ANÁLISIS Y CONSIDERACIONES SOBRE LA DEEP WEB

JOHN JADER CUESTA PALACIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA
TURBO
2020

ANÁLISIS Y CONSIDERACIONES SOBRE LA DEEP WEB

JOHN JADER CUESTA PALACIO

Monografía para optar al título de:
Especialista en Seguridad Informática

Director:
Msc. Katerine Márceles Villalba

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
TURBO
2020

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Turbo, abril 2 de 2020

A Dios, mi familia y padres

John Jader Cuesta Palacio

AGRADECIMIENTOS

John Jader expresa sus agradecimientos a:

Msc. Katerine Márceles Villalba por su dedicación constante y sus orientaciones

CONTENIDO

pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Lista de Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
CPU	Unidad Central de Procesamiento
LAN	Red de Área Local
OSI	Interconexión de sistemas abiertos
PC	Personal computer (computadora personal)
DB	Data Base (Bases de datos)
SGBD	Data Base Management System (sistema de gestión de bases de datos)

RESUMEN

Internet se ha convertido en la red más grande, importante y conocida a nivel mundial, su utilidad facilita entre otras cosas: el envío de datos, la conexión entre ordenadores y la transmisión de millones de bits de información cada segundo, por ello su crecimiento y utilidad es constante, al punto que en la actualidad no se ha dimensionado de manera precisa el tamaño de esta gran red. En ella se puede encontrar sitios con característica particulares que compartiendo rasgos comunes permiten su clasificación; sin embargo, existe una región de la internet que no es muy conocida, la cual puede despertar mucho interés por esa particularidad de ser ubicada, en el espectro de lo que “no es claramente clasificable”, por ello es que se especula mucho de ella, y su dominio no es de total conocimiento público; a esto que se conoce muy poco y que está relacionado con internet pero que puede ser algo diferente, se le llama la Deep web.

La Deep web es un espacio que muchos consideran un tanto oscuro o terrorífico, haciendo alusión a que existen supuestas barreras o niveles que ocultan lo que allí se encuentra, dificultando la navegación y no es tan asequible al público y por todo lo que se maneja puede estar libre de reglas convencionales y consecuentemente no todas las personas se les permite conocer.

Palabras clave: Internet, redes, niveles, seguridad, Deep Web.

SUMMARY

The Internet has become the largest, most important and well-known network worldwide, its usefulness facilitates among other things: the sending of data, the connection between computers and the transmission of millions of information every second, therefore its growth and utility It is constant, to the point that at present it is not possible to precisely size the size of this large network. In it you can find sites with particular characteristics that share common features allow classification; However, there is a region of the Internet that is not well known, which can arouse much interest in that particularity of being located, in the spectrum of what is "not clearly classifiable", so much is speculated about it, and his domain is not of total public knowledge; This is very little known and is related to the Internet but it may be something different, it is called the Deep web.

The Deep web is a space that many consider somewhat obscure or terrifying, alluding to the existence of supposed barriers or levels that hide what is there, hindering navigation and is not as accessible to the public and for everything that is handled can Be free from conventional rules and consequently not all people are allowed to know.

Keywords: Internet, networks, levels, security, Deep Web.

INTRODUCCIÓN

Hace aproximadamente 20 años atrás la información de trabajos, productos académicos, aportes institucionales o corporativos, no era el mismo porcentaje al de hoy, incluso para esa época muchas persona, no colocaban en consideración el potencial de la red para conseguir muchas herramienta que hoy son naturales en ella, ya sea porque eran tiempos donde aún se usaban métodos un tanto rudimentarios, habitualmente aceptables o porque simplemente no poseían el auge necesario que podría tener los sistemas de información y los aportes a la sociedad de la información, pero lo que si se tenía claro era que internet era importante y despertaba mucha fascinación como ahora, aunque no tenía el mismo volumen de información que en la actualidad, incluso el ritmo de subida de información a la red y todo lo que contenía equivalía a 5 exabytes para el 2003 (en palabras de Eric Schmidt CEO de Google en 2011)[1] pero hoy esta misma información puede verse fácilmente superada en poco menos de 3 días; esto apunta a la información que puede estar disponible para todos y de la cual se puede decir que está disponible para cualquier internauta o una población lo suficientemente amplia; ahora bien si se tiene en cuenta que no todo está tan disponible al público en general y que se sabe que hay algo que está en la red pero al parecer es "invisible a nosotros", ¿en qué lugar se encuentra? ¿Cuál es su tamaño? ¿Es posible acceder a ella? ¿Qué mecanismos se utilizan para que permanezca encubierta? La solución a estos interrogantes se ha estructurado en el presente trabajo con la intención de dar a conocer todo lo posible sobre aquellos que se llama la Deep web o web profunda, la cual se responde bajo la anterior pregunta de una manera un tanto especulativa; se intentara además contextualizar sobre los antecedentes del término y su uso, junto a un acercamiento a su estructura según lo que dicen los conocedores del tema y sobre todo cuales son las implicaciones de acceder a esta.

La temática presente señalará la importancia, el origen, los alcances de esta red, las posibles limitaciones, además la metodología empleada, para entender cuál es la visión que se tiene sobre lo que supone el significado que representa el estudio en este campo y su aplicación en el área investigada.

[1] universidad politecnica de madrid. (s.f.). las siglas y otras abreviaciones en el campo informatico. madrid: centro virtual cervantes.

1. PLANTEAMIENTO DEL PROBLEMA

La informática surge como una disciplina cuyo conocimiento es ocupado para resolver problemas vinculados al tratamiento de la información, nace a partir de la necesidad de crear, almacenar, transmitir información y dar soporte a los recursos que se relacionan, es decir, su objeto especifico que es la información; no obstante, surge a partir de ella un elemento que ocupa la atención de muchos, ya que si bien la informática no es un espectro u objeto de estudio, en su desarrollo ha generado interés en los elementos que nacen a través de ella[2]. Uno de ellos es la web profunda o Deep web. Esta es una incógnita para muchos, una referente falsa para otros, creado para despertar sensacionalismos en las personas, este tema hace surgir todo tipo de teorías conspirativas, ¿es un sitio real al que unos pocos pueden acceder por su complejidad? o simplemente puede ser algo sin importancia real. Basado en el hecho de que independientemente de las posiciones que se tienen y sus distintas ideas, el área tiene una relación muy estrecha con el internet, a pesar de las muchas particularidades que tiene, por ello se convierte en un propósito fundamental y el centro de esta cuestión esclarecer el tema, lo cual impulsa a mostrar verdades, confirmar o derogar afirmación o mostrar algo nuevo. El objeto es esclarecer los mitos que se han creado alrededor de ella y saber a ciencia cierta, cuál es su estructura y que elementos la componen. De lo anterior nace el siguiente planteamiento: ¿Cómo a través de identificar y analizar los elementos de la Deep Web y algunas consideraciones a sus características principales, se puede llegar a entender su estructura y sus diferencias con respecto a la red de internet?

Basado en la anterior pregunta el estudio de este tema amerita la exposición concreta, pero al mismo tiempo profunda sobre la investigación del tema en cuestión, principalmente se busca abordar el tema con un estudio monográfico, dado que las cualidades de este permite presentar la información de una manera organizada bibliográficamente, bajo la conformación de un trabajo explicativo cuya extensión refleje una variada referencia a fuentes contrastables y una investigación propia que esboce de una manera clara y objetiva el asunto que evoca este trabajo.

[2] LOPEZ, P.; MARTIN, H. The World's Technological Capacity to Store, Communicate, and Compute Information, {2011}. 1-4p

2. JUSTIFICACIÓN

Según datos del gigante corporativo Google en el año 2000 existían más de mil millones de URLs indexadas en su buscador, 8 años después esta cifra se multiplico exponencialmente al punto de que existe no menos de un billón de millones de sitios indexados[3]; la cifra es demasiado alta, y causa gran impacto saber que el crecimiento del volumen de la información en la red es algo que avanza generando gran asombro[4]; ahora bien si esos datos son ciertos y según la percepción general la información que brindan los navegadores, es solo una pequeña punta de iceberg, en comparación con lo que subyace en la red, ¿Qué decir de la Deep web?.

La Deep web es un espacio poco explorado y del que (se supone) hay poco conocimiento al menos convencionalmente; algunos establecen que es un sitio donde se realizan actividades ilegales, y no hay herramientas usadas habitualmente para acceder a ella, por lo que se entiende que solo algunos con conocimiento avanzado en informática o aquellos que se atreven "a un poco más" pueden acceder. Lo claro es que todas las afirmaciones coinciden que hay mucha más información de la que normalmente pueden encontrar los navegadores, por ello se hace necesario en lo más posible hacer una recopilación y estudio de todas aquellas consideraciones y perspectivas sobre el tema, que permitan no solo compendiar información de sitios externos a la Deep web sino compilar información de ella misma, dado que por ser en realidad un espectro informático. Este trabajo, es el análisis a algunas concepciones o ideas que han sido la base para el estudio del tema, pero con un tinte investigativo que permita estudiar la estructura, y generalidades de la Deep web, lo cual permitirá entender la realidad de esta, corregir algunas imprecisiones del tema y esclarecer mediante el análisis sus características.

[3] SETA, L. D. "Google alcanza el billon de paginas indexadas" {En linea}. {27 de Julio de 2008}. Disponible en: (https://dosideas.com/noticias/actualidad/146-google-alcanza-el-trillon-de-paginas-indexadas).

[4] MOORE, R. J. "¿Cuando datos se crean al dia en internet?" {En linea}.{08 de Febrero de 2011} disponible en: https://www.elmundo.es/elmundo/2011/02/08/navegante/1297179889.html

3. OBJETIVOS

3.1. GENERAL

Realizar un análisis general sobre lo que se le conoce como la Deep web, evaluando todos los posibles aspectos que nos den indicadores sobre esta dentro del internet.

3.2. ESPECÍFICOS

- Analizar definiciones sobre lo que significa la Deep web para brindar una definición propia y actual.
- Realizar una contextualización sobre el significado de la Deep web dentro del internet.
- Abordar protocolos que se utiliza en la Deep Web con la intensión de entender mecanismos de conexión dentro de esta.
- Sugerir algunas herramientas que son de utilidad para el acceso a sitios de la Deep web

4. MARCO REFERENCIAL

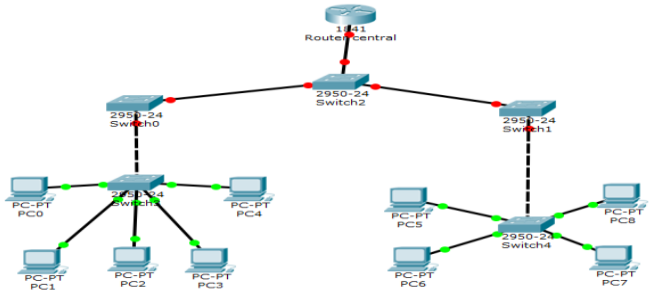
4.1. MARCO CONCEPTUAL

Este estudio se basa en un tema que, cobra importancia no por ser algo de la naturaleza o por pertenecer a lo sobre natural, sino que más bien es un enigma (podria decir que en algunos aspectos casi inconciente) creado por el hombre y situado en el ambito informatico, pero especificamente es algo que pertenece al estudio y análisis de las redes informaticas, pero que de alguna manera sus cualidades la hacen interesante, a continuación se hace referencia algunos conceptos relacionado con la temática.

4. 1.1 La red

Es la interconexión de dispositivos, que posibilitan el envío, recepción tratamiento de la información, a través de canales, analógicos físicos y lógicos[i]. El objetivo principal de la red es que distintos ordenadores puedan compartir recursos a cierta distancia. A los computadores[5] conectados se les llama host y para que ellos se conecten debe haber otros dispositivos especiales que hagan las veces de intermediarios ilustración 1.

Ilustración 1 red



Fuente: propiedad del autor

[5] NORTON, Peter. "introducción a la computación". 6ta.ed. McGraw. 2006. Hill, 65 páginas.

4.1.2. Clasificación de redes[6]

La definición de red lleva consigo una cantidad considerable de elementos, que pueden generar variaciones desde la perspectiva que se vea, por ello es posible realizar una clasificación de la red según un subconjunto o elementos comunes.

4.1.3. Red Según su tamaño

Red LAN: Sigla de la traducción de Local Área Network. Las redes de área local son redes de ordenadores cuya extensión es del orden de entre 10 metros a 1 kilómetro. Generalmente usan la tecnología de Broadcast siendo velocidades de transmisión típicas que van de 10 a 100 Mbps (Megabits por segundo).

Red MAN: Las (Metropolitan Área Network) redes de área metropolitana son redes de ordenadores de tamaño superior a una LAN. Su tamaño máximo, comprenden un área de unos 10 kilómetros.

Red WAN: Las redes de área amplia (Wide Área Network) tienen un tamaño superior a una MAN, y consisten en una colección de host o de interconexiones de redes LAN conectadas como subred. Esta subred está conformada por una serie de líneas de transmisión que involucran, aparatos de red encargados de dirigir los paquetes hacia la LAN o host adecuado (a estos dispositivos les llamamos Router, los cuales permiten el envío de paquetes de un Router a otro. El tamaño de la red puede oscilar entre 100 y 1000 kilómetros. Podría decir que internet está dentro de esta categoría.

Red SAN: Las redes de área de almacenamiento (Storage Área Network) se trata de una arquitectura que no se dirige al uso por host, sino que directamente se trata de una red dedicada que se interconecta y presenta agrupaciones, para permitir la comunicación entre servidores.

4.1.4. Red Según su relación funcional

Red cliente- servidor: Esta es un tipo de comunicación entre un pc, nodo o host que dirige su tráfico a un dispositivo central llamado servidor, el cual recibe las peticiones del primero para resolver o dar respuesta a los paquetes que le son enviado y devolver una respuesta.

---

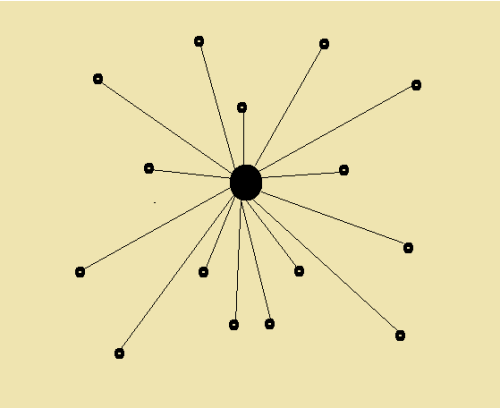
[6] ORELLANA CRUZ, Julio. “Clasificacion de redes”. {En linea}. {17 de Abril de 2011}. Disponible en: (https://julioorellanacruz.wordpress.com/2011/04/17/clasificacion-de-redes/)

Red peer to peer: La característica principal es que la comunicación en esta red, se da entre dos o más pc o host al mismo nivel, sin establecer necesariamente jerarquías en cuanto a la infraestructura.

4.1.5. Según la concentración de trabajo en sus nodos

Redes centralizadas: Este tipo de red está constituida obligatoriamente por distintos nodos a un mismo nivel y un nodo principal, el cual direcciona y orquesta la sintonía de todos los hosts que componen la red, ya que la comunicación se da, si y solo si el nodo central está disponible, no presenta fallos o no hay intermitencias y la conexión permite identificar a cada nodo. Si el nodo principal se cae la red cae. Ejemplo de ellos son redes servicios de streaming. Ver ilustración 2 red centralizada.

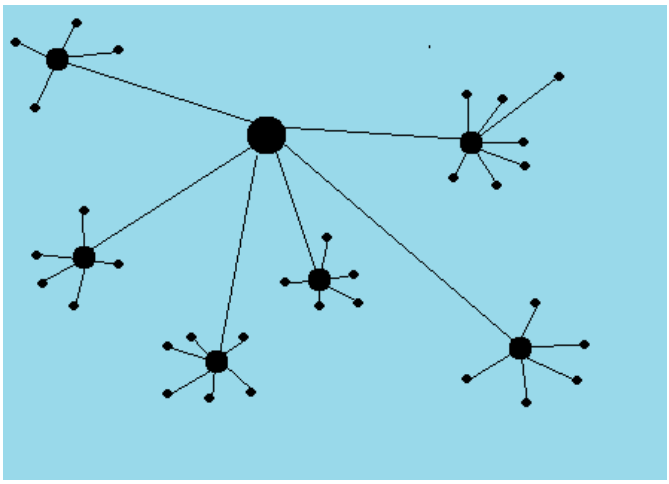
Ilustración 2 Red centralizada



Fuente: propiedad del autor

Redes descentralizadas: No existe un único nodo principal ya que hay una bifurcación de puertos y conexiones centrales que interconectan la red y retrasmiten o no la información o datos que les llegan. Ejemplo de ello es la red Wikipedia, ver ilustración 3 red descentralizada.

