RESEÑA

Ciberseguridad: análisis y aplicación de la herramienta forense ProDiscover

Bandr Siraj Fakiha

Introducción

A pesar de los numerosos beneficios asociados a las tecnologías de la información, varias organizaciones empresariales se enfrentan a una gran amenaza conocida como ciberdelincuencia. La incidencia de la piratería de sistemas y la intrusión de los ciberdelincuentes está resultando muy elevada. Según un artículo de Forbes escrito por Brooks (2022), aproximadamente el 93% de las redes de las empresas son vulnerables a la intrusión de los ciberdelincuentes. El artículo también informa de que el sector de la investigación y la educación es el más atacado por estos delincuentes, seguido por los sectores de la atención sanitaria, los ISP y MSP, y las comunicaciones. Además, el ransomware (el secuestro de datos digitales) como problema de ciberseguridad incurrió en más de 20 mil millones de dólares a nivel mundial en 2021 y afectó a cerca del 37% de todas las empresas y organizaciones comerciales (Brooks, 2020).

La protección del problema de la ciberseguridad ha costado al mundo aproximadamente 1 billón de dólares entre 2017 y 2021, que se espera que aumente a 1.75 en los próximos cinco años (Brooks, 2020). El problema de la ciberdelincuencia puede afectar negativamente a los usuarios individuales de dicho sistema, a las pequeñas y grandes organizaciones empresariales, además de algunas implicaciones financieras importantes, por ejemplo, costes directos como el robo de dinero, activos digitales e información sensible. También puede causar una serie de costes indirectos en lo que respecta a la interrupción de un servicio, bajo nivel de productividad y la responsabilidad legal general que se deriva de la desviación de recursos como la energía, capital y ancho de banda, lo que puede conducir además a una serie de costos que están asociados a los efectos a largo plazo en un ataque a la imagen de marca, la mala reputación y la competitividad (Budzier, 2011).

Para castigar la ciberdelincuencia, la dirección de la organización debe consolidar pruebas. Una de esas pruebas son los equipos de cómputo utilizados por el sospechoso. Los datos almacenados en dicho ordenador se toman como prueba a la hora de castigara a los autores del ciberdelito. Estas pruebas sólo pueden obtenerse a través de lo que los estudiosos denominan investigación forense. La informática forense se refiere a recorrer los incidentes en los sistemas informáticos para investigar delitos o para rastrear activos digitales. Algunos de los tipos de análisis forense digital son el análisis forense de equipos de cómputo, el análisis forense de cortafuegos, el análisis forense de bases de datos, el análisis forense de sistemas en tiempo real y el análisis forense de software, etc. De los mencionados, la informática forense es la más esencial, ya que implica el análisis y la investigación para la recopilación y preservación de pruebas (Naskar et al., 2017).

Revisión de la literatura

Amenazas a la ciberseguridad

La literatura afirma que la comunicación de la información en los tiempos actuales se ha vuelto más efectiva y eficiente (James, Nottingham & Kim, 2013). A pesar de ello, la preocupación por la seguridad en la transferencia de datos ha ido en aumento. Los ciberataques y otras amenazas relacionadas con los sistemas de comunicación de información están haciendo que la seguridad de las

Bandr Siraj Fakiha, Doctor.
Universidad de Al-Qur.
Arabia Saudí
Correo-e: bfageeha@hotmail.com

redes y los sistemas se convierta en un aspecto que merece una mayor consideración en el ámbito de la tecnología de la comunicación de la información (Kim, et al., 2015). Con el avance de la tecnología, los piratas informáticos y los intrusos tienen a su disposición herramientas muy complicadas que pueden utilizar para eludir los sistemas de seguridad en redes genéricos conocidos para causar un daño intencionado en todo el sistema (James, Nottingham y Kim, 2013). En concreto, las amenazas a la ciberseguridad se aprovechan actualmente de la conectividad y la complejidad de la infraestructura existente y lanzan ataques a sistemas considerados legítimos. A pesar de estos problemas, es importante tener en cuenta que el rendimiento económico de cualquier empresa suele depender del funcionamiento fiable de sus infraestructuras importantes, cuya seguridad puede correr un mayor riesgo debido a los ciberataques (James, Nottingham y Kim, 2013). Este tipo de ataques tienen importantes repercusiones en la viabilidad financiera general de la organización que puede verse afectada e incluso en la reputación general de la empresa (James, Nottingham y Kim, 2013). Los fallos y caídas de los sistemas son buenos ejemplos de los riesgos que la mayoría de las organizaciones temen actualmente en sus operaciones diarias y para los que se han considerado necesarias numerosas medidas de seguridad.

