­

Digital Forensics (CS4419-CS6419)



2021SM\_CS\_6419\_FRE1A

Assignment-03

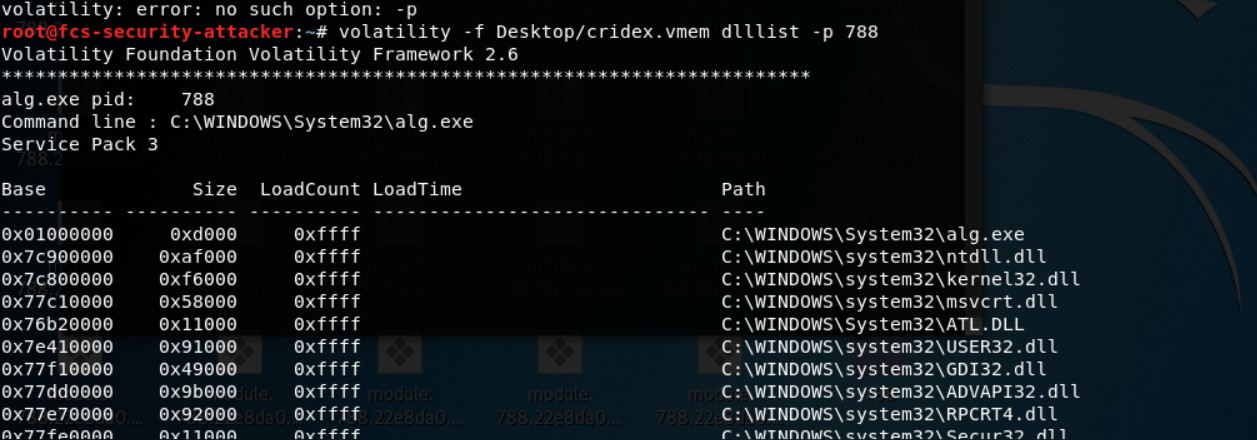
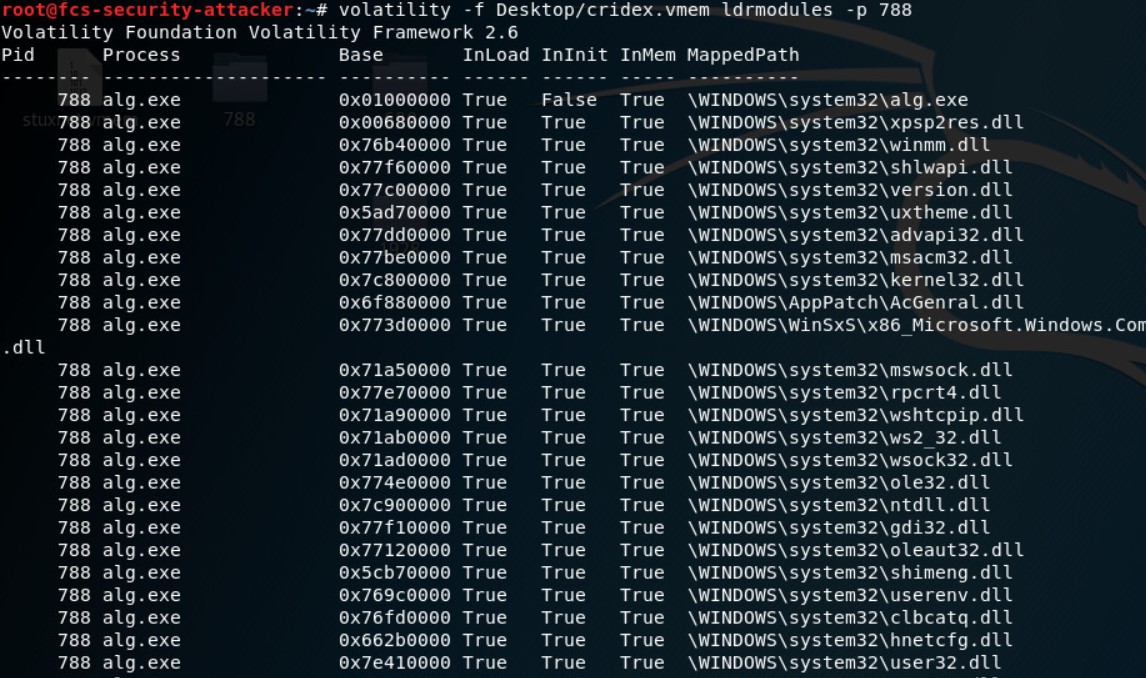
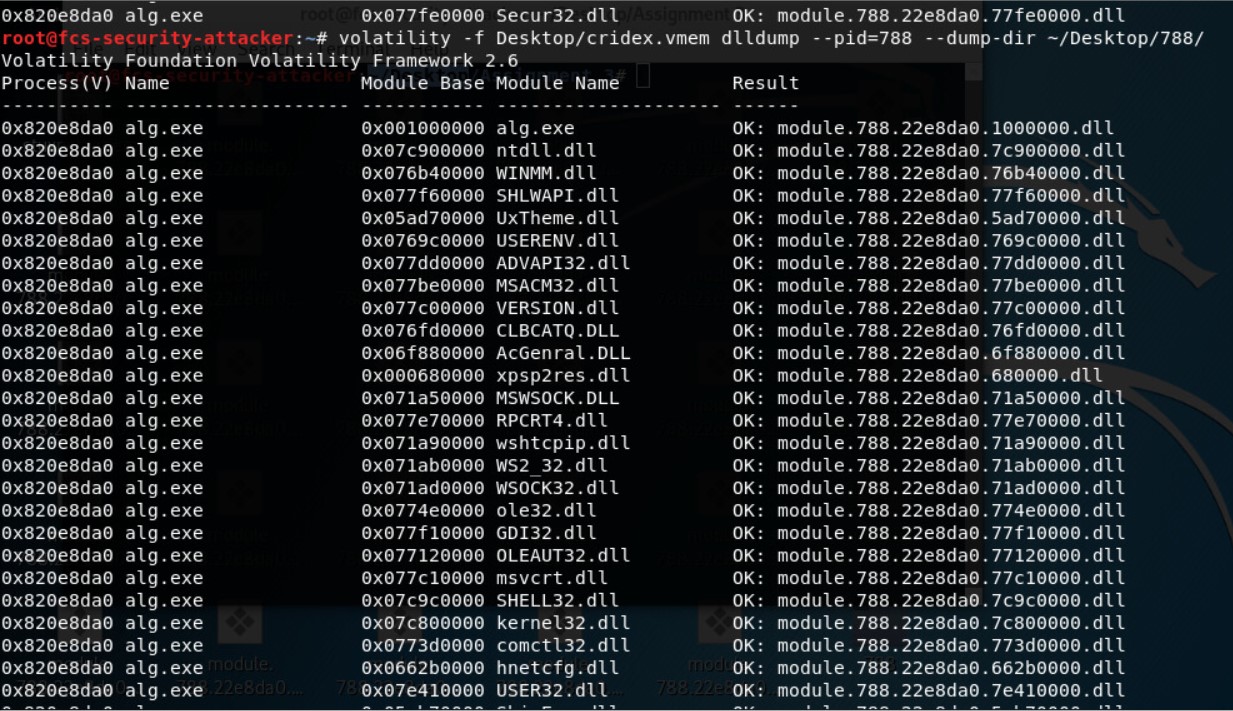
Prepared by:  
Mohammadali Rahnama