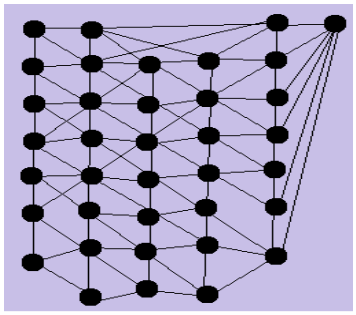
Ilustración 3 Red descentralizada (a continuación)



Fuente: propiedad del autor

Redes distribuidas: Todos los nodos receptores pueden ser emisores y viceversa, lo que facilita que haya una conexión en la cual la idea de nodo central o de receptores periféricos desaparecen, ver ilustración 4 red distribuida[7].

Ilustración 4 Red distribuida



Fuente: Autoría propia

4.1.6. Unidades de almacenamiento

Estas son la medidas que utiliza la informática para determinar el tamaño de información que se está manejando, es decir para determinar el tamaño de la red, no basta solo con definir la cantidad de sitios o dominios registrados o la cantidad de host o servidores que existen, ya que ello no tendría relevancia si no existieran los datos que son lo más importante, para ello se debe partir de la premisa de que la primera unidad de medida es el bit que equivale a un carácter en otras palabra cuando se escribe una palabra esta es la composición de bit y su número

[7] GATELL, Antonio. "Como funciona una red distribuida" {En línea} 8 julio 2018 {13 octubre 2019}. Disponible en: (https://www.gatellasociados.com/como-funciona-una-red-distribuida/)

corresponde a ello, a partir de allí se obtienen las otras unidades de medida que son el byte que equivale a 8 bits y sucesivamente viene un patrón de equivalencia de 1024 como se muestra en la ilustración 5**.**

Ilustración 5 Medida de almacenamiento

Medidas de almacenamiento

Unidades	Símbolos	Equivalencia	Valor en Bytes
Byte	B	8 bits	1 byte
Kilobyte	Kb	1024 Byte	1.024 Bytes
Megabyte	Mb	1024 Kilobyte	1.048.576 Bytes
Gigabyte	Gb	1024 Megabyte	1.073.741.824 Bytes
Terabyte	Tb	1024 Gigabytes	1.099.511.627.776 Bytes
Peta byte	Pb	1024 Terabyte	1.125.899.906.842 Bytes
Exabyte	Eb	1024 Peta byte	1.152.921.504.606.846.976 Bytes
Zettabyte	Zb	1024 Exabyte	1.180.591.620.717.411.303.424 Bytes
Yottabyte	Yb	1024 Zettabyte	1.208.925.819.614.629.174.706.176 Bytes
Brontobyte	BB	1024 Yottabyte	1.237.940.039.285.380.274.899.124.224 Bytes
Geopbyte	GeB	1024 Brontobyte	1.267.650.600.228.229.401.496.703.205.376 Bytes

Fuente: propiedad del autor

4.2. MARCO HISTÓRICO

En 1994 la Deep web se le llamo HIDDEN WEB hasta ser rebautizada en 2001 con el nombre que hoy en día todos conocen, pero además se le dice coloquialmente Internet profunda, ya que se ha establecido que todo el contenido de Internet que no forma parte del Internet superficial, es decir, los sitios no indexados por los motores de búsqueda más utilizados en la red, se encuentra en esta parte de la red; esta comenzó como un proyecto militar el cual pretendía almacenar la información de esta índole o de organizaciones como el FBI y la INTERPOL, además de muchas organizaciones mundiales que se han unido a la lista, por pertenecer a conglomerados secretos u algún otro que pretende llevar sus movimientos con un bajo perfil[8]. Por lo general muchos de las informaciones son documentos hackeados o robados por hackers no autorizadas revelando los secretos de algunas naciones. El proyecto mantuvo encubierto durante algún tiempo, permitiendo que su uso para el espionaje durante las guerras como la de Irak, la guerra contra la red extremista

[8] Lobo Romero, Mario. un paseo por la Deep Web. Catalunya 2018 p 20-22. Trabajo de grado. Universidad abierta de Catalunya

al qaeda y muchas naciones que pudieron ser espiadas, hasta que unos meses después de sus inicios en 1994 se perdió su control haciéndose pública ante las naciones y pobladores del mundo, lo que de alguna forma, posibilito que bajo ciertos mecanismos se lograran "acceder" con dificultad no obstante pronto llegarían programas y hackers que ayudarían a un acceso casi libre y sin ningún problemas. En la actualidad hay mucha bibliografía sobre cómo acceder o existen "manuales de supervivencia en este entorno digital" tal como lo propone Matia Zavia en un artículo publicado en Genbeta[9] en el año 2015, en la cual describe en primera instancia como acceder, señalando algunas herramientas como I2P o Tor, describe la forma como se daría la conexión, esquematizando la forma como se comunicaría el nodo a través de Tor.

4.3. ANTECEDENTES

Los estudios dirigidos a indagar sobre la Deep web no son algo nuevo, aunque seguramente con toda la bibliografía que pueda existir, siempre habrá más estudios al respecto; haciendo referencia a ello hay trabajos que dan cuenta de indagaciones e investigaciones sobre el tema que son importantes mencionar:
La revista mexicana de tecnología y sociedad Paakat, realizo una publicación en el año 2014 titulada "La web oculta y como los buscadores encuentran la información[10]" en la cual establecen que la Deep web es una parte de la internet con la diferencia de que no existe la indexación y por ser sitios altamente dinámico los robot o crawler de los navegadores no pueden identificar o detectar estos sitios, por lo que proponen que una modificación en la forma de cómo operan los rastreadores, además considera que debe haber un cambio del lado del cliente o host en cuanto la conexión lo que conllevaría a una reducción significativa en el acceso a esta red profunda; no obstante lo que se propone en este artículo, no es solo un estudio de la estructura o la forma de operar dentro de la red, sino que da por hecho de que habría un mayor acceso y reducción del tamaño del contenido inaccesible de web profunda. Complementario a lo anterior, en la universidad de La Salle se realizó un proyecto de investigación titulado: "proyecto de investigación Deep Web" en la cual se establece que cualquier sitio eliminado por entidades o agencias de inteligencia como el FBI o grupos poderosos de hacker es la Deep web, con la salvedad que no funciona como un sistema de reciclaje, dado que el sitio sigue teniendo un lugar, de manera útil y visible bajo parámetros que restringen su acceso; uno de los elemento que impide esto, es que el nombre de dominio resulta

[9] ZAVIA, Matías. "Kit de supervivencia en la Deep Web" {En línea} 2015. {12 octubre 2019}. Disponible en: (https://www.genbeta.com/a-fondo/kit-de-supervivencia-en-la-deep-web)

[10] AMARO LOPEZ, Jose A; CHAVEZ ACEVEZ Lazaro M. y VARELA NAVARRO, Alberto Varela. La Web Oculta y cómo los buscadores encuentran la información. Revista de tecnologia y sociedad. En: PAAKAT: Revista de Tecnologia y sociedad. Vol., No 7(agos-2014). 4-5.

ser la suma de muchos caracteres para nada nemotécnicos y que además el contenido rompe con la moral social. La investigación establece que la Deep web consta de nivel que parte desde el nivel 1, que corresponde a todo lo que normalmente se encuentra en internet, el nivel 2 muestra dificultades en su acceso y su contenido es algo normal pero con cierto matiz de perversidad, pues su contenido no se sujeta a normas convencionales; el nivel 3 con ciertas restricciones presenta contenidos "problemáticos" y de tinte antisocial e inmoral, el nivel 4 es básicamente contenido similar, pero su acceso requiere conocimientos avanzados en sistemas e informática, el nivel 5 es catalogado como de alta peligrosidad y de complicada navegabilidad, los estándares de seguridad contemplado por los navegador, antimalware no representa nada en comparación con la peligrosidad del sitio; además es aquí donde hacker venden informaciones sensibles de todo tipo, según la investigación el nivel 6 es el más profundo, y es llamado el gobierno negro pero no se tiene información segura de lo que allí se presenta[11].

En enero de 2017 en la universidad de Cantabria se desarrolló el trabajo de grado titulado: Deep Web: acceso, seguridad y análisis de tráfico, el cual hace una recopilación muy magistral y técnica sobre los términos más relevantes e importantes del tema, la cual facilita a nivel gráfico y conceptual la comprensión de la materia, es importante resaltar que haciendo una generalización del entorno, presenta herramientas para el acceso, creación de rutas, utilidad de y vulnerabilidades de la red Tor, además de la implementación de relé de salidas segura dentro del tráfico que proporciona la red Tor[12].

Otro trabajo que da cuenta de un estudio sobre la temática fue desarrollado en el 2018 con el título de "un paseo por la Deep Web" el cual basado en la idea inicial de que particularmente el común, vinculan el termino con ciberdelincuencia, trata de esclarecer cual es la estructura, diferencia entre lo que se llama la internet profunda y lo que no, además trata de analizar ataque que se han producido y sus consecuencia, cabe resaltar que por el significado que tiene analizar un ataque en este lado de la red, hay un espacio considerable en el cual se analiza tipos de cifrados, servicios, enrutamiento, relay, y navegación en algunos sitios[13].

5. ANÁLISIS DE DEFINICIONES ENTORNO A LA DEEP WEB

Existen muchas referencias sobre el concepto de la Deep web. Son varios autores que han tenido la disposición de vislumbrar lo que significa este concepto, por tanto, es importante resaltar algunos de ellos: Según Víctor García y Jorge Chinea en su

[11] Castrillon Merida, K. X., Torres Hernandez, A. J., & Sandoval Castillo, N. (2015). Deep Web
[12] Cagiga vila, I. (Enero de 2017). Deep Web: acceso, seguridad y análisis de tráfico
[13] Lavin Perrino, I. (Junio de 2018). Un Paseo Por la Dee Web.

trabajo académico titulado: “Un paseo por la Deep Web[14]”, establecen que la Deep web no es más que un conglomerado de sitios web no indexados, que por poseer tal característica simplemente no pueden ser accedidos o encontrados por el público, dado que no están “registrados en ningún buscador”; en pocas palabras la Deep Web incluye material que no necesariamente tiene que ser algo maquiavélico en su totalidad, según estos autores[15]. Por otro lado en el 2017 Diego Villada y Andrés Jiménez realizaron una publicación en la revista antioqueña de las ciencias computacionales y la ingeniería de software, en un artículo de carácter investigativo titulado: “La web semántica y la Web Profunda como sistema de información: Análisis a una realidad” según la cual, la Deep web es equiparable a un lugar compuesto por un número no determinados de base de datos accesibles mediante diferentes interfaces de consulta, que presenta la información como páginas web dinámicas que no funcionan ni utilizan los tradicionales hipervínculos y que además no se encuentran indexadas lo que imposibilitan su disponibilidad en la red, cabe resaltar que según estos autores el 90% de esta red se alimenta de páginas tradicionales y legalmente constituidas[16].Otro concepto que brinda el portal PC Advisor se refiere a la web profunda, como una colección de sitios que tienen una composición diferente a los sitios normales y se encuentran en una red encriptada, de tal manera que los navegadores normales no pueden ingresar a la red y descifrar el contenido de la página, lo cual hace que estos las omitan de las búsquedas. Algo similar menciona la empresa especializada en ciberseguridad Kasperky, la cual menciona que la web profunda son básicamente los sitios que no pueden ser encontrados por los navegadores, al mismo tiempo existe sitios que tienen esta cualidad, pero además su contenido es de tinte oscuro, lo cual hacen que se les cataloguen los sitios de la red oscura o Dark web.Una vez conocida los anteriores definiciones, para el presente trabajo se entenderá como Internet profunda o Deep web a todo el contenido que perteneciendo a la red, no utilizan los protocolos de comunicación, no se someten a resoluciones de dominios, enrutamiento, dinamismos e indexación de la web compatible con los navegadores tradicionales y el cifrado de esta, obedece a un tipo de estándar que no es de dominio público, aunque en términos generales forma parte del Internet, Esto se debe a las limitaciones que tienen las redes para acceder a todos los sitios web por distintos motivos[17]. Cabe resaltar que el hecho de que esta red tenga estas cualidades, no

[14] GARCIA, Víctor; CHINEA, Jorge. “Un paseo por la Deep Web”. Catalunya,2019. 12p. trabajo de grado Master seguridad del tic. Universidad Oberta de Catalunya.

[15] COST SANFELIU, Jordi. Un paseo por la Deep Web. {En linea}. 2019. {16 septiembre 2019}. Disponible en: (http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.8DD09846&lang=es&site=eds-live&scope=site)

[16] Villada V., D., & Jiménez V., A. (2017). La Web Semántica y la Web Profunda como Sistemas de Información: Análisis a una realidad. (Spanish). Revista Antioqueña de Las Ciencias Computacionales, 7(1), 43. Retrieved from http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edb&AN=123900187&lang=es&site=eds-live&scope=site

[17] ADSLZONE.” Guía Deep web 2019: como es, como entrar, link y diferencias con la Dark net”. {en línea}. {25 noviembre 2019} disponible en: https://www.adslzone.net/como-se-hace/internet/guia-deep-web

significa que todo su contenido este mediana o estrictamente ligado a actividades anti normativas o moralmente incorrecta; más bien de alguna forma se puede decir que la peligrosidad del internet superficial puede ser mayor en algunos aspectos, dado que todos las personas pueden acceder a un sitio, que sin previo aviso, este preparado para vulnerar la seguridad de cualquier persona y su acceso es de total normalidad para un navegador convencional; algo que de alguna manera ya está previsto en la Deep web, pues sus propios límites están marcados por la imposibilidad de indexación, no reconocimiento de protocolos, y difícil habilitación del dinamismo y estructuración de los sitios, el significado de riesgo para un usuario, surge solo con intentar romper esos límites y acceder. Ahora bien, dentro de los límites de la Deep web se encuentra una especie de ciberespacio un poco menos conocido por su complejidad, pero del que no se puede pasar por alto, esta es la Dark web.

5.1. DARK WEB

Para entender conceptualmente que es Dark Web, hay que contextualizar: la internet tal como se conoce se estableció como la interconexión en una red que funciona con protocolos de comunicación TCP/IP y un modelo de envió, segmentación reagrupamiento y entrega de información, que obedece a unas reglas específicas que se conoce como enrutamiento, se debe conocer el destino y origen desde donde se envía la información, para ello el host de origen identifica la máquina de destino, previa consecución de su identificación pública mediante la resolución del sistema de nombres de dominio (DNS); una vez identificada la ruta de envió, la información se divide (fragmenta) y cada paquete se etiqueta en la cabecera para que no halla confusión en su tránsito; ahora bien la información como tal, debe estar codificada de tal manera que sea acorde al protocolo de comunicación actual de internet, este idioma de comunicación entre un origen (llamado cliente) y un destino (llamado servidor) lo define el protocolo de transferencia de hipertexto HTTP del cual se tiene al 2019 la disponibilidad del mismo protocolo pero un poco más seguro, este es HTTPS. Lo anterior es lo básico pero no todo esta tan disponible o asequible, ya que no todas las organizaciones están dispuesta a que su información se a tan fácil de conseguir solo por someterse a los mismos estándares y sin duda con todo este conocimiento sería fácil establecer una comunicación en la red, por ello, sometiéndose a ciertos requerimientos de interconexión en red, se diseña de forma exclusiva una red con otros parámetros, pero con la particularidad de que no se puede acceder desde otra red, quedando automáticamente incluida en la Deep Web, el escenario fue diseñado de tal manera que estas redes fueran accedidas con aplicaciones creadas única y exclusivamente para ellas; si bien en la web conocida los paquetes se envían a una dirección IP conocida, en este espacio de la red, la dirección IP se tiende a ser ocultadas, por tanto ningún pc normal con las configuraciones, estándar jamás

ingresara allí; así mismo un DNS tradicional no servirá ya que estas redes tienen sus propios dominios como es el caso del dominio de la red Tor, por lo que ningún navegador podrá mostrar un sitio así, incluso si este se teclea textualmente. Cada una de estas redes se les llama Darknet las cuales a su vez alojan diversas Dark web

6. CONTEXTUALIZACIÓN SOBRE EL SIGNIFICADO DE LA DEEP WEB DENTRO DEL INTERNET.

6.1. SUPUESTOS RIESGOS

Todos los sitios independientemente de que sea o no de la Deep web, puede traer riesgos importantes para la seguridad de los dispositivos implicados en la navegación, para los datos de las personas o para el usuario que los opera; no obstante, se puede entender que por las diferencias que existen entre la red común y la web profunda esto presupone que en ambas hay riesgos, pero operan de forma diferente, he aquí un paralelo como se muestra a continuación en la tabla 1 diferencias entre internet y Deep Web.

