REDE
DE PESQUISA
EM GOVERNANÇA
DA INTERNET

Anais do Encontro Virtual da Rede de Pesquisa em Governança da Internet

Novembro de 2022

V ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - REDE 2022

FICHA TÉCNICA

ANAIS DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET - VOL. 5, ISSN 2675-1690

Editores
Diego Vicentin
Maria Vitoria Pereira de Jesus

Autores
Adriana Veloso
Cristina Carvalho
Hermann Bergmann
Javier de la Cruz Martínez
Julio Marinho
Maiara Stefany
Manuel Alberto
Mariana Gomes
Marina Gonçalves
Paula Guedes
Raimundo Miguel
Rebeca Souza

COMITÊ ORGANIZADOR

Núcleo de Coordenação da Rede de Pesquisa em Governança da Internet
Alexandre Arns Gonzales
Carolina Batista Israel
Diego Vicentin
Fernanda R. Rosa
Gustavo Ramos Rodrigues
Hemanuel Jhosé Alves Veras
Kimberly de Aguiar Anastácio
Maria Vitoria Pereira de Jesus
Nathan Paschoalini Ribeiro Batista

Comitê Científico
Carolina Batista Israel
Daniela Araújo
Diego Vicentin
Fernanda R. Rosa
Flávio Rech Wagner
Gills Vilar-Lopes
Jean Santos
Leonardo Ribeiro da Cruz
Maria Mónica Arroyo
Marta Mourão Kanashiro
Raquel Gatto
Rodolfo Avelino
Rosemary Segurado

Moderadores
Ana Claudia Farranha
Bianca Kremer
Carolina Batista Israel
Diego Vicentin
Fernanda R. Rosa
Flávio Rech Wagner
Jess Reia
Leonardo Ribeiro da Cruz
Marisa von Bulow

Debatedores
Adriana Veloso
Alessandra Ogassavara
Cristina Carvalho
Hermann Bergmann
Javier de la Cruz Martínez
Julio Marinho
Luis Henrique Antunes
Maiara Stefany
Manuel Alberto
Mariana Gomes
Marina Gonçalves
Paula Guedes
Raimundo Miguel
Rebeca Souza
Rosemary Segurado

O V Encontro da Rede de Pesquisa em Governança da Internet e a publicação dos Anais resultantes deste encontro receberam apoio de:

Internet Society - Capítulo Brasil

Programa de Pós-Graduação em Ciências Sociais do Instituto de Filosofia e Ciências Humanas (IFCH) da Universidade Estadual de Campinas (UNICAMP) por meio de recursos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - convênio n. 0524/2021.

Internet Society Capítulo Brasil

CAPES

ENCAPSULAMIENTO DE TRÁFICO DE TOR EN SISTEMAS MÓVILES LTE AUTÓNOMAS

Javier de la cruz Martínez

SUMÁRIO

DESCRIPCIÓN 5
Vigilancia en Internet 5
Evasión vigilancia en la red 6
Red Tor 6
Limitaciones y desventajas de conectividad 7
Software Libre 7
Anonimato 8
El software libre puede ser comercial 8
Migrando cabezas antes de equipos 9
Conectividad de Internet 9
Problemas de la brecha digital 10
Telefonía Celular Comunitaria en México 10
Cuarta Generación 4G 11
Estructura de una red 4G 11
Open5gs 11
CoLTE 11
Análisis de tráfico en Redes de computadoras 12
QUADROS, GRÁFICOS, FIGURAS 12
CONCLUSIONES 17
REFERENCIAS 18

ENCAPSULAMIENTO DE TRÁFICO DE TOR EN SISTEMAS MÓVILES LTE AUTÓNOMAS

Javier de la Cruz Martínez[1]

RESUMEN

Demostrar el funcionamiento de la conectividad de dispositivos móviles en redes LTE autónomas, así como de su valoración en el encapsulamiento del tráfico a través de la integración de la red Tor, como mecanismo de privacidad que es uno de los derechos humanos fundamentales y la evasión de la censura, como limitan otro de los derechos humanos fundamentales que es la libertad de expresión.

Se utilizó una metodología experimental, para lograr los objetivos y el autor integró varios componentes para poder demostrar su hipótesis.

El laboratorio que se implementó únicamente se enfocó al funcionamiento de datos móviles, es decir con él protocolo IP, sin enfocarse en las funcionalidades de llamadas y mensajería instantánea (SMS). Se realizaron análisis de tráfico desde la captura de datos a través de los componentes de red, tanto a nivel de red LTE como el intermediario a la conexión a internet.

PALABRAS CLAVE

Telecomunicaciones, Privacidad, Vigilancia, Anonimato, Autonomía tecnológica

ABSTRACT

Demostrated the connectivity of mobile devices in independent LTE networks and their positive performance in the encapsulation of traffic using the Tor network. This represents a mechanism for protecting the fundamental human right to privacy and avoiding censorship, the latter of which limits the human right to freedom of expression. The study applied an experimental methodology in which the author integrated multiple components to test the hypothesis.

The lab that was implemented worked only with mobile data (i.e., with the IP protocol), without considering calls or text messaging (SMS). An analysis of traffic was performed from the moment of data capture using the network components, both at the level of the LTE network and the intermediary internet connection.

[1] Maestro en Seguridad Informática, Universidad Internacional de la Rioja, México.

KEYWORDS
Telecomunnications, Privacy, Surveillance, Anonymity, Technological Autonomy

DESCRIPCIÓN

La metodología utilizada es de tipo experimental, con relación al tema y a que el autor integra varios componentes para poder demostrar su hipótesis, haciendo uso de al menos 2 dispositivos móviles (smartphone) uno conectado directamente a la red 4G, y al menos 5 dispositivos MiFi que tienen la función de convertir la señal 4G a un punto de acceso WiFi, probando con dispositivos (laptop, celulares) la conexión de los punto de acceso de los MiFi, corroborando el tráfico y la conexión a la red Tor.

