Evidence of persistence mechanisms:

- Windows run keys
- Startup Folders
- Windows Services
- Scheduled tasks
- Sysinternals autoruns

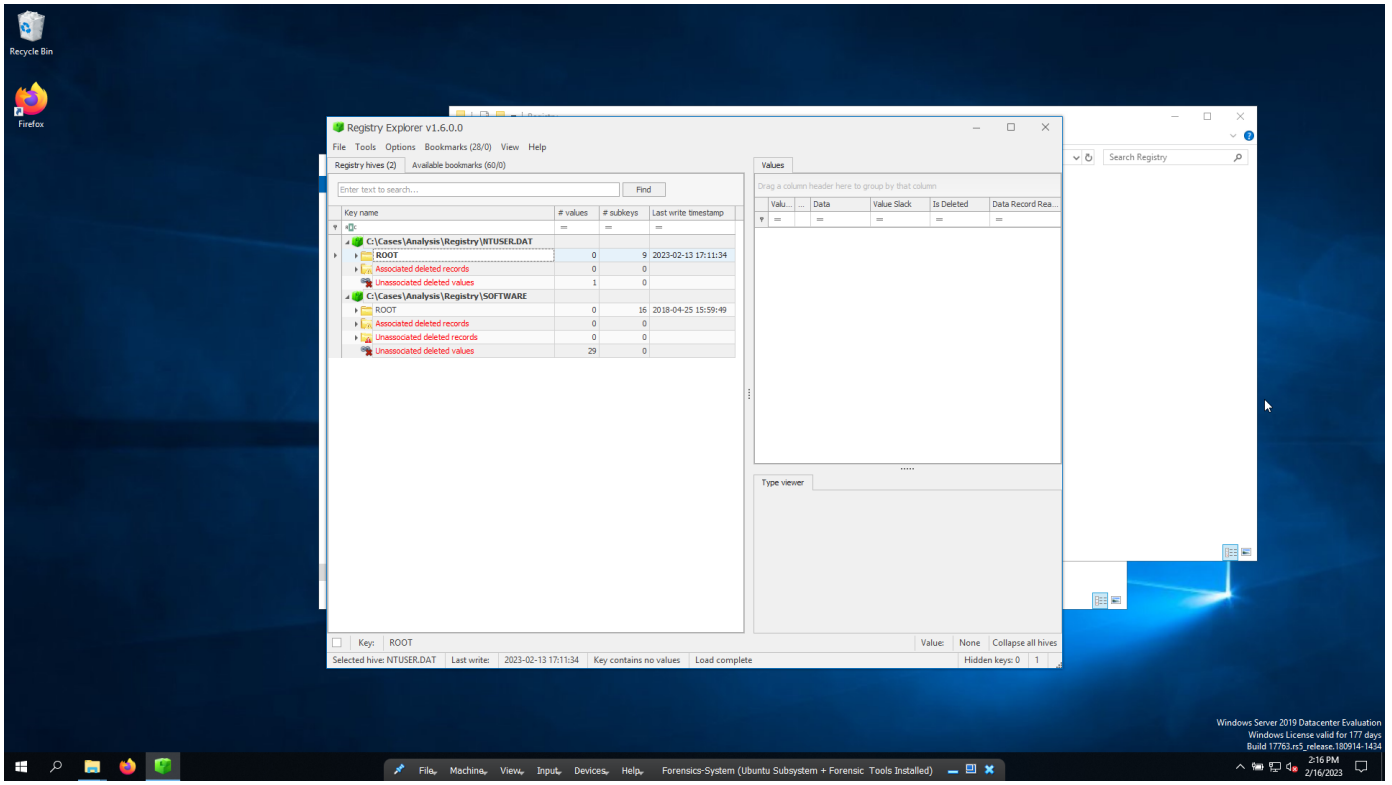
- Find:
    - Full path of AtomicService.exe that has been added to run keys.
    - Name of suspicious file in StartUp folder.
    - Time installation of atomic service.
    - What tasks did IEUser created, and what is the creation time.
    - How many times did they execute.

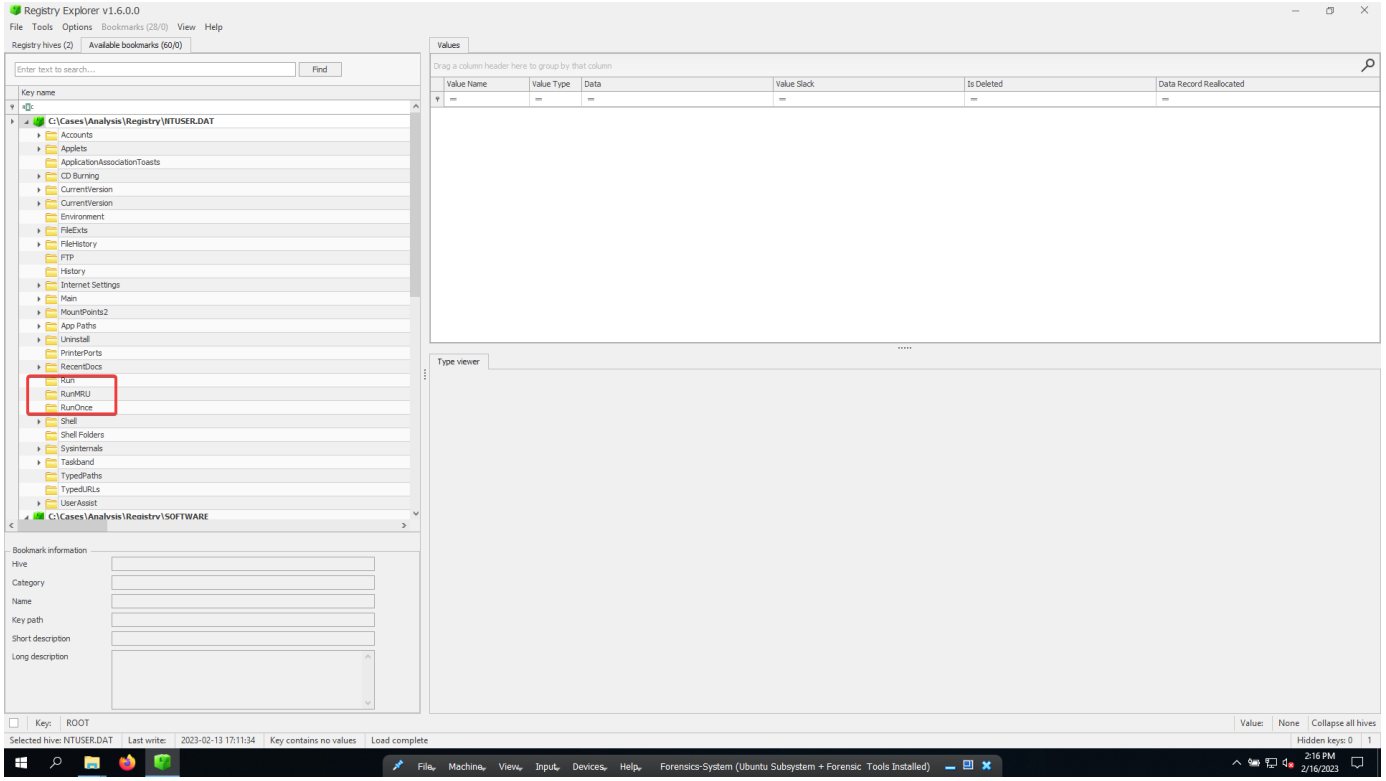
Windows run keys

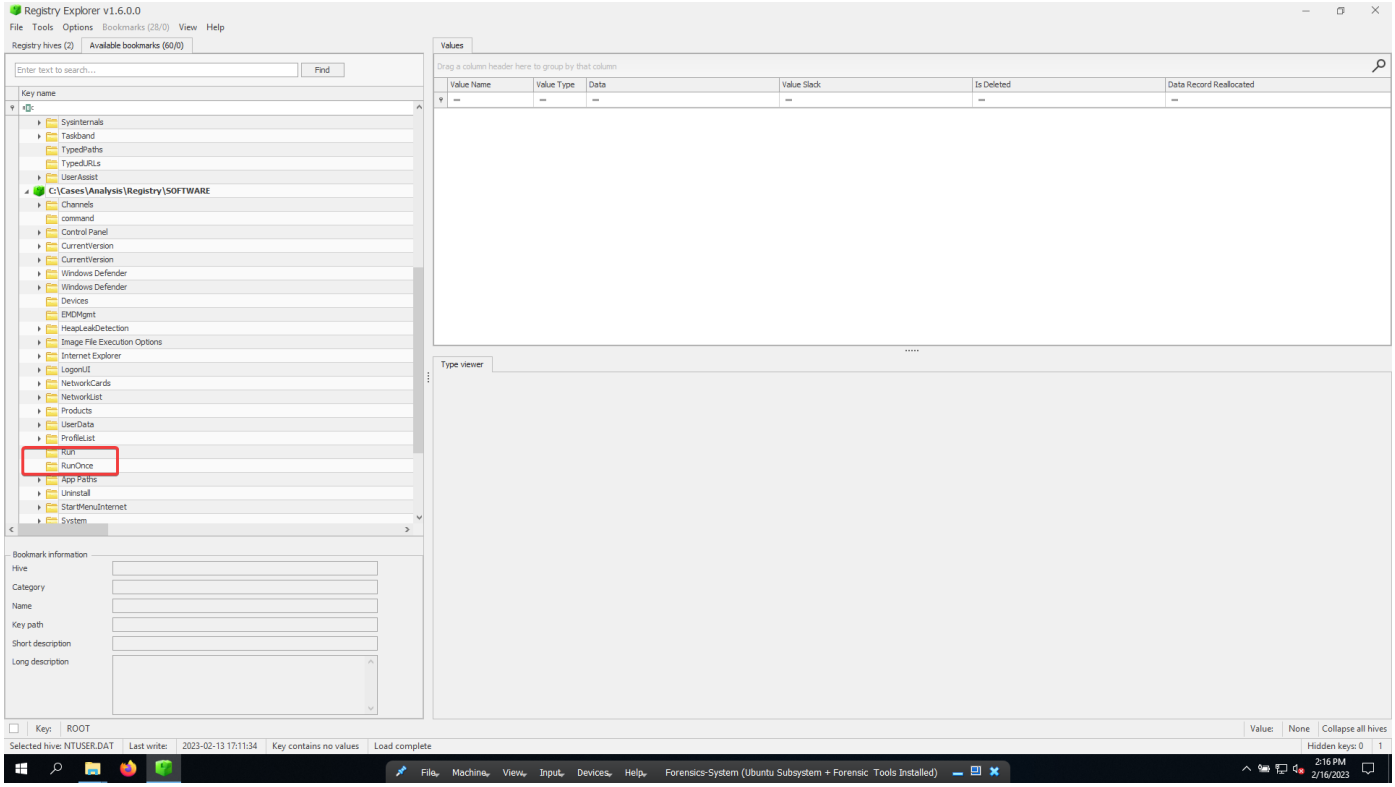
- Location of the registries artifacts:
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

- In these registries, windows automatically loads, when boots up, those applications that are referenced in this subkeys.
- HKEY_CURRENT_USER: User specific run keys (Loads when the user logs in into the system)
- HKEY_LOCAL_MACHINE: System specific run keys (Loads anyway, does not depend on what user logs in)

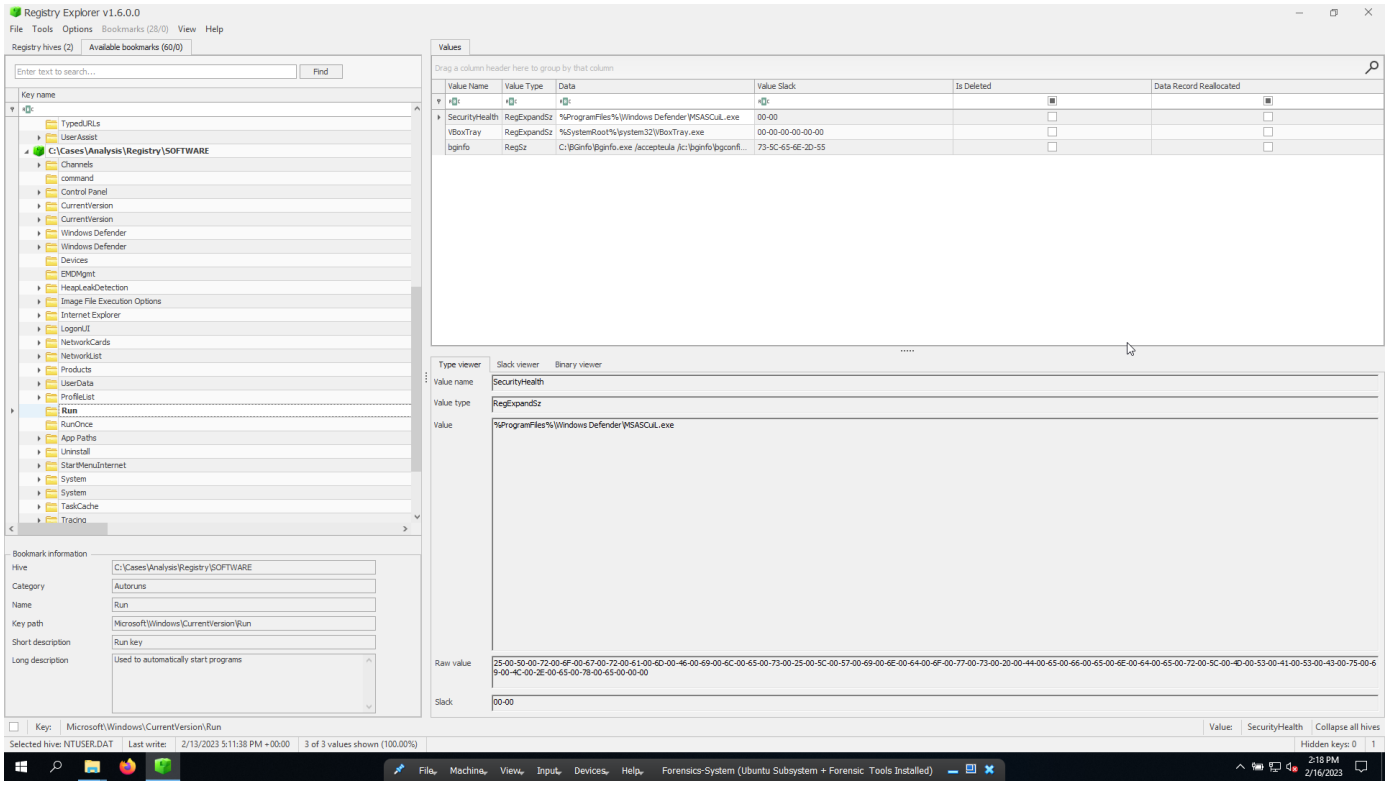
- Investigate NTUSER.DAT and SOFTWARE hives:

