

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
<ul style="list-style-type: none"> Windows version and installation date 	<ul style="list-style-type: none"> SOFTWARE\Microsoft\Windows NT\CurrentVersion 	<ul style="list-style-type: none"> Registry Explorer / Regrip
<ul style="list-style-type: none"> Computer name 	<ul style="list-style-type: none"> SYSTEM\ControlSet001\Control\ComputerName\ComputerName 	<ul style="list-style-type: none"> Registry Explorer / Regrip
<ul style="list-style-type: none"> Timezone 	<ul style="list-style-type: none"> SYSTEM\ControlSet001\Control\TimeZoneInformation 	<ul style="list-style-type: none"> Registry Explorer / Regrip

Network Information

What to look for?	Where to find it?	Investigation tool
<ul style="list-style-type: none"> Identify physical cards 	<ul style="list-style-type: none"> SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards 	<ul style="list-style-type: none"> Registry Explorer / Regrip
<ul style="list-style-type: none"> Identify interface configuration 	<ul style="list-style-type: none"> SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces 	<ul style="list-style-type: none"> Registry Explorer / Regrip
<ul style="list-style-type: none"> Connections History 	<ul style="list-style-type: none"> SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx 	<ul style="list-style-type: none"> WifiHistoryView

Users Information

What to look for?	Where to find it?	Investigation tool
Username, creation date ,login date, SID	<ul style="list-style-type: none"> SAM 	<ul style="list-style-type: none"> RegistryExplorer Regrip
Login, logout, deletion, creation	<ul style="list-style-type: none"> Security.evtx <ul style="list-style-type: none"> 4624 -> Successful logon event 4625 -> failed logon event 4634 -> Session terminated 	<ul style="list-style-type: none"> EventLog Explorer

	<ul style="list-style-type: none"> ○ 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	<ul style="list-style-type: none"> ● SAM 	<ul style="list-style-type: none"> ● RegistryExplorer ● Regrip

File Activities - what happened?

What to look for?	Where to find it?	Investigation tool
File name, path, timestamps, actions (i.e rename)	<ul style="list-style-type: none"> ● \$MFT, \$LogFile, \$UsnJrnl:\$J 	<ul style="list-style-type: none"> ● NTFS Log Tracker
Information about deleted files	<ul style="list-style-type: none"> ● \$I30 	<ul style="list-style-type: none"> ● INDXRipper

File Activities - who did it?

What to look for?	Where to find it?	Investigation tool
Failed/Succesful object access	<ul style="list-style-type: none"> Securit.evtx <ul style="list-style-type: none"> 4656 -> User tried to access an object 4660 -> object was deleted 4663 -> User accessed the object successfully 4658 -> the user closed the opened object (file) 	<ul style="list-style-type: none"> EventLog Explorer
Recently used files/folders	<ul style="list-style-type: none"> NTUSER.dat <ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> RegistryExplorer regrip
Accessed folders	<ul style="list-style-type: none"> ShellBags <ul style="list-style-type: none"> NTUSER.dat USRCLASS.dat 	<ul style="list-style-type: none"> Shellbags Explorer
Accessed files, its path, metadata, timestamps, drive letter	<ul style="list-style-type: none"> LNK files <ul style="list-style-type: none"> C:\Users<User>\Appdata\Roaming\Microsoft\Windows\Recent C:\Users<User>\Desktop C:\Users<User>\AppData\Roaming\Micros 	<ul style="list-style-type: none"> LECcmd

	oft\Office\Recent\	
Frequently accessed files	<ul style="list-style-type: none"> • JumpLists <ul style="list-style-type: none"> ○ C:\Users<User>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations ○ C:\Users<User>\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • RegistryExplorer • Regrip
Serial Number, First connection time, last connection time, last removal time	SYSTEM\ControlSet001\USBSTOR	<ul style="list-style-type: none"> • RegistryExplorer • Regrip
USB Label	SYSTEM\ControlSet001\Enum\SWD\WPDBUSENUM	<ul style="list-style-type: none"> • RegistryExplorer • Regrip
GUID, TYPE, serial number	SYSTEM\ControlSet001\Control\DeviceClasses	<ul style="list-style-type: none"> • RegistryExplorer • Regrip

VolumeGUID, Volume letter, serial number	SYSTEM\MountedDevices SOFTWARE\Microsoft\Windows Portable Devices\Devices SOFTWARE\Microsoft\Windows Search\VolumeInfoCache	<ul style="list-style-type: none"> • RegistryExplorer • Regrip
Serial number, first connection time	setupapi.dev.log	<ul style="list-style-type: none"> • notepad++
Serial number, connections times, drive letter	<ul style="list-style-type: none"> • SYSTEM.evtx <ul style="list-style-type: none"> ◦ 20001 -> a new device is installed • Security.evtx <ul style="list-style-type: none"> ◦ 6416 -> new external device recognized • Microsoft-Windows-Ntfs%4Operational.evtx 	<ul style="list-style-type: none"> • EventLog Explorer
Automation	<ul style="list-style-type: none"> • Registry • EventLogs • setupapi.dev.log 	<ul style="list-style-type: none"> • USBDeviceForensics • USBDetective

Execution Activities

What to look for?	Where to find it?	Investigation tool
Windows Services executable, date added	<ul style="list-style-type: none"> • SYSTEM\CurrentControlSet\Services 	<ul style="list-style-type: none"> • RegistryExplorer • Regrip

Service installation time, Service crashed, stop/start service event	<ul style="list-style-type: none"> • Security.evtx <ul style="list-style-type: none"> ◦ 4697 -> service gets installed • SYSTEM.evtx <ul style="list-style-type: none"> ◦ 7034 -> Service crashed ◦ 7035 -> start/stop requests ◦ 7036 -> service stoppped/started 	<ul style="list-style-type: none"> • Eventlog Explorer
Autorun applications	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • RegistryExplorer • regrip
Frequently run programs, last time, number of execution	<ul style="list-style-type: none"> • UserAssist <ul style="list-style-type: none"> ◦ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist 	<ul style="list-style-type: none"> • UserAssist by didier steven
Run of older applications on newer system	<ul style="list-style-type: none"> • SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache 	<ul style="list-style-type: none"> • ShimCache parser
Files path, md5 & sha1 hash	<ul style="list-style-type: none"> • Amcache.hve 	<ul style="list-style-type: none"> • Amcache parser
Background applications	<ul style="list-style-type: none"> • BAM & DAM <ul style="list-style-type: none"> ◦ SYSTEM\ControlSet001\Services\bam\State\UserSettings 	<ul style="list-style-type: none"> • RegistryExplorer • regrip

Filename, size, run count, each run timestamp, path	<ul style="list-style-type: none"> • Prefetch • C:\Windows\Prefetch 	<ul style="list-style-type: none"> • WinPrefetchView
Program network usage, memory usage	<ul style="list-style-type: none"> • SRUM • C:\Windows\System32\sru\SRUDB.dat 	<ul style="list-style-type: none"> • SrumECmd
Scheduled task	<ul style="list-style-type: none"> • C:\Windows\Tasks • Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tasks • Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tree • Microsoft-Windows-TaskScheduler%4Operational.evtx 	<ul style="list-style-type: none"> • Task Scheduler Viewer