La Importancia del Cómputo Forense en la Actualidad
The Importance of Computer Forensics in the Topicality

Yeiny Romero Hernández[1], María del Carmen Santiago Díaz[1], Judith Pérez Marcial[1], Ana Claudia Zenteno Vázquez[1],
Gustavo Rubin Trinidad Linares[1], Ricardo Martínez Pérez [1]

[1] Benemérita Universidad Autónoma de Puebla, Facultad de Ciencias de la Computación
Av. 14 sur y San Claudio, Col. San Manuel Puebla, México
{yeiny.romero,marycarmen.santiago, judith.perez, ana.zenteno, gustavo.rubin,}@correo.buap.mx,
ricardo.martinezp@alumno.buap.mx

Fecha de recepción: 23 de noviembre de 2022
Fecha de aceptación: 24 de marzo de 2023

Resumen. El cómputo forense es una rama de la ciberseguridad que estudia, analiza y previene delitos informáticos a través de la creación y aplicación de medidas que aportan la seguridad informática. Los métodos de cómputo forense aplicados sobre la investigación en México han encontrado resultados que dejan al país en una posición de altos niveles de inseguridad, por lo que, hay mucho trabajo por desarrollarse en estas prácticas de investigación de ciberseguridad. Con este proyecto se persigue aplicar métodos y técnicas donde se ocupan herramientas de Cómputo Forense basados en el sistema operativo Linux (Kali) para contrarrestar algunos ataques de la web, adicionalmente, se busca tener un impacto educativo en el tema de ciberseguridad con base a estas técnicas, herramientas y metodologías, montando un laboratorio forense y poniéndolo a disposición para las materias del área de redes en nuestra facultad.

Palabras clave: Ciberseguridad, Cómputo Forense, Delítos Informáticos, Actualidad.

Summary. Computer forensics is a branch of cybersecurity that studies, analyzes, and prevents computer crimes through the creation and application of measures that provide computer security. The computer forensic methods applied to the investigation in Mexico have found results that leave the country in a position of high levels of insecurity, therefore, there is a lot of work to be developed in these cybersecurity investigation practices. This project seeks to apply methods and techniques where Computer Forensics tools based on the Linux (Kali) operating system are used to counter some web attacks, additionally, it seeks to have an educational impact on the topic of cybersecurity based on these techniques, tools and methodologies, setting up a forensic laboratory and making it available for subjects in the area of networks in our faculty.

Keywords: Cybersecurity, Computer Forensics, Computer Crimes, Current Affairs

1 Introducción

Hoy en día el uso de los medios digitales ha tomado una gran relevancia, existen millones de dispositivos conectados a la red por minuto, lo que hace que fluyan millones de datos en cuestión de segundos, por lo que es de suma importancia la protección de todos los dispositivos que se encuentran conectados a la red, dado que debemos cuidar la información que fluye a través de ella, es decir, hay que librarla de ataques u otros fines maliciosos, aquí es donde damos cabida a la ciberseguridad. La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, acciones tecnológicas que pueden utilizarse para proteger nuestros equipos en la red de usuarios maliciosos o posibles ataques a nuestros datos. El número de incidentes de seguridad informática está creciendo exponencialmente y la capacidad de responder a este tipo de problemas se ve limitada por la falta de ingenieros profesionales capacitados.[1][2]

Dentro de la ciberseguridad existen varias ramas que protegen diferentes sectores en la red con el fin de librar los equipos de algún ataque. Entre los más destacados tenemos el Hacking Ético, las auditorías de sistemas y el Cómputo Forense.[3] El campo de la informática forense es prácticamente nuevo y se va actualizando hasta la fecha, podemos describir esta disciplina como la solución y desarrollo a los problemas críticos asociados con delitos informáticos de ciberseguridad o casos especiales que se dieron en un lugar en específico donde se indaga qué pasó con la información, como surgió el ataque, que dispositivos y herramientas se ocuparon para llevarlos a cabo y determinar qué fue lo que sucedió con la información. Estas ramas en particular nos sirven de apoyo para la prevención, dado que una vez estudiado el delito se pueden proponer reglas y estrategias que apoyen al sistema a evitar nuevos ataques. [3]

