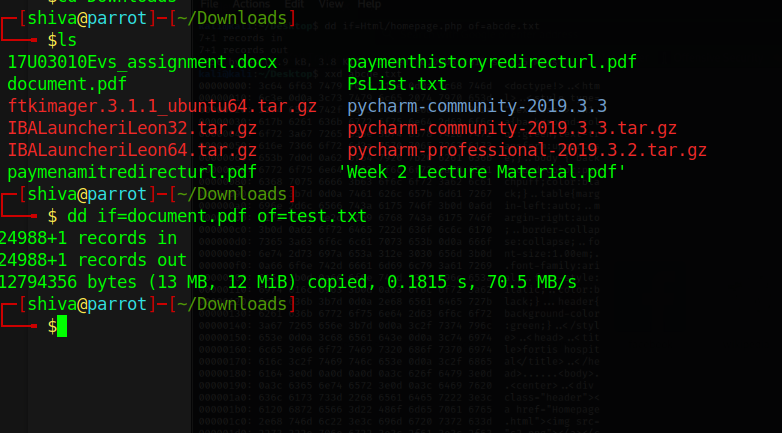
**ASSIGNMENT 1 DIGITAL FORENSICS**

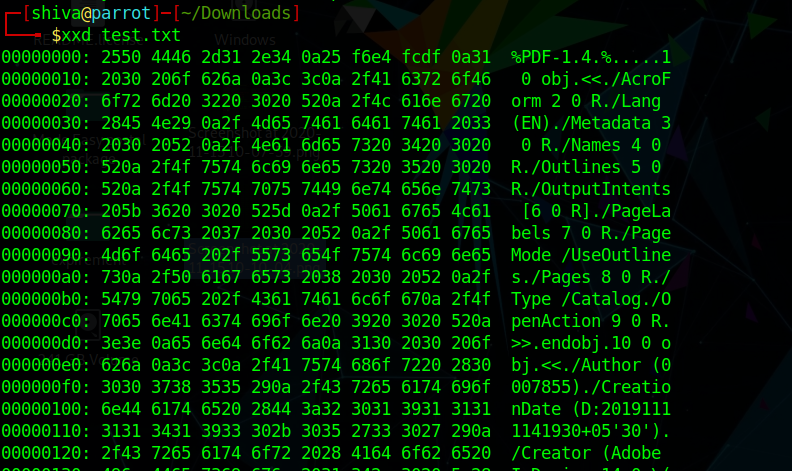
scholar no. 17U03010

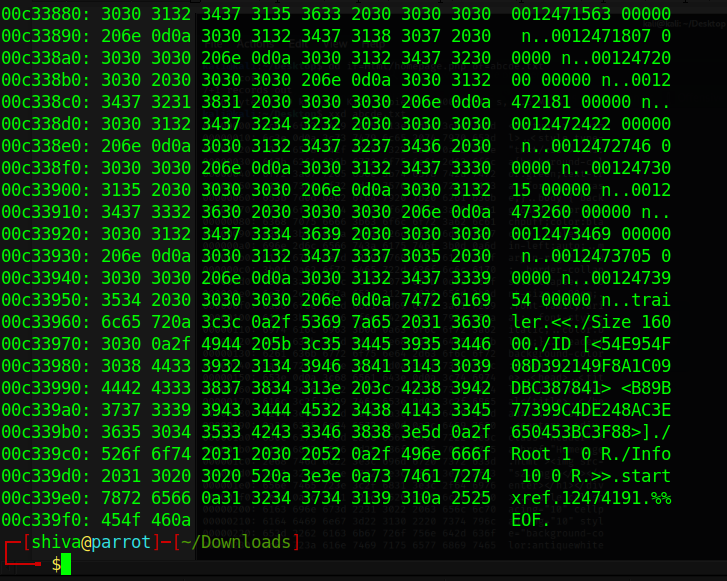
Name : Anurag sharma

1. DD command for raw forensic image creation .

Solution :

