RESEÑA

Aplicación y eficacia del editor *Hex Forensic* en la investigación de la ciberdelincuencia

Bandr Siraj Fakiha

Introducción

En la última década, el desarrollo y el uso de las tecnologías de la información han mejorado la eficiencia y la flexibilidad en la prestación de servicios, ya que la mayoría de las organizaciones dependen actualmente de las TSI para realizar la mayoría de sus tareas. Sin embargo, cuando el entorno informático se hace más diverso y complejo, se experimentan numerosos retos a la hora de realizar la gestión de registros, como la necesidad de una respuesta en tiempo real a la gestión de incidentes y amenazas.[1] Los obstáculos más comunes a la seguridad informática son los recursos, la concientización y los factores culturales. La mayoría de las organizaciones carecen de actividades coordinadas sobre cuestiones relacionadas con la seguridad informática, como la ciberseguridad. Del mismo modo, en la mayoría de las organizaciones falta una supervisión de la gestión de la seguridad informática. En caso de que estos riesgos no sean bien atendidos, los objetivos de la organización pueden verse afectados, en mayor o menor medida.[3] Además, la mayoría de las organizaciones carecen de tecnologías apropiadas para investigar las violaciones a los sistemas de seguridad de la información.

Para castigar la ciberdelincuencia, la dirección de la organización debe establecer algunas pruebas. Una de éstas son los ordenadores o dispositivos digitales utilizados por el sospechoso. Los datos almacenados en dicho ordenador puede prueba a la hora de castigar a los áutores de ciberdelitos, que pueden obtenerse a través de lo que los estudiosos denominan investigación forense.[4] El objetivo del presente proyecto es, por lo tanto, establecer la aplicación y la eficacia de *Hex Editor Forensic* en la gestión de riesgos de seguridad de las tecnologías de la información, concretamente en materia de investigación de la ciberdelincuencia. La informática forense se refiere a recorrer incidentes en los sistemas informáticos para investigar delitos o trazar el mapa de los activos digitales.[5] Algunos de los tipos de análisis forense es el de cortafuegos, el análisis forense de bases de datos, el análisis forense de sistemas en vivo y el análisis forense de software, etcétera. De estos tipos, la informática forense es el más esencial, ya que implica analizar e investigar la recogida y la conservación de pruebas.

Hex Editor, comúnmente conocido como HxD, es una herramienta que puede realizar las funciones de apertura y edición de código informático. Además[2] explica que Mael Horz desarrolló HxD para *Windows* y que edita el contenido en bruto de las unidades de disco, la aplicación también puede mostrar y editar la memoria que utilizan los procesos en ejecución. Según [2], HxD soporta la exportación de C#, C, Java, HTML, Visual Basic, discos e imágenes de disco, etcétera. HxD puede integrarse en el menú contextual para una mayor eficacia. Entre las características de HxD se encuentra un editor de RAM que edita la memoria principal, un editor de disco para la lectura y escritura RAW de unidades y discos, comparaciones de archivos y la visualización de datos en conjuntos de caracteres Ansi, DOS, EBCDIC y Macintosh, en el fundamental el análisis estadístico de los datos.

El proyecto propuesto pretende incorporar las capacidades analíticas de *Hex Editor* en el análisis de datos obtenidos de la minería de datos para actividades delictivas.

Bandr Siraj Fakiha. Profesor asociado, Departamento de Servicios Médicos de Salud, Facultad de Ciencias de la Salud, Universidad de Umm Al-Qura, K.S.A.

