

## IT8761 – Security Laboratory

Reshma Ramesh Babu

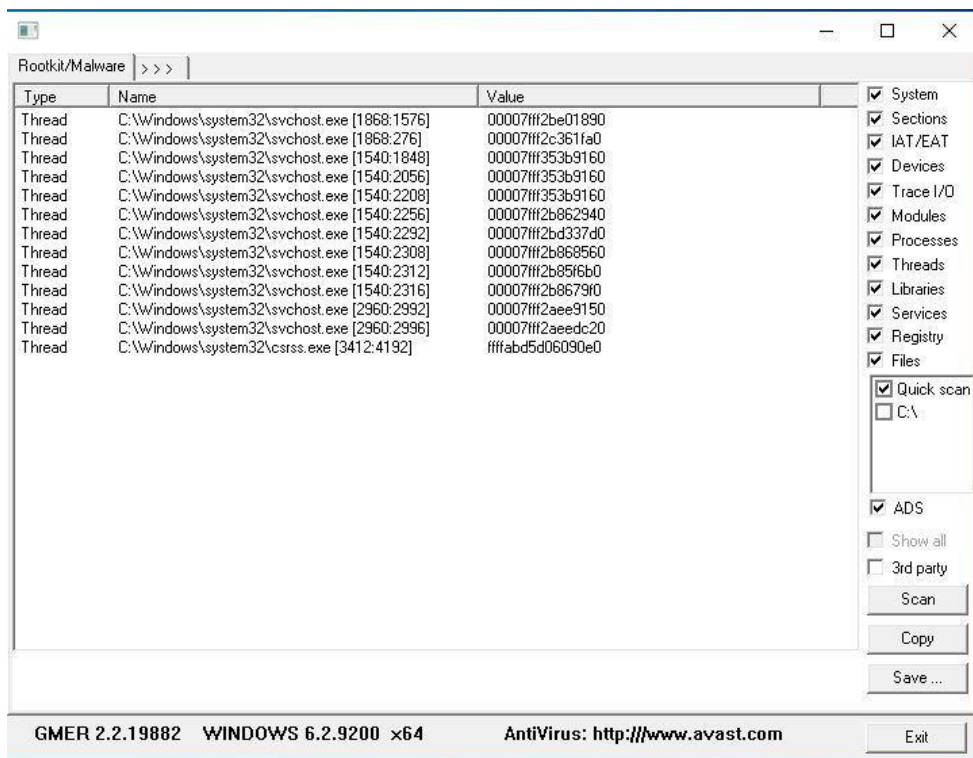
312217104129

### Exercise 12 b

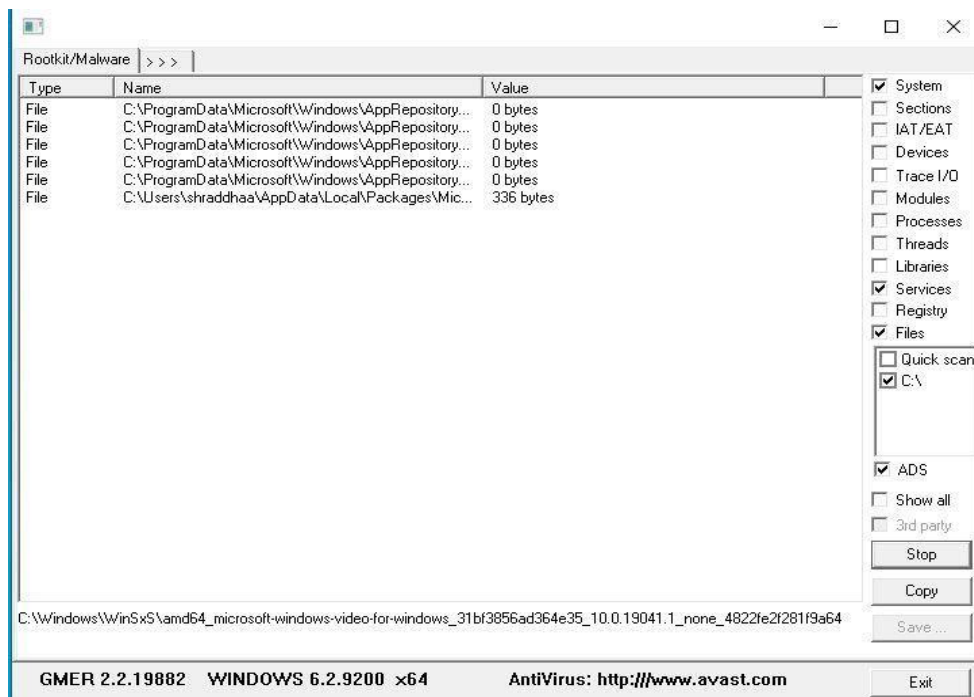
**Aim:** To install rootkit and to study about the variety of options

