[AtomicRedTeam]

[Chris Miele]

[5/21/2023]

Table Of Contents

Executive Summary

SHA256 hash (HDD)	6C1437944E4B4BCB313D1AF43B3B2BBD4E2EECDE69C301DC170895233AD38154
SHA256 hash (Memory)	8854CECB85373E32A30A72CFBBAD2A7BEDC9691A9BC04D50B6B28F6588A37CDC

The scope of this Computer Forensics report is to identify what malicious software was executed on 5/20/2023 on user IEUser computer.

Artifacts

Computer Name	MSEDGEWin10
Windows Version	Windows 10 Enterprise Evaluation Release ID 1809[1]
Network	IP:10.0.2.15 SubnetMask:255.255.255.0
Defender (Real Time Protection)	Off
User Account	IEUser [1001]
User Accounts Attack	Art-test [1002]
Directory Accessed	PWF-Main
Files Accessed	Mavininject.exe and Atomic Service.exe

Malicious Files

AtomicService.exe	C51217ce3d1959e99886a567d21d0b97022bd6e3

Mavininject.exe	800631FEF628DE40E7A8F30758D9EEA7E226E020CC5E8BD8D617E3B4E74DFE2F

AtomicService.exe

Atomic Service is the malicious file that exists on the system it is apart of Atomic Red Team Adversary Enumeration.

Mavininject.exe

Mavininject is used for injection a malicious dll into a running process.

TimeLine of Attack

The Breakdown of the event that occurred on Windows 10 Workstation is the following:

2023-05-20 00:29:42 (Install Date Win10)

2023-05-20 14:01:52 (IEUser Logged in Win10 Machine)

2023-05-20 14:02:29 (Windows Defender Real-Time Protection Disabled)

2023-05-20 14:02:10 (PWF Main Directory Accessed)

2023-05-20 14:08:45 (New User Account Created art-test)

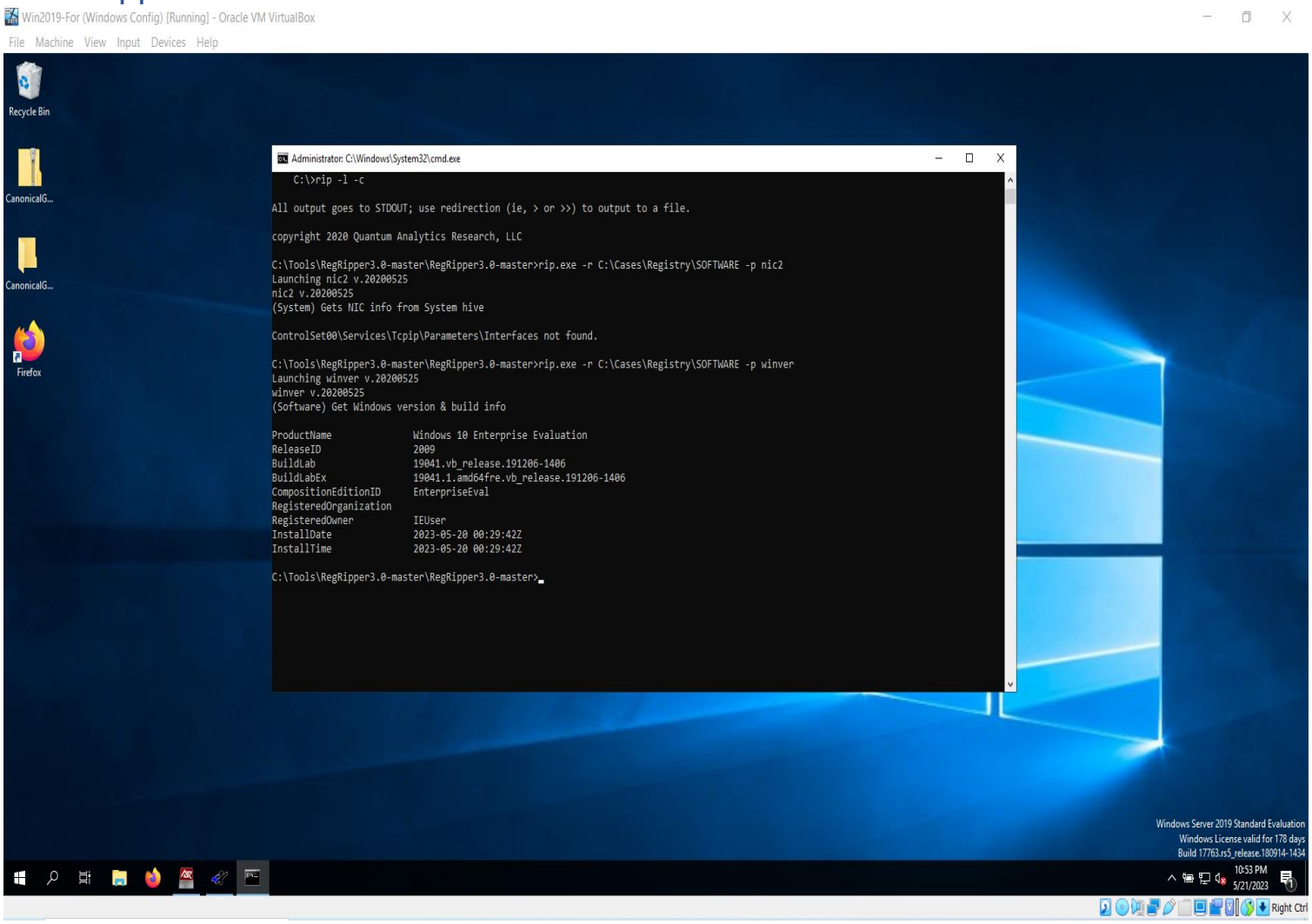
2023-05-20 14:09:10 (AtomicService.exe executed system)