En esta investigación demostraremos la eficiencia de cada una de estas herramientas, buscando implementar dentro de la materia de seguridad en redes Se abarcará desde el punto de vista teórico la importancia de la ciberseguridad.[4] El uso de un laboratorio de cómputo forense puede ayudar a solucionar diferentes problemas, los cuales pueden ser fiscales, investigativos, como diferentes ataques maliciosos a diferentes individuos, es por ello que surgen nuevas implementaciones de tecnologías que facilitan el proceso informático investigativo dentro de una investigación forense, la cual se resuelve por un análisis digital, donde se lleva a cabo una metodología que aplicando sus técnicas y las distintas herramientas existentes de cómputo forense resaltan diferentes hallazgos de evidencia digital.[5][6] Los beneficios de la implementación de un laboratorio de cómputo forense en diferentes organizaciones facilita actuar dentro de una mesa de trabajo de la manera más adecuada, donde existen diferentes herramientas de entorno confiable las cuales analizan los datos de forma segura y se encarga de proteger los datos recuperados y analizarlos desde diferentes dispositivos, tratando de proporcionar un reporte final como expediente, donde un juez o encargado de una investigación de casos en específico interviene de una manera más adecuada.[7][8]

1.1 Herramientas de Cómputo Forense

Existen diversas aplicaciones (herramientas) que se utilizan para realizar la labor de un pentester (auditor de ciberseguridad), que ayudan a los expertos a solucionar los problemas que surgen con los diferentes dispositivos electrónicos y así poder exponer estas pruebas ante una organización. Estas herramientas de ciberseguridad son muy significativas ya que aportan una gran solución ante la pérdida de información de los equipos o dispositivos, robo o modificación de la misma, el mal uso que le pueden dar distintos usuarios, cabe mencionar que estas pueden utilizar hardware y software con licenciamiento o de uso libre.[9] Existen diversas herramientas para computo forense que podemos utilizar: EnCase Enterprise, Autopsy, CAINE, NetworkMiner, Snort, Forensic Toolkit, NMAP, DEFT, SIFT, Nessus, Metasploit, Wireshark, Owasp Zap, Magnet Forensics, Volatility, Bulk-Extractor, etc., de las cuales se utilizan 3 de software libre que se consideran, por sus características adecuadas para el sistema operativo Kali Linux en el que desarrollaremos este trabajo.

Dichas herramientas son: NMAP (Network Mapper) es un software de código abierto que se ocupa tanto para el análisis de tráfico en la red como para facilitar auditorías de seguridad en los servidores de una red, donde podemos escanear puertos, protocolos y un mapeo completo de diferentes redes. Es multiplataforma para Linux y Windows cuenta con diferentes versiones que se pueden ocupar dependiendo del caso y las características que se necesiten para cumplir con las tareas a realizar que brinden un monitoreo útil y eficiente. [10] OWASP ZAP (zed attack proxy) escáner de seguridad web, esta aplicación de seguridad es ocupada para pruebas de penetración y análisis de datos, enfocada a la mejora y seguridad de diferentes softwares para darles un mejor uso. [11][12]

BULK-EXTRACTOR nos da la posibilidad de escanear la imagen de un disco duro, un archivo específico o varios directorios de archivos. Informando en un archivo los desplazamientos de la información que se llevaron a cabo.[13]

El objetivo de éste proyecto es desarrollar una metodología aplicando técnicas y medidas de ciberseguridad basadas en las herramientas del “cómputo forense” para prevenir delitos cibernéticos.

2 Metodología

Las 3 herramientas seleccionadas se consideran de gran importancia dentro del software libre y pueden ser complementarias para un buen escaneo. NMAP para la inspección de red, hacer auditorías de seguridad,y escaneo de puertos. OWASP ZAP que escanea la seguridad de la web que detecta fallos en diferentes softwares y sus aplicaciones, BULK-EXTRACTOR: diseñada para recabar información de la memoria física de una computadora, que permite al usuario recuperar, analizar e implementar un reporte de los datos que se utilizaron.

Para el uso de las herramientas se utilizará la distribución Linux KALI LINUX que es una distribución con herramientas por defecto dentro del sistema y que son útiles para hacer pruebas de seguridad; es una distribución de software libre que entre sus bondades tiene realizar pruebas de penetración, diversas investigaciones de seguridad, cómputo forense e ingeniería inversa. Este sistema operativo ofrece un entorno donde podemos desarrollar prácticas de seguridad informática y hacking ético. Además, de que es utlizado por diferentes tipos de profesionales para realizar investigaciones y pruebas de ciberseguridad.

