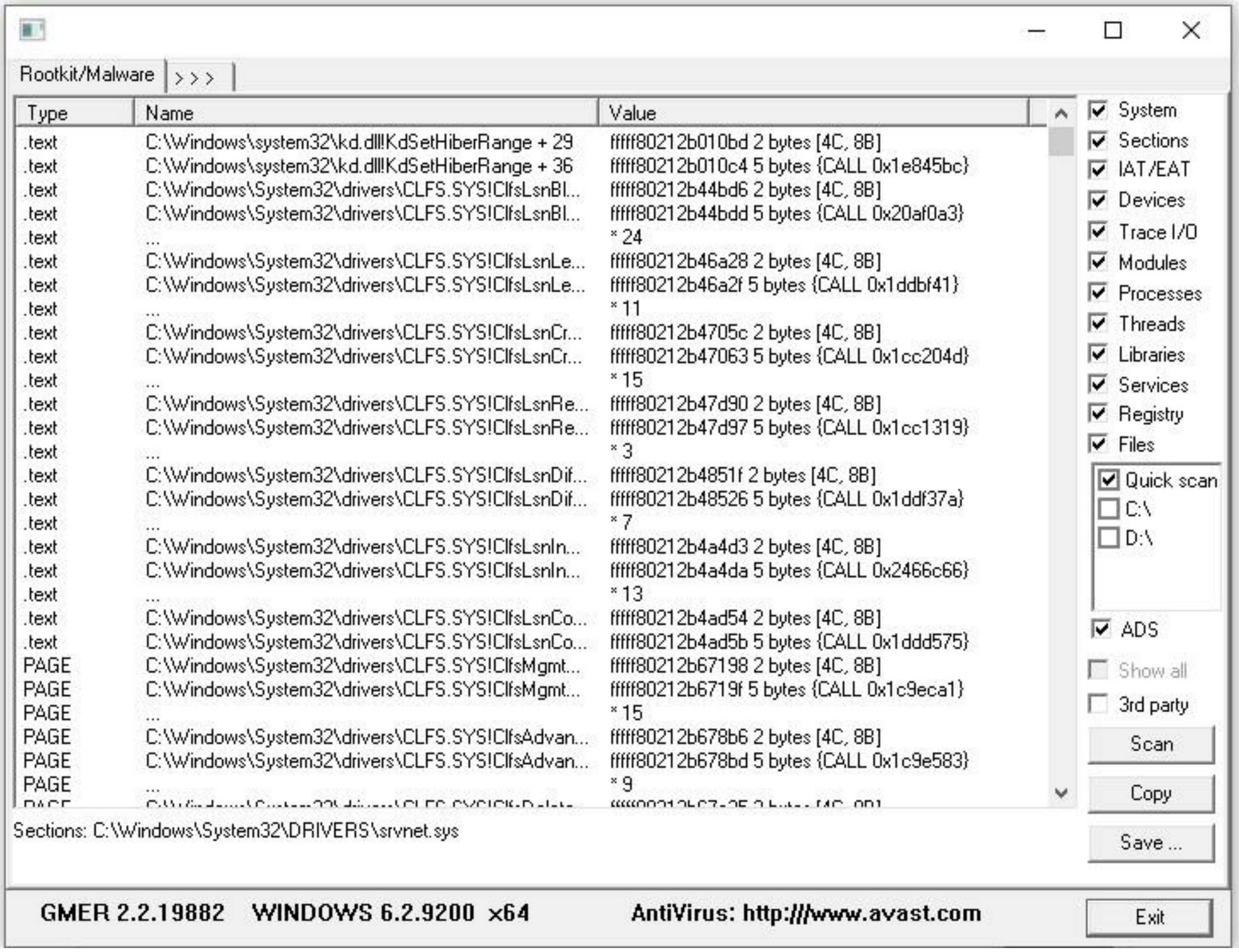
Name: Shweta Sanjay Kate

Roll No.: 3083

Div: B **Batch**: T4

Defeating Malware – Rootkit hunter

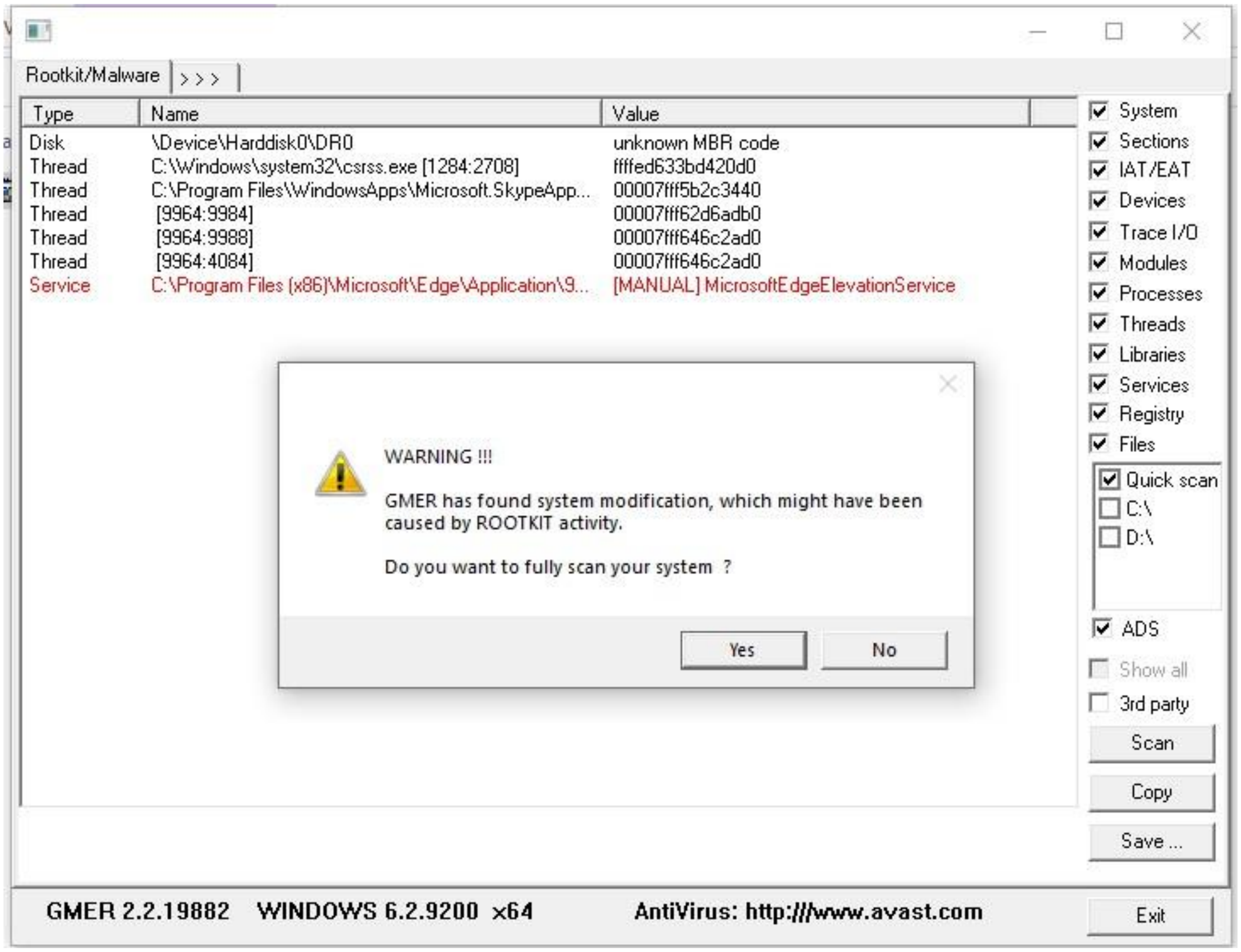


Type	Name	Value
.text	C:\Windows\system32\kd.dll!KdSetHiberRange + 29	fffff80212b010bd 2 bytes [4C, 8B]
.text	C:\Windows\system32\kd.dll!KdSetHiberRange + 36	fffff80212b010c4 5 bytes {CALL 0x1e845bc}
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnBl...	fffff80212b44bd6 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnBl...	fffff80212b44bdd 5 bytes {CALL 0x20af0a3}
.text	...	* 24
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnLe...	fffff80212b46a28 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnLe...	fffff80212b46a2f 5 bytes {CALL 0x1ddbf41}
.text	...	* 11
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnCr...	fffff80212b4705c 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnCr...	fffff80212b47063 5 bytes {CALL 0x1cc204d}
.text	...	* 15
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnRe...	fffff80212b47d90 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnRe...	fffff80212b47d97 5 bytes {CALL 0x1cc1319}
.text	...	* 3
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnDif...	fffff80212b4851f 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnDif...	fffff80212b48526 5 bytes {CALL 0x1ddf37a}
.text	...	* 7
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnIn...	fffff80212b4a4d3 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnIn...	fffff80212b4a4da 5 bytes {CALL 0x2466c66}
.text	...	* 13
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnCo...	fffff80212b4ad54 2 bytes [4C, 8B]