Materiales y métodos

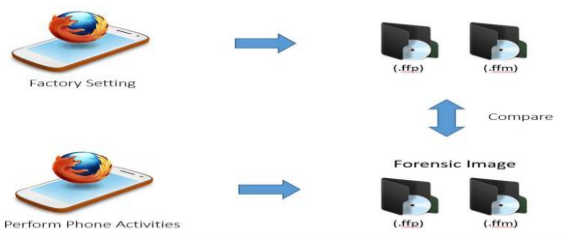
EL estudio llevó a cabo una investigación sobre Mozilla FxOS que se ejecuta en un teléfono, desarrollado por la compañía Peak. Después de haber sido introducido en el mercado en 2013, tiene una versión de FxOS. La especificación del teléfono se muestra a continuación:

Figura 1: especificaciones del teléfono

Hardware	Detail
Processor	1.2 GHz Qualcomm Snapdragon S4 8225 processor (ARMv7)
Memory	512 MB Ram
Storage	-Internal 4GB -Micro SD up to 16GB
Battery	- 1800 mAh - micro-USB charging
Data Inputs	Capacitive multi-touch IPS display

Como se muestra la configuración del teléfono se borró inicialmente, posteriormente se restauró de fábrica. A continuación, se realizó el proceso de adquisición para obtener la imagen del teléfono FxOS (.ffp), así como la imagen de la memoria (.ffm). En consecuencia, estas imágenes binarias se marcaron como imagen base y sus respectivos valores hash MD5 se conservaron de forma segura. Luego, el investigador instaló una aplicación de redes sociales en el teléfono a través de Mozilla Firefox y simuló el uso real de la aplicación ejecutando una serie de actividades, como la subida de imágenes y el envío de mensajes privados. Todos los pasos, las actividades de comunicación y las credenciales se documentaron de forma adecuada desde el punto de vista forense. Posteriormente, se llevó a cabo un segundo proceso de adquisición para identificar e investigar posteriormente en los artefactos reales cuales serían el tipo de credenciales y los datos que podrían extraerse o recuperarse tras su eliminación, lo que se muestra en la figura 2:

Figura 2: proceso de adquisición de teléfonos



Las pruebas se adquirieron mediante el uso de Ubuntu 14.04 LTS y se analizaron en una máquina Windows10. Para capturar la imagen del teléfono de forma adecuada utilizando Ubuntu, se ejecutó bajo *Android Debug Bridge* (ADB) sobre el teléfono. Se aplicó el siguiente comando para configurar el paquete ADB en Ubuntu: # suto apt-got install android-tools-adb

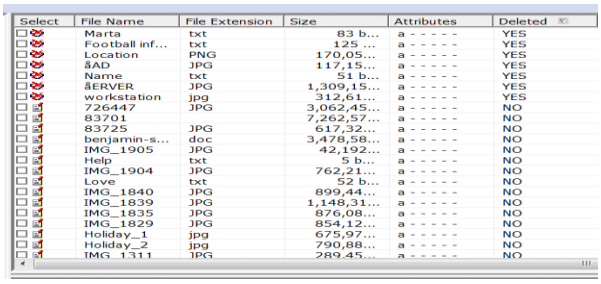
Para la adquisición de memoria volátil, el investigador configuró Linux Memory Extractor (LiME) mediante el siguiente comando: # suto apt-got install-forensics-dkms

Luego se instaló en la máquina HxD *Hex Editor* 1.6.6.0 para analizar las imágenes forenses capturadas previamente y los mensajes enviados y recibidos. Se extrajeron dos tipos de las imágenes binarias que se habían borrado inicialmente, destinadas a ser utilizadas como pruebas forenses en la investigación. Más concretamente, la imagen binaria se extrajo de la memoria interna utilizando el comando dd. El teléfono FxOS se conectó inicialmente a la máquina host especificada y luego se inició la conexión ADB antes de ejecutar el comando dd. Se aplicó el siguiente comando para iniciar la conexión ADB entre la máquina host y el teléfono: # adb shell

Una vez establecida la conexión, se ejecutó del siguiente comando dd para copiar *bit* por *bit* la memoria del teléfono en la tarjeta SD y el archivo en este caso se denominó memoria del teléfono FxOS (.ffp): # dd if=/dev/block/mmcblk0 of=/mnt/emmc/base.ffp bs=2048