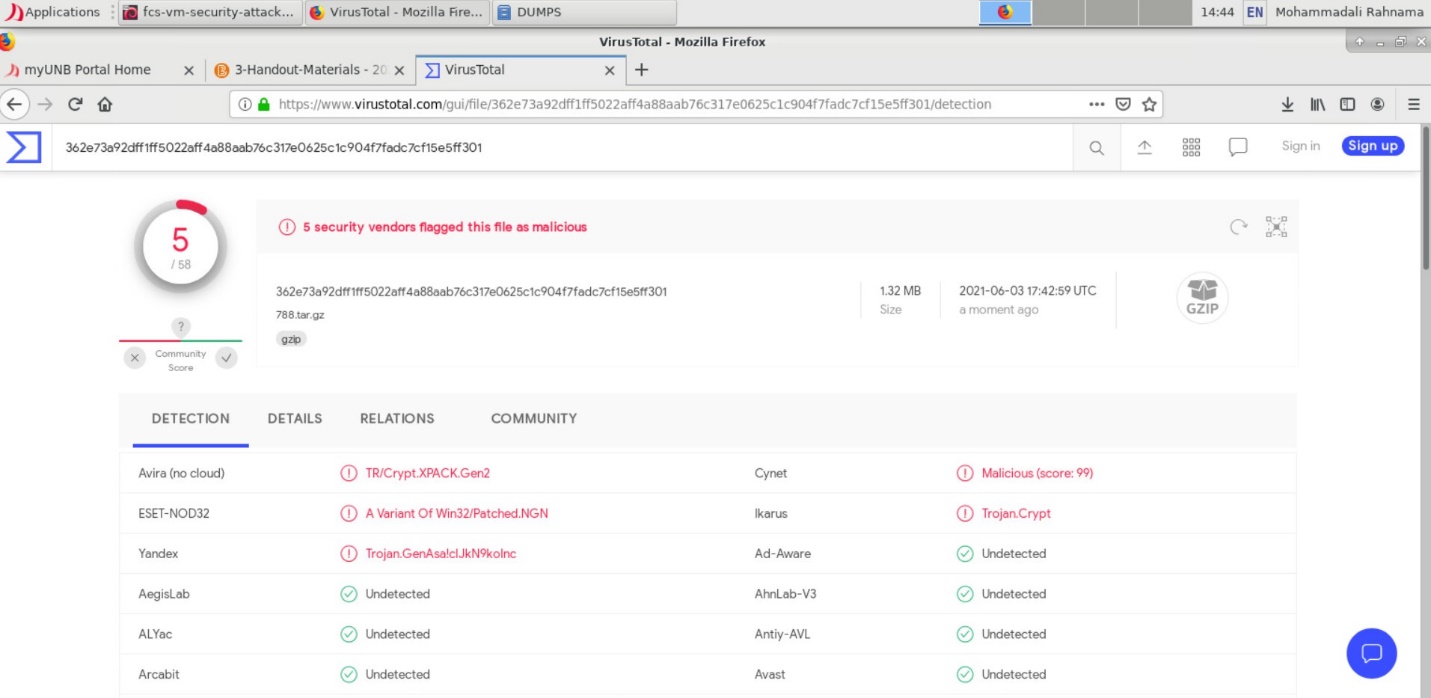
Student number:

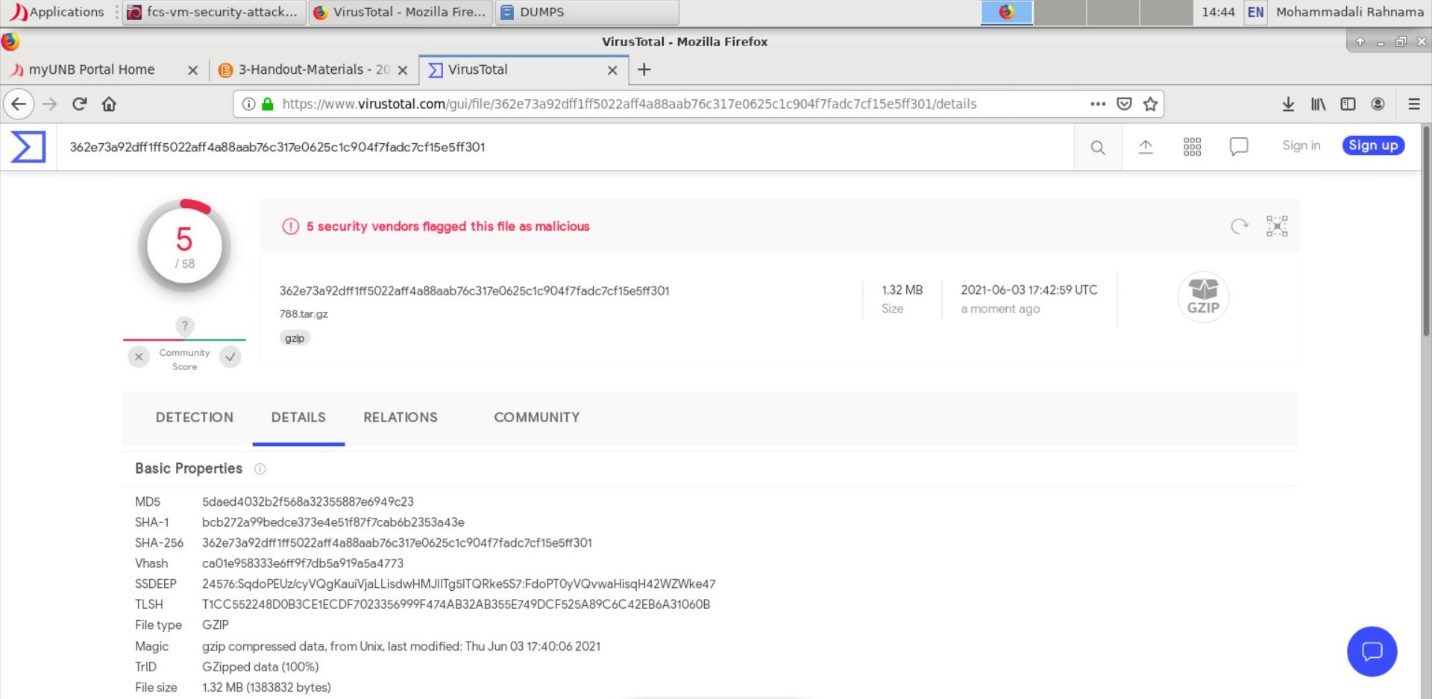
3709515

1. **Volatility commands and snapshot of the Virustotal detection results for the 4 PIDs**

