Lab 9:

Laster ned IW10 windows 7 zip filen

Laster ned dumpit I windows VM-en og dumper minnet

Bruker <https://www.transfernow.net/en> og sender filen på epost

Overfører til SANS SIFT VM-en (krever en bruker for å installeres , måtte opprette )

Deretter trykk på SANS SIFT ova fil og (trykk deretter import) så lastes den ned

Går inn på mail – inboxen og trykker på filen transfernow sendte meg og laster ned i SANS VM-en

**Oppgave 1 Volatility ImageDump:**

Et bilde som inneholder tekst

Automatisk generert beskrivelse

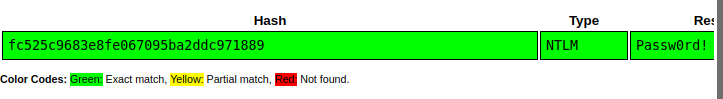
**Oppgave 2** (Finn passordet ved bruk av hashdump med –profile = Win7SP1x86) (vol.py hashdump -f «filplassering» --profile=Win7SP1x86

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Går inn på crackstation og limer inn Hashen til IEUser (Admin) og finner passordet : husk at hashen starter på f ….1889 . Limer inn i crackstation og får opp et resultat:

* **Hva er passordet til IEUser?**



* **Uten å bruke cracker – hva er passordet til Administrator?**

Passordet står i bakgrunnen på windows VM-en

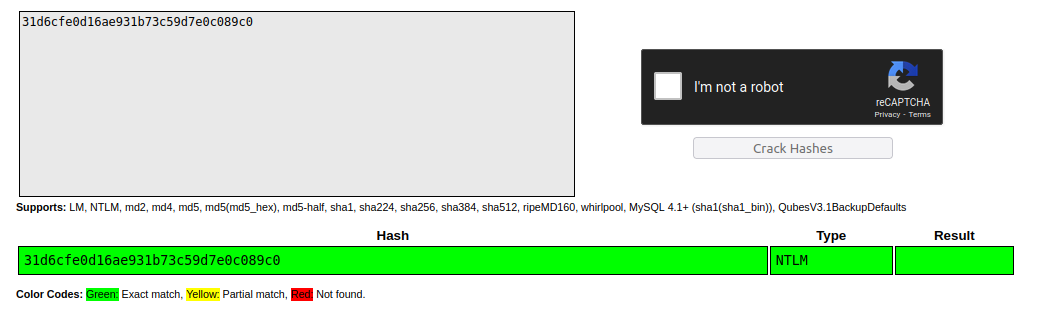
Et bilde som inneholder tekst

Automatisk generert beskrivelse

* **Fra timen i dag – hvordan kunne man ha unngått at pasordet til Administrator var så innlysende?**

Passordet burde ha vært kryptert med en enveis-hash før man hasher passordet er det lurt at den saltes

* **Hva er passord til Guest?**

****

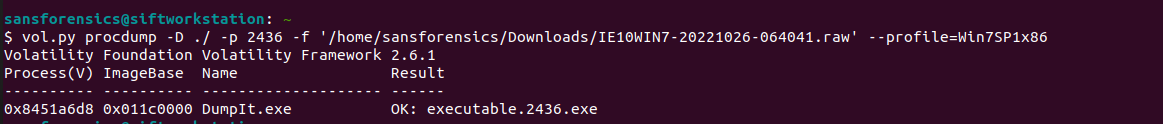
Det er ikke satt noen passord til Guest brukeren og derfor har den ingen passord

**Kjører pslist og får opp alle kjørende prosesser:**

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**Kjører en procdump rettet mot (PID =2436 på min maskin) til dumpit.exe**



**Så tar du md5sum av filen og tester mot VirusTotal. Traff ikke? Last opp hele filen! Du vil sannsynligvis få et fåtall treff på at dette er ondsinnet (generiske signaturer). Grunnen til at den ikke treffer på md5sum er at ting endres når den lastes til minne.**

