Extracción y análisis de artefactos de memoria de la aplicación Telegram Desktop

Pedro Fernández-Álvarez, Ricardo J. Rodríguez

Grupo de I+D en Computación Distribuida (DisCo)
Instituto de Investigación en Ingeniería de Aragón (I3A)
Universidad de Zaragoza, Mariano Esquillor s/n, 50018, Zaragoza, Spain.
Tel. +34-976762707, e-mail: pfernandez@unizar.es

Resumen

Este proyecto se centra en el desarrollo de un entorno de análisis forense para la obtención de artefactos presentes en memoria RAM relativos a aplicaciones de mensajería instantánea. Concretamente, el foco se ha puesto en la extracción de artefactos de memoria pertenecientes a la aplicación *Telegram Desktop*.

Introducción

Las aplicaciones de mensajería instantánea (MI) permiten comunicarse de una manera rápida y cómoda. Hoy en día, una parte notable de la sociedad hace uso de este tipo de aplicaciones para mantener conversaciones. Sin embargo, estas aplicaciones también son usadas en ocasiones como medio para cometer o esclarecer delitos. Es en estos últimos casos cuando el análisis forense de los dispositivos del criminal o de la víctima puede ser de gran ayuda, proporcionando evidencias vitales para la resolución o esclarecimiento del posible crimen acontecido.

Uno de los factores que en ocasiones dificulta la obtención de artefactos digitales relativos a aplicaciones de MI es la existencia de cifrado, tanto en las bases de datos locales de estas aplicaciones como en la información que las aplicaciones transmiten a través de la red. No obstante, los contenidos presentes en la memoria RAM deben encontrarse descifrados para que la aplicación pueda trabajar con ellos, haciendo que el análisis forense de la memoria RAM sea especialmente interesante cuando exista cifrado tanto de los datos almacenados de manera local como de las comunicaciones [1].

La presente investigación se focaliza en la plataforma de MI *Telegram*, la cual se encuentra entre las 5 más populares a nivel global. En particular, se ha analizado el cliente multiplataforma oficial de *Telegram* para ordenadores, llamado *Telegram Desktop*. El objetivo de este trabajo es investigar los contenidos presentes en memoria RAM relativos a la aplicación *Telegram Desktop* de cara a identificar artefactos digitales de interés para una investigación forense. La base de datos local de *Telegram Desktop* se encuentra cifrada [2] y las comunicaciones con sus servidores se llevan a cabo también de manera cifrada [3], provocando ambos hechos que el análisis de la memoria RAM se considere de gran importancia.

Durante la realización del presente proyecto se ha trabajado con la versión 2.7.1 de *Telegram Desktop* para el sistema operativo Windows 10. Se ha elegido Windows dado que es el sistema operativo para ordenadores con más cuota de mercado en la actualidad y Windows 10 dado que es la versión más popular a día de hoy [4].

Entorno de análisis desarrollado

De cara a analizar los contenidos que se encuentran en la memoria RAM de un sistema Windows es necesario, en primera instancia, obtenerlos. Además, dado un volcado de memoria RAM de un proceso, hay que identificar la localización con la que se corresponden las direcciones virtuales de dicho proceso. De esta manera, es posible acceder al elemento almacenado en una dirección virtual concreta. Con el objetivo de extraer los contenidos de la memoria RAM relativos a un proceso determinado en un formato que cumpla con el requisito previamente mencionado se ha elaborado la herramienta llamada *Windows Memory Extractor* [5].

La segunda herramienta desarrollada en este trabajo, denominada *Instant Messaging Artifact Finder* (abreviado como *IM Artifact Finder*) [6], se encarga de analizar un volcado de memoria de un proceso relativo a una aplicación de MI y de generar un informe en el que se refleje la información de los artefactos obtenidos. Estas dos herramientas elaboradas componen el entorno de análisis, cuyo diagrama de alto nivel se aprecia en la Figura 1. Ambas herramientas son utilidades de línea de comandos, lo cual permite que puedan ser integradas en flujos de análisis más amplios. De manera

adicional, el código fuente de estas herramientas se ha liberado bajo licencia GNU/GPLv3 [5, 6].