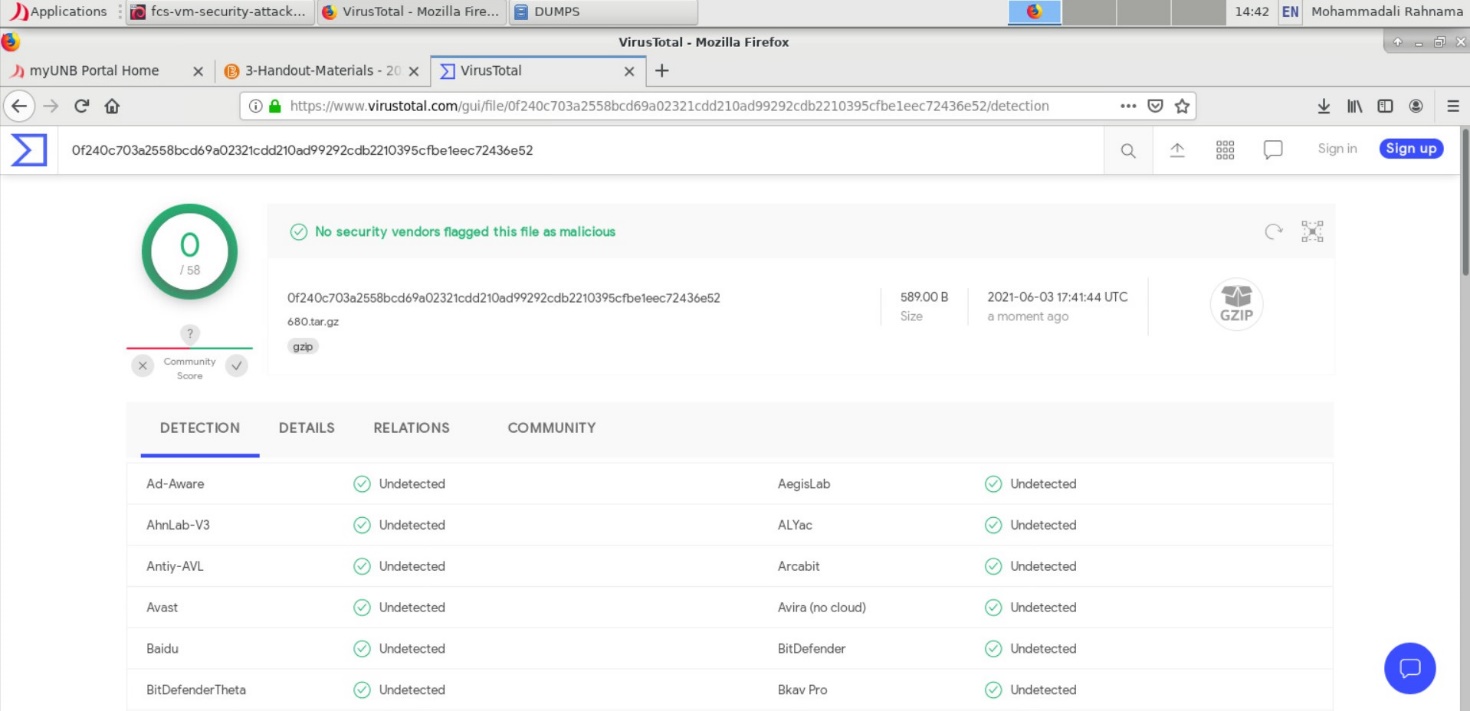
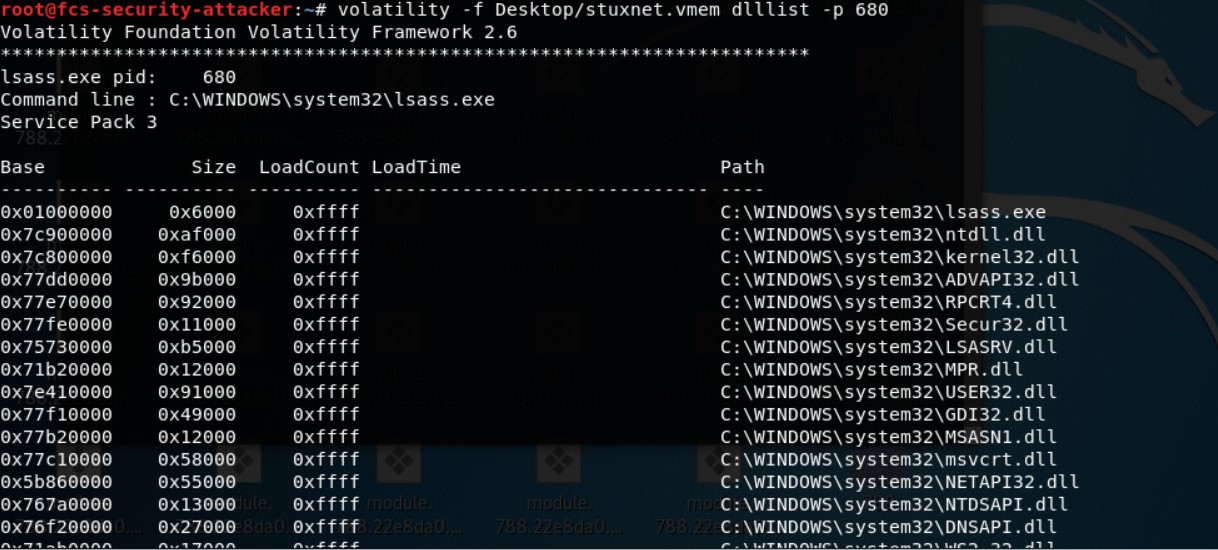
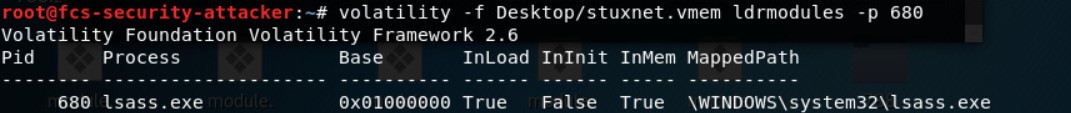
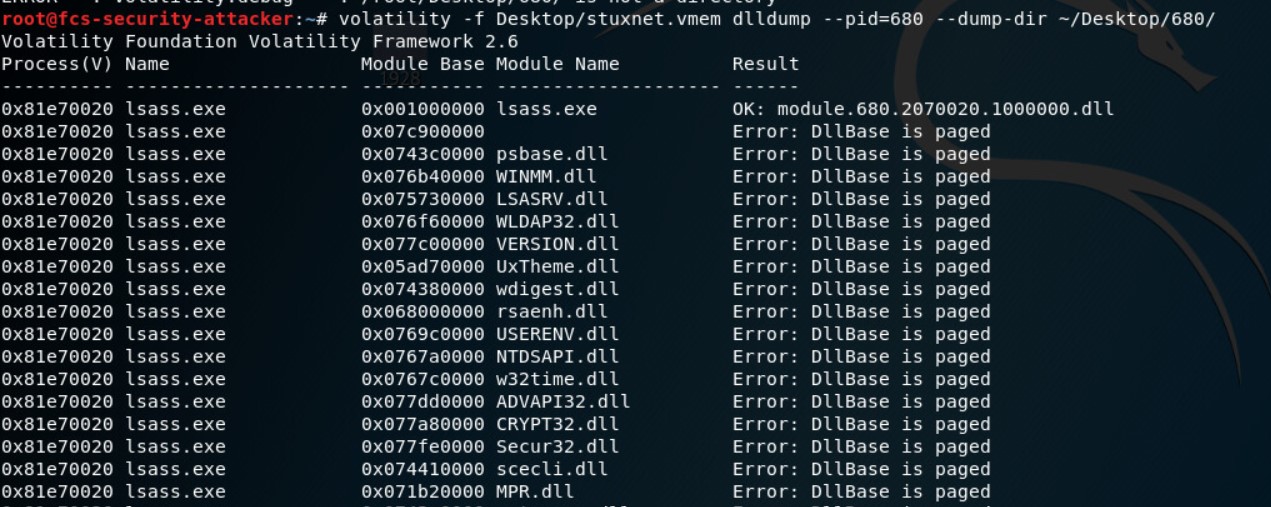
* volatility -f Desktop/ cridex.vmem dlllist -p 788
* volatility -f Desktop/ cridex.vmem ldrmodules -p 788
* volatility -f Desktop/cridex.vmem dlldump --pid=788 --dump-dir ~/Desktop/788/



