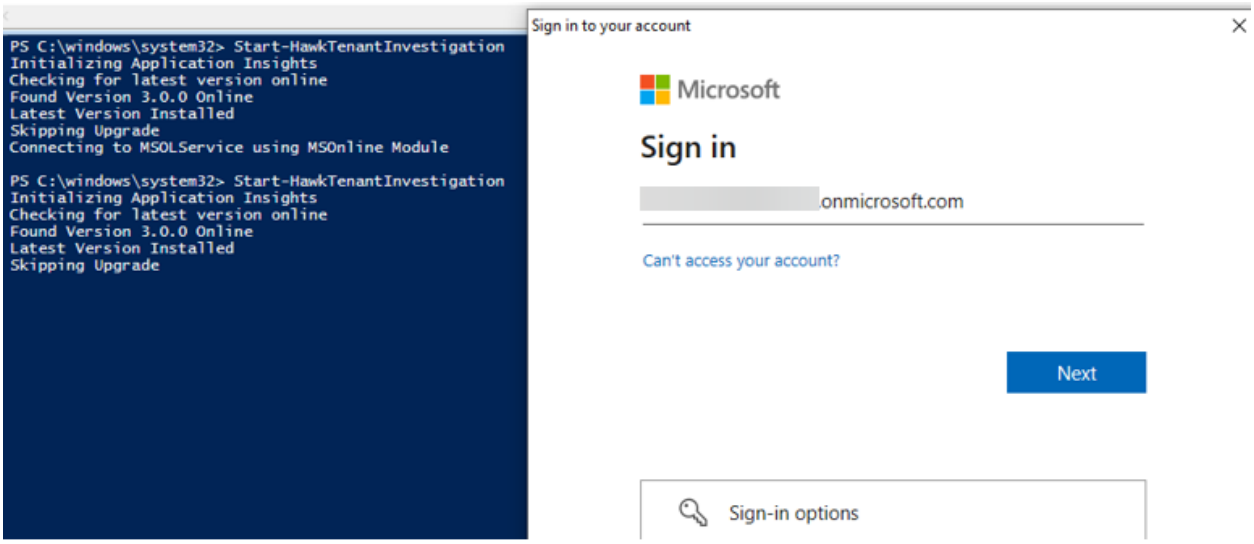
## Incident Response Utilizing Hawk Investigation Tool

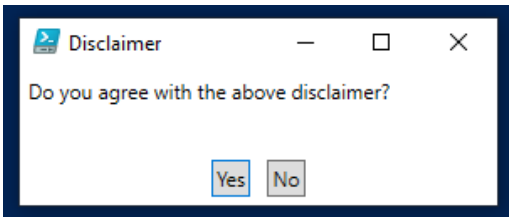
This tool is used to investigate or audit the Azure Active directory tenant.

First navigate to Powershell ISE or Powershell and use the command “Start-HawkTenantInvestigation” will allow to investigate Azure Active Directory tenant level.

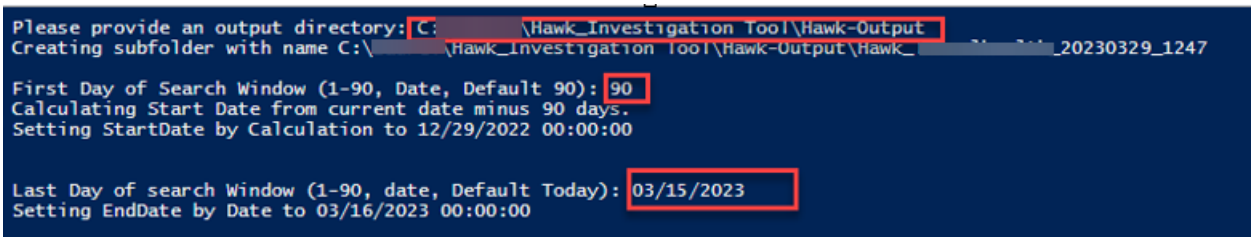
You will be prompted to sign in so that you can have access to Azure Active Directory Tenant, use your Microsoft admin account.



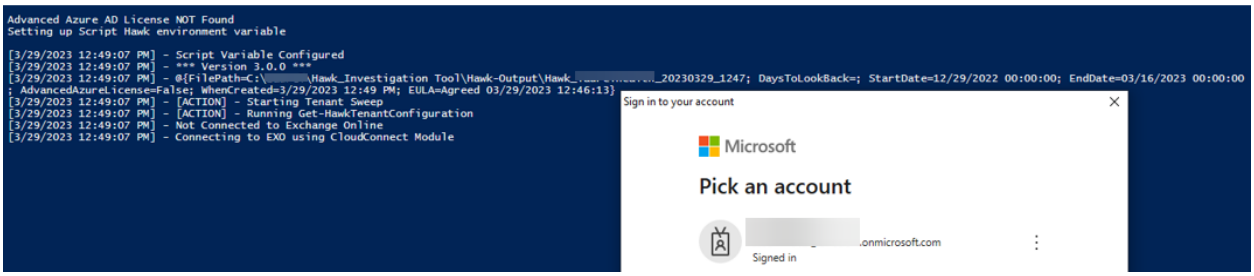

Click Yes to agree to “Disclaimer”.




Then, it will prompt you to provide an output directory, start date and last date of your search.




You will be prompted to sign in again using your Microsoft Admin account. Once you finish this step, the command will start running. The process will take about 5mn.




Reference:

[GitHub - T0pCyber/hawk: Powershell Based tool for gathering information related to O365 intrusions and potential Breaches]