**Output:**

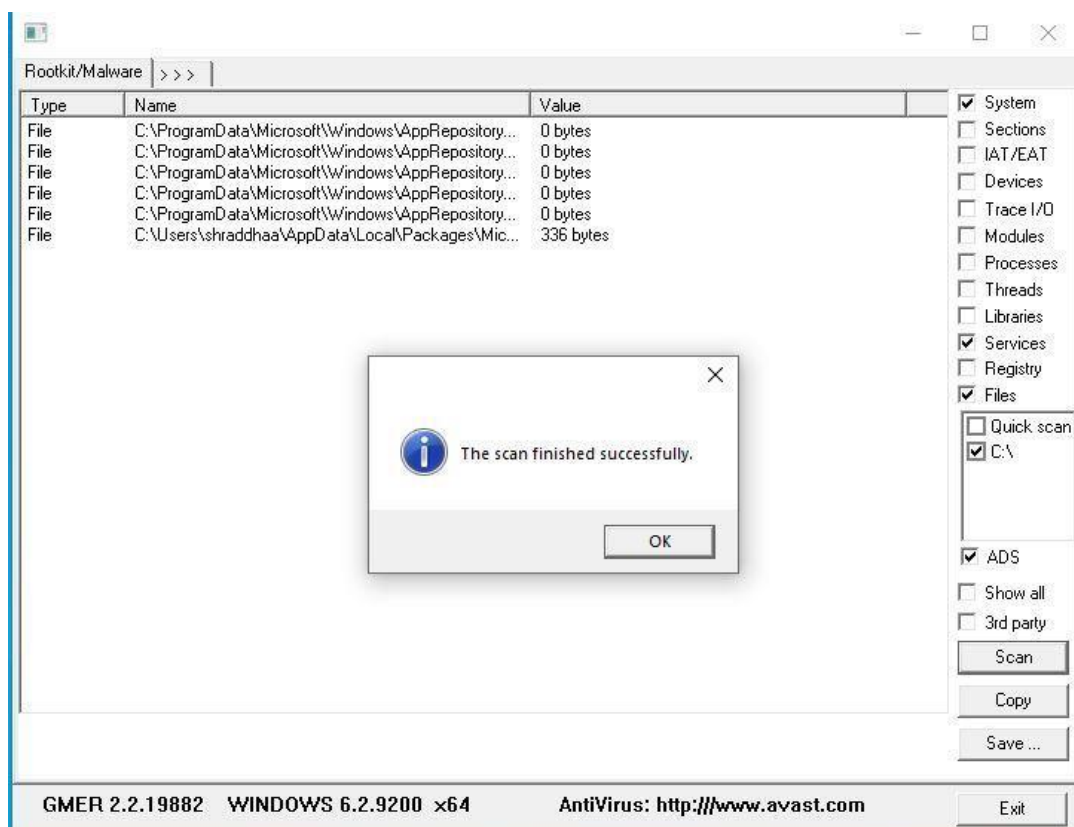
1. Download and install the Rootkit Tool from GMER website. [www.gmer.net](http://www.gmer.net)
2. Now the rootkit screen will be displayed