Tabla 1 Diferencias entre internet y Deep Web

Internet	Deep Web
Cualquier persona pueden verse influenciados por una publicidad engañosa o banner abusivos.	La publicidad o banner pueden tener script con ejecución automática y adueñarse del pc sin previo aviso.
Hay incitación a realizar compras por internet, de manera activa que conllevan a estafas	No necesariamente se requiere incitación para robar datos ya que el pc puede ser secuestrado con solo abrir el sitio.
Existen mecanismos de protección datos personales que impiden convertirles en víctimas de estafas o robos en páginas web poco fiable o controlada por terceros.	La seguridad no está garantizada, todo depende del conocimiento del usuario.
Hay muchos sitios de actividad criminal que pueden ofender la moral personal, pero suelen ser identificables y rastreables.	Los sitios con actividad criminal, son difíciles de rastrear, lo que significa que es más difícil alertar al usuario.
Los servicios adquiridos en algunos sitios pueden ser supervisados por entes de control, por lo que un tratamiento indebido de tus datos, o	No hay supervisión.

una vulneración a la intimidad está sometida al castigo	
Gran porcentaje de los malware son detectados estudiado y se provee una solución.	No hay entidad que estudie malware que se ejecuten en estos entornos.

6.2. COMO SE DA EL INGRESO A LA DEEP WEB

Para el acceso a la red lo primero que debe tener en cuenta es que, los patrones de seguridad serán completamente distintos, se deben tener en cuenta que no todo lo que normalmente se utiliza para acceder internet es igual que al ingresar aquí, por ello es conveniente utilizar programas que se encarguen de ocultar la identidad (para algunas ocasiones) evitando así posibles riesgos, especialmente porque no todas las configuraciones serán acordes a las necesitadas. Algunas de estas herramientas se pueden encontrar fácilmente en algunos sitios de descargas por Internet. Básicamente para ingresar se debe tener en cuenta que no todo funciona con dominios .Com, .es, .org, .net, o los que normalmente se promocionan en la web pública, sino que existen otros tipo de dominios que pertenecen a otra clase, para ello se debe utilizar un navegador especializado, que permita mostrar el contenido que no se encuentran bajos los dominios conocido, como es el caso de Tor; esta es una aplicación que permite visualizar muchos de estos sitios como aquellos con terminación .onion, ya que está diseñada para reconocer esta resolución. El acceso se da mediante el programa diseñado para ello, el cual a su vez procura la conexión por repetidores o nodo a nodo, dependiendo del caso, lo cual pasa por distintas troncales antes de llegar al destino indicado, con ello se logra perder la traza que deja una conexión normal y es mucho más difícil rastrear la conexión. Al igual que la red Tor existen otras alternativas como Freenet. Que es un poco menos conocido, pero al igual que él anterior permite ingresar a un sitio web o compartir archivos con un anonimato casi total. Otra opción menos conocida aun es usar un live llamado TAILS, que es una distribución live-USB para poder navegar, y realizar otras actividades como descargas de forma anónima y segura.

6.3 COMUNIDADES EN LÍNEAS Y FOROS VINCULADOS A LA DEEP WEB DESDE TOR

8chan: Se le considera como un poco oscura por la liberalidad manifiesta en el sitio es el equivalente al 4chan convencional, pero de ese lado en la red.

Cebolla Chan 3.0: es un foro donde se hablan de variedades de la Deep Web, con una sección de charla general como una especie de cafetería y otra donde la gente puede realizar comercio como en una plaza. Tienen casi 60.000 miembros registrados en español.

Chat With Strangers: es un servicio de chat en el que se conectan normalmente se conectan las personas para conversar e incluso conseguir artículos o hacer tratos con desconocido.

Facebook: Facebook también tiene un dominio en este sector de la red, es similar al que todos conocemos, sólo que funciona con un dominio que puede ser visto con la red Tor que han creado para poder utilizarlo desde la seguridad de la Deep Web.

Hidden Answers: es similar a foros como Taringa donde podemos recurrir a esta alternativa Sólo lanza tu pregunta y el resto de usuarios te responderá.

Temp mail: es un servicio anónimo de email, funciona como una bandeja de entrada que utiliza un correo descartable.

Mail2Tor: Un servicio de correo electrónico anónimo para enviar o recibir mensajes manteniendo nuestra privacidad, en ocasiones nos pide verificación de captcha.

6.4 BUSCADORES

- **DuckDuckGo:** Es un buscador muy seguro, no tan potente como Google, ni con un algoritmo de búsqueda similar peor es muy popular, tiene una alternativo en versión. onion. No sólo encuentra enlaces de la web convencional, sino también de la Deep Web.

- **Not Evil[18]:** Otro buscador que pretende ser el Google de la red Tor. No encuentra páginas convencionales, sólo las pertenecientes a la Deep Web.

[18] Not Evil. {en linea}. {24 de noviembre de 2019}. Disponible en: (hss3uro2hsxfogfq.onion)

- **The Hidden Wiki:** Vinculado directamente a Tor Se trata de uno de los índices en los que encontrar diferentes enlaces de páginas de interés en la red.

- **Torch:** Al igual que el primero otro de los principales buscadores de Tor. Se mantiene mediante publicidad, es un buen olfateador de los millones de páginas de la Deep Web.

6.5 COMERCIO

Así como en la vida normal se pueden hacer compras con dinero en efectivo o tarjetas de crédito existen monedas digitales, con las que se realizan comercio electrónico, no es que sustituían las monedas que conocemos como el dólar, euro, o el peso, sino que son monedas electrónicas que utilizan tecnología blockhain; entre esas están el bitcoin, el Dahs, el Ethereum, Bitcoin gold y más. Para guardar estas monedas la Deep web tiene sitios exclusivos como los siguientes:

Hidden Wallet: Es un monedero anónimo que soporta transacciones con Bitcoins, cobran un poco de comisiones por los retiros, pero da resultados.

OnionWallet: Este monedero oculto que ofrece una bóveda segura, y puede cifrar los datos protegiendo nuestros fondos con un código PIN, el registro es anónimo y una interfaz de usuario sencilla y fácil de utilizar.

Shadow Wallet: Tiene una interfaz de usuario sencilla de utilizar, el registro tiene políticas de tratamientos que no facilita la vigilancia de ningún ente de control cobra una comisión de 0,001 bitcoin por operación descontada del monto que se transfiere.

WeBuyBitcoins: Es un sito de compra de bitcoin, los pagos se realizan pagándote en varias divisas como el dólar o euro y es través de PayPal.

6.6. LA DEEP WEB

Hasta ahora se ha conceptualizado bastante sobre la Deep web, algunos de sus sitios, y lo que se puede conseguir, pero es necesario verificar a fondo la estructura de estos, la traza y demás, para ello se han seleccionado unos para verificarlos y contextualizar un poco más sobre estos dominios; cabe resaltar que hasta ahora solo se ha hablado de aquellos que se facilitan a través de la red Tor, pero existen muchos más, que diferentes a los dominios que existen en internet que tienen la particularidad de que usualmente terminan con dominios relacionados a alguna actividad comercial como los dominios .com, organizaciones gubernamentales como .gov, ubicación geográfica como .ar, .mx, .co entre otros, con la web profunda las cosas cambian bastante, a tal punto que el nombre de dominio, no significa ninguna relación con el contenido de lo que ofrece y mucho menos está ligado a una identidad o asociación en particular con un grupo de sitios.

6.6.1. Estructura de un sitio Onion

Para este apartado se mostrarán los dominios asociados a la Deep Web que se clasifican con la terminación. onion para analizarlos, a continuación, se muestra un listado de sitios agrupados por categorías, donde se han seleccionado al menos uno por categoría para especificar su estructura, especialmente para visualizar el sitio y encontrar detalles de estos, ver tabla 2 sitios Onion.

Tabla 2. Sitios Onion

Nombre	Link	Descripción
Comercio		
Empire Market	http://mqpawblcdfnwuyzv.onion/	Es un mini mercado online, su acceso es restringido. Pero utilizas firma hash 256.
BMG	http://5xxqhn7qbtug7cag.onion.plus/	Venta ilegal de armas (mercado negro).
Buscadores		
Torch	http://xmh57jrzrnw6insl.onion/	Buscador de sitios en la Deep web similar a los que se encuentran se la web tradicional, su motor de búsqueda es limitado.

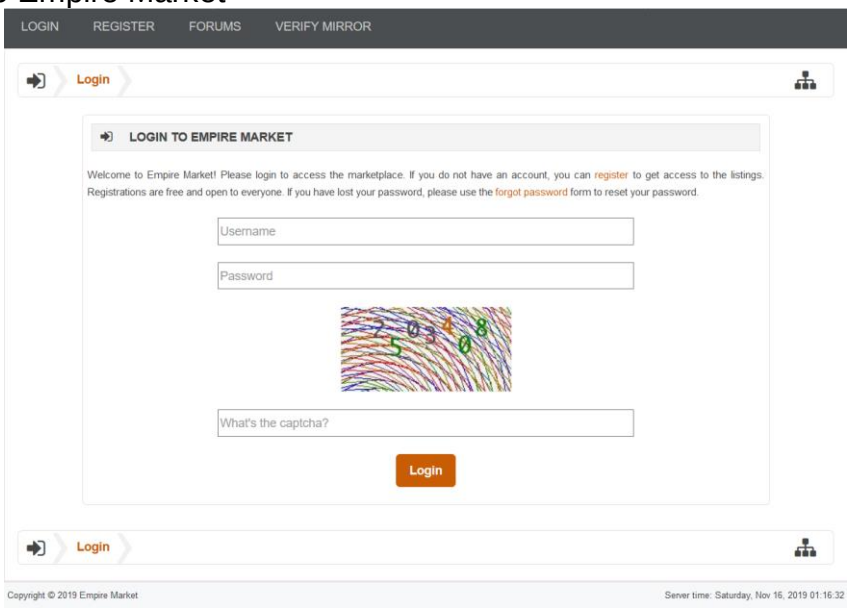
Not Evil	hss3uro2hsxfogfq.onion	Es un buscador que permite la búsqueda por palabra claves.
Venta de sitios o Dominios		
OnionName	http://onionname3jpufot.onion/	Venta de dominios. onion, los pagos se realizan en Bitcoin.
TorShop	http://shopsat2dotfotbs.onion/	Es un sitio para venta o apertura de tiendas online con dominios .onion.
Servicios financieros		
Zenith	http://zenithccalwhzy26.onion/	Servicio de transferencia de dinero.
onionWallet	http://ow24et3tetp6tvmk.onion/	Billetera online de bitcoin e intercambio de este.
Email		
TorGuerrillaMail	http://grrmailb3fxpjbwm.onion/	Servicio de email desechables.

6.6.1.1 Estructura de sitios de comercio

Empire Market[19]: Considerado como un heredero del famoso sitio Alphabay, este se encuentra alojado en la Deep web, cuyo propósito es el comercio de mercancía ilegal, en otras palabras su actividad está directamente involucrada con el mercado negro, y entre sus productos se encuentran: armas, drogas, tarjetas de débito y créditos robadas, transferencia ilegales de dinero, recargas PayPal ilícitas, malware, además de lo anterior también se realizan ventas de productos que en esencia no son dañinos no pero cuentan con las licencias respectivas de comercialización, como son la venta de medicamentos o artículos quirúrgicos entre otras. A continuación, se muestra la apariencia del sitio en la ilustración 6.

[19] EmpireMarket. {En línea}. {25 de noviembre de 2019}. disponible en: https://mqpawblcdfnwuyzv.onion.to/

Ilustración 6 Empire Market



Fuente: Empire Market disponible en https://mqpawblcdfnwuyzv.onion.to/

La moneda de referencia para el intercambio es el dólar estadounidense pero las transacciones que se realizan son en: Cryptomonedas Bitcoin, Litecoin y Monero, ya que así se puede preservar más, el anonimato de quienes efectúan el servicio; así mismo para la seguridad del sitio se utilizan 2-FA. Multisig, escrow, pin de seguridad, frase de inicio de sesión y frase de registro. Curiosamente el sitio cuenta con la insignia de copyright en el footer (como si de contrariar a la idea común de que todo es ilegal), en la página no se detecta ejecución de programa malicioso, no tiene certificado de seguridad valido, no es vulnerable a inyección SQL, requiere varios filtros para la conexión, por ello suele enviar errores de conexión de tipo 502; no utiliza Cookies que intenten ingresar a la computadora sin permiso y sin previo aviso, lo que hace entender que no se realiza ejecución no autorizada en el pc en este caso para saber quién accede al sitio. Para la autenticación requiere catpcha y funciona con un archivo. índex. al mirar su código se ve lo siguiente en la ilustración 7.

Ilustración 7 Código Empire Market

```
<!DOCTYPE html>
<html>
<head>
    <title>Empire Market</title>
    <link rel="stylesheet" type="text/css" href="http://mqpawblcdfnwuyzv.onion/public/css/style.css?v=4"/>
    <link rel="stylesheet" href="http://mqpawblcdfnwuyzv.onion/public/css/font-awesome.min.css"/>
    <link rel="icon" href="http://mqpawblcdfnwuyzv.onion/favicon.png" type="image/png"/>
```

Fuente: disponible en https://mqpawblcdfnwuyzv.onion.to/

La base es HTML y CSS, no tiene JavaScript ni está diseñado en PHP, la codificación de texto es UTF-8 el sitio es similar a cualquier otra página web de internet. La clave PGP oficial es, como se muestra en la ilustración 8.

