Herramientas Línea del Tiempo

Timesketch

Timesketch es una herramienta de análisis de línea de tiempo forense colaborativa de código abierto. Utiliza la búsqueda de texto completo para darle una idea de sus líneas de tiempo. Puede buscar cientos de millones de eventos en diferentes líneas de tiempo al mismo tiempo. Comparta sus hallazgos utilizando vistas guardadas y agregue significado a sus datos con etiquetas y comentarios. Dale vida a tu investigación con Timesketch Stories. Timesketch se basa en la colaboración, el intercambio y la búsqueda.

Comandos:

El comando *tsctl* nos permite controlar *timesketch,* para iniciar el servidor utilizamos el siguiente comando:

tsctl runserver -c /etc/timesketch.conf

Para agregar un usuario:

tsctl add_user

Con los parámetros:

--name / -n

--password / -p (opcional)

Para agregar un grupo utilizamos el siguiente comando:

tsctl add_group

Con el parámetro:

--name / -n

Para eliminar grupos aún no está implementado.

Para gestionar la membresía del grupo (agregar o eliminar un usuario del grupo) debemos especificar el grupo y el usuario:

tsctl manage_group

Con los parámetros:

--remove / -r (optional)

--group / -g

--user / -u

Podemos agregar un nuevo índice de búsqueda:

tsctl add_index

Con los parámetros:

--name / -n

--index / -i

--user / -u

Para migrar una base de datos:

tsctl db

Para eliminar una base de datos (se eliminarán todas las bases de datos):

tsctl drop_db

Para importar json a Timesketch

tsctl json2ts

Para purgar:

tsctl purge

Para exportar/importar plantillas de búsqueda a/desde un archivo:

tsctl search_template

Con los parámetros:

--import / -i

--export / -e

Para crear una nueva línea de tiempo de Timesketch a partir de un archivo. Los formatos de archivo admitidos son: plaso, csv y jsonl.

tsctl import

Con los parámetros:

--file / -f

--sketch_id / -s (optional)

--username / -f (optional)

--timeline_name / -n (optional)

Opciones: Cuenta con diferentes opciones, ya que la mayoría de los comandos permite ejecutarse con diferentes opciones.

Restricciones: No permite eliminar grupos.

Salida del comando: Permite la salida en diferentes formatos

- JSON File
- JSONL File
- CSV File
- Por interfaz gráfica

Ventajas: Al contar con una interfaz gráfica podemos visualizar la información de manera más clara ya que facilita su visualización.

Plaso

Aunque inicialmente se creó el plaso para reemplazar la versión Perl de log2timeline, su enfoque ha cambiado de una herramienta independiente a un conjunto de módulos que se pueden usar en varios casos de uso. Actualmente estos son:

- image_export: Es una herramienta de línea de comandos para exportar contenido de archivos desde una imagen o dispositivo de medios de almacenamiento en función de varios criterios de filtro, como nombres de extensiones, rutas de filtros, identificadores de firmas de formatos de archivos, fecha de creación de archivos y rangos de tiempo, etc.
- log2timeline: Es una herramienta de línea de comandos para extraer eventos de archivos individuales, recurriendo a un directorio (por ejemplo, un punto de montaje) o una imagen o dispositivo de medios de almacenamiento. log2timeline crea un archivo de almacenamiento plaso que puede analizarse con las herramientas pinfo y psort. El archivo de almacenamiento de plaso contiene los eventos extraídos y varios metadatos sobre el proceso de recopilación junto con la información recopilada de los datos de origen. También puede contener información sobre etiquetas aplicadas a eventos e informes de complementos de análisis.
- pinfo: Es una herramienta de línea de comandos para proporcionar información sobre el contenido de un archivo de almacenamiento de plaso.
- psort: Es una herramienta de línea de comandos para postprocesar archivos de almacenamiento de plaso. Le permite filtrar, ordenar y ejecutar el análisis automático de los contenidos de los archivos de almacenamiento de plaso.
- psteal: Es una herramienta de línea de comandos que combina la funcionalidad de log2timeline y psort.

Comandos:

Para crear una línea de tiempo utilizamos el siguiente comando, creando un archivo csv:

psteal.py --source ~/cases/greendale/registrar.dd -o l2tcsv -w /tmp/registrar.csv

Parámetros:

--source

SALIDA -w

FILTROS --file-filter --artifact-filters

LOGS --log-file

DEBUG –debug

Salida:

- xlsx: hoja de cálculo de Excel (XLSX)
- Guarda los datos en una base de datos SQLite, utilizada por la herramienta 4n6time.
- kml: Guarda eventos con datos geográficos en un formato KML
- json: guarda los eventos en un formato JSON.
- nulo: módulo de salida que no genera nada
- json_line: guarda los eventos en un formato de línea JSON.

Ventaja: Al contar con diferentes formatos de salida, nos permite utilizar el que más convenga al análisis, permitiéndonos una mayor flexibilidad de uso.

Comentario

La realización de una línea de tiempo es primordial para la realización de un buen análisis forense y al contar con diferentes opciones para realizarlo nos permite seleccionar el adecuado para la realización de un buen análisis forense, ya que cada uno nos proporciona ciertas características, las cuales serán necesarias para diferentes análisis forenses.

Referencias

http://timesketch.org/

https://github.com/google/timesketch

https://github.com/google/timesketch/blob/master/docs/Users-Guide.md

https://plaso.readthedocs.io/en/latest/sources/user/Users-Guide.html#the-tools