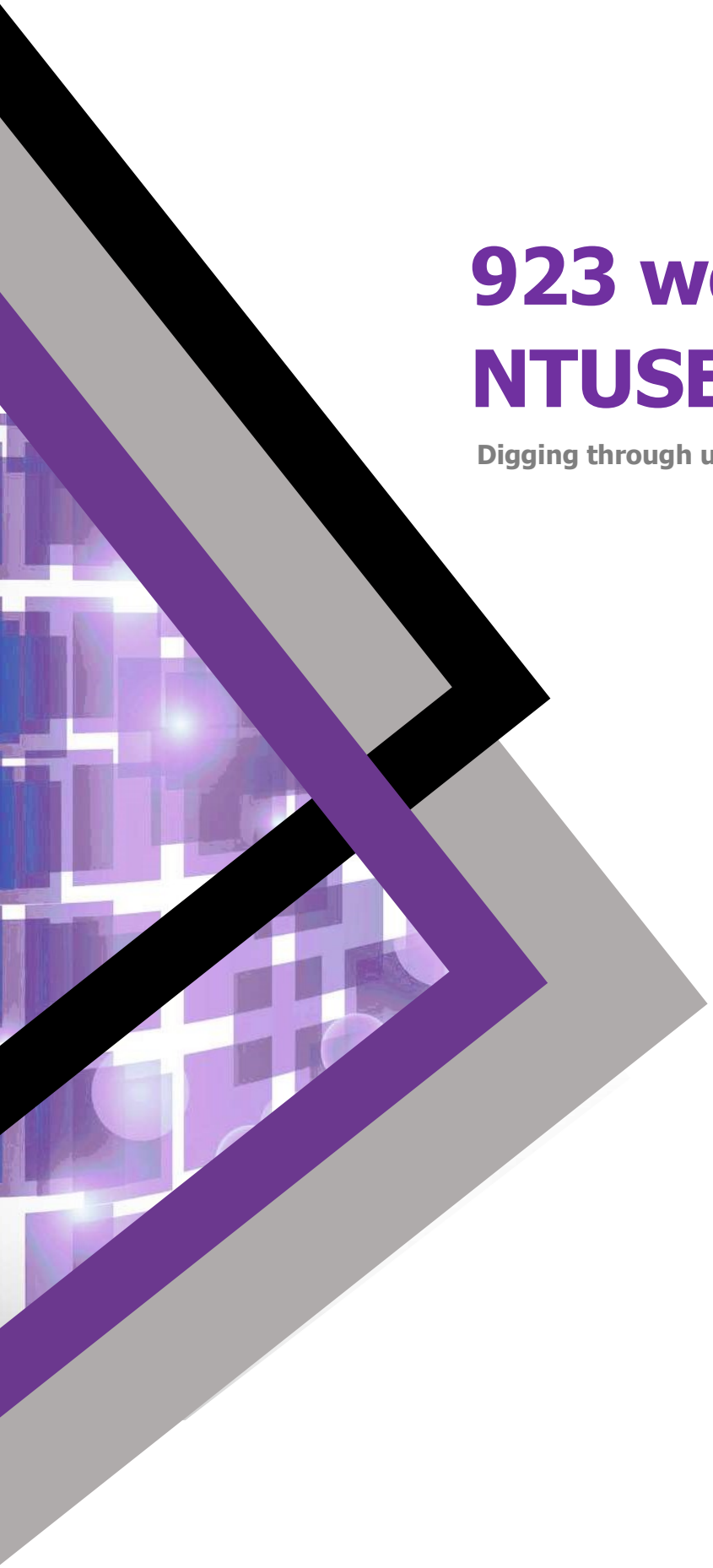
May 2020

923 words on NTUSER.DAT

Digging through user registry settings



LIFARS
your digital world, **secured**

Contents

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

ABSTRACT

In this technical guide, we will be focusing only on NTUSER.DAT and not on related registry hives or artifacts that are not located within NTUSER hive. This file which stores user profile and settings information can be useful in many use cases. We can gain evidence of program executions, torrent clients, or other unapproved applications that should not be present on the workstation. It can help us create rough timeline during forensic investigation or provide proof of tampering with file timestamps. Also, it can be very useful when searching for evidence of execution or access to specific file, or reassembling user activity. We can gain evidence of folder access/presence on the system, evidence of access or user activity. It can help us gain insight in user behavior during investigation of disgruntled employee or insider threat, finding out if user opened malicious file or accessed sensitive documents. We can find evidence of execution for files accessed on network share or removable media. It is a good place to look for persistence created by PUA, trojans or malwares running under permissions of a user.

INTRODUCTION

NTUSER.DAT file is part of Windows OS, which stores user profiles and settings. All the profile changes you make during your live user session such as accessing folders, opening files, mapping network shares, changing wallpaper, adding printer etc. gets stored in HKEY_CURRENT_USER registry hive. Windows stores all the changes during live session into a backup copy of NTUSER.DAT called NTUSER.DAT.LOG1 and 2. At logoff all the changes get saved in NTUSER.DAT file, from which the user settings get loaded during the next logon into HKEY_CURRENT_USER. With a little bit digging you can discover treasure trove of information, which can be utilized in your digital forensic investigation.

We can explore NTUSER.dat hive with tools such as: windows native regedit, registry ripper, registry viewer, Registry Explorer (By Eric Zimmerman). And further explore registries with another set of tools such as cafae.

In this article we will be using Registry explorer. We chose this tool because it has excellent documentation, versatility (GUI, plugins, CMD) and it is overall pleasure to work with, compared with some other alternatives. Most of the entries we will go through are easily accessible through bookmark tab in registry explorer. If you know what you are searching for you can use this feature to speed up your investigation.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

DIGITAL FORENSICS USING NTUSER.DAT

As with any forensics investigation, we need to have very clear idea what time zone settings were present on the machine we acquired image from and how our tools present time data to us. For example, if the image we are analyzing was acquired in New York with time zone set to UTC -4, and we are working on machine with UTC +1, then we should be mindful of time zone that gets displayed by our tools when creating time line or correlating user activity.

We will start by acquiring NTUSER.DAT from workstation so that we can explore it more deeply. For this we can use FTK lite imager and copy our files from live system. If Windows UAC stops you from running FTK on your own system, try launching it from PowerShell with administrative privileges.

Disclaimer: in case we want to acquire NTUSER.DAT file for forensic evidence or Incident response, we do not save it on local disk. If it is even remotely possible, we save all acquired data on remote disk or share, so that we won't make any changes to host system. Also, in 99.9% of cases we should not look for evidence directly on a live system that we are analyzing, instead we should work on copy of byte-per-byte image of original disk.