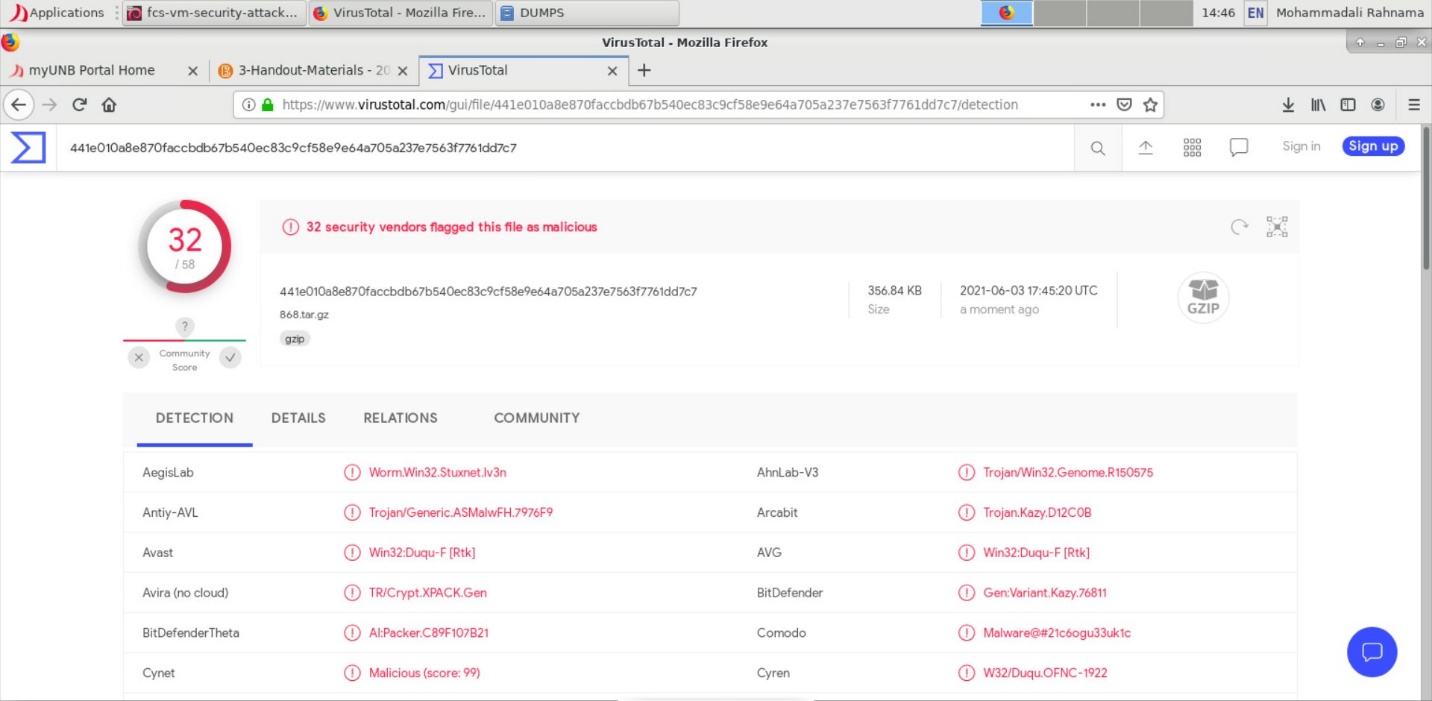
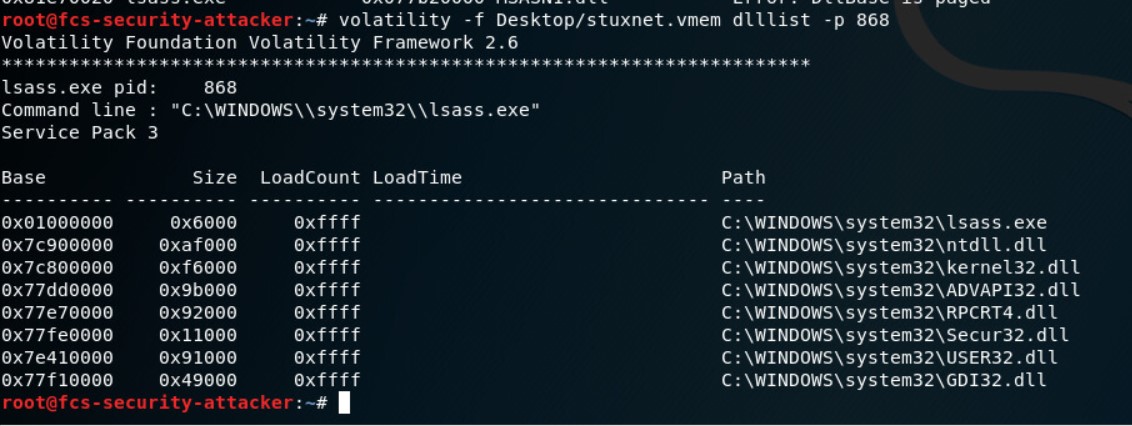
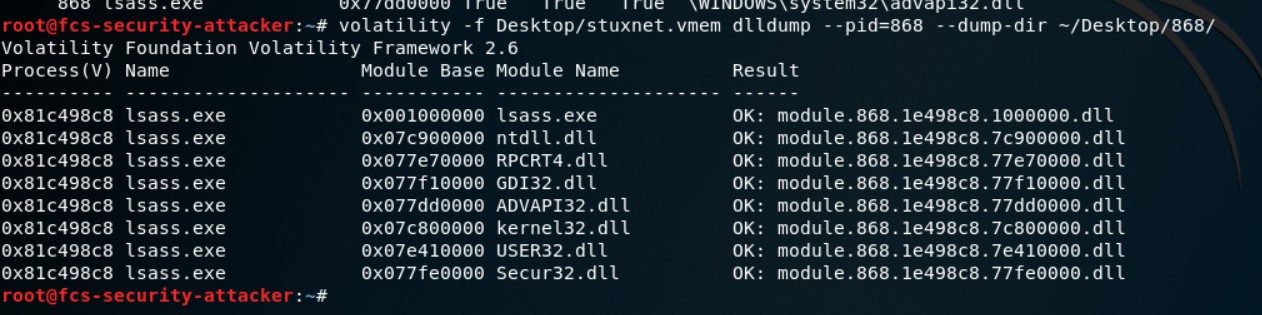
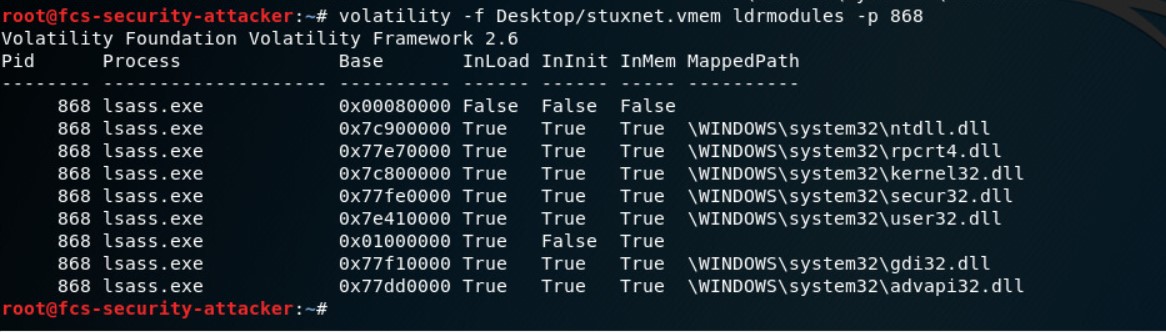