La herramienta *Windows Memory Extractor* está implementada en C++ y es una utilidad versátil, ya que puede extraer tanto módulos completos como regiones de memoria que cuenten con unas protecciones determinadas. Por su parte, la herramienta *IM Artifact Finder* se ha desarrollado en Python y no se ha confeccionado únicamente para analizar *Telegram Desktop*, sino que se ha desarrollado como un *framework* que pueda ser extensible a otras aplicaciones de MI.

Resultados y discusión

De cara a identificar artefactos relevantes desde un punto de vista forense se ha analizado el código fuente de *Telegram Desktop*, el cual se distribuye de manera libre. Para encontrar en un volcado de memoria objetos de interés se han realizado búsquedas de patrones de números de teléfono y de patrones horarios. Una vez que se han encontrado objetos, se han identificado dentro de ellos punteros a otros objetos, y de esta manera se han podido identificar nuevos objetos de interés para el análisis forense.

Mediante el entorno de análisis elaborado se ha conseguido saber el número de cuentas añadidas a la aplicación e información acerca de sus correspondientes propietarios. Por otro lado, es posible la reconstrucción de conversaciones a las que el usuario ha accedido, tanto en el caso de conversaciones individuales como en el caso de grupos y canales. En cuanto a los usuarios, se han logrado detectar aquellos que comparten su número de teléfono y también algunos que no lo comparten, siendo posible diferenciar si un usuario es un contacto o no. Adicionalmente, se ha podido recuperar información tras eliminar tanto contactos como conversaciones, tras bloquear la aplicación y tras cerrar sesión.

La posibilidad de recuperar esta información presente en la memoria volátil de un ordenador incautado puede proporcionar a un analista forense evidencias cruciales para la resolución de un caso. Entre otros, el hecho de saber datos sobre el propietario de una cuenta puede ayudar a identificar a quién pertenece un equipo. Por otra parte, la identificación de contactos puede proporcionar individuos relacionados con un sospechoso a los que poder investigar. De manera adicional, se considera importante la recuperación de información a la que un analista forense no podría acceder desde la interfaz de usuario, como los contactos borrados.

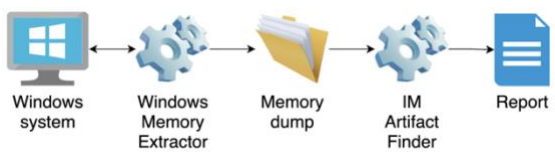

Figura 1: Diagrama de alto nivel del entorno de análisis

Conclusiones

En este proyecto se ha elaborado un entorno de análisis destinado a la obtención de artefactos forenses presentes en la memoria RAM del proceso de *Telegram Desktop* en sistemas Windows. Los resultados obtenidos tras la evaluación de dicho entorno han proporcionado una serie de artefactos relacionados con *Telegram Desktop* cuya relevancia puede ser notable de cara a la resolución de un caso forense.

REFERENCIAS

[1]. THANTILAGE, R. D. y LE KHAC, N. A. Framework for the Retrieval of Social Media and Instant Messaging Evidence from Volatile Memory. *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 13th IEEE International Conference On Big Data Science And Engineering (TrustCom / BigDataSE)*. 2019, págs. 476-482.

[2]. GREGORIO, J.; ALARCOS, B. y GARDEL, A. Forensic analysis of Telegram Messenger Desktop on macOS. *International Journal of Research in Engineering and Science*. 2018, vol. 6, núm. 8, págs. 39-48.

[3]. SATRYA, G. B.; DAELY, P. T. y SHIN, S. Y. Android forensics analysis: Private chat on social messenger. *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*. 2016, págs. 430-435.

[4]. Evolución de la cuota de mercado de las versiones del sistema operativo Windows [Online: https://www.statista.com/statistics/993868/worldwide-windowsoperating-system-market-share/]. 2021. Accedido el 28/09/2021.

[5]. Herramienta Windows Memory Extractor [Online: https://github.com/pedrofdez26/windows-memory-extractor]. 2021. Accedido el 27/09/2021.

[6]. Herramienta Instant Messaging Artifact Finder [Online: https://github.com/pedrofdez26/instant-messaging-artifact-finder]. 2021. Accedido el 27/09/2021.