Ilustración 8 Clave PGP

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFoTKj4BEADF8SRTYfFg17I5cYMbIGYBg2nLb8kCOL47vE6k38yUme0Lp42f
FKyoaSCaERFAjFwRKFpS1pRF2RDCFxC4dNGh3GusHpUcdw2WOE2wt+cKcuMjW1JU
asB6jOBw5UsKuHCMcPe6xur/rWvW80ZoijXHABsoiLjagmDRqNxLCGf06vrEfViD
uJchyusaM5WBxcDASBUPc65m0MecaB479kinxYjQWf0btadnuJVhHsv8hRosuC3x
FsHfDEsCB1A6nr0ivHa8gECEI/5mAYdB7fVWin6sig1aganAJmmqqbaveT/s7LvQ
JqQ2HAHLvUkqndQSPtuDboB+8FY2XDLPy+V7zP7McQJVHeUyiycVhsrZJnclZh/Y
/NAF9IcfiOcDYYoHntrU0inWjw6u+72UTtxMLZ4zIYxYVFiijyR855XmEfLz007E
Sk0h4FHojoJCl7wQVuSmxHXB/gLsGb+znDd/z4NMWFUJOVdKtdW76fINvkq4c51E
7ql8Cq1HkhYaUBvqovBrKvIII+cyFlu87WLGpCm0nQFNi+M5nuZ8U3sH2NJ4Nr9h
Bt4TdW/Qou9FmLFoWiqCXiUvlFMqhxBckaJtxqRV0KV/X7jVfaQpJCcWgJf2jhCy
6HR+8lB8uj9hCykpfLOTlZ61ET5jVJC5t6vHyEQDO/+r4LXhF9Io/ybqrQARAQAB
tCRFbXBpcmVNYXJrZXQgPGVtcGlyZW1hcmtldEBub251LmNvbT6JAjkEEwECACMF
AloTKj4CGwMHCwkIBwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCRYCb1bquDHnba
EADDNlgnN1w3BgXKiD4Ju8z9ddab91BdkspW3xdTUbqnN+uGNZhTgaIMosv6d11X
osqPBiDmaa9+afigf8KsqmqC6f3JxqaLkRug2JaEcHCH/hGBes36skxCF7zxk/Ju
Mmnu/I1mwt4fP/4ebdG2ygWU+MEVFhiy8GYGUQ7X2KOJcDQGP+8Sp4Zl6U/TL/9f
wg+ThXisiHEpOTDAbPDmf62JQO0D15tQMogpn156+xwlCon3Fhr0ycwkix2EJCzz
zHJaugCdVP8zsUobwsPB4QpEkubsOcfOKig2bxnM4CMYzMfSn7eXVvOM4qg3CGR5
kxha8LVC1ib/O7XJbvKbwxwjrO0/+PWeoLNwgYV40SJeI4jm/xi6hWqPGMObn/xx
+M13WUQA5LwfhUpmbLbplm8rt38BAld++tFTdNneQIPM74LXNUUuEWiKJPcAnx0L
GjWCMwsOOe/2D9178L5BXsLh0Ext9xNU3krp7VeHRtOF1RDOdg6YZbZ3nonLswLG
V9xrcMAYmEKwWNaLZAr/tPq6k8glo9rCfCCN50kG9h77kZi5zdUgHtxZFHUKs/Vs
0HhrdqXK6qGjQ/AijhA0IgPuWbCy9bUtU5iaUeA6z51+vxbda0bMmQwO1dv0JUKI
TeTDcleRszfXwsuiCwviiUloKKa27JuBChQ3vy6iVwBUB7kCDQRaEyo+ARAAsyNM
mlYo8a1qI8qOF2LEq8NoGTHBe8u1N4Q1rlOfIw6mEUgDD9G+QAUPPVcpwjTDdTC0
zzoRkpUbqOMpNJqpCA1xTUJBnuBdyRtq/vEyuV5xc8niji9sbkxj2psn5tu//dfy
2MxNbFP1JnBRQ5dEIj6d5kcZt0+EhwXqmKvKPPhMeVEz4E4fDOZeMqrbmcY4iiTT
qFdN8aJ3E+tJ6p86HUWwgMOwcQhCzah5q6eMaqtZA7PnuIpeudeVok0i5pvyfDmJ
zB4nqeeJFyzgNsGy5GkN4vI2zX7luYrxzrDIkmTIwCFmPk9PQHiAY0I+OqeUoPiL
HUizvschbKV3Tq8YNwlyi5GTymysCKbHvyqGdNgRJxAzV6htDymEBkB5egj98DhM
UxCP9P1lhjEkf6GSJK0Y6cppL1NkjD2VG/BT++SqznQCbey1kuZ1UGFaDOpN1vQv
F5zSG2t7WLmoZU3k7X3ljp2pSBD2EFcac/wQ+6uE9UMiFU1y9AImC/AqC3oIWE8S
gPmG7FULN2pjfQ7wPNqovChtxB3lAqzzzFTX+7UDMiGf8oakxkvwIjQkUL5zEOXn
rTvKLaSy4ehxpcyLvU5GXgMyWMaugp04ff3UeJ680eM+P/zJAt81hggOJNqqMVm5
aiEuY1yBV9Tc2F8qRNwX53UtjGg6YQ0wRgqAp2kAEQEAAYkCHwQYAQIACQUCWhMq
PgIbDAAKCRCRYCb1bquDHrKOEACtjY0GUx3wkoDXqLKErhsIwou1MBtQg8ZnkrU0
2MLrRgOa2sABIsFSSLRVJes4oNEYpq6s3dt7zZTBR4Xuc1MGQHbfW5LRnwi+oD+X
MqKLYwLPVU1xLdFvF5sl6I+LKRhQTm3CZ56RC2XEyhsBBDSFG6eJGkiV1WHqBBDW
OI6M/hCs05bpyCpMixXzagGv97j7JITNZd88NbiYU44jbqdTSa6sDvQ/gnPAB9p0
JAZCDmN0uLZ6zr2S7ovDl7O+1YUj8oKNkcnynlzl4CmQ539Js5SzdGaQ98fPIDgU
zDfP6m77+MlmgzDkOxsWfzK87Rw2AsWQTZILc7pZvLoTFHsMsp4nKUOTWj5Aj2PA
zngdH5wkYBTAb3aaVxfdw3HoJ6eKmAnK7fdmP9XBVCZF1JCppw91c6Jh6/8PcNbr
33rkvO88YTCq5nCwYEGlZ90PwHGGJqzNBW/v+MJf89eithynE74QRReVNuJDwmdd
qg0/+/nuFsfglbRHCAMGpFnYART42aHILnJAd86+9t6m9q3f3fUqR7e93Zl7R8I9
Ol3Mtrgn8/IyiqUvFxHM91BdWMkWRv4jirytBe8+JC49GNEf0hMuBw3IqukiQpC9
2J0mCuRoJwqtH101k226lRN7RVwTJFnZHXotewzMmmkEc+M8EHofjLLAw9p2VA8C
Y+2Rlg==
=eO6H
-----END PGP PUBLIC KEY BLOCK-----
```

Fuente: disponible en https://mqpawblcdfnwuyzv.onion.to/

MBG[20]: Este sitio de venta de armas, solo recibe pagos en bitcoin, no ejecuta ningún tipo de script malicioso, además tiene un proxy que anonimiza el sitio, lo que significa que fue diseñado para que las personas pueden ingresar evadiendo firewall, o cualquier herramienta de filtrado. Así se presenta el sitio ver ilustración 8 sitio MBG:

[20] BMG. “Black Market Guns”. {En línea}. {25 de noviembre de 2019}. Disponible en: http://5xxqhn7qbtug7cag.onion.plus/

Ilustración 9 Sitio BMG

Fuente: BMG disponible en http://5xxqhn7qbtug7cag.onion.plus/

Tiene la particularidad de que utilizan un servidor de correos de la Deep web el famoso secmail, Es decir, el sitio no cuenta con servidor propio de comunicaciones y utiliza una llave pública PGP que se puede apreciar al final del sitio siempre y cuando el usuario se halla registrado en el sitio, en este caso no se mostrara debido a que el acceso podría significar una participación de los ilícitos que suceden dentro del sitio. Este es un fragmento de su código fuente, el cual utiliza HTML y CSS, como se muestra en la ilustración 10 código fuente sitio MBG. Es de resaltar que por obvias razones el sitio opera bajo la ilegalidad.

Ilustración 10 Código fuente sitio BMG

```
<!DOCTYPE html>
<html lang="en">
<head>
    <title>BMG (Black Market Guns) : Trusted source for worldwide GUN shipment</title>
    <style>
        body {
            background: url("image/fondo.jpg");
            text-align: center;
        }

        body, input, textarea, button, legend {
            font-family: "Lucida Grande", Helvetica, Arial, Verdana, sans-serif;
            color: #333;
            font-size: 14px;
```

Fuente: http://5xxqhn7qbtug7cag.onion.plus/

6.6.1.2 Estructura de páginas web de buscadores

Torch: Este buscador indexa contenidos web de la red Tor y presenta las siguientes condiciones técnicas para los sitios a indexar:

- El tipo de archivo o extensión del banner para la página de resultados será JPG, GIF o PNG y el tamaño debe ser exactamente de 120 PX de ancho y 60 PX de alto.

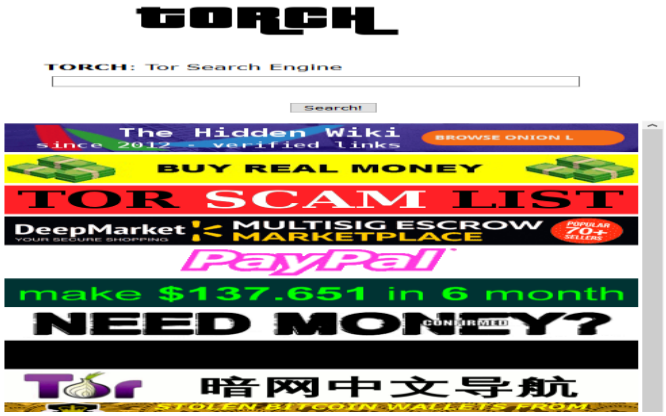
- El tipo de archivo del banner de la página frontal debe ser JPG, GIF o PNG y el tamaño debe ser exactamente de 468 PX de ancho y 60 PX de alto.

- Se permiten GIF animados.

- Para el enlace se debe utilizar etiqueta HTML <a> limpia. obligatoriamente está prohibido JavaScript[21].

No se conoce mucho de este buscador, pero lo que sí es claro es que al igual que cualquier otro, utiliza un algoritmo de búsqueda optimizado solo para sitio de la Deep web, aunque aun así se puede buscar sitios en la Clearnet, pero los resultados no serán iguales a los de buscadores como Google o Bing. Esta es la apariencia de la página del buscador, ilustración 11

Ilustración 11. Torch

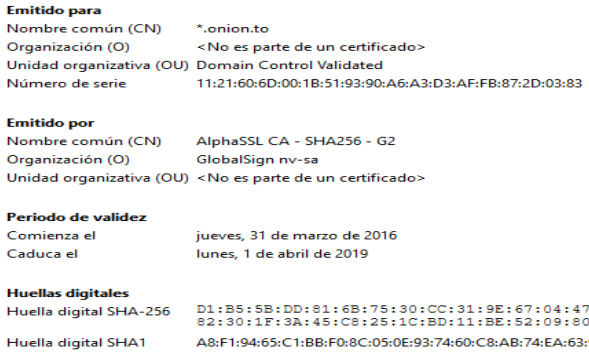


Fuente: disponible en http://xmh57jrzrnw6insl.onion/

[21] Torch. “Information for advertisers and users”. {en línea}. {18 noviembre 2019} disponible en: http://xmh57jrzrnw6insl.onion/adinfo.html

A continuación, se logra verificar los detalles del certificado los cuales son falsos, ya que las organizaciones y unidad organizativa que aparecen no corresponden, además no existen entidades que se dedique a realizar seguimientos a estos sitios primero porque irían en contra del anonimato del sitio, segundo debería entregar información total de las actividades de éstos, ilustración 12.

Ilustración 12. Certificado Torch



Emitido para

Nombre común (CN)	*.onion.to
Organización (O)	<No es parte de un certificado>
Unidad organizativa (OU)	Domain Control Validated
Número de serie	11:21:60:6D:00:1B:51:93:90:A6:A3:D3:AF:FB:87:2D:03:83

Emitido por

Nombre común (CN)	AlphaSSL CA - SHA256 - G2
Organización (O)	GlobalSign nv-sa
Unidad organizativa (OU)	<No es parte de un certificado>

Periodo de validez

Comienza el	jueves, 31 de marzo de 2016
Caduca el	lunes, 1 de abril de 2019

Huellas digitales

Huella digital SHA-256	D1:B5:5B:DD:81:6B:75:30:CC:31:9E:67:04:47:3A:CA:82:30:1F:3A:45:C8:25:1C:BD:11:BE:52:09:80:9C:E9
Huella digital SHA1	A8:F1:94:65:C1:BB:F0:8C:05:0E:93:74:60:C8:AB:74:EA:63:98:2F

Fuente: disponible en http://xmh57jrzrnw6insl.onion/

El código de la página utiliza, HTML, XML, CSS y JavaScript, mismos lenguajes que se utilizan para crear cualquier sitio web, incluso las imágenes tienen extensiones similares a las de cualquier página de la Clearnet, ilustración 13.

Ilustración 13. Código fuente sitio Torch

```
<head>
<title>TORCH: Tor Search!</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta name="description" content=""/>
<meta name="keywords" content=""/>
<link rel="shortcut icon" href="favicon.png" type="image/png" />

<style type="text/css">
body{
    text-align: center;
    font-family:Verdana, Arial, Helvetica, sans-serif;
    font-size:.7em;
    margin: 10px;
    color: #000;
    background: #fff;
    min-width: 520px;
```

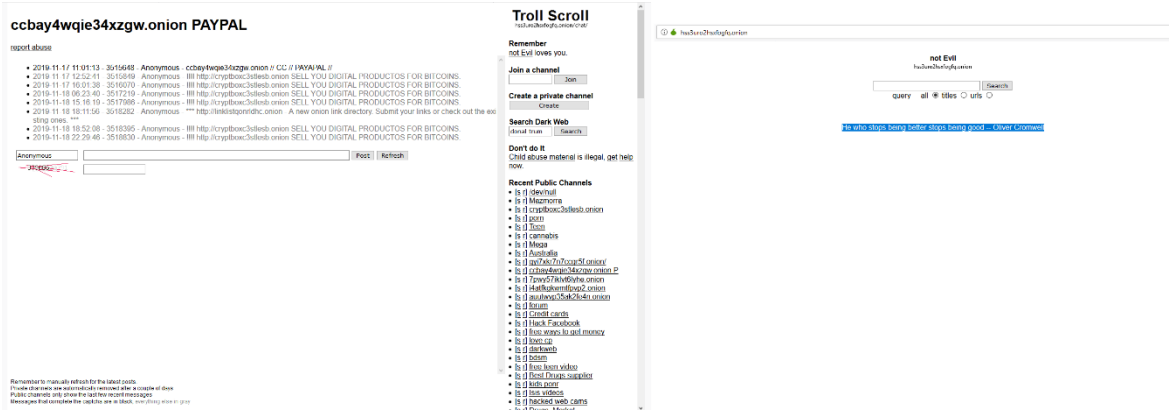
Fuente: http://xmh57jrzrnw6insl.onion/

NOT EVIL[22]: Es un buscador que se destaca por su facilidad de búsqueda pero con la limitación de que esta se realiza con palabras claves muy precisas; por

[22] Not Evil. {en línea}. {24 de noviembre de 2019}. Disponible en: (hss3uro2hsxfogfq.onion)

consiguiente es un buscador con pocos filtros por lo que una búsqueda puede arrojar todo tipo de contenido desde los más simples hasta sensibles, incluso si se busca algo como la palabra “manzana” puede arrojar a la par una tienda con objetos similares o una página pornográfica con dicha palabra; por otro lado y como regalo para el usuario, el navegador siempre está regalando una foto en cada ingreso (la primera foto al ingresar fue Donald Trump joven señalando un proyecto en new york). Como valor agregado el sitio, facilita la creación de canales para publicación privada y troll, ilustración 14.

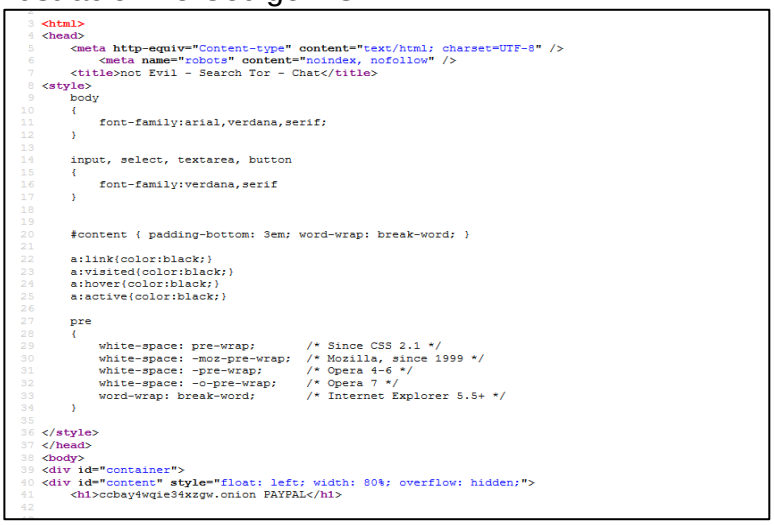
Ilustración 14. NOT EVIL



Fuente: disponible en hss3uro2hsxfogfq.onion

No es posible especificar exactamente los detalles, pero el sitio cuenta con al menos una base de datos diferente a la que normalmente tendría un sitio para almacenamiento de la información a mostrar, la cual recibe parámetros ingresados por tecla, cuenta con re direccionamiento a YouTube y otros sitios que se manifiestan en contra de la pedofilia y todo tipo de abuso a menores, y usa codificación UTF-8, como se muestra en la ilustración 15.

Ilustración 15 Código NOT EVIL



```
<html>
<head>
    <meta http-equiv="Content-type" content="text/html; charset=UTF-8" />
        <meta name="robots" content="noindex, nofollow" />
    <title>not Evil - Search Tor - Chat</title>
<style>
    body
    {
        font-family:arial,verdana,serif;
    }

    input, select, textarea, button
    {
        font-family:verdana,serif
    }


    #content { padding-bottom: 3em; word-wrap: break-word; }

    a:link{color:black;}
    a:visited{color:black;}
    a:hover{color:black;}
    a:active{color:black;}

    pre
    {
        white-space: pre-wrap;       /* Since CSS 2.1 */
        white-space: -moz-pre-wrap;  /* Mozilla, since 1999 */
        white-space: -pre-wrap;      /* Opera 4-6 */
        white-space: -o-pre-wrap;    /* Opera 7 */
        word-wrap: break-word;       /* Internet Explorer 5.5+ */
    }

