Certified CyberDefender Cheat Sheet [Forensics]

This cheat sheet is for CCD students who are getting ready for the exam.

Important Artifacts

Live system	Dead system	Investigation tool
HKEY_LOCAL_MACHINE/SYSTEM	C:\Windows\System32\config\SYSTEM	Registry Explorer / Regrip
HKEY_LOCAL_MACHINE/SOFTWARE	C:\Windows\System32\config\SOFTWARE	Registry Explorer / Regrip
HKEY_USERS	C:\Windows\System32\config\SAM	Registry Explorer / Regrip
HKEY_CURRENT_USER	C:\Users<USER>\NTUSER.dat C:\Users<user>\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat	Registry Explorer / Regrip
Amcache.hve	C:\Windows\appcompat\Programs\Amcache.hve	Registry Explorer / Regrip
Event viewer -> Windows Logs -> SECURITY	C:\Windows\winevt\Logs\Security.evtx	Event logs Explorer
Event viewer -> Windows Logs -> SYSTEM	C:\Windows\winevt\Logs\SYSTEM.evtx	Event logs Explorer
Event viewer -> Windows Logs -> Application	C:\Windows\winevt\Logs\Application.evtx	Event logs Explorer

Event viewer -> Applications & service logs -> Microsoft -> Windows -> TaskScheduler -> Operational	Microsoft-Windows-TaskScheduler%4Operational.evtx	Event Log Explorer
Event viewer -> Applications & service logs -> Microsoft -> Windows -> TaskScheduler -> Operational	Microsoft-Windows-TaskScheduler%4Operational.evtx	Event Log Explorer

System Information

What to look for?	**Where to find it?**	**Investigation tool**
• Windows version and installation date	• SOFTWARE\Microsoft\Windows NT\CurrentVersion	• Registry Explorer / Regrip
• Computer name	• SYSTEM\ControlSet001\Control\ComputerName\ComputerName	• Registry Explorer / Regrip
• Timezone	• SYSTEM\ControlSet001\Control\TimeZoneInformation	• Registry Explorer / Regrip

Network Information

What to look for?	Where to find it?	Investigation tool
• Identify physical cards	• SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards	• Registry Explorer / Regrip
• Identify interface configuration	• SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces	• Registry Explorer / Regrip
• Connections History	• SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged • SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles • Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx	• WifiHistoryView

Users Information

What to look for?	Where to find it?	Investigation tool
Username, creation date ,login date, SID	• SAM	• RegistryExplorer • Regrip

Login, logout, deletion, creation	• Security.evtx
	  ○ 4624 -> Successful logon event
	  ○ 4625 -> failed logon event
	  ○ 4634 -> Session terminated
		• EventLog Explorer

	○ 4647 -> User initiated logoff ○ 4672 -> Special privilege logon ○ 4648 -> User run program as another user (Runas administrator) ○ 4720/4726 -> Account creation/deletion	
Username, creation date ,login date, SID	• SAM	• RegistryExplorer • Regrip

File Activities - what happened?

What to look for?	**Where to find it?**	**Investigation tool**
File name, path, timestamps, actions (i.e rename)	• $MFT, $LogFile, $UsnJrnl:$J	• NTFS Log Tracker
Information about deleted files	• $I30	• INDXRipper

File Activities - who did it?

What to look for?	Where to find it?	Investigation tool

Failed/Succesful object access	• Securit.evtx
	  ○ 4656 -> User tried to access an object
	  ○ 4660 -> object was deleted
	  ○ 4663 -> User accessed the object successfuly
	  ○ 4658 -> the user closed the opened object (file)
		• EventLog Explorer

Recently used files/folders	• NTUSER.dat
	  ○ Software\Microsoft\Office\15.0<Office application>\File MRU
	  ○ Software\Microsoft\Office\15.0<Office application>\Place MRU
	  ○ Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU*
	  ○ Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
	  ○ Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
	  ○ Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths
		• RegistryExplorer
		• regrip

Accessed folders	• ShellBags
	  ○ NTUSER.dat
	  ○ USRCLASS.dat
		• Shellbags Explorer

Accessed files, its path, metadata, timestamps, drive letter	• LNK files
	  ○ C:\Users<User>\Appdata\Roaming\Microsoft\Windows\Recent
	  ○ C:\Users<User>\Desktop
	  ○ C:\Users<User>\AppData\Roaming\Micros
		• LECmd

	oft\Office\Recent\	

Frequently accessed files	• JumpLists
	  ○ C:\Users<User>\AppData\Roaming\Microsoft\ Windows\Recent\AutomaticDestinations
	  ○ C:\Users<User>\AppData\Roaming\Microsoft\ Windows\Recent\CustomDestinations
		• JumpLists Explorer

Connected Devices

What to look for?	**Where to find it?**	**Investigation tool**
Vendor ID, Product ID, Serial Number, Device name	SYSTEM\ControlSet001\Enum\USB	• RegistryExplorer • Regrip
Serial Number, First connection time, last connection time, last removal time	SYSTEM\ControlSet001\USBSTOR	• RegistryExplorer • Regrip
USB Label	SYSTEM\ControlSet001\Enum\SWD\WPDBUSENUM	• RegistryExplorer • Regrip
GUID, TYPE, serial number	SYSTEM\ControlSet001\Control\DeviceClasses	• RegistryExplorer • Regrip

VolumeGUID, Volume letter, serial number	SYSTEM\MountedDevices SOFTWARE\Microsoft\Windows Portable Devices\Devices SOFTWARE\Microsoft\Windows Search\VolumeInfoCache	• RegistryExplorer • Regrip
Serial number, first connection time	setupapi.dev.log	• notepad++

Serial number, connections times, drive letter	• SYSTEM.evtx
	  ○ 20001 -> a new device is installed
	• Security.evtx
	  ○ 6416 -> new externel device recognized
	• Microsoft-Windows-Ntfs%4Operational.evtx
		• EventLog Explorer

Automation	• Registry • EventLogs • setupapi.dev.log	• USBDeviceForensics • USBDetective

Execution Activities

What to look for?	**Where to find it?**	**Investigation tool**
Windows Services executable, date added	• SYSTEM\CurrentControlSet\Services	• RegistryExplorer • Regrip

Service installation time, Service crashed, stop/start service event	• Security.evtx
	  ○ 4697 -> service gets installed
	• SYSTEM.evtx
	  ○ 7034 -> Service crashed
	  ○ 7035 -> start/stop requests
	  ○ 7036 -> service stoppped/started
		• Eventlog Explorer

Autorun applications	• SOFTWARE\Microsoft\Windows\CurrentVersion\Run • SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce • SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run • SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce • NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run • NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce	• RegistryExplorer • regrip
Frequently run programs, last time, number of execution	• UserAssist ○ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist	• UserAssist by didier steven
Run of older applications on newer system	• SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache	• ShimCache parser
Files path, md5 & sha1 hash	• Amcache.hve	• Amcache parser
Background applications	• BAM & DAM ○ SYSTEM\ControlSet001\Services\bam\State\UserSettings	• RegistryExplorer • regrip

Filename, size, run count, each run timestamp, path	• Prefetch • C:\Windows\Prefetch	• WinPrefetchView
Program network usage, memory usage	• SRUM • C:\Windows\System32\sru\SRUDB.dat	• SrumECmd
Scheduled task	• C:\Windows\Tasks • Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tasks • Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tree • Microsoft-Windows-TaskScheduler%4Operational.evtx	• Task Scheduler Viewer