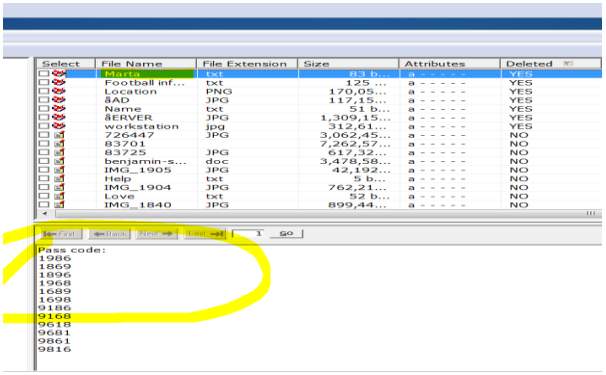
A continuación, se copió toda la imagen binaria de la memoria interna desde la tarjeta SD a la máquina host y al archivo se le denominó ffp. A continuación, el investigador creó el hash SHA1 y guardó el resultado en el bloc de notas. Luego, se seleccionó la imagen una vez extraída, se añadió la imagen y se crearon nuevas carpetas que se utilizaron para investigar todos los archivos eliminados.

Figura 3: ilustración de las distintas carpetas extraídas



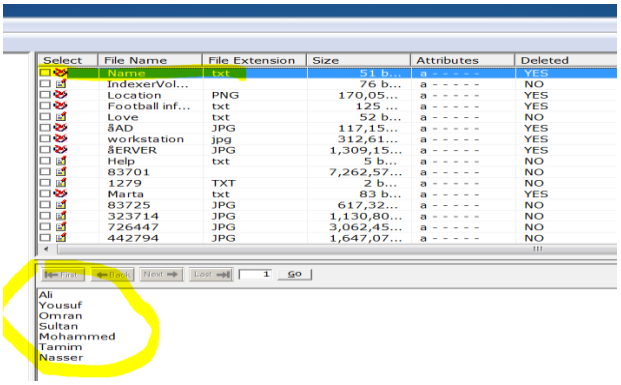
La investigación reveló algunos archivos interesantes; por ejemplo, Marta contenía códigos de acceso, como se muestra en la siguiente figura:

Figura 4 Fichereo llamado Marta y su respectivo código de acceso



El investigador también encontró otro archivo de texto llamado "Nombre" que contenía una lista de personas con las que se había comunicado anteriormente:

Figura 5 Fichero denominado "nombre" con una lista de nombres sospechosos contactados



Resultados y debate

El editor hexadecimal fue capaz de crear hashes y conjuntos de hashes para diferentes archivos, una única cadena de texto o un volumen completo con hashes SHA-1, CRC32, MD5 o SHA-256. El investigador pudo calcular el hash del archivo, de la cadena de texto individual o del volumen y, en consecuencia, compararlo con otro valor hash bien conocido. La función hash de creación/verificación se aplicó para obtener el hash de diferentes carpetas y archivos de una imagen forense. Como se muestra en la metodología, el editor Hex tiene la capacidad general de obtener el hash de las unidades individuales y de las carpetas/archivos de la unidad respectiva. El tiempo necesario para completar el hash variaba en función de la unidad a la que se aplicaba el hash y del tamaño del archivo.

En general, el editor Hex identificó imágenes e información de texto que se habían compartido a través del teléfono. La investigación identificó también información sensible que podría ayudar fácilmente a una investigación posterior, en caso de que fuera necesario. Más concretamente, la imagen binaria se extrajo fácilmente de la memoria interna del teléfono utilizando el comando dd.

Estos resultados demuestran que el editor hexadecimal puede utilizarse eficazmente para visualizar y ejecutar archivos codificados en editor hexadecimal, que puede comprobar el encabezado y el pie de página del formato del archivo. Por ejemplo, el formato de archivo JPG tiene encabezado y pie de página específicos FF D8 FF (encabezado), FF D9 (pie de página). Y para el formato de archivo zip (ZIP) también tiene encabezado y pie de página específicos 50 4B 03 04 14 (encabezado), 50 4B 05 06 00 (pie de página). El editor hexadecimal puede encontrar datos ocultos dentro de un archivo. Por ejemplo, podemos utilizar este editor para encontrar los datos ocultos encontrando otro encabezado y pie de página diferentes los originales.