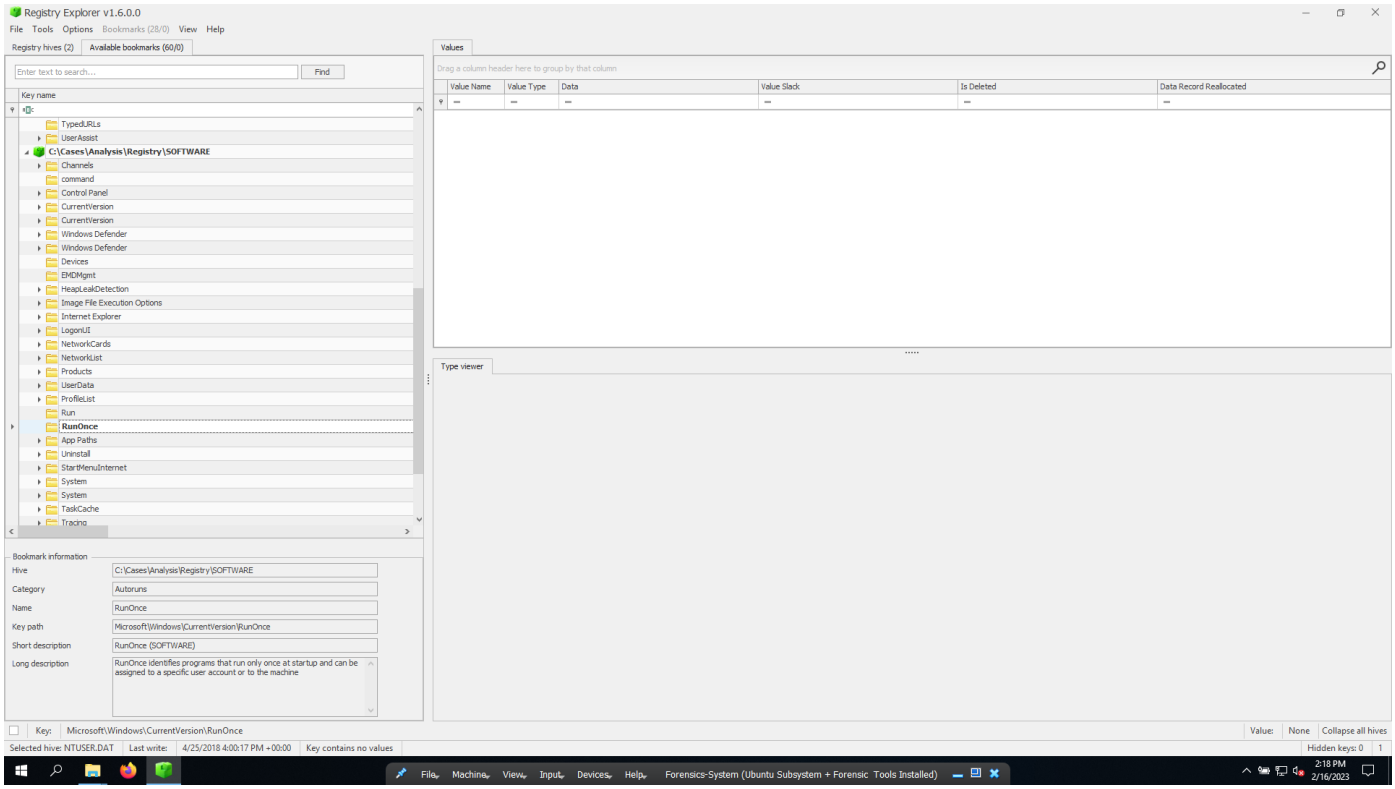




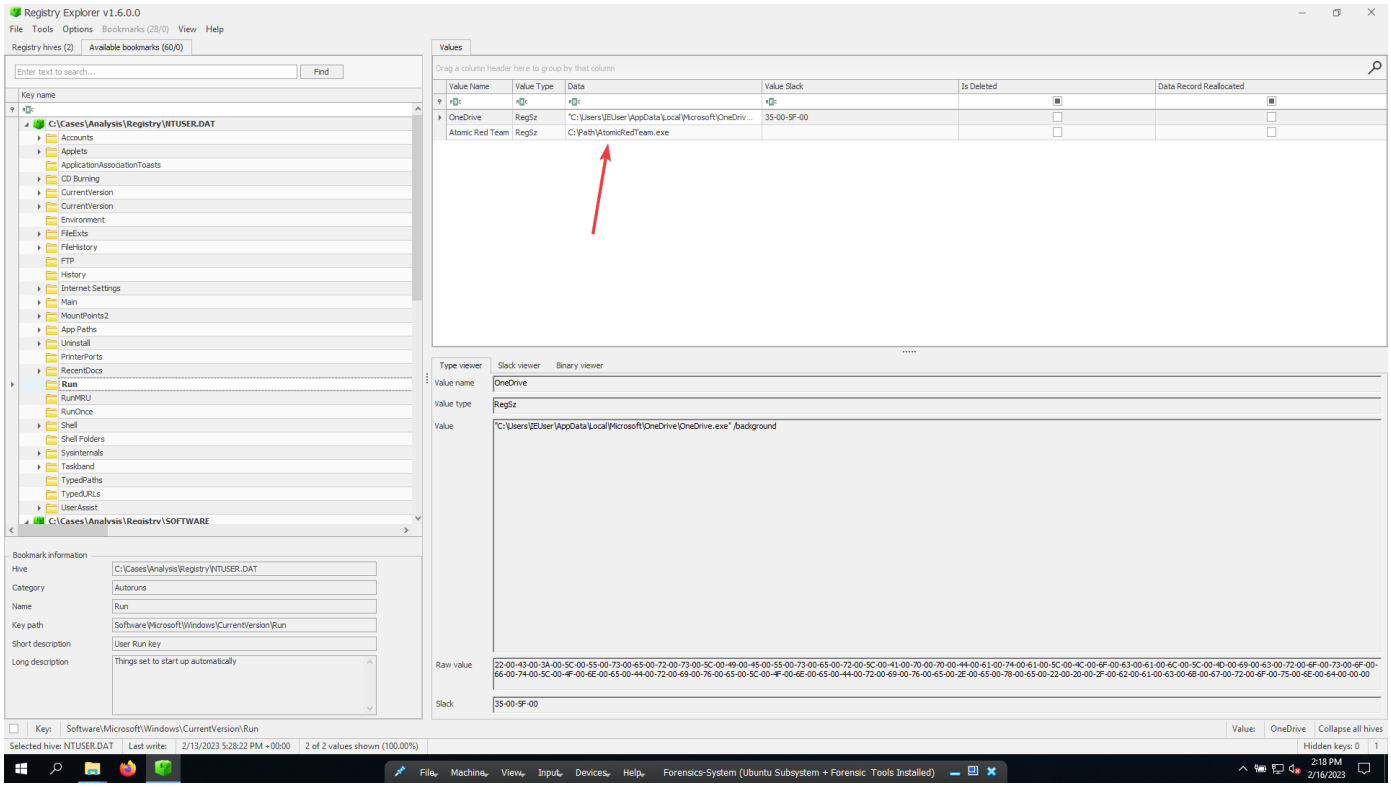


- SOFTWARE hive:





- Nothing special, moving to NTUSER.DAT hive:

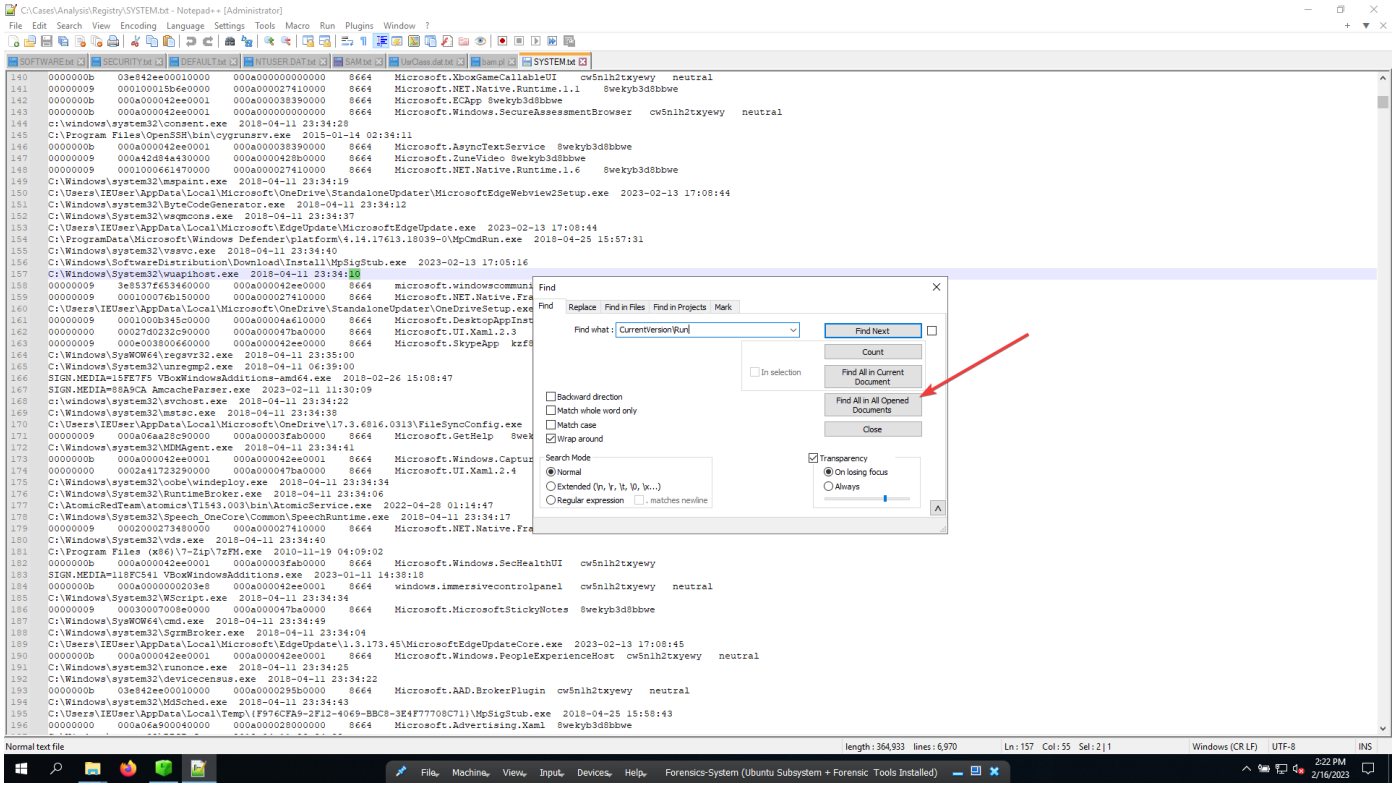


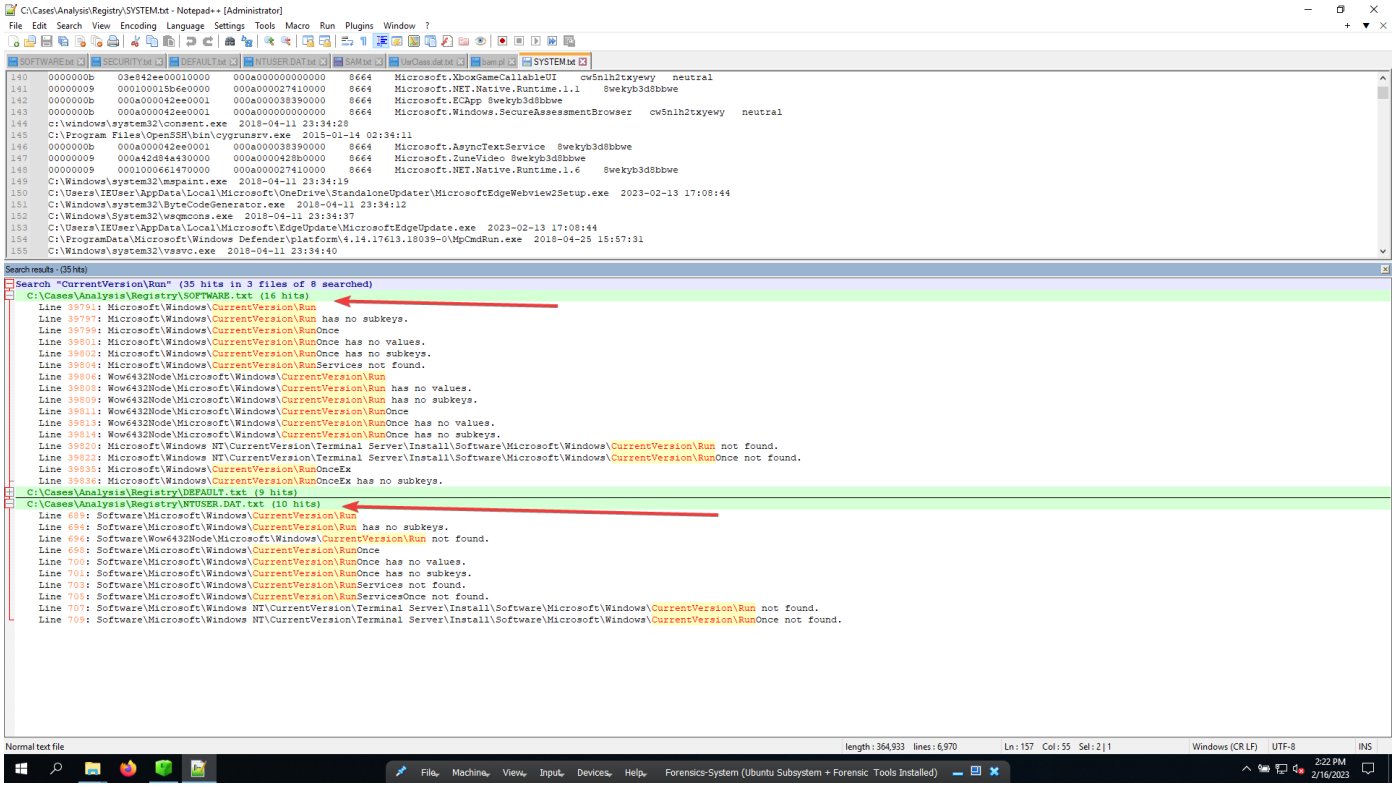
- Full path of AtomicService.exe that has been added to run keys.

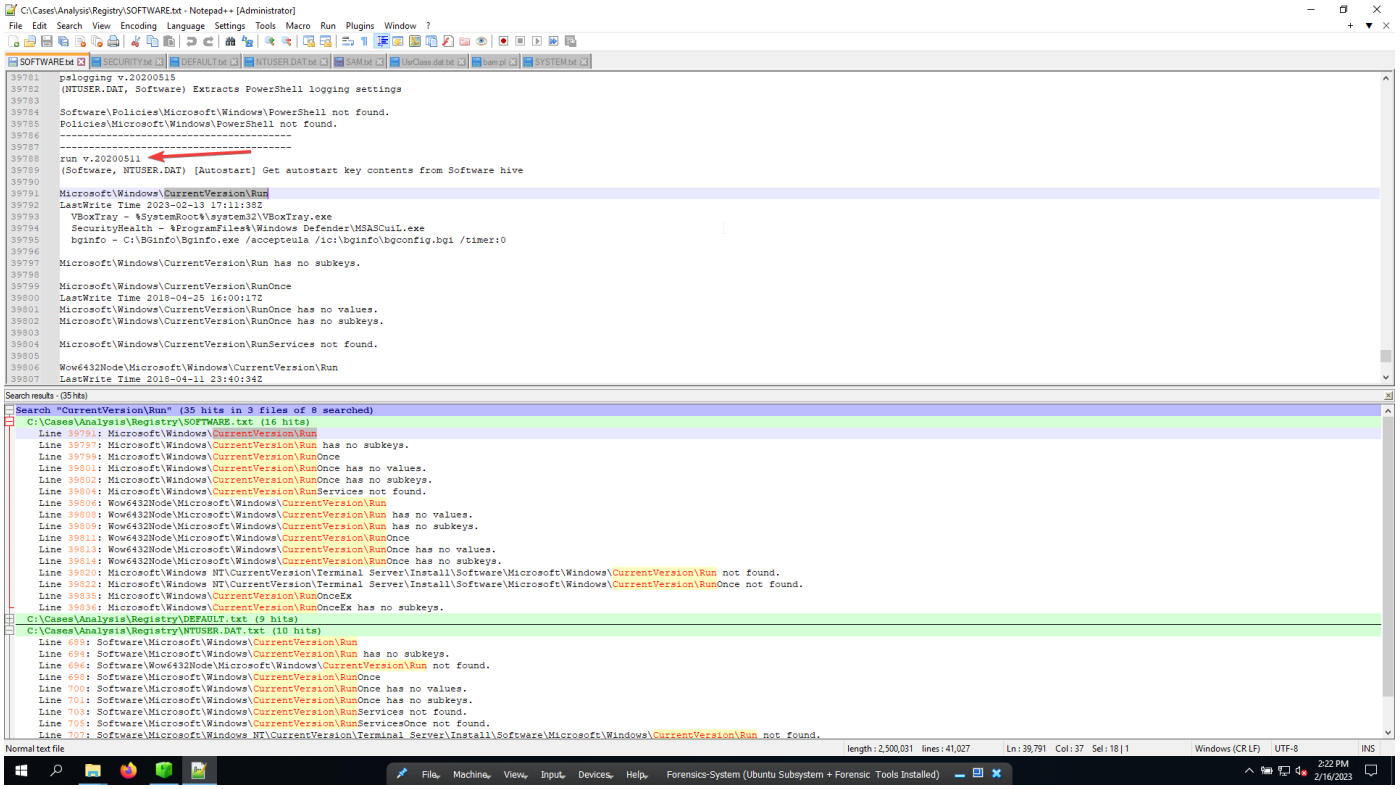
  C:\Path\AtomicRedTeam.exe

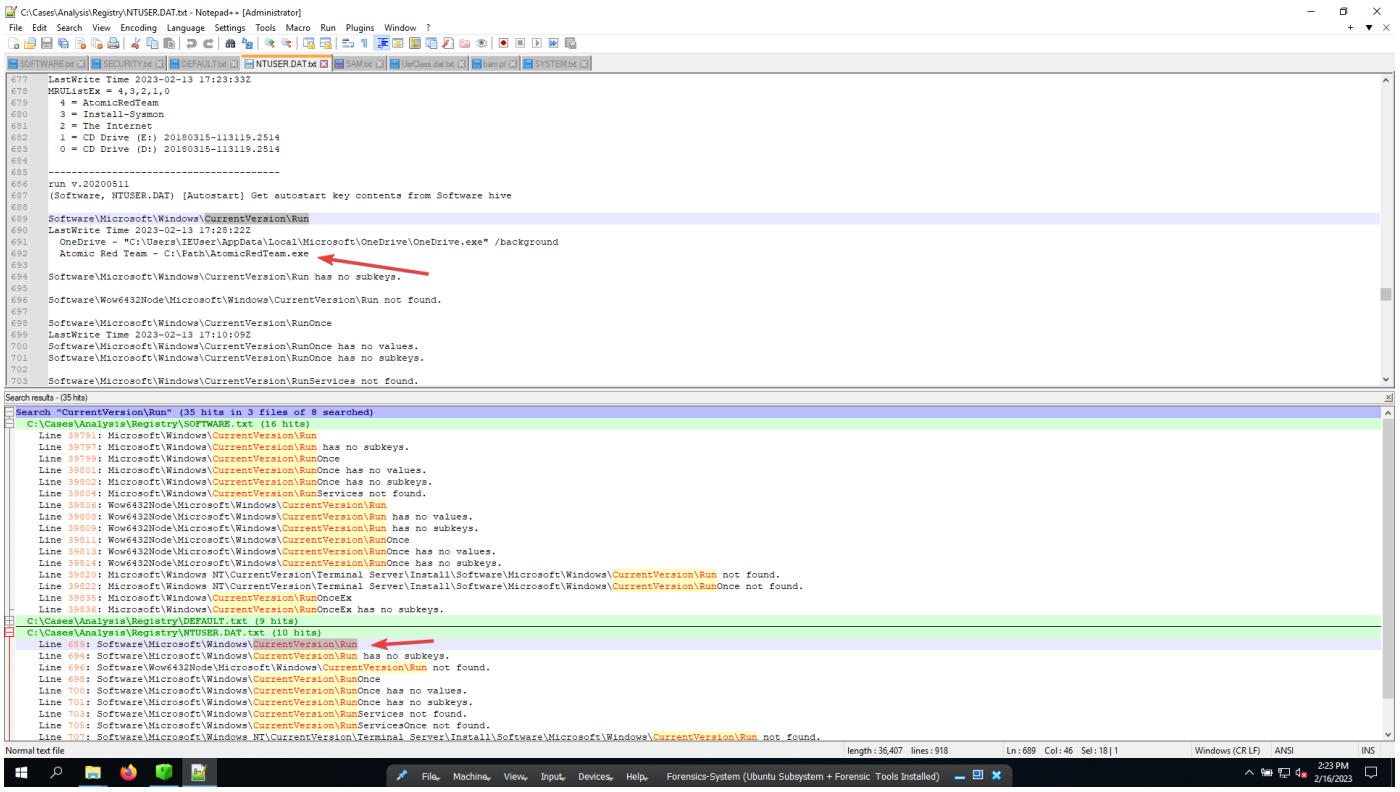
- This particular file, we cannot retrieve it or recover it , because it might have been deleted

- Search based on registry keys:


C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SOFTWARE.txt SECURITY.txt DEFAULT.txt NTUSER.DAT.txt SAM.txt UsrClass.dat.txt bam.pl SYSTEM.txt
Find
Find Replace Find in Files Find in Projects Mark
Find what : CurrentVersion\Run
Find Next
Count
In selection
Find All in Current Document
Find All in All Opened Documents
Close
Backward direction
Match whole word only
Match case
Wrap around
Search Mode
Normal
Extended (\n, \r, \t, \0, \x...)
Regular expression
. matches newline
Transparency
On losing focus
Always
Normal text file
length : 364,933 lines : 6,970
Ln : 157 Col : 55 Sel : 2 | 1
Windows (CR LF)
UTF-8
INS
File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed)
2:22 PM
2/16/2023


C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Search results - (35 hits)
Search "CurrentVersion\Run" (35 hits in 3 files of 8 searched)
C:\Cases\Analysis\Registry\SOFTWARE.txt (16 hits)
Line 39791: Microsoft\Windows\CurrentVersion\Run
Line 39797: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39799: Microsoft\Windows\CurrentVersion\RunOnce
Line 39801: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39802: Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39804: Microsoft\Windows\CurrentVersion\RunServices not found.
Line 39806: Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Line 39808: Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
Line 39809: Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39811: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
Line 39813: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39814: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39820: Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.
Line 39822: Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.
Line 39835: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39836: Microsoft\Windows\CurrentVersion\RunOnceEx has no subkeys.
C:\Cases\Analysis\Registry\DEFAULT.txt (9 hits)
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (10 hits)
Line 693: Software\Microsoft\Windows\CurrentVersion\Run
Line 694: Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 696: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Line 698: Software\Microsoft\Windows\CurrentVersion\RunOnce
Line 700: Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 701: Software\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 703: Software\Microsoft\Windows\CurrentVersion\RunServices not found.
Line 705: Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
Line 707: Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.
Line 709: Software\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.
Normal text file
length : 364,933 lines : 6,970
Ln : 157 Col : 55 Sel : 2 | 1
Windows (CR LF)
UTF-8
INS
File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed)
2:22 PM
2/16/2023



