucha cada vez que le hablas, y guarda celosamente esa información. Es útil para mejorar el reconocimiento de tu voz y poder usar la función Ok Google desde cualquier pantalla de tu teléfono. Para consultarlo sólo tienes que ir a esta dirección, iniciando sesión con tu cuenta de Google.

Aunque de por sí no es mucho peor que el Historial de búsquedas normal, lo cierto es que ver un recopilatorio con tus fragmentos de voz con todo lo que

[1] Fabrizio Mejía Madrid fue columnista por quince años del periódico La Jornada. Ha colaborado en medios como Proceso, Reforma, Letras Libres y Gatopardo.

has preguntando a tu teléfono da algo de repelús.

Si no quieres que Google siga guardando esta información, ve a las opciones de Búsqueda por voz en tu teléfono y desactiva el Historial de audio.

3.2.- El historial de ubicaciones

Parecido al anterior, el historial de ubicaciones es todavía más concreto. Tu teléfono Android toma buena nota de donde estás en todo momento, formando un planning extremadamente preciso de tu rutina diaria. De entrada da un poco de miedo, pero el historial puede ser útil. Además, los datos se muestran en un gráfico con la posibilidad de reproducirlo en forma de animación. En cualquier

caso, puedes eliminar del mapa manualmente puntos concretos, días o el historial entero de un plumazo.

Si lo que quieres es borrar todo el historial, entonces desactiva los Informes de Ubicación en los Ajustes de Ubicación de tu teléfono Android.

3.3.- La lista de aplicaciones instaladas

Google guarda una lista de todas y cada una de ellas. Este historial no se puede desactivar, pero sí puedes eliminar elementos independientes, eso sí, sólo desde tu teléfono.

3.4.- El historial de búsquedas en Facebook

¿Alguna vez te has preguntado cómo puede Facebook saber cuál de los millones de "Pedros" que hay en el mundo es el que quieres ver? No es tan difícil, Facebook recuerda a quién has buscado antes, y te los muestra los primeros.

El registro de búsquedas es obviamente privado y no se publica en tu biografía. Puedes eliminar búsquedas concretas haciendo clic en le icono de la señal de prohibido y después pulsando Eliminar.

3.5.- Los contactos importados en Facebook

Facebook recuerda todos los contactos que has importado desde Messenger, skype, twitter, gmail, etc. Y te ofrece como sugerencias de amistad a los amigos de tus amigos que has ido importando desde otras redes sociales.

3.6.- La lista de apps a las que te has registrado con Facebook y Google

El inicio de sesión con Facebook o Google es comodísimo. No necesitas escribir tus datos a mano o confirmar el correo. En unos segundos, ya lo tienes funcionando. Pero, con el paso del tiempo, la lista de apps en las que te has registrado crece y crece, con la posibilidad de que alguien las consulte.

Las buenas noticias son que Facebook ha mejorado el apartado de aplicaciones conectadas y ahora es bastante más fácil y rápido borrar apps que ya no usas.

3.7.- Tu edad, sexo, idiomas e intereses

Mientras navegas por la red, todo lo que haces es analizado por unos complejos sistemas cuyo único propósito es catalogarte lo mejor posible para ofrecerte la publicidad que mejor funciona para ti.

Este perfil se basa bien en tus datos reales de tu cuenta de Google o en los sitios webs que visitas. Si lo deseas, puedes deshabilitar esta personalización de los anuncios tanto en Google como en cualquier sitio web que use AdSense. Para ello, pulsa Inhabilitar los anuncios basados en intereses.

- Hay muchos más rastros que quedan marcados, pero estos son los más característicos.

4.- ¿Qué tenemos que hacer para ser anónimos?

Ya conocidas todas las acciones que van quedando registradas cuando nos conectamos, dónde quedan estas mismas y de qué manera, nos urge preguntarnos cómo poder hacer para que esto no ocurra y poder hacerlo de manera totalmente libre y "segura"

Como hemos dicho antes, la navegación privada u oculta podría ser una buena alternativa si esta estuviera implementada de otro modo, pero esta facilidad lo único que hace es no guardar ningún dato en nuestro navegador de esa conexión (lo cual nos beneficia para no recibir ningún tipo de anuncio o publicidad relacionada con el tema sobre el que hemos estado navegando) y también nos ayuda, ya que descarta todas las cookies recibidas en el acceso.

