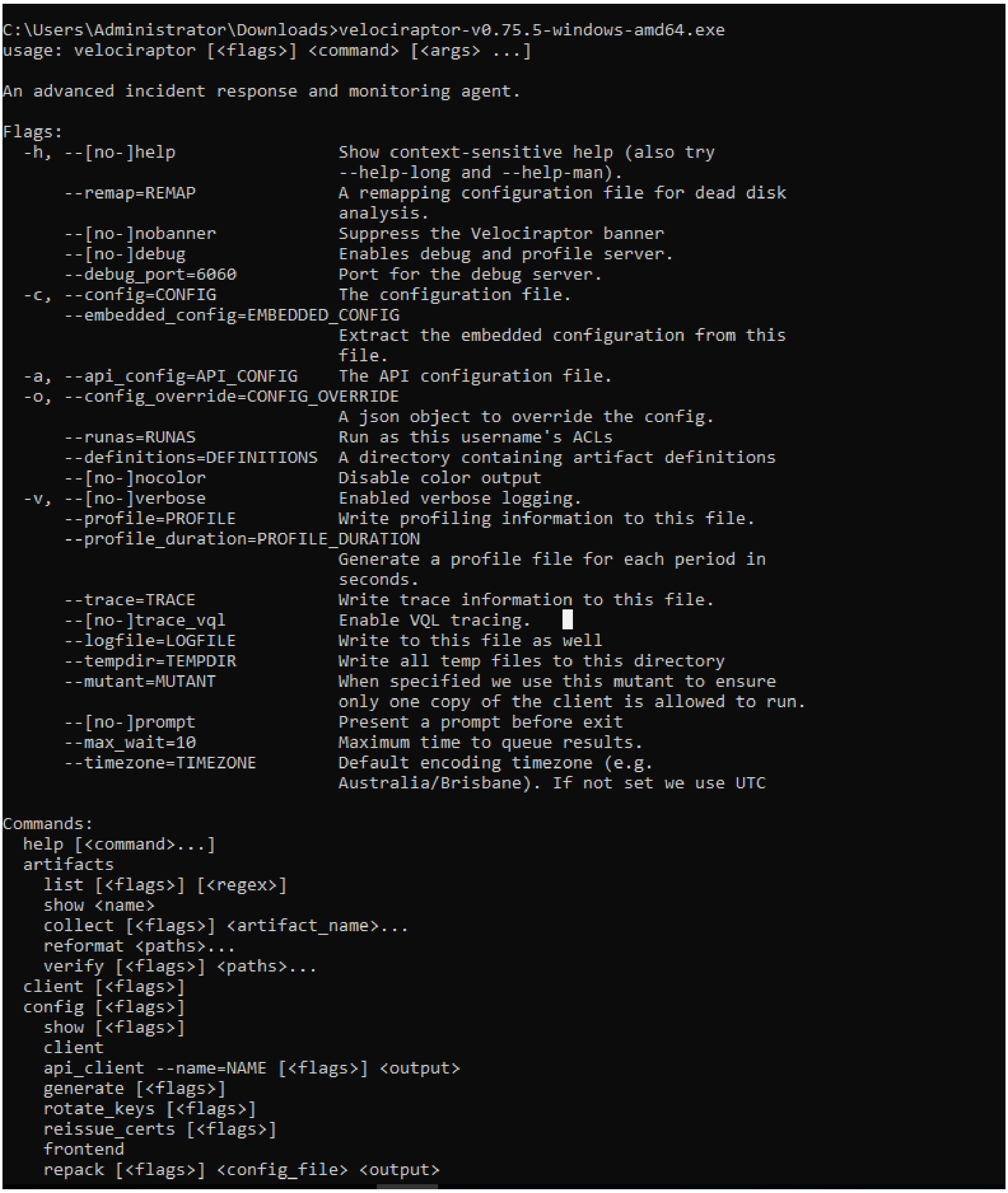
Evidence Preservation

Velociraptor:

Velociraptor is an advanced digital forensic and incident response tool that enhances your visibility into your endpoints.



```
C:\Users\Administrator\Downloads>velociraptor-v0.75.5-windows-amd64.exe
usage: velociraptor [<flags>] <command> [<args> ...]

An advanced incident response and monitoring agent.

Flags:
  -h, --[no-]help                Show context-sensitive help (also try
                                 --help-long and --help-man).
      --remap=REMAP              A remapping configuration file for dead disk
                                 analysis.
      --[no-]nobanner            Suppress the Velociraptor banner
      --[no-]debug               Enables debug and profile server.
      --debug_port=6060          Port for the debug server.
  -c, --config=CONFIG            The configuration file.
      --embedded_config=EMBEDDED_CONFIG
                                 Extract the embedded configuration from this
                                 file.
  -a, --api_config=API_CONFIG    The API configuration file.
  -o, --config_override=CONFIG_OVERRIDE
                                 A json object to override the config.
      --runas=RUNAS              Run as this username's ACLs
      --definitions=DEFINITIONS  A directory containing artifact definitions
      --[no-]nocolor             Disable color output
  -v, --[no-]verbose             Enabled verbose logging.
      --profile=PROFILE          Write profiling information to this file.
      --profile_duration=PROFILE_DURATION
                                 Generate a profile file for each period in
                                 seconds.
      --trace=TRACE              Write trace information to this file.
      --[no-]trace_vql           Enable VQL tracing.
      --logfile=LOGFILE          Write to this file as well
      --tempdir=TEMPDIR          Write all temp files to this directory
      --mutant=MUTANT            When specified we use this mutant to ensure
                                 only one copy of the client is allowed to run.
      --[no-]prompt              Present a prompt before exit
      --max_wait=10              Maximum time to queue results.
      --timezone=TIMEZONE        Default encoding timezone (e.g.
                                 Australia/Brisbane). If not set we use UTC

Commands:
  help [<command>...]
  artifacts
    list [<flags>] [<regex>]
    show <name>
    collect [<flags>] <artifact_name>...
    reformat <paths>...
    verify [<flags>] <paths>...
  client [<flags>]
  config [<flags>]
    show [<flags>]
    client
    api_client --name=NAME [<flags>] <output>
    generate [<flags>]
    rotate_keys [<flags>]
    reissue_certs [<flags>]
    frontend
    repack [<flags>] <config_file> <output>
```

Chain-of-Custody Documentation Template:

Item	Description	Collected By	Date	Hash Value
Memory Dump	Server-X Dump	SOC Analyst	2025-08-18	<SHA256>
Netstat CSV	Live network connections	SOC Analyst	2025-08-18	<SHA256>