Acquisition of NTUSER.DAT from a live disk using EnCase: New case (add name) -> Add evidence -> Add Local Device -> "select windows partition" -> "select device" press open -> %userprofile% -> Select NTUSER.DAT and NTUSER.DAT.LOG1 and 2 -> Click on Edit Menu -> Select Copy only Selected files inside each folder -> select Export folder

Acquisition of NTUSER.DAT from a live machine using FTK Imager lite: File -> Add evidence item -> Physical drive -> \\ PHYSICAL DRIVE – "disk name and size" . When we have our disk mounted we navigate into Windows 10 system partition -> [root] -> Users -> "username" -> NTUSER.DAT* (there will be several ntuser.dat.log files, copy those as well. Windows will make copy of NTUSER.DAT when there is some change in settings or preferences and save the backup as ntuser.dat.log. When the user logs off, the changes are saved into NTUSER.DAT however, we can still find some deleted entries in NTUSER.DAT.LOG.

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

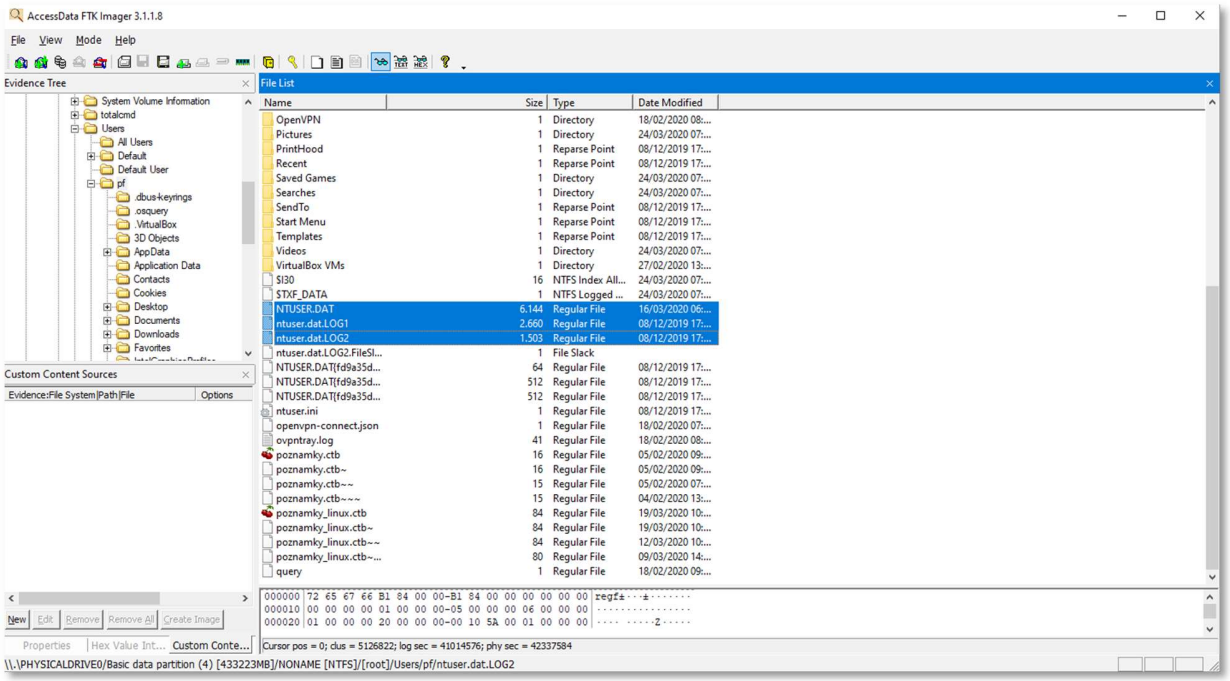


Figure 1- Exporting NTUSER.DAT from user profile.

In real world scenario we would be working on byte-per-byte image copy of original disk. The export of NTUSER.DAT would be basically the same, except we would choose "Image File" as evidence item.

We shall use Registry Explorer by Eric Zimmerman, to reconstruct the NTUSER file we acquired. We go to File -> Load Hive -> "folder with our ntuser export" -> select NTUSER.DAT -> Open (we will get warning -> click Yes) -> "add ntuser.dat.logs" -> "save clean hive" (click trough warnings).

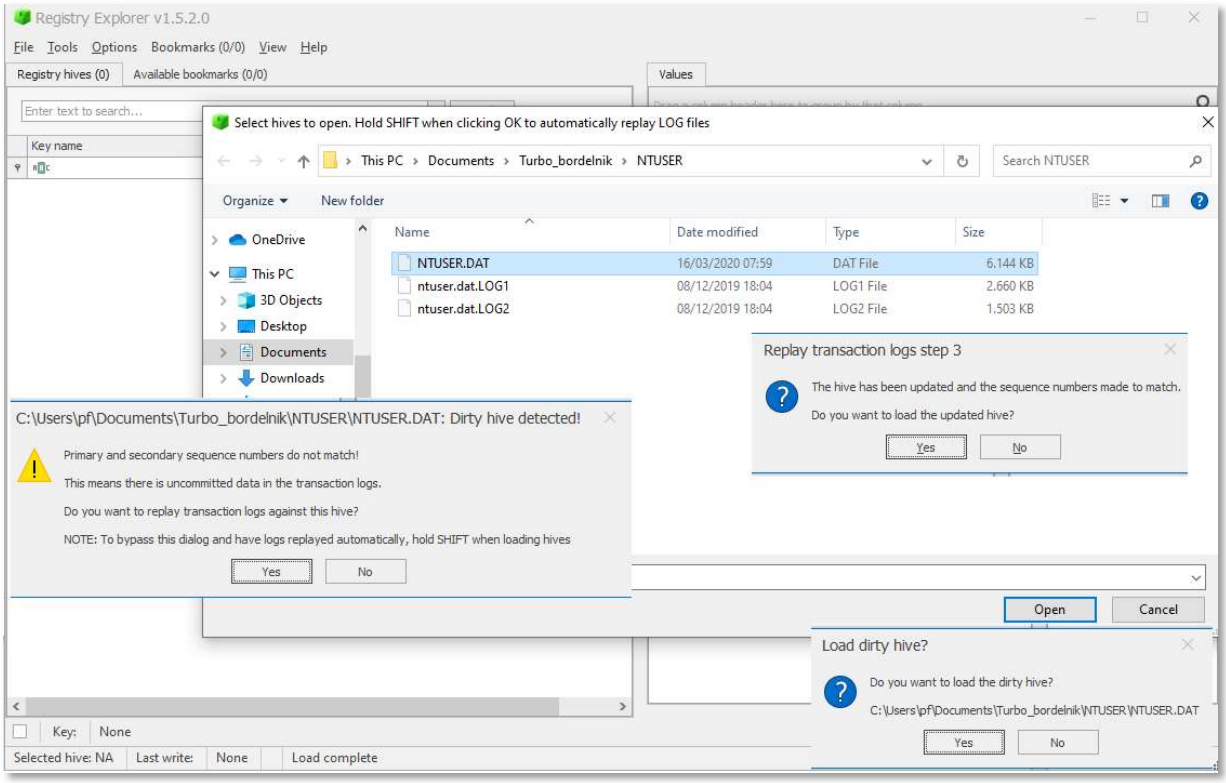


Figure 2- Reconstructing NTUSER.DAT after acquisition.

