VENSELVAM **231901061**

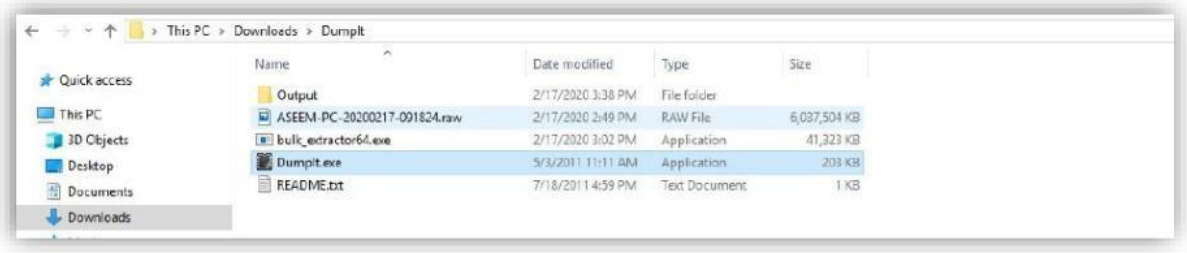
EXPERIMENT-08

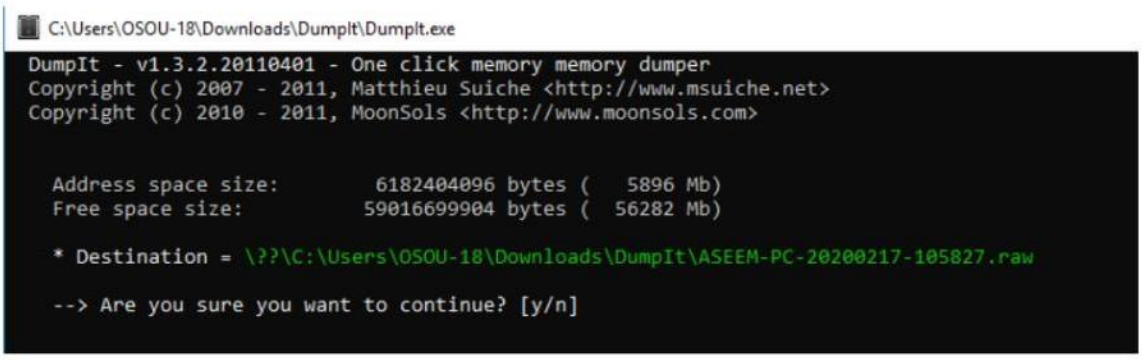
Aim :

How to Collect Email Evidence in Victim PC

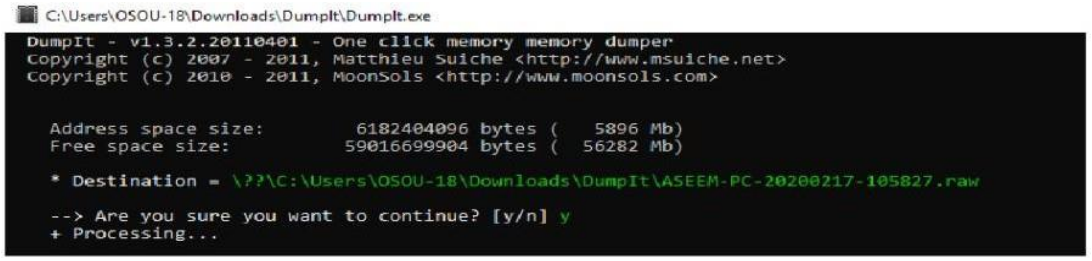
Procedure :

- To collect email evidence from Victim PC the first step is to capture the victim's RAM. This can be possible using **dumpit** tool.
- This utility is used to generate a physical memory dump of Windows machines.
- It works with both x86 (32-bits) and x64 (64-bits) machines. The raw memory dump is generated in the current directory, only a confirmation question is prompted before
- starting.
- Perfect to deploy the executable on USB keys, for quick incident responses needs.
- Run Dumpit.exe file the raw memory dump will be generated and save to the same directory