El sistema 4G autónomo que se implementa únicamente habilita el funcionamiento de datos móviles, sin las funcionalidades de llamadas y mensajería instantánea (SMS).

Se realizan algunos análisis de tráfico desde la captura de datos a través de los componentes de red, tanto a nivel de red LTE como el intermediario a la conexión a internet, es decir, mediante la conexión del router de red.

Vigilancia en Internet

Con el transcurso de los años, la tecnología ha dado grandes avances para la humanidad, parte principal para la mejora de la vida de los seres humanos, este trabajo de investigación se realiza a mediados del 2022, después de las oleadas de una pandemia que ha dejado una cifra elevada de muertes a nivel mundial, una de las tecnologías importantes han sido el desarrollo y la creación de las vacunas que entre las mismas personas expertas han sido de las más rápidas en su creación, muchos países vivieron confinamientos estrictos algunos moderados y otros sin afectaciones de movilidad.

Ésta pandemia ha sido uno de los hechos históricos en el cual el uso de la tecnología se disparó a nivel mundial, así como el cierre de fábricas por brotes como me medidas de detención de la enfermedad (GONZÁLEZ, 2021), incrementaron el número de empresas con trabajo desde casa (en países/ciudades en donde las personas trabajadoras tuvieran la posibilidad de hacerlo), ante la pandemia una de las medidas de muchos países fue la creación de aplicaciones para la “prevención” de brotes en zonas y regiones de diversos países, pero a su vez aprovecharse de las herramienta tecnológicas con dicha finalidad (NEHRING, 2020), previo a la pandemia de la COVID

19, existieron, y siguen vigentes evidencias de vigilancia masiva a través de la red de redes como se le conoce a “internet”.

Internet se ha transformado prácticamente en una fuerza incontrolable en materia de libertad de expresión, ofreciendo al anonimato como una regla para burlar la censura y resguardarse ante las persecuciones.

Evasión vigilancia en la red

Al igual que la tecnología va avanzando y los mecanismos de control, existen grupos de personas y organizaciones que se dedican a mantener internet más libre, lo cual conlleva evitar la censura y la vigilancia, herramientas como VPN’s, plataformas como Tor, los mecanismos de cifrado, que mantienen la información de nuestra información de manera privada, algunos hasta cierto nivel.

Red Tor

Tor cuenta con una cantidad de servidores que se les consideran “nodos” alrededor del mundo, no todos los nodos pueden ser implementados con facilidad por temas legales, como son los nodos de salida debido a los riesgos que implican. (Tor Project, s/fd)

Tor hace uso de cifrado de flujos, cifrado a través de claves públicas, así como de funciones hash y el mismo protocolo Diffie-Hellman, en su documentación explican que algunos cifrados ya quedan obsoletos para nuevos usos.

En cuestión de cifrados de flujo utilizan el AES de 128 bits en modo de contador, además suelen requerir AES 256, para cifrados con claves públicas utiliza RS 1024 bits con exponentes fijo de 65537, Para temas de relleno OAEP-MGF1 con SHA-1 para funciones de resumen. Además, en algunos lugares se hace uso del grupo Curve25519 y firmas en formato Ed25519, así como SHA256 y Sha3-256.

Como describen en la documentación de sus especificaciones Tor es una red de superposición que opera de manera distribuida y está diseñada para anonimizar aplicaciones que basan su conexión en el protocolo TCP de baja latencia como son la navegación web, Shell segura y mensajería instantánea. (Tor Project, s/f-c)

Cada cliente elige una ruta por medio de la red interna de Tor, la cual construyen lo que denominan un “circuito” por el que cada nodo dentro de la ruta de navegación conoce a su predecesor y el sucesor, pero no a otros nodos dentro del mismo circuito.

Este tráfico fluye a través del circuito enviándose en “celdas” que son de un tamaño establecido, que va comunicándose a través de una clave simétrica en cada nodo, a continuación, se describen los tipos de nodos dentro de un circuito.

Existen tres tipos de nodos:

• Un nodo de entrada (Guard relays) se comunica sólo con el cliente

• un nodo medio (Middle relays) se comunica solo con otros nodos de la red Tor

• Y el nodo de salida (Exit relays) es el punto final dentro de la red Tor, toman las solicitudes, las envían a los destinatarios, reciben respuestas y las envían de vuelta a la red para que llegue a quien hizo la solicitud originalmente. (Derechos Digitales, 2022)

Limitaciones y desventajas de conectividad

Una de las principales limitaciones al utilizar la conexión a internet ya sea través de una VPN o por la red Tor, será la velocidad de conexión, en el caso de una VPN (dependiendo del proveedor) puede elegir a que servidor puede conectarse (nordvpn, 2018) algunos proveedores tienen servidores en distintos puntos alrededor del mundo, con mejores velocidades, otros están limitados por servidores en pocos lugares pueden llegar a saturarse y limitar la velocidad de conexión.

La velocidad de conexión en una conexión por Tor puede verse afectada, a diferencia de una VPN, Tor realiza la conexión a través de cifrado de tráfico dentro de su red interna.

Lo que permite a que el tráfico de la red sea casi indescifrable, ni se conozca el origen de que dirección ni las características del equipo que realizó la solicitud, pero con una velocidad de conexión menor.

Software Libre

En su plataforma de información de la Free Software Foundation -Software libre- lo defino como el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, es una cuestión de libertad, no de precio.