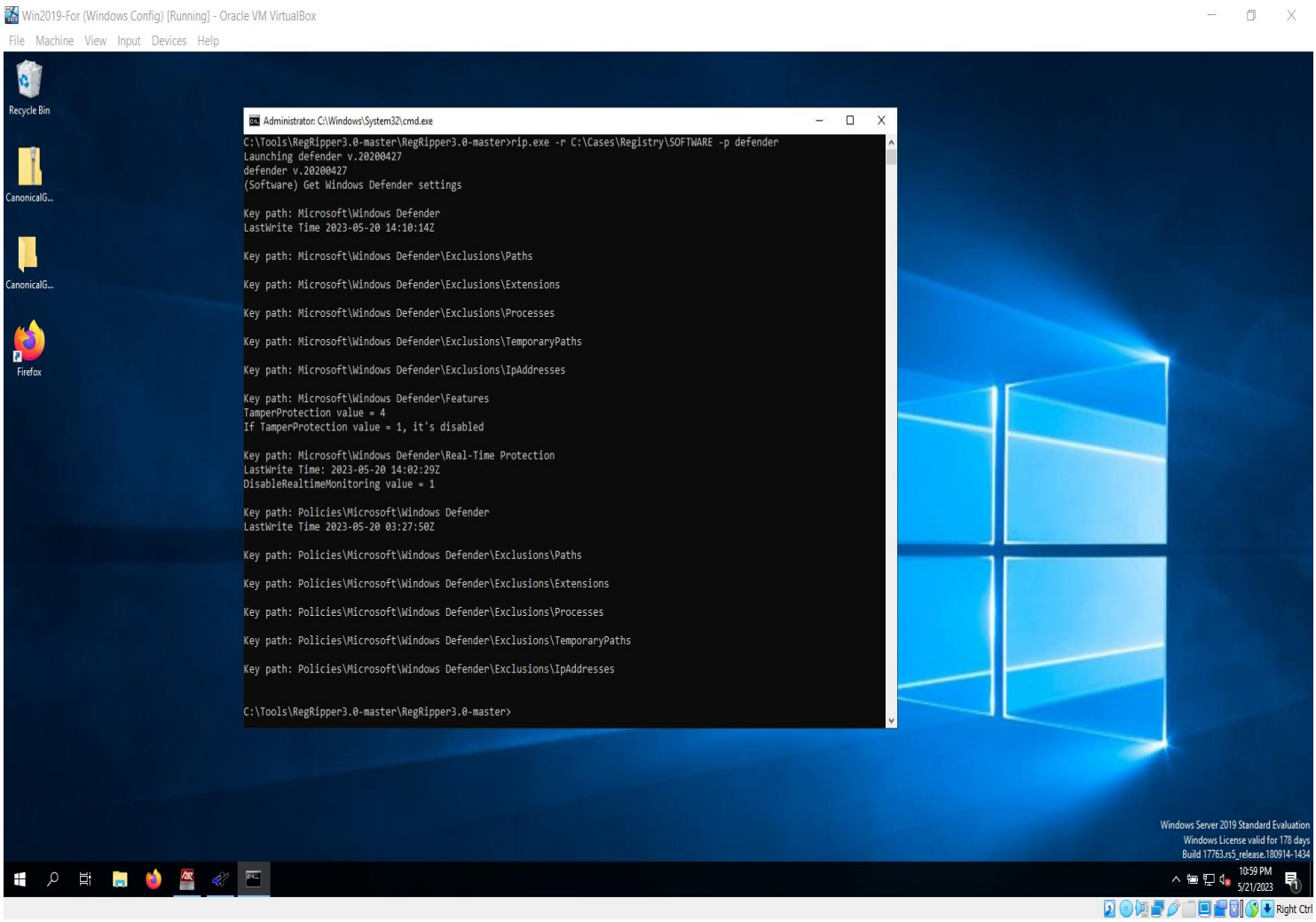
2023-05-20 14:09:14 (MavinInject.exe executed system)

Improvements

1) End-User IEUser should be retrained in information security awareness training.
2) Limit Permissions of IEUser should not be able to set the execution policy.

