

dumpit



context

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

installatie

1. as stand-alone as they come
2. [download](#) naar een gedeelde map op je [SIFT workstation](#).

werking

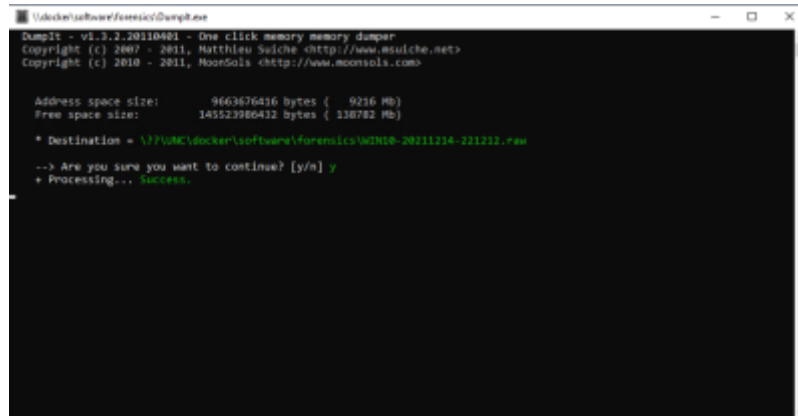
algemeen

in hoofdzaak kan je met dumpit:

- 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

- meld aan als local **administrator**
- dubbelklik.
de memory dump wordt aangemaakt in dezelfde map, met als naam: <computernaam>-<datum>-<uur>.raw
Op die manier kan je eindeloos veel dumps maken zonder dat die mekaar overschrijven.
- weinig output van de voortgang.
Je kan het ook wat opvolgen op de server ahv `watch -d du -m <image.raw>` of met [procmon](#), natuurlijk
maar op 't eind krijg je: succes



```
C:\docker\software\forensics\Dumpit.exe
Dumpit - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>

Address space size: 9663676416 bytes ( 9216 Mb)
Free space size: 145523986432 bytes ( 338782 Mb)

* Destination = \\?\UNC\docker\software\forensics\WDN10-20111214-221222.raw
--> Are you sure you want to continue? [y/n] y
+ Processing... Success.
```

memory dump bekijken

- zie: [Volatility](#)

beetje scheve bemerking

Dumpit is een oud stukje software (< 2011-05-03 05:23:10), maar goed, het doet het nog steeds goed, lijkt wel.

[Virusotal](#) maakt ook geen bezwaren.

meer info

- [artikel](#)

[RAM](#), [image](#)

From:

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

Permanent link:

https://www.louslab.be/doku.php?id=digital_forensics:dumpit

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