En tal caso el de software libre promueve las acciones de un movimiento que respetan las libertadas de las personas usuarias, teniendo como base las siguientes libertades, en caso de que una libertad no se cumpla, un software deja de ser libre

Anonimato

La palabra anonimato proviene de la palabra anónimo del griego annonymus la letra “a” significa sin y “nnonymus” significa nombre. Por lo tanto, el significado etimológico de la palabra es “sin nombre”. Por lo que la Real Academia Española considera que anónimos son los autores en el cual los nombre se desconoce o “secreto del autor que oculta su nombre”. Diego Fernando define al anonimato a la acción que realiza una persona ocultando su identidad o bien a la actuación de una persona desconocida para los autores. Así mismo menciona que más allá de todo, la acción anónima es una elección entre quienes deciden legitimar su privacidad, por vergüenza, o por la misma seguridad personal que puede llevar a que se tomen represalias en diferentes niveles con quien se expresa. En este sentido la asociación del anonimato, la tecnología y los fines honestos y trasparentes han logrado un avance significativo en la lucha por la libertad de los pueblos oprimidos, pero que es solo una apreciación, por lo que se debe de analizar el contexto, las situaciones y los fines de tales acciones. Obviamente siempre que esa asociación no constituya delito (MILOIORISI, 2016, p. 10).

Por otro lado, es sabido que el mundo criminal tiene una especial e histórica preferencia en el proceder anónimo, ya que se genera el efecto “terror” al presentarse como un enemigo o grupo oculto en búsqueda de impunidad.

Además, otra de las formas en que actúa la delincuencia es el denominado anonimato inducido, es decir, la víctima tiene una clara percepción del posible autor. Por lo que puede decirse que el anonimato es una ventaja para los criminales.

Pero también el anonimato es utilizado para fortalecer la libertad de expresión y protegerse de las persecuciones políticas e ideológicas por parte de grupos, gobiernos, personas o empresas.

El software libre puede ser comercial

Software libre no significa **no comercial**. Por el contrario, un programa libre debe estar disponible para el uso comercial, la programación comercial y la distribución comercial. Esto es de fundamental importancia, sin ello el software libre no podría alcanzar sus objetivos.

Migrando cabezas antes de equipos

Como lo ha comentado Javier Obregón quien se considera un militante del software libre, forma parte del desarrollo de algunas distribuciones GNU/Linux entre ellas EtherTICs distribución destinada a Radios Comunitarias y como fue expresado en secciones anteriores, el software libre no es un asunto técnico, sino un asunto ético, esto quiere decir de que a pesar de que exprese un tema tecnológico pero el tema principal es cambiar la perspectiva de la visión de las personas a que el software libre debe de primero comprenderse el porqué de su origen, para que las personas se interesen a migrar desde una perspectiva ético-social, y posteriormente a lo tecnológico (OBREGÓN, 2017).

Con experiencia en temas de software libre, se conocen mucho los beneficios de utilizar herramientas, sistemas y distribuciones libres, así como de código abierto, que nos gustaría migrar a todo el mundo para mejorar la experiencia, pero vivimos en una realidad en la cual se nos es más fácil seguir botones con la frase de “Siguiente”, a diferencia de la curva de aprendizaje que se requiere para poder operar sistemas y programas que sean de software libre o de código abierto, esto ha creado comunidades alrededor del mundo que generan y comparten conocimiento para mejorar y simplificar la puesta en marcha, pero lo principal es un acto de toma de decisión política a un cambio tecnológico.

Conectividad de Internet

De acuerdo en su artículo Mantenlo análogo: parámetros para una exclusión voluntaria de la conectividad Peter Bloom y Karla Prudencio mencionan que un porcentaje menor al 50% de la población mundial se encuentra desconectada a Internet, en la región Latinoamericana la cifra apenas alcanza al 30%, a partir de la pandemia de la COVID-19 se vio la necesidad de estar conectados a internet con mayor rapidez, algunos países requerían conexión a internet para poder obtener registros para los sistemas de vacunación, en donde gran cantidad de la población no conectada fueron quienes sufrieron al no poder vacunarse (PRUDENCIO; & BLOOM, 2021).

De la misma manera se vivió en el área de la educación en donde los estudiantes aproximadamente el 72% no pudieron acceder a educación a distancia, ya que tres cuartas partes de los escolares sin acceso viven en zonas rurales, como lo describe el artículo de la ONU (UNICEF, 2020).

Problemas de la brecha digital

Según Prudencio y Bloom (2021) parte del problema de la brecha digital responde a múltiples factores, pero los principales son cuatro: la falta de disponibilidad de servicios, los costos elevados del acceso, carencia de habilidades digitales y que el internet no ofrece contenidos de interés para las personas que continúan desconectadas. De acuerdo a los informes del Banco Mundial la expansión continúa siendo lenta entre un 2-3% (Unión Internacional de Telecomunicaciones, 2022) .

Telefonía Celular Comunitaria en México

En el Manual De Telefonía Celular describe que es un modelo que tiene como bases las Recomendaciones de Política Pública para el desarrollo de Tecnologías de la Información y Comunicación (TICs) para Comunidades Rurales e Indígenas de la ITU.

El modelo que presenta la organización sin fines de lucro Telecomunicaciones Indígenas Comunitarias A.C. está basado en una red local, que la propia comunidad opera y administra con el acompañamiento de una asociación cooperativa de la que ellas forman parte, actualmente el proyecto cuenta con servicios de tecnología 2G.

El sistema opera con llamadas locales y SMS gratuitos, para llamadas nacionales requieren de la conexión a internet para su funcionamiento, para ello otra parte importante es el servicio de Voz por IP (VoIP), que conecta las llamadas a la red global de voz.