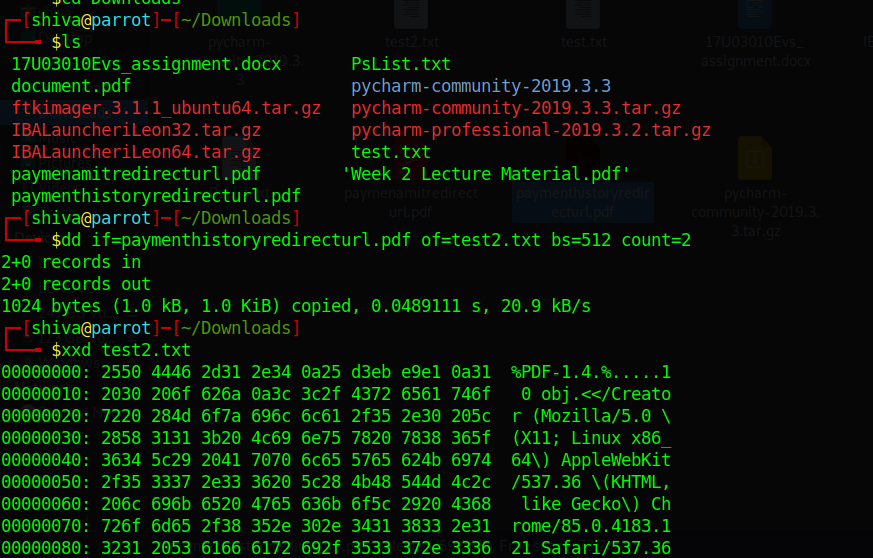


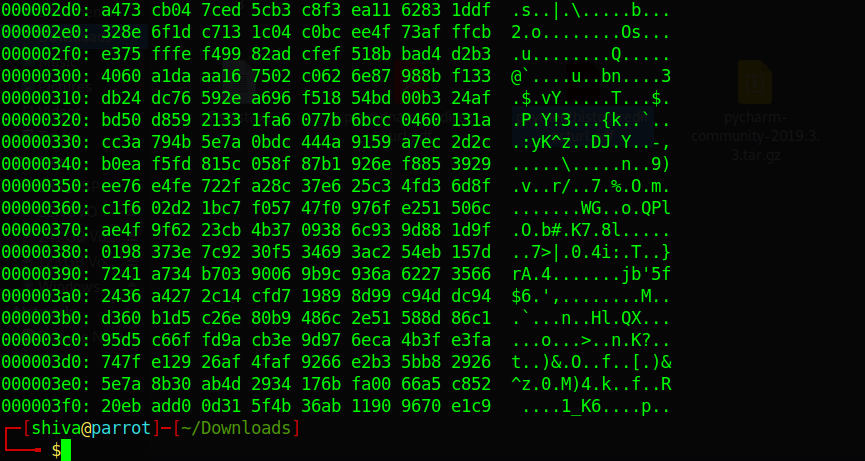




1. DD command for extracting specific block of sector (data carving).

Solution :

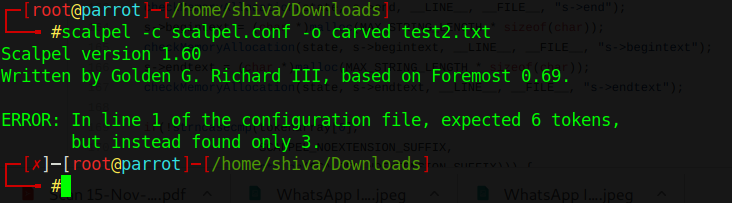




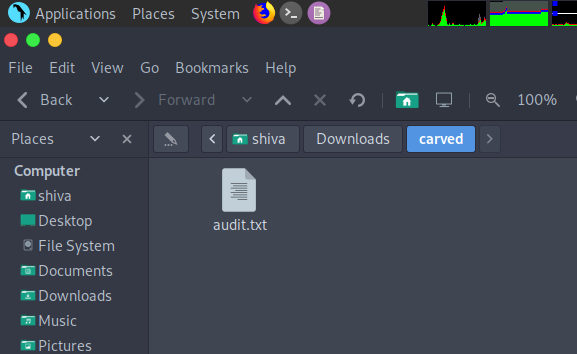
3.perform data carving expirement using open source scalpel and foremost tool .

