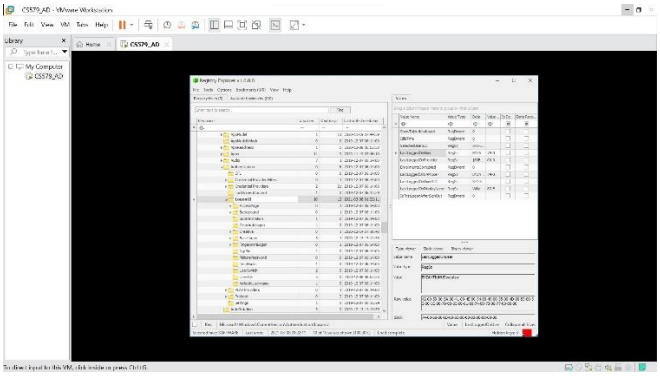
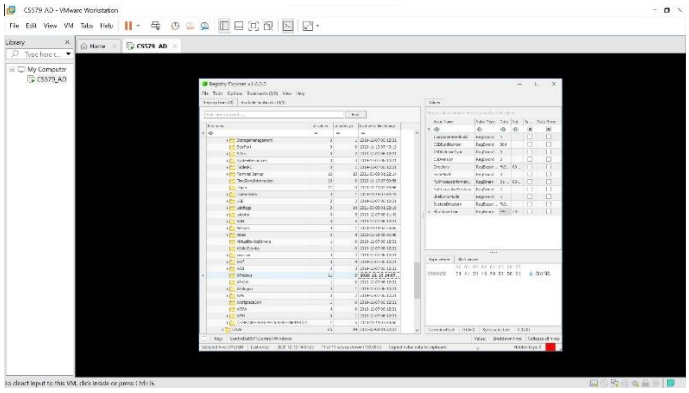
Registry Analysis and Report

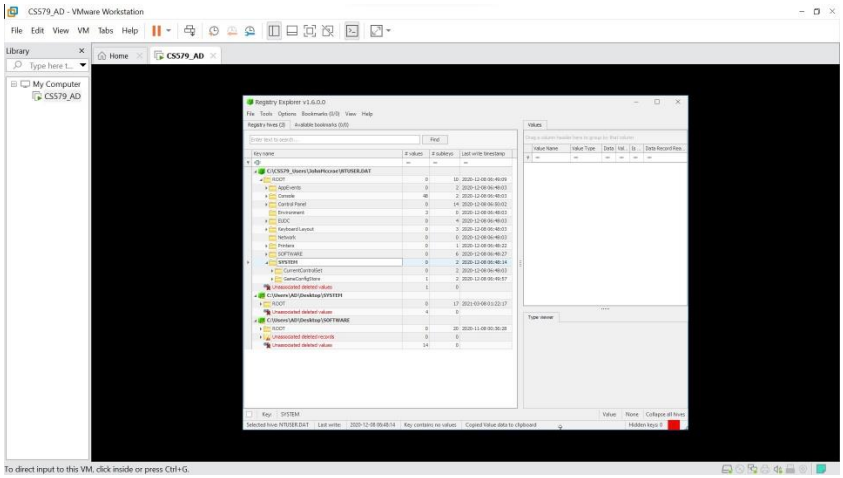
1. **Last Logged on user**: - BYZANTIUMUS/yeatsw



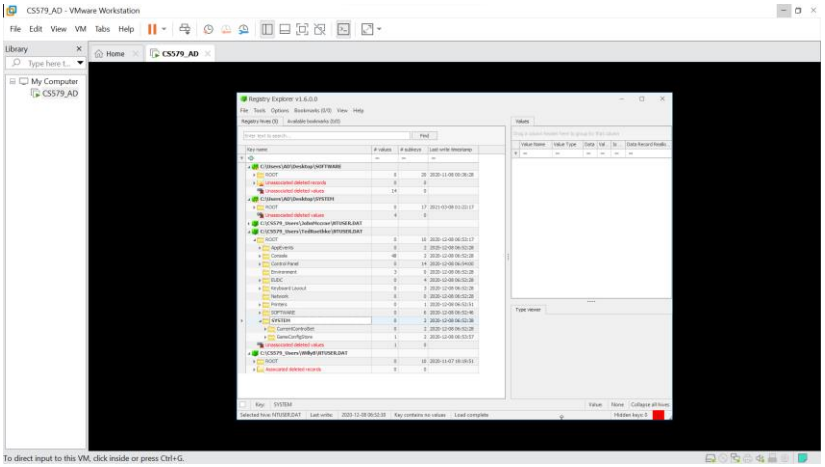
2. **Last Shutdown time**: - 2020-12-13 14:07:25