Ocupamos NMAP como herramienta de reconocimiento activo dónde existe cierta interacción directa con los objetivos, detección de servicios, descubrimiento de puertos, versiones de aplicaciones, detección de host y las posibles problemáticas de ataques que se pueden realizar a diferentes usuarios y dispositivos. Ver figura 1.

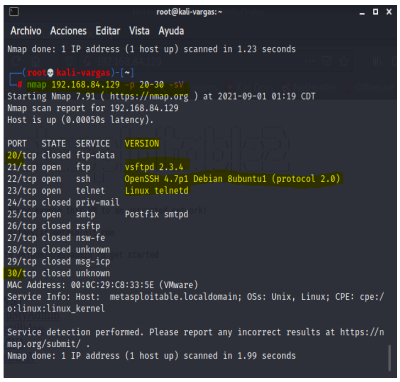

Figura 1. Vulnerabilidad de puertos específicos.

Owasp es una herramienta que le permite a profesionales, investigadores y a diferentes usuarios diagnosticar y resolver problemas de seguridad, generalmente se utiliza en laboratorios de cómputo forense donde para comprender el ¿por qué?, ¿cuándo? y ¿dónde se originó una brecha de ataques a sitios web, aplicaciones y sistemas que comparten cualquier tipo de información?. Ver las figuras 2 y 4.

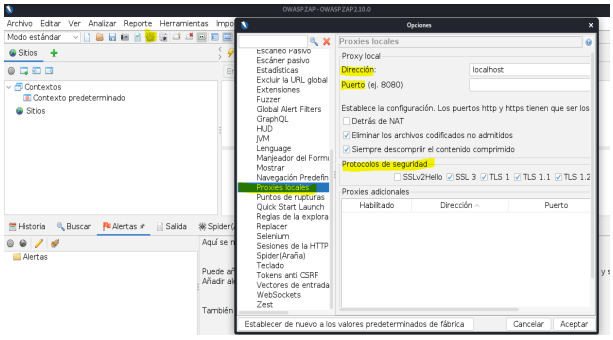

Figura 2 Ataque pasivo a un sitio web determinado servidor y puertos específicos.

Bulk-Extractor es una herramienta que permite recuperar (indagar) información de una memoria RAM, por ejemplo: correos electrónicos, números de teléfono, direcciones IP, tarjetas de crédito, archivos de texto de diferentes extensiones, procesamiento de datos, recuperación de datos, URL´S u otros archivos de evidencia digital. Toda ésta información se utiliza durante una investigación de cómputo forense, siendo muy útil para investigaciones de implantación de malware y ataques de intrusión. Podemos decir que “BULK-EXTRACTOR” es una excelente herramienta para realizar la recolección de información digital dentro de uno o distintos casos de cómputo forense, aportando un 90% de efectividad para indagar diferentes datos digitales. Ver Figura 3

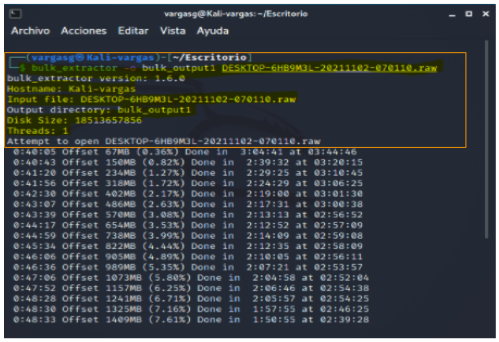

Figura 3. Extracción de información del archivo de volcado de memoria.

2.1 Propuesta de laboratorio de prácticas de un “laboratorio forense”

La infraestructura de hardware y software de un laboratorio de cómputo forense debe tener un espacio al menos de un aula de 5 x 7 mts (ver figura 4) donde tengamos acceso a la red en una o más computadoras y podamos instalar las herramientas de cómputo forense (NMAP, OWASP Y BULK-ESTRACTOR) para realizar diferentes pruebas, tratando de analizar diferentes casos de estudio como perdida de datos en dispositivos, recuperación de archivos en memorias, también tener diferentes equipos de trabajo como: discos duros que contengan al menos 500gb de información, memorias RAM de diferentes tamaños, memorias externas (USB) de 8, 16, 32, 64 gb, servidores, impresoras, ups, módems, cables para diferentes dispositivos, dispositivos móviles, etc. Estos serán los dispositivos para analizar y serán de utilidad para tomar experiencia. Es necesario contar con un laboratorio de cómputo forense, para resolver y adquirir experiencia en la solución de problemas.

