|  |  |  |
| --- | --- | --- |
| Evidence A | | |
| Question | Query | Result |
| What operating system was used on the computer? | $ rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/software -p winver | ProductName Microsoft Windows XP  CSDVersion Service Pack 3  BuildLab 2600.xpsp.080413-2111  RegisteredOrganization  RegisteredOwner Jim  InstallDate 2022-08-27 12:13:00Z |
| When was the install date? |  |  |
| What is the time zone settings? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/system -p timezone | Launching timezone v.20200518  timezone v.20200518  (System) Get TimeZoneInformation key contents  TimeZoneInformation key  ControlSet001\Control\TimeZoneInformation  LastWrite Time 2022-08-27 22:10:36Z  DaylightName -> E. Australia Standard Time  StandardName -> E. Australia Standard Time  Bias -> -600 (-10 hours)  ActiveTimeBias -> -600 (-10 hours) |
| Who is the registered owner? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/software -p winver | Launching winver v.20200525  winver v.20200525  (Software) Get Windows version & build info  ProductName Microsoft Windows XP  CSDVersion Service Pack 3  BuildLab 2600.xpsp.080413-2111  RegisteredOrganization  RegisteredOwner Jim  InstallDate 2022-08-27 12:13:00Z |
| What is the computer hostname? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/system -p compname | Launching compname v.20090727  compname v.20090727  (System) Gets ComputerName and Hostname values from System hive  ComputerName = PHELPS-PC  TCP/IP Hostname = Phelps-PC |
| When was the last recorded computer shutdown date/time? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/system -p shutdown | Launching shutdown v.20200518  shutdown v.20200518  (System) Gets ShutdownTime value from System hive  ControlSet001\Control\Windows key, ShutdownTime value  LastWrite time: 2022-08-28 05:29:53Z  ShutdownTime : 2022-08-28 05:29:53Z |
| How many accounts are recorded (total number)? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse | grep Username | Launching samparse v.20200825  Username : Administrator [500]  Username : Guest [501]  Username : HelpAssistant [1000]  Username : SUPPORT\_388945a0 [1002]  Username : Jim [1003] |
| What is the account name of the user who mostly uses the computer? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse | grep -C 9 "Login Count" | Username : Jim [1003]  Full Name : Jim  User Comment :  Account Type : Default Admin User  Account Created : 2022-08-27 12:25:06Z  Name :  Last Login Date : 2022-08-28 05:29:30Z  Pwd Reset Date : 2022-08-27 12:25:22Z  Pwd Fail Date : 2022-08-28 05:29:23Z  Login Count : 3  Embedded RID : 1003  --> Normal user account  --> Password does not expire |
| Who was the last user to logon to the computer? | rip.pl -r /mnt/windows\_mount/WINDOWS/system32/config/SAM -p samparse | grep Login | Launching samparse v.20200825  Last Login Date : 2022-08-27 12:24:26Z  Login Count : 2  Last Login Date : Never  Login Count : 0  Last Login Date : Never  Login Count : 0  Last Login Date : Never  Login Count : 0  Last Login Date : 2022-08-28 05:29:30Z  Login Count : 3 |
| grep -ir "Jim" /mnt/windows\_mount |  |  |
| Recent Docs | $ rip.pl -r /mnt/windows\_mount/Documents\ and\ Settings/Jim/NTUSER.DAT -p recentdocs\_tln | Launching recentdocs\_tln v.20140220  1661664041|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs - note2.txt  1661664041|REG|||RecentDocs - Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt - note2.txt |
| Recent Docs | rip.pl -r /mnt/windows\_mount/Documents\ and\ Settings/Jim/NTUSER.DAT -p recentdocs | Launching recentdocs v.20200427  recentdocs v.20200427  (NTUSER.DAT) Gets contents of user's RecentDocs key  RecentDocs  \*\*All values printed in MRUList\MRUListEx order.  Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs  LastWrite Time: 2022-08-28 05:20:41Z  1 = note2.txt  0 = note1.txt  Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt  LastWrite Time 2022-08-28 05:20:41Z  MRUListEx = 1,0  1 = note2.txt  0 = note1.txt |
| Recent Apps | rip.pl -r /mnt/windows\_mount/Documents\ and\ Settings/Jim/NTUSER.DAT -p recentapps | Launching recentapps v.20200515  recentapps v.20200515  - Gets contents of user's RecentApps key  Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found. |
| Recent Apps | rip.pl -r /mnt/windows\_mount/Documents\ and\ Settings/Jim/NTUSER.DAT -p recentapps\_tln | Launching recentapps\_tln v.20190513  Software\Microsoft\Windows\CurrentVersion\Search\RecentApps not found. |
|  | rip.pl -r /mnt/windows\_mount/Documents\ and\ Settings/Jim/NTUSER.DAT -p runmru | Launching runmru v.20200525  runmru v.20200525  (NTUSER.DAT) Gets contents of user's RunMRU key  RunMru  Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU  LastWrite Time 2022-08-28 05:27:56Z  MRUList = cba  a notepad\1  b firefox\1  c vlc\1 |