Solution : for this scalpel.conf file must be in the same folder as your ’ -o carved file’ .

Also if scalpel.conf file is commented you will need to edit and remove all comments from scalpel.conf but be carefully do not remove tokens with it.



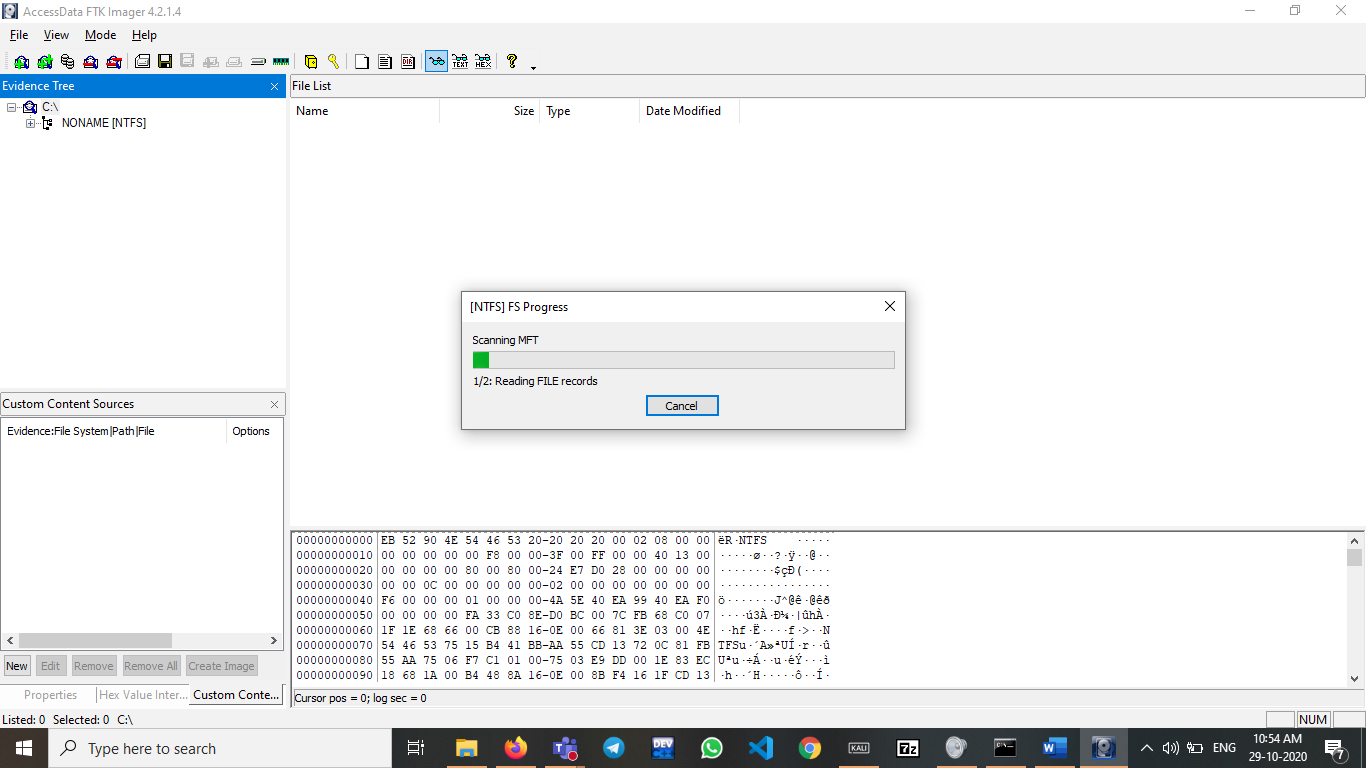
Output file :