Flores, Qazi & Jhumka (2016) reconocen que las amenazas a la ciberseguridad han seguido evolucionando y en aumento para, eventualmente, tomar nuevas formas. Symantec (2016) registra que en 2015 se detectaron 430 millones de nuevos malware, lo que representa un aumento del 36% respecto a lo registrado en 2014. Con el creciente ritmo de adopción de la tecnología por parte de las pequeñas empresas, estas estadísticas las dejan muy vulnerables.

A pesar de los desafíos asociados a la ciberseguridad, las pequeñas empresas están pasando continuamente por una transformación radical por la necesidad de abrazar la era actual de la información (Azodolmolky, Wieder & Yahyapour, 2017). Esto ha terminado por hacer que se apoyen en tecnologías de la información por la necesidad de manejar alguna parte importante de sus principales entregas de servicios y, en consecuencia, un activo propio muy valioso para la información de toda la organización. La protección contra el riesgo asociado a la ciberseguridad es una de las cosas más importantes que deben tener en cuenta las organizaciones empresariales actuales. Bandyopadhyay, Jacob y Raghunathan (2010) afirman que, aunque muchas organizaciones están avanzando hacia la creación de servicios electrónicos y haciendo que su información sea más digital, cómoda y accesible, existe un gran riesgo que viene con ello, una grave amenaza cibernética. Es probable que los datos sean robados, pirateados, borrados o incluso saboteados.

Entre estas medidas siempre han figurado sistemas de detección de cualquier forma de intrusión en la red (Wang, Chao & Wang, 2015) que suele analizar y predecir los comportamientos de un determinado sistema con el objetivo principal de contrarrestar aquellas actividades que puedan interpretarse como sospechosas (James, Nottingham & Kim, 2017). Una intrusión puede producirse de varias formas, un usuario legítimo de un determinado sistema haciendo un mal uso de los privilegios que tiene para acceder al sistema, un usuario legítimo que intenta obtener privilegios de acceso adicionales y, por último, un atacante externo que intenta acceder al sistema (James, Nottingham & Kim, 2013).

El sistema de detección de intrusos en la red funciona reconociendo los ataques o las actividades maliciosas, bloqueándolas, bien, detectándolos mediante el examen de las firmas del ataque dentro de los archivos de registro. Sin embargo, incluso con este tipo de sistemas de seguridad para redes, las organizaciones todavía no han conseguido mucho (Farahmand, et al., 2005). Para que cualquier organización empresarial esté a salvo de las ciberamenazas, necesita un sistema de seguridad complejo que pueda proteger sus redes informáticas existentes de las amenazas peligrosas. El sistema de seguridad puede constar de cortafuegos, un sistema que detecte y prevenga las intrusiones y soluciones para la gestión de rutas, junto con algún antivirus potente.

La aplicación ProDiscover Forensic en la investigación de la ciberdelincuencia

ProDiscover Forensic es una herramienta informática forense que "*7 Best Computer Forensic Tools*" (2019) describe como un sistema poderoso

que permite a los profesionales de la informática localizar todos los datos de los discos duros, incluso aquellos que habían sido borrados previamente. La herramienta forense ProDiscover recupera los archivos borrados, examina el espacio libre y permite de forma dinámica la previsualización, la captura de imágenes y la búsqueda del área protegida por hardware (HPA) mediante su tecnología ("*7 Best Computer Forensic Tools*", 2019). Sin embargo, la herramienta forense ProDiscover no determina los patrones de ciberataque ni encuentra los motivos de los ciberataques como lo hará el sistema de este proyecto; los conceptos forenses utilizados por serán útiles para este proyecto, ya que éste requiere de la ciencia forense digital para ayudar a frenar el problema de la ciberdelincuencia mediante la determinación de las actividades delictivas.

Algunas de las características de este software incluyen la recuperación de datos borrados, el borrado seguro del disco y el apoyo al análisis no destructivo del disco. Según Sanap y Mane (2015), la capacidad de búsqueda booleana completa del software implica que puede explorar todo el disco en busca de frases, palabras clave y expresiones regulares. Además, su compatibilidad con hash permite aislar los archivos ilegítimos de los buenos archivos del sistema.

