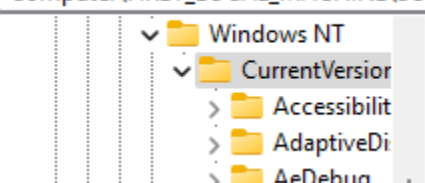
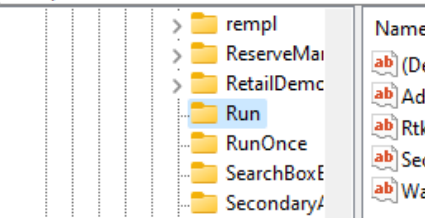
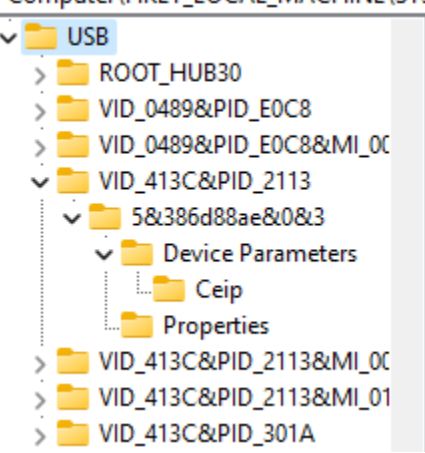
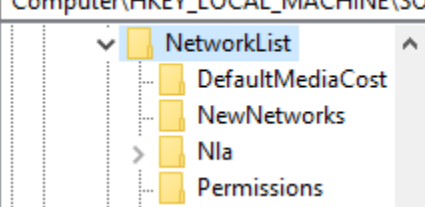
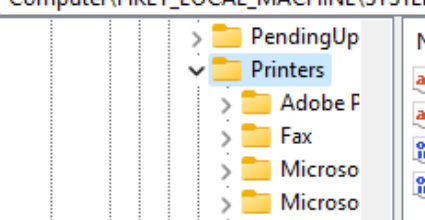
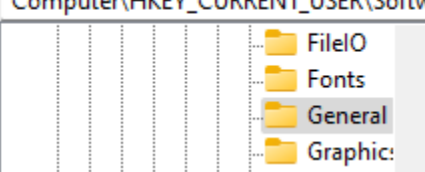


Registry Forensics

What	Where																								
Computer Name	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\OEMInformation</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)																		
Name	Type	Data																							
(Default)	REG_SZ	(value not set)																							
Dynamic Disks	<p>Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\IDConfigDB\CurrentDockInfo</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>AcpiSerialNumber</td> <td>REG_BINARY</td> <td>00 00</td> </tr> <tr> <td>Capabilities</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>DockID</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>DockingState</td> <td>REG_DWORD</td> <td>0x00000001 (1)</td> </tr> <tr> <td>SerialNumber</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)	AcpiSerialNumber	REG_BINARY	00 00	Capabilities	REG_DWORD	0x00000000 (0)	DockID	REG_DWORD	0x00000000 (0)	DockingState	REG_DWORD	0x00000001 (1)	SerialNumber	REG_DWORD	0x00000000 (0)			
Name	Type	Data																							
(Default)	REG_SZ	(value not set)																							
AcpiSerialNumber	REG_BINARY	00 00																							
Capabilities	REG_DWORD	0x00000000 (0)																							
DockID	REG_DWORD	0x00000000 (0)																							
DockingState	REG_DWORD	0x00000001 (1)																							
SerialNumber	REG_DWORD	0x00000000 (0)																							
Install dates	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>InstallationType</td> <td>REG_SZ</td> <td>Client</td> </tr> <tr> <td>InstallDate</td> <td>REG_DWORD</td> <td>0x634568a9 (1665493161)</td> </tr> <tr> <td>InstallTime</td> <td>REG_QWORD</td> <td>0x1d8dd7147a456c7 (133099667610425031)</td> </tr> </tbody> </table>	Name	Type	Data	InstallationType	REG_SZ	Client	InstallDate	REG_DWORD	0x634568a9 (1665493161)	InstallTime	REG_QWORD	0x1d8dd7147a456c7 (133099667610425031)												
Name	Type	Data																							
InstallationType	REG_SZ	Client																							
InstallDate	REG_DWORD	0x634568a9 (1665493161)																							
InstallTime	REG_QWORD	0x1d8dd7147a456c7 (133099667610425031)																							
Last user logged in	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>IdleTime</td> <td>REG_DWORD</td> <td>0x00003190 (12688)</td> </tr> <tr> <td>IsFirstLogonAfter...</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>LastLoggedOnP...</td> <td>REG_SZ</td> <td>{60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}</td> </tr> <tr> <td>LastLoggedOnS...</td> <td>REG_SZ</td> <td>CMVT\adensberger24</td> </tr> <tr> <td>LastLoggedOnUser</td> <td>REG_SZ</td> <td>CMVT\adensberger24</td> </tr> <tr> <td>LastLoggedOnU...</td> <td>REG_SZ</td> <td>S-1-5-21-3338642676-1505485127-1248795149-12327</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)	IdleTime	REG_DWORD	0x00003190 (12688)	IsFirstLogonAfter...	REG_DWORD	0x00000000 (0)	LastLoggedOnP...	REG_SZ	{60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}	LastLoggedOnS...	REG_SZ	CMVT\adensberger24	LastLoggedOnUser	REG_SZ	CMVT\adensberger24	LastLoggedOnU...	REG_SZ	S-1-5-21-3338642676-1505485127-1248795149-12327