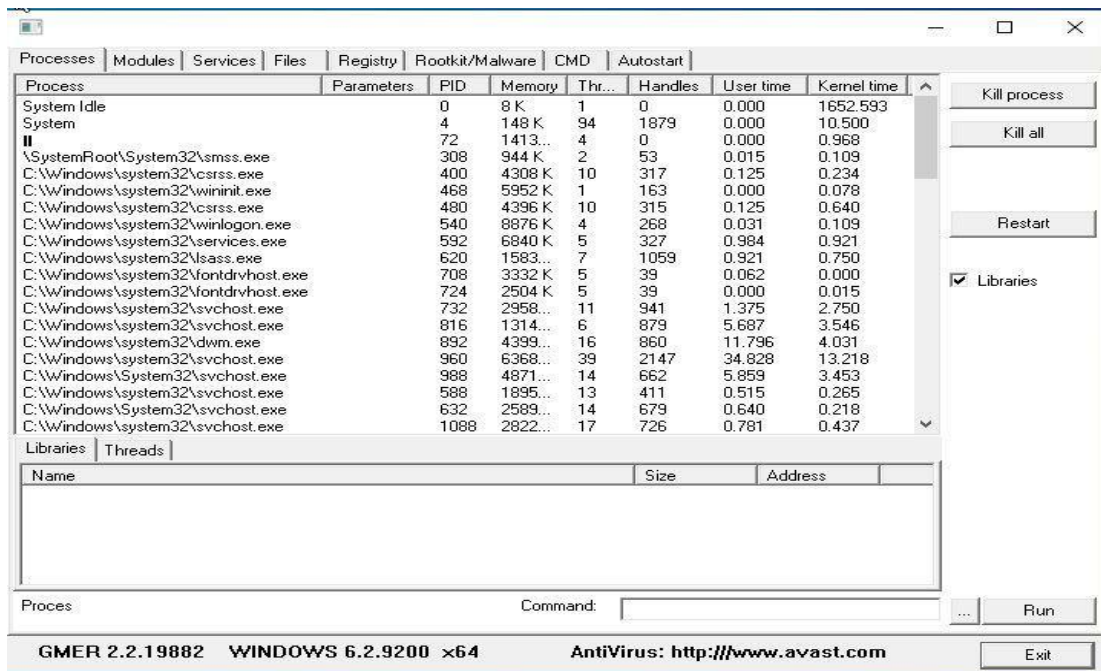
3. Select anyone of the drive which is shown at right side of the screen. After selecting the drive click on scan button.