El kit de herramientas ProDiscover Forensic 4.9 cuesta aproximadamente 2.195 dólares (Windowsbulletin, 2019). Sin embargo, la compra permite una única inspección forense de todo el sistema (SC Media, 2008). La herramienta ofrece una herramienta de informes incorporada para presentar fragmentos de pruebas en caso de requerirse para procedimientos legales. Además, recoge información sobre la zona horaria, las actividades en Internet y la información de las unidades de disco. Por lo tanto, el software tiene una amplia capacidad de búsqueda para obtener nombres de archivos y datos únicos, patrones de datos, tipos de archivos y rangos de fechas.
Existen diferentes investigaciones y recopilación de literatura sobre técnicas y metodologías forenses digitales, como el entorno Windows. Las investigaciones forenses digitales implican la retención de dispositivos y datos contenidos. Los datos se recogen y compilan con fines de investigación. Existen diferentes modelos forenses digitales adoptados en la investigación y el manejo de datos forenses, como el modelo de proceso de investigación, el proceso forense, el proceso de investigación digital integrada, el proceso forense informático y el modelo de proceso de triaje de campo forense informático (Kilungu, 2015). Los diferentes modelos tienen cuatro fases básicas adoptadas en el proceso de investigación. Incluyen la fase de preparación, la fase de adquisición de datos, la fase de investigación y la fase de información. En el caso del entorno Windows está compuesto por diferentes herramientas forenses digitales como OSForensics, HxD editor y ProDiscover. OSForesnic permite la extracción de pruebas forenses a partir de la implementación de la indexación y búsqueda de archivos. HxD Editor Tool es capaz de borrar archivos, recuperar datos, clonar y crear imágenes de disco de bajo nivel para fines de investigación forense. ProDiscover Herramienta forense que mejora la seguridad de los borrados de disco, la recuperación de datos borrados y el apoyo al análisis no destructivo del disco (Dweikat, Eleyan & Eleyan, 2020).

Metodología

Este documento explora el conjunto de herramientas forenses ProDiscover en el contexto de la vigilancia, gestión y control de la ciberseguridad en el lugar de trabajo. Introduce el tema y proporciona información creíble, relevante y fiable para mejorar la calidad y la cantidad del contenido relacionado. A continuación, explora un caso de la Jonson Corp, donde un empleado ha sido acusado de violaciones de ciberseguridad, e ilustra la eficiencia y la eficacia del Prodiscover Forensic Toolkit en la realización de la investigación.

El documento trata, a manera de ilustación, una investigación propia sobre un miembro del personal, el Sr. Juan, en Jonson Corp. Comienza situando el problema de la ciberseguridad en su contexto utilizando pruebas de varias fuentes fiables e ilustra cómo y por qué las empresas deben formular estrategias para mejorar la protección contra las amenazas actuales y futuras. El documento detalla cómo se aplicó el kit de herramientas forenses de ProDiscover para investigar las acusaciones contra el empleado, que implicaban quejas sobre su uso poco ético del

equipo de la empresa. Por lo tanto, utilizando los resultados del documento, las organizaciones, las empresas comerciales y otros investigadores pueden mejorar su conocimiento de las posibles herramientas y técnicas de mejora de la ciberseguridad, como el kit de herramientas forenses ProDiscover, y mejorar la seguridad general de su lugar de trabajo.

La información contenida en el documento se recopiló con base en criterios de credibilidad, relevancia y fecha. Todas las fuentes fueron revisadas por pares, académicas y eruditas, y se recuperaron de organismos relacionados con la tecnología de gran credibilidad, como Information Technology and Management e IEEE Communications. Además, las fuentes debían estar relacionadas con el tema de la ciberseguridad y explorar aspectos como la creación de redes, el análisis forense, las herramientas forenses y la recuperación de datos. Estas fuentes tampoco tenían más de 18 años de antigüedad para garantizar que la información fuera relativamente reciente, ya que el conjunto de conocimientos sobre ciberseguridad, como aspecto de la tecnología y el Internet de las cosas, se está expandiendo y avanzando exponencialmente.

La elaboración de este documento no presentó conflictos de intereses. Dado que la mayor parte de la información se obtuvo en línea, el proceso de investigación no planteó limitaciones financieras. Además, se concedió un amplio plazo para la realización del trabajo. Por lo tanto, las restricciones de tiempo no limitaron la planificación, la formulación y la finalización del estudio. La ausencia de estas limitaciones hizo que los resultados y las conclusiones no se vieran afectados, lo que contribuyó a la fiabilidad y credibilidad del documento.

