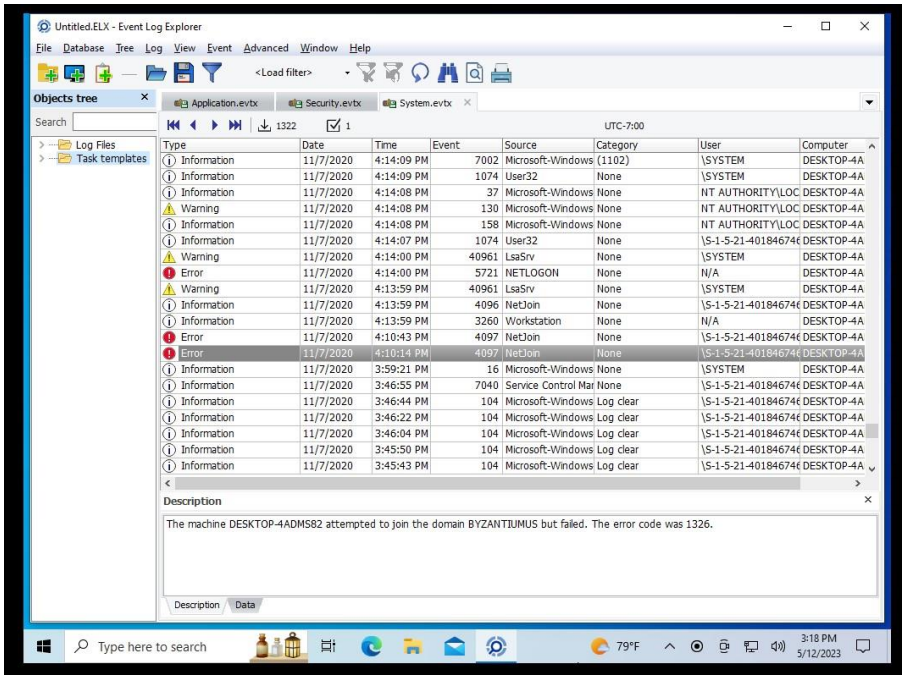
EVENT LOG ANALYSIS

We extracted event log files from the forensic image and analyzed it. To perform this task, we made use of Event Log Explorer. Before using the Event Log Explorer, we extracted all the log files from our image using Autopsy from the path “Windows/System32/winevt”.

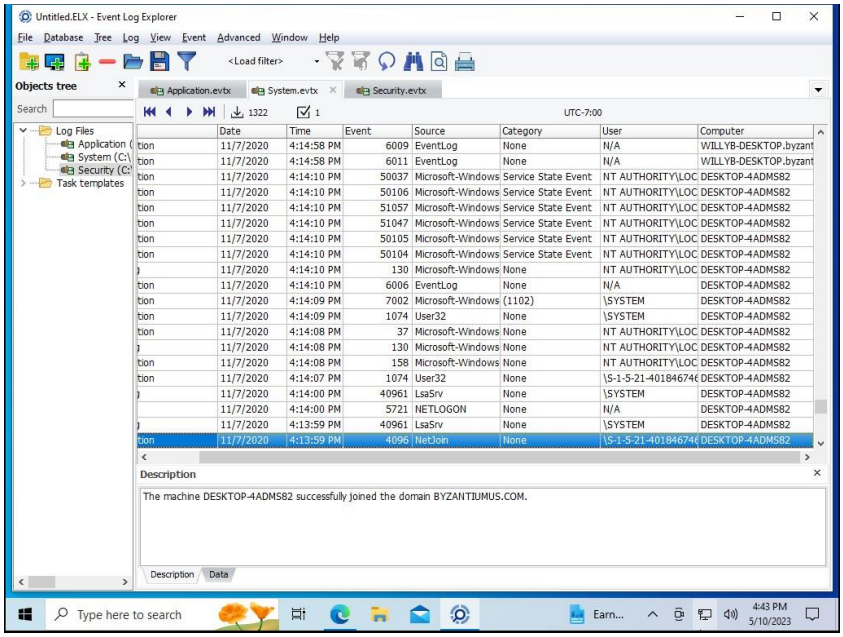
From the extracted log files, we opened three event files (Application.evtx, System.evtx and Security.evtx) into the Event Log Explorer. To avoid confusion, we removed the existing desktop logs from the Event Log Explorer and accessed the event log files extracted from our image.

Our motivation to explore the logs was to find out any pieces of evidence regarding any malicious software installed on the system, notable timestamps for domain account access, IP addresses associated with the domain controller, various accounts logged into the machine and signs of user behavior.