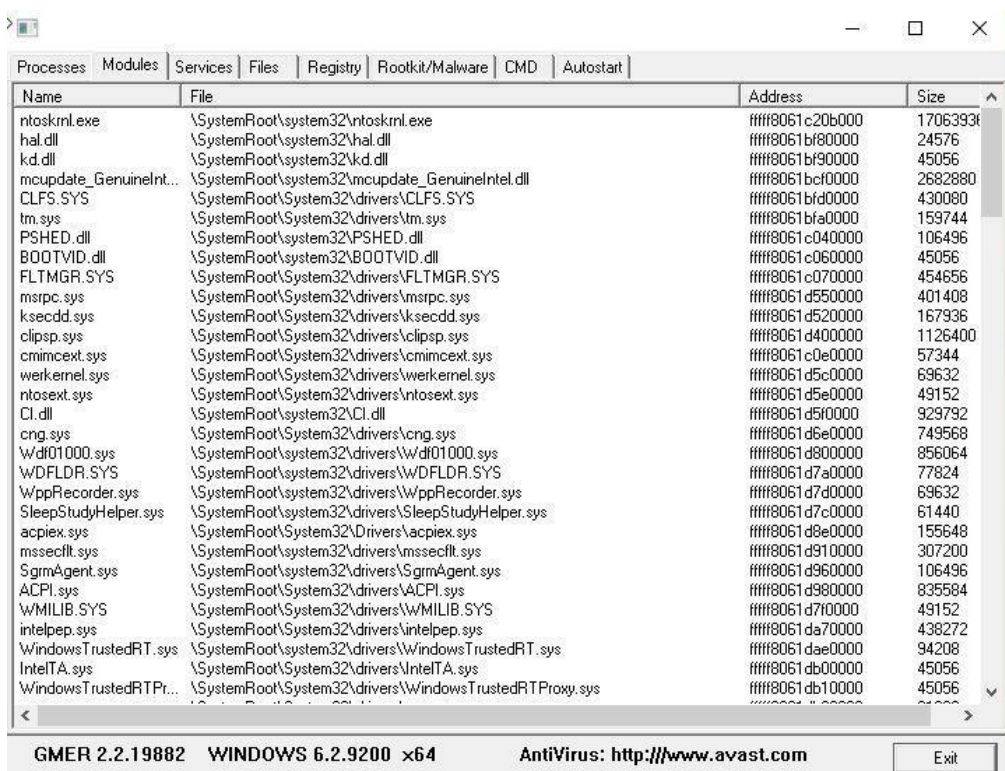
4. Wait for the scan to finish



5. Click on the options. This displays the Processes, Modules, Services, Files, Registry, RootKit/Malwares, Autostart, CMD of local host. Select Processes menu and kill any unwanted process if any. (Read the details listed, Malware affected processes, services if any will be shown in red. Before selecting the kill option, care must be taken, since the Rootkit tool's suspects may be systems core services.)



6. Modules menu displays the various system files like .sys, .dll



- Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.