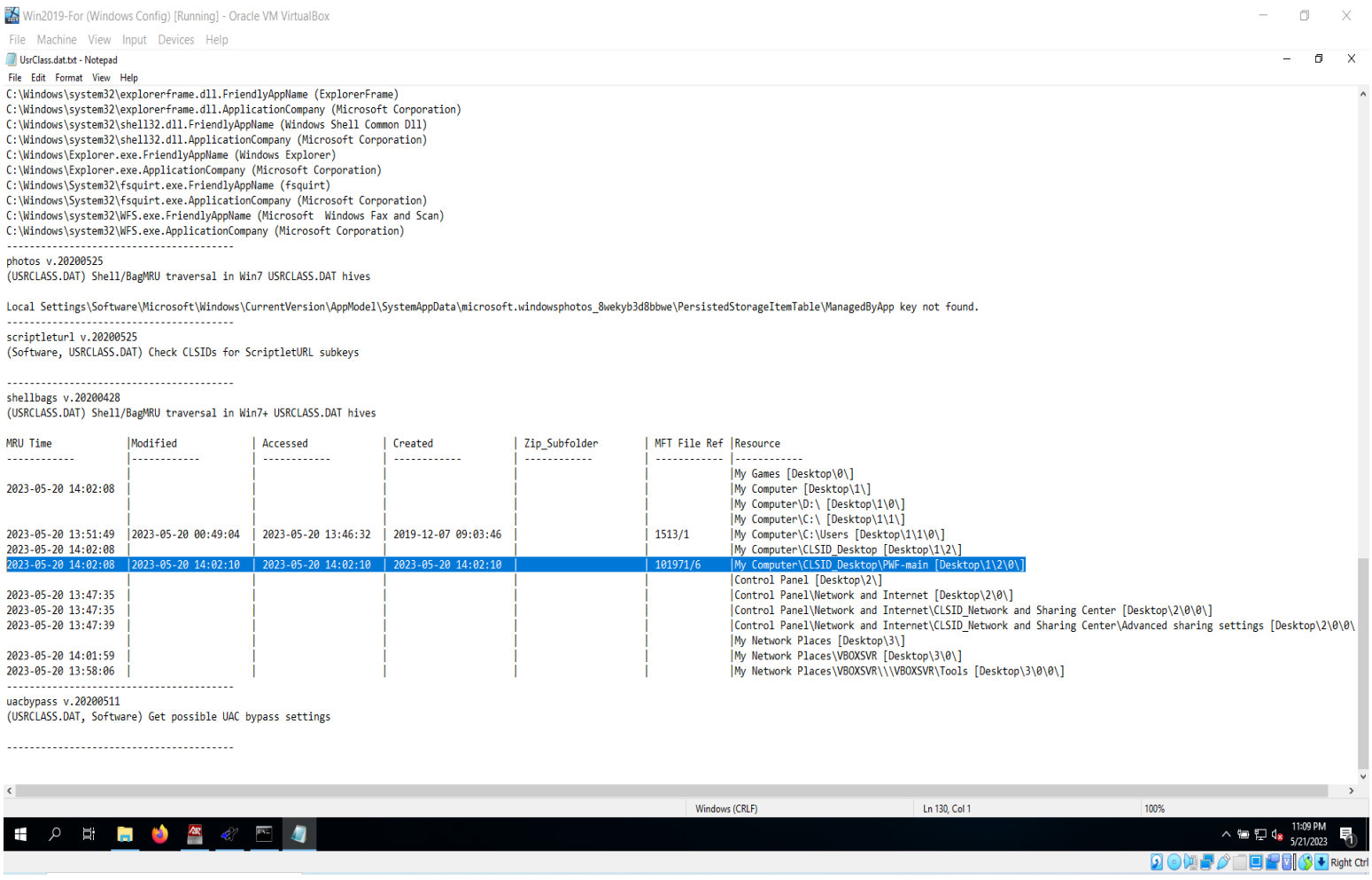
Appendix A

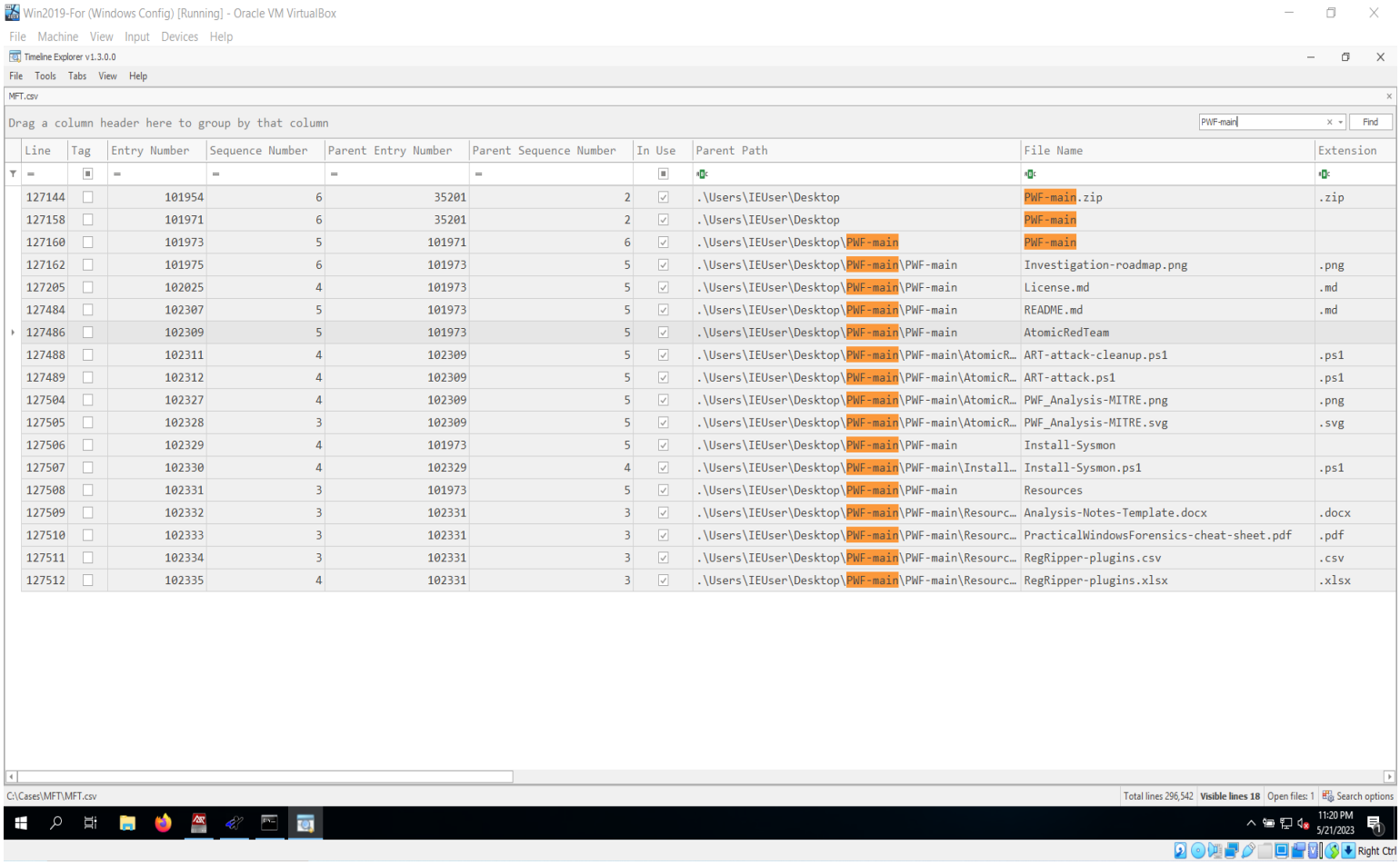

Win2019-For (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
CanonicalG...
CanonicalG...
Firefox
Administrator: C:\Windows\System32\cmd.exe
C:\>rip -l -c
All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.
copyright 2020 Quantum Analytics Research, LLC
C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Registry\SOFTWARE -p nic2
Launching nic2 v.20200525
nic2 v.20200525
(System) Gets NIC info from System hive
ControlSet00\Services\Tcpip\Parameters\Interfaces not found.
C:\Tools\RegRipper3.0-master\RegRipper3.0-master>rip.exe -r C:\Cases\Registry\SOFTWARE -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info
ProductName Windows 10 Enterprise Evaluation
ReleaseID 2009
BuildLab 19041.vb_release.191206-1406
BuildLabEx 19041.1.amd64fre.vb_release.191206-1406
CompositionEditionID EnterpriseEval
RegisteredOrganization
RegisteredOwner IEUser
InstallDate 2023-05-20 00:29:42Z
InstallTime 2023-05-20 00:29:42Z
C:\Tools\RegRipper3.0-master\RegRipper3.0-master>
Windows Server 2019 Standard Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
10:53 PM
5/21/2023
Right Ctrl