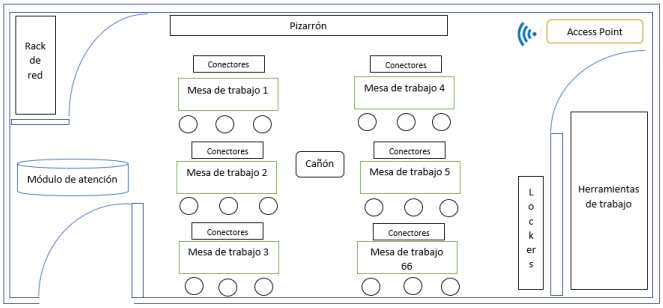

Figura 4. Croquis de la infraestructura del laboratorio de cómputo forense.

3 Resultados

OWASP y NMAP son herramientas que se complementan ya que mientras OWASP trabaja a nivel de sitios web buscando vulnerabilidades, NMAP descubre puertos y Sistemas Operativos a nivel de terminal lo que hace que nuestras pruebas nos brinden un escaneo de vulnerabilidades, mediante este desarrollo con el cual descubrimos e identificamos vulnerabilidades en una red, sitios web y aplicaciones que se utilizan hoy en día. Durante el proceso descrito se inspecciona una gran cantidad de tráfico de información proveniente de servidores, permitiendonos tomar decisiones de seguridad informática como condiciones de protección de servicios en los dispositivos de una red. Ver Fig. 5

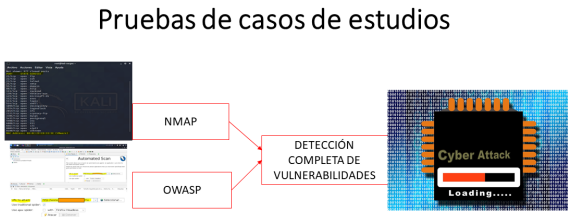

Figura 5. Diagrama de bloques que muestra el complemento de 2 herramientas del cómputo forense

Bulk-extractor es un software de código abierto que puede encontrar datos examinando una imagen de la memoria RAM de una computadora, el beneficio de ocupar esta herramienta es que siempre está en constante actualización por ello podemos considerarla una herramienta de cómputo forense moderna. Esta la podemos utilizar dentro de una estación de trabajo (laboratorio de cómputo forense) para recabar información de archivos y directorios de un disco duro en específico. Obteniendo esta información podemos saber qué información está dentro de una computadora en particular y donde se utilizó.

3.1 Resultados herramienta NMAP

Las pruebas se realizaron con diversos casos de uso, por ejemplo NMAP se probó para la identificación de host, donde obtuvimos resultados muy satisfactorios ya que se identificó a los que estaban conectados a nuestra red y los posibles ataques que puedan surgir en ésta. Ver fig. 6 y 7.

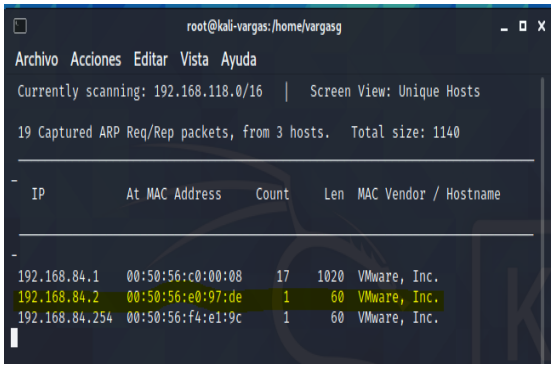

Figura 6. Identificación de dispositivos conectados a una red, host y Gateway.

