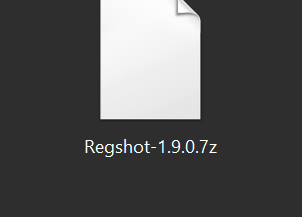
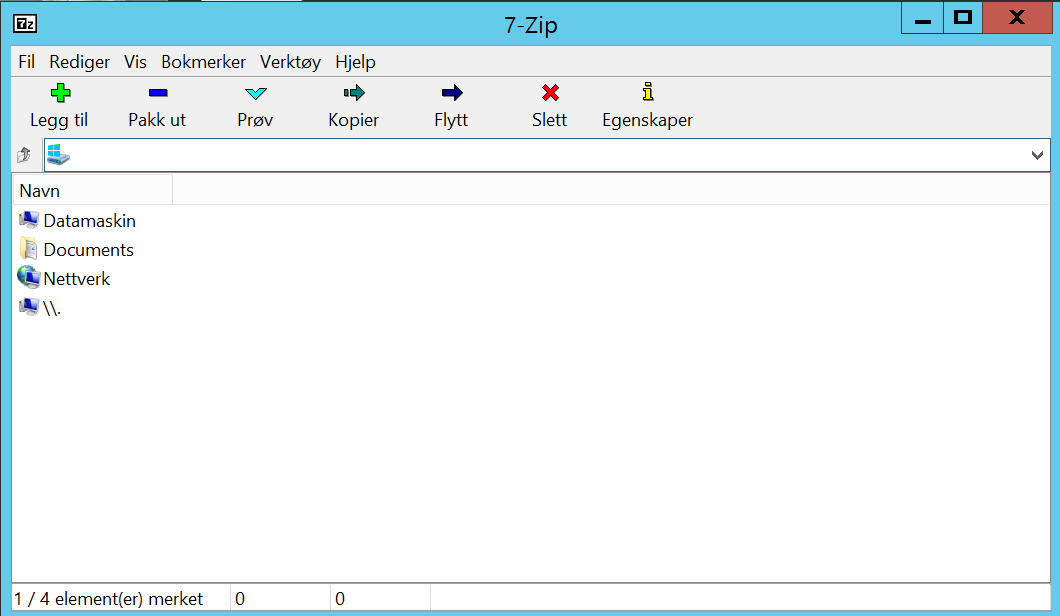
Lab 7 laster ned 7 zip i windows vm og legger inn regnshot filen



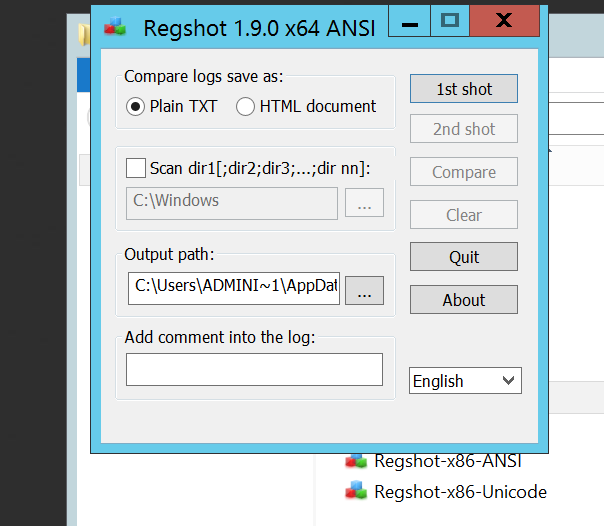


Pakker ut:



Går inn i mappen trykker

Regnshot ansi trykker 1st shot last ned winzip updater deretter 2nd shot og compare



Får opp en fil som skal være en rapport!

Et bilde som inneholder tekst

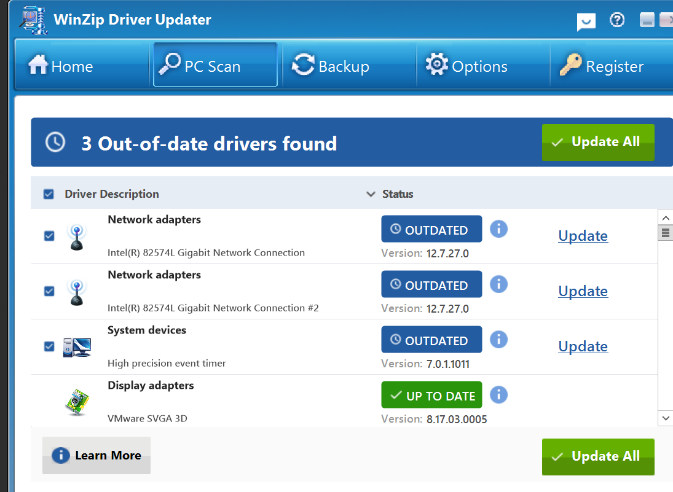
Automatisk generert beskrivelse

**Øverst i rapporten finner man bruker og maskinnavn. Hvem er bruker? Og hva**

**heter maskinen? Hvor tror du Regshot finner dette?**

Det er fordi regshot kjører en real time analyse av computeren og lagrer info om brukeren og hvilke OS analysen ble utført fra.