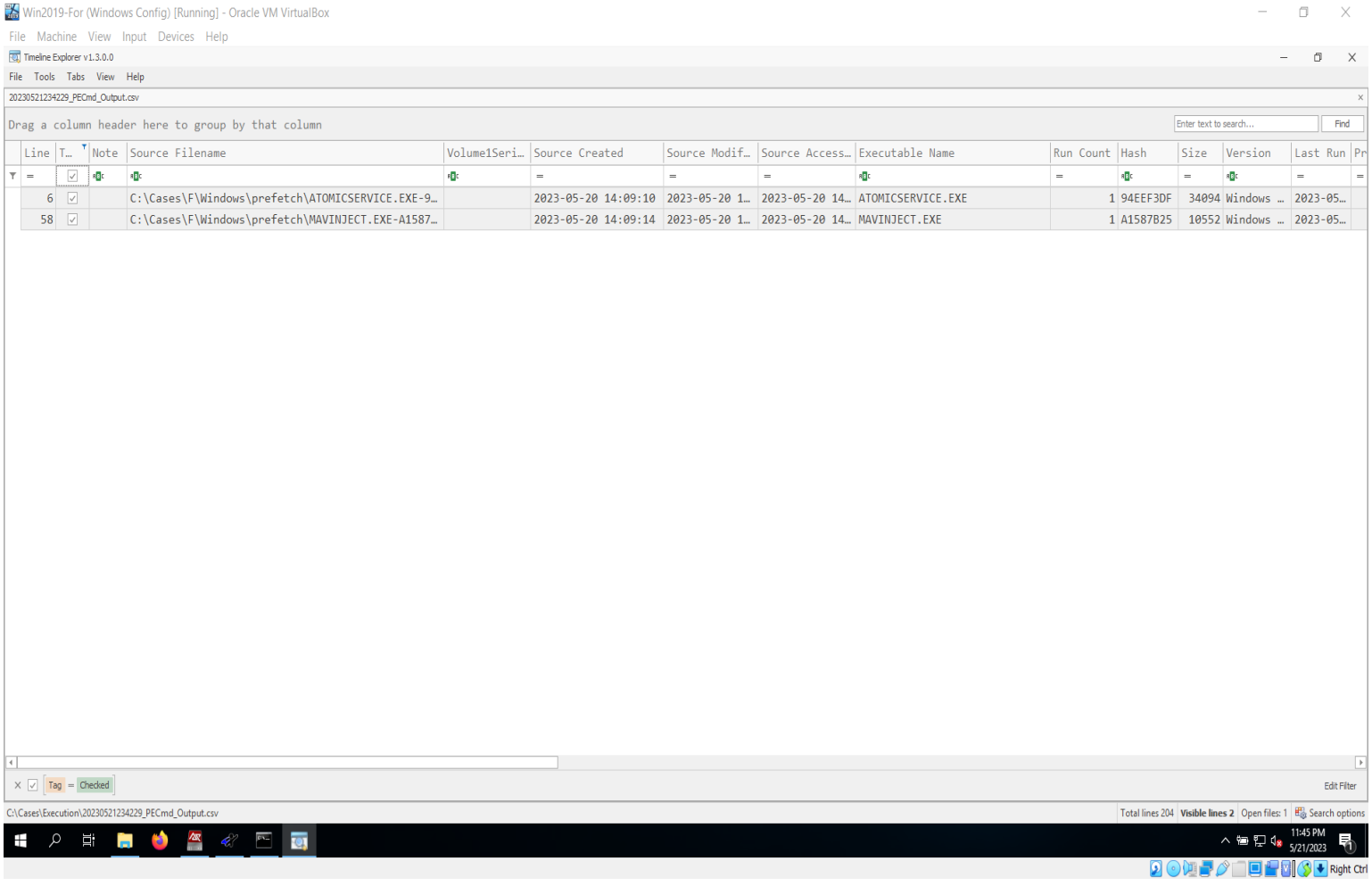


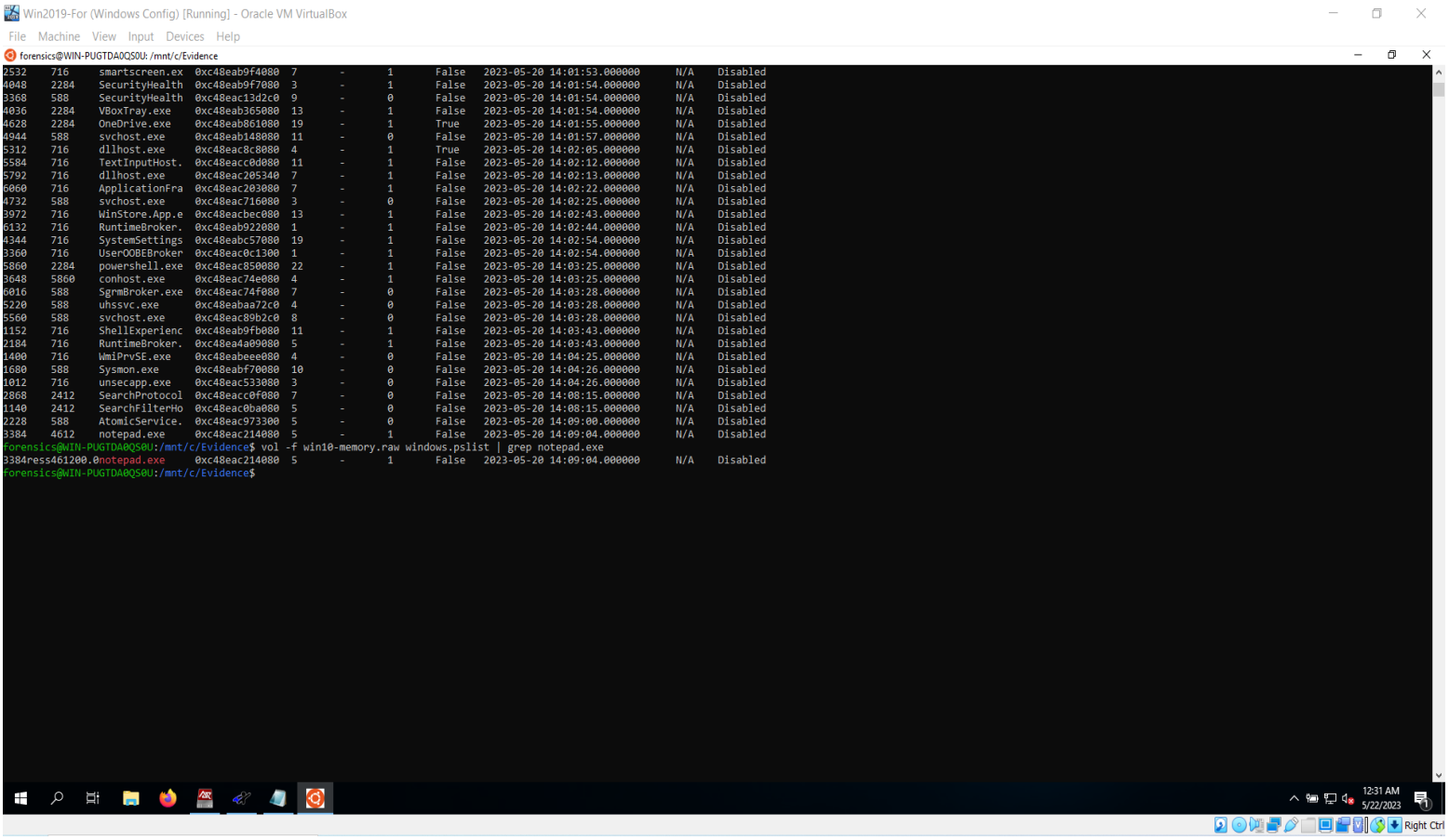

```
Username        : IEUser [1001]
SID             : S-1-5-21-2687985881-3977539135-878464447-1001
Full Name       :
User Comment    :
Account Type    :
Account Created : Sat May 20 00:31:56 2023 Z
Security Questions:
    Question 1  : What was your first pet's name?
    Answer 1    : asd
    Question 2  : What's the name of the city where your parents met?
    Answer 2    : asd
    Question 3  : What's the name of the city where you were born?
    Answer 3    : asd
Name            :
Last Login Date : Sat May 20 14:01:52 2023 Z
Pwd Reset Date  : Sat May 20 00:31:56 2023 Z
Pwd Fail Date   : Never
Login Count     : 6
  --> Password does not expire
  --> Password not required
  --> Normal user account
```