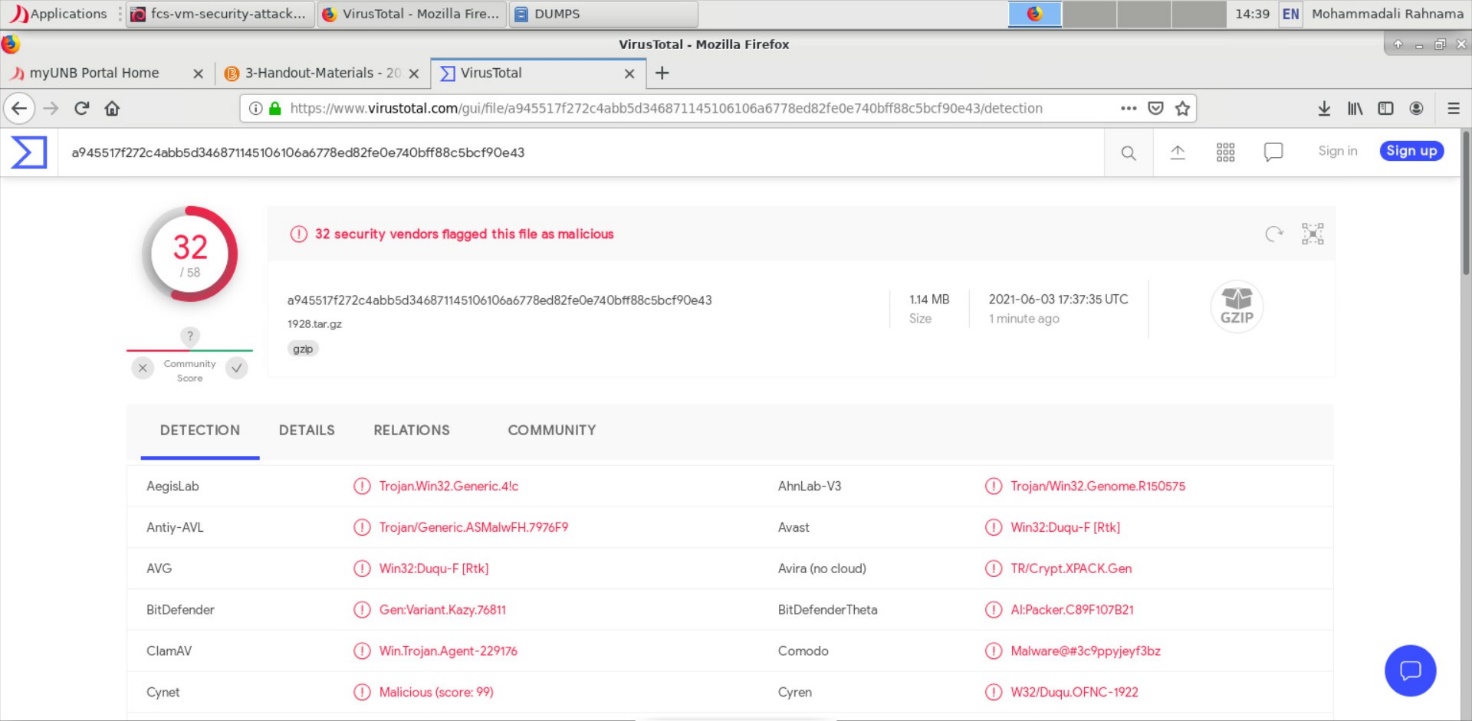
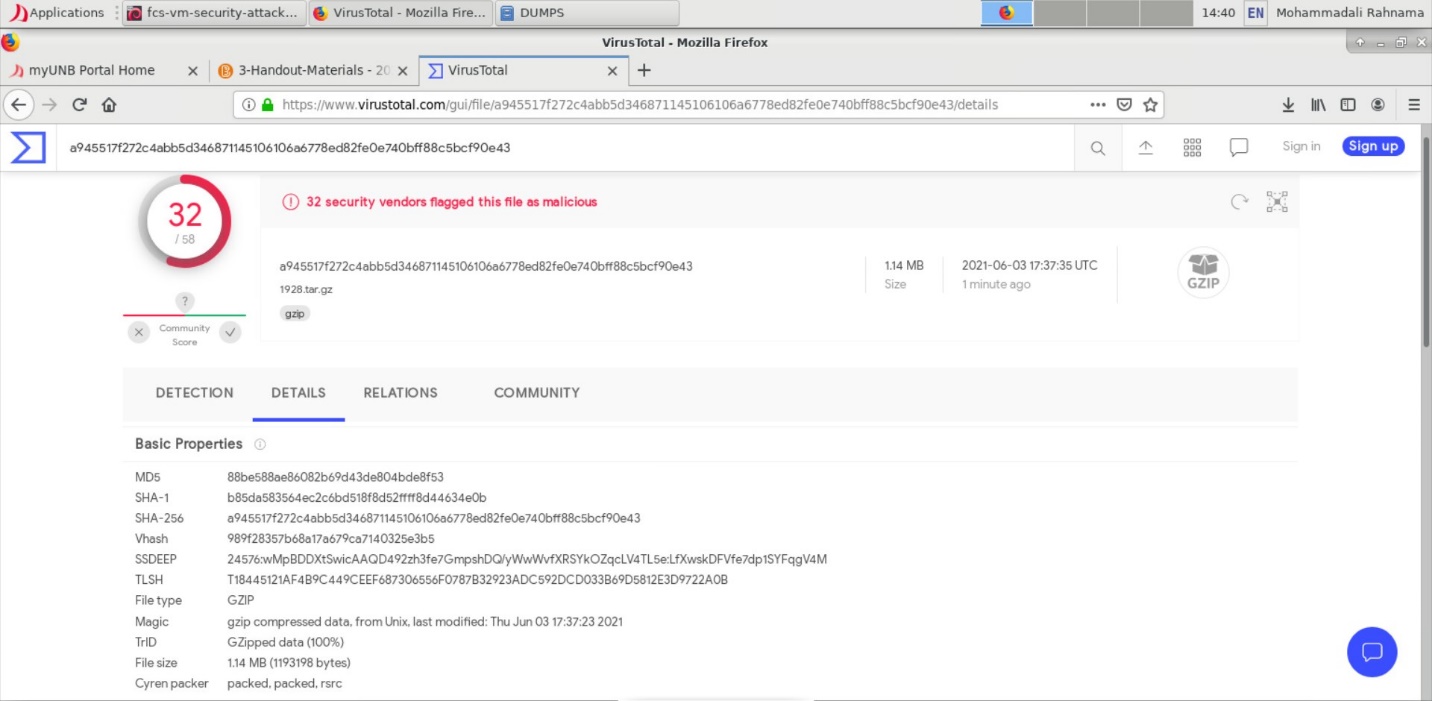
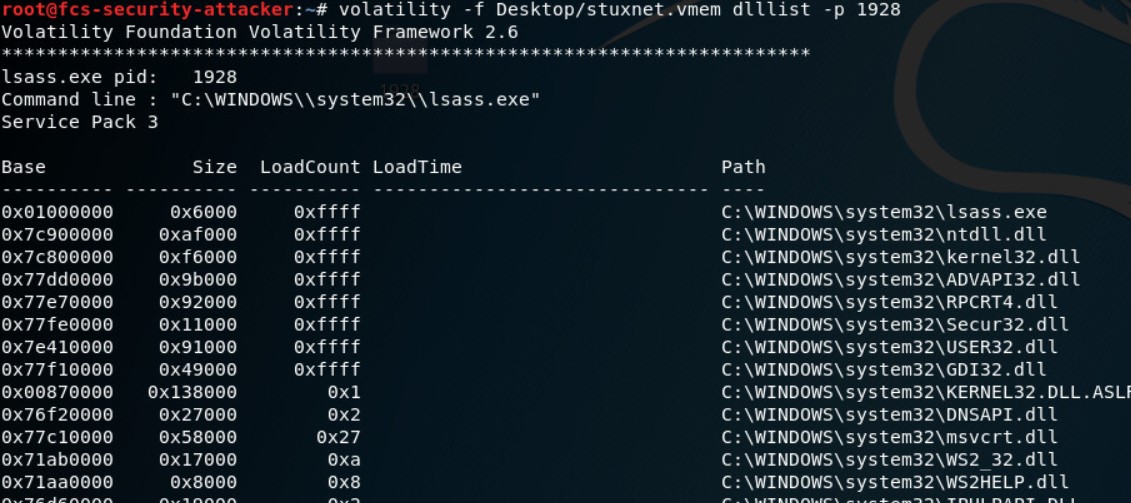
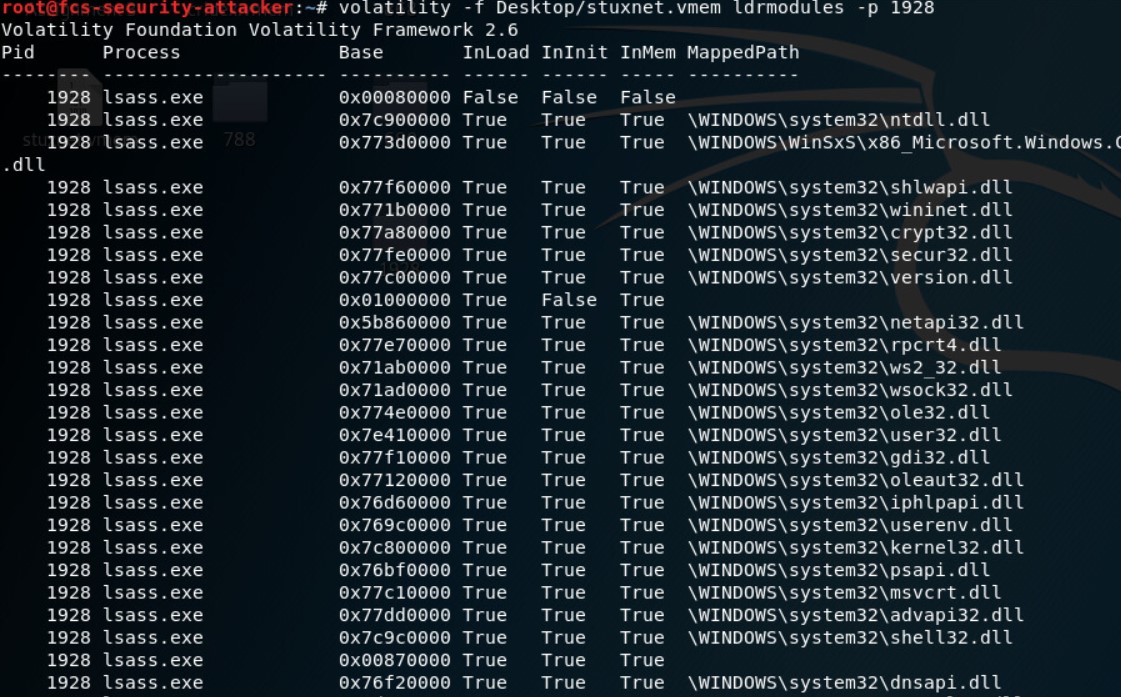
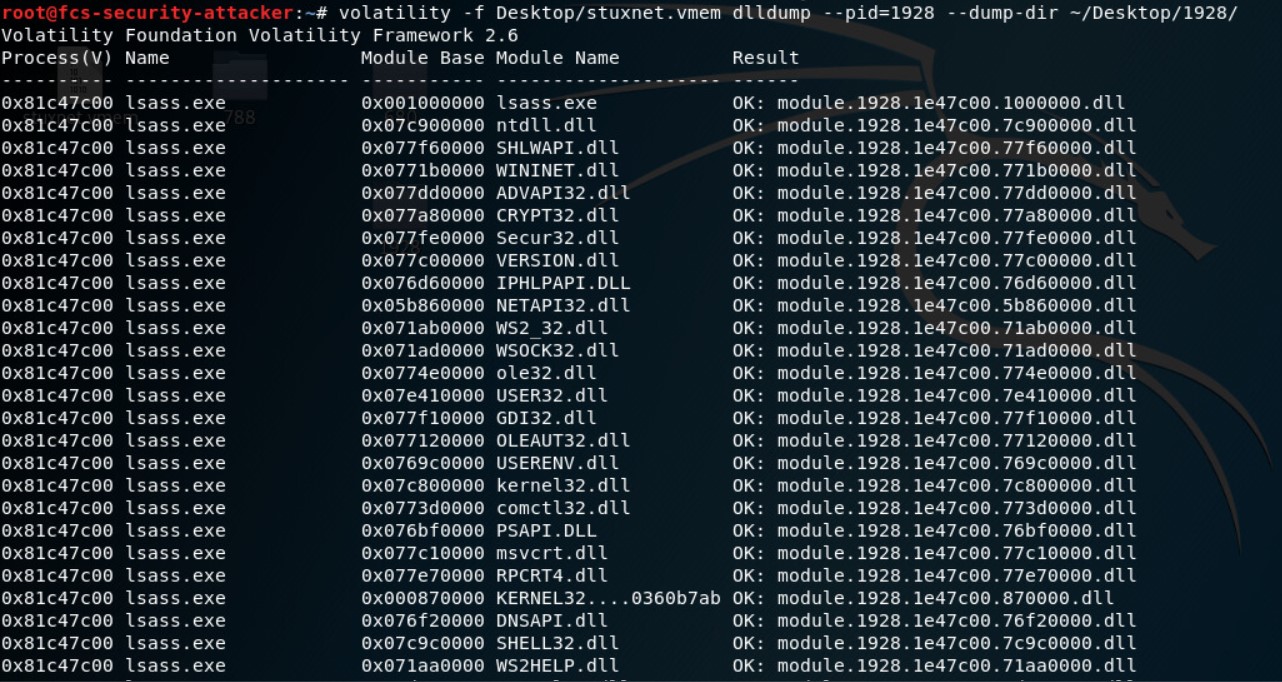
* volatility -f Desktop/stuxnet.vmem dlllist -p 680
* volatility -f Desktop/stuxnet.vmem ldrmodules -p 680
* volatility -f Desktop/ stuxnet.vmem dlldump --pid=680 --dump-dir ~/Desktop/680/