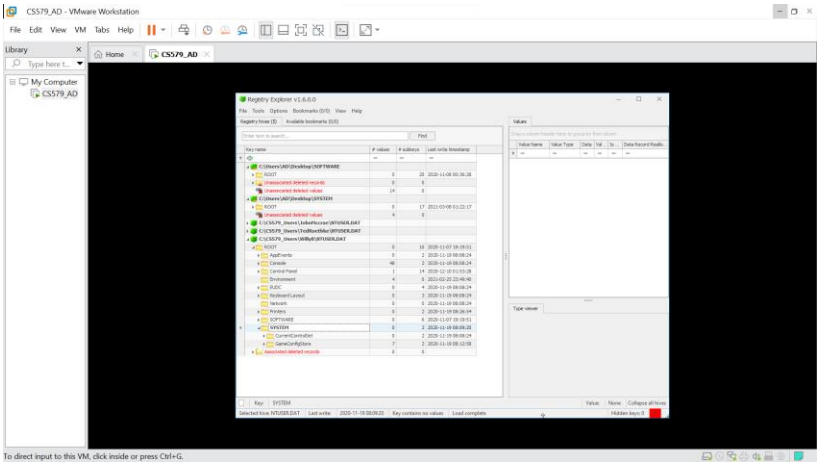
3. **Last write time on ntuser.dat**:
   a. **John Mccra**e: 2020-12-08 06:48:14



