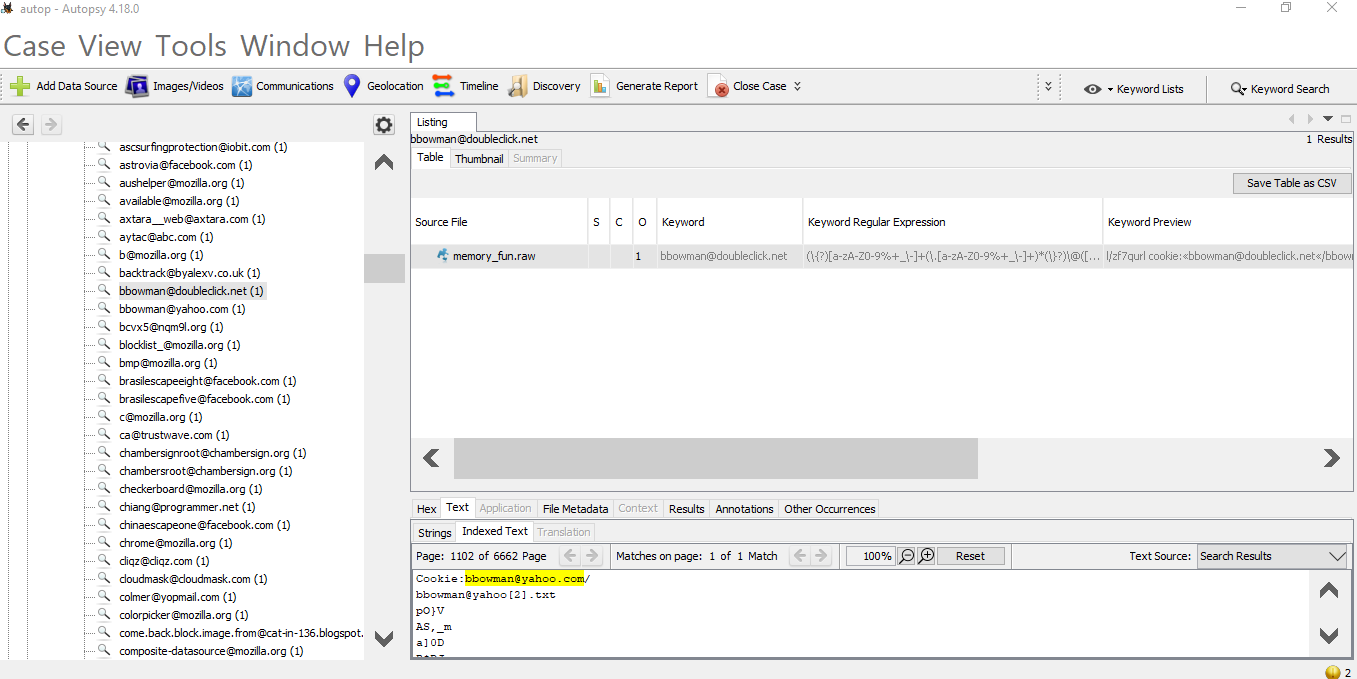
**Task: “Bobby Bowman has been fired. We need to log on to his account can you get his plaintext password for us?" --- Password: “venerable”**