**Et bilde som inneholder tekst

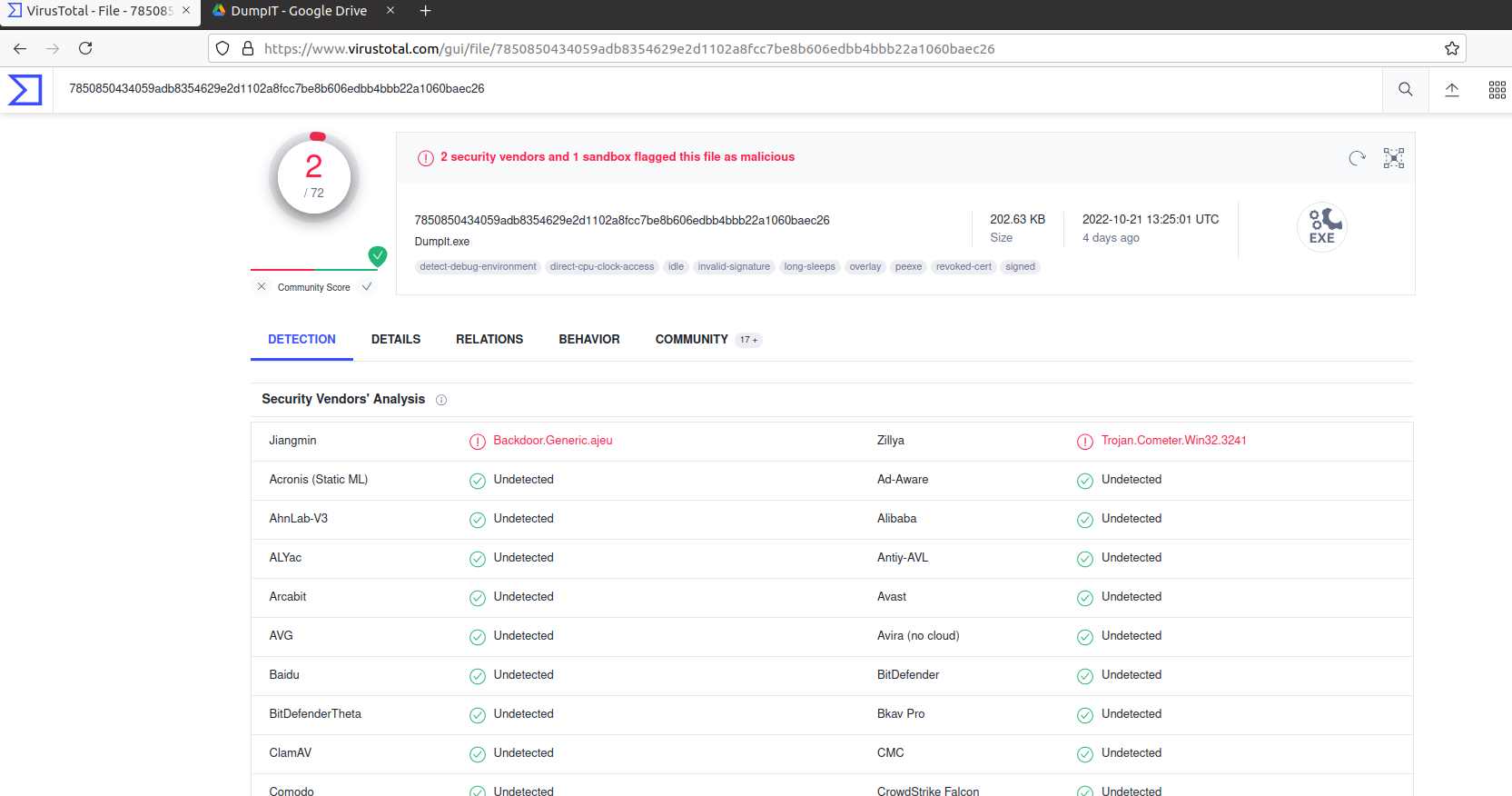
Automatisk generert beskrivelse**

Søker md5 summen , men får feilmelding prøver heller å laste opp hele raw filen (går heller ikke)

Laster ned dumpit på SANS SIFT VM-en skriver kommandoen: md5sum «filnavnet» i terminalen



Legger den inn i virus total og får opp at dette er en ondsinnet signatur:



**Lister ut TCP forbindelser i minne ved bruk av netscan kommandoen**