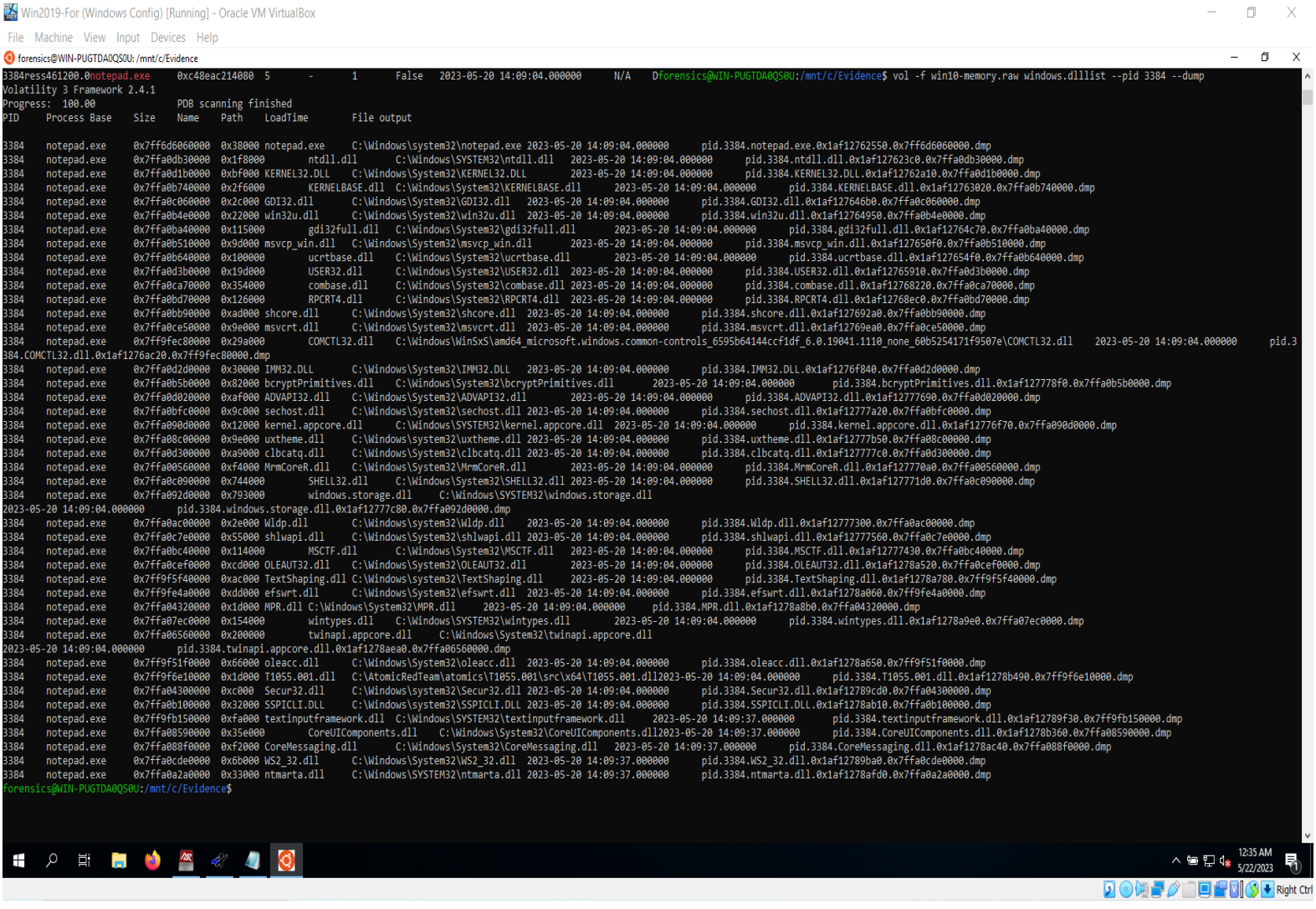
```
Username         : art-test [1002]
SID              : S-1-5-21-2687985881-3977539135-878464447-1002
Full Name        :
User Comment     :
Account Type     :
Account Created  : Sat May 20 14:08:45 2023 Z
Name             :
Last Login Date  : Never
Pwd Reset Date   : Sat May 20 14:08:45 2023 Z
Pwd Fail Date    : Never
Login Count      : 0
   --> Normal user account
```