Resultados y discusión

Los investigadores forenses digitales siguen las etapas y medidas específicas cuando trabajan en un incidente. Por ello, el investigador se asemeja a las herramientas, ya que actúan como tales en el seguimiento y la persecución de los delincuentes. En consecuencia, deben seguir un proceso estándar para obtener resultados creíbles. Del mismo modo, el enfoque adoptado en este proceso de investigación tenía cuatro fases, tal como propone Kilungu (2015). Siguiendo este enfoque, es posible dar cuenta de todos los datos y pruebas obtenidos durante el examen. Además, es más fácil mostrar los valores de tiempo y control como pruebas de investigación.

El investigador siguió un caso en el que una empresa llamada Jonson Corp. se había quejado de uno de sus empleados, un tal Sr. Juan, que había hecho un mal uso de su sistema informático. La empresa tenía la duda de si había estado utilizando el sistema informático para ver y posteriormente descargar imágenes pornográficas. La empresa buscaba pruebas para implicar al sospechoso en cuestión. Durante el registro del material físico del cajón del sospechoso, se encontró un disquete de 1,44 MB de capacidad. El disquete estaba etiquetado con su nombre.

Según Lovanshi y Bansal (2019), la recopilación de pruebas a partir de medios de almacenamiento, como en el caso del disco de Juan, está respaldada por los pasos fundamentales de la investigación de medios de almacenamiento. Estos incluyen la extracción de una imagen del sistema comprometido, la realización del cálculo de la integridad del valor de control, la recuperación de archivos o carpetas a nuevas ubicaciones, el examen de archivos específicos eliminados y la recopilación de pruebas. Las pruebas se recogieron de carpetas recicladas, sectores defectuosos, espacios libres, dispositivos auxiliares, registros de actividad de red y archivos de software de aplicación. Asimismo, la recopilación de pruebas implicó la copia adecuada de las mismas en archivos de texto apropiados, la búsqueda pertinente de cadenas de términos clave y el examen preciso de las aplicaciones o la indicación del cifrado, el borrado, la compresión y las utilidades de cifrado u ocultación de archivos.

Para examinar la infracción cometida por Juan, los investigadores decidieron utilizar el proceso de cuatro fases. El primer paso fue la fase de investigación, que consistió en solicitar el permiso de la autoridad competente para registrar e incautar los materiales. Se aseguró el lugar de los hechos y se documentó la cadena de custodia de los artículos

incautados. En particular, el investigador priorizó las acciones y justificó los recursos para la investigación.

La fase de adquisición de datos consistió en la obtención de las pruebas digitales iniciando primero el software ProDiscover Forensic 4.9, como se muestra en la figura siguiente:

Figura 1: Configuración del software ProDiscover Forensic

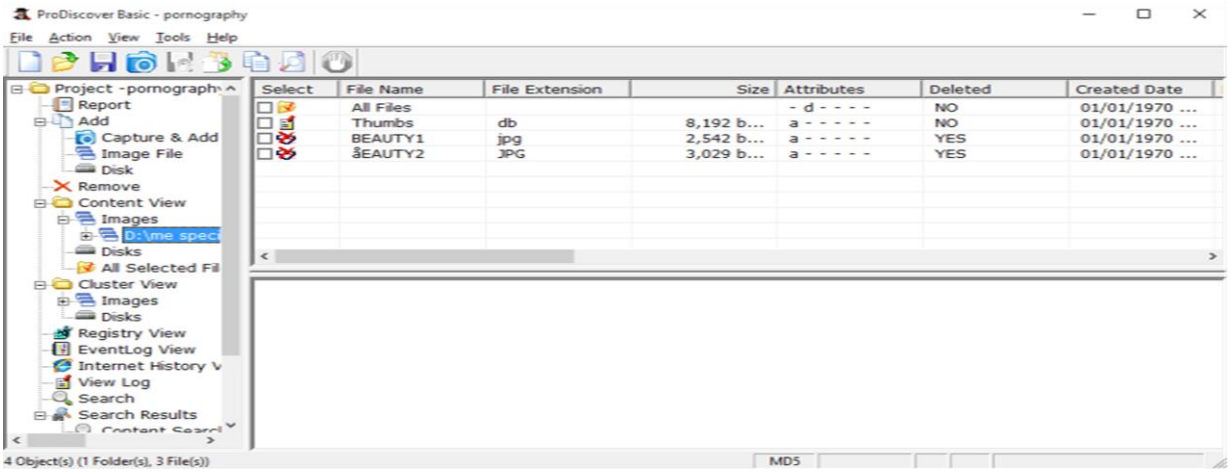
Fuente: Creada por el autor con el paquete de herramientas forenses ProDiscover

