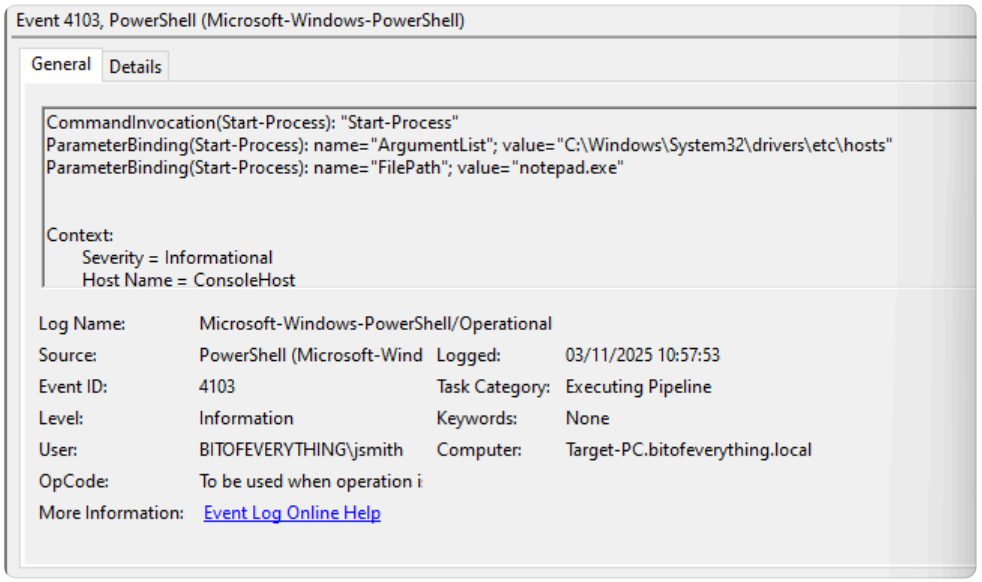
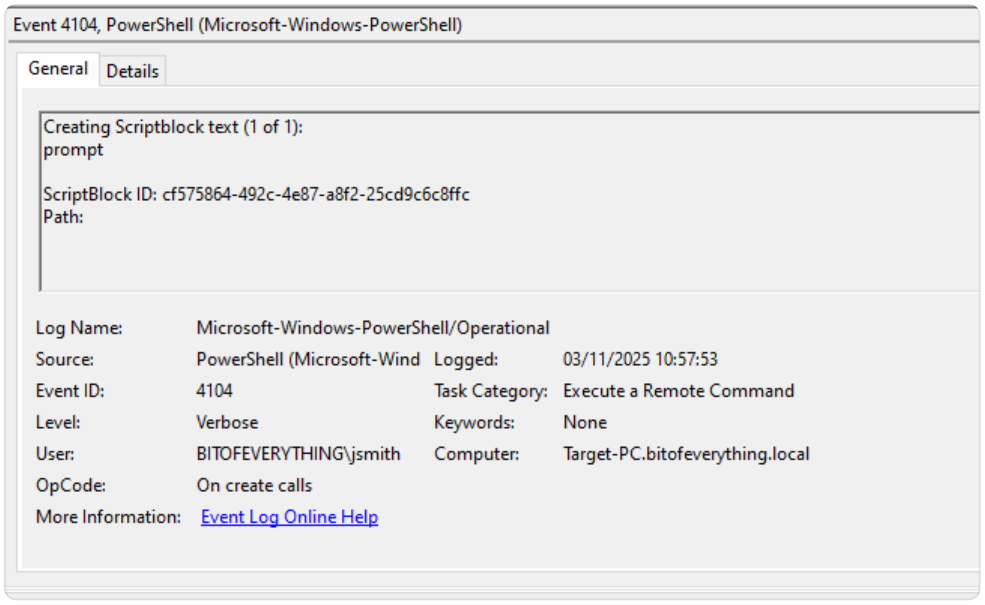
Day 3: Log Analysis Basics: Windows PowerShell Logs

Objective:
The objective of this lab is to explore and analyze Windows PowerShell logs to understand how PowerShell-related events are recorded and how they can be used to detect suspicious or malicious activity. It focuses on identifying, interpreting, and correlating PowerShell event IDs to recognize potential indicators of compromise or unauthorized script execution within a Windows environment.

Event ID **4103** records **detailed command execution information in PowerShell**. It captures each command that is run, including the parameters used, the process that invoked it, and the user account that executed it. This event is part of **script block logging** and is useful for monitoring what commands are actually being executed in the system, making it easier to detect suspicious or malicious activity, such as attempts to download files, execute payloads, or abuse legitimate tools (LOLBAS) for stealthy attacks.



Event ID **4104**, on the other hand, captures the **contents of executed script blocks**. Whenever a PowerShell script block is executed, 4104 logs the actual code that ran, providing visibility into the script's logic and any potentially malicious instructions. This is especially valuable for detecting obfuscated or hidden commands that may be used in attacks, since it shows the full PowerShell commands and scripts in their executed form.



Conclusion:
In this lab, I learned how to enable and analyze Windows PowerShell logs to monitor command executions and detect potential security threats. I explored key event IDs such as 4103 and 4104, which record detailed information about PowerShell commands, users, and timestamps. Through this process, I gained practical skills in using Event Viewer to identify legitimate versus suspicious PowerShell activity, recognize signs of post-exploitation techniques, and understand the importance of PowerShell logging in threat detection and incident response.