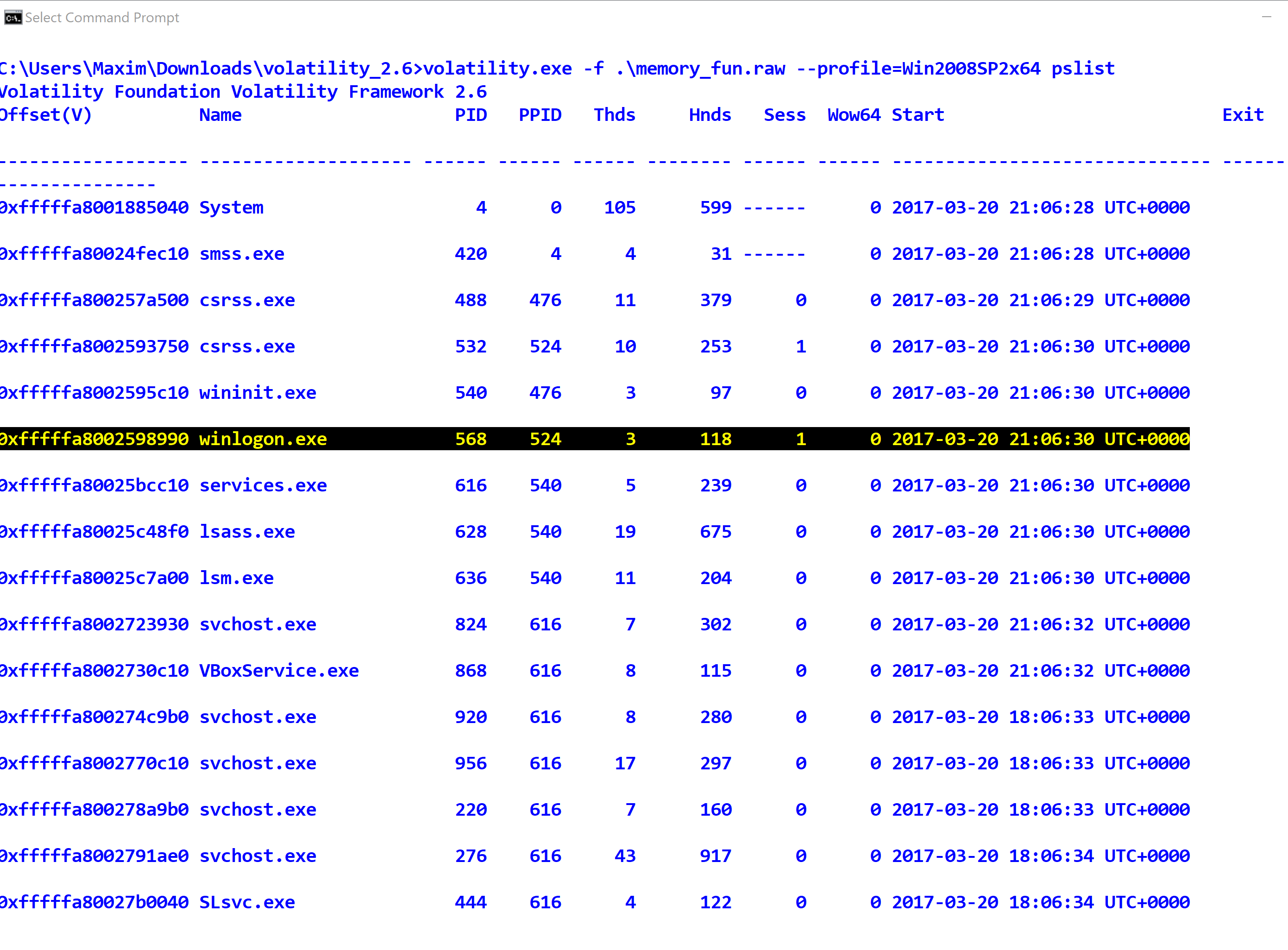
Seeing as the given file was zipped, we began with unzipping the file and found there was a single file within – memory\_fun.raw. We initially attempted to obtain the plaintext password by running the file through the tool “autopsy”, but had little luck beyond seeing the names of emails belonging to Bobby Bowman and some other people.



