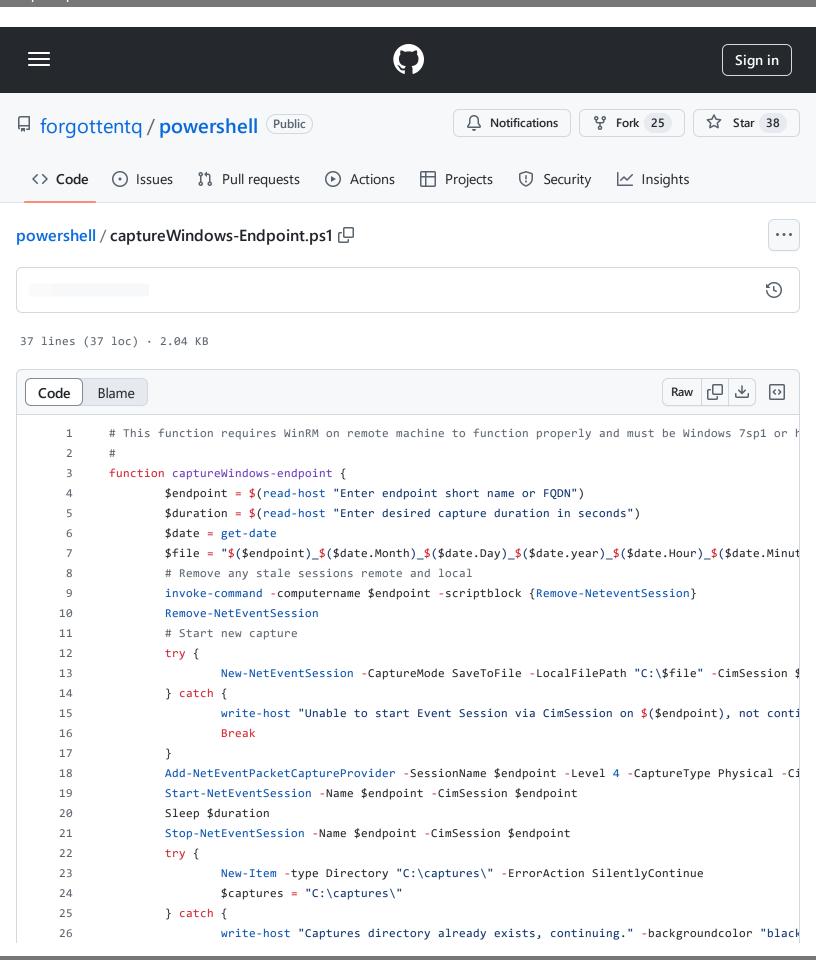
powershell/captureWindows-Endpoint.ps1 at 9e616363d497143dc955c4fdce68e5c18d28a6cb forgottentg/powershell · GitHub - 31/10/2024 17:25

https://github.com/forgottentq/powershell/blob/9e616363d497143dc955c4fdce68e5c18d28a6cb/captureWindows-Endpoint.ps1#L13



powershell/captureWindows-Endpoint.ps1 at 9e616363d497143dc955c4fdce68e5c18d28a6cb · forgottentq/powershell · GitHub - 31/10/2024 17:25

https://github.com/forgottentq/powershell/blob/9e616363d497143dc955c4fdce68e5c18d28a6cb/captureWindows-Endpoint.ps1#L13

```
27
                       $captures = "C:\captures\"
28
               }
               write-host "Copying endpoint capture file to local workstation!" -backgroundcolor "black"
29
30
               Copy-item "\\$endpoint\c$\$file" $captures
31
               Remove-Item "\\$endpoint\c$\$file"
               # Remove local and remote sessions.
32
33
               invoke-command -computername $endpoint -scriptblock {Remove-NeteventSession}
34
               Remove-NetEventSession
35
               write-host "Opening capture directory" -backgroundcolor "black" -foregroundcolor "green"
               ii $captures
36
37
       }
```