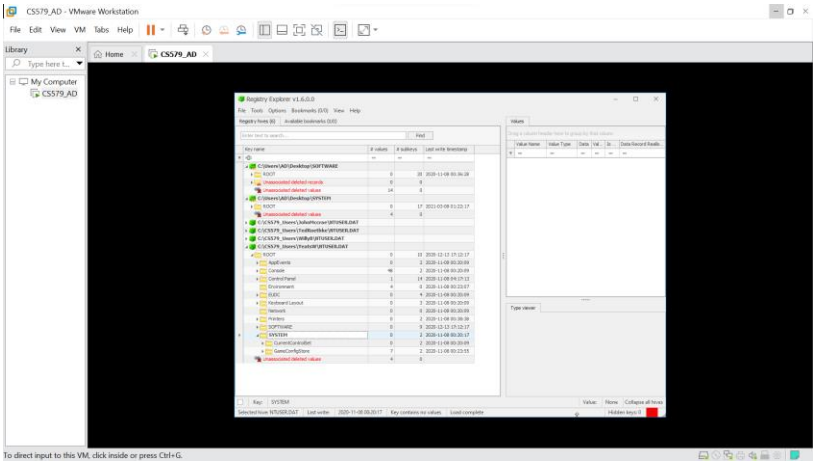
b. **Ted Roethke**: 2020-12-08 06:52:38



c. **Willy B**: 2020-11-09 08:09:20

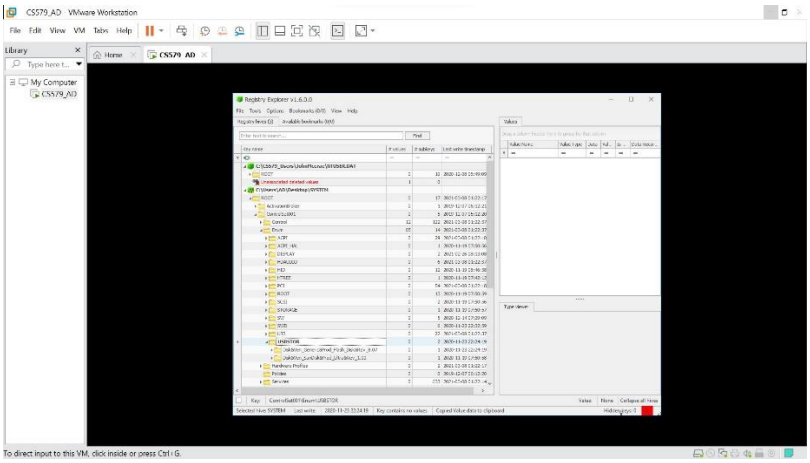


d. **Yeats W**: 2020-11-08 00:20:17

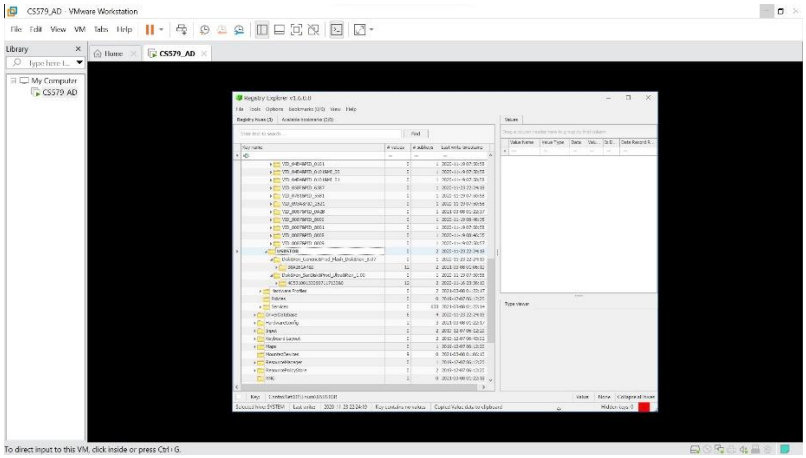


4. **Device type and serial number of any connected USB devices**:

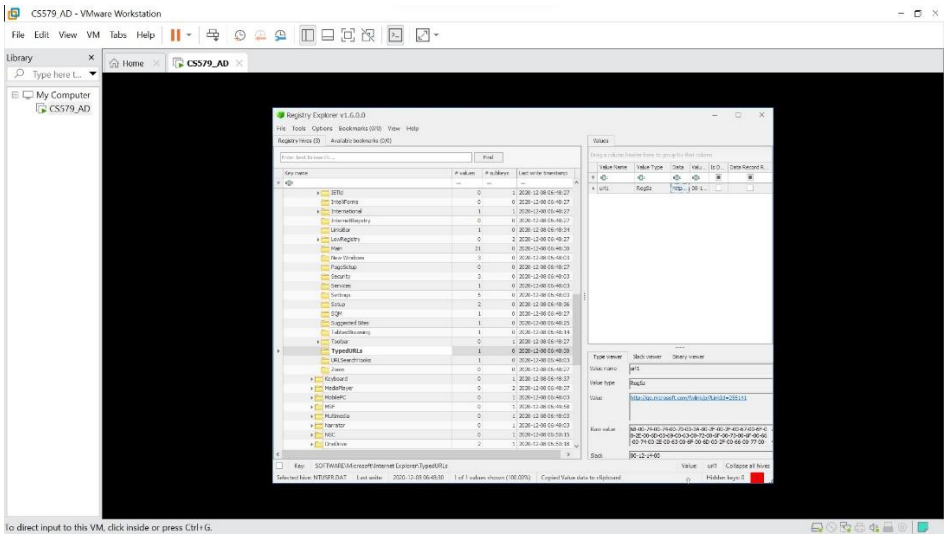
USB Drive with serial number "38A261A4&0" was last connected to the system.



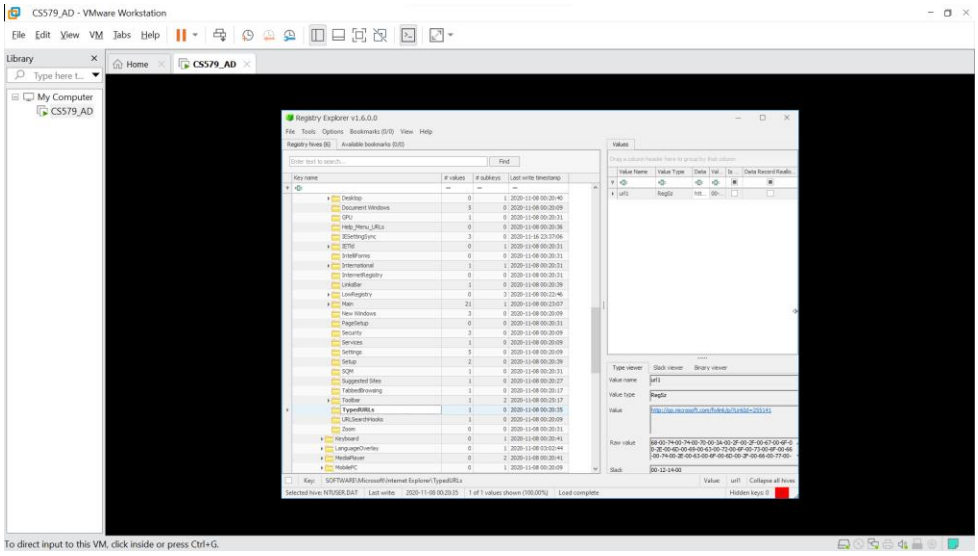
5. **Last time a device was attached:**
   USB device was last attached on March 8, 2021, at 01:06:10.



