

# Un Retrato de Darknet

Univ. Marleny Mollo Ala  
Universidad Mayor de San Andrés  
Carrera de Informática  
marleny\_270@hotmail.com

## RESUMEN

En este artículo, hablaremos de Darknet es una colección de redes y tecnologías donde lo más importante es compartir todo tipo información, aquí se trata de preservar el anonimato de quien origina la información y de quien la consume. Darknet no son redes físicas separadas de las redes de internet, son redes superpuestas que pueden usar protocolos y puertos "no estándar" sobre la red que todos conocemos. En esta red, los contenidos se mantienen inalcanzables para el usuario común de internet.

## Palabras clave

Redes superpuestas, algoritmos criptográficos, virtuales y hackers.

## 1. Introducción

El concepto de **red oscura**, también conocido por su nombre original en inglés **darknet**, ha ido evolucionando con el tiempo desde su definición original dada por unos investigadores de Microsoft. Actualmente el término Darknet no tiene una definición universalmente aceptada. Sin embargo, basándose en las versiones actuales más populares, se puede decir que la Darknet es una colección de redes y tecnologías usadas para compartir información y contenidos digitales (ej. textos, software, canciones, imágenes, películas) que está "distribuida" entre los distintos nodos y que trata de preservar el anonimato de las identidades de quienes intercambian dicha información, es decir, persiguen el anonimato del origen y el destino cuando se produce la transferencia de información. En la definición anterior, cuando se habla de redes, no se refiere a redes físicas separadas de las redes actuales sino a redes superpuestas que pueden usar protocolos y puertos "no estándar" sobre la red subyacente. Por eso se dice que estas redes operan aparte de las redes públicas sobre las que se montan y que sus contenidos se mantienen inalcanzables para el público general de la red subyacente (son **privadas**). Para acceder a la red y sus contenidos es necesaria cierta información adicional, la cual puede ser compartida por un grupo restringido de personas. Esa información suele incluir la necesidad de ejecución de un software específico y a veces es necesaria la conexión a algún tipo de servidor que no estará accesible vía los DNS tradicionales. Por esta dificultad de acceso los motores de búsqueda no suelen buscar en estas redes, permaneciendo sus contenidos invisibles. Por todos estos impedimentos

para acceder a la información a estas tecnologías se les llama *red oscura* o *Darknet*.

## 2. Marco teórico

El término **red oscura**, del inglés **Darknet**, fue acuñado en noviembre de 2002 en el documento "The Darknet and the Future of Content Distribution" escrito por cuatro investigadores de Microsoft: Peter Biddle, Paul England, Marcus Peinado y Bryan Willman. Este documento se publicó en un entorno post-Napster y antes de que se implantara masivamente Gnutella. En él se definen las Darknets como 'una colección de redes y tecnologías usadas para compartir contenido digital. Las Darknet no son una red física separada sino una aplicación y una capa de protocolo montada sobre las redes existentes(normalmente sobre Internet). Ejemplos de Darknets son redes peer-to-peer de compartición de archivos, copias de CD y DVD y claves o password compartidas mediante email y grupos de noticias'.

En este documento propone que el origen de las Darknets está basada en tres suposiciones:

Cualquier elemento compartido ampliamente distribuido está disponible a una fracción de usuarios en un formato que permite copiarlos.

Los usuarios copian objetos si esto es posible e interesante.

Los usuarios están conectados mediante canales de banda ancha.

La presencia de la Darknet es el obstáculo principal para el desarrollo de tecnologías de DRM ya que permiten que una vez que un objeto haya sido desprotegido (todos los sistemas de DRM tienen debilidades) y se obtenga una versión en ese estado, entonces esta puede ser accesible vía la Darknet. Además la información sobre cómo romper las tecnologías de DRM son distribuidas, a pesar de las leyes existente para que esto no ocurra, de forma muy eficiente, fácil y rápida pudiendo hacer uso de la propia Darknet.

Desde la propuesta inicial el término se ha ido filtrando a los medios de comunicación de masas y ha sido usado para referirse a tecnologías que se usan sobre Internet para dar soporte a actividades 'clandestinas'.

### 3. Darknet se ha separado en varios niveles que describo a continuación

**Nivel 1:** Web común – El más superficial de todos, dominando por un pequeño número de páginas que todos conocemos; aquí están sitios como Google, Youtube, el mundo Yahoo!, Wikipedia, Redes sociales y similares.

**Nivel 2:** Web Superficial – Aquí se encuentran webs un poco menos conocidas pero de fácil acceso, sitios web que han sido suprimidos de los motores de búsqueda, páginas de descarga de material considerado pirata así como foros con contenido y material explícito. Ejemplo de ellos son Taringa, Mega, canales como 4Chan, Dig, Reedit, servicios de email temporal entre otros.