If we want to just play around and get some hands-on experience, we can use Registry Explorer to probe ntuser.dat on our live system. However, it is not advisable to make any changes, unless you know what you are doing. In order to look at live

NTUSER.DAT file, we need to run Registry Explorer with administrative privileges and select user we want to explore.

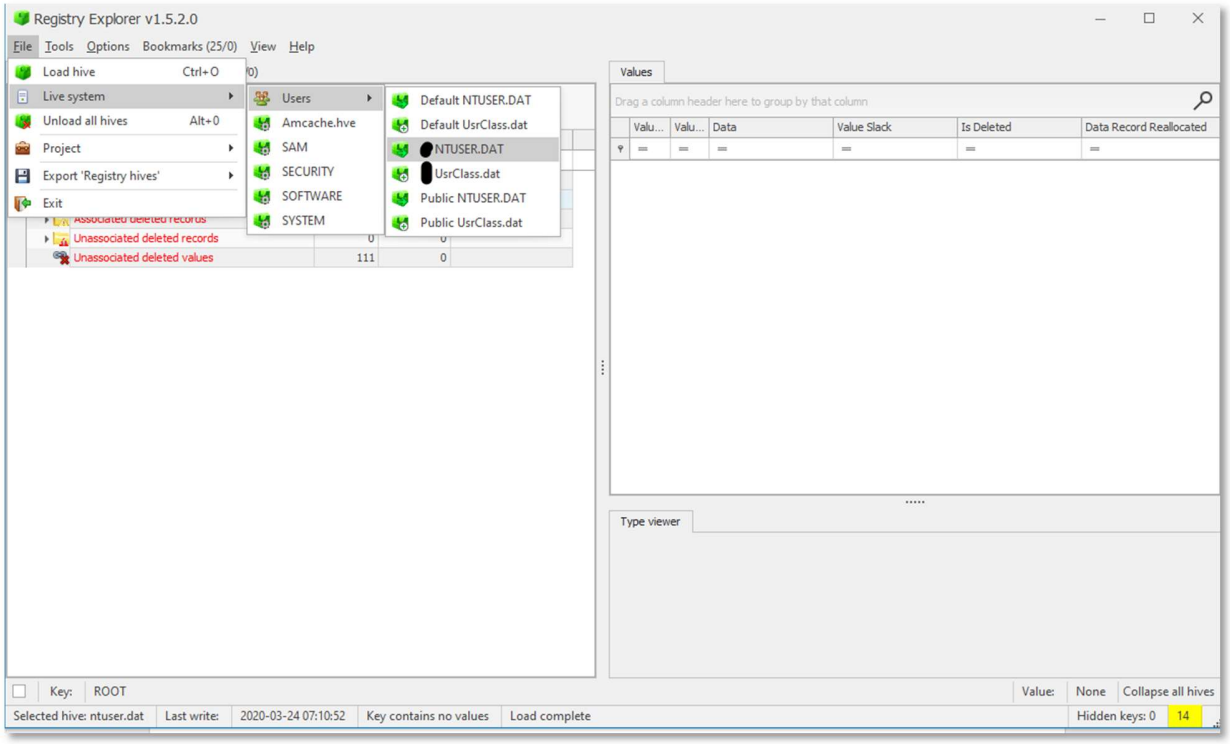


Figure 3- Opening NTUSER.DAT on live system with Registry Explorer.

We shall take a look on keys that are useful during an investigation or just plain interesting. NTUSER hive hides information such as most recently accessed files, folders, documents, network shares, URLs and much more. So, let us start with looking at recently accessed items.

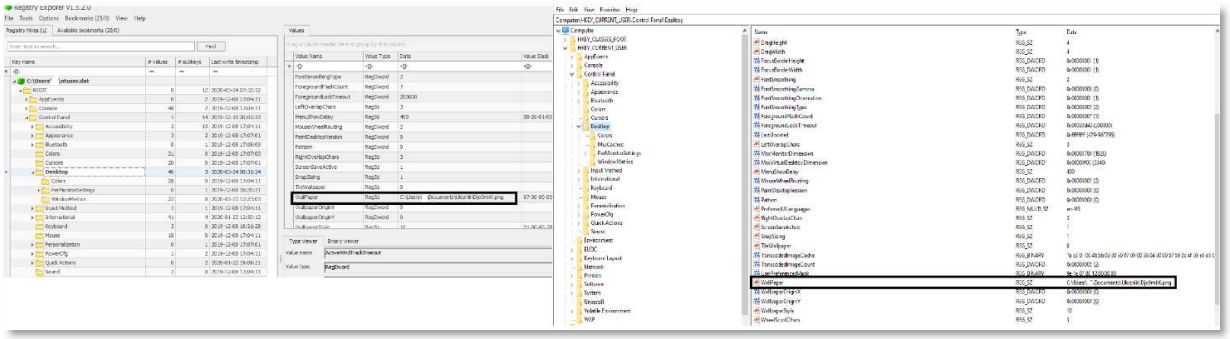


Figure 4 - Here we can see NTUSER.DAT stores settings in HKEY_CURRENT_USER hive.

EXECUTED PROGRAMS AND APPLICATIONS: key values at ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> UserAssist -> #GUID -> **Count**

Registry Explorer will automatically translate most of the key values into readable format, however if you would look at those same keys in regedit, or with some other tool that shows you the keys in their original format, you'd notice that the values are obfuscated. Key values are ciphered with ROT13, which is just variant of Caesars cipher(skip 13 letters ahead). We can transform the key values into readable format with scripts or we can use tools such as CyberChef.

