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

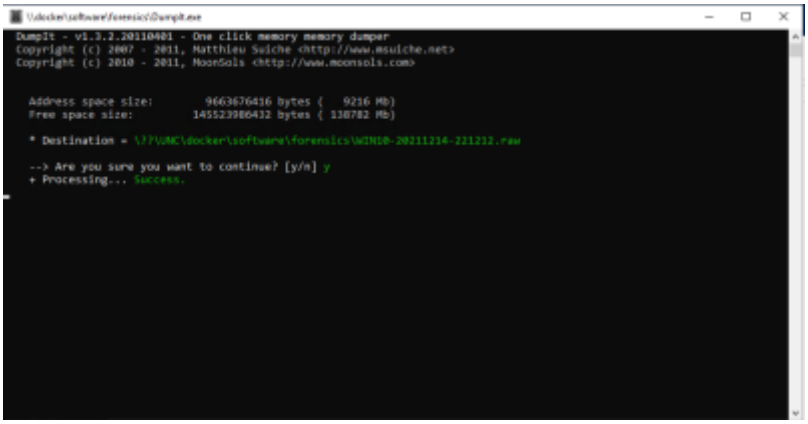
algemeen

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



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.
Virustotal maakt ook geen bezwaren.

meer info

- artikel

RAM, image