Introduction

simple-evtx is a fork of @EricRZimmerman's excellent Event log parser and command line tool.

Whilst I use the original version with the maps functionality I also need a really simple version, one that only provides the payload, and minimal other data for when I have lots (20+ hosts) of Event logs to parse, aggregate, and then search, resulting in a CSV file of over 20 GB. The output from simple-evtx allows me to use LogViewer to get rid of noise, reducing the data set, then as I have the JSON payload I can use sift or grep to pull out precise items from the JSON payload.

The only other change than removing columns and maps is to allow the selection of from/to timestamps using the **--from** and **--to** parameters.

Note: this tool is designed to implement a different workflow to EvtxCmd, and not replace it 😉