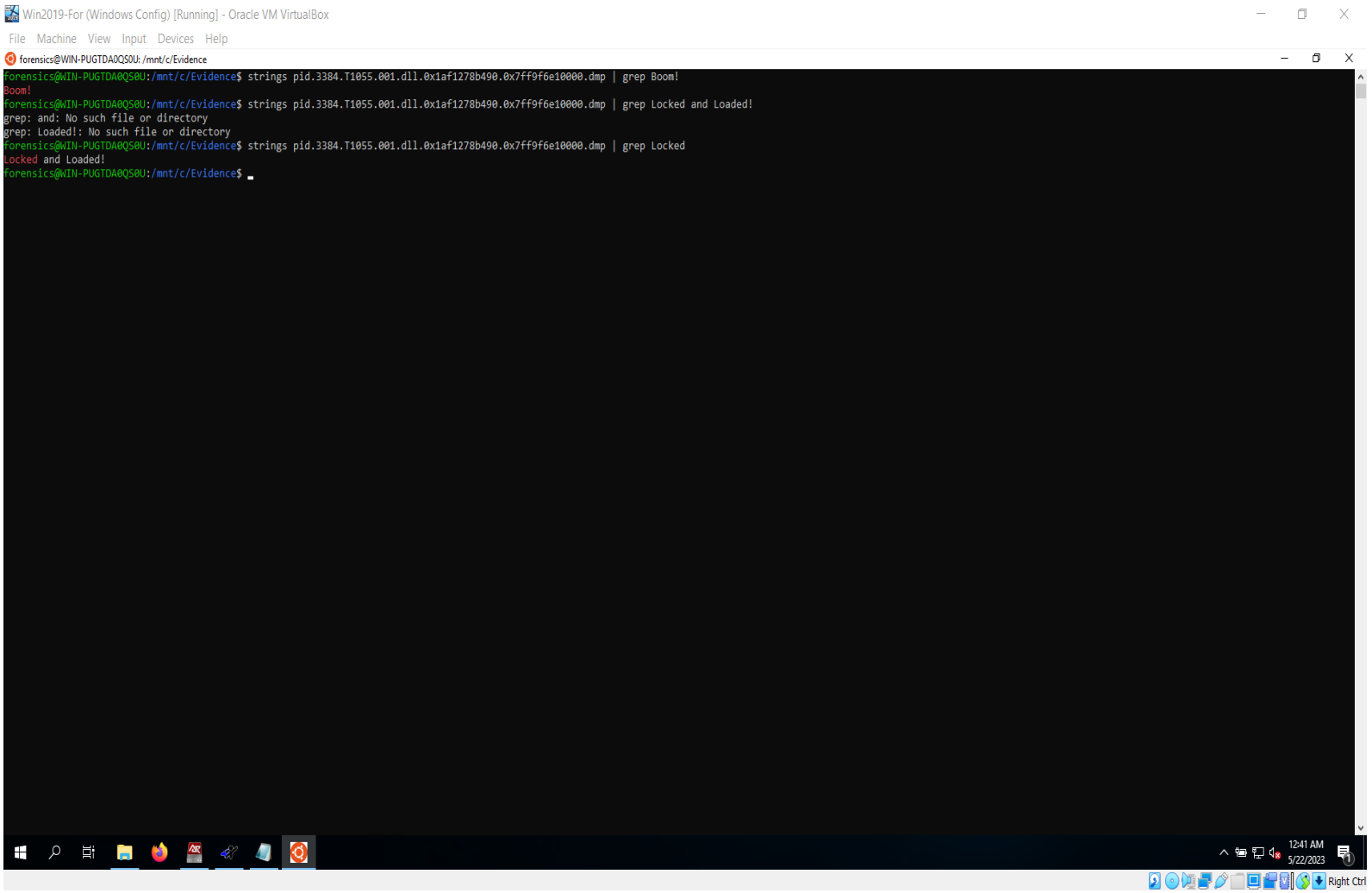



Win2019-For (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
MFT.csv
Drag a column header here to group by that column
PWF-main
Find
Line | Tag | Entry Number | Sequence Number | Parent Entry Number | Parent Sequence Number | In Use | Parent Path | File Name | Extension
127144 | 101954 | 6 | 35201 | 2 | .\Users\IEUser\Desktop | PWF-main.zip | .zip
127158 | 101971 | 6 | 35201 | 2 | .\Users\IEUser\Desktop | PWF-main
127160 | 101973 | 5 | 101971 | 6 | .\Users\IEUser\Desktop\PWF-main | PWF-main
127162 | 101975 | 6 | 101973 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main | Investigation-roadmap.png | .png
127205 | 102025 | 4 | 101973 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main | License.md | .md
127484 | 102307 | 5 | 101973 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main | README.md | .md
127486 | 102309 | 5 | 101973 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main | AtomicRedTeam
127488 | 102311 | 4 | 102309 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicR… | ART-attack-cleanup.ps1 | .ps1
127489 | 102312 | 4 | 102309 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicR… | ART-attack.ps1 | .ps1
127504 | 102327 | 4 | 102309 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicR… | PWF_Analysis-MITRE.png | .png
127505 | 102328 | 3 | 102309 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicR… | PWF_Analysis-MITRE.svg | .svg
127506 | 102329 | 4 | 101973 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main | Install-Sysmon
127507 | 102330 | 4 | 102329 | 4 | .\Users\IEUser\Desktop\PWF-main\PWF-main\Install… | Install-Sysmon.ps1 | .ps1
127508 | 102331 | 3 | 101973 | 5 | .\Users\IEUser\Desktop\PWF-main\PWF-main | Resources
127509 | 102332 | 3 | 102331 | 3 | .\Users\IEUser\Desktop\PWF-main\PWF-main\Resourc… | Analysis-Notes-Template.docx | .docx
127510 | 102333 | 3 | 102331 | 3 | .\Users\IEUser\Desktop\PWF-main\PWF-main\Resourc… | PracticalWindowsForensics-cheat-sheet.pdf | .pdf
127511 | 102334 | 3 | 102331 | 3 | .\Users\IEUser\Desktop\PWF-main\PWF-main\Resourc… | RegRipper-plugins.csv | .csv
127512 | 102335 | 4 | 102331 | 3 | .\Users\IEUser\Desktop\PWF-main\PWF-main\Resourc… | RegRipper-plugins.xlsx | .xlsx
C:\Cases\MFT\MFT.csv
Total lines 296,542 Visible lines 18 Open files: 1 Search options
11:20 PM 5/21/2023
Right Ctrl


Win2019-For (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Timeline Explorer v1.3.0.0
File Tools Tabs View Help
20230521234229_PECmd_Output.csv
Drag a column header here to group by that column
Enter text to search...
Find
Line | T… | Note | Source Filename | Volume1Seri… | Source Created | Source Modif… | Source Access… | Executable Name | Run Count | Hash | Size | Version | Last Run | Pr
6 | C:\Cases\F\Windows\prefetch\ATOMICSERVICE.EXE-9… | 2023-05-20 14:09:10 | 2023-05-20 1… | 2023-05-20 14… | ATOMICSERVICE.EXE | 1 | 94EEF3DF | 34094 | Windows … | 2023-05…
58 | C:\Cases\F\Windows\prefetch\MAVINJECT.EXE-A1587… | 2023-05-20 14:09:14 | 2023-05-20 1… | 2023-05-20 14… | MAVINJECT.EXE | 1 | A1587B25 | 10552 | Windows … | 2023-05…
Tag = Checked
Edit Filter
C:\Cases\Execution\20230521234229_PECmd_Output.csv
Total lines 204 Visible lines 2 Open files: 1 Search options
11:45 PM 5/21/2023
Right Ctrl


Win2019-For (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
forensics@WIN-PUGTDA0QS0U: /mnt/c/Evidence
2532 716 smartscreen.ex 0xc48eab9f4080 7 - 1 False 2023-05-20 14:01:53.000000 N/A Disabled
4048 2284 SecurityHealth 0xc48eab9f7080 3 - 1 False 2023-05-20 14:01:54.000000 N/A Disabled
3368 588 SecurityHealth 0xc48eac13d2c0 9 - 0 False 2023-05-20 14:01:54.000000 N/A Disabled
4036 2284 VBoxTray.exe 0xc48eab365080 13 - 1 False 2023-05-20 14:01:54.000000 N/A Disabled
4628 2284 OneDrive.exe 0xc48eab861080 19 - 1 True 2023-05-20 14:01:55.000000 N/A Disabled
4944 588 svchost.exe 0xc48eab148080 11 - 0 False 2023-05-20 14:01:57.000000 N/A Disabled
5312 716 dllhost.exe 0xc48eac8c8080 4 - 1 True 2023-05-20 14:02:05.000000 N/A Disabled
5584 716 TextInputHost. 0xc48eacc0d080 11 - 1 False 2023-05-20 14:02:12.000000 N/A Disabled
5792 716 dllhost.exe 0xc48eac205340 7 - 1 False 2023-05-20 14:02:13.000000 N/A Disabled
6060 716 ApplicationFra 0xc48eac203080 7 - 1 False 2023-05-20 14:02:22.000000 N/A Disabled
4732 588 svchost.exe 0xc48eac716080 3 - 0 False 2023-05-20 14:02:25.000000 N/A Disabled
3972 716 WinStore.App.e 0xc48eacbec080 13 - 1 False 2023-05-20 14:02:43.000000 N/A Disabled
6132 716 RuntimeBroker. 0xc48eab922080 1 - 1 False 2023-05-20 14:02:44.000000 N/A Disabled
4344 716 SystemSettings 0xc48eabc57080 19 - 1 False 2023-05-20 14:02:54.000000 N/A Disabled
3360 716 UserOOBEBroker 0xc48eac0c1300 1 - 1 False 2023-05-20 14:02:54.000000 N/A Disabled
5860 2284 powershell.exe 0xc48eac850080 22 - 1 False 2023-05-20 14:03:25.000000 N/A Disabled
3648 5860 conhost.exe 0xc48eac74e080 4 - 1 False 2023-05-20 14:03:25.000000 N/A Disabled
6016 588 SgrmBroker.exe 0xc48eac74f080 7 - 0 False 2023-05-20 14:03:28.000000 N/A Disabled
5220 588 uhssvc.exe 0xc48eabaa72c0 4 - 0 False 2023-05-20 14:03:28.000000 N/A Disabled
5560 588 svchost.exe 0xc48eac89b2c0 8 - 0 False 2023-05-20 14:03:28.000000 N/A Disabled
1152 716 ShellExperienc 0xc48eab9fb080 11 - 1 False 2023-05-20 14:03:43.000000 N/A Disabled
2184 716 RuntimeBroker. 0xc48ea4a09080 5 - 1 False 2023-05-20 14:03:43.000000 N/A Disabled
1400 716 WmiPrvSE.exe 0xc48eabeee080 4 - 0 False 2023-05-20 14:04:25.000000 N/A Disabled
1680 588 Sysmon.exe 0xc48eabf70080 10 - 0 False 2023-05-20 14:04:26.000000 N/A Disabled
1012 716 unsecapp.exe 0xc48eac533080 3 - 0 False 2023-05-20 14:04:26.000000 N/A Disabled
2868 2412 SearchProtocol 0xc48eacc0f080 7 - 0 False 2023-05-20 14:08:15.000000 N/A Disabled
1140 2412 SearchFilterHo 0xc48eac0ba080 5 - 0 False 2023-05-20 14:08:15.000000 N/A Disabled
2228 588 AtomicService. 0xc48eac973300 5 - 0 False 2023-05-20 14:09:00.000000 N/A Disabled
3384 4612 notepad.exe 0xc48eac214080 5 - 1 False 2023-05-20 14:09:04.000000 N/A Disabled
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$ vol -f win10-memory.raw windows.pslist | grep notepad.exe
3384ress461200.0notepad.exe 0xc48eac214080 5 - 1 False 2023-05-20 14:09:04.000000 N/A Disabled
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$
12:31 AM
5/22/2023
Right Ctrl