La herramienta ProDiscover Forensic 4.9 se utilizó para crear una imagen informática forense de las pruebas confiscadas. Antes de la creación de la imagen, se calculó el valor de control MD5 de la prueba digital, el disco flexible, para comprobar su autenticidad. Posteriormente, se examinó la imagen forense de las pruebas en la fase de investigación. Más concretamente, se hizo clic en la imagen para ver su contenido. Esto permitió ver el contenido de la imagen del disco dentro del panel derecho. Como se muestra en la siguiente figura, los investigadores pudieron ver las imágenes BEAUTY1.jpg y BEAUTY2.jpg que habían sido borradas del disco blando.

El software ProDiscover Forensic 4.0 ofrece un examen de seguridad del disco duro. El software fue capaz de dar detalles sobre lo que se había borrado del disco duro. Una vez que se iniciaba y se creaba una imagen forense de las pruebas confiscadas, ProDiscover Forensic generaba automáticamente un informe con la información necesaria para presentarla como prueba para una acción legal. El software ayudó a recopilar los datos de la zona horaria, la actividad en Internet y la información de la unidad. A la larga, los investigadores pudieron ver las imágenes BEAUTY1.jpg y BEAUTY2.jpg que habían sido borradas del disco duro.

Estos resultados confirman los hallazgos de Sanap y Mane (2015), quienes realizaron un estudio con las fases descritas utilizando el software ProDiscover para analizar un archivo “de arranque". Según los resultados simulados de un estudio comparativo, ProDiscover es el que mejor funciona en la recuperación de datos. La base de la comparación entre Active File Recovery y ProDiscover se basó en los siguientes aspectos: sistemas de archivos soportados, investigación de

Figura 2: Archivos recuperados con ProDiscover Forensic



Fuente: Creada por el autor con el paquete de herramientas forenses ProDiscover

archivos, investigación de registros, índice de archivos eliminados, imágenes de disco soportadas e investigación de volcados de memoria (Conner, 2020). Dado que la herramienta ProDiscover presentaba ventajas únicas, el mérito de la selección depende de los requisitos y las aplicaciones de la herramienta.

Según Hidayat et. al. (2018), el software ProDiscover restaura los datos borrados de forma eficaz, en particular los datos eliminados por los autores. En su estudio, Sharma & Nagpal (2020) realizaron un análisis comparativo de ProDiscover en cuatro fases. Realizaron la comparación con los kits de herramientas forenses Disk Genius, GetDataBack y Diskdigger para la recuperación de datos en el sistema operativo Windows 8 (Ghazinour, et al., 2017). El análisis comenzó con el formateo de la unidad de dsico flexible y el posterior llenado de datos en la unidad de disco. Se eliminaron todos los datos del disco y se vació la papelera de reciclaje. A continuación se utilizaron los kits de herramientas forenses digitales para la recuperación de datos. El kit ProDiscover recuperó los datos borrados con mayor precisión en comparación con Disk Genius, GetDataBack y Diskdigger (Hidayat, Sudarmaji, Dedi, & Lilik, 2018).

Conclusión

ProDiscover forense es una herramienta muy útil ya que ofrece potentes funcionalidades de seguridad para la información. Esta herramienta puede ser aplicada eficazmente por expertos forenses digitales para buscar información digital para su uso en informes para procesos judiciales. ProDiscover permite realizar búsquedas por palabras clave. Por ejemplo, en la investigación mostrada anteriormente, el investigador pudo identificar el archivo ya eliminado, su contenido y sus nombres. Además, se pueden buscar archivos borrados, por fecha de modificación, fecha de acceso y fecha de creación de los archivos. ProDiscover permite la investigación de la información digital como respuesta a incidentes en ciberseguridad sin alertar los valiosos metadatos, por ejemplo, la última vez que se accedió a ella. Por lo tanto, la herramienta ProDiscover puede ser aplicada por cualquier organización ya que mejora las funciones de seguridad para la información, la búsqueda, la minería y la presentación de informes sobre la información digital obtenida para los procedimientos legales. La herramienta forense digital en este caso puede ser vital para la identificación, extracción, análisis y presentación de pruebas digitales contenidas en dispositivos digitales. Es necesario investigar el funcionamiento y la eficacia de las diferentes herramientas en la identificación, recopilación y análisis de las pruebas digitales para un procedimiento legal. Este enfoque mejora las capacidades de la organización para investigar y responder adecuadamente a la ciberdelincuencia.