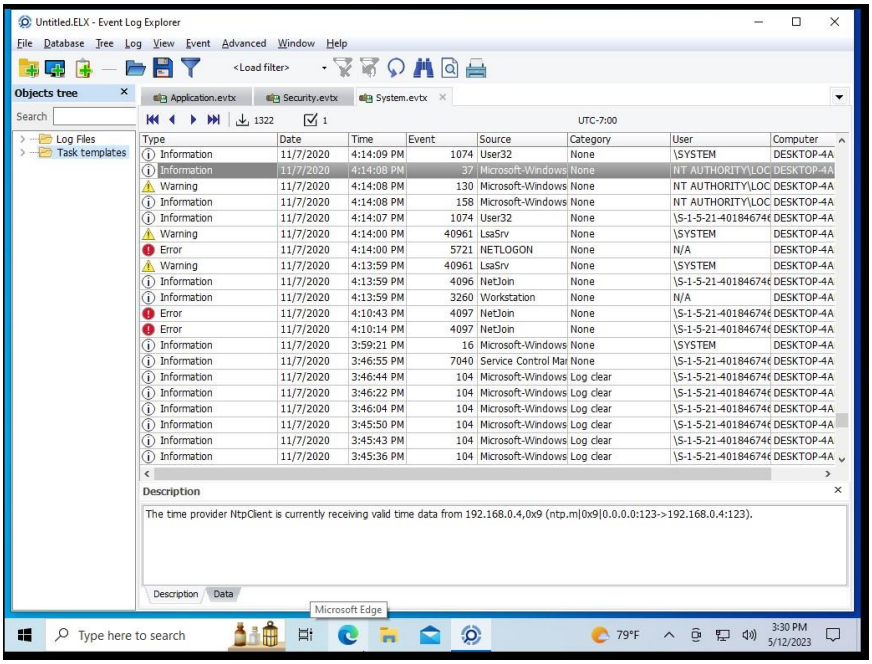
The machine ‘DESKTOP-4ADMS82’ was attempting to join the domain ‘BYZANTIUMUS.COM’. However, there were two instances to join the domain which failed twice due to error code 1326 (an error caused due to bad username or password) on 11/7/2020 at 16:10:14 and 16:10:43 respectively. This information was extracted from the ‘System event log’ file. Below is a screenshot of the same.



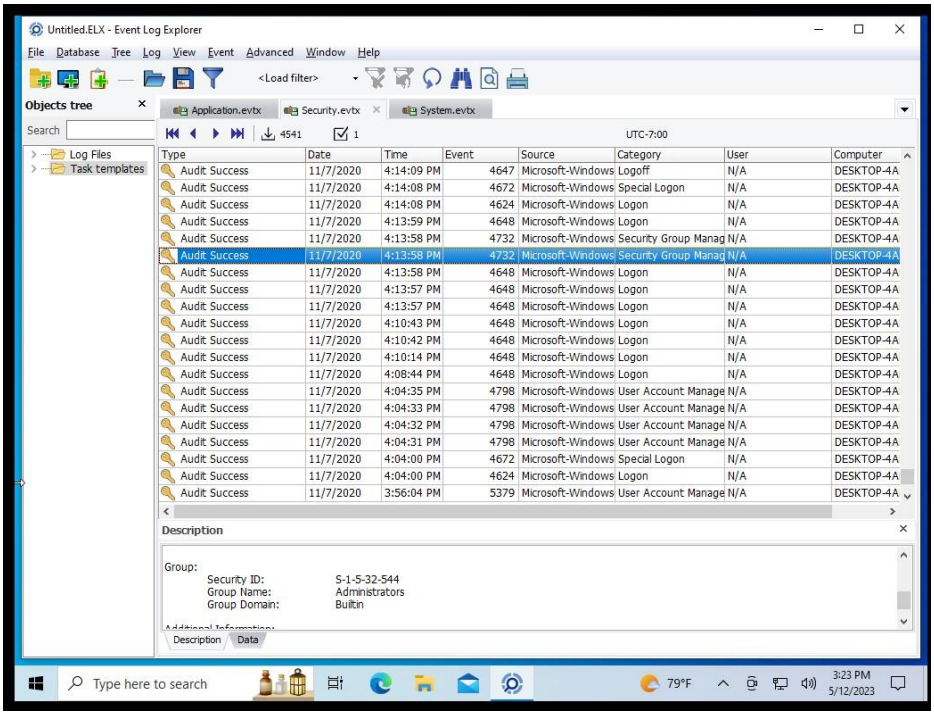
Finally, the computer system ‘DESKTOP-4ADMS82’ joined the domain ‘BYZANTIUMUS.COM’ on 11/7/2020 at 16:13:59. Below is the screenshot of the same.