* volatility -f Desktop/stuxnet.vmem dlllist -p 868
* volatility -f Desktop/stuxnet.vmem ldrmodules -p 868
* volatility -f Desktop/ stuxnet.vmem dlldump --pid=868 --dump-dir ~/Desktop/868/



* volatility -f Desktop/stuxnet.vmem dlllist -p 1928
* volatility -f Desktop/stuxnet.vmem ldrmodules -p 1928
* volatility -f Desktop/ stuxnet.vmem dlldump --pid=1928 --dump-dir ~/Desktop/1928/

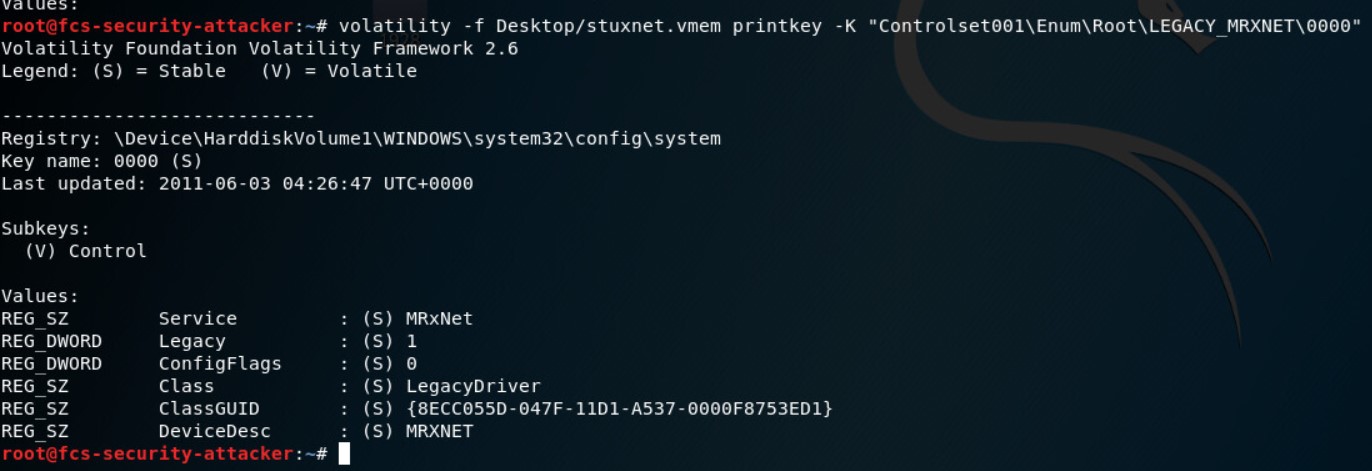
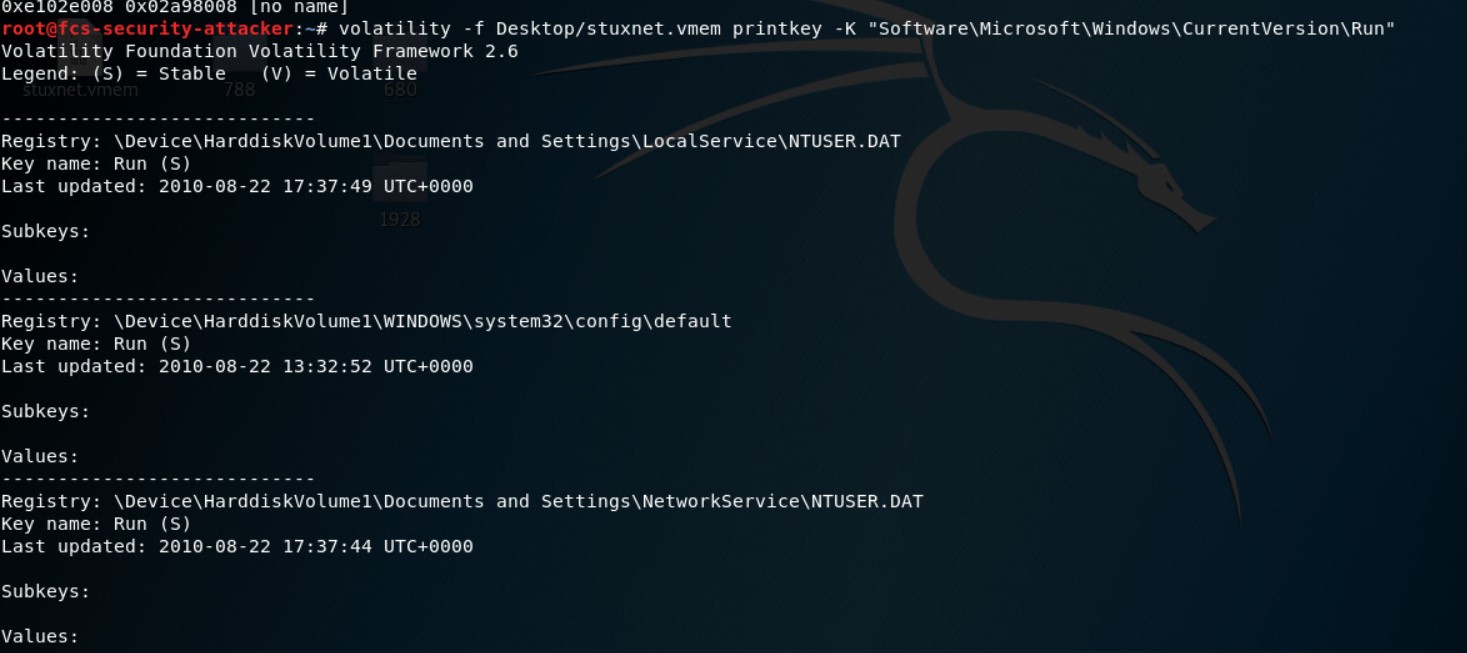
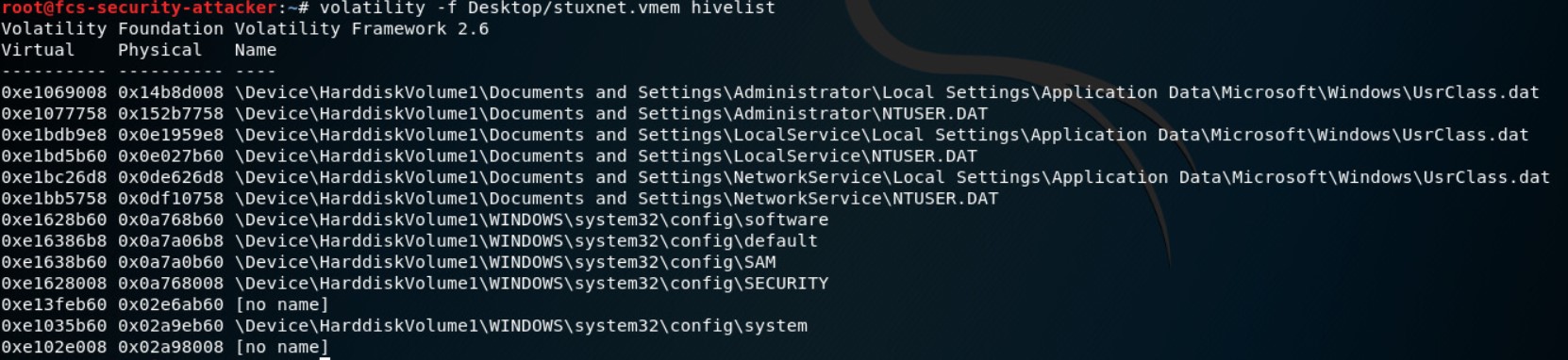
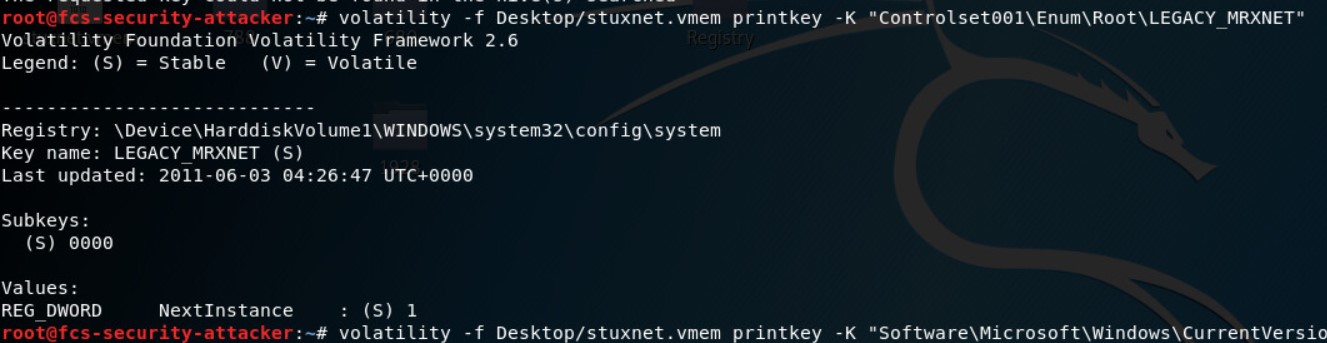
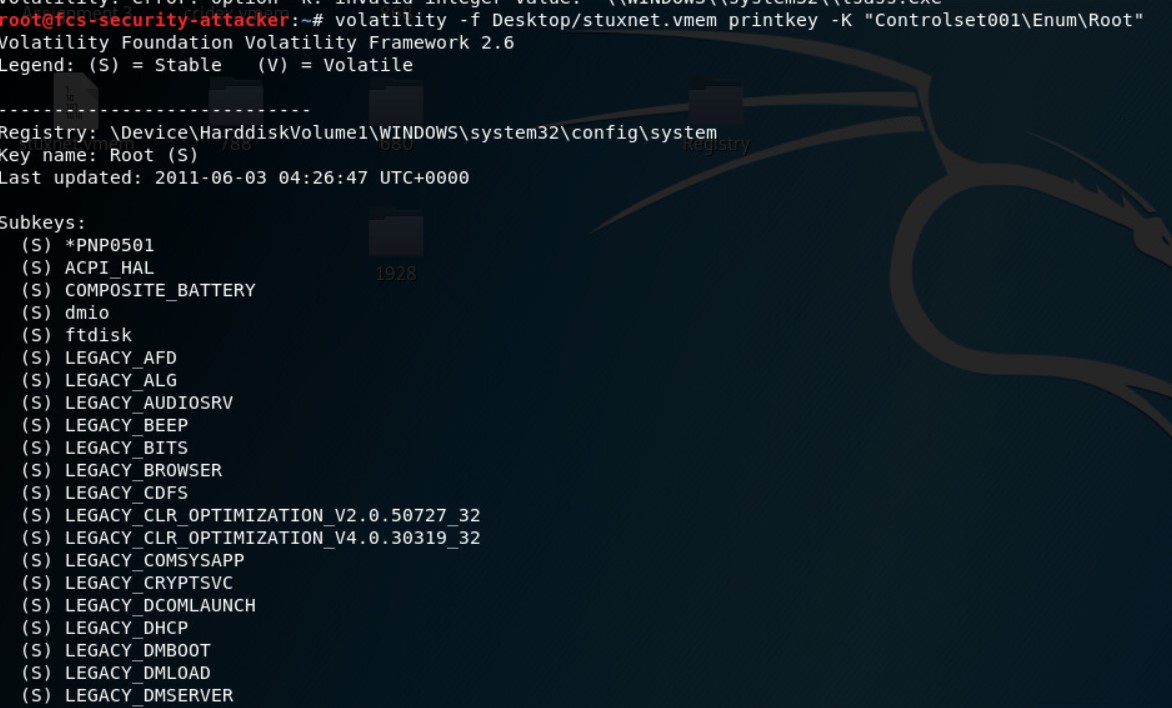


1. **How many register keys in Stuxnet case have been added to the computer?**

According to [Panda Security](https://www.pandasecurity.com/en/security-info/222123/information/Stuxnet.A/) Stuxnet will create the following entries in the Windows Registry:

* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXCLS
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXCLS\0000
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXCLS\0000\Control
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXNET
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXNET\0000
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXNET\0000\Control
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxCls
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\Enum
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxNet
* HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\Enum
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXCLS
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXCLS\0000
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXCLS\0000\Control
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXNET
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXNET\0000
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXNET\0000\Control
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\Enum
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\Enum

We were able to find most of them in our file the screenshots are as follows:



1. **Why does Stuxnet need these register keys?**

Stuxnet creates these entries so that the rootkits can register as a service and run whenever the computer boots. They are also injected into the lsass.exe process so that they cannot be viewed.