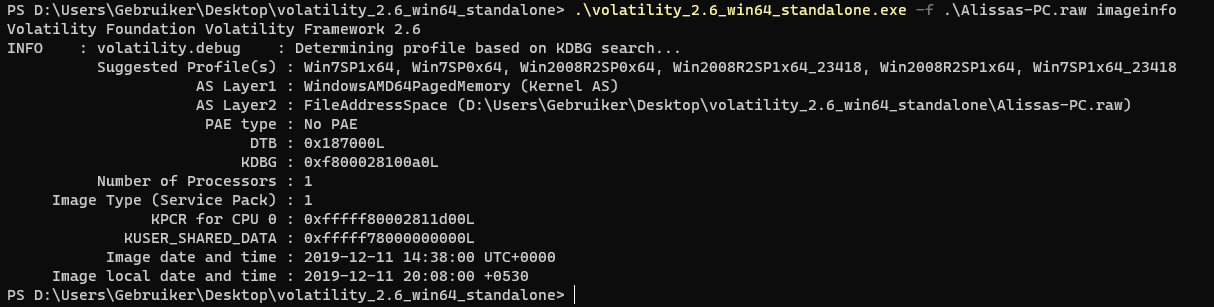
**Wachtwoord vinden**

Voor het wachtwoord uit de. Raw file te halen heb ik eerst gezocht naar software waarmee dit mogelijk is. Na een tijdje zoeken en een aar programma’s uit te proberen die ik in de cursus besproken werden heb ik uiteindelijk volatility geprobeerd een hiermee kon ik aan het werk gaan.

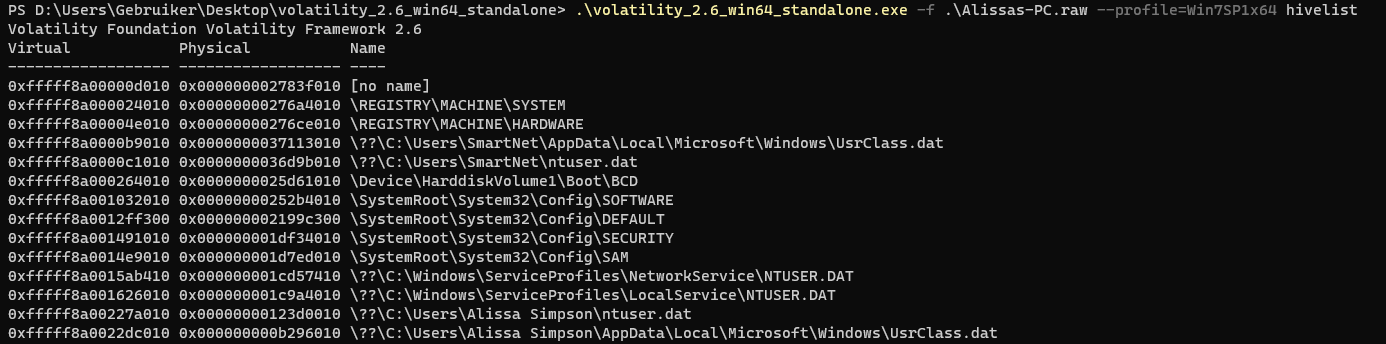
Voor het vinden van het wachtwoord heb ik proberen op te zoeken hoe ik dit moest doen en ben ik uiteindelijk op een YouTube video gekomen die dit zeer snel en simpel voordeed.

Dit zijn de stappen die ik heb uitgevoerd.

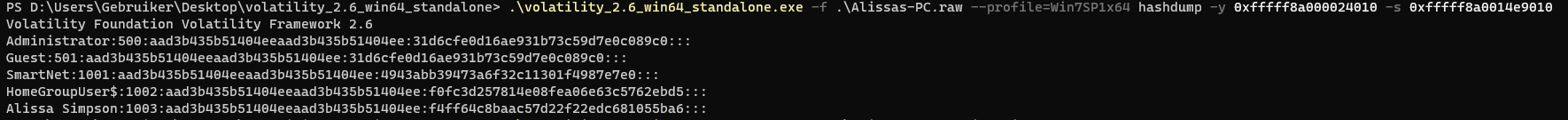
1. Voor het gemakelijk gebruiken van volatility moest ik eerst het juiste profiel van de memory dump vinden dit deet ik met het commando “.\volatility\_2.6\_win64\_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 imageinfo” Dit gaf mij de informatie over de memory dump (Zie foto).



1. Daarna ben ik de virtuele adressen van het register van het systeem gaan zoeken met het commando: “.\volatility\_2.6\_win64\_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 hivelist” (zie foto). Hieruit ben ik dan het virtuele address van de hardware van het systeem gaan halen en die van de gebruiker SAM.



1. Deze 2 virtuele adressen heb ik dan gebruikt om het volgende commando uit te voeren: “.\volatility\_2.6\_win64\_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0014e9010” (zie foto). Hier kunnen we dan de hash van het wachtwoord van de gebruiker Alissa zien.



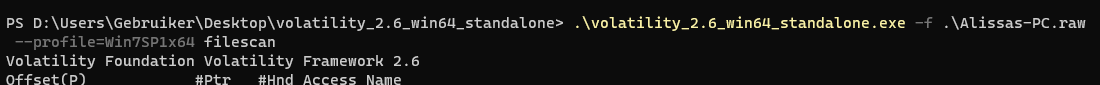
1. Deze hash kunnen we dan in een hash data base zoeken hier kregen wij als resultaat. Goodmorningindia



**Rar file**

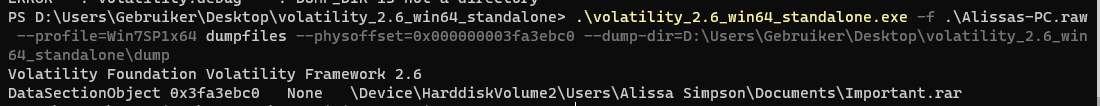
Voor het vinden van important.rar hebben we de volgende stappen uitgevoerd.

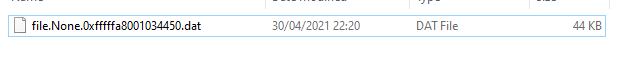
1. Als eerste stap hebben we een scan gemaakt van alle files die op het systeem staan. Dit hebben we gedaan met het volgende commando: “.\volatility\_2.6\_win64\_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 filescan” (zie foto). Hieruit konden we dan de offset van de rar file halen





1. Deze offset hebben we dan gebruikt om de file uit het systeem te halen met het commando: “.\volatility\_2.6\_win64\_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 dumpfiles --physoffset=0x000000003fa3ebc0 --dump-dir=D:\Users\Gebruiker\Desktop\volatility\_2.6\_win64\_standalone\dump” (zie foto).





1. Nu dat we de .dat file hebben moesten we enkel nog de file uit de rar halen dit deden we door de .dat file te oppennen met winrar en de file te extracten met behulp van het gevonden paswoord.