Name	Type	Data																							
(Default)	REG_SZ	(value not set)																							
IdleTime	REG_DWORD	0x00003190 (12688)																							
IsFirstLogonAfter...	REG_DWORD	0x00000000 (0)																							
LastLoggedOnP...	REG_SZ	{60B78E88-EAD8-445C-9CFD-0B87F74EA6CD}																							
LastLoggedOnS...	REG_SZ	CMVT\adensberger24																							
LastLoggedOnUser	REG_SZ	CMVT\adensberger24																							
LastLoggedOnU...	REG_SZ	S-1-5-21-3338642676-1505485127-1248795149-12327																							
Mounted devices	<p>Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>??Volume{748...</td> <td>REG_BINARY</td> <td>5c 00 44 00 65 00 76 00 69 00 63 00 65 00 5c 00 56 00...</td> </tr> <tr> <td>\DosDevices\C:</td> <td>REG_BINARY</td> <td>44 4d 49 4f 3a 49 44 3a 80 c8 4c 91 fa 35 ac 40 af d8 ...</td> </tr> <tr> <td>\DosDevices\G:</td> <td>REG_BINARY</td> <td>5c 00 44 00 65 00 76 00 69 00 63 00 65 00 5c 00 56 00...</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)	??Volume{748...	REG_BINARY	5c 00 44 00 65 00 76 00 69 00 63 00 65 00 5c 00 56 00...	\DosDevices\C:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 80 c8 4c 91 fa 35 ac 40 af d8 ...	\DosDevices\G:	REG_BINARY	5c 00 44 00 65 00 76 00 69 00 63 00 65 00 5c 00 56 00...									
Name	Type	Data																							
(Default)	REG_SZ	(value not set)																							
??Volume{748...	REG_BINARY	5c 00 44 00 65 00 76 00 69 00 63 00 65 00 5c 00 56 00...																							
\DosDevices\C:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 80 c8 4c 91 fa 35 ac 40 af d8 ...																							
\DosDevices\G:	REG_BINARY	5c 00 44 00 65 00 76 00 69 00 63 00 65 00 5c 00 56 00...																							
Windows OS product key	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>CurrentMinorVe...</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>CurrentType</td> <td>REG_SZ</td> <td>Multiprocessor Free</td> </tr> <tr> <td>CurrentVersion</td> <td>REG_SZ</td> <td>6.3</td> </tr> <tr> <td>DigitalProductId</td> <td>REG_BINARY</td> <td>a4 00 00 00 03 00 00 00 30 30 33 32 38 2d 31 30 30 3...</td> </tr> <tr> <td>DigitalProductId4</td> <td>REG_BINARY</td> <td>f8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32 00...</td> </tr> <tr> <td>DisplayVersion</td> <td>REG_SZ</td> <td>72H2</td> </tr> </tbody> </table>	Name	Type	Data	CurrentMinorVe...	REG_DWORD	0x00000000 (0)	CurrentType	REG_SZ	Multiprocessor Free	CurrentVersion	REG_SZ	6.3	DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 30 30 33 32 38 2d 31 30 30 3...	DigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32 00...	DisplayVersion	REG_SZ	72H2			
Name	Type	Data																							
CurrentMinorVe...	REG_DWORD	0x00000000 (0)																							
CurrentType	REG_SZ	Multiprocessor Free																							
CurrentVersion	REG_SZ	6.3																							
DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 30 30 33 32 38 2d 31 30 30 3...																							
DigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32 00...																							