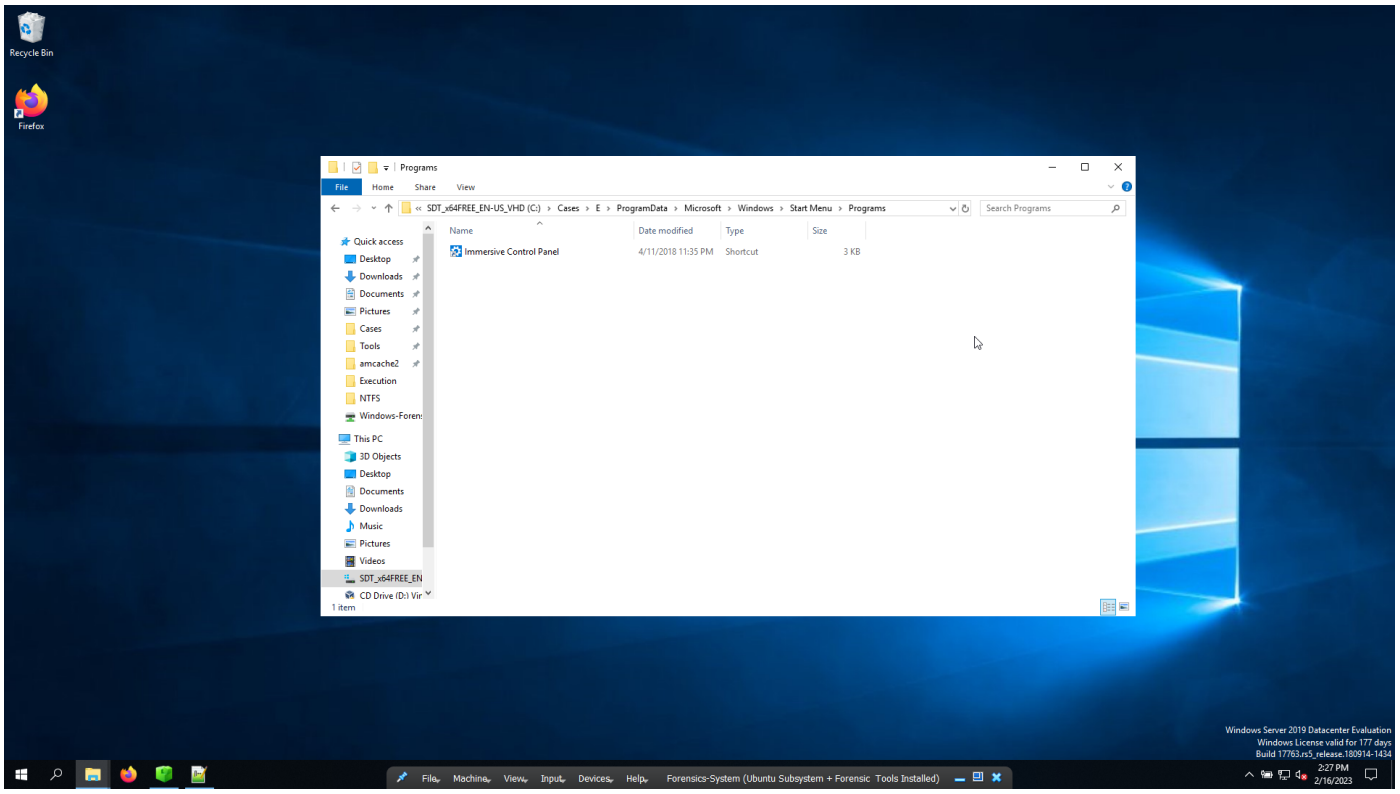


Startup Folders

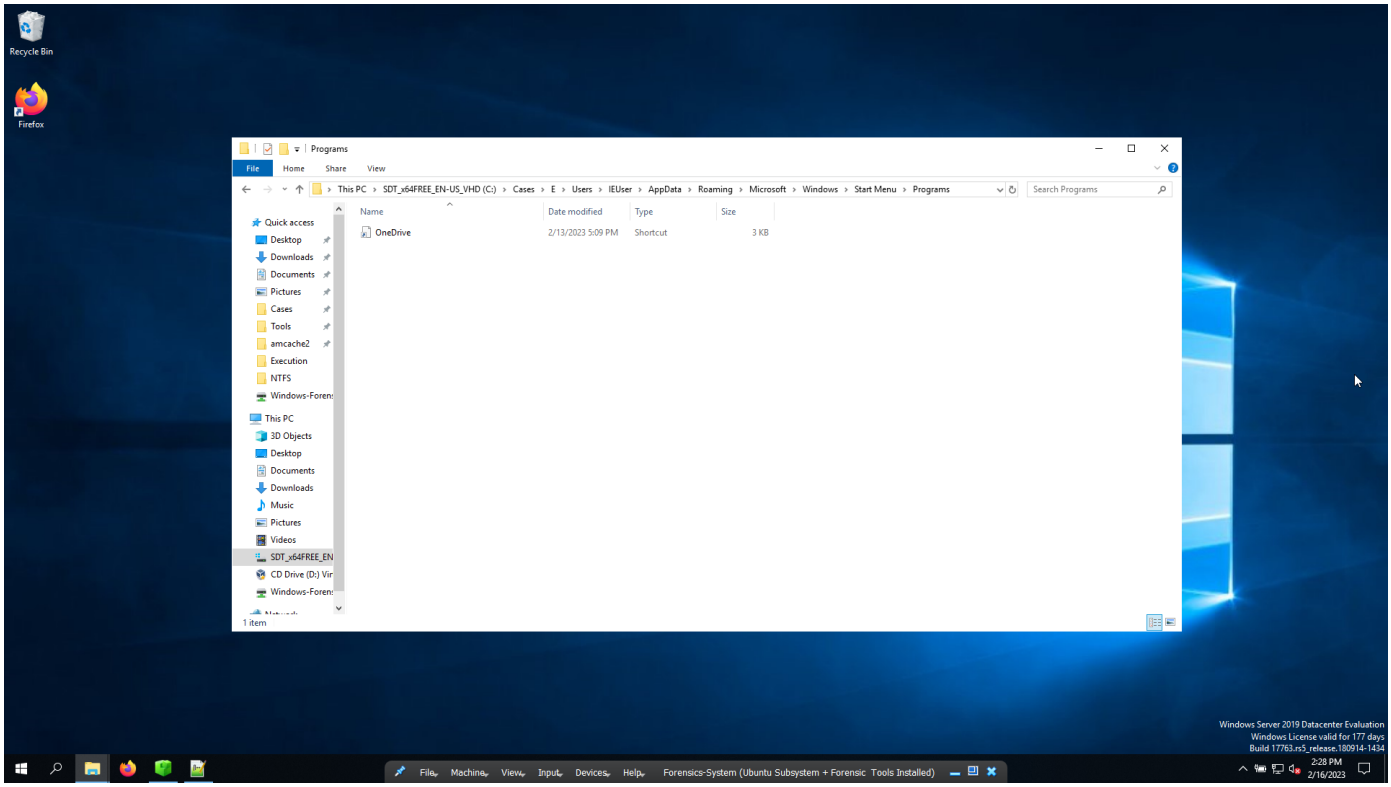
- Locations:

- C:\Users\'username'\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

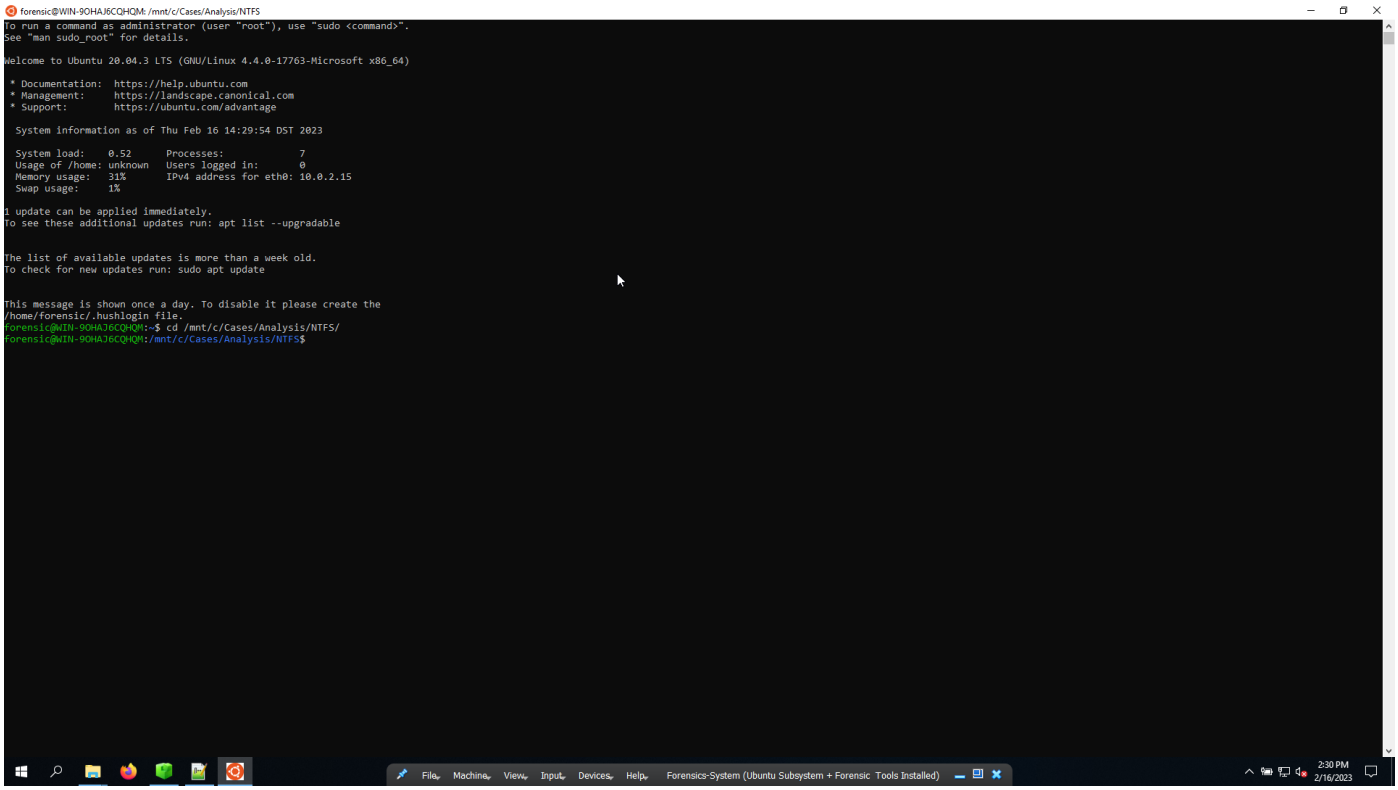
- Placing an executable in each of this paths, the windows will execute them at startup.
- We will search in these folders, and hope to find something:



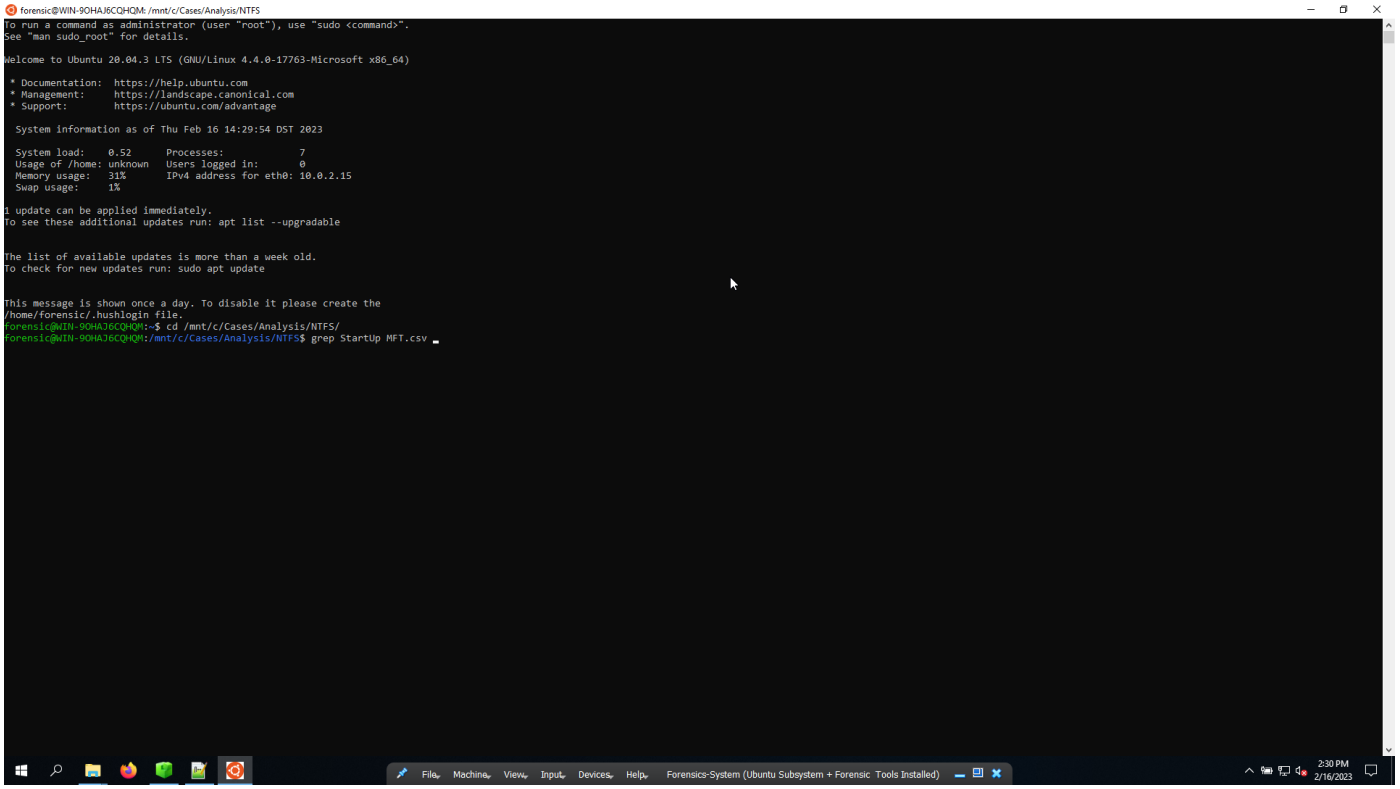
- Nothing. Moving on.

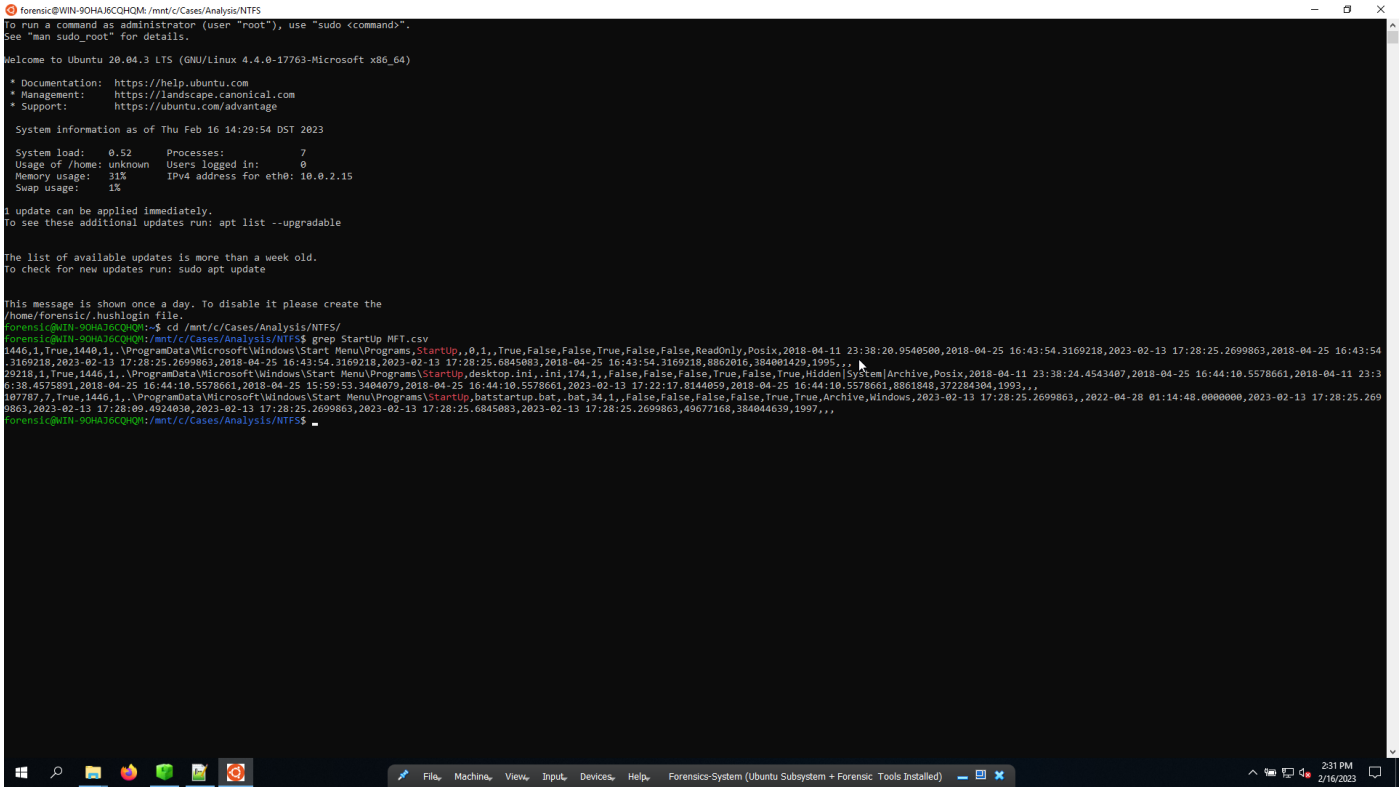


- Nothing as well.
- Lets search for the file paths in the MFT with ubuntu subsystem.
- Change directory to the NTFS folder, for the MFT file:

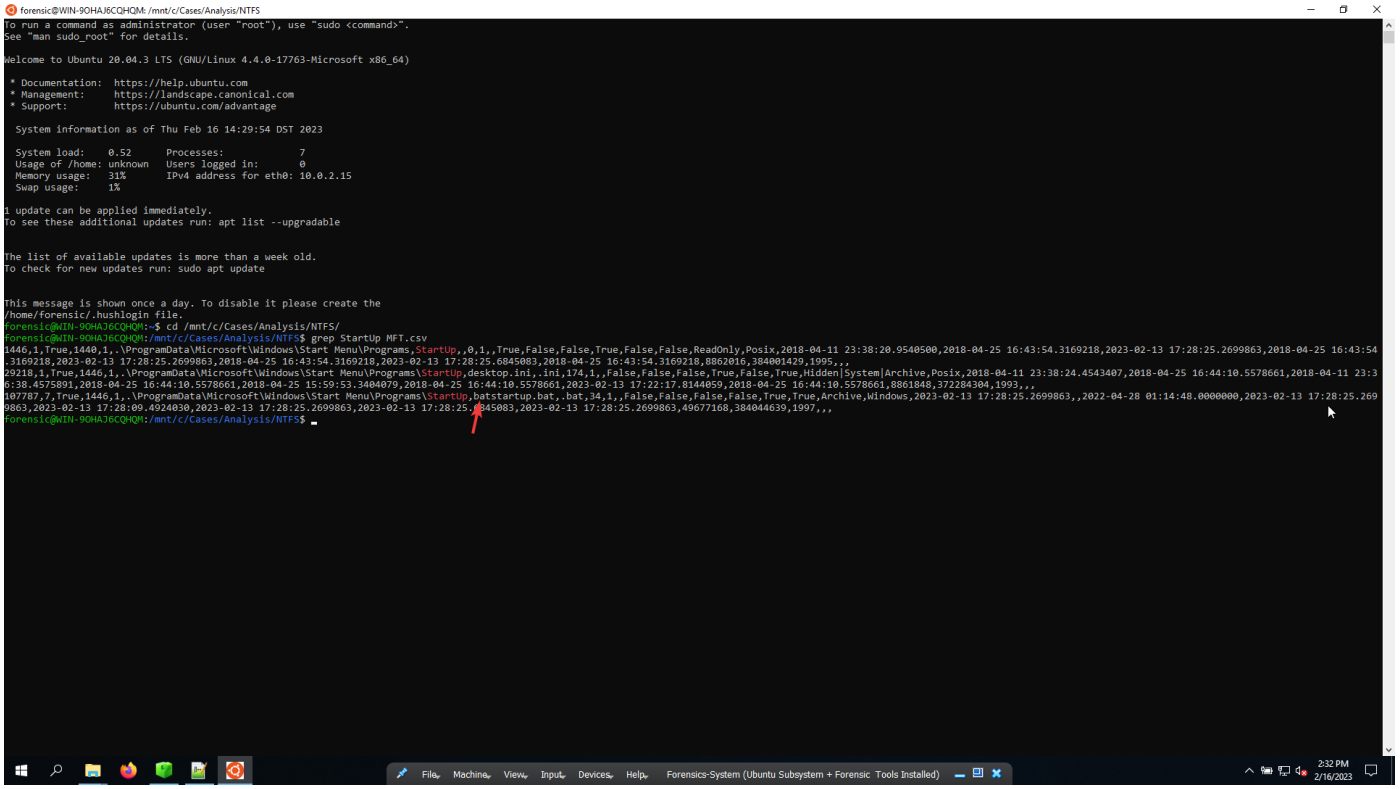


- Search in the MFT for the Startup.





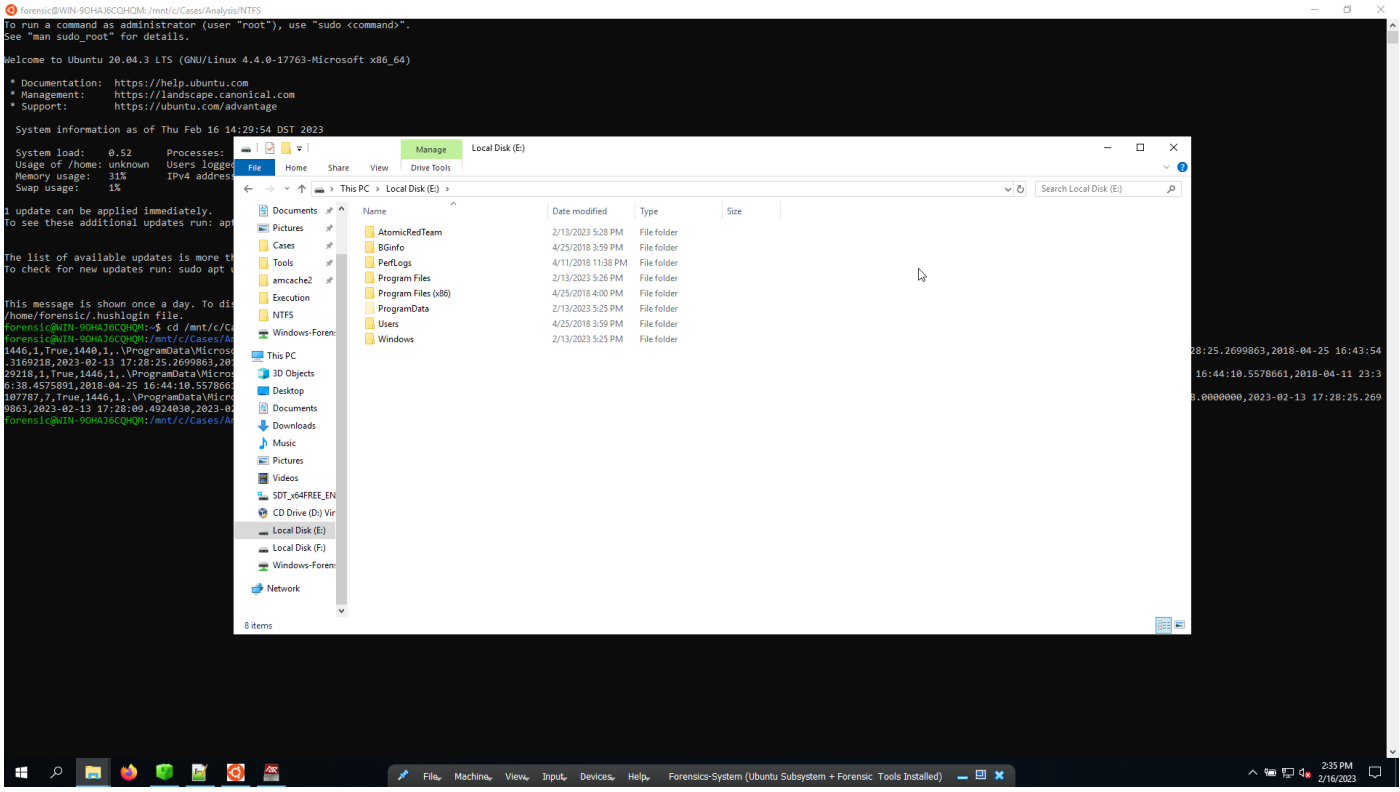
- Interesting file:



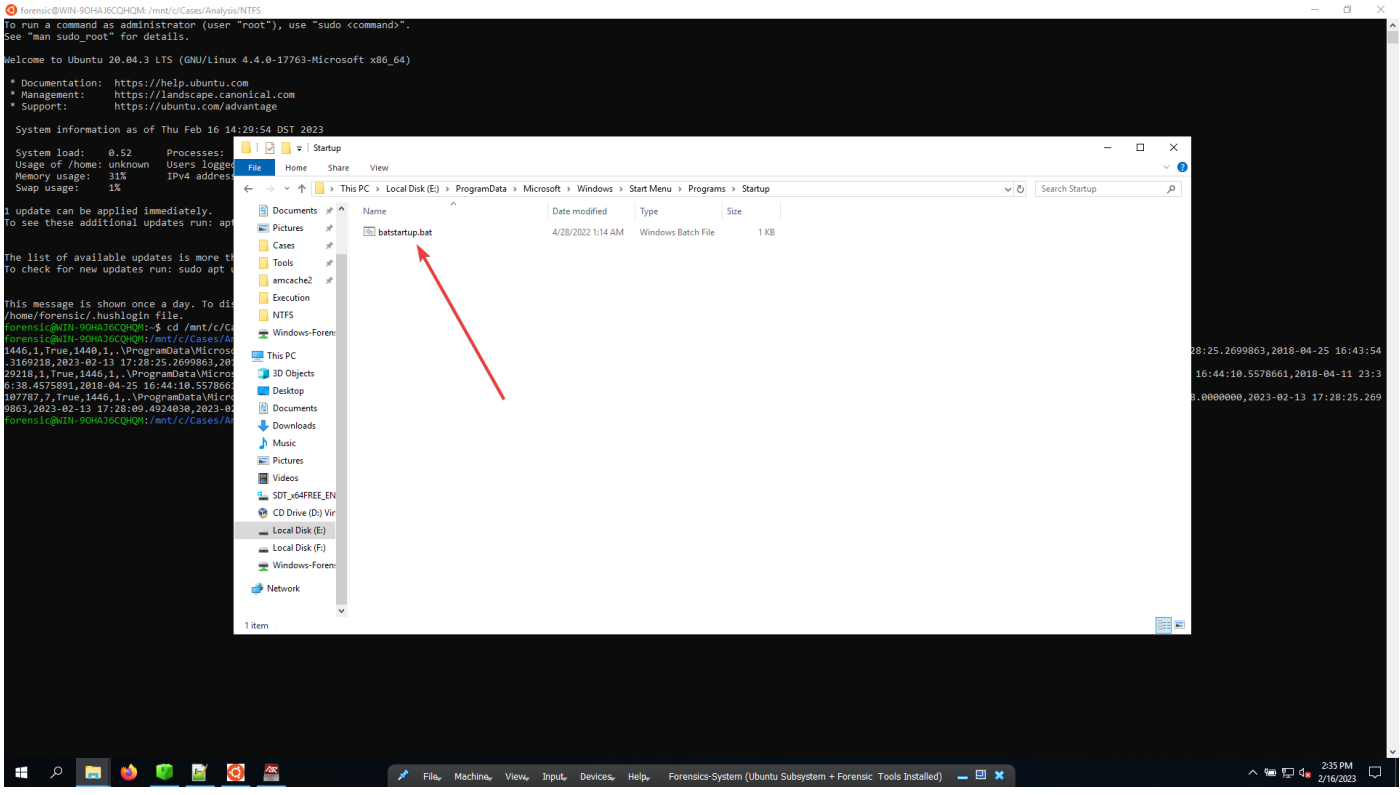
- Name of suspicious file in StartUp folder.

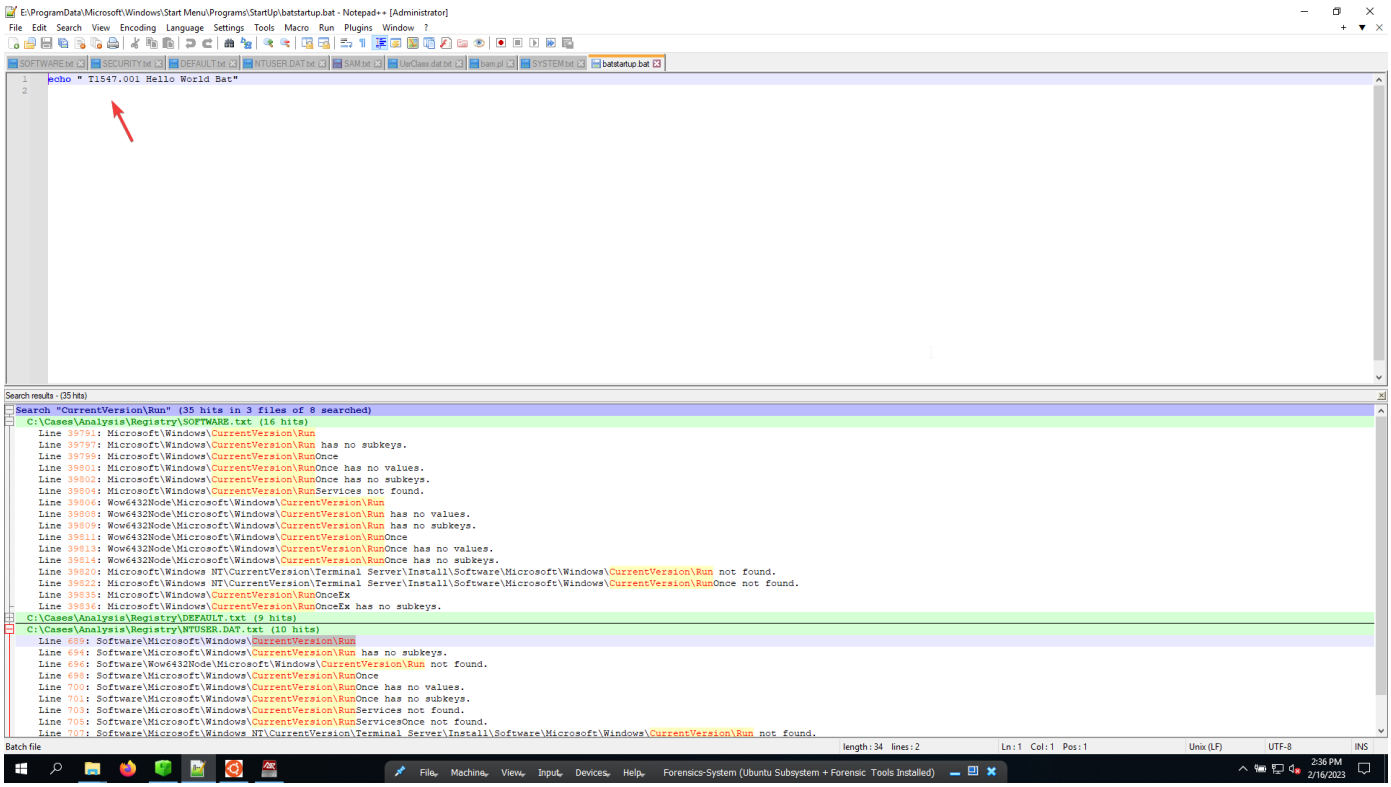
batstartup.bat

- Mount the .vhd and search for the file.



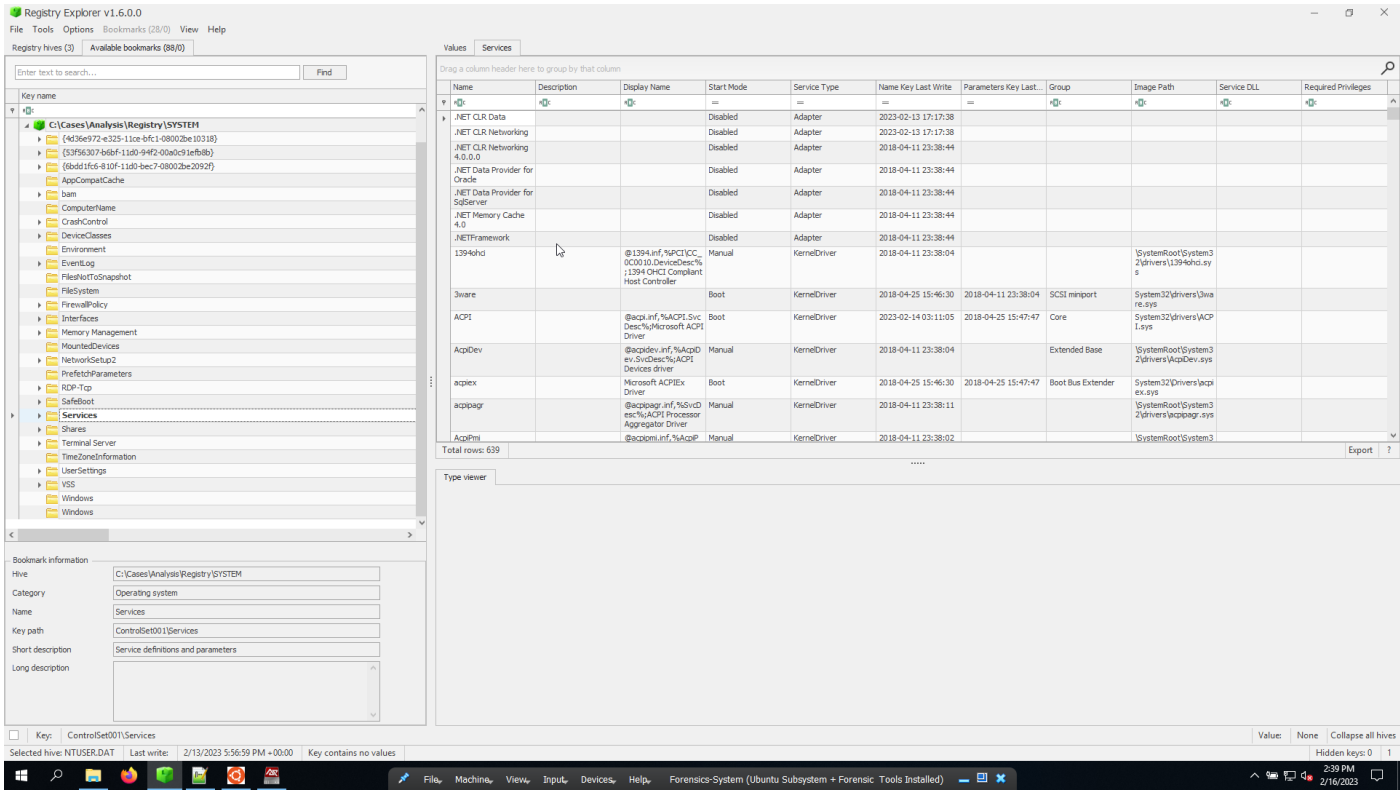
- Search the startup folder path in the mounter image:



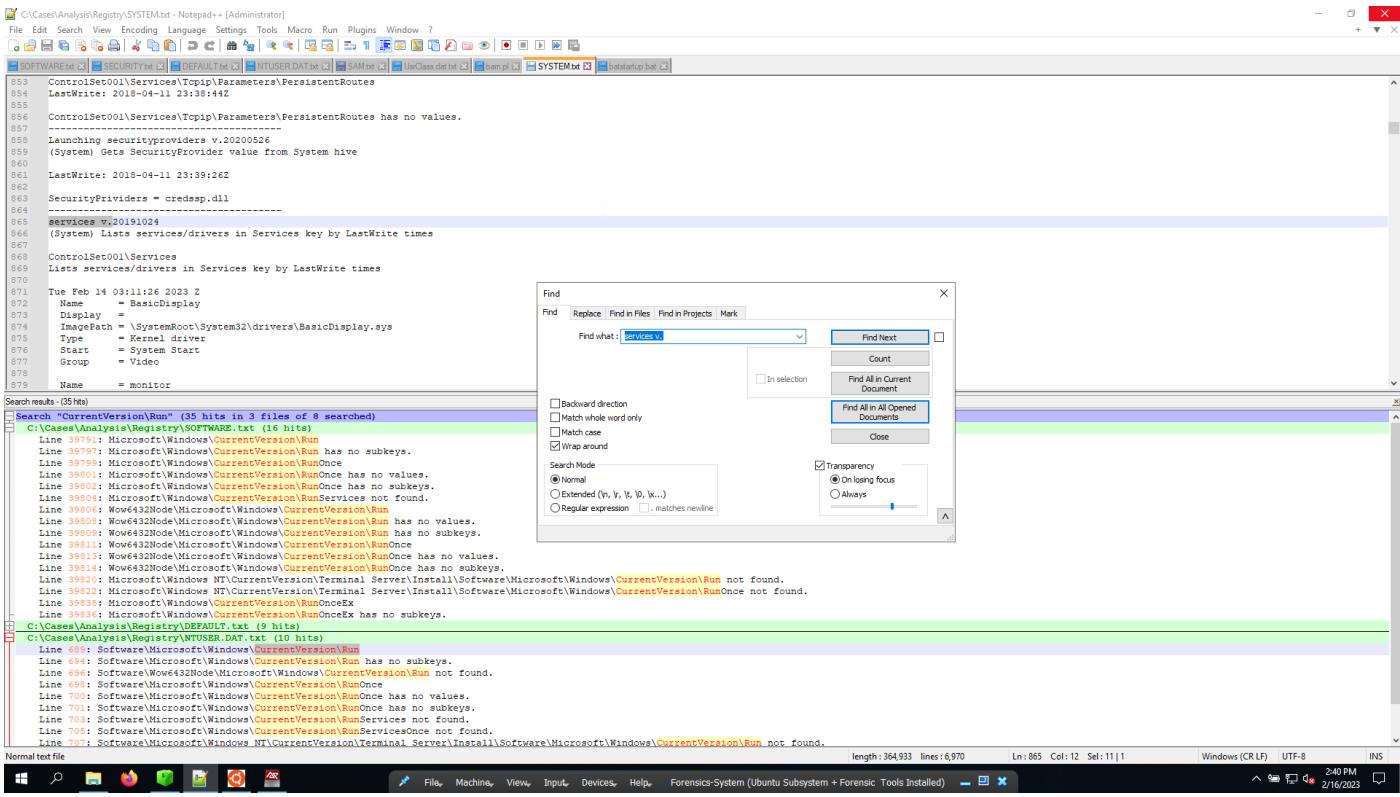


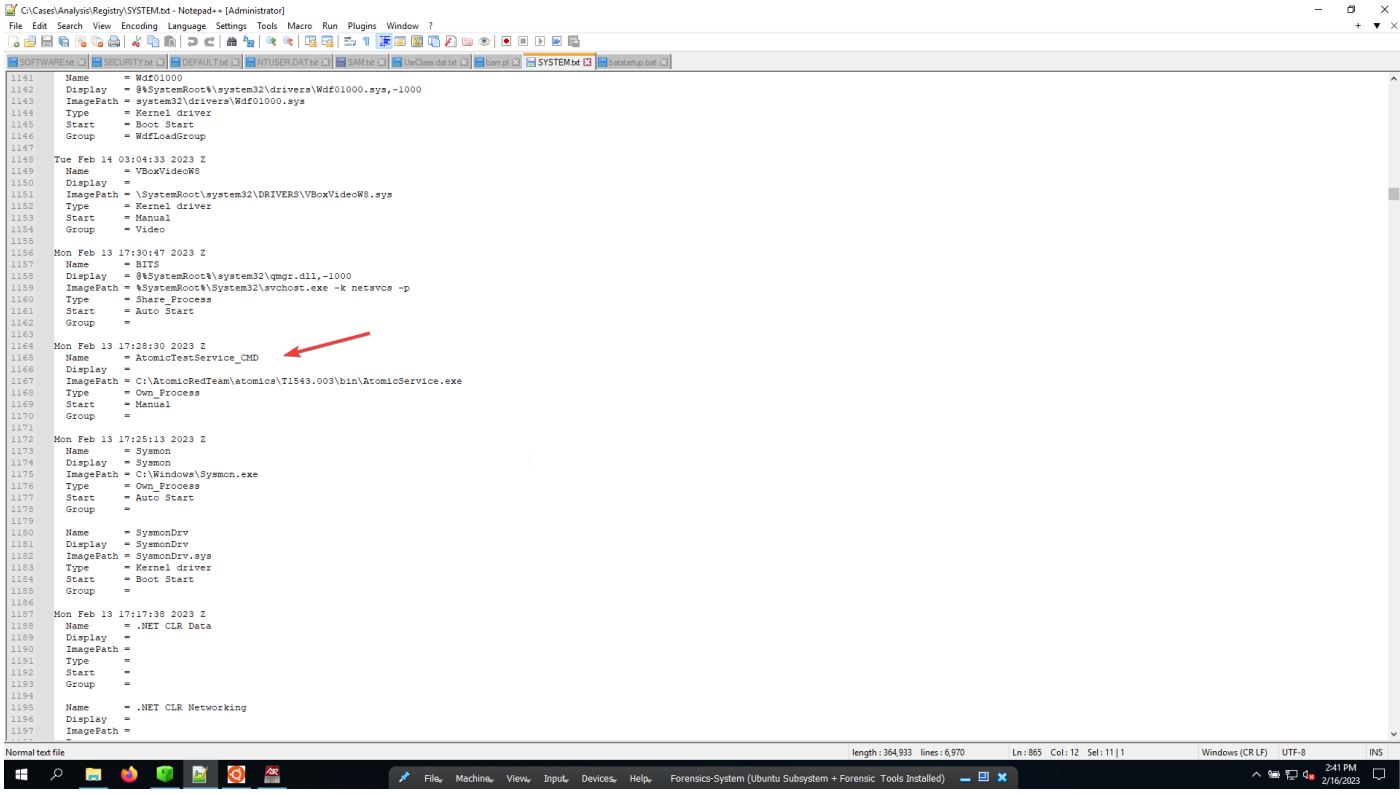
Windows Services

- Registry location : HKLM\SYSTEM\CurrentControlSet\Services
- View the registry hive with registry explorer:



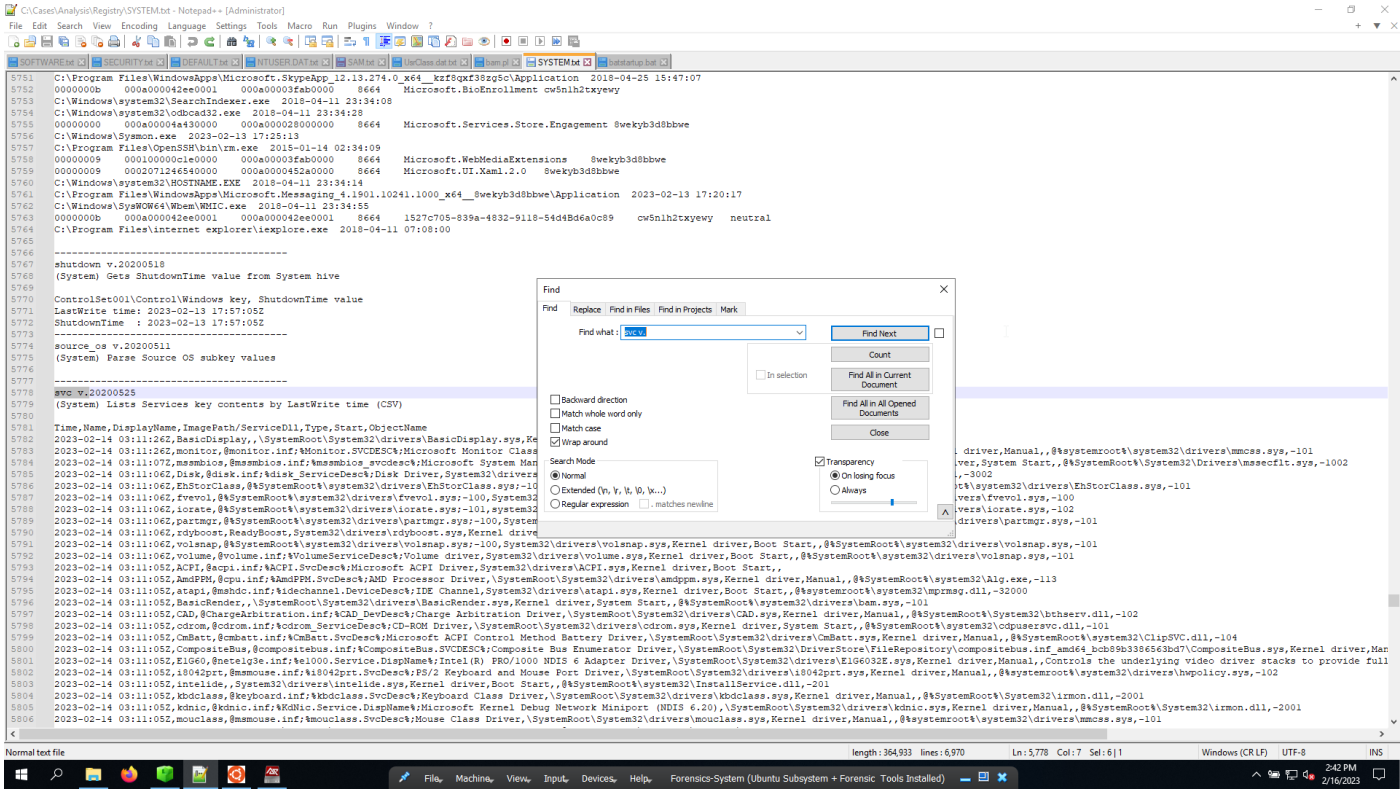
- Search the registry hive with text file with 2 plugins:
- First.



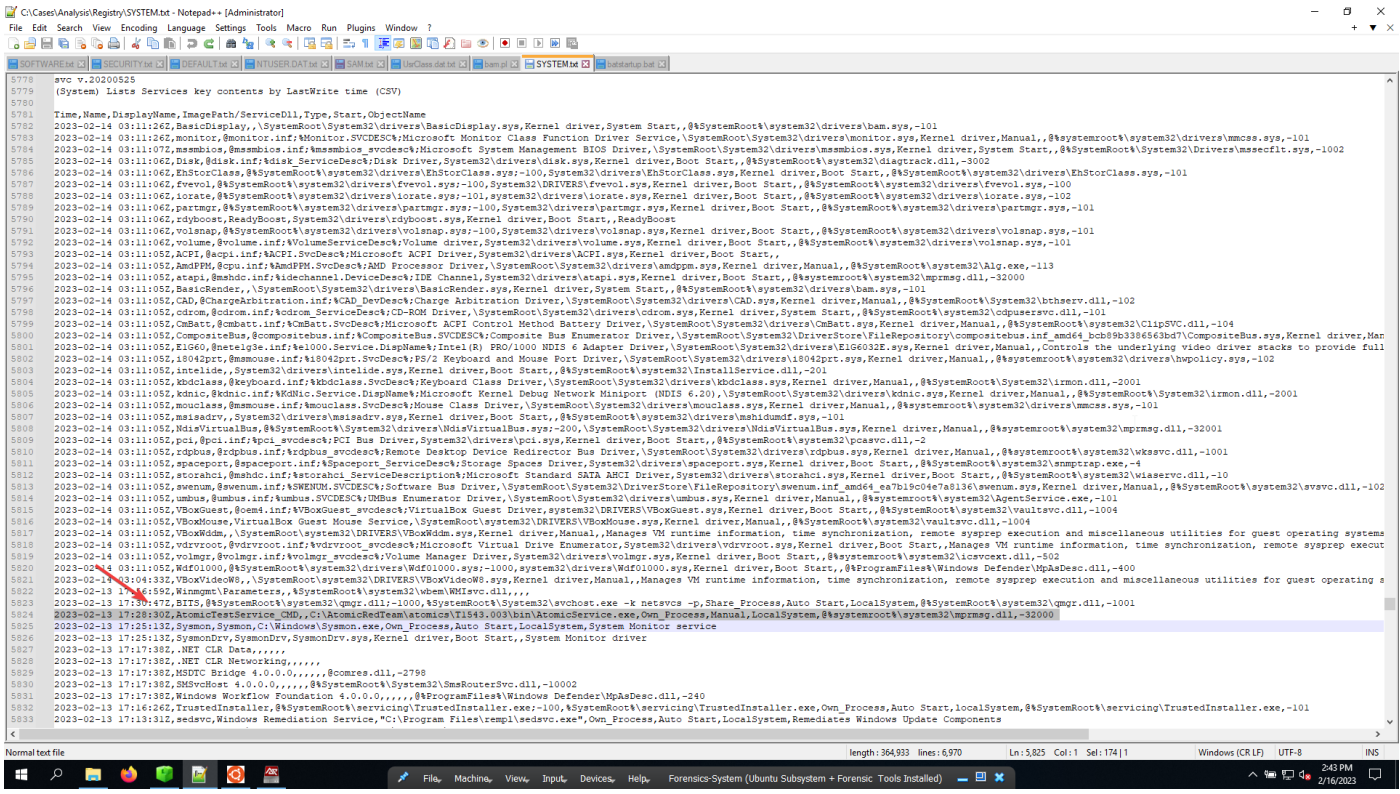


```
Name      = Wdf01000
Display   = @%SystemRoot%\system32\drivers\Wdf01000.sys,-1000
ImagePath = system32\drivers\Wdf01000.sys
Type      = Kernel driver
Start     = Boot Start
Group     = WdfLoadGroup

Tue Feb 14 03:04:33 2023 Z
Name      = VBoxVideoW8
Display   =
ImagePath = \SystemRoot\system32\DRIVERS\VBoxVideoW8.sys
Type      = Kernel driver
Start     = Manual
Group     = Video

Mon Feb 13 17:30:47 2023 Z
Name      = BITS
Display   = @%SystemRoot%\system32\qmgr.dll,-1000
ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs -p
Type      = Share_Process
Start     = Auto Start
Group     =

Mon Feb 13 17:28:30 2023 Z
Name      = AtomicTestService_CMD
Display   =
ImagePath = C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
Type      = Own_Process
Start     = Manual
Group     =

Mon Feb 13 17:25:13 2023 Z
Name      = Sysmon
Display   = Sysmon
ImagePath = C:\Windows\Sysmon.exe
Type      = Own_Process
Start     = Auto Start
Group     =

Name      = SysmonDrv
Display   = SysmonDrv
ImagePath = SysmonDrv.sys
Type      = Kernel driver
Start     = Boot Start
Group     =

Mon Feb 13 17:17:38 2023 Z
Name      = .NET CLR Data
Display   =
ImagePath =
Type      =
Start     =
Group     =

Name      = .NET CLR Networking
Display   =
ImagePath =
```

- Second.



```
C:\Program Files\WindowsApps\Microsoft.SkypeApp_12.13.274.0_x64__kzf8qxf38zg5c\Application  2018-04-25 15:47:07
0000000b    000a000042ee0001    000a00003fab0000    8664    Microsoft.BioEnrollment cw5n1h2txyewy
C:\Windows\system32\SearchIndexer.exe  2018-04-11 23:34:08
C:\Windows\system32\odbcad32.exe  2018-04-11 23:34:28
00000000    000a00004a430000    000a000028000000    8664    Microsoft.Services.Store.Engagement 8wekyb3d8bbwe
C:\Windows\Sysmon.exe  2023-02-13 17:25:13
C:\Program Files\OpenSSH\bin\rm.exe  2015-01-14 02:34:09
00000009    000100000c1e0000    000a00003fab0000    8664    Microsoft.WebMediaExtensions    8wekyb3d8bbwe
00000009    000207124654000     000a0000452a0000    8664    Microsoft.UI.Xaml.2.0   8wekyb3d8bbwe
C:\Windows\system32\HOSTNAME.EXE  2018-04-11 23:34:14
C:\Program Files\WindowsApps\Microsoft.Messaging_4.1901.10241.1000_x64__8wekyb3d8bbwe\Application  2023-02-13 17:20:17
C:\Windows\SysWOW64\Wbem\WMIC.exe  2018-04-11 23:34:55
0000000b    000a000042ee0001    000a000042ee0001    8664    1527c705-839a-4832-9118-54d4Bd6a0c89    cw5n1h2txyewy   neutral
C:\Program Files\internet explorer\iexplore.exe  2018-04-11 07:08:00

---------------------------------------
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2023-02-13 17:57:05Z
ShutdownTime  : 2023-02-13 17:57:05Z
---------------------------------------
source_os v.20200511
(System) Parse Source OS subkey values

---------------------------------------
svc v.20200525
(System) Lists Services key contents by LastWrite time (CSV)

Time,Name,DisplayName,ImagePath/ServiceDll,Type,Start,ObjectName
2023-02-14 03:11:26Z,BasicDisplay,,\SystemRoot\System32\drivers\BasicDisplay.sys,Ke
2023-02-14 03:11:26Z,monitor,@monitor.inf;%Monitor.SVCDESC%;Microsoft Monitor Class
2023-02-14 03:11:07Z,msmbios,@msmbios.inf;%msmbios_svcdesc%;Microsoft System Man
2023-02-14 03:11:06Z,Disk,@disk.inf;%disk_ServiceDesc%;Disk Driver,System32\drivers
2023-02-14 03:11:06Z,EhStorClass,@%SystemRoot%\system32\drivers\EhStorClass.sys;-10
2023-02-14 03:11:06Z,fvevol,@%SystemRoot%\system32\drivers\fvevol.sys;-100,System32
2023-02-14 03:11:06Z,iorate,@%SystemRoot%\system32\drivers\iorate.sys;-101,system32
2023-02-14 03:11:06Z,partmgr,@%SystemRoot%\system32\drivers\partmgr.sys;-100,System
2023-02-14 03:11:06Z,rdyboost,ReadyBoost,System32\drivers\rdyboost.sys,Kernel drive
2023-02-14 03:11:06Z,volsnap,@%SystemRoot%\system32\drivers\volsnap.sys;-100,System32\drivers\volsnap.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\volsnap.sys,-101
2023-02-14 03:11:06Z,volume,@volume.inf;%VolumeServiceDesc%;Volume driver,System32\drivers\volume.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\drivers\volsnap.sys,-101
2023-02-14 03:11:05Z,ACPI,@acpi.inf;%ACPI.SvcDesc%;Microsoft ACPI Driver,System32\drivers\ACPI.sys,Kernel driver,Boot Start,,
2023-02-14 03:11:05Z,AmdPPM,@cpu.inf;%AmdPPM.SvcDesc%;AMD Processor Driver,\SystemRoot\System32\drivers\amdppm.sys,Kernel driver,Manual,,@%SystemRoot%\system32\Alg.exe,-113
2023-02-14 03:11:05Z,atapi,@mshdc.inf;%idechannel.DeviceDesc%;IDE Channel,System32\drivers\atapi.sys,Kernel driver,Boot Start,,@%systemroot%\system32\mprmsg.dll,-32000
2023-02-14 03:11:05Z,BasicRender,,\SystemRoot\System32\drivers\BasicRender.sys,Kernel driver,System Start,,@%SystemRoot%\system32\drivers\bam.sys,-101
2023-02-14 03:11:05Z,CAD,@ChargeArbitration.inf;%CAD_DevDesc%;Charge Arbitration Driver,\SystemRoot\System32\drivers\CAD.sys,Kernel driver,Manual,,@%SystemRoot%\System32\bthserv.dll,-102
2023-02-14 03:11:05Z,cdrom,@cdrom.inf;%cdrom_ServiceDesc%;CD-ROM Driver,\SystemRoot\System32\drivers\cdrom.sys,Kernel driver,System Start,,@%SystemRoot%\system32\cdpusersvc.dll,-101
2023-02-14 03:11:05Z,CmBatt,@cmbatt.inf;%CmBatt.SvcDesc%;Microsoft ACPI Control Method Battery Driver,\SystemRoot\System32\drivers\CmBatt.sys,Kernel driver,Manual,,@%SystemRoot%\system32\ClipSVC.dll,-104
2023-02-14 03:11:05Z,CompositeBus,@compositebus.inf;%CompositeBus.SVCDESC%;Composite Bus Enumerator Driver,\SystemRoot\System32\DriverStore\FileRepository\compositebus.inf_amd64_bcb89b3386563bd7\CompositeBus.sys,Kernel driver,Man
2023-02-14 03:11:05Z,E1G60,@netel9e.inf;%e1000.Service.DispName%;Intel(R) PRO/1000 NDIS 6 Adapter Driver,\SystemRoot\System32\drivers\E1G6032E.sys,Kernel driver,Manual,,Controls the underlying video driver stacks to provide full
2023-02-14 03:11:05Z,i8042prt,@msmouse.inf;%i8042prt.SvcDesc%;PS/2 Keyboard and Mouse Port Driver,\SystemRoot\System32\drivers\i8042prt.sys,Kernel driver,Manual,,@%systemroot%\system32\drivers\hwpolicy.sys,-102
2023-02-14 03:11:05Z,intelide,,System32\drivers\intelide.sys,Kernel driver,Boot Start,,@%SystemRoot%\system32\InstallService.dll,-201
2023-02-14 03:11:05Z,kbdclass,@keyboard.inf;%kbdclass.SvcDesc%;Keyboard Class Driver,\SystemRoot\System32\drivers\kbdclass.sys,Kernel driver,Manual,,@%SystemRoot%\System32\irmon.dll,-2001
2023-02-14 03:11:05Z,kdnic,@kdnic.inf;%KdNic.Service.DispName%;Microsoft Kernel Debug Network Miniport (NDIS 6.20),\SystemRoot\System32\drivers\kdnic.sys,Kernel driver,Manual,,@%SystemRoot%\System32\irmon.dll,-2001
2023-02-14 03:11:05Z,mouclass,@msmouse.inf;%mouclass.SvcDesc%;Mouse Class Driver,\SystemRoot\System32\drivers\mouclass.sys,Kernel driver,Manual,,@%systemroot%\system32\drivers\mmcss.sys,-101
```



- Time installation of atomic service.