Win2019-For (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
forensics@WIN-PUGTDA0QS0U: /mnt/c/Evidence
3384ress461200.0notepad.exe 0xc48eac214080 5 - 1 False 2023-05-20 14:09:04.000000 N/A Dforensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$ vol -f win10-memory.raw windows.dlllist --pid 3384 --dump
Volatility 3 Framework 2.4.1
Progress: 100.00 PDB scanning finished
PID Process Base Size Name Path LoadTime File output
3384 notepad.exe 0x7ff6d6060000 0x38000 notepad.exe C:\Windows\system32\notepad.exe 2023-05-20 14:09:04.000000 pid.3384.notepad.exe.0x1af12762550.0x7ff6d6060000.dmp
3384 notepad.exe 0x7ffa0db30000 0x1f8000 ntdll.dll C:\Windows\SYSTEM32\ntdll.dll 2023-05-20 14:09:04.000000 pid.3384.ntdll.dll.0x1af127623c0.0x7ffa0db30000.dmp
3384 notepad.exe 0x7ffa0d1b0000 0xbf000 KERNEL32.DLL C:\Windows\System32\KERNEL32.DLL 2023-05-20 14:09:04.000000 pid.3384.KERNEL32.DLL.0x1af12762a10.0x7ffa0d1b0000.dmp
3384 notepad.exe 0x7ffa0b740000 0x2f6000 KERNELBASE.dll C:\Windows\System32\KERNELBASE.dll 2023-05-20 14:09:04.000000 pid.3384.KERNELBASE.dll.0x1af12763020.0x7ffa0b740000.dmp
3384 notepad.exe 0x7ffa0c060000 0x2c000 GDI32.dll C:\Windows\System32\GDI32.dll 2023-05-20 14:09:04.000000 pid.3384.GDI32.dll.0x1af127646b0.0x7ffa0c060000.dmp
3384 notepad.exe 0x7ffa0b4e0000 0x22000 win32u.dll C:\Windows\System32\win32u.dll 2023-05-20 14:09:04.000000 pid.3384.win32u.dll.0x1af12764950.0x7ffa0b4e0000.dmp
3384 notepad.exe 0x7ffa0ba40000 0x115000 gdi32full.dll C:\Windows\System32\gdi32full.dll 2023-05-20 14:09:04.000000 pid.3384.gdi32full.dll.0x1af12764c70.0x7ffa0ba40000.dmp
3384 notepad.exe 0x7ffa0b510000 0x9d000 msvcp_win.dll C:\Windows\System32\msvcp_win.dll 2023-05-20 14:09:04.000000 pid.3384.msvcp_win.dll.0x1af127650f0.0x7ffa0b510000.dmp
3384 notepad.exe 0x7ffa0b640000 0x100000 ucrtbase.dll C:\Windows\System32\ucrtbase.dll 2023-05-20 14:09:04.000000 pid.3384.ucrtbase.dll.0x1af127654f0.0x7ffa0b640000.dmp
3384 notepad.exe 0x7ffa0d3b0000 0x19d000 USER32.dll C:\Windows\System32\USER32.dll 2023-05-20 14:09:04.000000 pid.3384.USER32.dll.0x1af12765910.0x7ffa0d3b0000.dmp
3384 notepad.exe 0x7ffa0ca70000 0x354000 combase.dll C:\Windows\System32\combase.dll 2023-05-20 14:09:04.000000 pid.3384.combase.dll.0x1af12768220.0x7ffa0ca70000.dmp
3384 notepad.exe 0x7ffa0bd70000 0x126000 RPCRT4.dll C:\Windows\System32\RPCRT4.dll 2023-05-20 14:09:04.000000 pid.3384.RPCRT4.dll.0x1af12768ec0.0x7ffa0bd70000.dmp
3384 notepad.exe 0x7ffa0bb90000 0xad000 shcore.dll C:\Windows\System32\shcore.dll 2023-05-20 14:09:04.000000 pid.3384.shcore.dll.0x1af127692a0.0x7ffa0bb90000.dmp
3384 notepad.exe 0x7ffa0ce50000 0x9e000 msvcrt.dll C:\Windows\System32\msvcrt.dll 2023-05-20 14:09:04.000000 pid.3384.msvcrt.dll.0x1af12769ea0.0x7ffa0ce50000.dmp
3384 notepad.exe 0x7ff9fec80000 0x29a000 COMCTL32.dll C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.19041.1110_none_60b5254171f9507e\COMCTL32.dll 2023-05-20 14:09:04.000000 pid.3384.COMCTL32.dll.0x1af1276ac20.0x7ff9fec80000.dmp
3384 notepad.exe 0x7ffa0d2d0000 0x30000 IMM32.DLL C:\Windows\System32\IMM32.DLL 2023-05-20 14:09:04.000000 pid.3384.IMM32.DLL.0x1af1276f840.0x7ffa0d2d0000.dmp
3384 notepad.exe 0x7ffa0b5b0000 0x82000 bcryptPrimitives.dll C:\Windows\System32\bcryptPrimitives.dll 2023-05-20 14:09:04.000000 pid.3384.bcryptPrimitives.dll.0x1af127778f0.0x7ffa0b5b0000.dmp
3384 notepad.exe 0x7ffa0d020000 0xaf000 ADVAPI32.dll C:\Windows\System32\ADVAPI32.dll 2023-05-20 14:09:04.000000 pid.3384.ADVAPI32.dll.0x1af12777690.0x7ffa0d020000.dmp
3384 notepad.exe 0x7ffa0bfc0000 0x9c000 sechost.dll C:\Windows\System32\sechost.dll 2023-05-20 14:09:04.000000 pid.3384.sechost.dll.0x1af12777a20.0x7ffa0bfc0000.dmp
3384 notepad.exe 0x7ffa090d0000 0x12000 kernel.appcore.dll C:\Windows\SYSTEM32\kernel.appcore.dll 2023-05-20 14:09:04.000000 pid.3384.kernel.appcore.dll.0x1af12776f70.0x7ffa090d0000.dmp
3384 notepad.exe 0x7ffa08c00000 0x9e000 uxtheme.dll C:\Windows\system32\uxtheme.dll 2023-05-20 14:09:04.000000 pid.3384.uxtheme.dll.0x1af12777b50.0x7ffa08c00000.dmp
3384 notepad.exe 0x7ffa0d300000 0xa9000 clbcatq.dll C:\Windows\System32\clbcatq.dll 2023-05-20 14:09:04.000000 pid.3384.clbcatq.dll.0x1af127777c0.0x7ffa0d300000.dmp
3384 notepad.exe 0x7ffa00560000 0xf4000 MrmCoreR.dll C:\Windows\System32\MrmCoreR.dll 2023-05-20 14:09:04.000000 pid.3384.MrmCoreR.dll.0x1af127770a0.0x7ffa00560000.dmp
