

Kape



context

dit document beschrijft installatie en werking van Kape, een tool van Eric Zimmerman voor triage van Windows artefacts

installatie

1. [download](#) het zip-bestand.
2. pak het uit naar een directory op een gedeelde map.

werking

- meld (**altijd**) aan als local administrator
verhindert dat kape exit met een dubbelzinnige "*file(s) not found*" fout); terwijl beperkte rechten het eigenlijke probleem zijn.
- blader naar kape . exe en start.

meer info

- [Kape on Kroll](#)
- [webcasts](#)
- [official documentations](#)
- [autopsy](#)

From:
<https://louslab.be/> - **Lou's lab**

Permanent link:
https://louslab.be/doku.php?id=digital_forensics:kape

Last update: **2024/11/16 18:14**