DisplayVersion	REG_SZ	72H2																							

Registered owner	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion</p>  <table border="1" data-bbox="747 220 1559 401"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>ProductName</td> <td>REG_SZ</td> <td>Windows 10 Education</td> </tr> <tr> <td>RegisteredOrga...</td> <td>REG_SZ</td> <td>Columbia-Montour AVTS</td> </tr> <tr> <td>RegisteredOwner</td> <td>REG_SZ</td> <td>Columbia-Montour AVTS</td> </tr> </tbody> </table>	Name	Type	Data	ProductName	REG_SZ	Windows 10 Education	RegisteredOrga...	REG_SZ	Columbia-Montour AVTS	RegisteredOwner	REG_SZ	Columbia-Montour AVTS						
Name	Type	Data																	
ProductName	REG_SZ	Windows 10 Education																	
RegisteredOrga...	REG_SZ	Columbia-Montour AVTS																	
RegisteredOwner	REG_SZ	Columbia-Montour AVTS																	
Programs run automatically	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run</p>  <table border="1" data-bbox="747 430 1559 646"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>AdobeAAMUpd...</td> <td>REG_SZ</td> <td>"C:\Program Files (x86)\Common Files\Adobe\OO...</td> </tr> <tr> <td>RtkAudUService</td> <td>REG_SZ</td> <td>"C:\WINDOWS\System32\DriverStore\FileReposito...</td> </tr> <tr> <td>SecurityHealth</td> <td>REG_EXPAND_SZ</td> <td>%windir%\system32\SecurityHealthSystray.exe</td> </tr> <tr> <td>WavesSvc</td> <td>REG_SZ</td> <td>"C:\WINDOWS\System32\DriverStore\FileReposito...</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)	AdobeAAMUpd...	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\OO...	RtkAudUService	REG_SZ	"C:\WINDOWS\System32\DriverStore\FileReposito...	SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe	WavesSvc	REG_SZ	"C:\WINDOWS\System32\DriverStore\FileReposito...
Name	Type	Data																	
(Default)	REG_SZ	(value not set)																	
AdobeAAMUpd...	REG_SZ	"C:\Program Files (x86)\Common Files\Adobe\OO...																	
RtkAudUService	REG_SZ	"C:\WINDOWS\System32\DriverStore\FileReposito...																	
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe																	
WavesSvc	REG_SZ	"C:\WINDOWS\System32\DriverStore\FileReposito...																	
USB devices	<p>Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB</p>  <table border="1" data-bbox="747 676 1559 1125"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)												
Name	Type	Data																	
(Default)	REG_SZ	(value not set)																	
Networks	<p>Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList</p>  <table border="1" data-bbox="747 1155 1559 1360"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>192.228.79.201</td> </tr> <tr> <td>FirstNetwork</td> <td>REG_DWORD</td> <td>0x00000000 (0)</td> </tr> <tr> <td>RootDnsIpv6Addr</td> <td>REG_SZ</td> <td>2001:478:65::53</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	192.228.79.201	FirstNetwork	REG_DWORD	0x00000000 (0)	RootDnsIpv6Addr	REG_SZ	2001:478:65::53						
Name	Type	Data																	
(Default)	REG_SZ	192.228.79.201																	
FirstNetwork	REG_DWORD	0x00000000 (0)																	
RootDnsIpv6Addr	REG_SZ	2001:478:65::53																	
Printers	<p>Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Printers</p>  <table border="1" data-bbox="747 1390 1559 1608"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>(Default)</td> <td>REG_SZ</td> <td>(value not set)</td> </tr> <tr> <td>DefaultSpoolDir...</td> <td>REG_SZ</td> <td>C:\windows\system32\spool\PRINTERS</td> </tr> <tr> <td>LANGIDOfLastD...</td> <td>REG_DWORD</td> <td>0x00000409 (1033)</td> </tr> <tr> <td>ResetDevmodes...</td> <td>REG_DWORD</td> <td>0x00000003 (3)</td> </tr> </tbody> </table>	Name	Type	Data	(Default)	REG_SZ	(value not set)	DefaultSpoolDir...	REG_SZ	C:\windows\system32\spool\PRINTERS	LANGIDOfLastD...	REG_DWORD	0x00000409 (1033)	ResetDevmodes...	REG_DWORD	0x00000003 (3)			
Name	Type	Data																	
(Default)	REG_SZ	(value not set)																	
DefaultSpoolDir...	REG_SZ	C:\windows\system32\spool\PRINTERS																	
LANGIDOfLastD...	REG_DWORD	0x00000409 (1033)																	
ResetDevmodes...	REG_DWORD	0x00000003 (3)																	
Most Recently Used Files	<p>Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\General</p>  <table border="1" data-bbox="747 1638 1559 1808"> <thead> <tr> <th>Name</th> <th>Type</th> <th>Data</th> </tr> </thead> <tbody> <tr> <td>Queries</td> <td>REG_SZ</td> <td>Queries</td> </tr> <tr> <td>RecentFiles</td> <td>REG_SZ</td> <td>Recent</td> </tr> <tr> <td>ShownFirstRun</td> <td>REG_DWORD</td> <td>0x00000000</td> </tr> </tbody> </table>	Name	Type	Data	Queries	REG_SZ	Queries	RecentFiles	REG_SZ	Recent	ShownFirstRun	REG_DWORD	0x00000000						
Name	Type	Data																	
Queries	REG_SZ	Queries																	
RecentFiles	REG_SZ	Recent																	
ShownFirstRun	REG_DWORD	0x00000000																	