Este esquema ayuda a disminuir los costos, además beneficia a las comunidades, esto permitiendo a que parte de los ingresos un porcentaje mayor se quede en la comunidad, el autor ha formado parte del proyecto desde el 2015 por lo que aporta los siguientes puntos. Por el pago de $42 pesos Mexicanos (aprox 2USD – dependiendo del valor de la moneda) de cada persona usuario, aproximadamente 2% se mantiene en un fondo de emergencia que las comunidades tienen que formar parte de ello, debido a que si algún desperfecto o problema de cuestión climatológica que afecte a los equipos, parte del fondo es utilizado para solucionar y que la comunidad no desembolse la cantidad por completo, aproximadamente el 36% se destina a la asociación que da acompañamiento continuo como lo son soporte técnico remoto, legal y social, el 62% se queda para la comunidad que debe asumir gastos operativos básicos (HUERTA; VELÁZQUEZ, 2016).

Cuarta Generación 4G

De acuerdo al artículo publicado por (ORTEGA, 2010, p. 4-6) para la revista de ciencia y tecnología INGENIUS esta generación está soportada por el estándar 3GPP, que basa su sistema con el protocolo IP. Tiene la posibilidad de dar velocidades de hasta 100Mbps a personas usuarias en movimiento y 1Gbps a personas en reposo. A diferencia de las generaciones anteriores la cuarta generación fue desarrollada con la característica de ser eficiente haciendo uso adecuado en temas de energía.

Parte de sus objetivos principales es la mejora del uso del espectro, la reducción de los costos, mejora de los servicios y la integración con estándares abierto.

La velocidad tiene una tasa de transferencia de datos con picos de 100Mbs para enlace de bajada (Downlink) y hasta 50 Mbps en enlaces de subida (Uplink).

Estructura de una red 4G

La arquitectura de una red de sistema LTE se conoce como System Architecture Evolution SAE a continuación se presentan alguno de los componentes principales

SOFTWARE PARA IMPLEMENTACIÓN DE REDES 4G AUTÓNOMAS

Open5gs

Es el programa que permite la implementación de redes privadas NR(5G) o LTE (4G).

Open5gs implementa 5GC (5G) y EPC (4G) haciendo uso de lenguaje C, además proporciona una interfaz de usuario Web para fines de prueba, a través del uso de Node.JS y React (Information and Communication Technology for Development (ICTD) Lab, 2022b).

CoLTE

CoLTE es el acrónimo de Community LTE Project que en español es Proyecto LTE Comunitario. Este software fue diseñado como una herramienta que integra las funciones elementales para la configuración de una red celular LTE de escala pequeña que es administrada de manera local (Information and Communication Technology for Development (ICTD) Lab, 2022b).

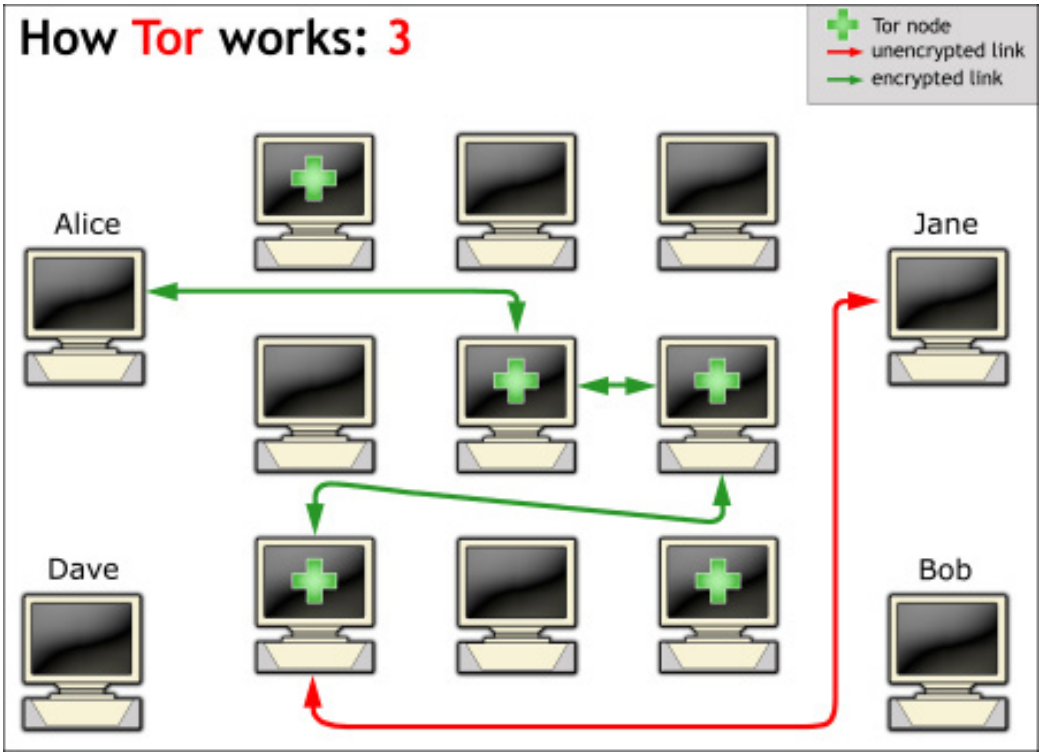
Análisis de tráfico en Redes de computadoras

Como describe el documento de Análisis de tráfico con Wireshark del INCIBE (MERINO; FEBRERO, 2011, p. 4) en el informe de Análisis de tráfico con Wireshark, el análisis de tráfico es de gran ayuda para el monitoreo de las redes, que a su vez sirven para detectar fallas en las mismas y resolver malas configuraciones.