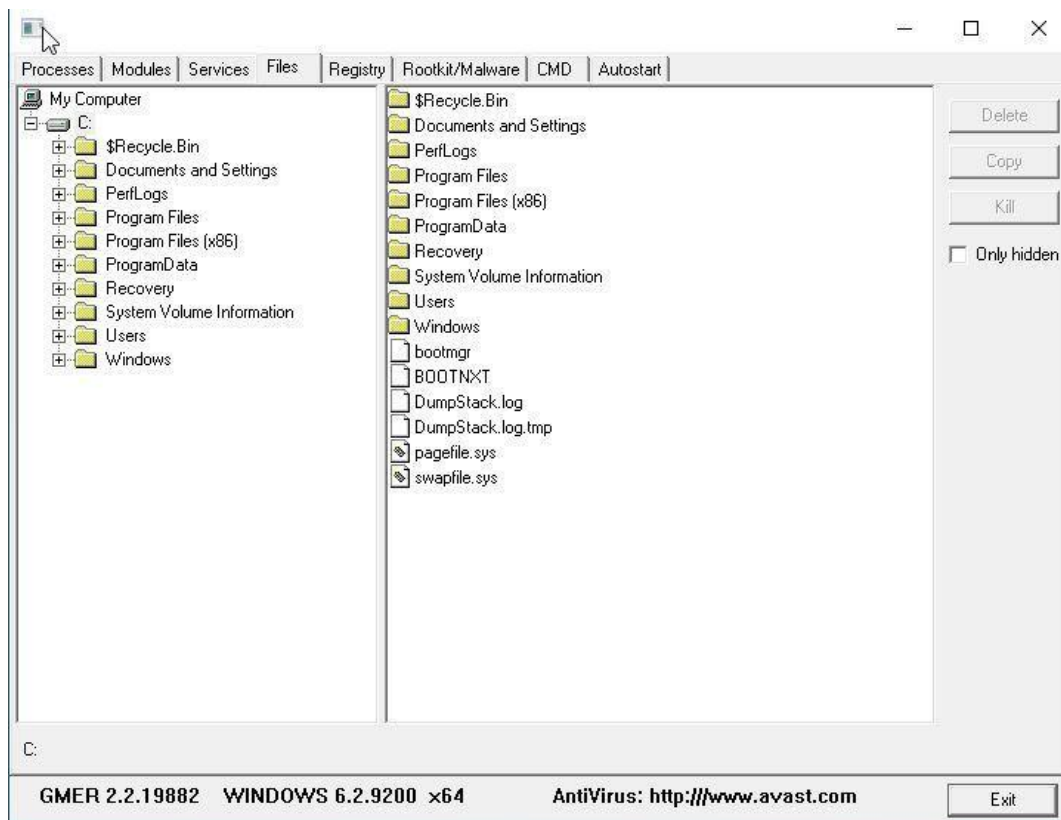
Processes   Modules   <b>Services</b>   Files   Registry   Rootkit/Malware   CMD   Autostart				
Name	Start	File name	Description	
.NET CLR Data		%systemroot%\system32\netfxperf.dll		
.NET CLR Netwo...		%systemroot%\system32\netfxperf.dll		
.NET CLR Netwo...		%systemroot%\system32\netfxperf.dll		
.NET Data Provid...		%systemroot%\system32\netfxperf.dll		
.NET Data Provid...		%systemroot%\system32\netfxperf.dll		
.NET Memory Ca...		%systemroot%\system32\netfxperf.dll		
.NETFramework		%systemroot%\system32\mscorlib.dll		
1394ohci	MANUAL	\SystemRoot\System32\drivers\1394ohci.sys		
3ware	BOOT	System32\drivers\3ware.sys		
AarSvc	MANUAL	%SystemRoot%\System32\AarSvc.dll		
AarSvc_407ac	MANUAL	C:\Windows\system32\svchost.exe -k AarSvcG...	Agent Activation Runtime_407ac	
ACPI	BOOT	System32\drivers\ACPI.sys		
AcpiDev	MANUAL	\SystemRoot\System32\drivers\AcpiDev.sys		
acpiex	BOOT	System32\drivers\acpiex.sys	Microsoft ACPIEX Driver	
acpipagr	MANUAL	\SystemRoot\System32\drivers\acpipagr.sys		
AcpiPmi	MANUAL	\SystemRoot\System32\drivers\acpipmi.sys		
acptime	MANUAL	\SystemRoot\System32\drivers\acptime.sys		
Acx01000	MANUAL	system32\drivers\Acx01000.sys		
AD0VMPPackage				
ADP80XX	BOOT	System32\drivers\ADP80XX.SYS		
adsi				
AFD	SYSTEM	\SystemRoot\system32\drivers\afd.sys		
afunix	SYSTEM	\SystemRoot\system32\drivers\afunix.sys	afunix	
ahcache	SYSTEM	system32\DRIVERS\ahcache.sys		
AJRouter	MANUAL	%SystemRoot%\System32\AJRouter.dll		
ALG	MANUAL	%SystemRoot%\System32\alg.exe		
amdgp2	MANUAL	\SystemRoot\System32\drivers\amdgp2.sys		
amd2c	MANUAL	\SystemRoot\System32\drivers\amd2c.sys		
AmdK8	MANUAL	\SystemRoot\System32\drivers\amdK8.sys		
AmdPPM	MANUAL	\SystemRoot\System32\drivers\amdppm.sys		
amdsata	BOOT	System32\drivers\amdsata.sys		
amdsata	BOOT	System32\drivers\amdsata.sys		