</style>
</head>
<body>
<div id="container">
<div id="content" style="float: left; width: 80%; overflow: hidden;">
    <h1>ccbay4wqie34xzgw.onion PAYPAL</h1>
```

Fuente: disponible en hss3uro2hsxfogfq.onion

6.6.1.3 Estructura en páginas de venta de sitios web y dominios

OnionName[23]: El sitio representa un riesgo potencial de seguridad, en la cual muestra compatibilidad con diferentes estándares, pero no se somete a ninguna directiva y los detalles en su certificado, que se encuentran caducados lo cual se confirma; además se evidencia la ejecución XML, xhtml y algunos scripts para recopilar información de quien ingresa al sitio. Algunos detalles de su certificado se muestran en la siguiente tabla:

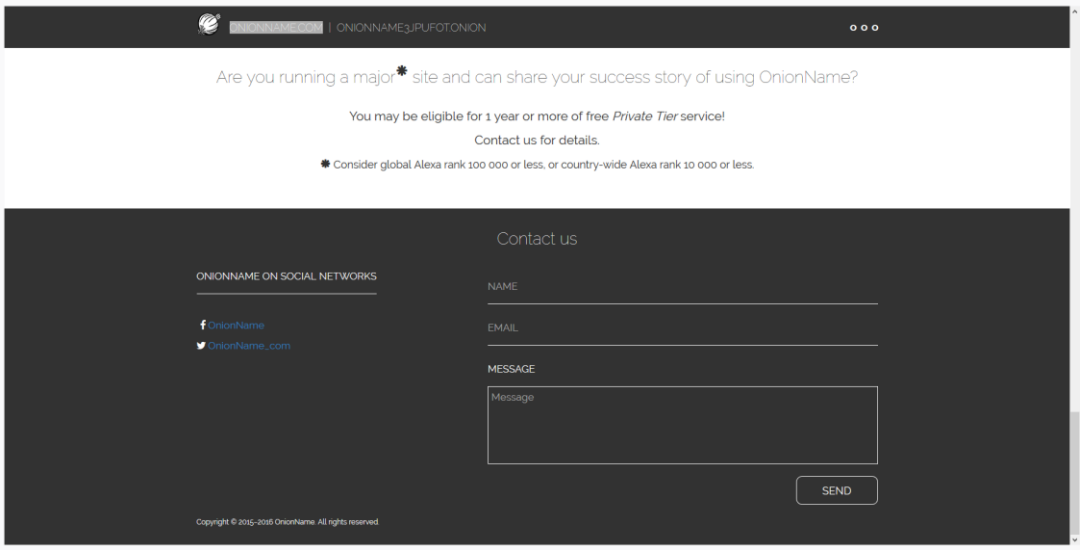
Tabla 3 certificado ONIONNAME

Campo	Valor
Emitido por	AlphaSSL –SHA256 –G2
Valido	Desde 31 marzo 2016 hasta 1 abril 2019
Huella digital	a8f19465c1bbf08c050e937460c8ab74ea63982f
ID de clave	Id. de clave=f5cdd53c0850f96a4f3ab797da5683e669d268f7

La apariencia gráfica del sitio es como está en la ilustración 16.

[23] OnionName. {En linea}. {24 de noviembre de 2019}. Disponible en. (http://onionname3jpufot.onion/)

Ilustración 16 ONIONNAME



Fuente: disponible en http://onionname3jpufot.onion/

El sitio cuenta con un par, muy similar en diseño y ejecución con la dirección de anionname.com, Esta desarrollado en HTML, CSS, y JavaScript, realiza consumo de web service con Jasón, ejecuta muchos scripts y utiliza landind pages y tiene palabras claves en la cabecera para que sea indexado en esta zona de la red en el caso del sitio cuyo dominio termina en .onion y las mismas palabras claves para que el sitio con dominio.com pueda ser indexado en la clearnet; utiliza una codificación de caracteres UTF-8, esto usualmente es, para que al no ser leído por http pueda haber una lectura correcta de los caracteres en el navegador, mediante la interpretación por HTML. El código fuente del sitio se ve así en la ilustración 17, Parte del Código fuente ONIONNAME:

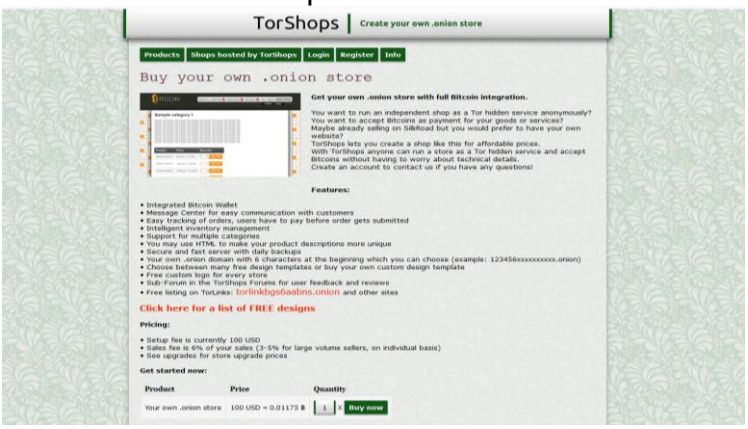
Ilustración 17. Parte del Código fuente ONIONNAME

```
<!doctype html>
<html>
<head>
<meta charset="UTF-8">
<title>OnionName: Obtain your vanity .onion domain name in Tor network without much hazzle!</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0,maximum-scale=1.0, user-scalable=no">
<meta name="description" content="Choose your desired domain name prefix, and order the .onion domain, starting from 0.45 mBTC for 8 letters.">
<meta name="keywords" content="Tor,Onion,domain,hidden service,Darknet,DNS,GoDaddy,purchase,buy,order,Bitcoin,XBT,BTC">
<link rel="stylesheet" type="text/css" href="/static/landing/css/bootstrap.min.css"/>
<link rel="stylesheet" type="text/css" href="/static/landing/css/bootstrap-theme.min.css"/>
<link rel="stylesheet" type="text/css" href="/static/landing/css/font-awesome.min.css"/>
<link rel="stylesheet" type="text/css" href="/static/landing/css/slick.css"/>
<link rel="stylesheet" type="text/css" href="/static/landing/css/slick-theme.css"/>
<link rel="stylesheet" type="text/css" href="/static/landing/css/style.css"/>
<link rel="stylesheet" type="text/css" href="/static/landing/css/style-custom.css"/>
<link rel="shortcut icon" href="/static/landing/images/favicon.png" />

<script language="JavaScript">
    var randomWordsToDisplay = [
        'No more complex software configuration...',
        'Without purchasing expensive GPU hardware...',
        'No long wait for mining to complete...',
    ];
</script>
<script type="application/ld+json">
{
  "@context": "http://schema.org/",
  "@type": "Product",
  "name": "OnionName Tier 8",
  "description": ".onion domain starting from any keyword 8 letters or less long",
  "sku": "tier8",
  "url": "https://onionname.com/order?tier=tier8",
  "offers": [
    {"@type": "Offer", "priceCurrency": "XBT", "price": "0.00045"}
  ]
```

Fuente: disponible en http://onionname3jpufot.onion/

TorShop[24]: Tiene la apariencia de un sitio web tradicional; solo recibe pagos mediante bitcoin. No emite claves ni restricciones de acceso. Como cualquier sitio de comercio cuenta con un centro de mensajería para facilitar la comunicación con los clientes, para ello utiliza servidores propios; otra de las bondades es que tal como sucede con otros proveedores de dominios, cuenta con servicios de copias de seguridad diarias, muchas plantillas de diseño gratuitas y personalizada, logotipo gratuito para cada tienda, foro alojados en los foros de TorShops, que funcionan como subforos para comentarios y reseñas de usuarios y como guía para los usuario provee un listado gratuito en TorLinks y otros sitios en la siguiente ilustración 17.

Ilustración 18 TorShop



Fuente: disponible en http://shopsat2dotfotbs.onion/

Su código permite ver que está diseñado con HTML 4 y es complementado con CSS para darle algunos atributos al sitio, ya que está diseñado en una versión de HTML que no era tan dinámica como la actual, utiliza palabras claves para que sea indexado por los buscadores de la Deep Web; también se utiliza PHP por lo que la ejecución del script es del lado del servidor por obvias razones, ver ilustración 19.

[24] TorShop. {En linea}. {24 de noviembre de 2019}. Disponible en: (http://shopsat2dotfotbs.onion/)

Ilustración 19 código fuente TorShop

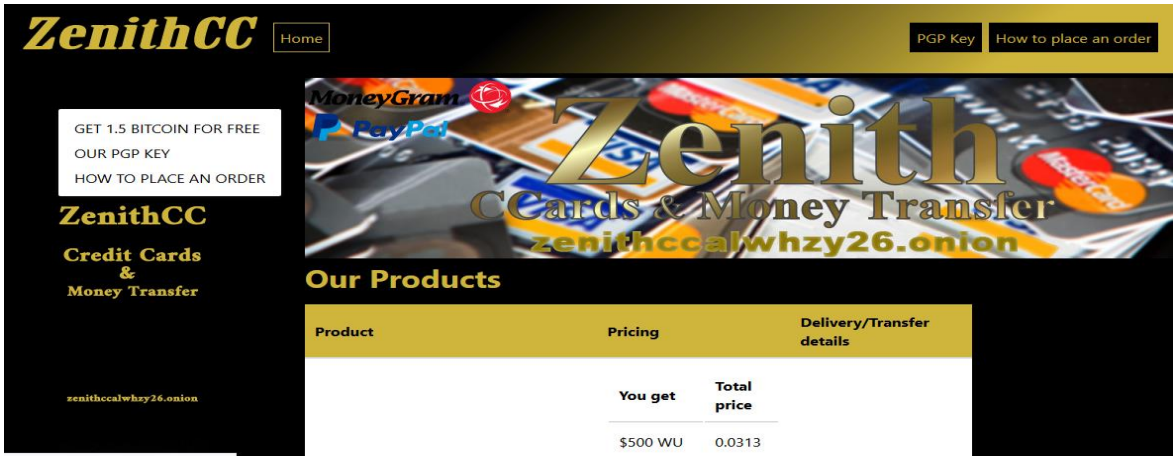
```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta name="description" content="TorShops - buy and sell drugs, guns, counterfeits, fake ids, fake passports for bitcoin - great silk road alternative - get your .onion store today"/>
<link rel="shortcut icon" type="image/x-icon" href="favicon.ico">
<title>TorShops | Create your own .onion store - buy and sell drugs, guns, counterfeits, fake ids, fake passports for bitcoin</title>
<style type="text/css">
body {
background:url(background.png);
background-attachment:fixed;
color:#000;
margin:0;
padding:0
}

body,.buttn,.txt,textarea,#menu a {
font:13px Verdana,Tahoma,sans-serif
}

div {
position:relative
}

#header {
margin-bottom:20px
}
```

Fuente: disponible en View: http://shopsat2dotfotbs.onion/

6.6.1.4 Servicios financieros

Zenithcc[25]: Es un sitio de transferencia dinero online, compra de tarjetas de créditos y tarjetas de regalos Amazon, cuenta con diferentes modalidades de transferencia sin limitaciones legales o restricciones regionales, lo único que se necesita es ponerse en contacto con el sitio a través de correo electrónico, solicitar el producto, concretar la cantidad a pagar, y el país; después del acuerdo se realizan los depósitos a través de fideicomiso y listo; formalmente se realizan los pagos a través de bitcoin, ver ilustración 20 ZENITHCC.

Ilustración 20. ZENITHCC



Fuente: disponible en http://zenithccalwhzy26.onion/

[25] Zenithcc. {En linea}. {25 de noviembre de 2019}. Disponible en: (http://zenithccalwhzy26.onion/)

El sitio fue creado en HTML y CSS, en la cual se evidencia varios tags: el primero para indicar el tipo de carácter que reconoce y muestra el sitio (utf-8), cuenta con un atributo para la identificación de encabezados de los mensajes de respuesta http, por lo que se establece que el sitio está completamente sujeto al protocolo HTTP, pero sin las respectivas directivas de seguridad, el sitio muestra palabras claves importantes en su cabecera que es información útil sobre el sitio, pero no permite la posibilidad de indexación, ver ilustración 21 Parte del código fuente ZENITHCC.

Ilustración 21. Parte del código fuente ZENITHCC

```
<!DOCTYPE html>
<html lang="en">

<head>
  <title>ZenithCC | Credit cards, PayPal, MoneyTransfer..</title>
  <link rel="icon" href="assets/favicon.png">
  <meta charset="utf-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge, chrome=1">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no, user-scalable=no">
  <meta name="keywords"
    content="ZenithCC, Carding, Credit cards, Paypal, Buy credit cards, MoneyTransfer, MoneyGram, Mastercard, Bitcoin
  <meta name="description"
    content="Get your credit card, Paypal, MoneyTransfer or Amazon Gift card with the lowest prices in the market.">
  <meta name="author" content="zenithcc">
  <meta name="theme-color" content="#000000">
  <meta name="msapplication-navbutton-color" content="#000000">
  <meta name="apple-mobile-web-app-status-bar-style" content="#000000">
  <meta name="msapplication-TileColor" content="#000000">
  <!-- Stylesheets here -->
  <link rel="stylesheet" href="assets/css/main.min.css">
  <link rel="stylesheet" href="assets/css/main-icons.min.css">
  <link rel="stylesheet" href="assets/css/main-exp.min.css">
  <link rel="stylesheet" href="assets/css/app.css">
</head>

<body style="background-image: url('assets/images/background/backg.png');">
```

Fuente: http://zenithccalwhzy26.onion/

OnionWallet[26]: Aunque la unidad monetaria no corresponde al dólar, euro o similares, el sitio entra en la categoría de servicio financiero por la sencilla razón de servir como una especie de banco para cryptomonedas, es decir es una billetera online para depósito y transferencia de Bitcoin, pero la diferencia entre esta billetera y otras como Coinbase, cryptonator y demás, es que debido a que cada vez son más las tecnologías para rastrear este tipo de transacciones y descifrar el contenido o la información que involucra cada envió, algo que no sucede tan fácil con OnionWallet ya que está alojada en la red Tor y su conexión es que no es fácil de rastrear, además no se somete a ningún tipo de regulación financiera de ningún gobierno o institución especialmente no se acoge a KYC (Know Your Customer) ni a AML (Anti-money Laundering) convirtiéndola en un sitio ideal para depósitos ilegales, lavado de dinero o para aquellos que por alguna razón necesitan esconder sus ingresos, como se muestra en la ilustración 22.

[26] OnionWallet. {En línea}. {25 de noviembre de 2019}. Disponible en: (http://ow24et3tetp6tvmk.onion/)

Ilustración 22. OnionWallet

Fuente: http://ow24et3tetp6tvmk.onion/

OnionWallet está diseñado en HTML 4 y CSS tiene link que redirigen a sitios de la clearnet para la compra e intercambio de Bitcoin. Las transacciones son realizadas con APIS de PHP y están etiquetadas con un ancla que dirige a cada página, como se identifica en la ilustración 23.

Ilustración 23. Parte del Código fuente OnionWallet

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=utf-8">
<meta name="description" content="OnionWallet is a Tor based Bitcoin Wallet and Bitcoin Laundry / Mixer, launder your
<link rel="shortcut icon" type="image/x-icon" href="favicon.ico">
<title>OnionWallet Anonymous and secure Bitcoin Wallet and Bitcoin Mixer, Laundry. Wash your Bitcoins. Tor Web Wallet
<style type="text/css">
body {
background-image: url("background.png");
color:#00576A;
margin:0;
padding:0
}
```

Fuente: http://ow24et3tetp6tvmk.onion/

6.6.1.5 Email

TorGuerrillaMail[27]: Es un proveedor de correo electrónico anónimo de propiedad de la compañía desarrolladora de software Jamit software limitada, fundada en Sídney- Australia, pero que en la actualidad tiene su sede en Hong Kong. El sitio

[27] TorGuerrillaMail. {En línea}. {25 de noviembre de 2019}. Disponible en: (http://grrmailb3fxpjbwm.onion/)

como tal cuenta con uno similar a él, en la clearnet y con un dominio .com, según la compañía ambos sitios operan bajo legalidad, tienen políticas de privacidad de datos, marcas registradas y términos y condiciones, lo que permite entender que este sitio aunque funciona en la Deep web, no está diseñado para facilitar la ilegalidad, pero se aclara que la información enviada por tercero y la vulneración que alguno usuario cometa a otros queda bajo responsabilidad de este, dado que aunque tienen normas, no se descarta la posibilidad del mal uso, ilustración 24.

Ilustración 24. GuerrillaMail

Fuente. http://grrmailb3fxpjbwm.onion/

El sitio tiene incrustado elementos de Jquery, no utiliza las cookies para recolectar las preferencias del usuario, también emplea herramientas de Google analytics y Google adsense en los correos y todos sus datos podrían estar sujetos a futuras investigaciones contra correos no deseados, antimalware o anti Phishing. Aunque ese sitio opera en la Deep Web no significa que este bajo la ilegalidad, por ello el proveedor señala que se utilizan datos de correo electrónico (spam) para investigaciones que estén relacionadas con algún delito. Además, el sitio utiliza cifrado HTTPS. La moneda oficial del sitio que está en la Deep web es el Ethereum, ilustración 25.

Ilustración 25 Código fuente sitio guerrilla mail

```
<!DOCTYPE html>
<html lang="en"  dir="ltr" >
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta name="HandheldFriendly" content="true">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
    <title>✉ Guerrilla Mail on Tor</title>
        <meta name="description"
          content="Don't want to give them your real email? Use a temporary email. No registration, lasts 60 mins. Pr
        <link rel="stylesheet" type="text/css"
          href="/js/jquery-ui/css/gm-theme/jquery-ui-1.10.3.custom.min.css">
    <link rel="stylesheet" type="text/css" href="/js/intro/introjs.min.css">
    <link rel="stylesheet" type="text/css" href="/css/gm.css">
    <link rel="stylesheet" type="text/css" href="/js/jquery-modal/jquery.modal.css">

        <style>
```

Fuente: http://grrmailb3fxpjbwm.onion/

Finalmente, a partir de lo anterior se llegó a determinar que todos los sitios que pertenece a la red Tor o que tienen la misma estructura, trabajan con el dominio. onion no presentan ninguna diferencia en cuanto a su código fuente, pues aunque si utilizan versiones de HTML bastantes en desuso, operan bajo las mismas reglas de sintaxis, además la mayoría de los sitios con extensión .onion se caracterizan por mostrar más compatibilidad con archivos de sistemas Windows, aunque se pueden ejecutar en ambos entornos sin problemas, y se diferencian porque las rutas no son directas y su alojamiento y enrutamiento son más intrincados, debido a las configuración de la red Tor

6.6.1.6 Comparativa Clearnet vs sitios onion

Usualmente se describe una página web como un documento estructurado y codificado en un lenguaje HTML y otros compatibles y complementarios, con el fin de que pueda ser leído por un programa llamado navegador, y a este conjunto de páginas se les llama, sitio web. Ahora bien se podría pensar que debido a la diferencia entre la navegación en la clearnet y los sitios anteriormente descritos, también hay una diferencia radical entre los sitios web que los componen pero la realidad es que sin distinción alguna todos estos sitios utilizan HTML como el insumo base de su creación, es decir todos contiene HTML, pero la diferencia está en que los sitios .onion utilizan versiones anteriores a HTML 5 por lo que se puede inferir que son sitios semánticamente muy pobres, por lo general no utilizan ninguna clase de API de Google por razones obvias, cuando se tratan de sitios de contenido ilegal, dificulta el almacenamiento de datos de lado del cliente y corta tajantemente la conexión, los recursos multimedia son muy limitados a tal punto que no se enfocan en usar, WebGL, SVG, o streaming; así mismo la integración entre recursos de hardware y software es pobre en comparación a todos los que se encuentran en la Clearnet.