En Europa la Comisión Europea es una de las que más presión ha estado haciendo para intentar asegurar al máximo la privacidad de los usuarios dentro de su territorio. Si bien se permite el uso de *cookies* no se permite que lo hagan de forma invisible para el usuario, los sitios web tienen que informar de forma clara que el sitio está guardando estos datos en su equipo, con que objetivo lo hace, y por cuanto tiempo serán guardados. El usuario será el que tiene que decidir si permite guardar que se guarde la cookie o no. Aunque hay pequeñas excepciones: se salvan las cookies más importantes, que sean imprescindibles para el correcto funcionamiento del sitio web.

Pero todas nuestras búsquedas y accesos que hemos ido haciendo en nuestra incursión quedan totalmente registrados en los archivos log de cada servidor y en los servidores de nuestra proveedora de servicios de Internet ISP.

Esto nos lleva a cuestionarnos si de verdad existe alguna manera de poder ser **ANÓNIMO** en la red.

La respuesta a esta pregunta es: Si eres una persona normal y corriente que para lo único que utiliza Internet es para hacer unas cuantas búsquedas en Internet y beneficiarse de esta utilidad; no, en ningún momento se te ofrecerá la opción de poder navegar con total libertad por así decirlo. Pero no se te ofrece,

no para poder aprovecharse de ti, no, al contrario, no se te ofrece para poder ayudarte y así que se te haga más sencillo en tus próximas búsquedas.

Pero en cambio, si eres una persona que necesita que sus datos sean totalmente secretos o confidenciales sí que podrás conectarte a Internet sin revelar tu identidad. Esta funcionalidad la aplican altos cargos de la NSA y de los gobiernos de distintos países, al igual que la CIA, el FBI u organismos que requieran de esta utilidad en beneficio de la seguridad de su país.

Estos organismos secretos, o confidenciales, lo que hacen es crear un software que tienen en todos sus dispositivos electrónicos conectados a la red que les permite, al mismo tiempo que se conectan, ir borrando los archivos log de cada servidor relacionados con ellos. Para ello, utilizan, obviamente, una orden judicial de la que deben requerir y una ISP propia.

5.- El mundo del misterio y el anonimato

Dado que hay personas y organismo que poseen esta funcionalidad de poder conectarse a Internet anónimamente, sería conveniente saber cuáles son y por qué pueden hacerlo

Como he mencionado antes, todos los organismos confidenciales, privados o de seguridad nacional, por razones obvias son capaces de mantenerse en la sombra mientras observan las acciones que las personas normales vamos realizando.

Pero después, se encuentran los “hackers”, “ladrones de capucha informática” o como bien se les quiera llamar.

Estos, son usuarios normales y corrientes de Internet pero con grandes conocimientos cibernéticos, que aplican para evitar ser detectados por las autoridades o de los que se benefician para robar o defraudar.

Todos los hackers no son ladrones, es más, muchas de las personas que trabajan en las agencias del estado para velar por nuestra seguridad en la red han sido o son hackers. Pueden no trabajar para el estado, y solo usarlos para su propio beneficio olvidándose del fraude o luchando contra cosas que ellos creen que están más.

6.- Anonymous

Por eso, vamos a hablar de una organización mundialmente conocida, Anonymous.

Anonymous, es una organización compuesta por diferentes grupos e individuos que realizan acciones individuales o concertadas. Este grupo surgió del imageboard 4chan; que es un foro abierto sin moderadores totalmente libre. Por esto mismo, se cree que este grupo sigue algún tipo de política anarquista, ya que va en contra de muchas acciones capitalistas y no tiene ningún representante ni grupo que lidere.

Son personas con grandes conocimientos en informática, que pretenden hacer ver al mundo todo lo que las compañías secretas esconden, ya que defienden que toda la información en Internet debería ser abierta para que todo el mundo esté al tanto de ella.

Anonymous se organiza de manera difusa en la red, lo que dificulta encontrar algo oficial relacionado con Anonymous. Sin embargo, esta comunidad de personas organiza operaciones, debate del estado de los países y demás asuntos valiéndose de distintos canales online.

El nombre de *Anonymous* en sí mismo está inspirado en el anonimato que perciben los usuarios cuando publican comentarios e imágenes en Internet.

Su lema es:

Knowledge is free.	*El conocimiento es libre.*
We are Anonymous.	*Somos Anónimos.*
We are Legion.	*Somos Legión.*
We do not forgive.	*No perdonamos.*
We do not forget.	*No olvidamos.*
Expect us!	*¡Esperadnos!*

No todas las acciones de Anonymous son mencionadas ya que Anonymous ha estado activo por todo el mundo, solo se mencionarán las acciones más destacadas hablando a nivel mundial.

De entre los cientos de ataques que Anonymous ha realizado, destacaremos unos cuantos en Estados Unidos y en España.