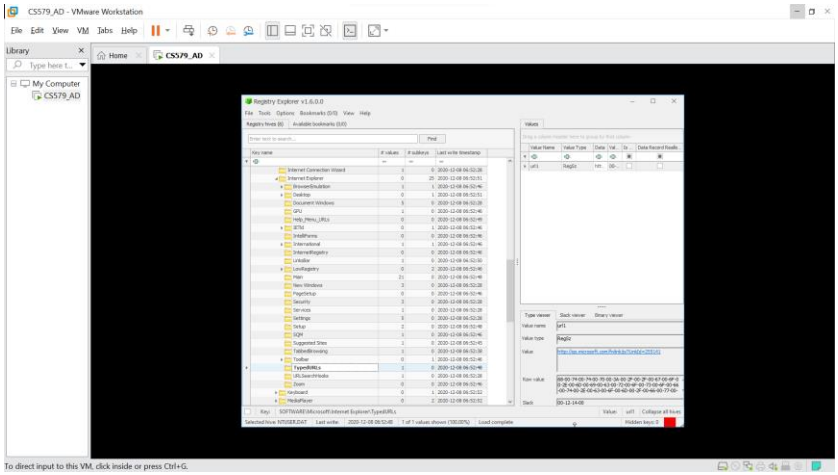
6. **Recently typed URLs in Internet Explorer:**
   a. **Willy B**: - http://go.microsoft.com/fwlink/p/?LinkId=255141



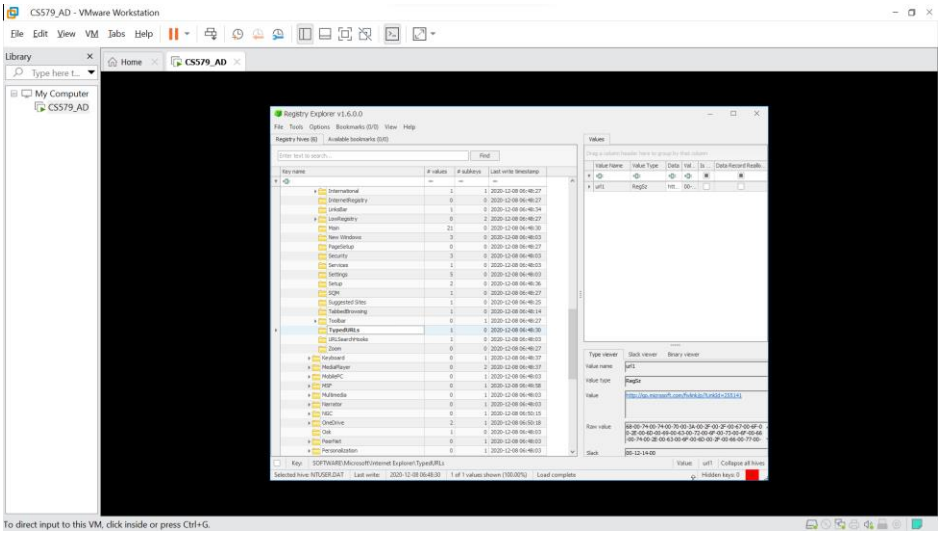
b. **Yeats W**: - http://go.microsoft.com/fwlink/p/?LinkId=255141



