Ng Jong Ray, Edward A02126695U e0540252@u.nus.edu

Challenge 1:

Qn.	Registry Value	Data
1.	SYSTEM\Select\Default	1
	SYSTEM\Select\Current	1
2.	SYSTEM\ControlSet001\Control\ComputerName\ComputerName\ComputerName	IE11WIN8_1
3.	SYSTEM\ControlSet001\Control\SessionManager\Environment\PROCESSOR_ARCHITECTURE	x86
	SYSTEM\ControlSet001\Control\Session Manager\Environment\PROCESSOR_IDENTIFIER	x86 Family 6 Model 60 Stepping 3, GenuineIntel
	SYSTEM\ControlSet001\Control\Session Manager\Environment\NUMBER_OF_PROCESSORS	2
4.	SYSTEM\ControlSet001\Control\TimeZoneInformation\TimeZoneKeyName	Eastern Standard Time
5.	SYSTEM\ControlSet001\Control\Windows\ShutdownTime	C6BA99839C3CD201 2016-11-12 04:23:26 (UTC)
6.	SYSTEM\ControlSet001\Control\Windows\SystemDirectory	%SystemRoot%\system32
7.	SYSTEM\ControlSet001\Services\EventLog\Security\File	%SystemRoot%\System32\winevt\Logs\Security.evtx
8.	SYSTEM\ControlSet001\Services\EventLog\System\File	%SystemRoot%\System32\winevt\Logs\System.evtx
9.	SYSTEM\\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Fit&Rev_2.01\4C530012230531102000&0	SanDisk Cruzer Fit USB Device
10.	SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1D5B7BD9-5379-4025-BB4B-BB2491FECAB3}\DhcpIPAddress	192.168.0.127
	SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1D5B7BD9-5379-4025-BB4B-BB2491FECAB3}\DhcpSubnetMask	255.255.255.0

Ng Jong Ray, Edward A02126695U e0540252@u.nus.edu

Challenge 2:

Qn.	Registry Value	Data
1.	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	Windows 8.1 Enterprise Evaluation
2.	SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner	IEUser
	SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOrganization	No data
3.	SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	0x5260562A 10/17/2013 9:27:06 PM (UTC)
4.	SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser	CFTT
	SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUserSID	S-1-5-21-2968750198-2704521508-3360548841-1002
5.	SOFTWARE\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2968750198-2704521508-3360548841-1001	IEUser
	SOFTWARE\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2968750198-2704521508-3360548841-1003	Forensics
	SOFTWARE\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2968750198-2704521508-3360548841-1005	CFReDS
	SOFTWARE\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2968750198-2704521508-3360548841-1006	cfttu_000
6.	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultUserName	IEUser
	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\DefaultDomainName	IE11WIN8_1
7.	SOFTWARE\Clients\StartMenuInternet\Google Chrome	Google Chrome
	SOFTWARE\Clients\StartMenuInternet\IEXPLORE.EXE	Internet Explorer

8.	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ccleaner.exe	C:\Program Files\CCleaner\CCleaner.exe
	SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ccleaner.exe\Path	C:\Program Files\CCleaner
9.	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VBoxTray	C:\Windows\system32\VBoxTray.exe
	SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Adobe ARM	"C:\Program Files\Common Files\Adobe\ARM\1.0\AdobeARM.exe "
10.	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\1\Description	Microsoft Hyper-V Network Adapter
	SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\5\Description	Intel(R) PRO/1000 MT Desktop Adapter

Ng Jong Ray, Edward A02126695U e0540252@u.nus.edu

Challenge 3:

Qn.	Registry Value	Data
1.	IEUser-NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs\url1	http://go.microsoft.com/fwlink/p/?LinkId=255141
2.	IEUser-NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\b	shutdown.exe -l\1
	IEUser-NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\a	netplwiz\1
3.	IEUser-NTUSER.DAT\Software\Sysinternals\Process Monitor\DbgHelpPath	C:\Windows\system32\dbghelp.dll
	IEUser-NTUSER.DAT\Software\Sysinternals\Process Monitor\Logfile	\\VBOXSVR\VMPOP_SHARED_DIR\temp_6f6a07b223dbd60ed9d80be924de02a032c22ccd\temp_2.pml
4.	CFTT-NTUSER.DAT\Software\7-Zip	7-Zip
	CFTT-NTUSER.DAT\Software\7-Zip\Path	C:\Program Files\7-Zip\
5.	CFTT-NTUSER.DAT\Software\Microsoft\OneDrive\Version	17.3.6390.0509
	CFTT-NTUSER.DAT\Software\Microsoft\OneDrive\CurrentVersionPath	C:\Users\CFTT\AppData\Local\Microsoft\OneDrive\17.3.6390.0509
6.	CFTT-NTUSER.DAT\Software\Netscape\Netscape Navigator\Viewers\application/msword	C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE
7.	CFTT-NTUSER.DAT\Software\Netscape\Netscape Navigator\User Trusted External Applications\C:\Program Files\Adobe\Reader 11.0\Reader\AcroRd32.exe	Yes
8.	CFTT-NTUSER.DAT\Software\Microsoft\Office\16.0\Word\File MRU\Item 1	Raw Data:[F00000000][T01D23C9A2E04EAB1][O00000000]*w:\ND+Samples\dir-1\dir-1-2\document6.docx Document name: document6.docx Time last opened in UTC: Saturday 12th November 2016 04:06:44
	CFTT-NTUSER.DAT\Software\Microsoft\Office\16.0\Word\File MRU\Item 2	Raw Data: [F00000000][T01D23C9A09E70192][O0

		0000000]*w:\ND+Samples\dir-1\dir-1-2\document5.docx Document name: document5.docx Time last opened in UTC: Saturday 12th November 2016 04:05:43
	CFTT-NTUSER.DAT\Software\Microsoft\Office\16.0\Word\File MRU\Item 3	Raw Data: [F00000000][T01D23C934F444921][O00000000]*C:\Users\CFTT\Desktop\RM2+Samples\dir-1\dir-1-2\document6.docx Document name: document6.docx Time last opened in UTC: Saturday 12th November 2016 03:17:33
	CFTT-NTUSER.DAT\Software\Microsoft\Office\16.0\Word\File MRU\Item 4	Raw Data: [F00000000][T01D23C9333FF63C2][O00000000]*C:\Users\CFTT\Desktop\RM2+Samples\dir-1\dir-1-2\document5.docx Document name: document5.docx Time last opened in UTC: Saturday 12th November 2016 03:16:47
9.	CFTT-NTUSER.DAT\Software\Microsoft\Office\16.0\Excel\File MRU\Item 1	Raw Data: [F00000000][T01D23C9A68296862][O00000000]*w:\ND+Samples\dir-1\dir-1-2\document8.xlsx Document name: document8.xlsx Time last opened in UTC: Saturday 12th November 2016 04:08:21