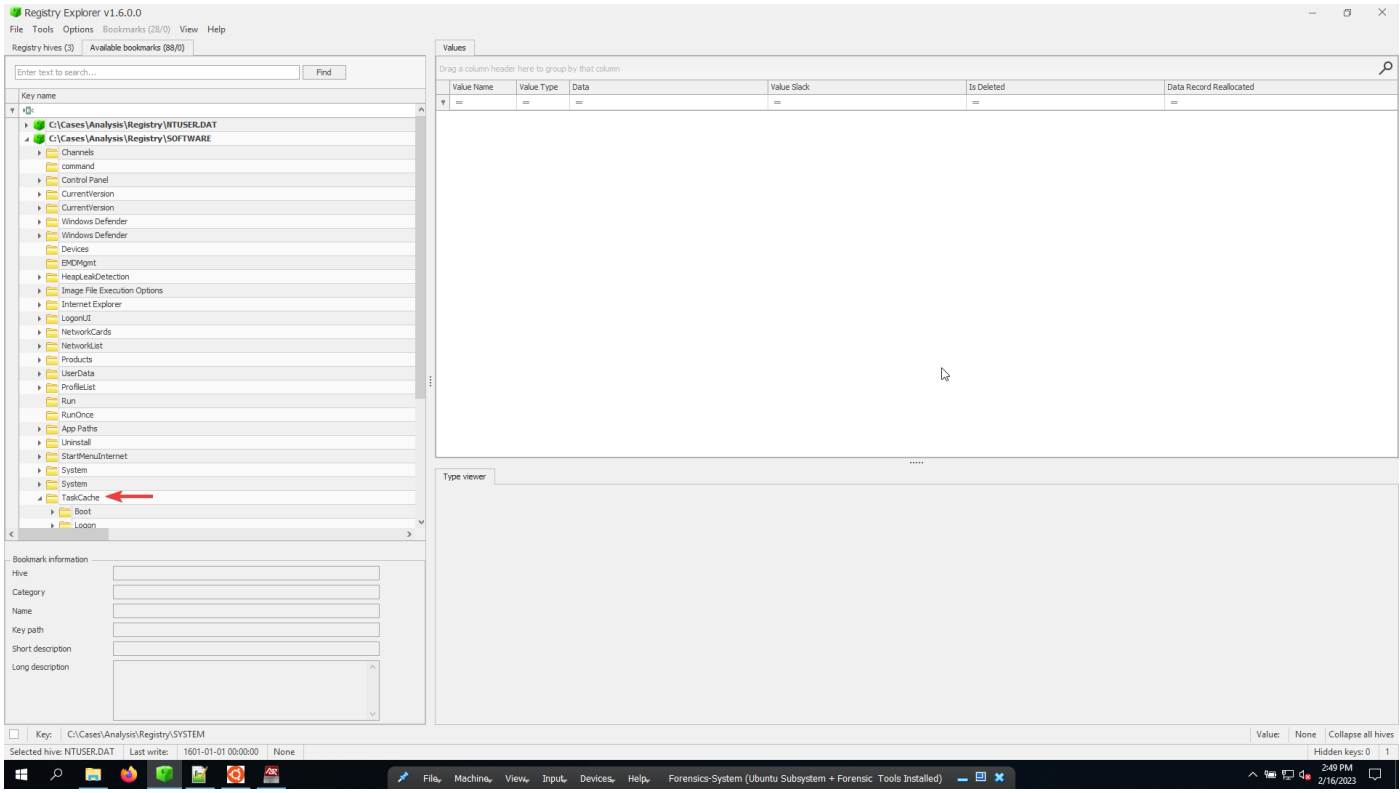
  2023-02-13 17:28:30Z

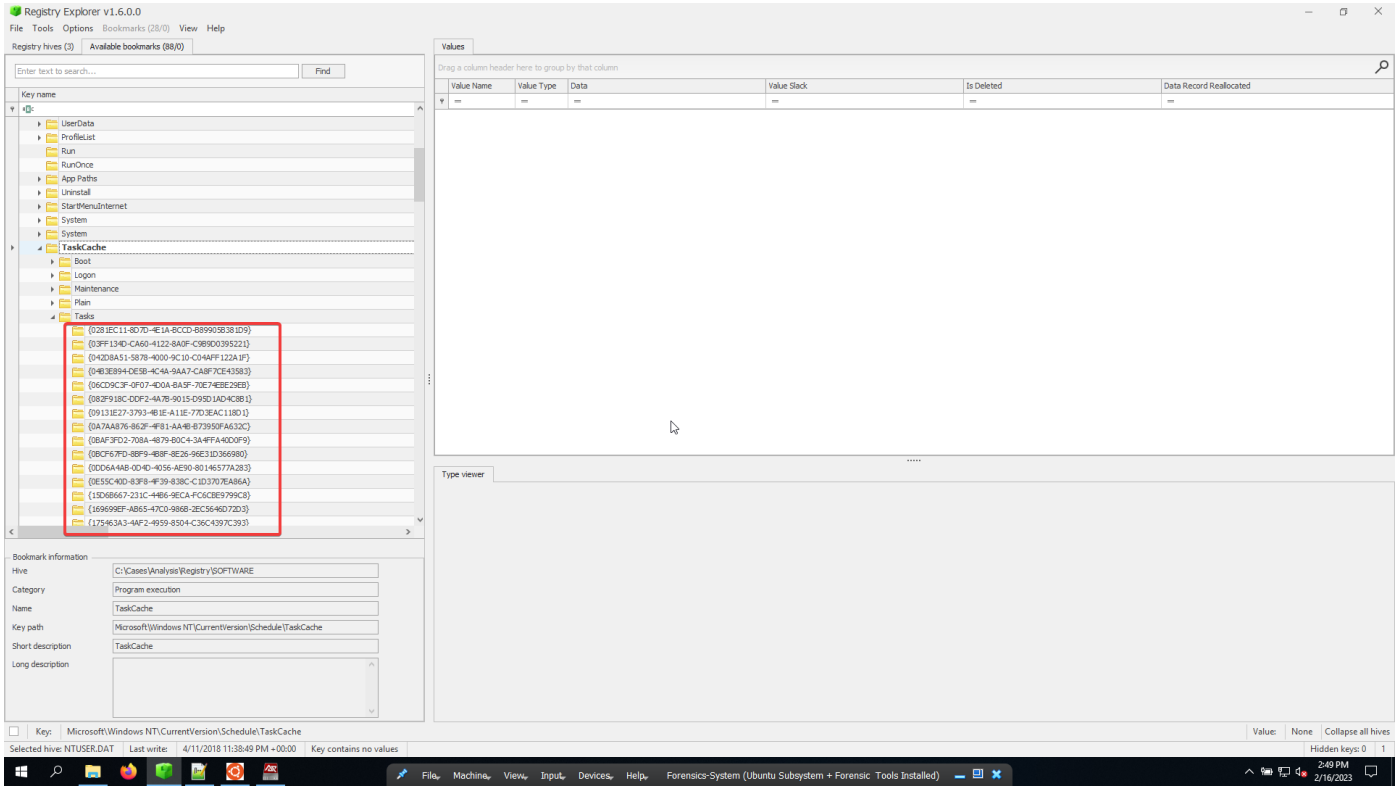
Scheduled tasks

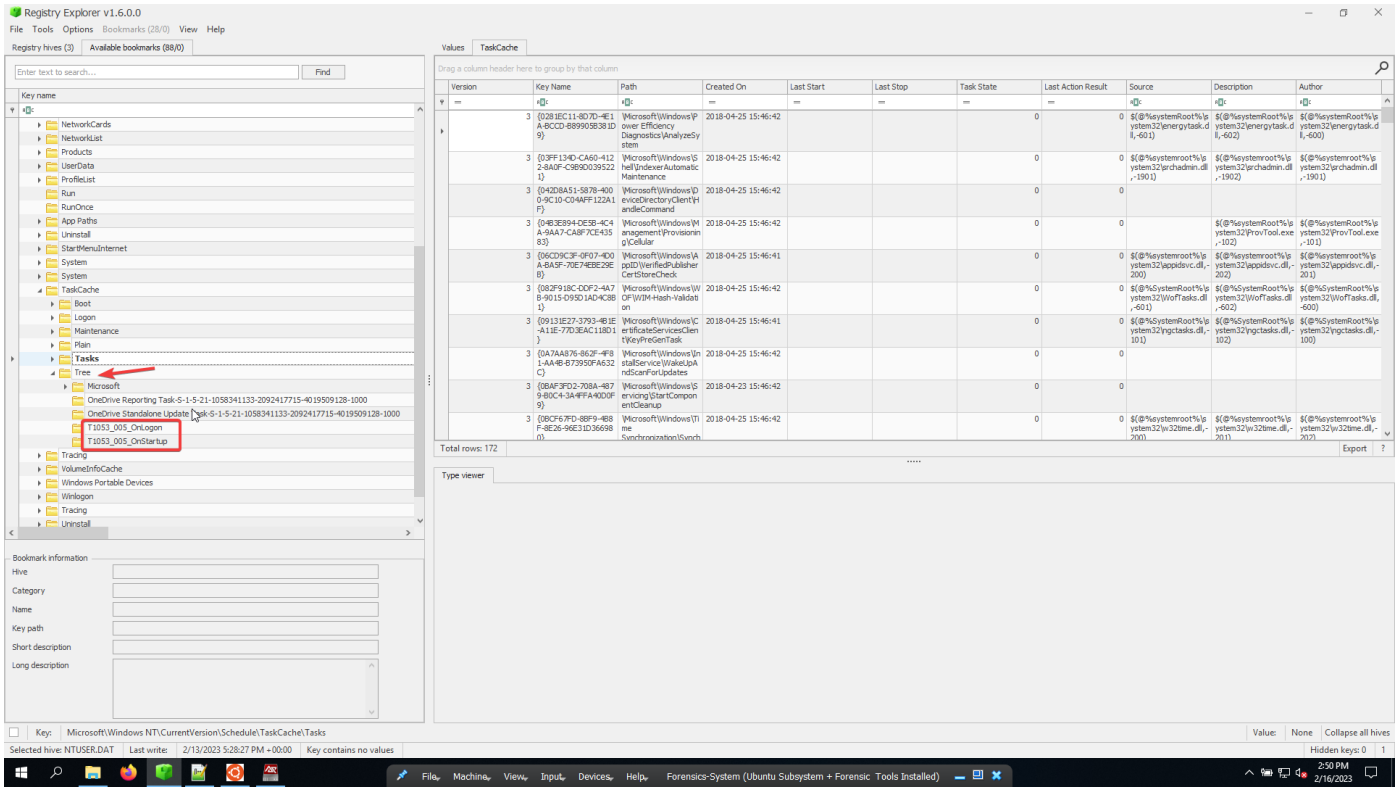
- Locations:
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree
  - C:\Windows\System32\Tasks

- Tasks can execute applications at any time based on specific triggers.

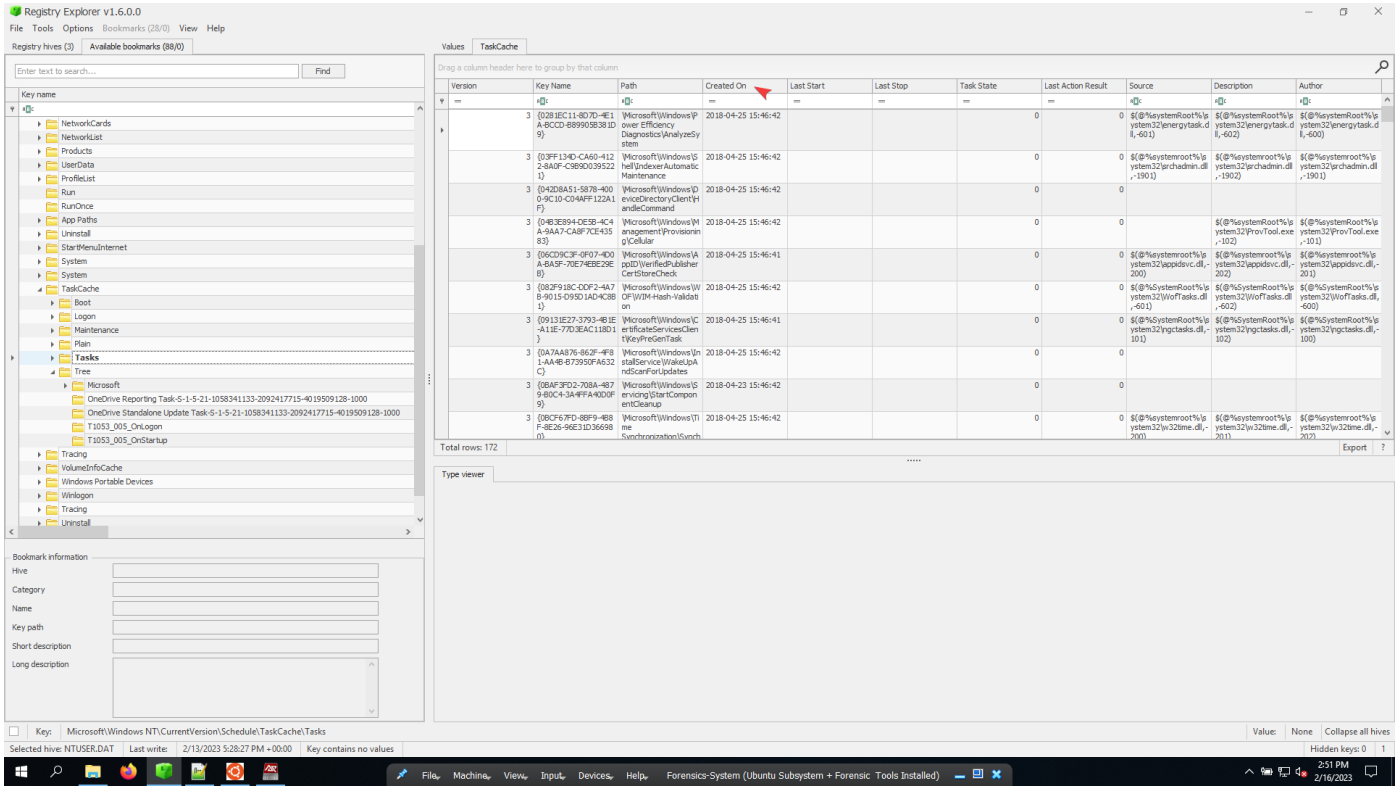
- Search for tasks subkey in registry explorer:



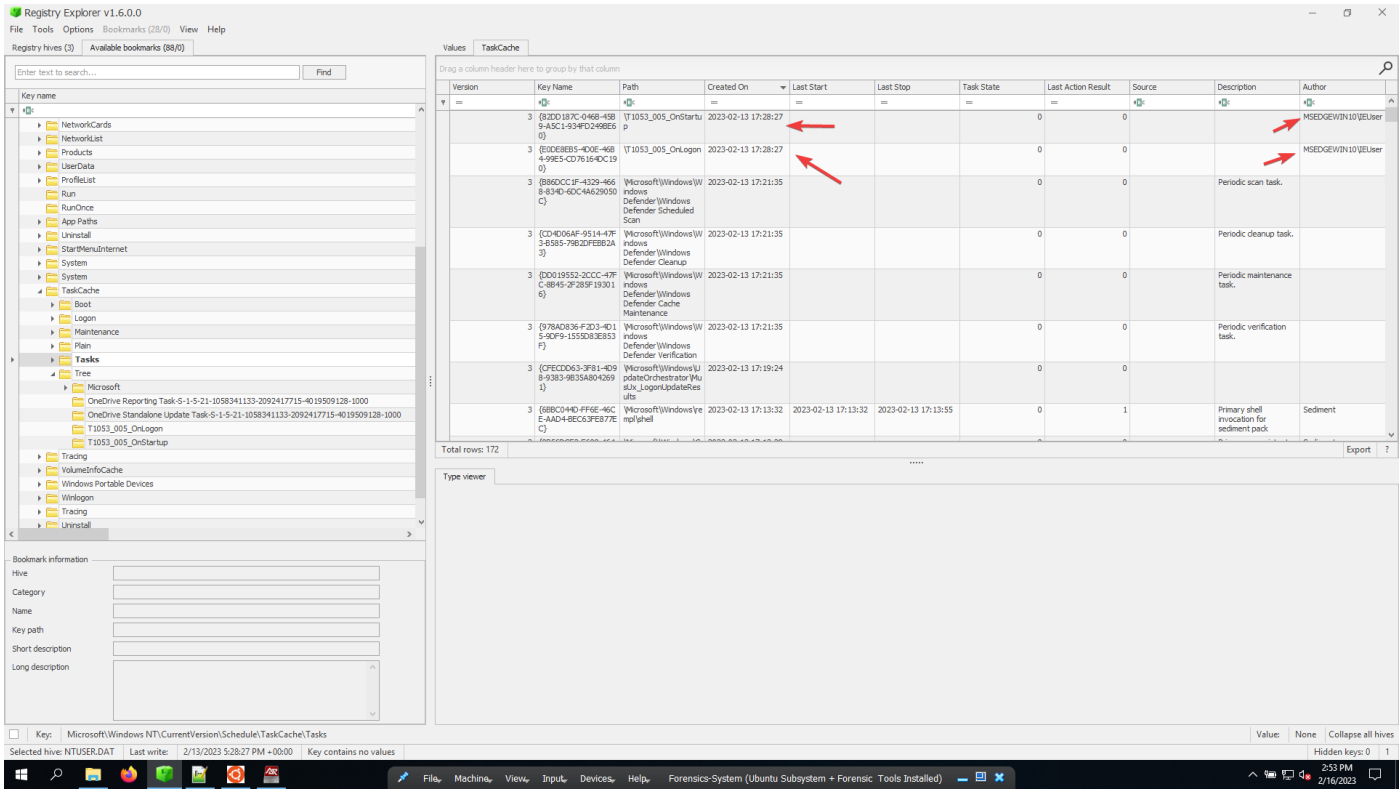




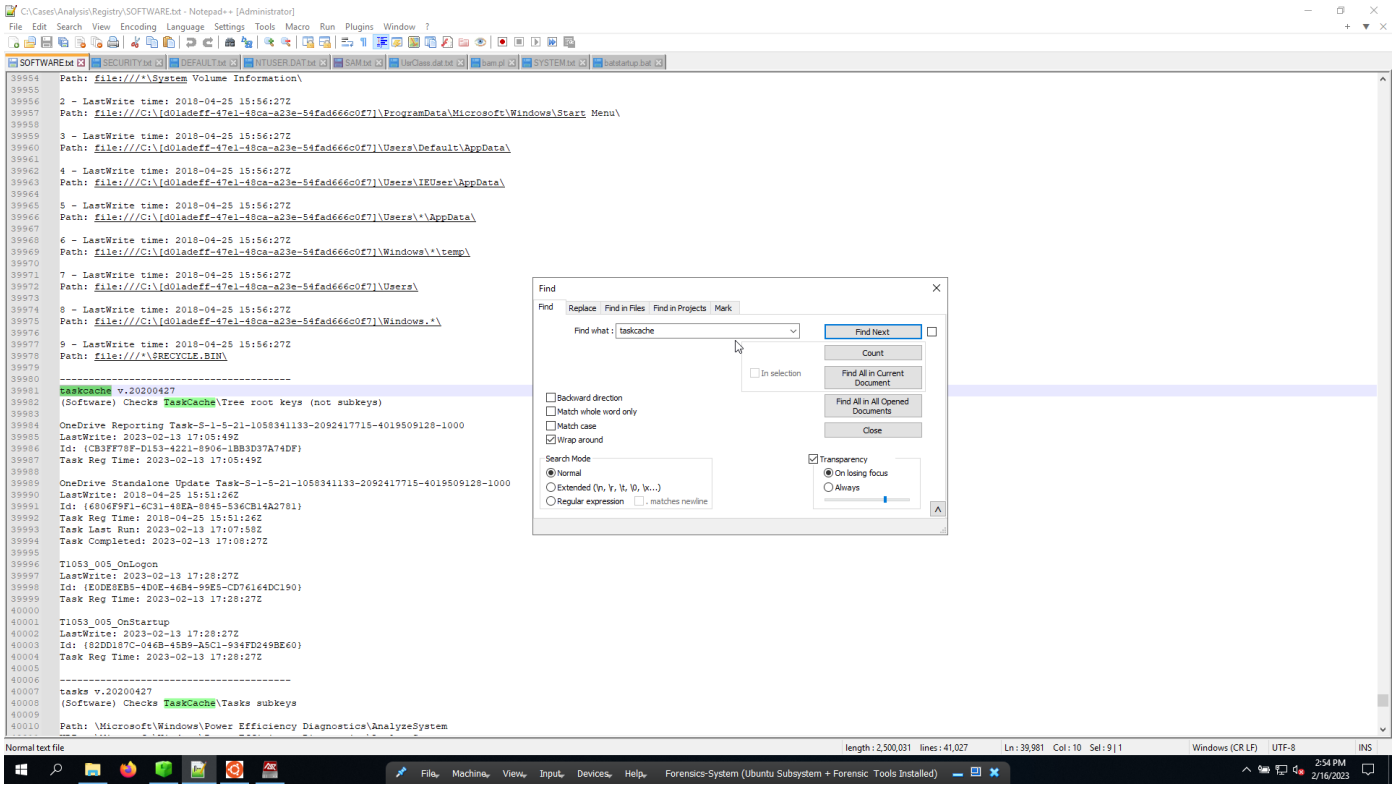
- Sort based on created on:



- Created date and author:



- Using regripper output for the same problem:



- What tasks did IEUser created, and what is the creation time.

T1053_005_OnLogon

LastWrite: 2023-02-13 17:28:27Z

Id: {E0DE8EB5-4D0E-46B4-99E5-CD76164DC190}

Task Reg Time: 2023-02-13 17:28:27Z

T1053_005_OnStartup

LastWrite: 2023-02-13 17:28:27Z

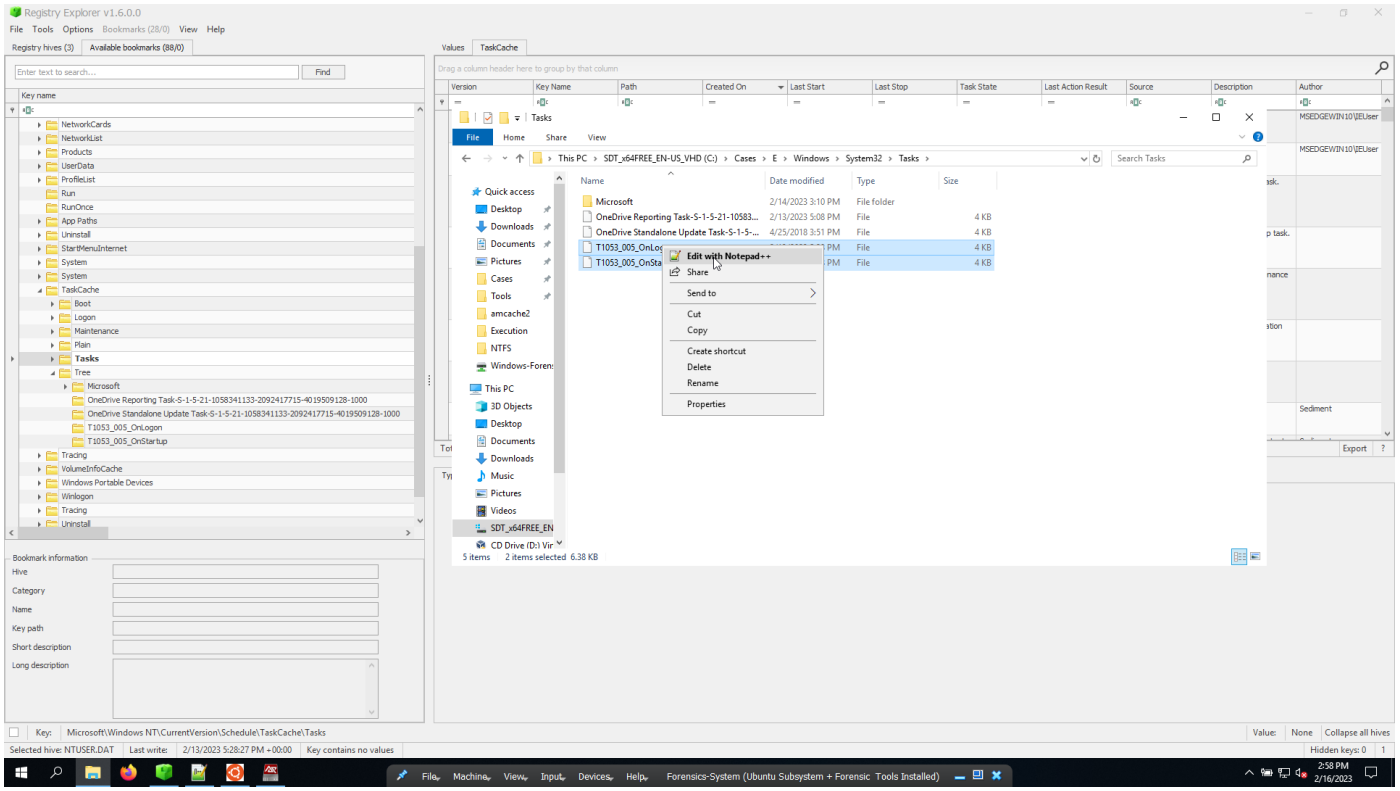
Id: {82DD187C-046B-45B9-A5C1-934FD249BE60}

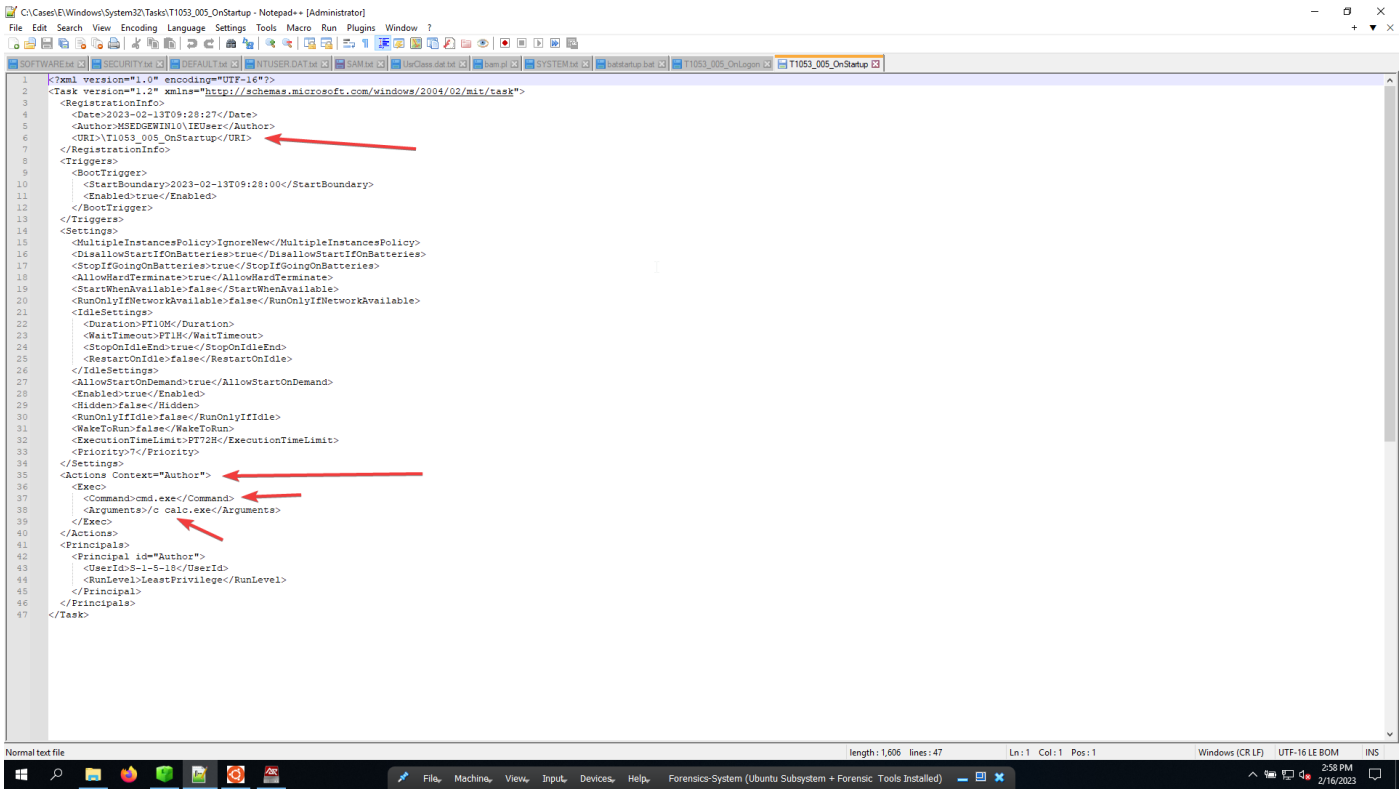
Task Reg Time: 2023-02-13 17:28:27Z

- How many times did they execute.
  - The tasks didn't had time to execute, because the lack of booting, or rebooting the system.

3	{82DD187C-046B-45B9-A5C1-934FD249BE60}	\T1053_005_OnStartup	2023-02-13 17:28:27			0	0			MSEDGEWIN10\IEUser
3	{E0DE8EB5-4D0E-46B4-99E5-CD76164DC190}	\T1053_005_OnLogon	2023-02-13 17:28:27			0	0			MSEDGEWIN10\IEUser

- YYou can see the information about tasks by opening them and view the xml code related to it .