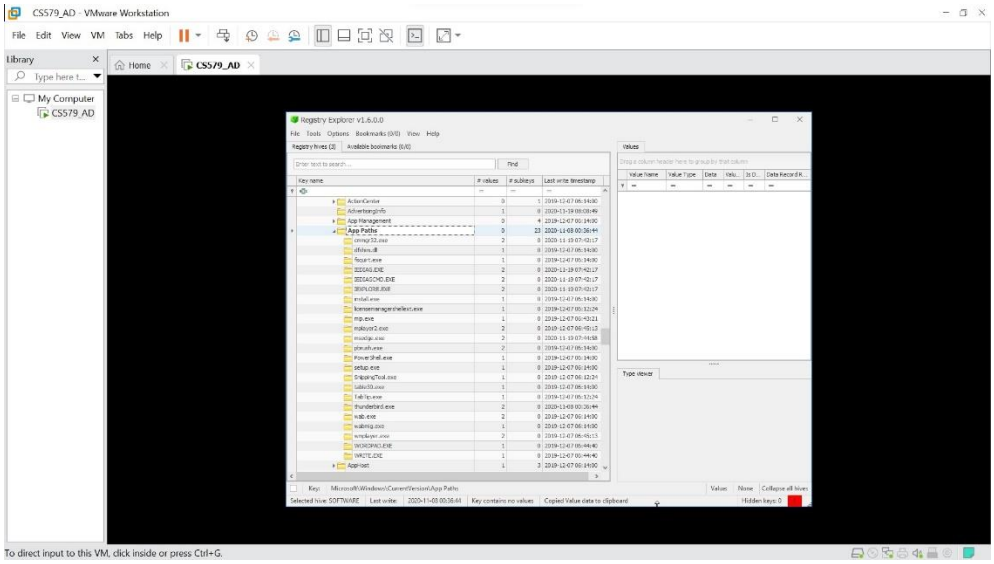
c. **Ted Roethke**: - http://go.microsoft.com/fwlink/p/?LinkId=255141



d. **John Mccrae**: - http://go.microsoft.com/fwlink/p/?LinkId=255141



7. Paths to installed executables:



We were able to view/find some local hives while accessing the image of a hard drive for domain account of YeatsW. To view them, we made use of a tool called Registry Explorer which helped us to extract information about them.

The last logged on user was BYZANTIMUS\YeatsW. Based on this, we can see that the user logged in using a domain account. It was observed that the "Last Logged on Display Name" was Willy B. Willy Yeats was last seen by locals on the evening of March 8th. After viewing information from the registry, we were able to extract the hexadecimal value of the last shutdown time of the system. Converting it into actual date time format was difficult, but it was 2020-12-13 at 14:07:25 which is 4 days past last seen.

Two USB drives were accessed during that time with serial numbers '38A261A4&0' and '4C53100133060711713330'. The latter had a last write timestamp of 2020-11-16 23:36:10, while the former drive was accessed the very day at 01:06:10 when Willy B went missing. Exploring HKLM\SYSTEM\MountedDevices helped us extract information about 9 such mounted drives among which 4 devices were disk drives containing disk letters C, D, E, and F. The remaining devices were volume drives.

The last typed URL from the system was made to http://go.microsoft.com/fwlink/p/?LinkId=255141 (Microsoft default homepage) on December 08 2020, at 06:48:30. This suggests that either all URLs accessed before that time were deleted or someone did not make use of Internet Explorer to perform actions on the internet. The computer system might have been thrown into a dumpster by that person to hide any piece of evidence that it might hold.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths was used to extract information about installed executables. "App Paths" is used to store executable file as individual subkeys in the registry along with the path for these executables and their last write time.

The path HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run led us to a subkey – "SecurityHealth" which is a file path to launch Windows security agent. The registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nia\Cache stores cached information related to network connectivity status indicator for windows system. From the path, we observed that 'Home' network was last accessed.

We were able to find 4 devices in the path HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices. The friendly names of all 4 drives were Ubuntu srv, Easter 1916 and E:\ and Easter 1916. The registry key HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer did not contain any information for the directories ComDlg32, RecentDocs, RunMRU, TypedPaths and UserAssist.

There were some questions about the existence of multiple user accounts on that system each having a similar lastly typed URL, but different last write times and shutdown times as well. There is very little information about this, and we need more evidence to connect the dots between these users.

Overall, exploring the registry gave us great insights into the user Willy B which will be used for further investigation. The evidence from this investigation suggested that some data from the system was deleted on that very day when Willy was last seen. This could further open several questions about this incident and the people involved in it.