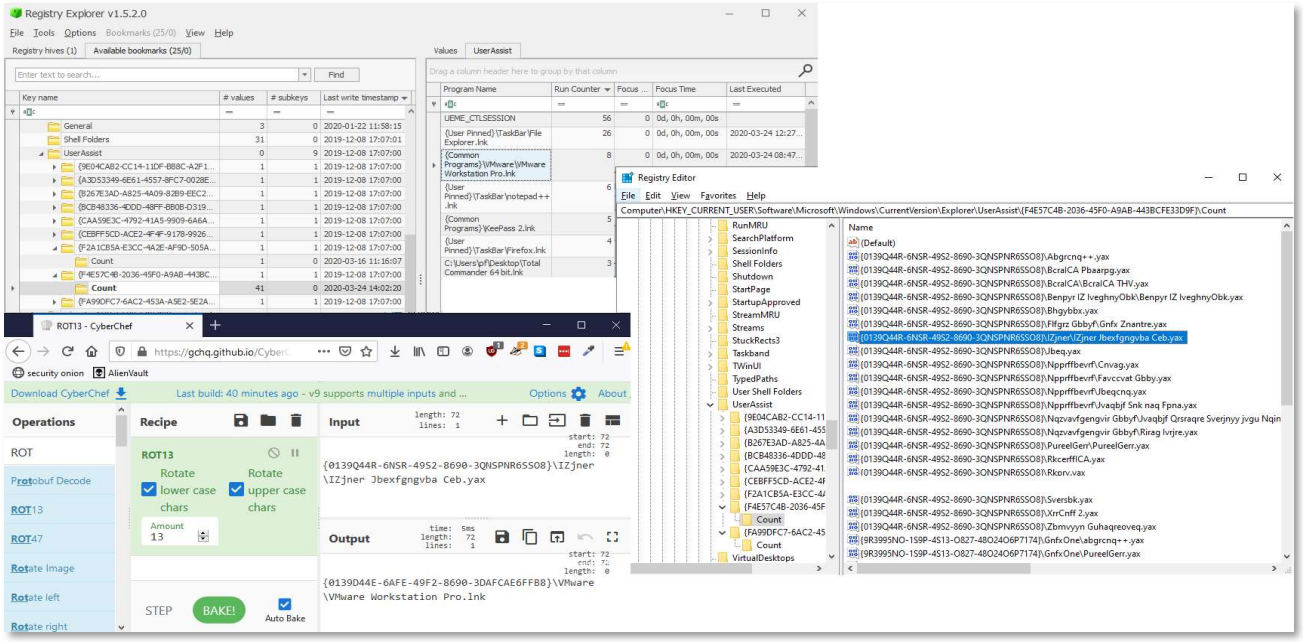


Figure 5- Here we can see how the key values are originally stored in registry and de-obfuscation of the key value.

UserAssist Count key holds the list of applications that were executed on user's system. That means, we can find applications executed by the user, file path to where the application was installed and link or shortcut to application that was executed. For example, GUID for list of shortcut links used to start programs is {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}, list with applications, files, links and other objects can be found in {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}[1]. It should be noted that it is only items that were accessed through Windows Explorer and not through command line, PowerShell or windows-linux shell. Additionally, you can find how often and when each item was run.

[1] https://www.scitepress.org/Papers/2017/64167/64167.pdf accessed on 30th March 2020

Use case: *good place to start when looking for outliner items during an investigation. Provides evidence of program execution. Ties together a GUI program that was run on the system with user account that actually ran that program.*

FILE EXTENSIONS: key values at ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> **FileExts**

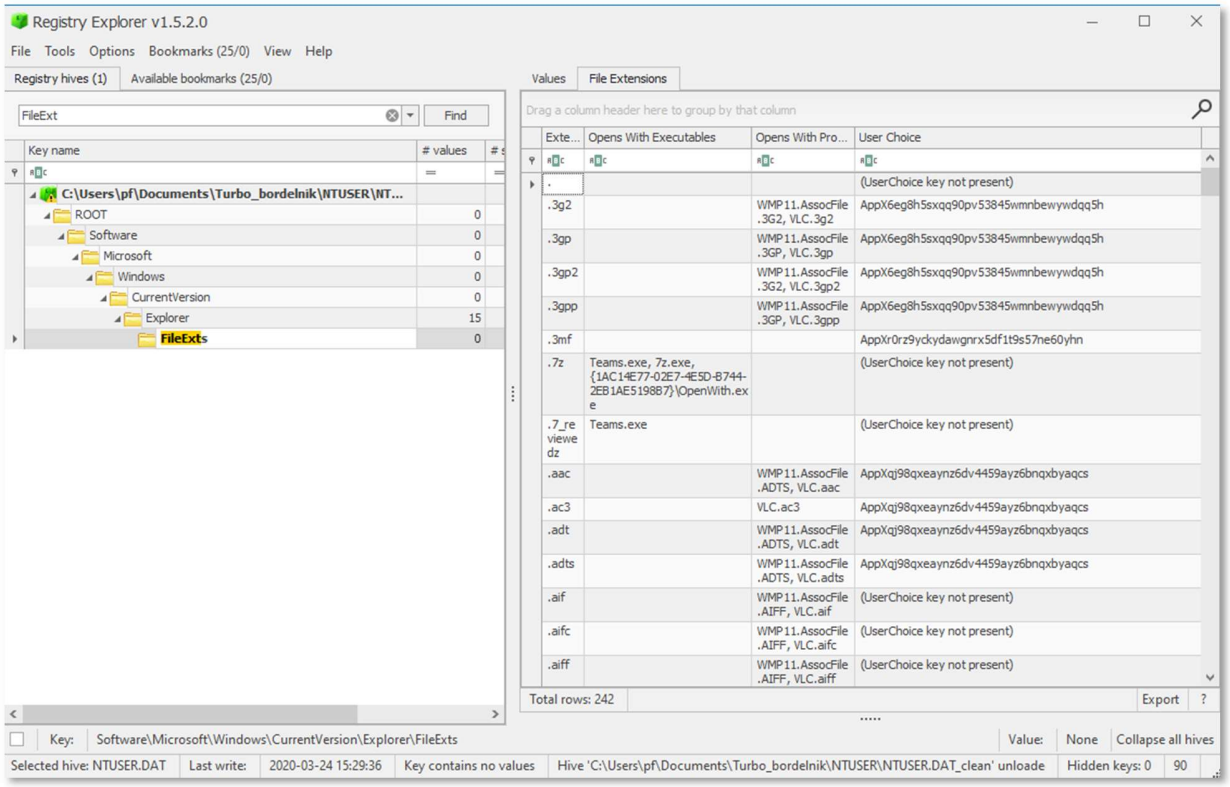


Figure 6- Table with extensions and programs they are associated with.

You can use "Opens with Executables" column to look for any programs that warrants a closer look.

Use case: *you can find torrent clients or other unapproved applications that should not be present on the workstation.*

RECENTLY OPENED DIRECTORIES, FILES, APPLICATIONS: key values are located in ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> **ComDlg23**