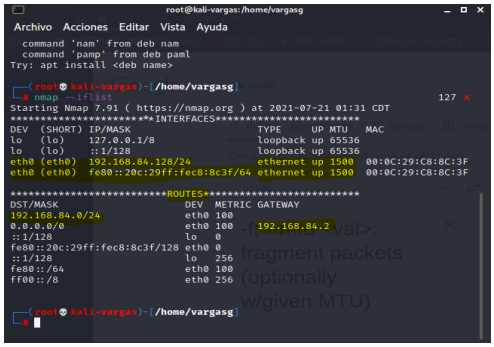

Figura 7. Identificación de red IP X.X.X.X en forma de tabla arrojando nombre de la tarjeta de red.

3.2 Resultado herramienta OWASP

Owasp es una herramienta utilizada en el cómputo forense, además de ser muy completa para diferentes investigaciones, ayuda a profesionales así como a diferentes usuarios a comprender los fallos de seguridad (vulnerabilidades) que existen dentro un sitio web, aplicación o sistemas de infraestructura que ocupan las diferentes organizaciones. Utilizamos esta herramienta comunmente para evaluar la seguridad de un sitio web, identificando cada vulnerabilidad en este a fin de poder minimizar un ataque malicioso, preservando la información de lo que contenga este. Utilizando un sitio web como prueba “http://------.mx” realizamos un análisis de vulnerabilidades en éste, donde los motores de búsqueda de esta herramienta nos brindan información detallada del sitio web. Ver fig.8

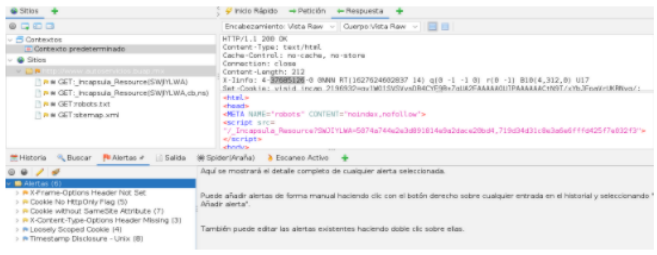

Figura 8. Ataque activo a un sitio web con protocolo de seguridad de transferencia “http” específico.

3.3 Resultado herramienta BULK-EXTRACTOR

Esta herramienta es importante en diferentes escenarios de trabajo que involucren incidentes de ciberseguridad, sobre todo en memorias con datos perdidos. Esta herramienta brinda un 95% de efectividad en investigaciones complejas de cómputo forense. Despues de realizar diversos análisis dentro de nuestra estación de trabajo observamos que es muy eficiente para la recolección de información, en comparación con VOLATILITY, FTK-IMAGER y MAGNET FORENSICS, ya que ésta nos ayuda a realizar un análisis minucioso (escaneo) de todos los archivos que se encuentran ocultos dentro de la memoria RAM. Ver. Fig. 9

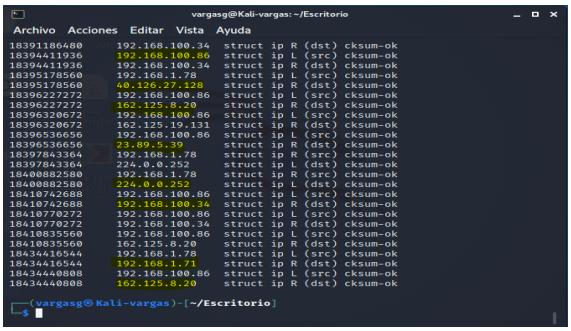

Figura 9. Inspección de IP´s almacenadas en la memoria RAM.

4 Conclusiones

La experiencia que nos brindó el cómputo forense fue satisfactoria dado que nos ayudó a comprender y analizar la evidencia de delitos cibernéticos, por ello se necesita un conocimiento complejo en la teoría de la ciberseguridad, así como el manejo de herramientas especializadas para esta, cuyo objetivo es la revisión de la información recolectada por estas herramientas mediante las técnicas que utilizamos, conociendo estos componentes tecnológicos de software podremos analizar diferentes casos de estudio que puedan surgir en la actualidad, dando una solución científica que puede ser evaluada por un experto o investigador. Podemos concluir que aplicándo las herramientas presentadas, dentro de una computadora conectada a una red, obtendremos resultados sobre diferentes dispositivos electrónicos que podríamos analizar. Adicionalmente la metodología propuesta (ver figura 10) está basada en modelos de recolección de evidencias digitales forenses por autores que realizan pentesting, lo cual significa que las evidencias digitales analizadas tienen un fin forense.

