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), Universidad de Zaragoza, España

Instituto Universitario de Investigación en Ingeniería de Aragón
Universidad Zaragoza

X JORNADA DE JÓVENES INVESTIGADORES DEL I3A

Introducción

- Aplicaciones de **mensajería instantánea** (MI)
  - Permiten comunicarse de una manera rápida y cómoda
  - Usadas por una parte notable de la sociedad
  - Empleadas en ocasiones para **cometer o esclarecer delitos**
- Análisis forense de los dispositivos del criminal o de la víctima de un crimen para **obtener evidencias**
- **Cifrado** de las bases de datos locales y de comunicaciones **dificulta** la obtención de evidencias
  - **Los contenidos en la memoria RAM están descifrados para que la aplicación trabaje con ellos**
- **Telegram**: **Top 5 de plataformas de MI más populares**
- `Telegram Desktop`: Cliente multiplataforma oficial de Telegram

Objetivo

- Investigar los contenidos en memoria RAM relativos a `Telegram Desktop` (en Windows 10) de cara a **identificar artefactos digitales** de interés para una investigación forense

Entorno de Análisis

- **Elaborado entorno de análisis** (diagrama de alto nivel en la Figura 1) compuesto por dos herramientas de línea de comandos:
  - Herramienta `Windows Memory Extractor` [1]
    - **Obtención** del volcado de un proceso en un sistema Windows
    - El formato de la salida generada permite identificar la localización con la que se corresponden las direcciones virtuales del proceso
    - **Versátil**: Extracción de módulos completos o de regiones de memoria que cuenten con unas protecciones determinadas
  - Herramienta `IM Artifact Finder` [2]
    - **Análisis** del volcado de un proceso relativo a una aplicación de MI
    - Generación de un informe con la información de los artefactos forenses obtenidos
    - **Desarrollada como framework** extensible a otras aplicaciones de MI, además de `Telegram Desktop`
- Código fuente de ambas herramientas bajo **licencia GNU/GPLv3**

Resultados

- Identificación de artefactos de memoria
  - Analizada la versión 2.7.1 de `Telegram Desktop` [3] (extracto del diagrama de clases en la Figura 2)
  - Búsquedas de patrones de **números de teléfono** (atributo *_phone* de la clase *UserData*) y de **patrones horarios** (atributo *_timeText* de la clase *HistoryMessage*)
  - **Identificación de punteros** dentro de los objetos encontrados para obtener nuevos objetos de interés
- Información obtenida de mayor relevancia:
  1. Número de **cuentas** añadidas a la aplicación
  2. Información acerca de **propietarios** de las cuentas
  3. **Reconstrucción de conversaciones** accedidas
  4. Detección de **usuarios que comparten su número de teléfono** y también de algunos que no lo comparten
  5. **Recuperación (parcial) de artefactos después de**:
     - Eliminar contactos y conversaciones
     - Bloquear la aplicación
     - Cerrar sesión de la aplicación

Discusión

- Esta información de un ordenador incautado puede proporcionar **evidencias cruciales para resolución de un caso forense**
  - **Identificar a quién pertenece un equipo**
  - **Individuos relacionados con un sospechoso**
  - **Recuperar artefactos inaccesibles desde interfaz de usuario**

Diagramas

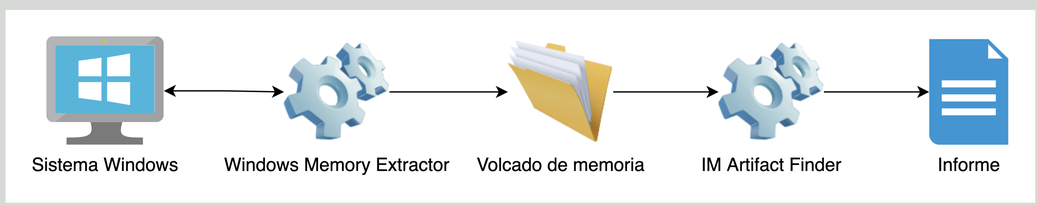

Figura 1: Diagrama de alto nivel del entorno de análisis

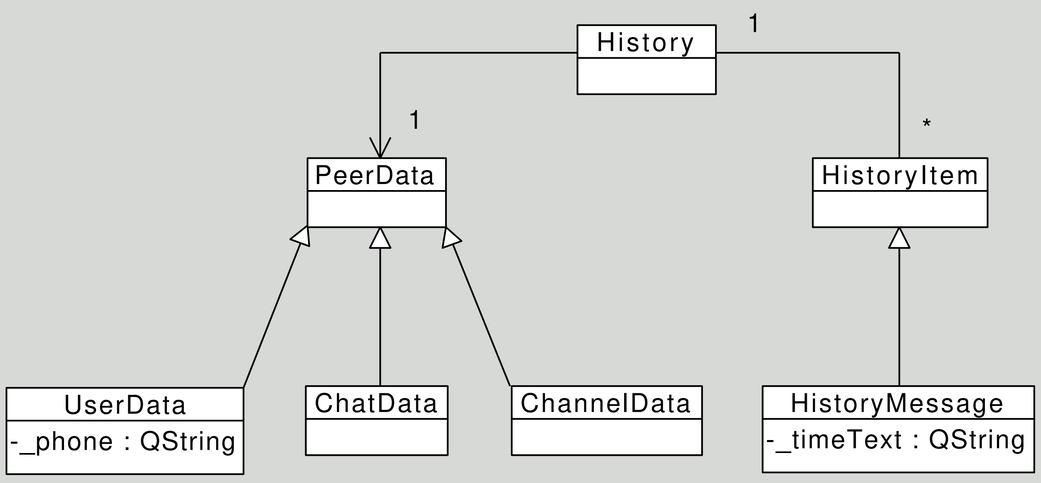

Figura 2: Extracto del diagrama de clases de `Telegram Desktop`

Conclusiones

- Elaborado un entorno de análisis para **obtención de artefactos forenses de la memoria RAM** del proceso de `Telegram Desktop`
- Extracción de artefactos relacionados con `Telegram Desktop` **de relevancia notable para la resolución de un caso forense**

Referencias

[1] Herramienta Windows Memory Extractor.
[Online: `https://github.com/pedrofdez26/windows-memory-extractor`], 2021.
Accedido el 18 de octubre de 2021.

[2] Herramienta IM Artifact Finder.
[Online: `https://github.com/pedrofdez26/instant-messaging-artifact-finder`], 2021.
Accedido el 18 de octubre de 2021.

[3] Código fuente de la versión 2.7.1 de Telegram Desktop.
[Online: `https://github.com/telegramdesktop/tdesktop/releases/tag/v2.7.1`], 2021.
Accedido el 17 de octubre de 2021.

Más Información

- Si desea saber más, contacte mediante correo electrónico: pfernandez@unizar.es