Una característica importante para cualquier sitio web es la ejecución de contenidos incrustados o embebidos, cosa que se encontraran en los sitios onion, pero estos por lo general son pequeños script para procesar información del usuario y realizar algunas actividades del lado del cliente, de la misma manera que en los sitios convencionales.

Además de HTML se puede percibir la utilización de lenguajes como JavaScript, PHP, CSS, se realizan mucho consumo de web services, a través de SOAP, dado que para el intercambio de datos hay sitios que utilizan XML y este es el ideal para las comunicaciones entre las máquinas. Casi todos los sitios en esta parte de la red, son completamente dinámicos al punto de que se pueden conseguir servicios similares a los de la red de internet: como calculadoras de precios, en los sitios, páginas con foros de diversos temas, sitios con reservas de productos, y como consecuencia de estos servicios e inherente a esto la gestión de estos sitios, hay una enorme gestión de base de datos, lo que se traduce en toda una arquitectura de procesamiento de consultas SQL.Contrario a lo que muchas personas pueden suponer, todos los sitios encontrados tienen hipervínculos y enlaces interno y externos, incluso hay una gran cantidad de sitios que tienen enlaces a otras páginas conocidas en la Deep web o en la Clearnet, muchos tienen contenidos en YouTube, Facebook (en la web normal), Twitter; existen muchas campañas en muchos de estos sitios que dependen notoriamente de servicios de estas plataformas y brindan su servicios en ambos lados de la red, uno como complemento de la otra.En cuanto a servicios, si se toman cada sitio por categoría no habría ninguna diferencia particular, más que en la limitación y restricciones que tienen los sitios de la red profunda para conservar su anonimato, los ataques o saboteos.

Hay algunos mitos que existen y que es preciso señalar y aclarar, dado que son solo rumores:

- Es completamente falso que los sitios de la red. onion no estén indexado, pues muchos de estos utilizan palabras claves en sus cabeceras para ser fácilmente identificados por navegadores como Torch; lo que hay que aclarar es que, por pertenecer a otro tipo de red, estos sitios no son detectados por navegadores que no estén configurados para acceder a esta red.

- La navegación no es lineal, ni muestra los sitios bajo capas o nivel, incluso los buscadores de esta red pueden traer miles de sitios con solo iniciar la búsqueda con una palabra y mostrarlos sin ninguna limitación. En otras palabras, durante la navegación no se da la sensación de estar subiendo o descendiendo a ningún nivel.

- No todos los sitios tienen contenido ilegal o son altamente dañinos, pues algunos son creados dentro de la red con el fin de promocionar algunas campañas o brindar ayuda académicamente como el caso de Jiskopedia.

- Comúnmente se tiene la concepción de que no hay ley en estos sitios o que todo lo ilegal es permitido, pero hay sitios con políticas claras y definidas que prohíben conductas inapropiadas, intentos de vulneración al sitio o a otros en donde se deja claro al usuario el castigo por la infracción, incluso hay sitios que ofreciendo contenido ilegal o productos no legales tienen normas que señalan estar en desacuerdo con otro tipo de vulneración.No hay clasificación de contenidos por grados de sensibilidad, ni los sitios están etiquetados para ser mostrados bajo algún criterio relacionado al juicio moral.

6.6.2 Estructura de un sitio I2P

Los sitios que hacen parte de la red I2P[28] se les llama Eppsite su característica principal es que la url termina en i2p, son bastante difíciles de encontrar, debido a la forma como se realizan las peticiones de cliente al servidor y la respuesta del servidor al cliente, la cual se caracteriza por nodos de entrada y salidas inversas. El acceso se permite configurando varios parámetros como un proxy para el navegador y un puerto para la conexión, quitando las restricciones de un cortafuego (o firewall) y dándole el ancho de banda correspondiente al software diseñado para ello. Esta red es mucho más pequeña que Tor y tiene un sitio bastante organizado ya que brinda sugerencias para navegar en muchos de sus sitios, cabe resaltar que mientras se navega en esta red no es posible ingresar a otra red. Sus sitios al igual que los demás también utilizan HTML, XML y cualquier otro lenguaje para su diseño, ver ilustración 26 Estructura I2P.

[28] I2P. “que es I2P”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://geti2p.net/es/)

Ilustración 26. Estructura I2P

Fuente: Propiedad del autor I2P router console. 127.0.0.1:7657/home

6.6.3 Estructura de un sitio Freenet

Al igual que otros sitios de cualquier otra red, están diseñados con HTML versión 4 o anterior, utilizan XML, JavaScript, PHP, y otros más; todas sus cabeceras son bastante limitada, proporcionan información del sitio, pero por lo general no usan palabras claves y las líneas de código en esta sección son pocas en comparación a sitios de la red Tor o Clearnet. El código fuente de la página principal si visualiza en la siguiente ilustración 27 Parte del código fuente de la estructura de Freenet[29].

Ilustración 27. Parte del código fuente de la estructura de Freenet

Fuente: propiedad del autor freenet: USK localhost:8888

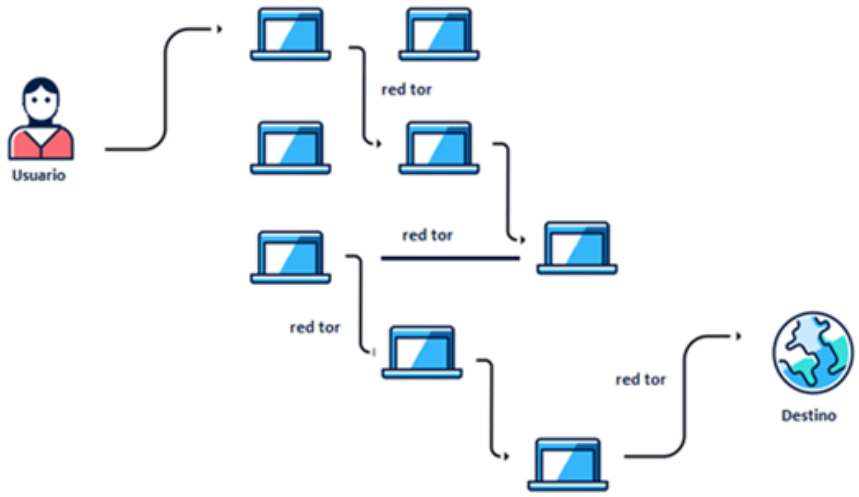
[29] Freenetproject.” Browse websites, post on forums, and publish files within Freenet with strong privacy protections.” {En línea}. {25 de noviembre de 2019}. Disponible en: (https://freenetproject.org/fr/index.html)

7. PROTOCOLES EN LA DEEP WEB

7.1 LA RED TOR ENRUTAMIENTO TIPO CEBOLLA

Esta red es también denominada tipo cebolla (onion cebolla en inglés) por la forma en que opera para brindar anonimato al tráfico de red, en el cual, su técnica consiste en el encubrimiento por capas de la información para ocultar la comunicación desde el origen hasta su destino, por ello a esta técnica se le conoce como enrutamiento cebolla o por su nombre en inglés The Onion Router (TOR); funciona con los protocolos TCP y está compuesta por una red de servidores que funcionan como enrutadores que solo conocen los servidores anterior y siguiente en la conexión, sin la información de origen y destino[30]; el enrutamiento en esta red no es totalmente directo ya que la tecnología tipo cebolla se apoya en el uso de distintos nodos que se encuentran alrededor del mundo formando una red, ilustración 28.

Ilustración 28 conexión red Tor



Fuente: propiedad del autor

[30] ARREDONDO, Víctor y CARO, Roberto. “Aspectos técnicos de la red TOR”. {En línea}. {24 de noviembre de 2019}. Disponible en: (http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G19/Informe_TOR.pdf)

7.1.1 NODOS[31]

También llamados relays, son diversas máquinas que operan alrededor del mundo con la intención de permitir la conexión en la red, no todos tienen la misma función ni características similares, pero se pueden agrupar dependiendo del bloque de funciones que realizan[32]:

Nodos de entradas: Estos son el primer contacto entre el usuario o cliente y la red Tor, permite la conexión con la red y facilitan el acceso a ella.

Nodos medios[33]: Estos nodos solo tienen contacto con otros nodos de la red, ya que están configurados para que permanezcan en la red y solo retransmiten la información recibida dentro de la misma red y la pasen a otro nodo de la red, el tráfico de estos nodos, está limitada solo al perímetro de la red.

Nodos puente: Estos interconectan segmentos de red, pero con la característica de ser auxiliares secretos de los nodos medios, ya que los anteriores, por su servicio en la red tienden a ser públicos y visibles a proveedores de internet y organizaciones que pueden censurar dichas direcciones IP, estos son una especie de entrada secreta, para dificultar la censura.

Nodos de salida: En términos coloquiales son el extremo final de la conexión, estos reciben todas las solicitudes y las envían al host de la petición, reciben la respuesta y luego la envían a la red; una cualidad de la red Tor es que permite conectarse a la Clearnet sin problema, bueno estos nodos son quienes facilitan esta tarea de salir de la red con una petición del usuario, llegar al sitio y volver la petición a la red, pero esto tiene un riesgo ya que esta petición una vez fuera de la red puede ser tomada y analizada, lo que significa que estos nodos no son mantenidos por cualquier usuario sin conocimientos o sin la capacidad de resolver cualquier acción legal que surja como consecuencia de lo que transmite.

[31] CC-BY-NC. “Tipos de nodos”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://tor.derechosdigitales.org/torificate/p1.3/#:~:targetText=Nodos%20de%20puente%20(Bridge%20relays,registro%20p%C3%BAblico%20de%20nodos%20elegibles.)

[32] Tor soportes. “glosario de Tor”. {En línea}. {25 de noviembre de 2019}. Disponible en: https://support.torproject.org/es/misc/glossary/

[33] CC-BY-NC “Tipos de nodos”. {en línea}. {24 noviembre 2019} disponible en: https://tor.derechosdigitales.org/torificate/p1.3/

7.1.2 Protocolo TLS

Transport Layer Security (TLS)[34], este protocolo nace a partir de SSL, pero no es compatible con este; el objetivo principal es la privacidad en la conexión, integridad de los datos, la identificación y autenticación mediante certificados digitales. Permite el intercambio de datos mediante POP3, SSH, HTTP, SMTP y otros. El protocolo permite la identificación y autenticación entre las partes, con total confidencialidad mediante el establecimiento de claves secretas durante la comunicación. Además, proporciona lo siguiente:

- Cifrado mediante clave asimétrica.

- Los protocolos criptográficos deben ser acorde a los algoritmos de una conexión segura.

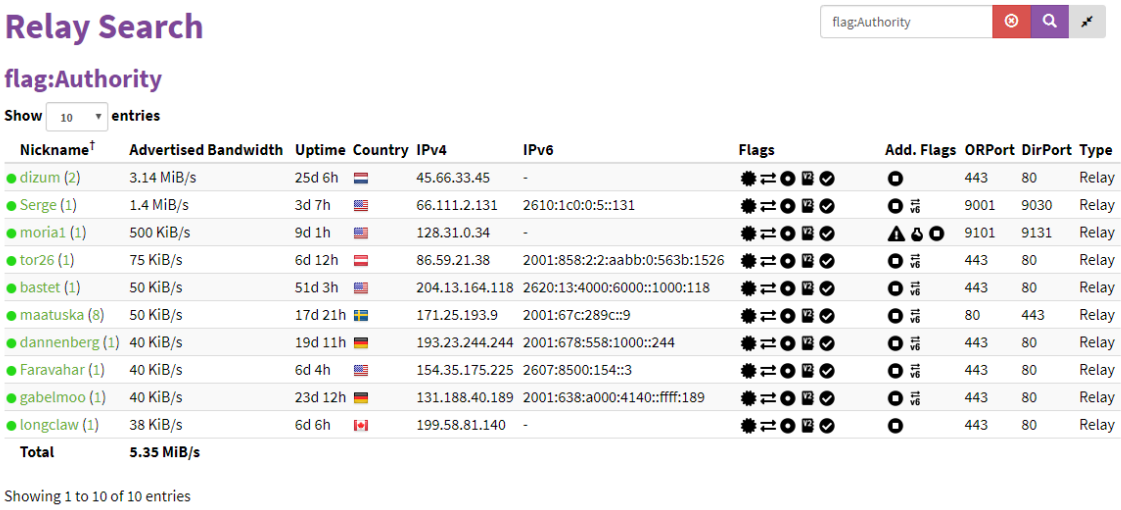
- Utiliza la suite de algoritmos CipherSuite que consta de algoritmo de intercambio y autenticación de claves, algoritmo de cifrado y algoritmo de código de autenticación de mensajes.

7.1.3 Autoridades de directorios

Estos son nodos especiales (y por ello es que se considera la red Tor como centralizada) que mantienen una lista de todos los nodos con los que cuenta la red, esto se da mediante una revisión general que se realiza una vez cada hora, para verificar que todos los repetidores estén funcionando. Al momento de escribir estas líneas hay 10 nodos especiales (ver ilustración 28 autoridades de directorios) que se publican y 7372 nodos de salida. El problema con esta información es que un gobierno u organización lo suficientemente grande podría intentar bloquear (para molestar a los usuarios) los nodos de salida, validando primero sus estados, eso sí tendría que procesar todo este listado de servidores.

[34] Redalia. “Que es el protocolo SSL/ TLS”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://www.redalia.es/ssl/protocolo-ssl/)

Ilustración 29. Autoridades de directorios



Relay Search

flag:Authority

flag:Authority

Show 10 entries

Nickname†	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
dizum (2)	3.14 MiB/s	25d 6h		45.66.33.45	-			443	80	Relay
Serge (1)	1.4 MiB/s	3d 7h		66.111.2.131	2610:1c0:0:5::131		v6	9001	9030	Relay
moria1 (1)	500 KiB/s	9d 1h		128.31.0.34	-			9101	9131	Relay
tor26 (1)	75 KiB/s	6d 12h		86.59.21.38	2001:858:2:2:aabb:0:563b:1526		v6	443	80	Relay
bastet (1)	50 KiB/s	51d 3h		204.13.164.118	2620:13:4000:6000::1000:118		v6	443	80	Relay
maatuska (8)	50 KiB/s	17d 21h		171.25.193.9	2001:67c:289c::9		v6	80	443	Relay
dannenberg (1)	40 KiB/s	19d 11h		193.23.244.244	2001:678:558:1000::244		v6	443	80	Relay
Faravahar (1)	40 KiB/s	6d 4h		154.35.175.225	2607:8500:154::3		v6	443	80	Relay
gabelmoo (1)	40 KiB/s	23d 12h		131.188.40.189	2001:638:a000:4140::ffff:189		v6	443	80	Relay
longclaw (1)	38 KiB/s	6d 6h		199.58.81.140	-			443	80	Relay
Total	**5.35 MiB/s**									

Showing 1 to 10 of 10 entries

Fuente: disponible en https://support.torproject.org/es/misc/glossary/

7.2 I2P UNA RED DISTRIBUIDA

Como se mencionaba al principio una red distribuida o descentralizada se caracteriza porque no existe un punto central de administración o un host que controle la totalidad de la red y por ende como su nombre lo indica hay un distribución de actividades por parte de distintos nodos para cada tarea, esto se traduce en que un daño puntual en la red no genera mayor impacto en la totalidad de la red, por ello su funcionamiento no se vería completamente afectado, en teoría habría una mejor gestión de riesgo y recuperación ante el daño. I2P[35] surge como una red que intenta mitigar la vulnerabilidad presente en la red Tor una de ella en el sentido estricto de su filosofía de centralización, especialmente en la administración de sus nodos. I2p cuenta con una base de datos distribuida que al igual que Tor maneja la información de router y nodos I2P e información de contactos o de destino, pero cada una firmada por cada propietario y almacenada y verificada por cada nodo donde es almacenado.

