POWERSHELL FORENSICS

[PowerShell Command History Forensics - Blog - Sophos Labs - Sophos Community](https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics)

<https://community.sophos.com/sophos-labs/b/blog/posts/powershell-command-history-forensics>

POWERFORENSICS

[PowerForensics](https://powerforensics.readthedocs.io/en/latest/)

<https://powerforensics.readthedocs.io/en/latest/>

https://www.tevora.com/threat-blog/5-minute-forensics-decoding-powershell-payloads/