**• Hvor mange entries lagde winzipupdater?**

****

Winzip lagde fant 67 entries

3 driver entries

**• Hvordan får den til autostart? (ASEP)**

**Ta et nytt snapshot i Regshot (clear først)**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Gå inn i winzipupdater og skru av «Kjør ved oppstart»**

**Ta nytt snapshot**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Spørsmål:**

**• Hvilke reg keys (regnshot keys) ble fjernet nå?**

Windowszip update reg keys ble fjernet når den installerte og det ble lagt til nye regnshot keys :24352 keys ble lagt til

**• Har du nå et inntrykk av hva som får autostart?**

Ja det er i innstillingene i winzip updater : options er satt til kjør ved oppstart

****

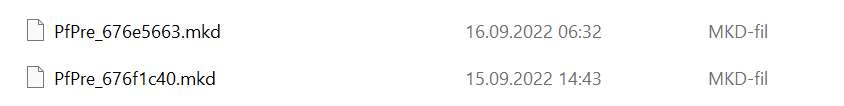
**Se etter prefetch filler**

**• Hvor finner du prefetch filer?**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**• Finner du artifacts fra det du nettopp har kjørt?**

****

Artifacts opptrer som oftest i md filer , men mkd filene kan også konverteres eller lagres som md – filer .

**• Inspiser filene vha et passende program (PECmd, Axiom,**

**Encase). Hva slags informasjon finner du?**

**Se etter lnk filer**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**• Hvor finner du lnk filer? (PATH)**

**C:\Users\usah5\Links**

**• Finner du de?**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**• Trenger du spesial software?**

Link filene er lokalisert på hostmaskin og krever ingen programmer , men lnk filene tilhører en spesifikt program og åpner det programmet hver gang du trykker på lnk filen.

**• Hva står det i de?**

Hver program har en unik lnk fil eller snarvei hvis det er laget noen snarveier

**Trykker på dumptit.exe filen lokaliserer den og går inn i filen**

**Et bilde som inneholder tekst

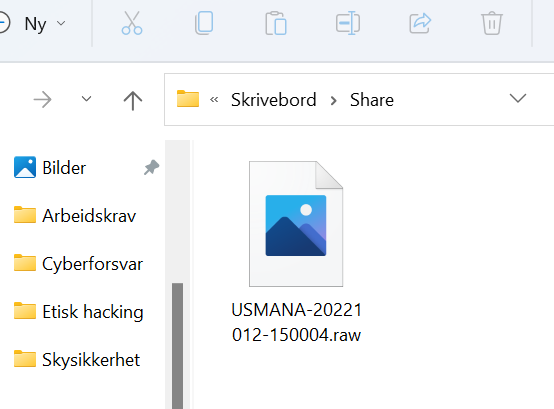
Automatisk generert beskrivelse**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

Kjører dumpit i Windows VM-en

**Får opp success melding**

****

**Kopierer filen over til kali ikke ubuntu (klarer ikke å kopiere til ubuntu!!!):**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Kjørte deretter:** python3 vol.py -f /home/kali/Desktop/USMANA-20221013-073858.raw windows.pslist (Dette skanner hele minnet etter prosesser)

**Et bilde som inneholder bord

Automatisk generert beskrivelse**

**Og med:** python3 vol.py -f /home/kali/Desktop/USMANA-20221013-073858.raw windows.pstree

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Klarer du å se kjørende prosesser via Volatility?**

Ja rapporten som ble generert i terminalen viser kjørende prosseser som windows zip updater (volatility er en opensource program for scanning av RAM- minnet)

**• Finner du igjen noen av prosessene våre? F.eks winzipupdater?**

Fant noen kjente prosesser som regshot – 64 Ansi , Winzip Smart M og Microsoft active

Et bilde som inneholder tekst, plakett

Automatisk generert beskrivelse

**• Finn passord til User ved bruk av Volatility**

**Hint: https://andreafortuna.org/2017/11/15/how-to-retrieve-users-passwords-**

**from-a-windows-memory-dump-using-volatility/**

Får error når jeg prøver guiden ☹ får error når jeg kjører imageinfo

Men kjører heller:

**python vol.py -f /home/kali/Desktop/USMANA-20221013-073858.raw windows.info**

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**Passord knekking volatility: bruker windows fikk det ikke til på kali**

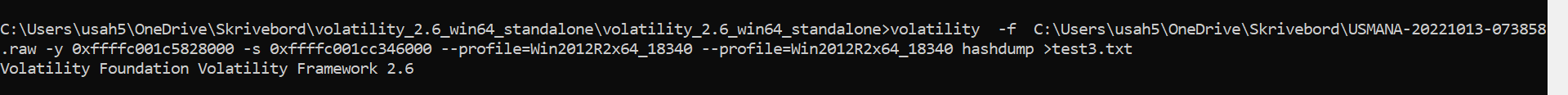
**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Bruker virtual hashene på SYSTEM og SAM men får ingen hashdump liste med brukernavn og passord etter å ha åpnet filen. Den er tom**

****

**Prefetch er:**

**Forhåndshenting lar en nettleser i det stille hente de nødvendige ressursene som trengs for å vise innhold som en bruker kan få tilgang til i nær fremtid.**

**Husk å kjøre mot pf filene!**

**Brukte en prefetch file i pecmd: (Slik finner man artifacts i pf filer: )**

.\PECmd.exe -f "C:\Windows\Prefetch\CMD.EXE-0BD30981.pf"

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Et bilde som inneholder tekst

Automatisk generert beskrivelse**

**Fant dll og exe filer som er en type artifact ifølge**

**Se link:**

[**https://learn.microsoft.com/en-us/azure/devops/pipelines/artifacts/artifacts-overview?view=azure-devops&tabs=nuget**](https://learn.microsoft.com/en-us/azure/devops/pipelines/artifacts/artifacts-overview?view=azure-devops&tabs=nuget)