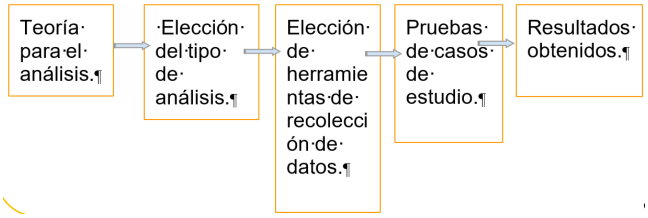

Figura 10. Metodología basada para el análisis de información con herramientas de cómputo forense.

Estas herramientas de identificación, preservación y análisis de información pueden ser utilizadas para que se analicen dispositivos recolectados por un área legal y se juzguen los delitos cometidos por una o más personas. De acuerdo con esto, si utilizamos más herramientas dentro del laboratorio de cómputo forense propuesto y agregando más componentes (dispositivos de software y hardware), podríamos realizar investigaciones más complejas, reflejando la importancia de la ciberseguridad y ayudando a recolectar información que sirva para detectar nuevas vulnerabilidades y minimizar los riesgos de ciberataques.

Referencias

1 Sánchez Cano, Gabriel. Seguridad Cibernética, Hackeo ético y programación defensiva. (PP 268). Alfaomega; 1era Edición (2018).

2 Gil Vera VD, Gil Vera JC. Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. Scientia et Technica. 2017;22(2):193-197. doi:10.22517/23447214.11371. Recuperado de: https://web-a-ebscohost-com.proxydgb.buap.mx/ehost/pdfviewer/pdfviewer?vid=5&sid=d44920b6-e80b-49a4-8a70-0a4bb35e64d8%40sessionmgr4007
3 Caneda Martínez, Fanl. (Julio 10,2020) Ramas de la ciberseguridad: divisiones de una profesión con futuro. Revista: Campus Training. Recuperado de: https://www.campustraining.es/noticias/ramas-ciberseguridad-profesion-futuro/
4 Arnedo Blanco, Pedro. García Rosado, David. (Marzo 11, 2014). Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos. (Trabajo fin de máster). Universidad Internacional de la Rioja, La Rioja, Recuperado de:https://reunir.unir.net/bitstream/handle/123456789/2828/arnedo%20blanco.pdf?sequence=1&isAllowed=y
5 García Garduño, Eladia Salgado Gallegos, Mireya. (2013). Análisis documental del Cómputo Forense y su situación en México. 20 Abril 2021, de IS-UAEM. Recuperado de: http://ri.uaemex.mx/bitstream/handle/20.500.11799/14288/404004.pdf?sequence=1&isAllowed=y
6 Lázaro Domínguez, Francisco. Introducción a la Informática Forense. (PP 329). Ra-Ma. (2014).
7 Cole, Arthur. Brett, Johnson. (Enero 9,2020). Lista de las mejores herramientas de informática forense, recuperación forense de datos, análisis forense digital. Clever How-To´s. Recuperado de: https://www.cleverfiles.com/howto/es/computer-forensic.html
8 Coscollano, Carlos. (Marzo 3,2019). Análisis forense de dispositivos móviles. Revista: Red Seguridad. Recuperado de: https://www.redseguridad.com/especialidades-tic/auditoria-e-investigacion/analisis-forense-en-dispositivos moviles_20190313.html#:~:text=Al%20igual%20que%20para%20los,cada%20modelo%20de%20sistema%20operativo.
9 López Delgado, Miguel. (Junio 2007) Análisis Forense Digital. 2da Edición. Recuperado de: https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
10 NMAP.ORG. (2021). Capítulo 15. Guía de referencia de Nmap. 23 Junio 2021, de NMAP.ORG. Recuperado de: https://nmap.org/book/man.html#man-description
11 OWASP. (2021). Acerca de la Fundación OWASP. 30 Junio 2021, de Owasp.org. Recuperado de: https://owasp.org/about/
12 Caballero Quezada, Alonso Eduardo. Pruebas de penetración con Zed Attack Proxy. (Noviembre 23, 2016). Recuperado de: https://owasp.org/www-pdf-archive//OWASP_ZAP_Alonso_ReYDeS.pdf
13 Lorenzo, Antonio José. (Agosto 18, 2020). Mejores herramientas gratuitas de informática forense. 1 Julio 2021, de RZ redes zone. Recuperado de: https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/