


←

Post



Grzegorz Tworek

@0gtweet

⋮

If you have Microsoft DTrace handy, you can make live kernel dump with one cmdline: dtrace.exe -w "syscall:::return {lkd(0); exit(0);}"

LiveKernelReports

ShareView

This PC > Local Disk (C:) > Windows > LiveKernelReports

Name	Date modified	Type	Size
DTRACE	12/26/2021 1:20 AM	File folder	
DTRACE-20211226-0120.dmp	12/26/2021 1:20 AM	DMP File	538,272 KB

Administrator: Command Prompt

C:\Program Files\DTrace>dtrace.exe -w -n "syscall:::return { lkd(0); exit(0); }"
dtrace: description 'syscall:::return ' matched 470 probes
dtrace: allowing destructive actions
CPU ID FUNCTION:NAME
1 181 NtDeviceIoControlFile:return

C:\Program Files\DTrace>

1:27 AM · Dec 26, 2021

95 Reposts1 Quote321 Likes53 Bookmarks

💬

↺↻

❤️


🔖53

↗️

New to X?

Sign up now to get your own personalized timeline!

 Sign up with Google

 Sign up with Apple

Create account

By signing up, you agree to the [Terms of Service](#) and [Privacy Policy](#), including [Cookie Use](#).

Something went wrong. Try reloading.

↺ Retry

Terms of Service

Privacy Policy

Cookie Policy

Accessibility

Ads info

More ...

© 2024 X Corp.

Don't miss what's happening

People on X are the first to know.

Log in

Sign up

Welcome to x.com!

We are letting you know that we are changing our URL, but your privacy and data protection settings remain the same.

For more details, see our Privacy Policy: <https://x.com/en/privacy>.

×

Did someone say ... cookies?

X and its partners use cookies to provide you with a better, safer and faster service and to support our business. Some cookies are necessary to use our services, improve our services, and make sure they work properly. [Show more about your choices.](#)

Accept all cookies

Refuse non-essential cookies

Page 1 of 1