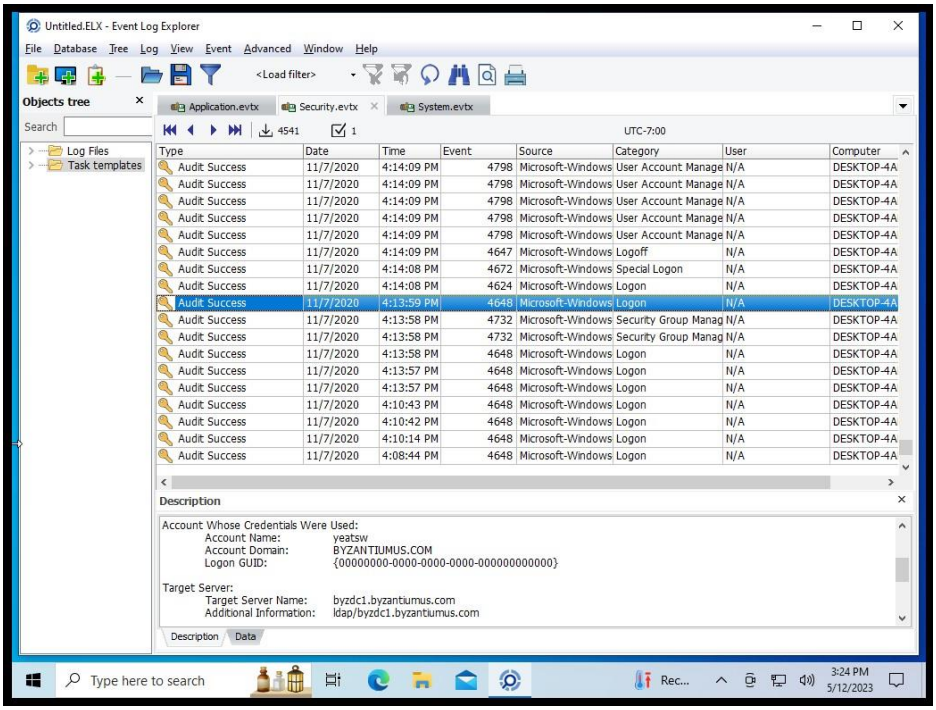


Upon checking some more logs, we were able to find out the IP address for the domain controller that was joined by the computer machine which was ‘192.168.0.4’ and it occurred on 11/7/2020 at 16:14:08.

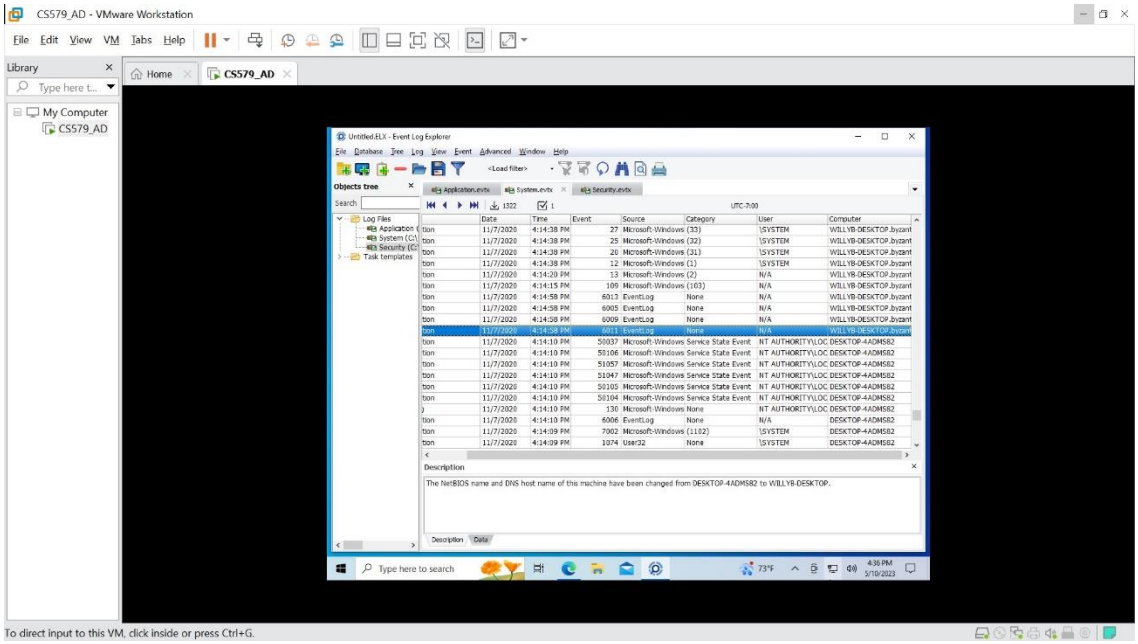


Initially, it was Willy B who was a user on this system. But, later using the administrator access, a new account was added to a local security group on 11/7/2020 at 16:13:58. Exploring this deeply helped us identify the added account along with the timestamp associated with it. Moments after adding an account to a local security group, we observed an account login into the system on 11/7/2020 at 16:13:59. The account whose credentials were used belonged to 'yeatsw' and the account domain was 'BYZANTIUMUS.COM'. This information was extracted from the 'System event log' file. Below are the screenshots of this observation.





Finally, we observed that the NETBIOS name and the host name of the machine was changed from ‘DESKTOP-4ADMS82’ to ‘WILLYB-DESKTOP’ at 11/7/2020 16:14:58. Below is the screenshot for this observation.



By examining the Application event log file, we were able to observe that there were instances of the machine being connected to an external internet connection.

As far as the user behavior is concerned, we observed that the user was trying to join the domain and accessing the user accounts from it. But, since all users did not have access to the domain, they were given special access by the administrator. This led to the change in the computer host name. The activities carried out seem to be suspicious, but there was no track of malicious software present.

In order to find more information about the user accounts, domain controller and signs of malicious applications, we would have to explore the log files more deeply and extract relevant information in order of the timeline when it took place.