6.1.- Principales acciones en EEUU

6.1.1.- Operación Payback

En el 2010 varias compañías de Bollywood contrataron a la compañía Aiplex Software para lanzar ataques DDoS contra sitios web que no respondieron a su advertencia de cierre. Activistas a favor de la piratería crearon entonces Operation Payback en Septiembre del 2010. El plan original era atacar Aiplex Software directamente, pero después de darse cuenta horas antes del ataque planeado que otra persona había denegado el servicio del sitio de la firma por su cuenta, Operation Payback dirigió su ataque contra sitios que defienden los derechos de autor como la MPAA y la IFPI, manteniendo los sitios desconectados un total combinado de 30 horas.En los siguientes días, atacaron a muchos de los sitios afiliados a la MPAA.

En diciembre de 2010, Operation Payback puso su atención en atacar a las páginas web de las compañías en contra de WikiLeaks.

6.1.2.- Gene Simmons

En una convención en 2010, Gene Simmons, miembro de la banda de rock Kiss, pidió a las compañías que tomaran medidas más agresivas hacia las infracciones de copyright. Miembros de Operation Payback pusieron su atención en sus dos sitios,simmonsrecords.com y genesimmons.com, dejándolos fuera de servicio a ambos por un total de 1 día y 14 horas. Durante el ataque la página genesimmons.com fue hackeada y redirigida hacia The Pirate Bay. Gene Simmons declaró a través de su página web que los miembros de Anonymous iban a terminar en la cárcel. Estas declaraciones fueron seguidas por más ataques contra sus sitios.

6.1.3.- WikiLeaks

A finales de 2010, la organización WikiLeaks estuvo sometida a mucha presión debido a la filtración de documentos diplomáticos de los Estados Unidos. En respuesta, Anonymous anunció su apoyo a WikiLeaks. Operation Payback cambió de objetivo para apoyar a WikiLeaks lanzando ataques DDoS contra Amazon, PayPal, MasterCard, Visa y el banco suizo PostFinance, en represalia por el bloqueo económico a WikiLeaks. Debido a los ataques, las páginas de MasterCard y Visa no fueron accesibles el día 8 de diciembre. Estos ataques también son conocidos con el nombre de “Operation Avenge Assange” (en español: Operación vengar a Assange).
Un investigador de amenazas de PandaLabs dijo que Anonymous también lanzo un ataque que tiró la página web del ministerio sueco cuando el fundador de WikiLeaks, Julian Assange, fue arrestado en Londres y rechazada su libertad bajo fianza.

6.1.4.- Ataque a HBGary Federal

El fin de semana del 5 y 6 de febrero de 2011 Aaron Barr, director ejecutivo de la firma de seguridad informática HBGary Federal (subsidiaria de HBGary), anunció que se había infiltrado con éxito en Anonymous, había logrado desenmascarar las identidades reales de la jerarquía del grupo e iba a revelar sus resultados en una conferencia posterior en San Francisco. En represalia por las declaraciones de Aaron Barr, los miembros de Anonymous hackearon el sitio web de HBGary Federal y reemplazaron la página inicial con un mensaje indicando que no deben «meterse» con Anonymous, y que el hackeo de la página web era necesario para defenderse a sí mismos.

6.1.5.- Operación Sony

El 5 de abril de 2011 Anonymous, comienza sus ataques DDoS a sitios web de Sony. Los ataques son a raíz de la puesta en marcha por parte de la compañía de acciones judiciales contra los usuarios “Geohot” y “Graf-Chokolo”, los cuales lograron “hackear” la PS3.También fue atacado de forma simultánea el sitio web del bufete de abogados Kilpatrick Townsend, que representa a Sony en su batalla legal.

El 7 de abril, dos días después, Anonymous anunció que detenia sus ataques contra Sony porque estaba perjudicando a los usuarios de PlayStation.

El 4 de mayo, Sony anuncia que Anonymous ha sido el causante del segundo ataque, en el que fueron robados todo tipo de datos personales y bancarios, de más de 100 millones de jugadores online. Sus afirmaciones se basaron en que encontraron un archivo en sus servidores llamado “Anonymous” con el texto “We are Legion”.

6.1.6.- Clausura de Megaupload

El 19 de enero de 2012, el FBI provocó el cierre del portal de descargas Megaupload, motivado por acusaciones de infracción de derechos de autor.En el operativo, fueron arrestadas siete personas en los Estados Unidos y cuatro en Nueva Zelanda, entre ellos el fundador, el ex hacker Kim Schmitz. Los acusados podrían enfrentar una pena de hasta 50 años de prisión.

