Cheatography

Forensique Windows Cheat Sheet

by KorielZeth (Outis) via cheatography.com/188050/cs/39222/

Informations liés au système

SOFTWARE-\Microsoft\Windows NT\CurrentVersion	Information généralistes
SYSTEM\CurrentControlSet	Control Set actuel
SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName	Nom de la machine
SYSTEM\CurrentControlSet\Control\TimeZoneInformation	Fuseau horaire
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces	Interfaces réseaux
SOFTWARE-\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged	Réseaux utilisés
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run(Once)	Programmes lancés au démarrage
SOFTWARE-\Microsoft\Windows\CurrentVersion\Run(Once)	Programmes lancés au démarrage (2)
HKEY_LOCAL_MACHINE\SAM	Base de données SAM

Utilisation de fichiers et dossiers

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\	Dernier fichiers utilisés par l'utilisateur
NTUSER.DAT\Software\Microsoft\Office\	Documents ouvert via Office
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\	Fichiers utilisés par les boîtes de dialogue
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths	Barre de recherche Windows Explorer
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery	Barre de recherche Windows Explorer (2)

Exécution de programmes

NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\[GUID]\Count	Programmes lancés sur la machine
Amcache.hve-\Root\File\[GUID du volume]\	Programmes récemment exécutés

Exécution de programmes (cont)

SYSTEM\CurrentControlSet\Services\[bam/-dam]\UserSettings\[SID]	Programmes récemment exécutés (2)

Périphériques tiers

SYSTEM\CurrentControlSet\Enum\USB	Périphériques USB (1)
SYSTEM\CurrentControlSet\Enum-\USBSTOR	Périphériques USB (2)
SOFTWARE\Microsoft\Windows Portable Devices\Devices	Périphériques USB (3)