GMER 2.2.19882 WINDOWS 6.2.9200 x64

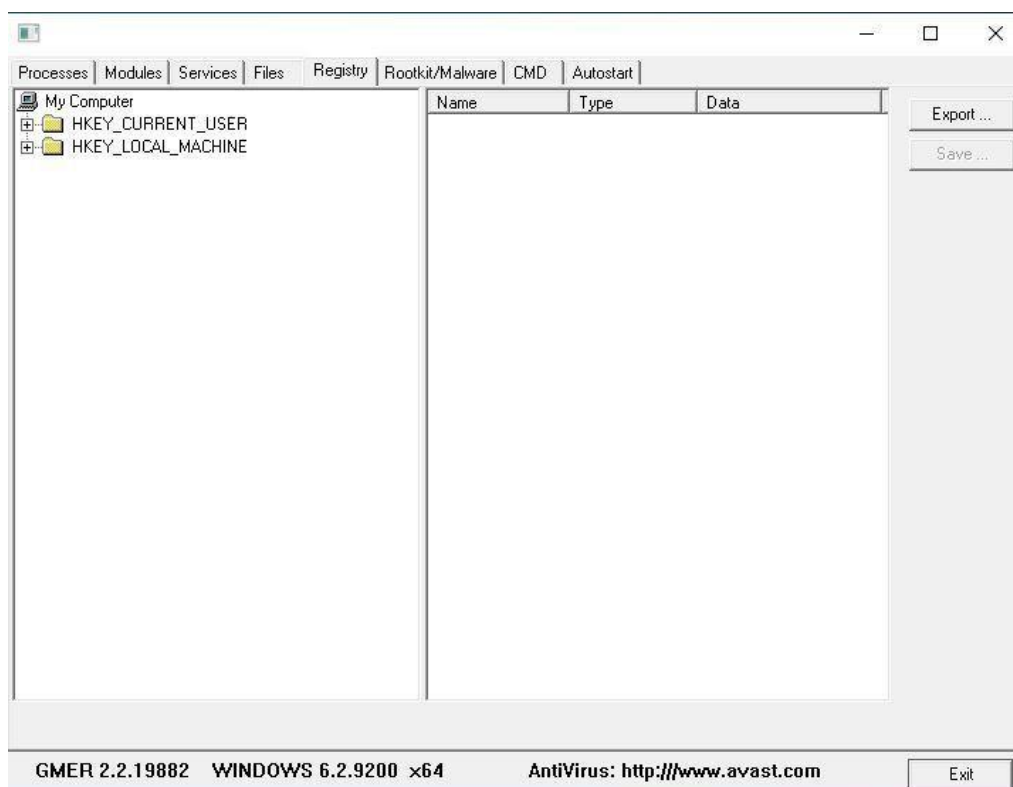
AntiVirus: <http://www.avast.com>

Exit

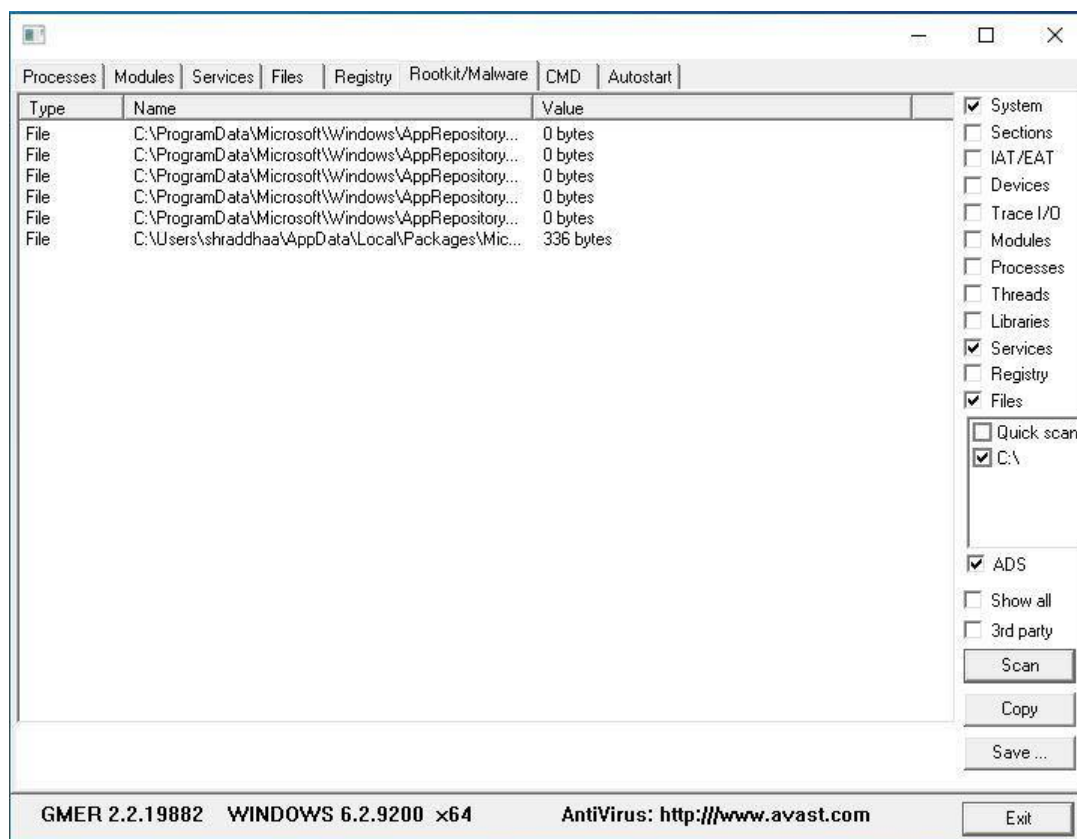
8. Files menu displays full files on Hard-Disk volumes.