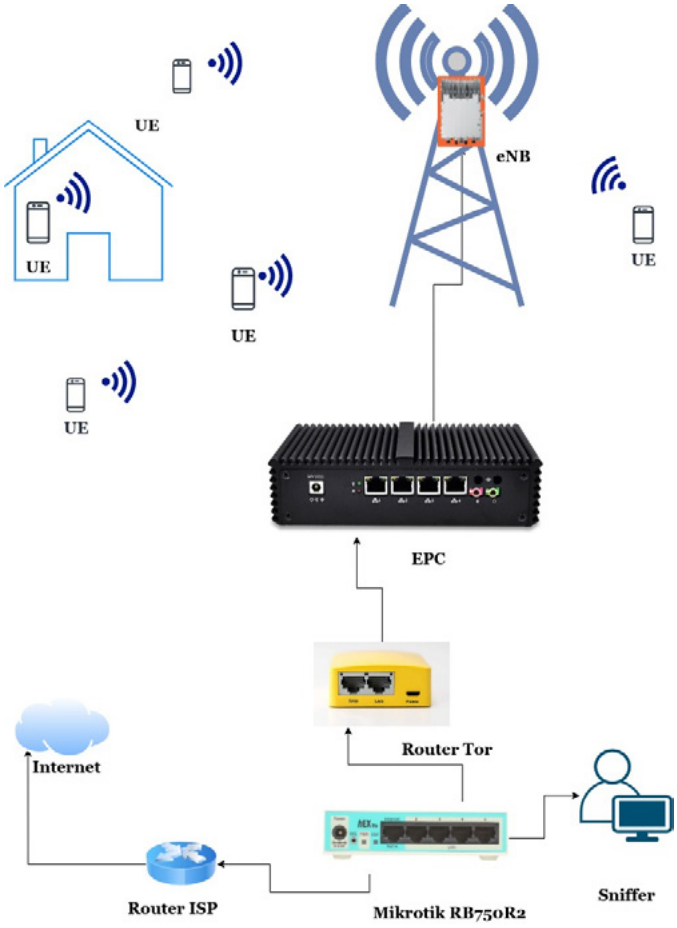
Pero también el análisis de tráfico tiene una faceta distinta como menciona (BOTERO; CABRERA, 2018) en donde la agencia de inteligencia de Estados Unidos de América la NSA, ha interceptado las comunicaciones en su país copiando tanto contenido como los metadatos de todo lo que transita en sus redes.

QUADROS, GRÁFICOS, FIGURAS

Gráfica del funcionamiento de la red Tor

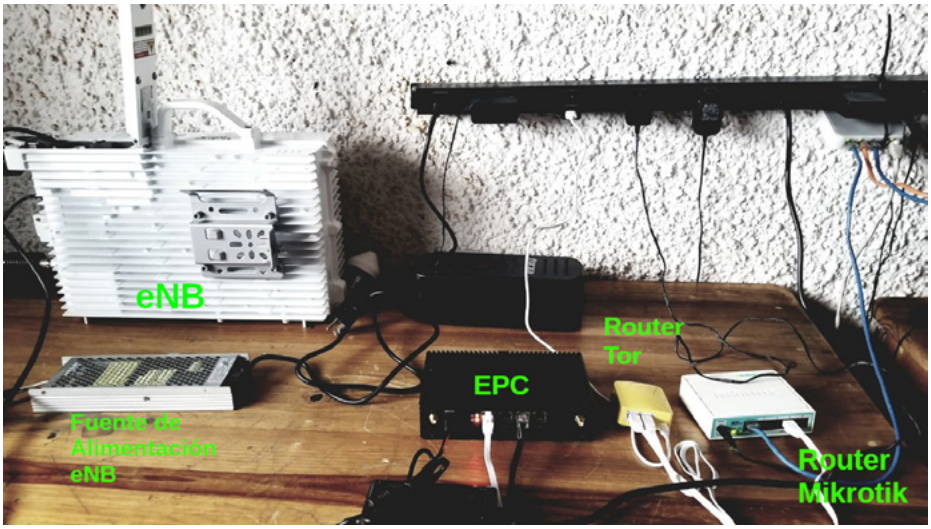


En la imagen que a continuación se presenta se puede ver las conexiones físicas de los dispositivos utilizados en las pruebas realizadas, el eNB utilizado es para exteriores.



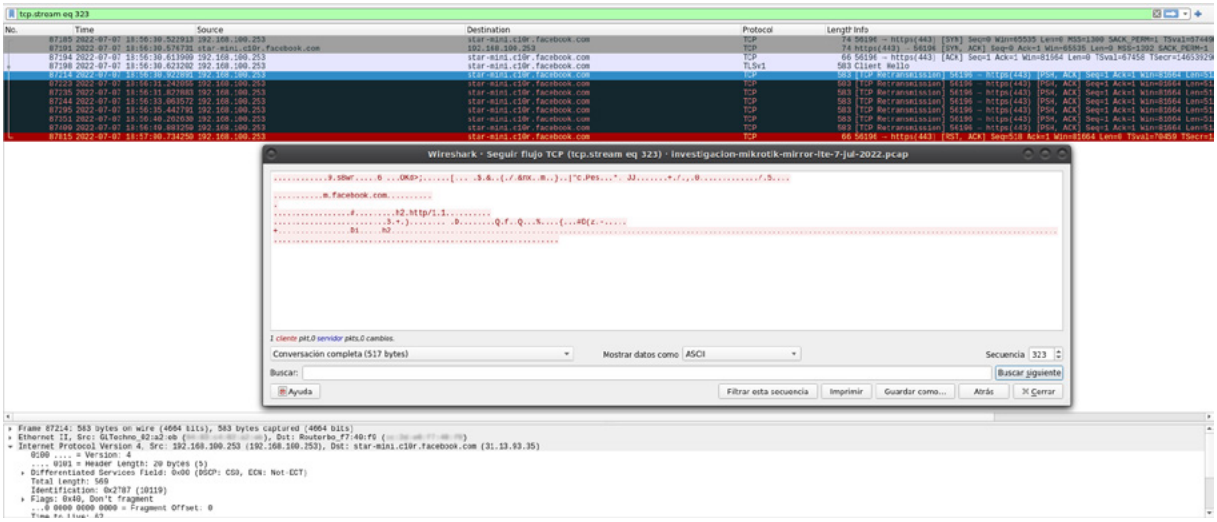
A continuación, se presenta el entorno de pruebas com los dispositivos que fueron utilizados para las pruebas