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

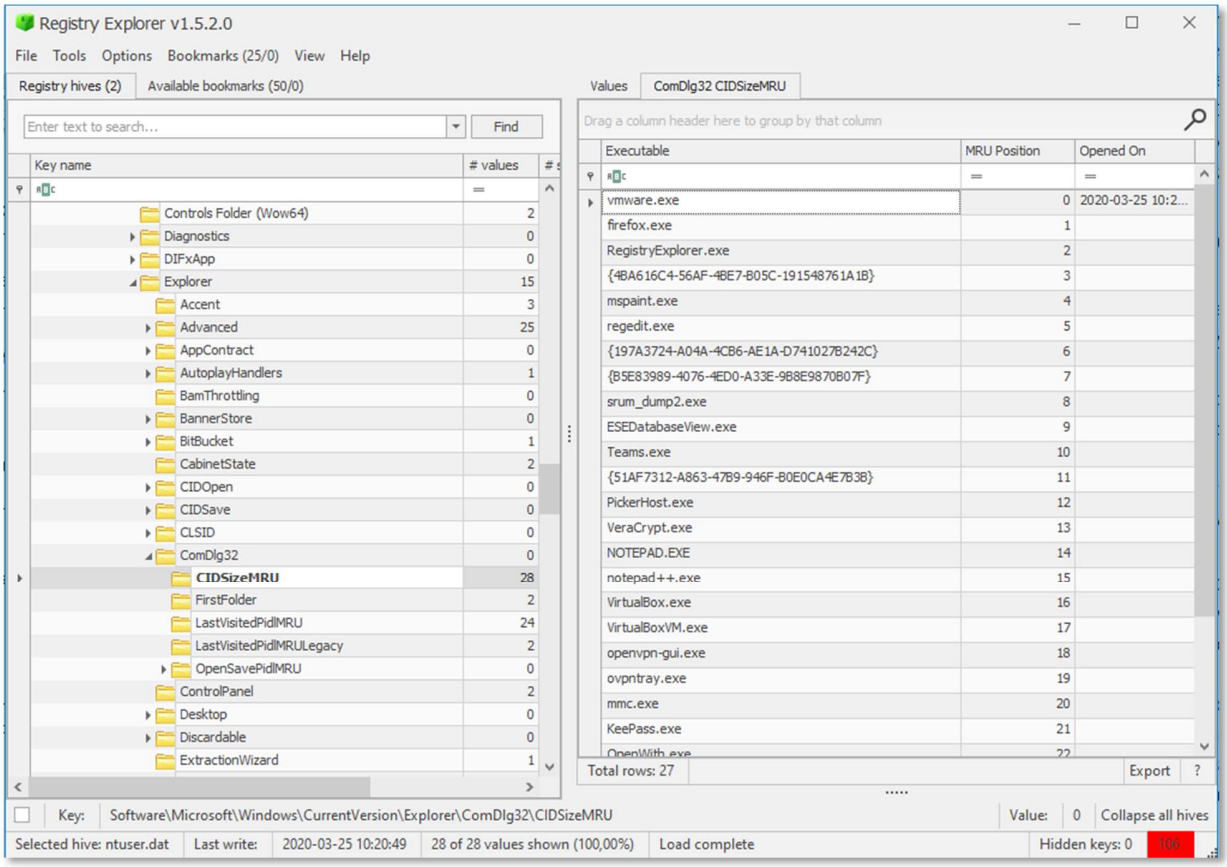


Figure 7- Table with recently launched applications.

In this registry's sub-directory we have arguably most useful entries which are:

CIDSizeMRU – recently launched applications.

LastVisitedPidMRU - tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key and points to directory location for the last file accessed by that application. [2]

LastVisitedPidMRULegacy – previously visited folders.

OpenSavePidMRU – recently opened files within Windows shell dialog box. Moreover, this also includes files opened on network shares and external hard drives.

Use case*: This key is very valuable location when searching for evidence of file access, execution, or mapping user interaction within system. "Opened on" values in OpenSavePidMRU table can help us create rough timeline during investigation or provide proof of tampering with file timestamps.*

[2] https://www.sans.org/blog/opensavemru-and-lastvisitedmru/

FILES EXECUTED WITH RUN COMMAND: key values are located in ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> **RunMRU**

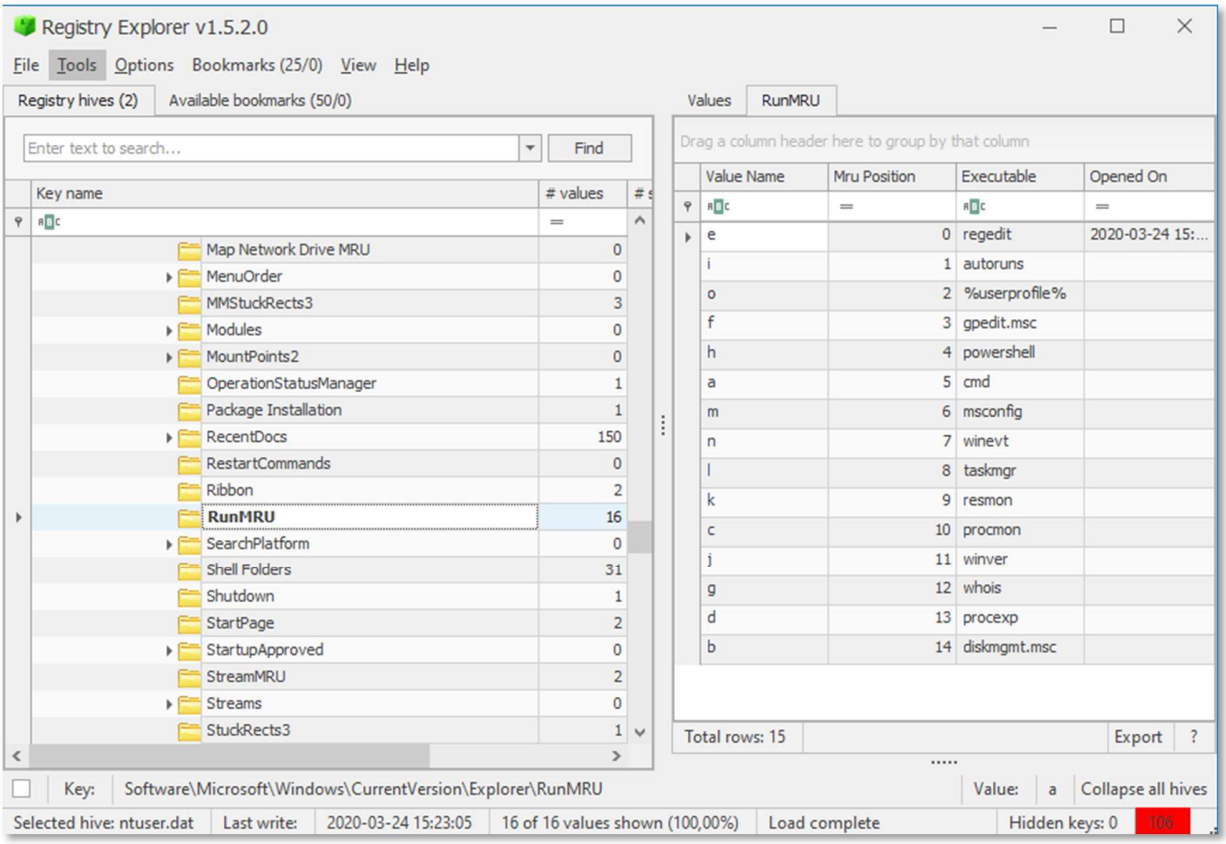


Figure 8- Table with arguments executed in Run command box.

As mentioned above, this table holds expressions ran in windows Run command box. These values are also what is shown as history in Run box, if you delete those entries, you will remove the history for Run application. Malicious actor can try to remove the evidence of command executions and delete those entries. If you have registry

auditing turned on you can search for Windows security event log # 4657 to see evidence of registry tampering.