Referencia

7 Best Computer Forensic Tools. (2019, February 18). Retrieved from https://resources.infosecinstitute.com/7-best-computer-forensics-tools/#gref

Azodolmolky, S., Wieder, P., & Yahyapour, R. (2017). Cloud computing networking: challenges and opportunities for innovations. *IEEE Communications Magazine*, *51*(7), 54-62.

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. *Information Technology And Management*, *11*(1), 7-23. doi:10.1007/s10799-010-0066-1

Brooks, C. (2022, January 21). *Cybersecurity in 2022 – A fresh look at some very alarming stats*. Forbes. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

Budzier, A. (2011). The risk of risk registers – managing risk is managing discourse not tools. *J Inf Technol*, *26*(4), 274-276. doi:10.1057/jit.2011.13

Conner, T. (2020). *A Review of the Challenges Anti-Forensics Present to the Viability of File Recovery* (Doctoral dissertation, Utica College).

Dweikat, M., Eleyan, D., & Eleyan, A.(2020). Digital Forensic Tools Used in Analyzing Cybercrime.

Farahmand, F., Navathe, S., Sharp, G., & Enslow, P. (2005). A Management Perspective on Risk of Security Threats to Information Systems. *Information Technology And Management*, *6*(2-3), 203-225. doi:10.1007/s10799-005-5880-5

Flores, D. A., Qazi, F., & Jhumka, A. (2016, August). *Bring your disclosure: analysing BYOD threats to*

corporate information. Paper presented at 2016 IEEE International Conference on Turst, Security and Privacy in Computing and Communications, Tianjin, China.

Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017, September). A study on digital forensic tools. In *2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI)* (pp. 3136-3142). IEEE.

Hidayat, A., Sudarmaji, D., Irawan, D., Susanto, L. J., & Mustika, H. P. (2018). Comparative Analysis Of Applications OSforensics, GetDataBack, Genius, and Diskdigger On Digital Data Recovery in the Computer Device. International Journal of Technology & Engineering, 7(4.7), 445-448.

James, T., Nottingham, Q., & Kim, B. (2017). Determining the antecedents of digital security practices in the general public dimension. *Information Technology And Management*, *14*(2), 69-89. doi:10.1007/s10799-012-0147-4

Kilungu, M. K. (2015). An Investigation of Digital Forensic Models Applicable in the Public Sector: A case of Kenya National Audit Office. Nairobi: University of Nairobi.

Kim, S., Kim, G., & French, A. (2015). Relationships between need-pull/technology-push and information security management and the moderating role of regulatory pressure. *Information Technology And Management*. doi:10.1007/s10799-015-0217-5

Lovanshi, M., & Bansal, P. (2019). Comparative study of digital forensic tools. In *Data, Engineering and Applications* (pp. 195-204). Springer, Singapore.

Naskar, R., Malviya, P., & Chakraborty, R. S. (2017). Digital Forensics

Sanap, V. K., & Mane, V. (2015). Comparative Study and Simulation of Digital Forensic Tools Tools. International Conference on Advances in Science and Technology (pp. 1-4). Mumbai: Ramrao Adik Institute of Technology.

SC Media. (2008, May 7). *Security Weekly Labs: Technology Pathways ProDiscover Forensics 4.9*. https://www.scmagazine.com/editorial/product-test/-/technology-pathways-prodiscover-forensics-4-9

Sharma, P., & Nagpal, B. (2020). Regex: an experimental approach for searching in cyber forensic. *International Journal of Information Technology*, *12*(2), 339-343.

Symantec. (2016). Internet security threat report (21). Retrieved from https://know.elq.symantec.com/e/f2

Wang, P., Chao, K., Lo, C., & Wang, Y. (2015). Using ontologies to perform threat analysis and develop defensive strategies for mobile security. *Information Technology And Management*. doi:10.1007/s10799-014-0213-1

Windowsbulletin.com. (2019). ProDiscover Basic and ZeroView. Retrieved February 14, 2020, from Windows Bulletin-Tutorials: http://windowsbulletin.com/de/files/exe/technology-pathways/prodiscover-basic-and-zeroview/

Recibido: 06 de julio de 2022.
Aceptado: 15 de julio de2022.
Conflicto de intereses: ninguno.