7.2.1 Como funciona I2P

[35] I2P. “Una breve introducción de cómo funciona I2P”. {En línea}. {25 de noviembre de 2019}.

Disponible en: (https://geti2p.net/es/docs/how/intro)

Esta red tiene similitudes a la red Tor, pero con ciertas mejoras pues se utiliza para establecer comunicación; cada aplicación (browser, cliente o navegador que en términos coloquiales podría usarse indistintamente para la conexión) crea un túnel de comunicación temporal con una sola vía de entrada y una de salida unidireccionalmente, durante la cual los clientes, realizan una consulta a la base de datos de la red llamada netDb, Para identificación de los clientes a conectarse y establecer cuál es el túnel de comunicación (entradas y salidas) para cada uno; vale resaltar que esto túneles son una secuencia de nodos que transportaran la información unidireccionalmente, estableciendo el camino más óptimo, esto se da primero en el cliente que inicia la conexión al cual se le asigna su nodo de salida y su nodo de entrada, así mismo al receptor se le establece un nodo de entrada y uno de salida sin que ninguno de estos se repitan, esto hace mucho más difícil el rastreo de paquetes, ya que la red asigna diferentes host para cada cliente.

7.2.2 Cifrado

Esta red utiliza dos algoritmos de cifrado que se van desarrollando en distintas capas de la red durante el viaje de la información, el primero de ellos es el algoritmo de criptografía asimétrica ELGamal[36] de 2048 bit y el segundo es AES 256, estos son usados para el cifrado de fin a fin, funcionando como una combinación de ambos llamada ELGamal/AES+Session Tags. En la capa más baja el Router inicia el cifrado del mensaje proveyendo una clave de sesión AES256 con ElGamal y añade la payload cifrada después del bloque cifrado, ElGamal. Junto al payload cifrado, la sección del cifrado AES contiene el tamaño de la carga, con el hash SHA256 del payload no cifrado, y con ello un número de etiquetas. Una vez hecho este procedimiento no es necesario repetirlo ya que, en vez de cifrar una nueva clave de sesión con ElGamal, simplemente elijen una de las etiquetas enviadas con anterioridad y se cifran con AES el payload de la misma manera que al principio, utilizando la clave de sesión usada con la etiqueta de la sesión. El Router está a la expectativa de recibir un mensaje cifrado, y sucedido esto comprueba los primeros 32 bytes para ver si coinciden con la etiqueta de sesión disponible, en caso afirmativo descifran el mensaje con AES, en caso contrario, descifran el primer bloque con ElGamal. Para evitar robos de paquetes las etiquetas de sesión están disponible solo una vez; las sesiones son unidireccionales y cuentan con administradores de claves de sesión separados para evitar la intrusión.

[36] GetI2P. “Cifrado ElGamal/AESSessionTag. {en línea}. {24 noviembre 2019} disponible en: https://geti2p.net/es/docs/how/elgamal-aes

7.2.3 Capas y protocolos I2P

Al igual que la Clearnet, la I2P utiliza el modelo OSI para comunicación, pero con muchas variaciones para robustecer la red y mantener su filosofía de anonimato y seguridad, mediante:

Capa de aplicación: Al igual que el modelo OSI esta capa tiene las aplicaciones y todas las herramientas para la interacción del usuario con el sistema.

Capa de cifrado ajo: En esta capa se da la comunicación entre la capa de aplicación y las siguientes, aquí es donde se cifran los mensajes y se permiten la entrega de estos. Los mensajes son cifrados y envueltos en otro mensaje estándar con información para su entrega.

Capa de túneles: En esta capa se establecen las instrucciones y comunicaciones en cada túnel, aquí solo pueden ser descifrados las instrucciones de entregas ya que con esta información se direccionan el mensaje al siguiente nodo.

Capa de transporte i2p: Este es el que brinda las conexiones cifradas entro los dos router, para ello utiliza dos protocolos para ello, que son NTCP y SSU, el primero mucho más ligero que el protocolo TCP y el segundo soportado por UDP facilita una capa de transporte segura para la conexión además permite la detección de servicios NAT, detección IP y detección de firewall.

Capa de transporte: Esta funciona como apoyo a la capa descrita anteriormente, tiene las mismas características que la capa que lleva el mismo nombre en el modelo OSI.

Capa IP: Esta provee conectividad entre las dos máquinas, ya que recibe y envía mensajes de las máquinas

7.2.4 Túneles

No se puede pasar por alto mencionar algo tan importante como es el concepto de túnel, ya que al ser definidos como los caminos formados por una secuencia de router que forman la conexión entre dos puntos, es un elemento central en la red se

le llama túnel, debido a que siendo la conexión entre las máquinas lo principal es el anonimato entre clientes.
Túnel de entrada: Es aquella conexión formada por un nodo que permite entrar los datos desde la red.

Túnel intermedio: Es el túnel que conecta los túneles de entrada y salida en la red facilitando la vía de comunicación entre estos.

Túnel de salida: Es un túnel formado por el nodo para sacar la información hacia la red.

7.2.5 Diferencia frente a Clearnet y la red Tor

Como se ha hecho referencia anteriormente, la Clearnet es la red de internet tal como la conocen la mayoría de las personas que navegan en ella, el termino se utiliza dado que ya se ha mencionado que hay otra red dentro de internet y se utilizan términos para diferencia a cada una, ambas redes tienen características que las hacen únicas y a pesar de que parece tener mucha afinidad con la filosofía de otras redes hay ciertas características que permiten diferenciar a la red I2P, se puede decir que pertenece a la Deep web y nace como una red independiente que buscaba tener las mismas cualidades de anonimato y libertar que la red Tor, las mismas o mejores finalidades que la web tradicional pero corrigiendo en sí misma la dificultades de la red Tor:

- Es una red totalmente distribuida.

- Utiliza varios túneles paralelos que la hace más resistente a fallos que Tor y la Clearnet.

- La tunelización de la conexión es unidireccional contrario a la direccionalidad de la red tradicional.

- Los túneles de comunicación no permanecen durante mucho tiempo lo que reduce drásticamente las posibilidades de un ataque al host.

- Utiliza TCP y UDP como tipo de transporte, pero impide la detección de paquetes, incluso usando snifer.

- Las aplicaciones peer to peer no tiene mayores problemas de compatibilidad en comparación con Tor.

7.3 Otras redes

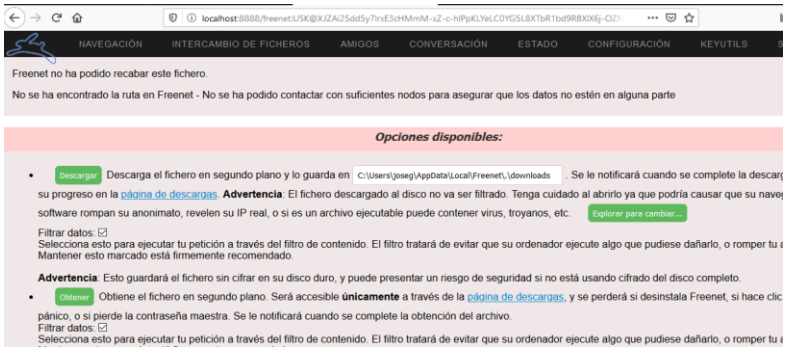
7.3.1 Freenet[37]

Esta es una red muchos más antigua que Tor o I2P, pero menos popular que ambas. Esta es una red totalmente descentralizada y según mi experiencia es más fácil de acceder que I2P y se caracteriza por ser más pequeña. Para sorpresa esta red no está conectada al resto de redes de internet, es decir es imposible navegar en ella e ir a solicitar algún servicio en la red Tor, el I2P o similares, lo que prácticamente la define como una VPN gigante; además de lo anterior, al iniciar en la red se solicita información de algún amigo (esto es alguna subred antes creada o algún host que les da acceso a su entorno; esto permite intuir que Freenet es una red peer to peer, en otras palabra está basada en la tecnología P2P[38]. algo muy importante a la hora de acceder aquí es que no se necesita servidor para centralizar servicios, pero tiene la debilidad de que, al bloquear un nodo, todo su contenido queda asilado del resto de la red.

Freenet permite crear subredes internas y que estando dentro de la red, no permite el acceso de otras redes u otros usuarios, en la cual solo se permite la comunicación entre sus miembros o se puede acceder a los contenidos solo si eres parte de la red. Una ventaja significativa para grupos terroristas y aquí es donde se supone que es imposible ingresar y que de alguna manera es erróneo, pero no tanto el hecho de que muchos hablan de niveles profundos en la Deep web haciendo referencia a que no se puede acceder a estos entornos, pero la verdad es que no hay linealidad en la navegación que permita describir esta parte de la red como algo profundo, más bien este se describiría como un compartimiento cerrado, cuyos habitantes permiten el acceso o no. No obstante, también hay Freenet que simplemente están disponible para todo público, por ejemplo, ilustración 30.

[37] The Freenet Project Inc. “FREENET”. {en línea}. {25 de noviembre 2019}. Disponible en: (https://freenetproject.org/)
[38] CASTRO, Luis. “Que es P2P y para qué sirve”. {En línea}. {25 de noviembre 2019}. Disponible en: (https://www.aboutespanol.com/que-son-los-programas-p2p-y-como-funcionan-157981)

Ilustración 30 Sitios Freenet



Fuente: propiedad del autor localhost:8888/freenet: USK@XJZAi25dd5y7lrxE3cHMmM-xZ

7.3.2 Resilio[39]

Esta es una red de uso privativo y su acceso no es libre como las anteriormente descritas, es una red descentralizada, pero con una interface de administración que realiza actividades de monitoreo. Utiliza un protocolo para el trabajo en redes mixtas llamado µTP2. La arquitectura de este protocolo facilita la transferencia masiva de información, los paquetes perdidos se retransmiten una vez por RTT para reducir retransmisiones innecesarias; además, maximiza las transferencias de datos independientemente de las condiciones de la red. Al estar enfocada al entorno corporativo, optimiza la conexión en centro de datos, operaciones remotas y la nube, así como también facilita la sincronización de carpetas y archivos grandes.

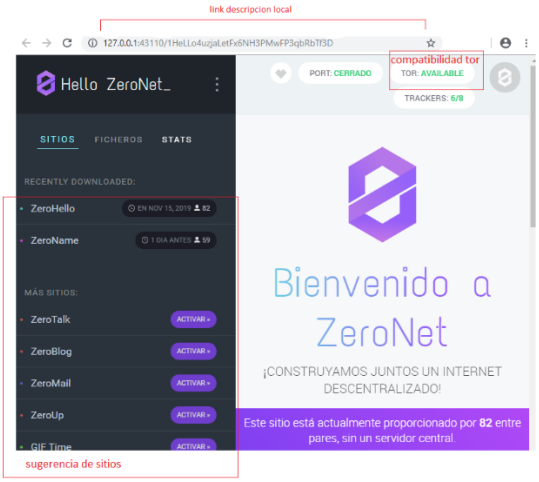
7.3.3 ZeroNet[40]

Es una red descentralizada de código abierto, por defecto no es una red anónima, pero, facilita el ocultamiento de las direcciones IP mediante la configuración en el navegador; para acceder a esta red solo se necesita descargar la aplicación dispuesta para ello en su sitio oficial. Los dominios terminan en BIT y no es necesario un servidor central, ya que el contenido se distribuye entre los visitantes de la red, lo que elimina la dependencia de empresas de alojamiento y la censura; debido a la forma de cómo opera la red todo el sitio se descarga en el equipo del

[39] Resilio Inc. “Resilio Connet”. {En línea}. {25 de noviembre de 2019} disponible en: (https://www.resilio.com/connect/)
[40] ZeroNet. “sitio abierto, gratis y sin censura, usando la criptografía Bitcoin y la red BitTorrent”. {En línea}. {25 noviembre de 2019}. Disponible en: https://zeronet.io/es

cliente haciéndolo funcionar como un servidor, lo que disminuye la necesidad de conexión a internet, Ilustración 31.

Ilustración 31. Página inicial ZeroNet



Fuente: propiedad del autor
127.0.0.1:43110/1HeLLo4uzjaLetFx6nh3pMwFP3qbRbTf3D

7.3.3.1 Qué ofrece zeroNet

Este es un lugar muy variado, más sencillo que Tor y un poco más amigable, pero con muchas más libertades que los sitios tradicionales a tal punto que se puede encontrar todo tipo de información y sitios con todo tipo de ofrecimientos:

Zerotalk[41]: Este es un foro de contenido muy variado, con una comunidad muy activa y dispuesta a compartir todo tipo de información, está disponible en más de 10 idiomas diferente y se pude acceder a los foros por temas creados o puedes crear uno.

Zerome[42]: Es una red social no tan activa como las tradicionales, Facebook o Twitter, pero mucho más anónima que estas, para ingresar se solicitan permisos de escritura y lectura para ver el contenido del sitio.

[41] Zeronet. “zerotalk”. {En línea}. {25 de noviembre de 2019}. Disponible en: (talk.zeronetwork.bit)
[42] ZeroNet. “Zerome”. {En línea}. {25 de noviembre de 2019}. Disponible en: (Zero/1MeFqFfFFGQfa1/3gjyYYUvb5Lksczq7nH)

Zerosites[43]: Este es una especie de directorio, útil para las personas que ingresan por primera vez, éste cuenta con un listado de muchos sitios populares, organizados por categorías, durante la ejecución se despliegan los sitios en diferentes idiomas.

YouTube: No es de extrañar que en esta red descentralizada también se encuentren los servicios de YouTube, claro está que en este lado de la red, no hay ningún tipo de restricciones similares a las que usualmente tiene el sitio en la Clearnet, es más por lo general las sugerencias ponen en primera lista, contenidos sexuales o películas con derechos de autor que usualmente bloquearían las grandes productoras, es de aclarar que para ver un canal, éste debe estar creado de este lado de la red, de lo contrario no podrás ver tus sitios favoritos, cabe anotar que realicé una prueba buscando un canal creado por mí y no lo conseguí, ya que en el YouTube de Zero net no existe.

Debo resaltar, que en Zeronet la navegación no es lineal, ni por capas, ni da la sensación de estar subiendo o bajando de nivel o llegando a ninguna superficie, lo particular es que al acceder a un sitio este se descarga en su totalidad al equipo para poder abrirse en el navegador.

7.3.4 Morphis[44]

Es un proyecto de código abierto diseñado para el intercambio de archivos cifrados basados en la filosofía P2P; esta tecnología es ejecutada en cada host, creando una red independiente que no necesita servidores centralizados, ni vigilancia alguna, ya que la idea es que haya una total libertad de expresión, sin restricción alguna y sin dominio de gobiernos o corporaciones. Hay 3 interfaces de usuario: la primera como una especie de capa de aplicación, es la primera vista al usuario que se puede ver través del navegador web, la siguiente es a través del cliente SSH para la conexión y, por último, la línea de comando Morphis UI. La red está optimizada para el mejor rendimiento y la baja latencia con la intención de que las aplicaciones se construyan para funcionamiento en la red puedan usar Morphis como base de datos[45]. A demás utiliza el protocolo TCP para ser compatible con la red Tor.

[43] Zerosites. {en línea}. {24 de noviembre de 2019}. Disponible en: (127.0.0.1)
[44] ELIZALDE, Inma. “Morphis o como modernizar los sistemas de las empresas”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://directortic.es/talleres-del-cio/morphis-modernizar-los-sistemas-las-empresas-2019050921182.htm)

[45] Mable. “Freenet y entropy, redes anónimas”. {en línea}. {25 noviembre 2019}. Disponible en: marblestation.com/? p=176

7.3.5 GnuNet[46]

Es una red descentralizada con cifrados y protocolos de red para crear aplicaciones seguras, distribuidas y que resguardan la privacidad. Esta red funciona como una red ubicada sobre la infraestructura de Internet existente, formando la base de una red híbrida punto a punto y una red troncal de retransmisión para que las aplicaciones se ejecuten[47]. No es complemente dependiente de la transmisión por la red de internet, ya que puede ejecutarse independientemente de ésta, a través de radio y cable dedicados. Utiliza claves públicas para las direcciones y algoritmos de enrutamiento descentralizados que reemplazan los protocolos TCP / IP. Cada subsistema se ejecuta como un proceso separado, ya que su arquitectura es multiproceso que proporciona aislamiento de fallas y permite otorgar permisos estrictos a cada subsistema. la implementación es un paquete GNU cuya aplicación es en teoría imposible de censurar.

7.3.6 Entropy[48]

Es muy similar a freenet pues al igual que esta es P2P y todas sus aplicaciones corren en ambas sin mayores complicaciones, algunas de sus diferencias es que entropy es escrito en c y es mucho más pequeña, además algunos de sus servicios no funcionan correctamente en la instalación de inicio. La interface funciona localmente con el puerto 9999, tiene incorporado un servidor POP3 que utiliza el puerto 10110, un servidor SMTP que utiliza el puerto 10025.

