

Erledigt

"Du hast ja Alles" - hmmm vielleicht, wenn ich einen Laptop habe.

Beitrag von „andreas_55“ vom 2. Februar 2018, 20:39

Zitat

Dazu zieht man einfach die Startadresse des Kextes von der Rücksprungadresse ab.

Habe mal die erste rote Return Adress genommen und den Startspeicherbereich von IOACPIFamiliy:

$0xffffffff7f85621d08 - 0xffffffff7f83b96000 = 0x1A8BD08 \neq 0x10d08$

Was mache ich denn hier falsch?

Edit: Hab was vergessen: Cooler dritter Teil. 👍