Esta implementación en un sitio en producción debe de contar con un sistema de protección de variación de voltaje, así como de aterrizaje, para evitar posibles daños a los dispositivos en el lugar, contemplar cableado de radiofrecuencia (RF) con las medidas adecuadas para su instalación.

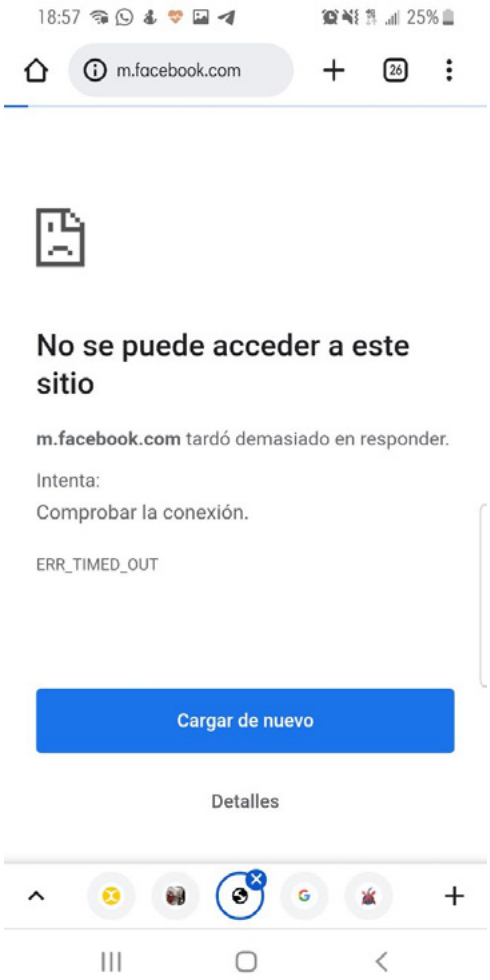


En la siguiente imagen se muestran 5 dispositivos MiFi y 1 smartphone que fueron utilizados para las pruebas.

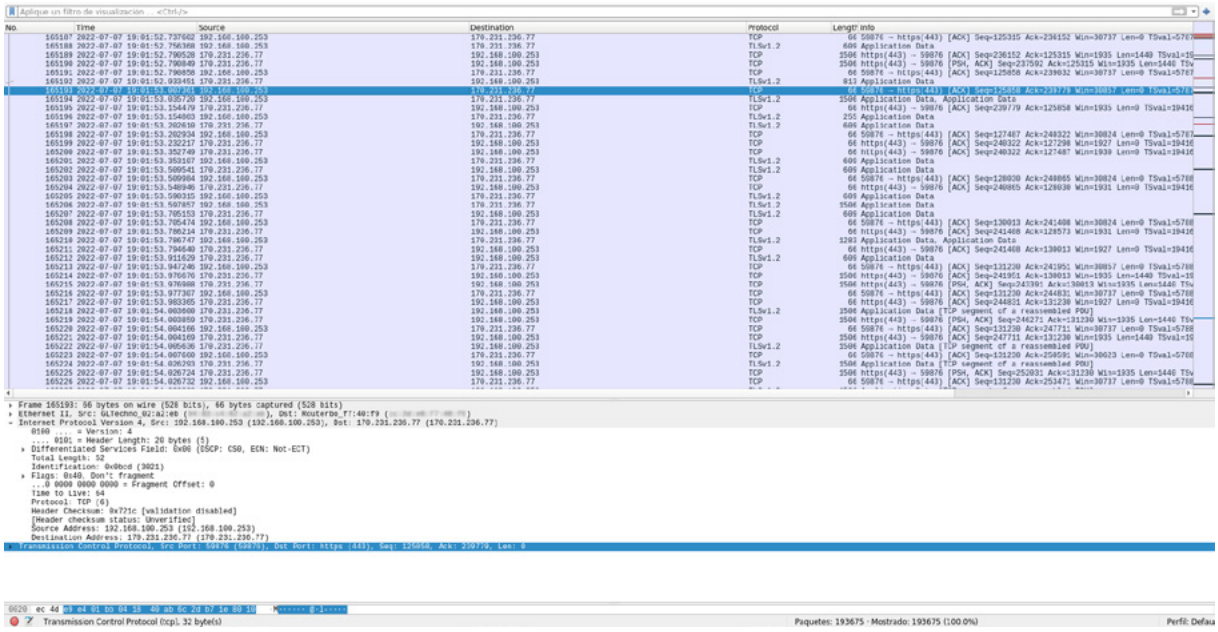
La siguiente ilustración presenta el análisis de tráfico, ante un bloqueo de dominio que en este caso es la red social Facebook, puede ser utilizado cualquier dominio.