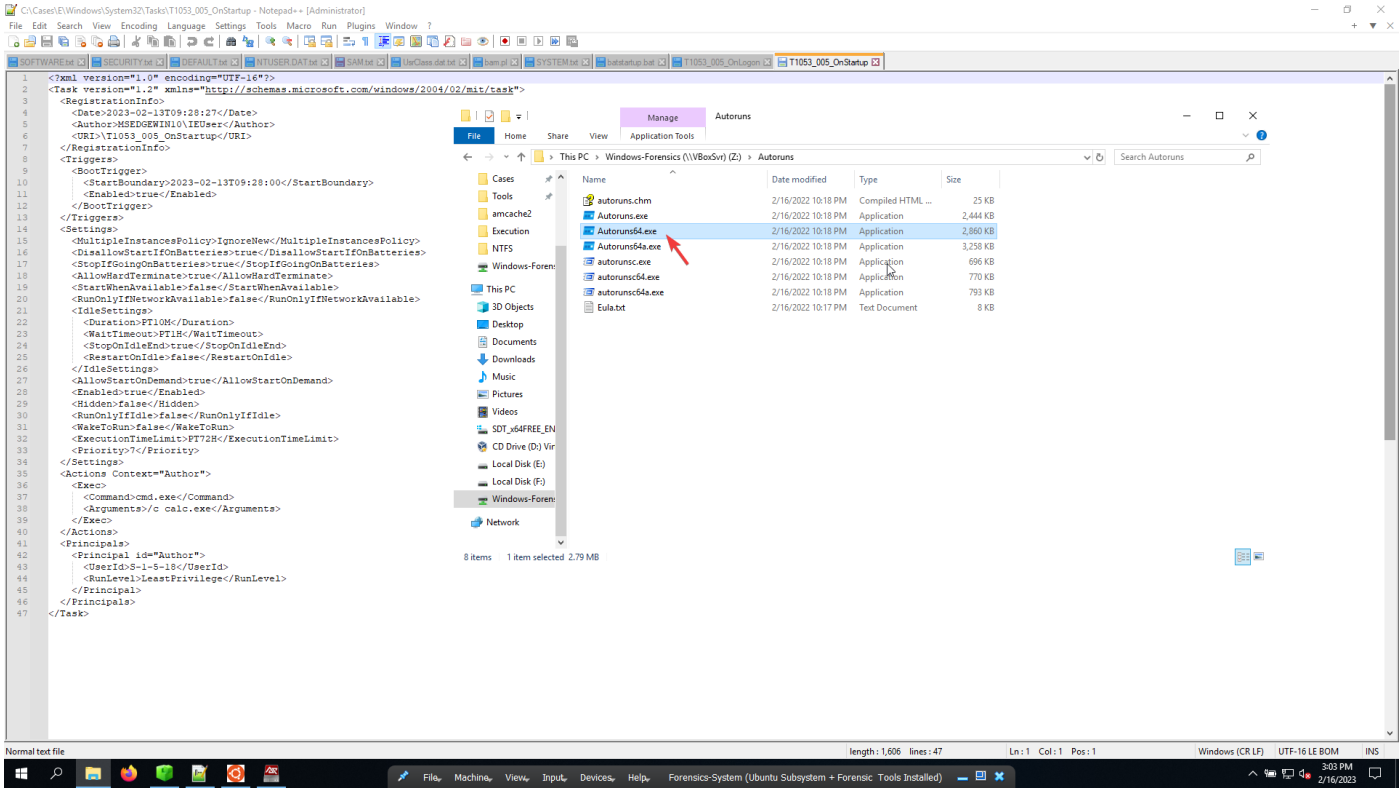




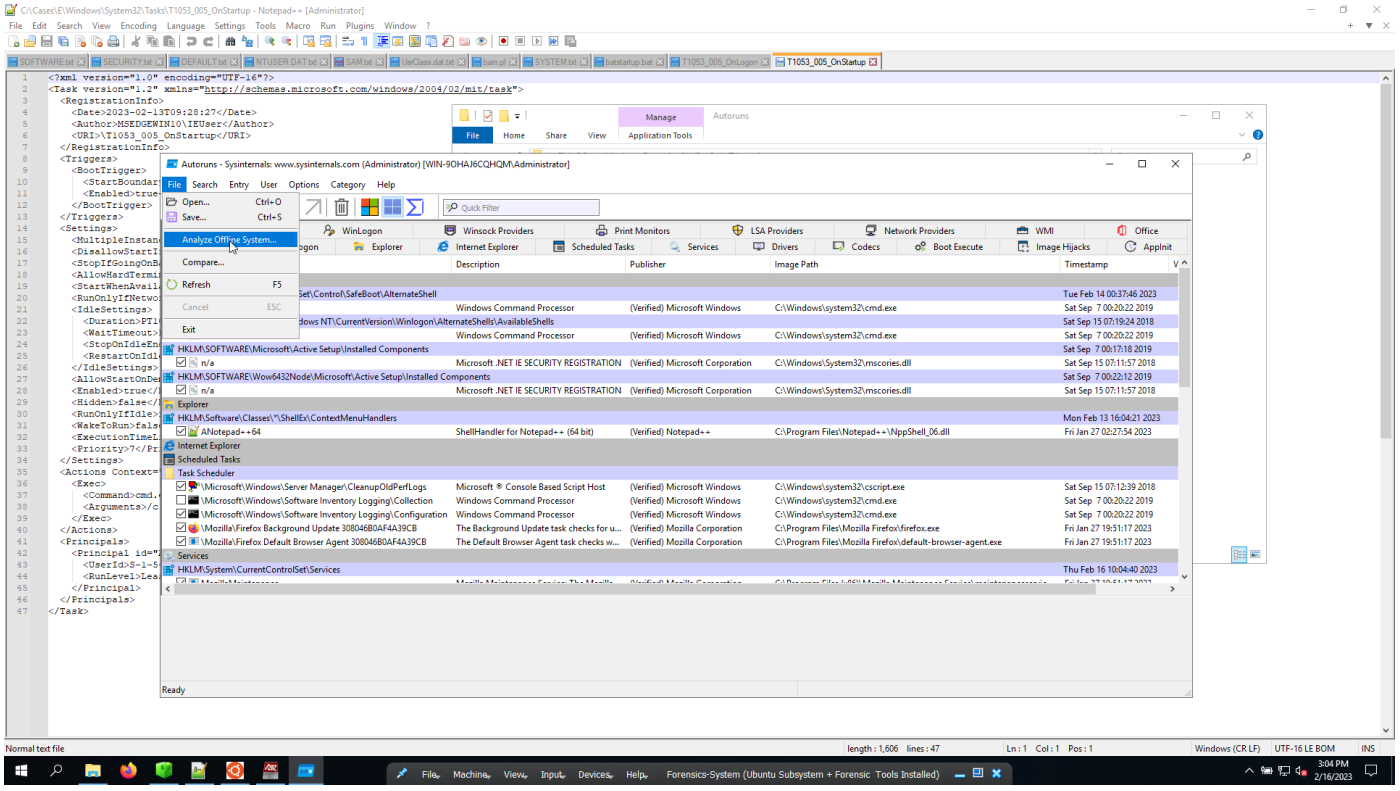
Sysinternals autoruns

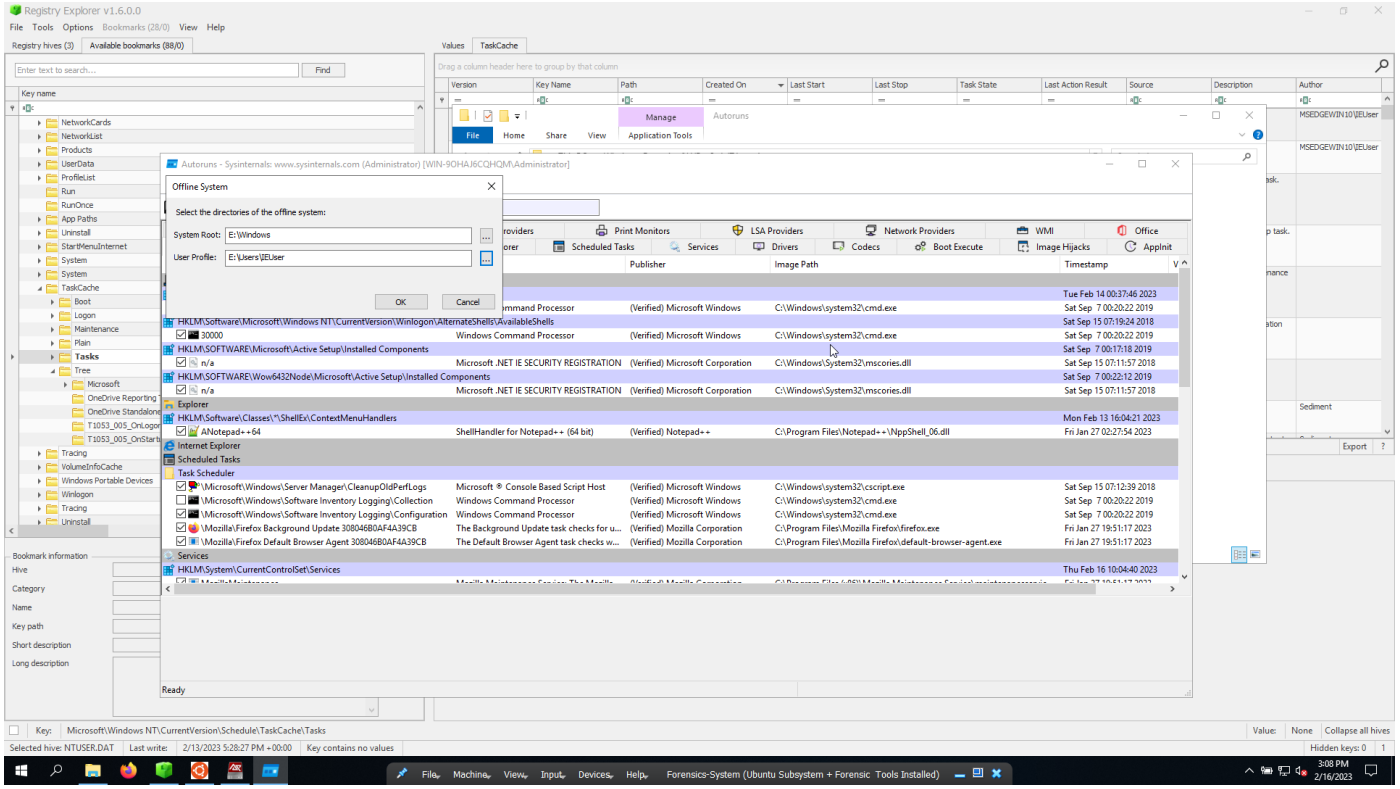
- Easier information gathering with Sysinternals Autoruns.

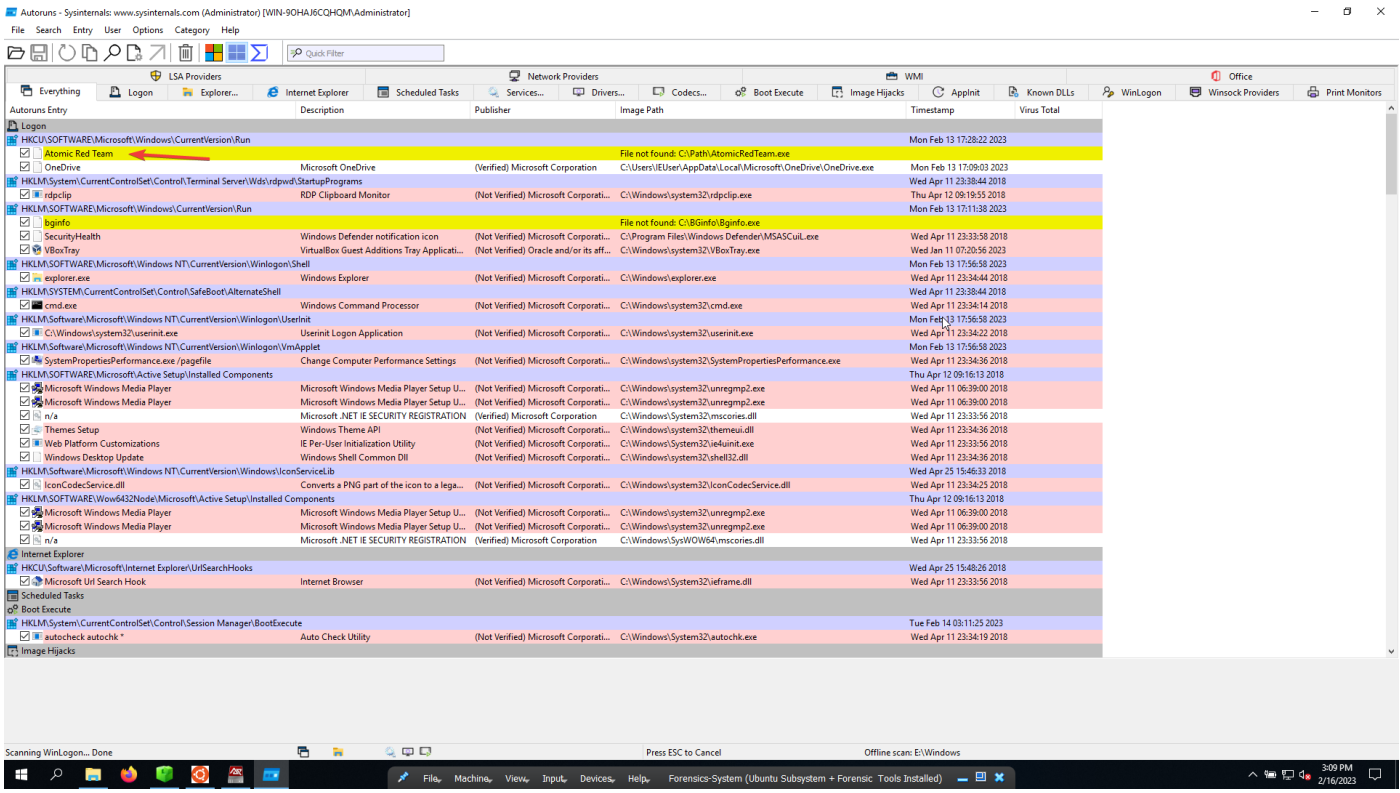
- Sysinternals Autoruns: https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns

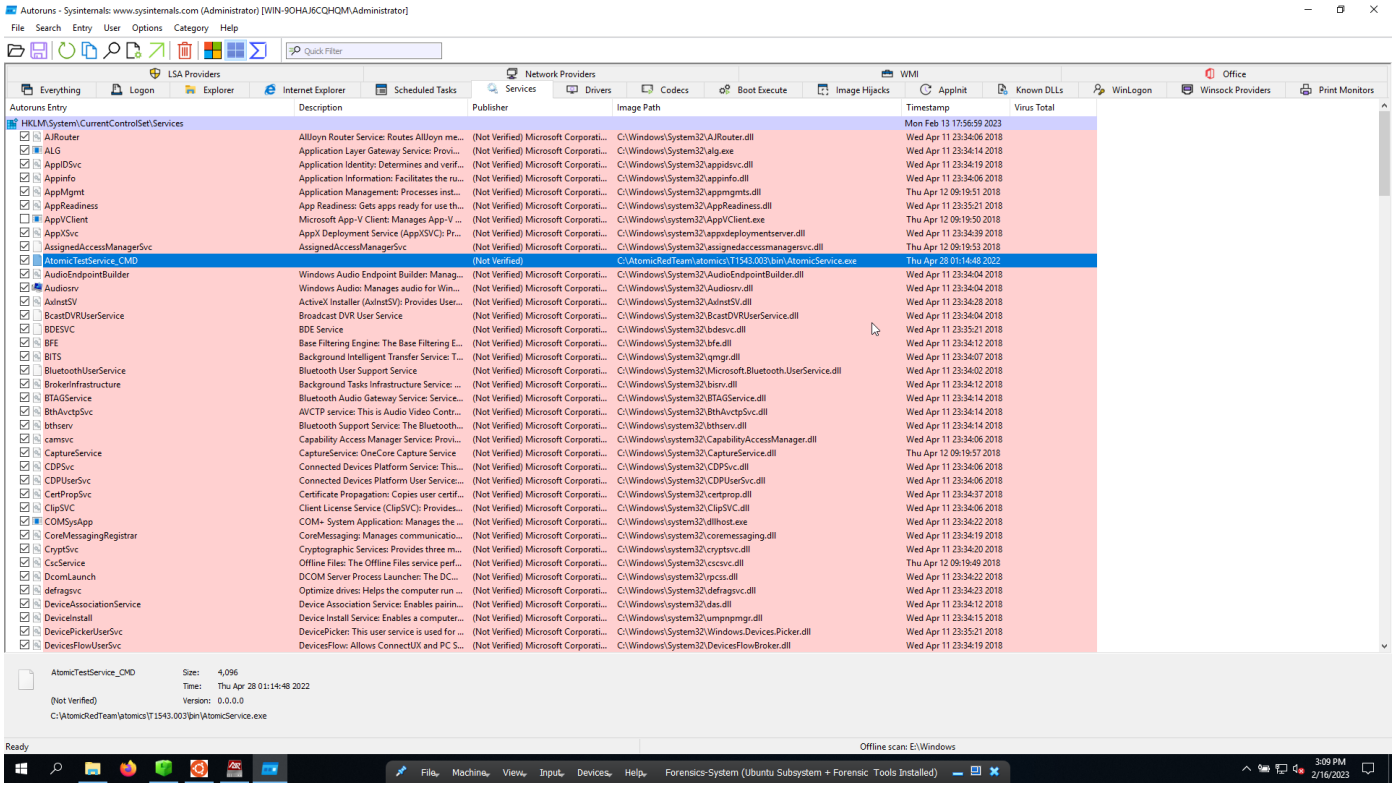


- Mount the image again and run the application as Administrator.




Registry Explorer v1.6.0.0
Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-9OHAJ6CQHQM\Administrator]
Offline System
Select the directories of the offline system:
System Root: E:\Windows
User Profile: E:\Users\IEUser
OK
Cancel
Ready


Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-9OHAJ6CQHQM\Administrator]
Atomic Red Team
File not found: C:\Path\AtomicRedTeam.exe
bginfo
File not found: C:\BGinfo\Bginfo.exe
Scanning WinLogon... Done
Press ESC to Cancel
Offline scan: E:\Windows


Autoruns - Sysinternals: www.sysinternals.com (Administrator) [WIN-9OHAJ6CQHQM\Administrator]
File Search Entry User Options Category Help
Quick Filter
LSA Providers
Network Providers
WMI
Office
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks
Services
Drivers
Codecs
Boot Execute
Image Hijacks
AppInit
Known DLLs
WinLogon
Winsock Providers
Print Monitors
Autoruns Entry
Description
Publisher
Image Path
Timestamp
Virus Total
HKLM\System\CurrentControlSet\Services
Mon Feb 13 17:56:59 2023
AJRouter
AllJoyn Router Service: Routes AllJoyn me...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\AJRouter.dll
Wed Apr 11 23:34:06 2018
ALG
Application Layer Gateway Service: Provi...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\alg.exe
Wed Apr 11 23:34:14 2018
AppIDSvc
Application Identity: Determines and verif...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\appidsvc.dll
Wed Apr 11 23:34:19 2018
Appinfo
Application Information: Facilitates the ru...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\appinfo.dll
Wed Apr 11 23:34:06 2018
AppMgmt
Application Management: Processes inst...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\appmgmts.dll
Thu Apr 12 09:19:51 2018
AppReadiness
App Readiness: Gets apps ready for use th...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\AppReadiness.dll
Wed Apr 11 23:35:21 2018
AppVClient
Microsoft App-V Client: Manages App-V ...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\AppVClient.exe
Thu Apr 12 09:19:50 2018
AppXSvc
AppX Deployment Service (AppXSVC): Pr...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\appxdeploymentserver.dll
Wed Apr 11 23:34:39 2018
AssignedAccessManagerSvc
AssignedAccessManagerSvc
(Not Verified) Microsoft Corporati...
C:\Windows\System32\assignedaccessmanagersvc.dll
Thu Apr 12 09:19:53 2018
AtomicTestService_CMD
(Not Verified)
C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
Thu Apr 28 01:14:48 2022
AudioEndpointBuilder
Windows Audio Endpoint Builder: Manag...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\AudioEndpointBuilder.dll
Wed Apr 11 23:34:04 2018
Audiosrv
Windows Audio: Manages audio for Win...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\Audiosrv.dll
Wed Apr 11 23:34:04 2018
AxInstSV
ActiveX Installer (AxInstSV): Provides User...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\AxInstSV.dll
Wed Apr 11 23:34:28 2018
BcastDVRUserService
Broadcast DVR User Service
(Not Verified) Microsoft Corporati...
C:\Windows\System32\BcastDVRUserService.dll
Wed Apr 11 23:34:04 2018
BDESVC
BDE Service
(Not Verified) Microsoft Corporati...
C:\Windows\System32\bdesvc.dll
Wed Apr 11 23:35:21 2018
BFE
Base Filtering Engine: The Base Filtering E...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\bfe.dll
Wed Apr 11 23:34:12 2018
BITS
Background Intelligent Transfer Service: T...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\qmgr.dll
Wed Apr 11 23:34:07 2018
BluetoothUserService
Bluetooth User Support Service
(Not Verified) Microsoft Corporati...
C:\Windows\System32\Microsoft.Bluetooth.UserService.dll
Wed Apr 11 23:34:02 2018
BrokerInfrastructure
Background Tasks Infrastructure Service: ...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\bisrv.dll
Wed Apr 11 23:34:12 2018
BTAGService
Bluetooth Audio Gateway Service: Service...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\BTAGService.dll
Wed Apr 11 23:34:14 2018
BthAvctpSvc
AVCTP service: This is Audio Video Contr...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\BthAvctpSvc.dll
Wed Apr 11 23:34:14 2018
bthserv
Bluetooth Support Service: The Bluetooth...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\bthserv.dll
Wed Apr 11 23:34:14 2018
camsvc
Capability Access Manager Service: Provi...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\CapabilityAccessManager.dll
Wed Apr 11 23:34:06 2018
CaptureService
CaptureService: OneCore Capture Service
(Not Verified) Microsoft Corporati...
C:\Windows\System32\CaptureService.dll
Thu Apr 12 09:19:57 2018
CDPSvc
Connected Devices Platform Service: This...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\CDPSvc.dll
Wed Apr 11 23:34:06 2018
CDPUserSvc
Connected Devices Platform User Service:...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\CDPUserSvc.dll
Wed Apr 11 23:34:06 2018
CertPropSvc
Certificate Propagation: Copies user certif...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\certprop.dll
Wed Apr 11 23:34:37 2018
ClipSVC
Client License Service (ClipSVC): Provides...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\ClipSVC.dll
Wed Apr 11 23:34:06 2018
COMSysApp
COM+ System Application: Manages the ...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\dllhost.exe
Wed Apr 11 23:34:22 2018
CoreMessagingRegistrar
CoreMessaging: Manages communicatio...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\coremessaging.dll
Wed Apr 11 23:34:19 2018
CryptSvc
Cryptographic Services: Provides three m...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\cryptsvc.dll
Wed Apr 11 23:34:20 2018
CscService
Offline Files: The Offline Files service perf...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\cscsvc.dll
Thu Apr 12 09:19:49 2018
DcomLaunch
DCOM Server Process Launcher: The DC...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\rpcss.dll
Wed Apr 11 23:34:22 2018
defragsvc
Optimize drives: Helps the computer run ...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\defragsvc.dll
Wed Apr 11 23:34:23 2018
DeviceAssociationService
Device Association Service: Enables pairin...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\das.dll
Wed Apr 11 23:34:12 2018
DeviceInstall
Device Install Service: Enables a computer...
(Not Verified) Microsoft Corporati...
C:\Windows\system32\umpnpmgr.dll
Wed Apr 11 23:34:15 2018
DevicePickerUserSvc
DevicePicker: This user service is used for ...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\Windows.Devices.Picker.dll
Wed Apr 11 23:35:21 2018
DevicesFlowUserSvc
DevicesFlow: Allows ConnectUX and PC S...
(Not Verified) Microsoft Corporati...
C:\Windows\System32\DevicesFlowBroker.dll
Wed Apr 11 23:34:19 2018
AtomicTestService_CMD
Size: 4,096
Time: Thu Apr 28 01:14:48 2022
(Not Verified)
Version: 0.0.0.0
C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
Ready
Offline scan: E:\Windows
File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed)
3:09 PM
2/16/2023