INFO SHEET

Digital Guardian WINGMAN

Forensic Artifact Collection Tool for Windows

During an incident, its critical to collect all necessary forensic data to properly investigate and scope an intrusion. With DG Wingman you can instantly perform this function to extract key forensic artifacts such as the master file table ($MTF), Windows registry, and Windows events logs for further analysis. You also have the option to execute custom commands as SYSTEM, or run a full scan of the endpoint and collect metadata from portable executable files such as hashes, certificates, and more.

DG Wingman is a go-to utility in your security arsenal for Incident Response!

This utility was developed by the Digital Guardian ATAC (Advanced Threat & Analysis Center) team that delivers our Managed Detection & Response service. For feedback, comments, or questions please contact the ATAC team at: wingman@digitalguardian.com

Types of Artifacts Collected

- System Information
  - Prefetch
  - Named Objects
  - Scheduled Tasks
  - Etc.
- Active Scan Data
  - Open Handles
  - Recently Opened/Recently Closed Files
- Static Scan Data
  - Binary Attribute / Version Information
  - Binary Import/Export Sections
  - Strings
  - Digital Certificate Information
- WMI Data
- Network Information
- Event Log Entries
  - System Event Log
  - Application Event Log
  - Security Event Log
  - Terminal Services Log
- Registry Hives
  - System Hive
  - Software Hive
  - Security Hive
  - SAM Hive
  - NTUSER Hives
- Master File Table
- Network Information
- Web History

Example Usage

Help Menu
wingman.exe /h

Collect Master File Table and Registry
wingman.exe -mft -r

Collect Web History Data
wingman.exe -b -bf BrowserHistoryFiles.dat

Note: BrowserHistoryFiles.dat contains the location of all web history files. This config file can be modified to suit your needs.

Collect Static Scan Data from PE files in Windows Temp Directory
wingman.exe -e -f c:\windows\temp

Execute a Custom Command to Acquire Running Services
wingman.exe -ac “wmic service get /format:list”

By default, the output will create a folder titled EDR at the root of where the tool is executed from; and will then create a compressed file of the evidence. The ‘-x’ flag can be used to configure a different location.

To download DG Wingman today, visit: https://info.digitalguardian.com/wingman.html