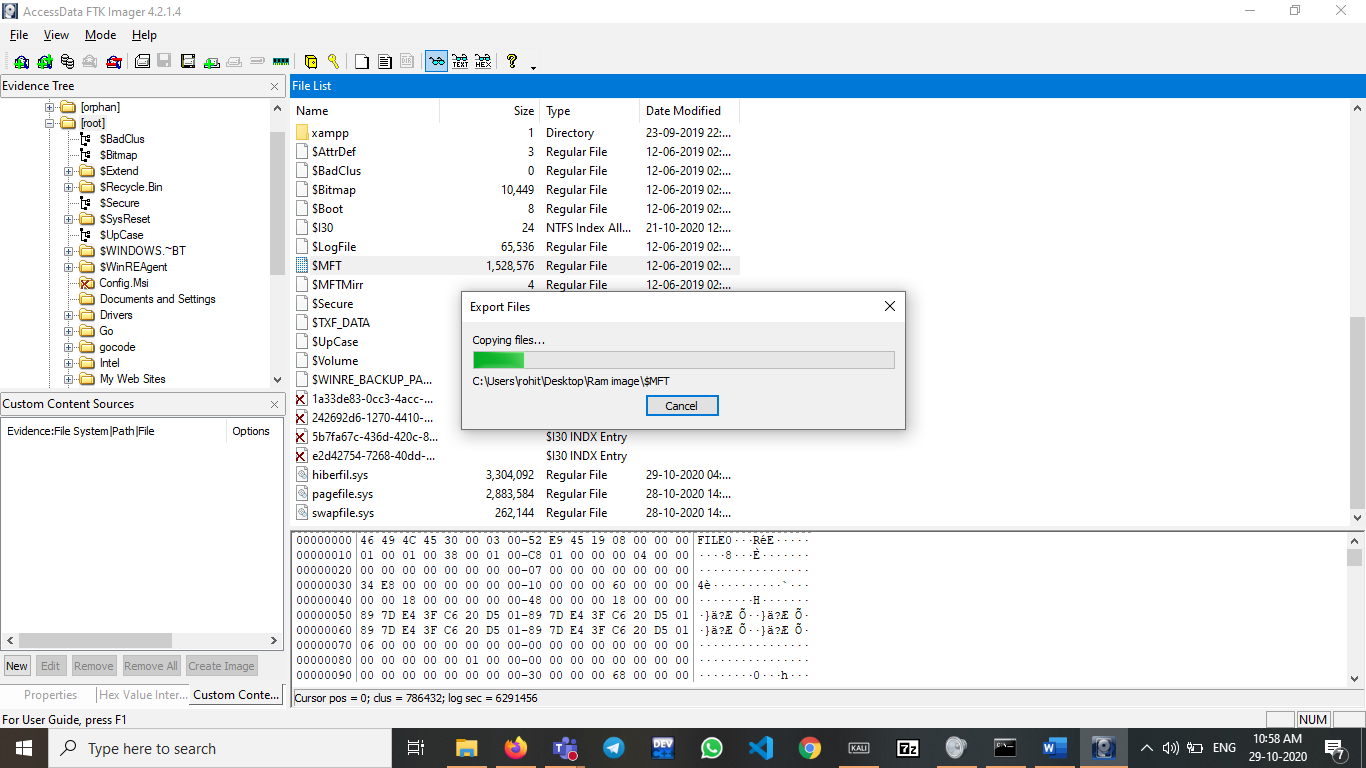


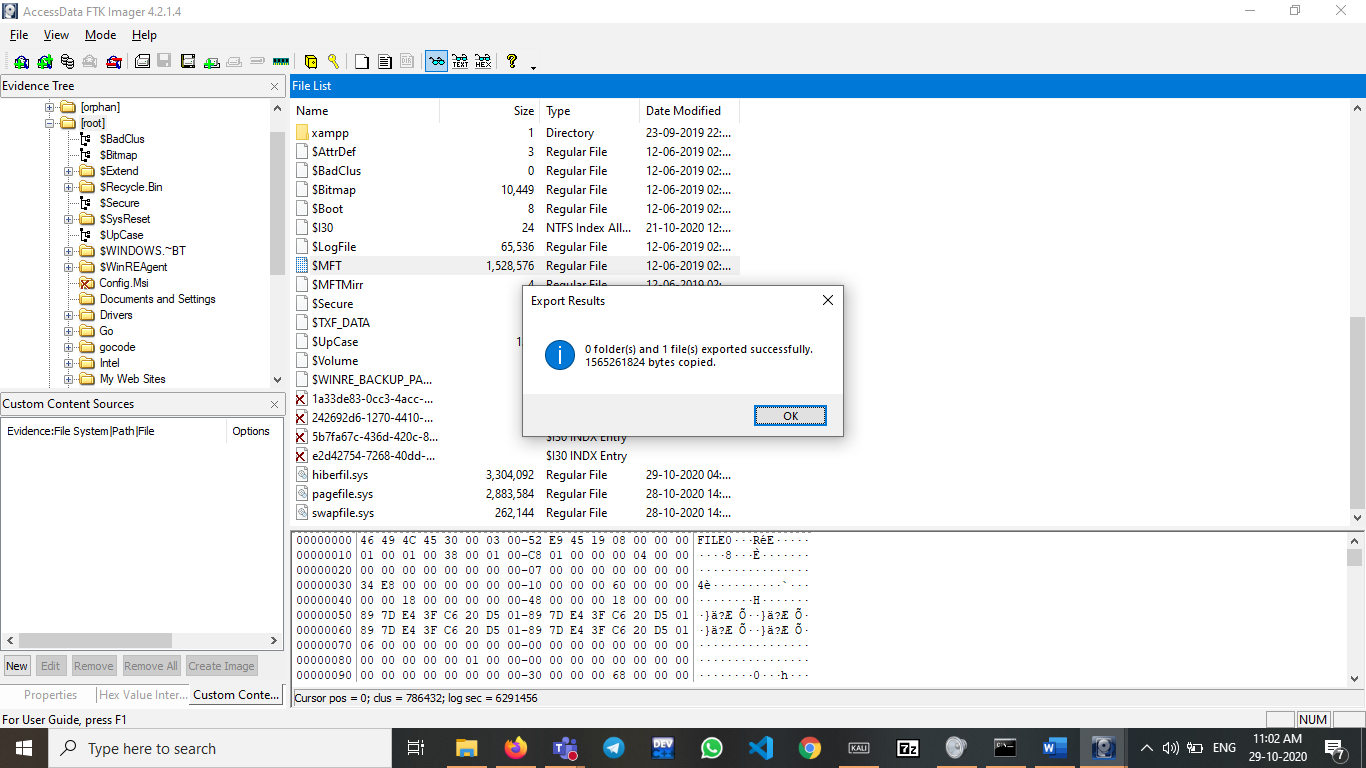
4.using ftk imager tool extract the $MFT table of NTFS partition .

Solution : **FILE> ADD EVIDENCE>LOGICAL MEMORY>DRIVE>ROOT>$MFT**

**RIGHT CLICK ON $MFT AND EXTRACT**





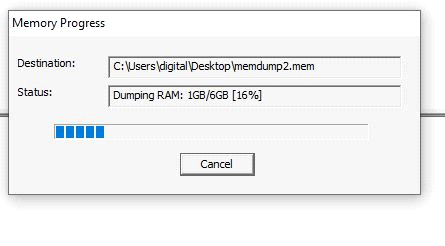


5. create a RAM image dump using opensource tools.

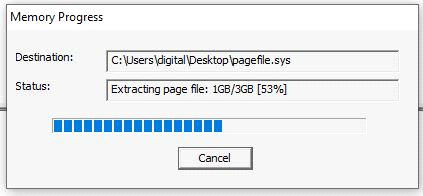
Ans . install FTK imager tool . then follow .

File > Capture memory > Name of memory> Export location > Capture Memory (button)

RAM(4gb) + GPU(2gb) capture = memdump.mem



page file capture = pagefile.sys



6. Install Volatility 3 tool for ram image examination and try to examine potential source of artifacts from ram captured .

Solution : if you don’t have git installed install it first via <https://git-scm.com/download/win> link

Then your git will work fine in cmd.

I have analyzed same file which is captured in above Question memdump.mem.