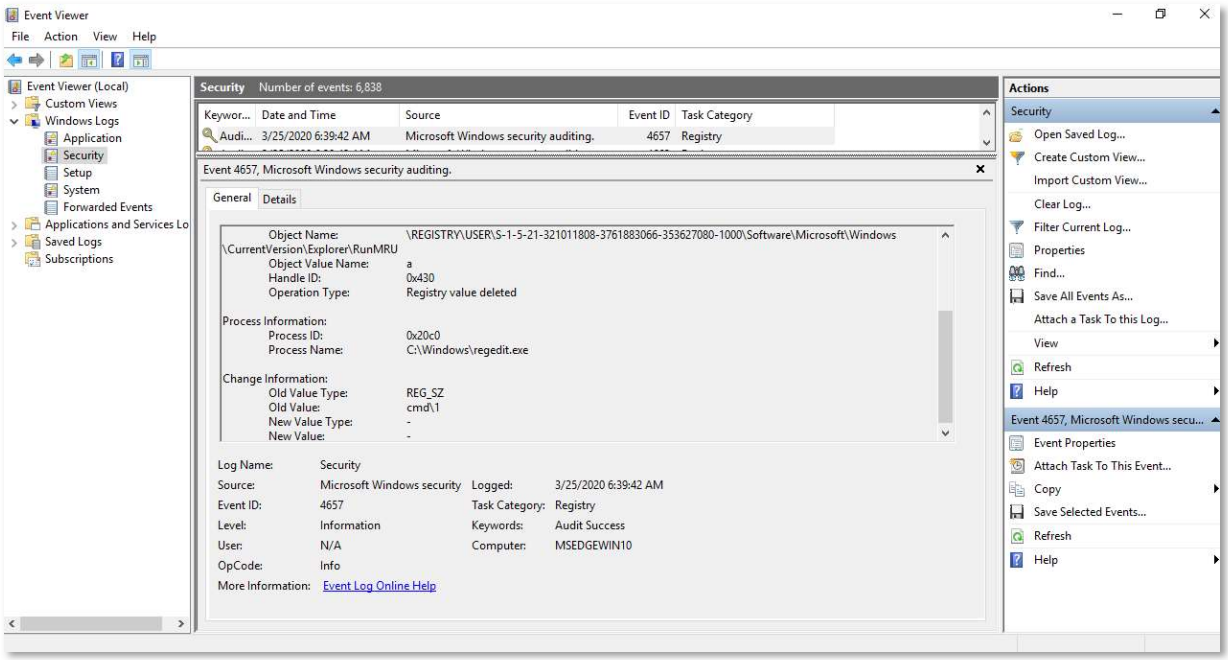


Figure 9- Windows event log - registry deletion audit trail.

Use case: *secondary or tertiary source of forensic artifacts.*

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

DOCUMENTS OPENED IN OFFICE SUITE: key values located in ROOT -> Software -> Microsoft -> Office -> #number -> Word/Excel/Powerpoint/Onenote... -> User MRU -> #profile ID -> **File MRU / Place MRU**

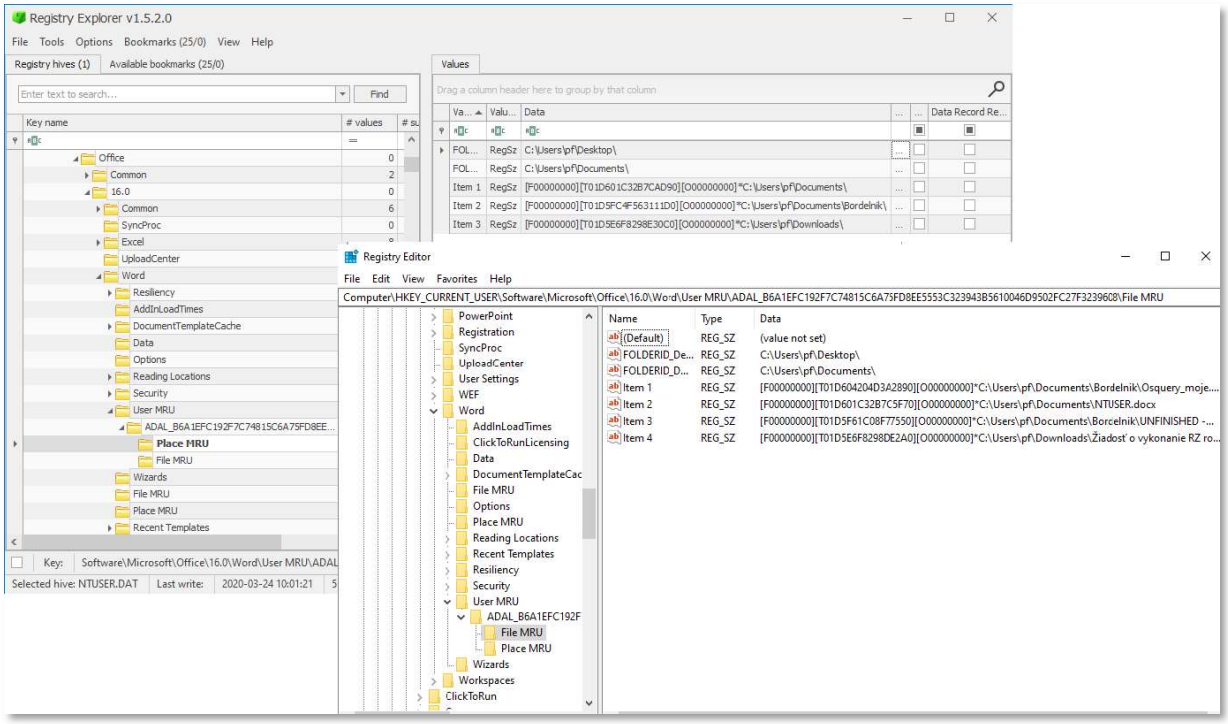


Figure 10- Values in "Place MRU" contains parent directories of files run in "File MRU".

"File MRU" key holds previously accessed file documents and with the help of key "Place MRU", we can get an idea where user keeps his documents (including USB and network shares) and what did he access. You should be able to find parent directory of every file that you can see in "File MRU".

Use case: *when searching for evidence of execution or access to specific file or when you are trying to reassemble user activity.*

PATHS TYPED INTO WINDOWS EXPLORER: key values are located in ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> **TypedPaths**