.text	C:\Windows\System32\drivers\CLFS.SYS!ClfsLsnCo...	fffff80212b4ad5b 5 bytes {CALL 0x1ddd575}
PAGE	C:\Windows\System32\drivers\CLFS.SYS!ClfsMgmt...	fffff80212b67198 2 bytes [4C, 8B]
PAGE	C:\Windows\System32\drivers\CLFS.SYS!ClfsMgmt...	fffff80212b6719f 5 bytes {CALL 0x1c9eca1}
PAGE	...	* 15
PAGE	C:\Windows\System32\drivers\CLFS.SYS!ClfsAdvan...	fffff80212b678b6 2 bytes [4C, 8B]
PAGE	C:\Windows\System32\drivers\CLFS.SYS!ClfsAdvan...	fffff80212b678bd 5 bytes {CALL 0x1c9e583}
PAGE	...	* 9

☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
□ C:\
□ D:\
☑ ADS
□ Show all
□ 3rd party

Sections: C:\Windows\System32\DRIVERS\srvnet.sys

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http:///www.avast.com



Type	Name	Value
Disk	\Device\Harddisk0\DR0	unknown MBR code
Thread	C:\Windows\system32\csrss.exe [1284:2708]	ffffed633bd420d0
Thread	C:\Program Files\WindowsApps\Microsoft.SkypeApp...	00007fff5b2c3440
Thread	[9964:9984]	00007fff62d6adb0
Thread	[9964:9988]	00007fff646c2ad0
Thread	[9964:4084]	00007fff646c2ad0
Service	C:\Program Files (x86)\Microsoft\Edge\Application\9...	[MANUAL] MicrosoftEdgeElevationService

WARNING !!!

GMER has found system modification, which might have been caused by ROOTKIT activity.

Do you want to fully scan your system ?

☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
□ C:\
□ D:\
☑ ADS
□ Show all
□ 3rd party

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http:///www.avast.com

Conclusion:

In this experiment a rootkit hunter software tool has been installed and the rootkit have been detected.