

whois



context

dit document beschrijft enkele zoekacties met whois

context

1. bevraagt whois databases waarin informatie rond domein registratie bewaard wordt.

werking

standaard

`whois <domein>-H -verbose:`

vraagt info op, met meest mogelijke details (oa gebruikte whois server) met uitzonderin van legalese.

algemeen

in hoofdzaak kan je met FTK:

- een identieke kopie (**image**) maken van disk/partitie/mappen
- een **memory** dump doen.
- een dump van **protected files** (registry, SAM account, ...) doen
- de **image mounten** en van daaruit bestanden onderzoeken.

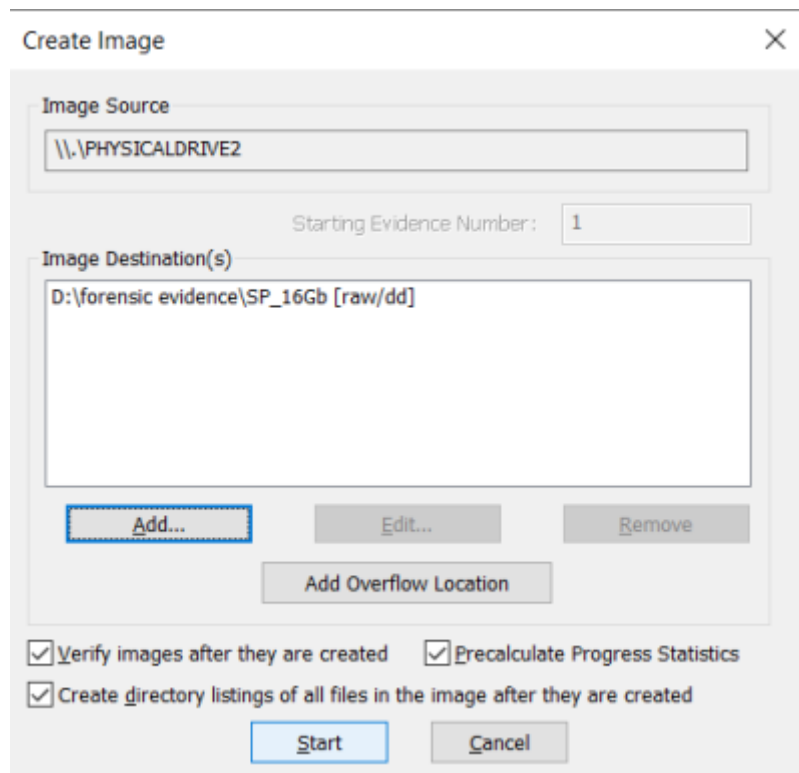
disk image maken

Note: Controleer dat je write-blocker is aangesloten zodat je geen data naar de schijf schrijft die je wilt imagen.

Je kan ook USB-apparaten [write-protect](#) zetten

1. **File > Create Disk Image**
2. **Source:**

1. Physical Drive: volledige schijf
2. Logical Drive: partitie met drive letter (C, D, ...)
Geen gemonteerde gedeelde mappen!
3. Image file: bestaande image file
4. Contents of a Folder: geselecteerde map.
3. **Image destination:** plaats waar je image wilt bewaren.
4. **Image type:** raw, AFF
5. **Evidence item information:** administratieve data mbt de case
6. **Image file name:** bestandsnaam.
7. zet volgende **opties** aan:
 1. verify images,
 2. create listing,
 3. calculate progress,
8. **START**



9. na afloop heb je een aantal aff-bestanden, een bestandslijst en een rapportje.

disk image bekijken

- **Add Evidence Item**
- **Source Evidence Type:** cfr hierboven. Meestal: **Image File**
- blader naar het image bestand
- nu kan je doorheen het bestand **bladeren** en de **eigenschappen** van bestanden bekijken.

problemen, problemen

logboeken

- in locatie waar je image bewaart: <NaamImage>.txt

werking

Note: schakel slaapstand uit anders zal je image onderbroken worden

meer info

voeg hier linken toe naar verdere uitleg

[autopsy](#)

From:

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

Permanent link:

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

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