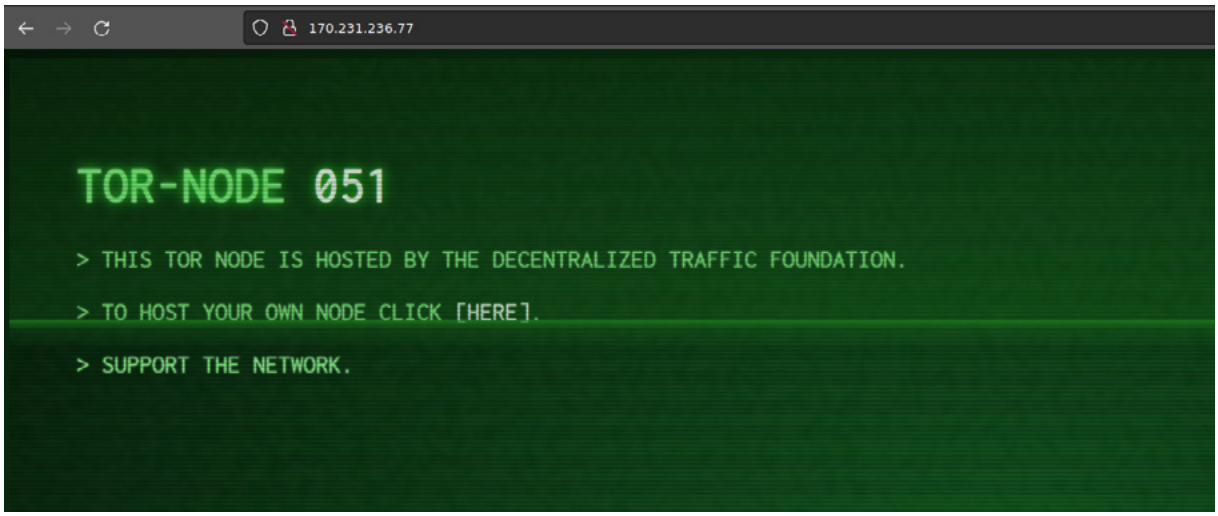
A continuación se tiene la vista desde el dispositivo móvil, para verificar que el bloqueo se haya realizado de manera exitosa.



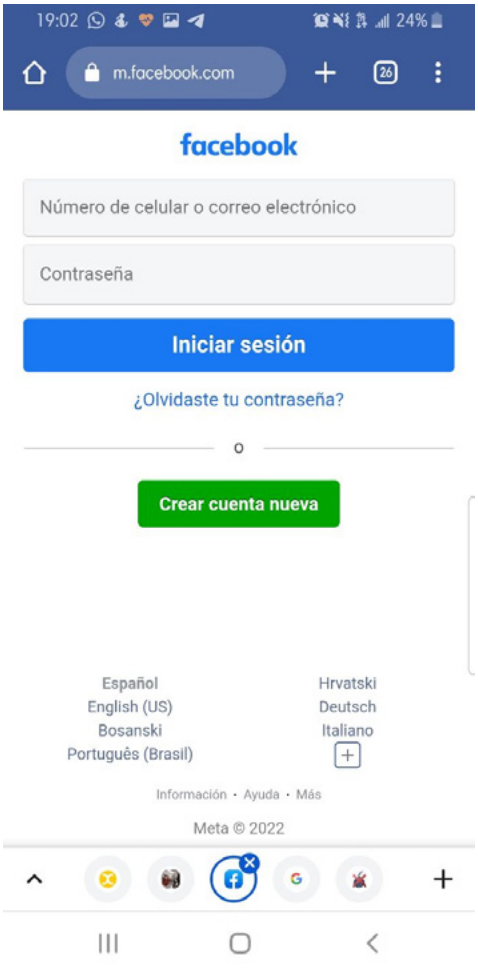
En la ilustración siguiente se muestra el tráfico una vez activado el servicio de la red Tor en el router utilizado, con el firmware previamente cargado para funcionar bajo la red Tor.



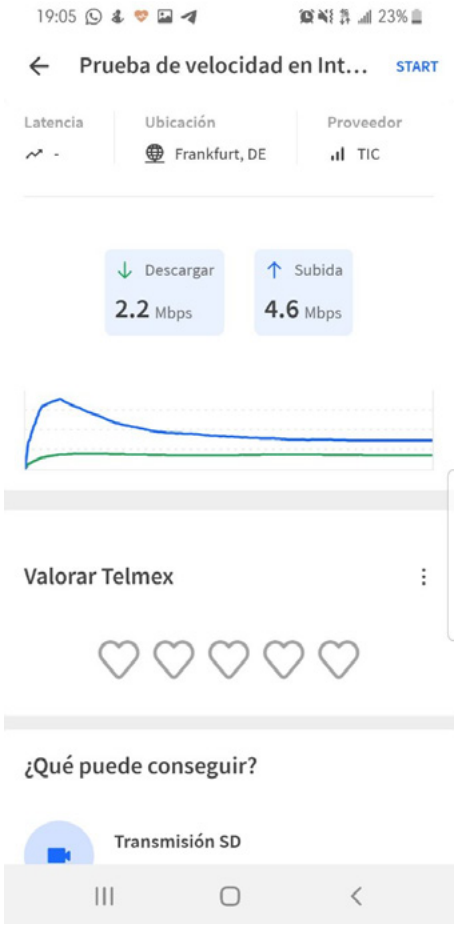
Se realiza la verificación de la dirección que se aprecia em el análisis de tráfico de la red, obteniendo la IP 170.231.236.77, que efectivamente nos muetra que es un nodo de Tor.



Se accede nuevamente desde el smartphone al dominio bloqueado, para verificar la evasión del bloqueo.



Teniendo una conexión de 30 Mbps de Descarga y 10 Mbps de Subida, al realizar una prueba de velocidad con el smartphone y la red Tor activa, la velocidad baja considerablemente.