3384 notepad.exe 0x7ffa0c090000 0x744000 SHELL32.dll C:\Windows\System32\SHELL32.dll 2023-05-20 14:09:04.000000 pid.3384.SHELL32.dll.0x1af127771d0.0x7ffa0c090000.dmp
3384 notepad.exe 0x7ffa092d0000 0x793000 windows.storage.dll C:\Windows\SYSTEM32\windows.storage.dll
2023-05-20 14:09:04.000000 pid.3384.windows.storage.dll.0x1af12777c80.0x7ffa092d0000.dmp
3384 notepad.exe 0x7ffa0ac00000 0x2e000 Wldp.dll C:\Windows\system32\Wldp.dll 2023-05-20 14:09:04.000000 pid.3384.Wldp.dll.0x1af12777300.0x7ffa0ac00000.dmp
3384 notepad.exe 0x7ffa0c7e0000 0x55000 shlwapi.dll C:\Windows\system32\shlwapi.dll 2023-05-20 14:09:04.000000 pid.3384.shlwapi.dll.0x1af12777560.0x7ffa0c7e0000.dmp
3384 notepad.exe 0x7ffa0bc40000 0x114000 MSCTF.dll C:\Windows\System32\MSCTF.dll 2023-05-20 14:09:04.000000 pid.3384.MSCTF.dll.0x1af12777430.0x7ffa0bc40000.dmp
3384 notepad.exe 0x7ffa0cef0000 0xcd000 OLEAUT32.dll C:\Windows\System32\OLEAUT32.dll 2023-05-20 14:09:04.000000 pid.3384.OLEAUT32.dll.0x1af1278a520.0x7ffa0cef0000.dmp
3384 notepad.exe 0x7ff9f5f40000 0xac000 TextShaping.dll C:\Windows\system32\TextShaping.dll 2023-05-20 14:09:04.000000 pid.3384.TextShaping.dll.0x1af1278a780.0x7ff9f5f40000.dmp
3384 notepad.exe 0x7ff9fe4a0000 0xdd000 efswrt.dll C:\Windows\System32\efswrt.dll 2023-05-20 14:09:04.000000 pid.3384.efswrt.dll.0x1af1278a060.0x7ff9fe4a0000.dmp
3384 notepad.exe 0x7ffa04320000 0x1d000 MPR.dll C:\Windows\System32\MPR.dll 2023-05-20 14:09:04.000000 pid.3384.MPR.dll.0x1af1278a8b0.0x7ffa04320000.dmp
3384 notepad.exe 0x7ffa07ec0000 0x154000 wintypes.dll C:\Windows\SYSTEM32\wintypes.dll 2023-05-20 14:09:04.000000 pid.3384.wintypes.dll.0x1af1278a9e0.0x7ffa07ec0000.dmp
3384 notepad.exe 0x7ffa06560000 0x200000 twinapi.appcore.dll C:\Windows\System32\twinapi.appcore.dll
2023-05-20 14:09:04.000000 pid.3384.twinapi.appcore.dll.0x1af1278aea0.0x7ffa06560000.dmp
3384 notepad.exe 0x7ff9f51f0000 0x66000 oleacc.dll C:\Windows\System32\oleacc.dll 2023-05-20 14:09:04.000000 pid.3384.oleacc.dll.0x1af1278a650.0x7ff9f51f0000.dmp
3384 notepad.exe 0x7ff9f6e10000 0x1d000 T1055.001.dll C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll2023-05-20 14:09:04.000000 pid.3384.T1055.001.dll.0x1af1278b490.0x7ff9f6e10000.dmp
3384 notepad.exe 0x7ffa04300000 0xc000 Secur32.dll C:\Windows\system32\Secur32.dll 2023-05-20 14:09:04.000000 pid.3384.Secur32.dll.0x1af12789cd0.0x7ffa04300000.dmp
3384 notepad.exe 0x7ffa0b100000 0x32000 SSPICLI.DLL C:\Windows\system32\SSPICLI.DLL 2023-05-20 14:09:04.000000 pid.3384.SSPICLI.DLL.0x1af1278ab10.0x7ffa0b100000.dmp
3384 notepad.exe 0x7ff9fb150000 0xfa000 textinputframework.dll C:\Windows\SYSTEM32\textinputframework.dll 2023-05-20 14:09:37.000000 pid.3384.textinputframework.dll.0x1af12789f30.0x7ff9fb150000.dmp
3384 notepad.exe 0x7ffa08590000 0x35e000 CoreUIComponents.dll C:\Windows\System32\CoreUIComponents.dll2023-05-20 14:09:37.000000 pid.3384.CoreUIComponents.dll.0x1af1278b360.0x7ffa08590000.dmp
3384 notepad.exe 0x7ffa088f0000 0xf2000 CoreMessaging.dll C:\Windows\System32\CoreMessaging.dll 2023-05-20 14:09:37.000000 pid.3384.CoreMessaging.dll.0x1af1278ac40.0x7ffa088f0000.dmp
3384 notepad.exe 0x7ffa0cde0000 0x6b000 WS2_32.dll C:\Windows\System32\WS2_32.dll 2023-05-20 14:09:37.000000 pid.3384.WS2_32.dll.0x1af12789ba0.0x7ffa0cde0000.dmp
3384 notepad.exe 0x7ffa0a2a0000 0x33000 ntmarta.dll C:\Windows\SYSTEM32\ntmarta.dll 2023-05-20 14:09:37.000000 pid.3384.ntmarta.dll.0x1af1278afd0.0x7ffa0a2a0000.dmp
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$
12:35 AM
5/22/2023
Right Ctrl


Win2019-For (Windows Config) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
forensics@WIN-PUGTDA0QS0U: /mnt/c/Evidence
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$ strings pid.3384.T1055.001.dll.0x1af1278b490.0x7ff9f6e10000.dmp | grep Boom!
Boom!
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$ strings pid.3384.T1055.001.dll.0x1af1278b490.0x7ff9f6e10000.dmp | grep Locked and Loaded!
grep: and: No such file or directory
grep: Loaded!: No such file or directory
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$ strings pid.3384.T1055.001.dll.0x1af1278b490.0x7ff9f6e10000.dmp | grep Locked
Locked and Loaded!
forensics@WIN-PUGTDA0QS0U:/mnt/c/Evidence$
12:41 AM
5/22/2023
Right Ctrl