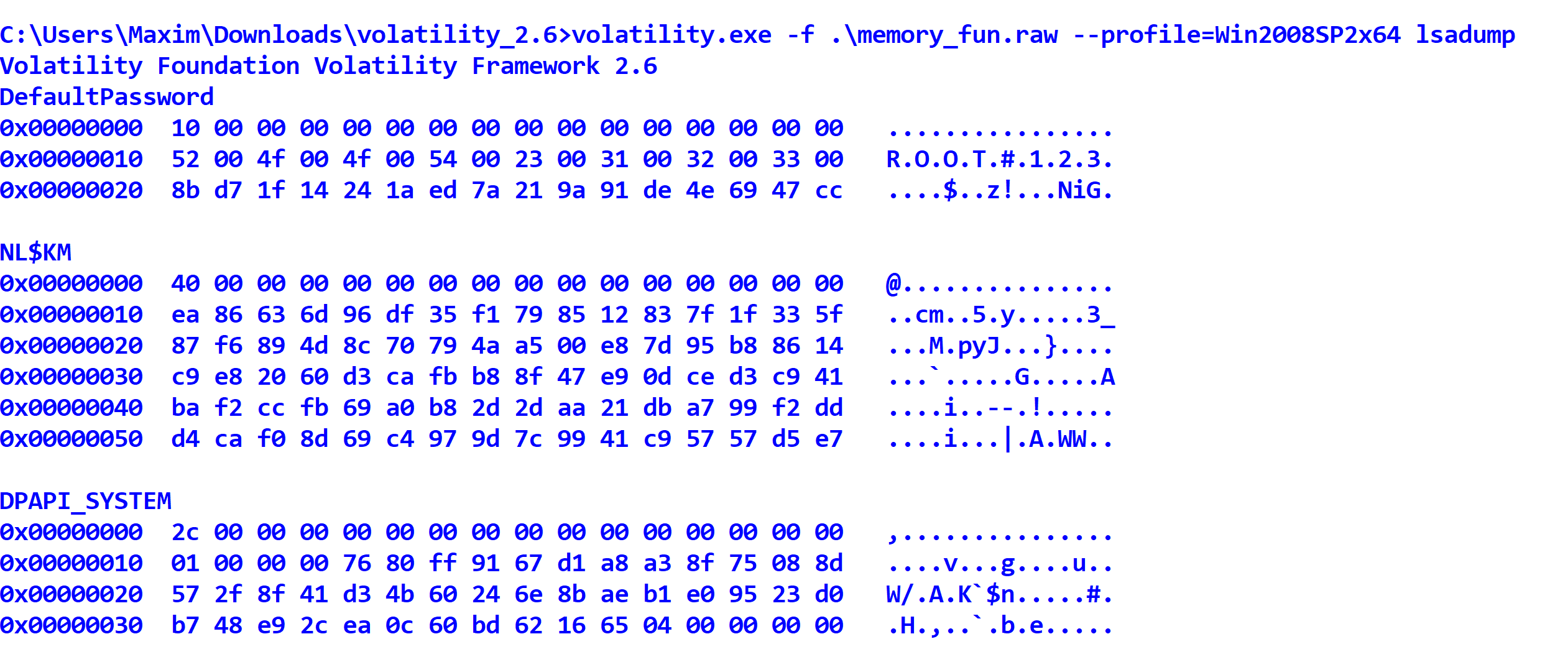
We then moved on to using Volatility, beginning with getting the image info of the file with the command “volatility.exe -f .\memory\_fun.raw imageinfo”. This command told us that the most likely profile was a Windows 2008 64 bit machine which we would include in further commands.



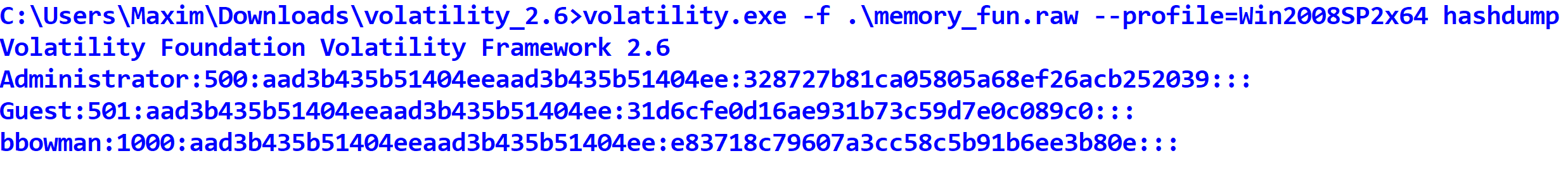
We then ran “volatility.exe -f .\memory\_fun.raw –profile=Win2008SP2x64 pslist” to see the running processes of the image and noticed a winlogon.exe.



Unsure of how to exactly get a password from this process, we moved on to lsadump which told us a default password but not much more beyond that.



Finally, we had some luck with the hashdump command (volatility.exe .\memory\_fun.raw –profile=Win2008SP2x64 hashdump) which told us the encrypted cached domain credentials of the admin, guest, and bbowman account.



We ran the hash (e83718c79607a3cc58c5b91b6ee3b80e) through a hash cracker and determined that the password of Bobby Bowman is “venerable”.

