

# TrID



## context

dit document bevat installatie en werking rond [TrID](#), een programma om een bestandstype te identificeren.

## installatie

### Windows

```
choco install trid
```

### Linux

- deel van [SIFT](#) workstation.  
tridupdate doet db update.
- handmatig:
  - mkdir /tmp/trid && cd /tmp/trid
  - download de 3 componenten:  
for i in defs update \_linux\_64; do wget [https://www.mark0.net/download/trid\\$i.zip](https://www.mark0.net/download/trid$i.zip); done
  - pak alles netjes uit:  
for i in defs update \_linux\_64; do unzip -x trid\$i.zip; done
  - verwijder de zipbestanden:  
rm -f \*.zip readme.txt
  - verplaats naar bin directory:  
mv \* /usr/local/bin && chmod -R 755 /usr/local/bin
  - ruim netjes op:  
cd / && rm -rf /tmp/trid

## update

```
python /usr/local/bin/tridupdate.py: werkt de bestandsdefinities bij.
```

## gebruik

- start een DOS prompt
- voer uit: " trid.exe -v <naamBestand>"
- de waarschijnlijkheid van het juiste resultaat wordt in percent uitgedrukt: 100%: absoluut zeker, 75%: behoorlijk zeker, etc ...
- file types worden uit de databank (triddef.trd) gelezen.  
Bijwerken van TrID is dus nodig om nieuwe types toe te voegen.  
Je kan het bestand inlezen ahv bv strings  
aantal bestandstypes worden weergegeven
- interessante opties:
  - trid -ae: voegt bestandstype toe, zodat je bestand de extensie krijgt die het allicht verdient.  
handig als je een boel bestanden hebt zonder extensie (uit file recovery, bv)
- VirusTotal gebruikt het ook, ten andere.

## problemen, problemen

### Linux: fout bij starten:

```
trid: loadlocale.c:129: _nl_intern_locale_data: Assertion `cnt < (sizeof (_nl_value_type_LC_TIME) / sizeof (_nl_value_type_LC_TIME[0]))' failed.  
Aborted (core dumped)
```

**oplossing:** voeg onderstaande lijn toe aan .bashrc: `export LANG=C`

[windows](#), [TrID](#)

From:

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

Permanent link:

[https://louslab.be/doku.php?id=digital\\_forensics:trid](https://louslab.be/doku.php?id=digital_forensics:trid)

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

