Tarea 2.

Herramienta timeline.

Log2timeline

log2timeline -z <system-timezone> -f <type-input> filename -w timeline.csv

Opciones:

-f <Type-input> define el formato de entrada

-o <type output> define el formato de salida

-w <file> agregar resultados al log actual

-z <system timezone> timezone del sistema

-Z <output timezone> timezone de salida

-r modo recursivo

-p (se usa con –r) son modulos que buscan a través de la unidad sospechosa y extraen información necesaria para otros modulos.

La salida es un archivo tipo excel con terminación csv.

Referencia:

https://www.sans.org/blog/digital-forensic-sifting-targeted-timeline-creation-and-analysis-using-log2timeline/