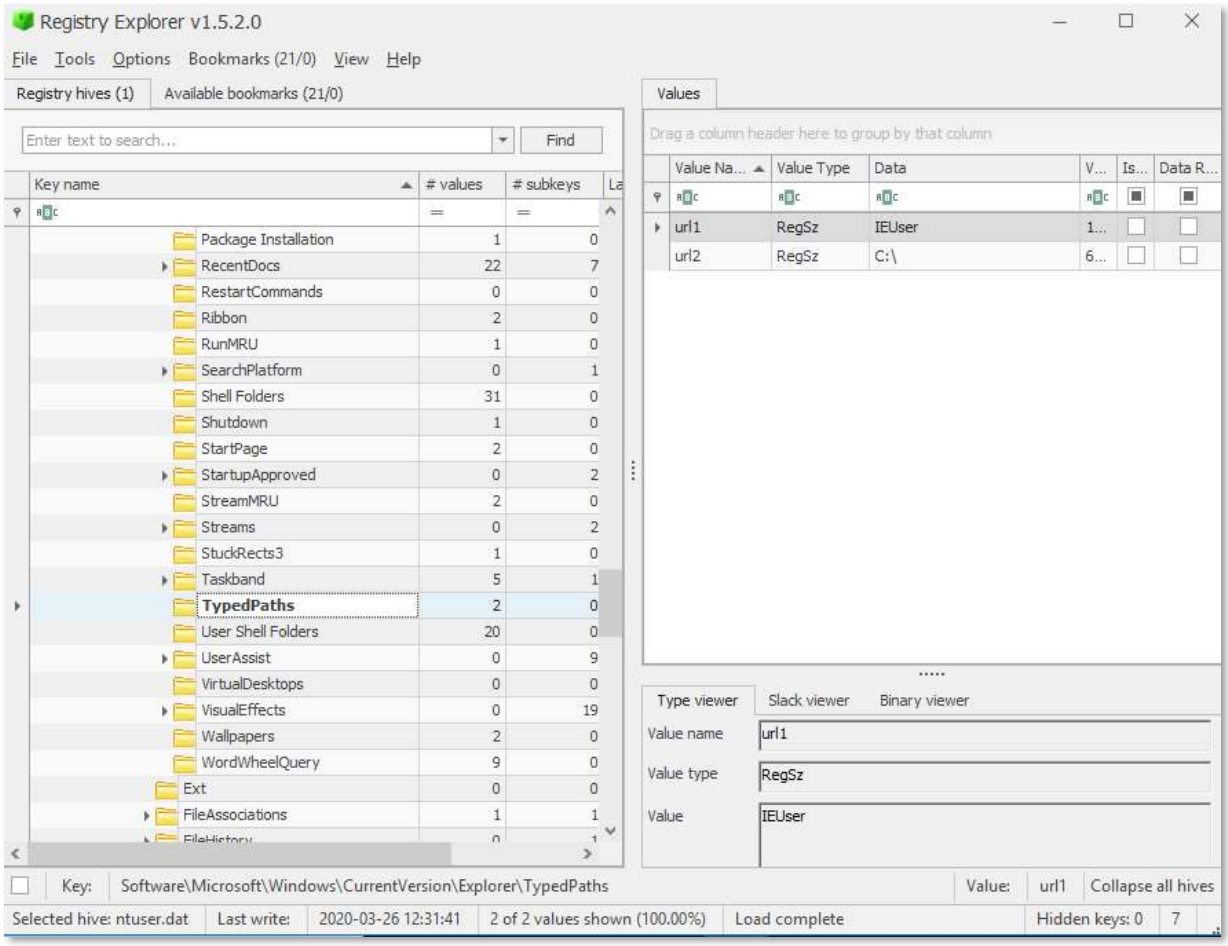


Figure 11- Here we can see values typed into Windows Explorer, you can see network shares in this directory as well.

This key is populated by last 25 directories manually typed into Windows explorer. Value in key is named url1, url2 and so on. When the first value is added it gets assigned value of "url1", the next key will get value "url1" and the previous entry will move to "url2".[3] However, each Explorer window saves only typed directories for its current

[3] Harlan Carvey, Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, pg.159

session. So if you have two windows open and you close them consecutively, entries will get overwritten and only final windows will remain in registry.

Use case: *secondary or tertiary source of forensic artifacts.*

DESKTOP CONTENTS, SHELLBAGS: key values at ROOT -> Software ->Microsoft -> Windows -> Shell -> Bags -> #number -> Desktop (Windows 10)

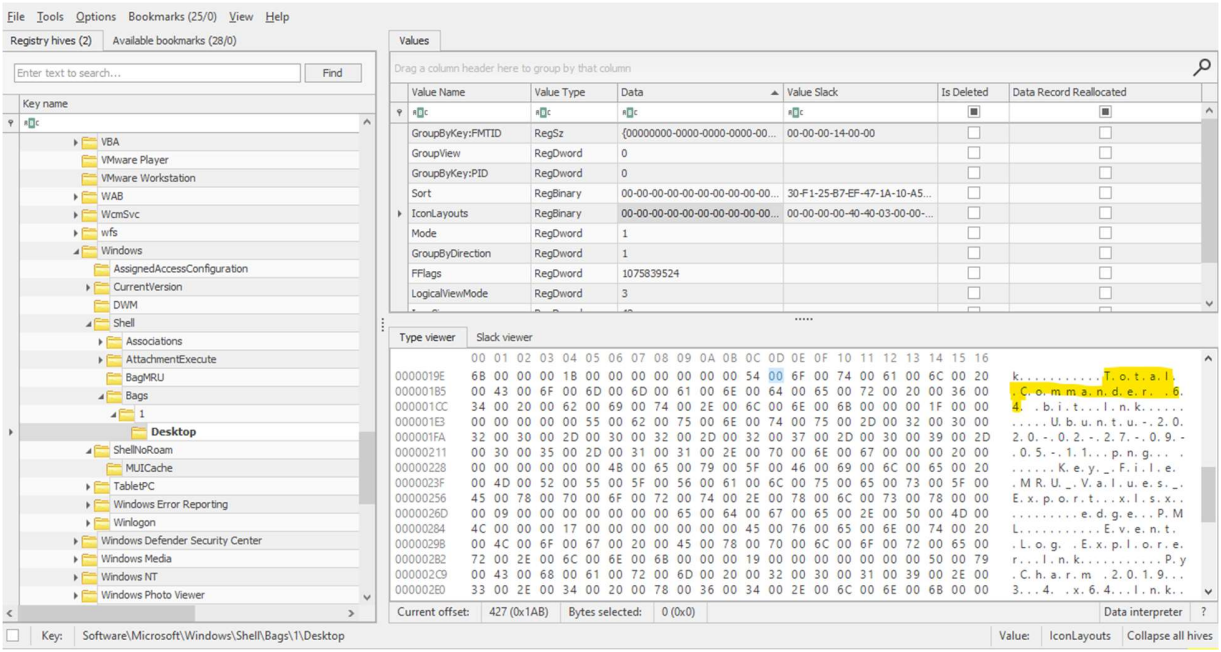
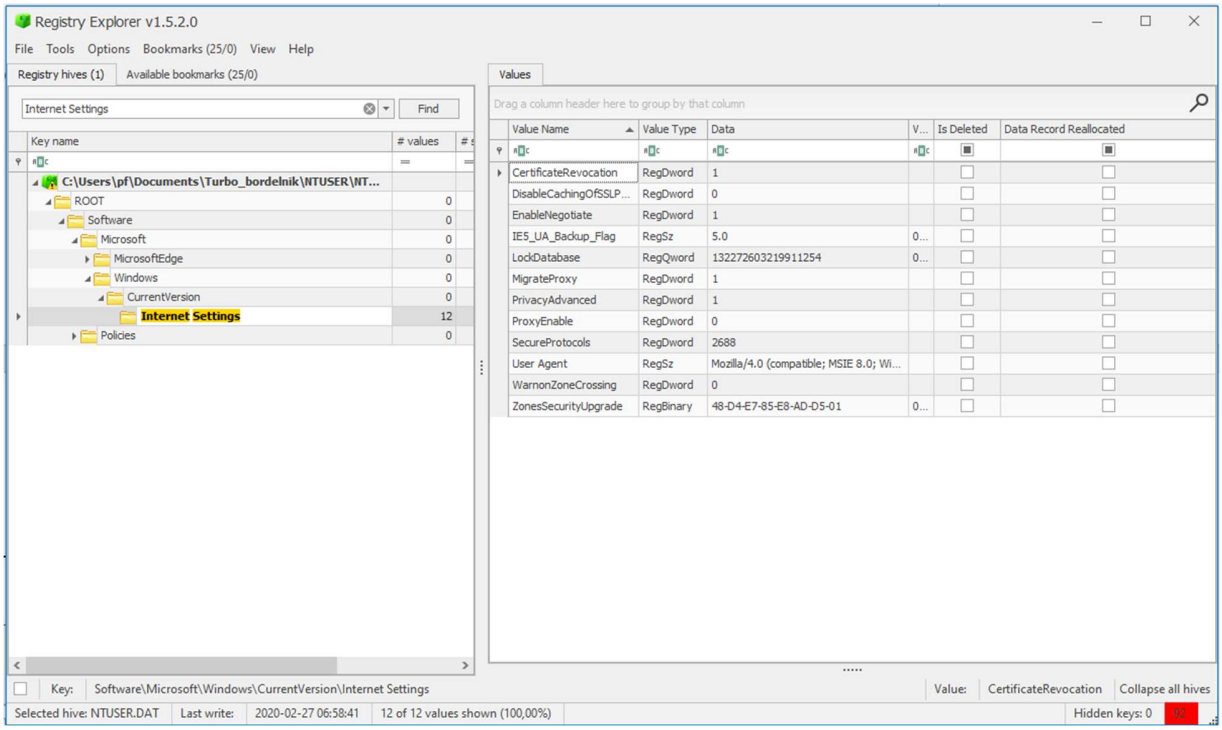


