Volatility

context

dit document beschrijft de werking van Volatility, een memory forensics framework

profiles

- afhankelijk van het OS waarop je dump nam
- overzicht: `vol.py --info`
- Windows minidump (.dmp) worden (nog) niet ondersteund.

modules

- analyseren verschillende componenten van de dump
- overzicht: `vol.py --info`

werking

1. bepaal het profiel (OS) van je memory dumpfile: `time vol.py -f <dumpfile> imageinfo`
   `time` commando staat er -ter info- bij, omdat deze stap wel wat kan duren.
   Als je geen beweging ziet, doen dan even een `top`. Zolang het RAM/CPU verbruikt, is het bezig.
   Vooral de CPU krijgt het wat zwaar te verduren, precies.

verder ...

meer info

voeg hier linken toe naar verdere uitleg

digital forensics, RAM, volatility

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

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

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