CONCLUSIONES

Esta investigación se realizó con base a una metodología experimental en la cual se demostró el funcionamiento de la conectividad de dispositivos móviles en redes LTE autónomas a través de las pruebas de laboratorio, haciendo uso de varios dispositivos, que algunos por la banda de frecuencia utilizado para la implementación de la red LTE autónoma, de la cual no todos los dispositivos celulares fueron compatibles para la detección de la red, esto debido a que la frecuencia utilizada no es común en el país.

Se valoró el funcionamiento del encapsulamiento del tráfico a través de la integración de la red Tor, como intermediaria entre la red LTE y el proveedor de internet, permitiendo la privacidad del tráfico de las personas usuarias conectadas a dicha red LTE, logrando visualizar que el tráfico que se envía al proveedor del servicio de inter-

net o cualquier entidad intermediaria hacía el exterior, no pueda observar el tráfico real generado por las personas usuarias de la red LTE.

Además, se determinó a través de pruebas de tráfico y evidencias con dispositivos conectados que se logró la evasión de bloque (censura) a dominios que previamente fueron bloqueados para simular un bloqueo para acceder a plataformas, lo más difícil en la comprobación de la investigación es la adquisición de un dispositivo que logre generar una señal de radiofrecuencia, como lo es un eNB.

No se observaron limitaciones de uso de la tasa de transferencia de los dispositivos conectados a pesar de la cantidad de velocidad de navegación que ofrece una conexión mediante la red Tor, esto por la cantidad de dispositivos conectados, y la mínima cantidad de tráfico generado, a pesar de ancho de banda ofrecido por el proveedor de internet, al utilizar la red Tor, no se logró tener más de 7Mbps de Descarga y Subida, esto es variable de acuerdo al circuito que se conecte el cliente.

Al ser una red autónoma, la comunidad/entidad/organismo que esté a cargo del servicio puede operar el servicio bajo las normas que decidan, la cual se recomendaría seguir principios éticos y que sigan un modelo de gobernanza neutral que no afecte a las personas usuarias.

REFERENCIAS

BOTERO CABRERA, Carolina. **La vigilancia masiva viola los derechos humanos**. elespectador.com. Disponible en: https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-vigilancia-masiva-viola-derechos-humanos-column-814883/. 28 sep, 2018.

DERECHOS DIGITALES. 3: Tipos de nodos - Torifícate. (s/f). Disponible en: https://tor.derechosdigitales.org/torificate//p1.3/ Accedido el 15 de junio, 2022

GONZÁLEZ, Alejandro. **Escasez de chips, una consecuencia de la pandemia de COVID-19**. Disponible en: https://oncenoticias.digital/ciencia/escasez-de-chips-una-consecuencia-de-la-pandemia-de-covid-19/. 25 Nov, 2021.

HUERTA VELÁZQUEZ, Erick. **Manual de telefonía celular comunitaria**: Conectando al Siguiente Billón. Redes por la Diversidad, Equidad y Sustentabilidad A.C. 2016. https://wiki.rhizomatica.org/images/Manual_Telefonia_Comunitaria.pdf

INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT (ICTD) LAB. *Haulage* [Rust]. **UW ICTD Lab**. https://github.com/uw-ictd/haulage .2022a (Original work published 2018)

INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT (ICTD) LAB. *CoLTE* [JavaScript]. **UW ICTD Lab**. https://github.com/uw-ictd/colte/blob/

223077ce09275c879da597312a4871ea477edeca/README.md 2022b. (Original work published 2018).

MERINO FEBRERO, Borja. Análisis de tráfico con Wireshark. **Instituto Nacional de Tecnlogía de la Comunicación.** P. 52, 2011. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

MILOIORISI, Diego Fernando. **Internet profunda**: Anonimato, libertad de expresión y censura en Internet. 1a. Edición, 2016. http://www.internetprofunda.com.ar/wp-content/uploads/2016/05/Internet-Profunda.pdf

NEHRING, Christopher. Luchar contra el coronavirus con aplicaciones espía y de ubicación. **DW.** 24 marzo, .2020. https://www.dw.com/es/luchar-contra-el-coronavirus-con-aplicaciones-esp%C3%ADa-y-de-ubicaci%C3%B3n/a-52904411

OBREGÓN, Javier. El software libre no va en la computadora sino en la cabeza de las personas. Disponible en:. https://www.youtube.com/watch?v=OZ1LAjuYotc 27 Junio, 2017. (14min)

PRUDENCIO, Karla , & BLOOM, Peter. Mantenlo análogo: Parámetros para una exclusión voluntaria de la conectividad. 9 de Junio, 2021.
Disponible en: https://www.rhizomatica.org/mantenlo-analogo-parametros-para-una-exclusion-voluntaria-de-la-conectividad/

TOR PROJECT. *Anti-censorship / Pluggable Transports / Snowflake*. GitLab. Accedido el 26 de junio de 2022, de https://gitlab.torproject.org/tpo/anti-censorship/pluggable-transports/snowflake/-/wikis/home. (s/f-a).

TOR PROJECT. El Proyecto Tor - Privacidad & Libertad en línea. Accedido el 10 de junio de 2022, de https://torproject.org (s/f-b).

TOR PROJECT. Tor Specifications - GitLab. GitLab. Accedido el 26 de junio de 2022, de https://gitlab.torproject.org/tpo/core/torspec/-/blob/main/tor-spec.txt (s/f-c)

TOR PROJECT. Community and legal resources. https://community.torproject.org/relay/community-resources/ (s/f-d)

UNICEF. Uno de cada tres niños en el mundo no puede acceder a clases a distancia si su escuela cierra. **Noticias ONU**. https://news.un.org/es/story/2020/08/1479572 27 Agosto, 2020.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Personas que usan Internet (% de la población) | Data. Accedido el 18 de junio de 2022, Disponible en: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS (s/f)