7.3.7 ANts P2P[49]

Es una red basado en un sistema de código abierto, soportado bajo licencia GNU[50]; es una red P2P que cifra todo el tráfico de la red mediante la combinación del algoritmo de cifrado AES 128 – DH 512, por otra parte, utiliza su propio protocolo de enrutamiento (ARA y MANET). Algunas de sus características son:

- Mensajería es completamente anónima.
- Posee varias rutas de enrutamiento.
- La red indexa documentos basado en palabras completas.
- El protocolo de enrutamiento es orientado a objetos.
- Permite la comunicación por cualquier proxy, servidor NAT, o HTTP.

[46] WayBack. “repositorios GNUnet git”. {En línea}. {24 de noviembre de 2019}. Disponible en: https://web.archive.org/web/20190418080225/https://git.gnunet.org/

[47] BibGnunet. “artículos seleccionados”. {en línea}. {27 noviembre 2019} disponible en: bib.gnunet.org

[48] Fanpage. “Deep Web”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://www.facebook.com/laDeepWeb/posts/otra-red-que-conforma-la-deep-weba-zentropy-entropy-fue-una-red-peer-to-peer-des/326126044187156/)

[49] Mino.”Ants P2P”. {En linea}. {25 de noviembre de 2019}. Disponible en: (https://sourceforge.net/projects/antsp2p/)

[50] ANts P2P. {En línea}. {25 de noviembre de 2019}. Disponible en: http://antsp2p.sourceforge.net/

- Es compatible con el protocolo de comunicación en tiempo real IRC.
- Sus links son compatibles con EDONKEY2000 (aunque en la actualidad este no tiene soporte).

8 SUGERENCIAS DE ALGUNAS HERRAMIENTAS DE UTILIDAD PARA EL ACCESO A SITIOS DE LA DEEP WEB

La red es muy amplia y para acceder a ella se necesitan de algunas aplicaciones y herramientas que faciliten la navegación, o permiten el acceso a estas, algunas son completamente sencillas de configurar y funcionan en diferentes plataformas mientras que otras requieren un poco más de conocimiento o dedicación para utilizarlas:

Tor browser: Es el navegador por excelencia de la red Tor, es muy fácil de instalar y permite el acceso a todos los sitios con dominios onion. A demás permite salir de esta red y navegar por sitios de la Clearnet, Freenet, entre otros.

Plugin I2P: Es un complemento que se utiliza en Mozilla para acceder a los sitios de la red I2P su utilidad es un poco compleja, ya que requiere de la configuración de servidores proxy, ancho de banda y demás configuraciones por consola, en ocasiones se requiere una VPN para que los proveedores no impidan el acceso.

Mozilla, Chrome, Edge: Aunque no lo creas, estos navegadores también tienen la posibilidad de ingresar a ciertas regiones de la Deep Web y a la totalidad de la red Tor; ¿cómo? Mediante el proyecto TOR2WEB, este permite que añadiendo la palabra .to, sw o sh y algunas otras, al final de la url en los navegadores, estos puedan direccionar las búsquedas enviando el tráfico a los nodos y las ruta a seguir para encontrar los servidores que alojan estos sitios. Por ejemplo, el sitio http://grrmailb3fxpjbwm.onion/ se convierte en http://grrmailb3fxpjbwm.onion.to o http://grrmailb3fxpjbwm.onion.sw. Todos ellos funcionan como un proxy

Freenet: Esta aplicación funciona como un complemento de cualquier navegador, para ingresar a Freenet, lo que se debe hacer es instalarla y el navegador por defecto abrirá un sitio inprivate con la página de bienvenida al sitio.

Bitcoin, Monero, Ethereum: En la Deep Web no se realizan transferencia a banco vigilado o entidades que se sometan a alguna jurisprudencia, por ello se necesitan monedas que se puedan almacenar sin restricción algunas, es por ello que las

monedas digitales cobran mucha relevancia en este sentido; ahora no todas las transferencias son ilegales, ni todo lo que se ofrece es ilegal, pero todo dinero que se tiene si se debe reportar a alguna entidad, pero no todos están dispuesto a mostrar su dinero, por ello la utilidad de esta monedas.

RECOMENDACIONES

Una vez concluido este trabajo se considera importante, seguir investigando, analizando y teniendo en cuenta lo siguiente:

- Al investigar en el área informática sobre un tema de redes, hay que ser cuidadosos con los “convencionalismos” ya que no siempre las cosas funcionan como normalmente creemos que son.
- Al intentar acceder a las redes no centralizadas procurar la utilización de sistemas operativos de alguna distribución de Linux, especialmente Ubuntu, red hat, Debian o sus derivados, ya que presentan muchas más compatibilidades que otros sistemas[51].
- Las conexiones de red en la Deep Web son más anónimas, pero en algunas como la red Tor, lo es mucho más cuando usas Proxy y un VPN, pero si la intención es una exploración básica, basta con utilizar Tor browser y evitar la ejecución de script y descargas de esos sitios.
- Por tener características distintas a las de una red usual, sus parámetros de accesos son completamente diferentes al de los normales, por ello se debe tener una ida de este tema.
- Cada red tiene su propia configuración, por ello es importante tener en cuenta que para acceder a cada una de ella los controles de seguridad varían, pero en general no se debe acceder a sitios sin antes una reseña de ellos.
- Las redes albergadas en ZeroNet tienen cierta similitud a los entornos Windows, por ello su navegación y controles muy parecidos.
- Es recomendable ingresar a estas redes en máquinas virtuales con instalaciones de distros de Linux para inhibir la ejecución de malware, y en caso de que se presente alguna dificultad, eliminarla sin que se afecte todo el pc.
- Los sitios de la red Tor no utilizan Cookies por ello no es necesario configurar ningún navegador para impedirlos.

[51] Gnunet. “gnunet”. {en línea}. {27 noviembre 2019} disponible en: gnunet.org/en/

CONCLUSIONES

El tema en cuestión, permiten establecer en forma lógica qué lo que todos llaman internet en realidad no es solo el conjunto de sitios disponibles al público en general, sino que además existen un grupo de sitios y diversas redes que se conectan como el caso de la red Tor e I2p, o simplemente existen paralelamente sin permitirse ningún tipo de contacto o acceso desde una a otras. Toda la red de internet si está conectada, pero hay algunos espacios de ellas que pueden funcionar independientemente como es el caso de GNUnet.

Con los resultados del trabajo se puede decir con exactitud que en la navegación por la red no existe la mínima sensación de ir bajando a ningún nivel, ya que esto conllevan a una práctica que permitiría conocer y dimensionar el espacio y la ubicación de la red o al menos el lugar de la Deep web desde donde se ubica el usuario, cosa que es casi imposible calcular y para lo cual no están diseñados ninguno de las redes expuesta, ya que su filosofía es la libertad y el anonimato, además el tráfico en estas redes no se puede capturar. Lo anterior se concluye no solo con opiniones personales sino en la experiencia de técnicas basadas en la exploración y conocimiento tecnológicos a partir del presente trabajo; cabe señalar que hay una parte sensacionalista del asunto, que empiezan a mezclarse con teorías conspirativas, rumores infundados y conclusiones solo por imaginaciones sin comprobar. Uno de los aspectos más importantes es que la informática es un área de conocimiento y de la que se puede entender que al estar a disposición del planeta, todos aquellos que tengan un vínculo con ella va ha aportar significativamente a esto, pero no significa que hará que la tendencia sea tan maligna como es el caso de la idea general que se vende de la Deep Web, incluso se hablan de nivel de acceso como si la analogía del iceberg apuntara a que al adentrarnos en la navegación nos encontraremos con algo mucho más oscuro que lo anterior cosa que se desmiente con la forma como opera el buscador Torch[52]. La diferencia más notoria es que los sitios de la Deep Web en su mayoría son un sub entorno de red que opera bajo otras reglas, configuraciones y protocolos que la internet no tiene y además en esta ultima el contenido está disponible con un clic, pero en la primera, simplemente no serán visibles a menos que se utilicen los mecanismos y herramientas adecuados para ellos y eso no significa que todo lo que se consiga sea maligno.

[52] Del que se habló capítulos anteriores pero su análisis en profundidad no es el objetivo del presente trabajo.

BIBLIOGRAFÍA

ADSLZONE.” Guía Deep web 2019: como es, como entrar, link y diferencias con la Dark net”. {en línea}. {25 noviembre 2019} disponible en: https://www.adslzone.net/como-se-hace/internet/guia-deep-web

AMARO LOPEZ, Jose A; CHAVEZ ACEVEZ Lazaro M. y VARELA NAVARRO, Alberto Varela. La Web Oculta y cómo los buscadores encuentran la información. Revista de tecnologia y sociedad. En: PAAKAT: Revista de Tecnologia y sociedad. Vol., No 7(agos-2014). 4-5.

ANts P2P. {En línea}. {25 de noviembre de 2019}. Disponible en: http://antsp2p.sourceforge.net/

ARREDONDO, Víctor y CARO, Roberto. “Aspectos técnicos de la red TOR”. {En línea}. {24 de noviembre de 2019}. Disponible en: (http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G19/Informe_TOR.pdf)

BibGnunet. “artículos seleccionados”. {en línea}. {27 noviembre 2019} disponible en: bib.gnunet.org

BMG. “Black Market Guns”. {En línea}. {25 de noviembre de 2019}. Disponible en: http://5xxqhn7qbtug7cag.onion.plus/

CAGIGA VILA, Ignacio. Deep Web: acceso, seguridad y análisis de tráfico. Madrid, 2017. 51p. Trabajo de grado (Ingenieria de tecnologia de telecomunicacion). Universida de cantabria. E.T.S de ingenieros industriales y de telecomunicaciones.

CASTRILLON MERIDA, K; TORRES HERNANDEZ, A y SANDOVAL CASTILLO, N. “Deep Web”. (2015).

CASTRO, Luis. “Que es P2P y para qué sirve”. {En línea}. {25 de noviembre 2019}. Disponible en: (https://www.aboutespanol.com/que-son-los-programas-p2p-y-como-funcionan-157981)

CC-BY-NC “Tipos de nodos”. {en línea}. {24 noviembre 2019} disponible en: https://tor.derechosdigitales.org/torificate/p1.3/

CC-BY-NC. “Tipos de nodos”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://tor.derechosdigitales.org/torificate/p1.3/#:~:targetText=Nodos%20de%20puente%20(Bridge%20relays,registro%20p%C3%BAblico%20de%20nodos%20elegibles.)

COST SANFELIU, Jordi. Un paseo por la Deep Web. {En linea}. 2019. {16 septiembre 2019}. Disponible en: (http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.8DD09846&lang=es&site=eds-live&scope=site)

EmpireMarket. {En línea}. {25 de noviembre de 2019}. disponible en: https://mqpawblcdfnwuyzv.onion.to/

ELIZALDE, Inma. “Morphis o como modernizar los sistemas de las empresas”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://directortic.es/talleres-del-cio/morphis-modernizar-los-sistemas-las-empresas-2019050921182.htm)

Fanpage. “Deep Web”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://www.facebook.com/laDeepWeb/posts/otra-red-que-conforma-la-deep-weba-zentropy-entropy-fue-una-red-peer-to-peer-des/326126044187156/)

Freenetproject.” Browse websites, post on forums, and publish files within Freenet with strong privacy protections.” {En línea}. {25 de noviembre de 2019}. Disponible en: (https://freenetproject.org/fr/index.html)

GARCIA, Víctor; CHINEA, Jorge. “Un paseo por la Deep Web”. Catalunya,2019. 12p. trabajo de grado Master seguridad del tic. Universidad Oberta de Catalunya.

GATELL, Antonio. “Como funciona una red distribuida” {En línea} 8 julio 2018 {13 octubre 2019}. Disponible en: (https://www.gatellasociados.com/como-funciona-una-red-distribuida/)

GetI2P. “Cifrado ElGamal/AESSessionTag. {en línea}. {24 noviembre 2019} disponible en: https://geti2p.net/es/docs/how/elgamal-aes

Gnunet. “gnunet”. {en línea}. {27 noviembre 2019} disponible en: gnunet.org/en/

I2P. “Una breve introducción de cómo funciona I2P”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://geti2p.net/es/docs/how/intro)

I2P. “que es I2P”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://geti2p.net/es/)

LAVIN PERRINO, Irene. Un paseo por la Deep Web, 2018, 51p. Trabajo fin de master (Master inteuniversitario en seguridad de las TIC- MISTIC. Universidad Oberta de Catalunya.

Lobo Romero, Mario. un paseo por la Deep Web. Catalunya 2018 p 20-22. Trabajo de grado. Universidad abierta de Catalunya

LOPEZ, P.; MARTIN, H. The World’s Technological Capacity to Store, Communicate, and Compute Information, {2011}. 1-4p

Mable. “Freenet y entropy, redes anónimas”. {en línea}. {25 noviembre 2019}. Disponible en: marblestation.com/? p=176

Mino.”Ants P2P”. {En linea}. {25 de noviembre de 2019}. Disponible en: (https://sourceforge.net/projects/antsp2p/)

MOORE, R. J. “¿Cuando datos se crean al dia en internet?” {En linea}.{08 de Febrero de 2011} disponible en: https://www.elmundo.es/elmundo/2011/02/08/navegante/1297179889.html

Morphis.” Morphis is one world”. {En línea}. {27 noviembre 2019}. Disponible en: https://morph.is/v0.8/#contact

NORTON, Peter. "introducción a la computación". 6ta.ed. McGraw. 2006. Hill, 65 páginas.

Not Evil. {en linea}. {24 de noviembre de 2019}. Disponible en: (hss3uro2hsxfogfq.onion)

OnionName. {En linea}. {24 de noviembre de 2019}. Disponible en: (http://onionname3jpufot.onion/)

OnionWallet. {En línea}. {25 de noviembre de 2019}. Disponible en: (http://ow24et3tetp6tvmk.onion/)

ORELLANA CRUZ, Julio. “Clasificacion de redes”. {En linea}. {17 de Abril de 2011}. Disponible en: (https://julioorellanacruz.wordpress.com/2011/04/17/clasificacion-de-redes/)

Redalia. “Que es el protocolo SSL/ TLS”. {En línea}. {25 de noviembre de 2019}. Disponible en: (https://www.redalia.es/ssl/protocolo-ssl/)

Resilio Inc. “Resilio Connet”. {En línea}. {25 de noviembre de 2019} disponible en: (https://www.resilio.com/connect/)

SETA, L. D. “Google alcanza el billon de paginas indexadas” {En linea}. {27 de Julio de 2008}. Disponible en: (https://dosideas.com/noticias/actualidad/146-google-alcanza-el-trillon-de-paginas-indexadas).

The Freenet Project Inc. “FREENET”. {en línea}. {25 de noviembre 2019}. Disponible en: (https://freenetproject.org/)

Torch. “Information for advertisers and users”. {en línea}. {18 noviembre 2019} disponible en: http://xmh57jrzrnw6insl.onion/adinfo.html

TorGuerrillaMail. {En línea}. {25 de noviembre de 2019}. Disponible en: (http://grrmailb3fxpjbwm.onion/)

Tor soportes. “glosario de Tor”. {En línea}. {25 de noviembre de 2019}. Disponible en: https://support.torproject.org/es/misc/glossary/

TorShop. {En linea}. {24 de noviembre de 2019}. Disponible en: (http://shopsat2dotfotbs.onion/)

Universidad politecnica de madrid. (s.f.). las siglas y otras abreviaciones en el campo informatico. madrid: centro virtual cervantes.

VILLADA, Diego y JIMÉNEZ, Andrés. La Web Semántica y la Web Profunda como Sistemas de Información: Análisis a una realidad. En: Revista Antioqueña de Las Ciencias Computacionales, No.7 p 43-51

WayBack. “repositorios GNUnet git”. {En línea}. {24 de noviembre de 2019}. Disponible en: https://web.archive.org/web/20190418080225/https://git.gnunet.org/

ZAVIA, Matías. “Kit de supervivencia en la Deep Web” {En línea} 2015. {12 octubre 2019}. Disponible en: (https://www.genbeta.com/a-fondo/kit-de-supervivencia-en-la-deep-web)

Zenithcc. {En línea}. {25 de noviembre de 2019}. Disponible en: (http://zenithccalwhzy26.onion/)

ZeroNet. “sitio abierto, gratis y sin censura, usando la criptografía Bitcoin y la red BitTorrent”. {En línea}. {25 noviembre de 2019}. Disponible en: https://zeronet.io/es

ZeroNet. “Zerome”. {En línea}. {25 de noviembre de 2019}. Disponible en: (Zero/1MeFqFfFFGQfa1/3gjyYYUvb5Lksczq7nH)

Zeronet. “zerotalk”. {En línea}. {25 de noviembre de 2019}. Disponible en: (talk.zeronetwork.bit)

Zerosites. {en línea}. {24 de noviembre de 2019}. Disponible en: (127.0.0.1)

Zerosites. {en línea}. {24 de noviembre de 2019}. Disponible en: (127.0.0.1)