Como argumenta, Le marter, [5] existen diferentes investigaciones y recopilaciones bibliográficas sobre técnicas y metodologías forenses digitales, como las correspondientes al entorno Windows, implica la retención de dispositivos y datos contenidos. Los datos se recogen y compilan con fines de investigación. Existen diferentes modelos forenses digitales adoptados para la investigación y el tratamiento 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[10] . Los diferentes modelos tienen cuatro fases básicas adoptadas en el proceso de investigación que incluyen la de preparación, la de adquisición de datos, la fase de investigación y la fase de elaboración de informes. El entorno Windows se compone de diferentes herramientas forenses digitales, como el Editor HxD, que permite la extracción de pruebas forenses a partir de la implementación de la indexación y búsqueda de archivos, así como de ordenadores. Además de que la herramienta Editor HxD es capaz de limpiar archivos, recuperar de datos, clonación, y de trabajar con imágenes de disco a bajo nivel para fines de investigaciones forenses. La herramienta Editor HxD Forense mejora la seguridad del borrado de disco, recuperación de datos borrados, y apoyo al análisis de disco no destructivo[9] .

De acuerdo a Le Master,[6] aunque existen diferentes herramientas forenses digitales, la herramienta más común y eficaz es el editor Hex. Estas herramientas se utilizan en el análisis y la manipulación de pruebas digitales propensas a sufrir cambios. Las pruebas digitales pueden transmitirse y almacenarse en diferentes formas digitales, por lo que necesitan un tratamiento especializado utilizando herramientas forenses digitales eficaces. La herramienta de edición hexadecimal es crucial para el inicio de las investigaciones, ya que tiene la capacidad de proveer los detalles del caso y su sistematización en nuevos archivos[5]. Además, se puede extraer datos de descargas recientes, acceder a sitios web y unidades USB, mejora las funciones de seguridad de la información y la búsqueda, la extracción y la generación de informes de información digital para procedimientos legales. Es fundamental para ubicar datos ocultos dentro de diferentes archivos para investigaciones forenses.[8] Esta herramienta forense digital es vital en la identificación, extracción, análisis y presentación de pruebas digitales contenidas en dispositivos digitales. Además,[4] blaheley et al sostiene que es necesario investigar el funcionamiento y la eficacia de diferentes herramientas en la identificación, recopilación y análisis de pruebas digitales para un procedimiento judicial. Este enfoque permite a las distintas organizaciones e individuos determinar las herramientas que mejor se adaptan a sus operaciones y tipo de trabajo.

Sanchez[9] descatca que incluso en el caso de que el sospechoso hubiera borrado todos los archivos y los hubiera sobrescrito el disco duro, uno puede aplicar fácilmente un editor hexadecimal para recuperar cualquier dato que hubiera sido almacenado previamente tanto dentro de los sectores del disco como de los archivos. Un editor hexadecimal permite echar un vistazo a los contenidos físicos individuales almacenados en el disco, independientemente de los límites puestos a archivos, particiones y directorios. Como afirma le Master[5] , los editores hexadecimales se pueden aplicar fácilmente para descifrar incluso software protegido contra copia, estudiar la forma en que funcionan los virus en los ordenadores o, en el proceso de investigación forense, identificar y posteriormente recuperar información específica a la que el sistema operativo no puede acceder normalmente.

Hay que entender que toda la información guardada en el disco duro se graba siempre dentro de las pistas, que en realidad son anillos concéntricos dentro de la superficie de cada plato individual, como los anillos dentro del tronco.[7] Los editores hexadecimales tienen la capacidad de leer directamente el búfer del medio físico sin

tener que depender de los servicios de ningún sistema operativo.