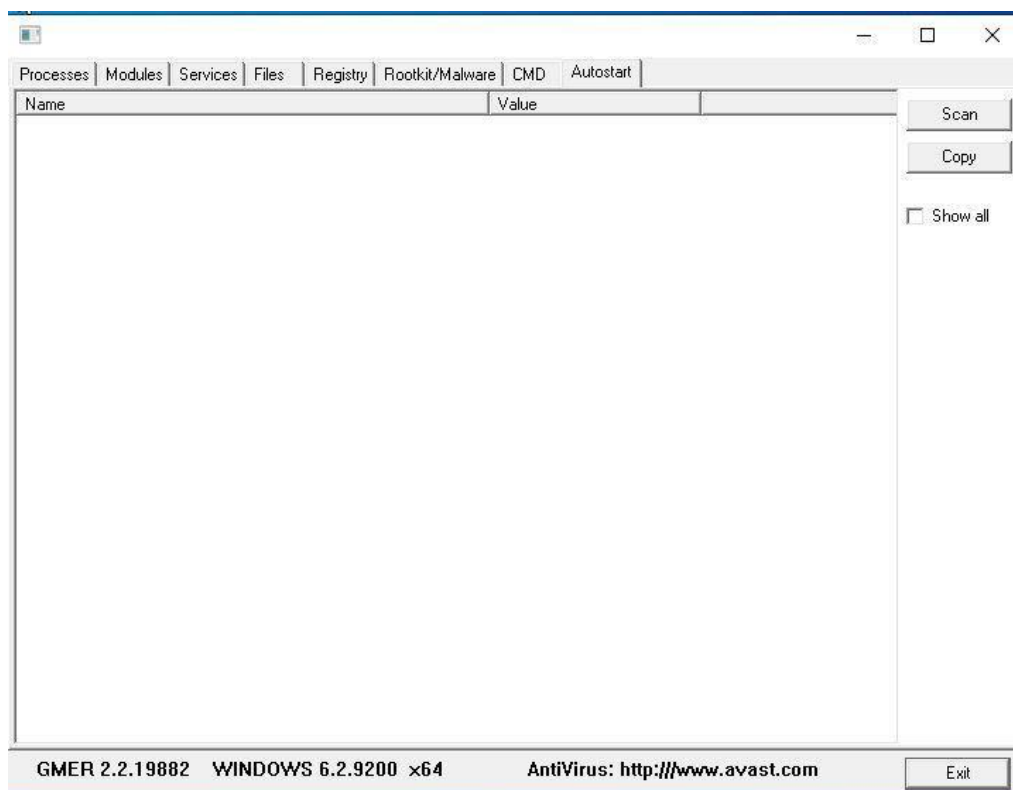
9. Registry displays Hkey\_Current\_user and Hkey\_Local\_Machine.



10. Rootkits/Malwares scans the local drives selected.



11. Autostart displays the registry base Autostart applications.



## 12. CMD allows the user to interact with command line utilities or Registry