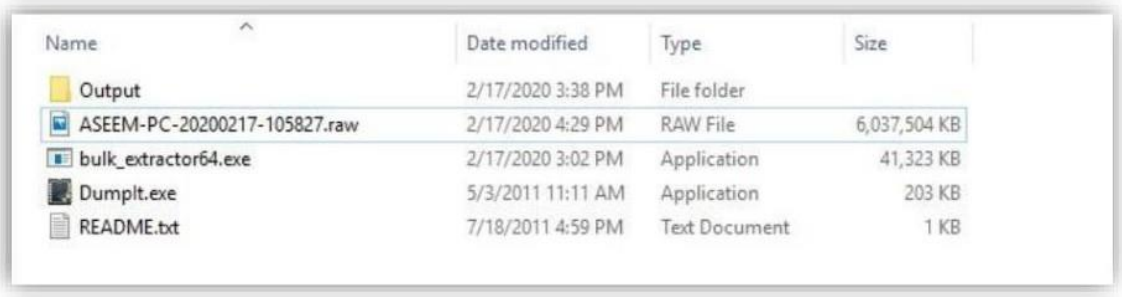




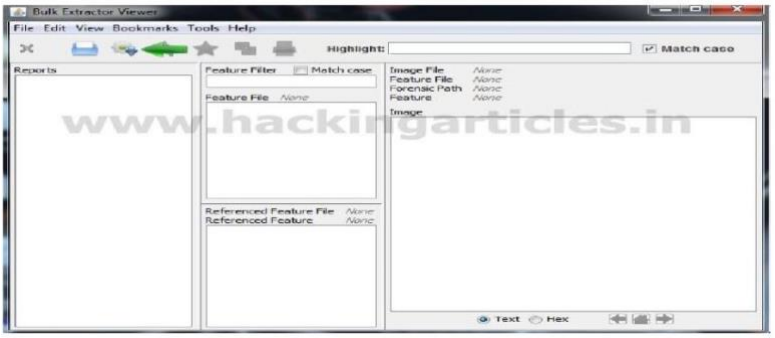
Write 'Y' for processing



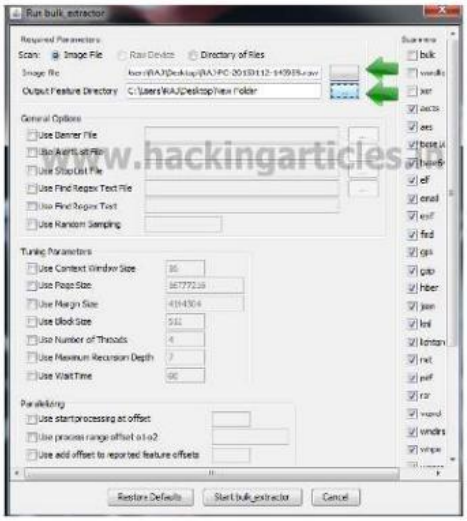
The output .RAW file will be as follows



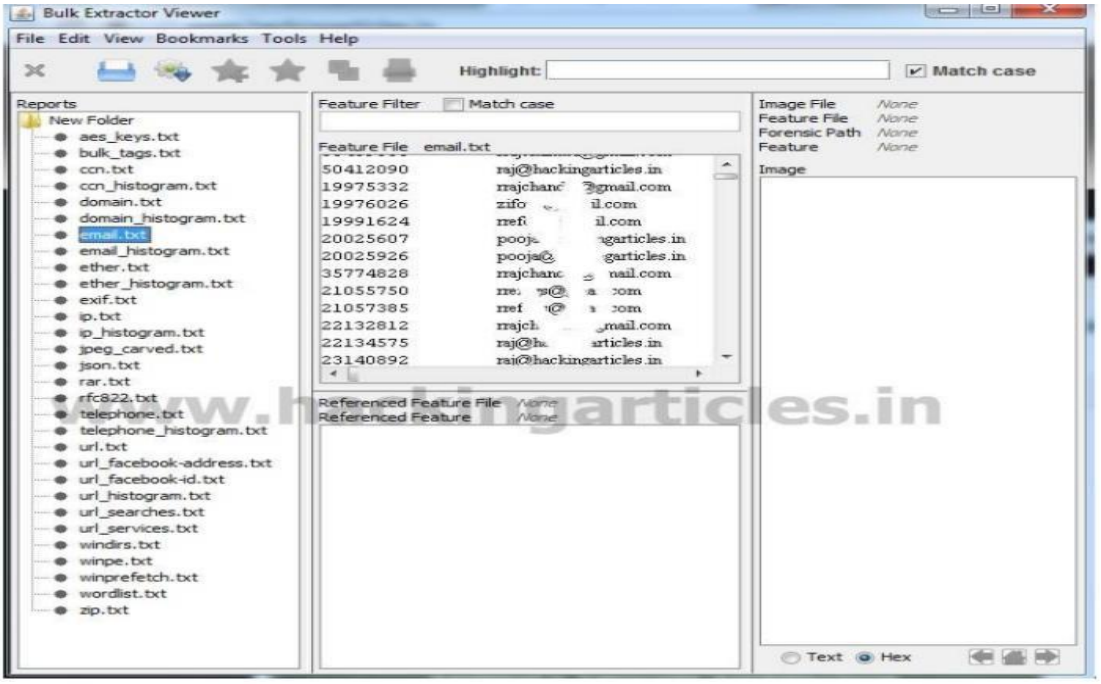
Then Download bulk extractor viewer from GitHub and install it in your PC. Now open bulk extractor viewer and click on to generate report.



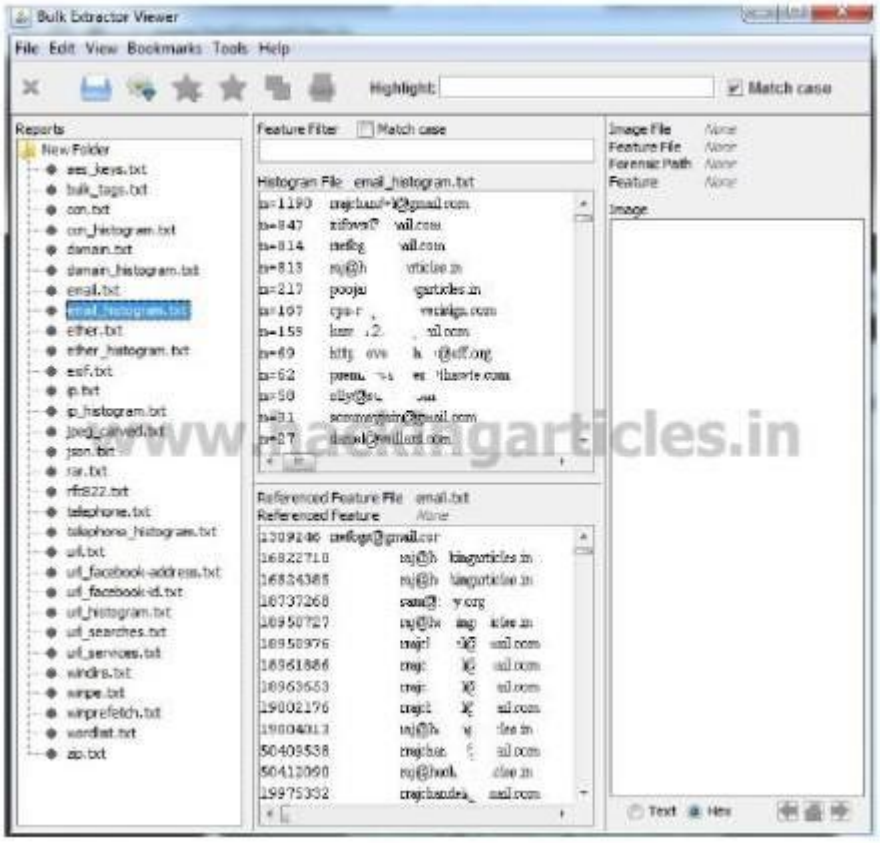
Now select the dump it image file and select an output folder for the report and click onstart bulk extractor as seen below



Now in order to investigate the victim saved information of Email ID Click on email.txt as seen Below.



And also click on email_histogram.txt



Result:

Thus, the forensic tools executed successfully, and the evidence was captured and analyzed accurately.