

magnet RAM Capture



context

dit document beschrijft de werking van magnet RAM Capture, een tool om een RAM image te maken

installatie

1. as stand-alone as they come
2. vriendelijk op je knieën gaan en via email krijg je je [download](#) link
3. laat de download gerust es langs [VirusTotal](#) passeren.
Kans is groot dat er wel een paar aan de bel trekken. Een memory dump geeft je tenslotte toegang tot heel veel info.
Met een hamer kan je een kast bouwen, je kan er ook iemand mee de schedel inslaan. Ja, dat is ons wel bekend.

werking

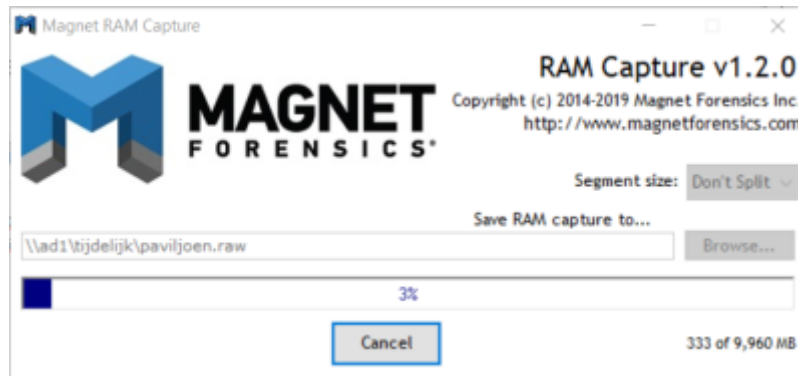
algemeen

in hoofdzaak kan je met Magnet RAM Capture:

- een volledige dump van het geheugen maken.
- alle processen, threads, netwerkverbindingen, registry waarden, credentials die op dat moment in het geheugen zijn geladen, naar een bestand dumpen.
- dat bestand kan je dan later volledige analyseren ahv bv [Volatility](#)

memory dump maken

- kopieer het bestand naar een (voldoende grote) USB-stick en dubbelklik.
De exe draaien vanaf een UNC pad werkt wel, maar niet vanaf een gemonteerde drive letter.
- geef een pad op waar je het RAW image bestand wilt opslaan en klik **Start**
UNC-paden worden ook hier ondersteund



memory dump bekijken

- zie: [Volatility](#)

meer info

[artikel op MagnetForensics](#)

[RAM, image](#)

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

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

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