Conclusión

La investigación forense digital implica auditoría en informática, que parte de la evaluación, investigación y análisis de los sistemas informáticos para mapear activos digitales y delitos. Es necesario llevar a cabo una investigación forense para desentrañar los daños causados, el alcance del ataque, el enfoque de los ataques y las futuras medidas a adoptar, las mejores prácticas y enfoques para contrarrestar futuros ataques. Las innovaciones tecnológicas han permitido el desarrollo de nuevas herramientas forenses digitales con la capacidad de combinar investigaciones forenses digitales y actividades ilegales forenses digitales.

La investigación tenía por objeto determinar las tecnologías existentes en las investigaciones forenses digitales, las medidas para optimizar los análisis forenses digitales y los retos experimentados en el curso de la realización de investigación forense digital. La investigación ha establecido que el Editor HEX puede adoptarse en operaciones forenses y con diferentes capacidades y posibilidades. Las herramientas forenses de este Editor permiten localizar los datos al tiempo que protegen las pruebas y crean pruebas de calidad para su uso en procedimientos judiciales. Esta herramienta es eficaz para frenar los ciberdelitos mediante la determinación y dilucidación de actividades delictivas, tiene capacidades analíticas adaptadas para la minería y análisis de datos relacionados con delitos. Además, mejora la investigación digital mediante el uso de *Hash Set* para establecer archivos seguros en sistemas operativos o en un programa, lo que identifica ciberdelitos como *scripts* de *hackers*, virus o troyanos. La herramienta *Hex Editor Incident Response* investiga la información digital sin alterar metadatos valiosos como la última vez que se accedió. Por lo tanto, la herramienta ser aplica con facilidad por una organización ya que mejora las funciones de seguridad de la información que optimizan la búsqueda, extracción y presentación de documentación sobre la manipulación de la información digital para procedimientos legales. La herramienta forense digital, en este caso, puede ser crucial en la identificación, extracción, análisis y presentación de pruebas digitales contenidas en dispositivos digitales.

Agradecimientos

Como siempre, un agradecimiento especial a la Universidad de Umm Al-Qura.

Referencias

1. Hsu, Y.M. y Chang, C.C., 2011. Analysis and improvement on frequency sensitivity of series photodetector frequency circuit system and its application for HEX fluorescence measurement. Optical Engineering, 50(4), p.044401.
2. Schaefer, T., Höfken, H. y Schuba, M., 2011, octubre. Windows phone 7 desde una perspectiva forense digital. En International Conference on Digital Forensics and Cyber Crime (pp. 62-76). Springer, Berlín, Heidelberg.
3. Simon, M. y Slay, J., 2010, febrero. Recuperación de datos de actividad de la aplicación skype de la memoria física. En 2010 International Conference on Availability, Reliability and Security (pp. 283-288). IEEE.
4. Blakeley, B., Cooney, C., Dehghantanha, A. y Aspin, R., 2015, noviembre. Almacenamiento en la nube forense: hubiC como estudio de caso. En 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom) (pp. 536-541). IEEE.
5. LeMaster, A., 2011. Heap spray detection with heap inspector. Blackhat USA, Las Vegas, Nevada, Estados Unidos.
6. Naick, B.D. y Bachalla, N., 2016. Aplicación de la ciencia forense digital en las bibliotecas digitales. International Journal of Library & Information Science (IJLIS), 5(2), pp.89-94.
7. Jain, N. y Kalbande, D.R., 2015, septiembre. Herramienta forense informática utilizando el enfoque de la historia y la retroalimentación. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-5). IEEE.

8. Ryczkowski, A. y Piotrowski, T., 2011. Tomotherapy archive structure and new software tool for loading and advanced analysis of data contained in it. Reports of Practical Oncology & Radiotherapy, 16(2), pp.58-64.
9. Sánchez, L. (2017). Multiplatformní *Hex Editor* (Tesis de licenciatura, České vysoké učení technické v Praze. Vypočetní a informační centrum).
10. Sun, J.L., Zhang, S.W., Huang, S. y Hui, Z.W., 2018, julio. Diseño y aplicación de una herramienta de captura-repetición basada en Sikuli. En 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 42-44). IEEE.

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