En señal de protesta, Anonymous generó la caída de varios sitios, entre ellos el del Departamento de Justicia de los EEUU y el de Universal Music Group.

El día 24 de enero consiguió gran parte de las canciones de Sony Music y también varios videos y los pusieron para descarga gratuita., dando por inicio según Anonymous a “la guerra cibernetica mundial”

6.2.- Principales acciones en España

6.2.1.- Proyecto Chanology

Anonymous ganó fama mundial con el Proyecto Chanology, una protesta contra la Iglesia de la Cienciología.
El 14 de enero de 2008, un vídeo producido por la Iglesia de la Cienciología que mostraba una entrevista con Tom Cruise, un conocido cienciólogo, fue filtrado en Internet y subido a YouTube.
La Iglesia de la Cienciología pidió a YouTube que eliminara el vídeo por una violación del copyright. En respuesta Anonymous creo el Proyecto Chanology, considerando las acciones de la Iglesia de la Cienciología como censura y manifestando su intención de "expulsar a la iglesia de Internet". Los miembros del Proyecto Chanology organizaron ataques de denegación de servicio contra las páginas web de la Iglesia, bromas telefónicas y envíos de "faxes negros" a la Iglesia de la Cienciología.
El 21 de enero de 2008, Anonymous anunció sus objetivos e intenciones mediante un vídeo publicado en YouTube titulado "Mensaje a la Cienciología" ("Message to Scientology") y un comunicado de prensa declarando la "Guerra contra la Cienciología" ("War on Scientology") contra la Iglesia de la Cienciología y el Centro Tecnológico Religioso. En los contactos que tuvieron con los medios de comunicación se dio a conocer que los ataques contra la Iglesia de la Cienciología continuarán con el fin de proteger el derecho a la libertad de expresión y porque ellos creen que los miembros de la Iglesia son explotados económicamente.

El 27 de enero de 2008 un nuevo vídeo "Llamando a la acción" ("Call to Action") apareció en YouTube convocando protestas a las puertas de los centros de la Iglesia de la Cienciología el 10 de febrero de 2008.

Protestas en contra de las prácticas y el estatus fiscal de la Iglesia de la Cienciología.

El 2 de febrero de 2008, 150 personas se reunieron fuera del centro de la Iglesia de la Cienciología en Orlando, Florida para protestar contra las prácticas de la organización. Otras pequeñas protestas tuvieron lugar en Santa Bárbara, California y en Manchester, Inglaterra.
El 10 de febrero de 2008, unas 7.000 personas en más de 93 ciudades del mundo acudieron a las protestas.Muchos manifestantes llevaban máscaras del personaje V de Vendetta (inspirado en Guy Fawkes, para simbolizar la lucha desigual del individuo contra el Estado) o tapado el rostro de alguna forma para proteger sus identidades frente a posibles represalias de la Iglesia.
Anonymous convocó una segunda ola de protestas el 15 de marzo de 2008 en ciudades de todo el mundo incluyendo Boston, Dallas, Chicago,Los Ángeles, Londres, París, Vancouver, Toronto, Berlín, y Dublín. La asistencia global fue estimada entre 7000 y 8000 manifestantes, un número similar al de las primeras protestas.

La tercera ola de protestas tuvo lugar el 12 de abril de 2008. Nombrada "Operación reconectar" ("Operation Reconnect"), tenía como objetivo aumentar el conocimiento sobre las técnicas de desconexión usadas por la Iglesia de la Cienciología.
El 17 de octubre de 2008, un chico de 18 años de Nueva Jersey reconoció ser miembro de Anonymous y se declaró culpable de haber participado en enero de 2008 en los ataques de denegación de servicio contra las páginas web de la Iglesia.
El 2 de diciembre de 2009, Anonymous convocó una competición "La cienciología apesta: un concurso" ("Scientology Sucks: A Contest") y pidió a los concursantes que hicieran bromas "legales" a la Iglesia de la Cienciología. Ofrecieron $1.000, $300 y $75 (inicialmente $400, $100 y $50) del dinero de las donaciones a los tres ganadores.Elconcurso fue ganado por un usuario llamado "MalcontentNazi" con su video "Scientology's Secret Nazi Ties" en el que aparece vestido de Nazi a la puertas de la Iglesia y empieza a alabarla. En la segunda parte hace una broma telefónica a la Iglesia preguntándoles por qué no fueron capaces de detener al chico que hizo que la gente de la calle se riera.
Las protestas continuaron y se aprovecharon de los actos mediáticos como el estreno de la película Valkyrie de Tom Cruise.