**Nivel 3:** Este nivel ya es considerado la web profunda, son en su mayoría son sitios de descargas masivas, foros de activista de derechos humanos y perseguidos políticos, también páginas o servidores donde sus contenidos sobre pasan la legalidad, aquí puedes descargar software, videos explícitos completos, entre otros. Seguramente para muchos es muy común The Pirate Bay, Bitorrent y Emule.

En los **niveles 4, 5 y 6** los contenidos se salen de lo común, es donde darknet empieza a tornarse oscura. Aquí los nombres de dominios como google, facebook, youtube o loquedicen.com, no existen; en cambio estos nombres están compuesto por un sinnúmero de caracteres puestos al azar (<http://5onwnspjvuk7cvvvk.onion>), y no busques las terminaciones .com, .org o .net, porque todos los dominios termina en .onion.

**Nivel 4:** Servicios de hacking, pornografía infantil, venta de objetos robados y todo tipo de drogas.

**Nivel 5:** Lo más insignificante en este nivel, son páginas donde ofrecen sus servicios los asesinos o sicarios. Aquí hay un alto nivel de maldad es común el tráfico de cuerpos muertos y órganos, así como la venta de todo tipo de armamento.

**Nivel 6:** Este nivel se le conoce como “Islas Marianas”; se dice que, para el curioso, es un nivel muy peligroso y que si lo descubren entrando puede terminar muerto. Dicen que es el lugar de los hackers pagados por agencias gubernamentales y donde las agencias de inteligencia mueven información restringida. Se calcula que en este nivel se encuentra entre el 80% y 94% de la información total de internet.

### 4. Aplicación

Este tipo de tecnologías y redes tienen como objetivo permitir a sus participantes diseminar toda aquella información y contenido que deseen, creando una especie de 'zona de libre información' donde cualquier tipo de restricción legal carece de sentido porque es inaplicable debido a que no se puede identificar ni el origen ni destino de las transferencias de información, a veces no se sabe el contenido de la misma o incluso si ha habido algún tipo de transferencia de esta. Por tanto no es posible ninguna forma de vigilancia o control. El resultado es que estas redes se convierten en un foro con ilimitada libertad de expresión que puede ser

aprovechado para saltarse cualquier límite que se quiera imponer bajo coerción. Por ejemplo, se puede usar para: Difusión de conocimientos (Ej. científicos), opiniones (Ej. ideológicos o políticos), información, cultura y software prohibidos o censurados en distintos países, que no sería accesible de otra manera.

Difusión de pornografía infantil.

Difusión de informaciones aprovechable para el crimen organizado.

Violación de leyes de protección de la propiedad intelectual, en los países en los que esto es considerado delito.

Expresar rechazo o aceptación a cualquier tipo de idea política.

### 5. Desventajas

Los principales problemas que tienen este tipo de tecnologías para ser mucho más masivas son los siguientes:

Son muy ineficientes, dando la sensación de ser lentos comparados con otras herramientas que también permiten compartir información. Esto es debido a que, al perseguir el anonimato de las entidades, se obliga por un lado a usar algoritmos criptográficos (lo que requiere su tiempo de proceso) y por otro lado, el más importante, se requiere que los datos vayan de unos nodos a otros en lugar de ir directamente desde el origen al destino.

Tienen un número de usuarios bajo comparados con otras aplicaciones que también permiten compartir información. La gran diferencia en el número de usuarios puede hacer que cierta transferencia de información pase desapercibida, y por tanto no sea atacado el anonimato de sus interlocutores, en una transferencia de información en una red tradicional que en una red de Darknet. Por ejemplo Kazaa se estima que tiene 20 millones de usuarios y sin embargo Freenet tiene sobre 10000 usuarios.

Personas que no quieren que se les vincule con ciertas aficiones o ideas.

Usuarios que quieren comunicarse en un entorno de **total** libertad.

### 6. Conclusión

Darknet permanece invisible cada vez que te conectas, pero representa la mayor parte de los contenidos en la red: un mercado libre en el que todo está en venta y donde nadie deja rastro. Hemos querido conocer qué se cuece en este subterráneo virtual en el que el anonimato y el caos dibujan el retrato más oscuro de los internautas.

### 7. Bibliografía

- 1)file:///E:/%C2%A0/EI%20coraz%C3%B3n%20de%20las%20tiniéblas%202.0%20un%20retrato%20robo%20de%20la%20Deep%20Web.htm
- 2)file:///E:/%C2%A0/Darknet%20(with%20images)%200%C2%B7%20RaulGtz%20%C2%B7%20Storify.htm
- 3)file:///E:/%C2%A0/Darknet%20Wikipedia,%20la%20enciclopedia%20libre.htm

- 4)file:///E:/%C2%A0/Internet%20Profunda,%20un%20mundo%20oscuro%20y%20aislado.%20\_%20loquedic en.com.htm
- 5) J. Bethencourt "Establishing Darknet"