6.2.2.- Ataques contra la Ley Sinde

El 21 de diciembre de 2010, mismo día que se realiza la votación en el Congreso de los Diputados de la llamada Ley Sinde que daría pleno poder para cerrar sitios webs de enlaces de contenidos sin la necesidad de contar con la autorización de un juez, se organizó como protesta ataques masivos DDoS a las páginas del PSOE (Partido Socialista Obrero Español), SGAE (Sociedad General de Autores de España), Congreso y Ministerio de Cultura, colapsándolas mucho antes de la hora de la votación.

Finalmente la ley no se aprobó aunque el gobierno la recuperó para su voto en el Senado e introdujo cambios para ganar el apoyo del principal partido de la oposición.
El 16 de enero de 2011, Anonymous ataca la web del Senado Español y la del PP (Partido Popular) como protesta contra la "renovada" Ley Sinde.
El 13 de febrero de 2011, se inicia la llamada "Operación Goya" la cual provocó a las 16:00 horas el colapso de la web de la Academia de cine, y durante la celebración de la gala de entrega de los Premios Goya una serie de protestas y abucheos por parte de varios centenares de Anonymous,que acudieron usando la tradicional careta de Guy Fawkes.
El 19 de marzo de 2011, Anonymous se infiltró en la entrega del premio "Miguel Picazo" de la Diputación de Jaén donde la ministra de cultura Ángeles González-Sinde Reig dio un discurso. Los integrantes de la protesta ocultaron su rostro con máscaras y la abuchearon al terminar su discurso.
En julio de 2011, la sede de la SGAE es registrada y su cúpula detenida, acusada de desviar fondos y otros delitos societarios.

7.- Conclusión

Como conclusión hemos de sacar que Internet es una compleja red de redes y que se tiene que tener cuidado con las acciones que se realizan en ella ya que hay muchas personas que están detrás viendo qué hacemos y qué dejamos de hacer y con qué fines.

Espero que mi trabajo haya ayudado a las personas que no tenían ningún conocimiento de la estructuración de esta inmensa red a darse cuenta de todas las opciones que esta nos brinda, para bien, y para mal. Y que, sin ninguna duda, el desarrollo de Internet para fines benignos nos llevará a un desarrollo inmenso de nuestra civilización.

Además, hemos podido aprender más acerca de la organización Anonymous, que muchas veces pasa desapercibida, a pesar de estar mundialmente extendida, por estar involucrada en temas cibernéticos a los que la gran mayoría de personas no les prestan atención.

En mi opinión deberíamos hacer muchos más caso a estos temas ya que son muy interesantes y la mayoría se relacionan con temas de la vida cotidiana que nos afectan de una u otra manera.

Porque al fin y al cabo, Internet es un reflejo de la realidad, ya que en esta inmensa red nos sirve para almacenar, editar y crear todo tipos de archivos que después nos son útiles en nuestro día a día.

Referencias externas al trabajo de investigación

1 http://www.ordenadores-y-portatiles.com/estructura-internet.html

2 http://www.ipv6.mx/index.php/informacion/fundamentos/ipv4

3 https://es.wikipedia.org/wiki/Log_(registro)

4 http://www.ordenadores-y-portatiles.com/estructura-internet.html

5 http://www.monografias.com/trabajos55/sobre-internet/sobre-internet2.shtml

6http://www.monografias.com/trabajos55/sobre-internet/sobre-internet2/protocolo.shtml

7 http://www.definicionabc.com/tecnologia/navegador.php

8 https://es.wikipedia.org/wiki/Fabrizio_Mej%C3%ADa_Madrid

9 http://articulos.softonic.com/7-huellas-que-dejas-en-internet-y-telefono

10 https://es.wikipedia.org/wiki/Anonymous

11 http://despertares.org/2010/12/10/wikileaks-operacion-payback/

12 http://www.darkreading.com/attacks-and-breaches/kiss-off-anonymous-hacker-took-on-gene-simmons-feds-say/d/d-id/1101836?

13 http://despertares.org/2010/12/10/wikileaks-operacion-payback/

14 http://www.blackploit.com/2011/02/el-ataque-de-anonymous-hbgary.html

15 https://es.wikipedia.org/wiki/Anexo:Acciones_de_Anonymous#Operaci.C3.B3n_Sony

16 http://www.publico.es/culturas/anonymous-responde-ataques-al-cierre.html

17 https://quesabesobreanonymous.wordpress.com/actividad-de anonymous/principales-ataques-de-anonymous/