Figure 12- Contents of users' Desktop as seen in NTUSER hive.

ShellBag data is located not only in NTUSER.DAT hive, but in USRLCLASS.DAT as well. There are different values in each hive, which describe different events. In USRSCLASS.DAT hive we can find ShellBag values that point to folders accessed via Explorer and in NTUSER hive, we can find folders accessed from Desktop. In the …\Shell\Bags\1\Desktop key we can find the contents and the order they appear in on user's desktop. Value {645FF040-5081-101B-9F08-00AA002F954E} represents the Recycle Bin. Every value you see in this key is proof that the folder was present at some point in time on the system. However, only those from last closed window will remain in registry.

Use case: *Evidence of folder access/presence on the system.*

INTERNET SETTINGS AND SHAREPOINT NAME: key values at ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> **Internet Settings** / -> Zone Map -> Domains -> sharepoint.com



In this key we can see user is running Mozilla browser. However, the version number does not corelate with the user agent version that is being run on this machine, so it should not be used as a reference for UserAgent version. There are other usefull entries in "Internet Settings" directory, such as Zone Map -> **domains/Escdomains** -> sharepoint.com, which holds SharePoint URLs accessed by the user.

If we tried to look for browser history for Mozilla Firefox in registry, we would not be able to find it. Neither, Chrome, Opera or Firefox stores browsing history in registry, only Microsoft Edge or Internet Explorer stores their history there.

Use case: *evidence of access, user activity.*

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

URLS TYPED INTO INTERNET EXPLORER: key values are located in ROOT -> Software -> Microsoft -> Internet Explorer -> **TypedURLs**

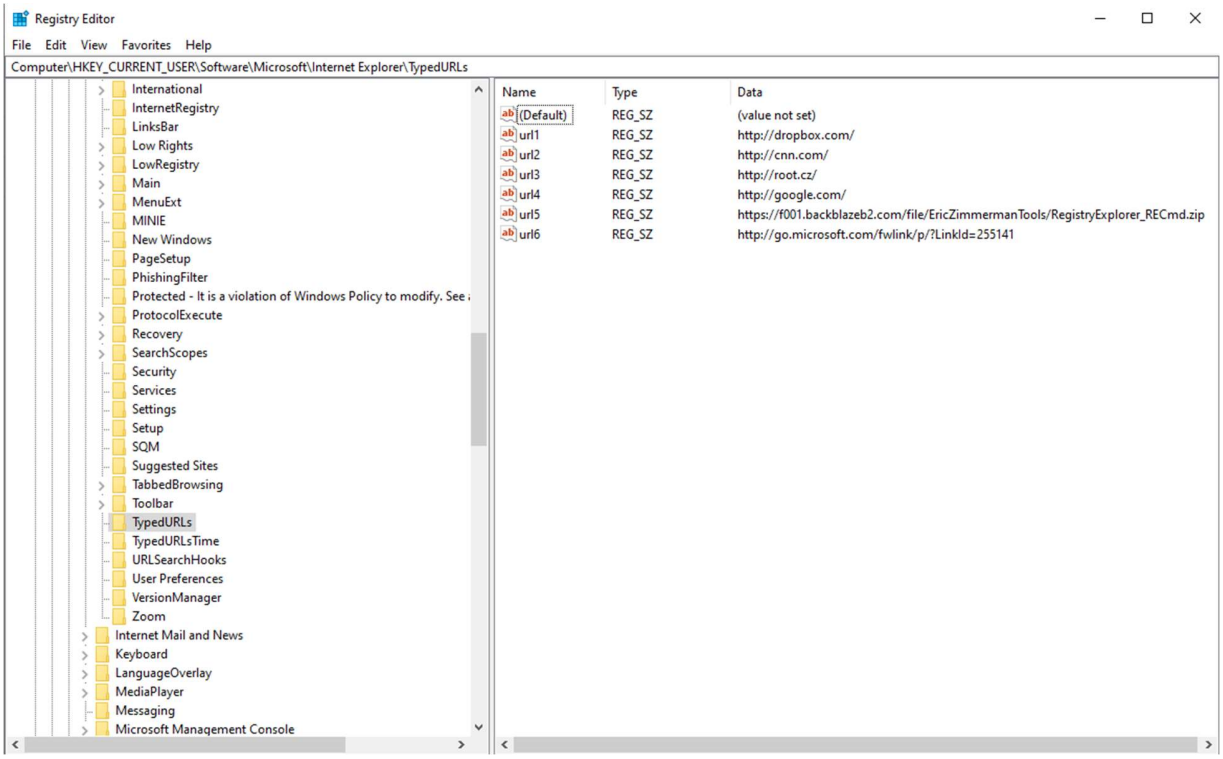


Figure 13-Here we can see URLs typed into IE, in this case we see it in Windows native registry editor. Path is in this case is HKEY_CURRENT_USER\... which is one of the locations from which NTUSER.DAT is populated.

This key contains a listing of 25 recent URLs (or file path) that is typed in the Internet Explorer (IE) or Windows Explorer address bar: the key will only show links that are fully typed, automatically completed while typing or links that are selected from the list of stored URLs in IE address bar. If we explore related registry key "TypedURLsTime" we can see when was the last time user accessed the site trough Internet Explorer. Same as with "TypedPaths", latest entry gets assigned value "url1" which then correlates with value in "TypedURLsTime". If we want to translate the number to human readable time, we should access it with windows native RegEdit, as Registry Explorer has a bit of trouble

with those values. They are stored in Little Endian Hex value in windows FILETIME format, so for decoding we can use DCode.

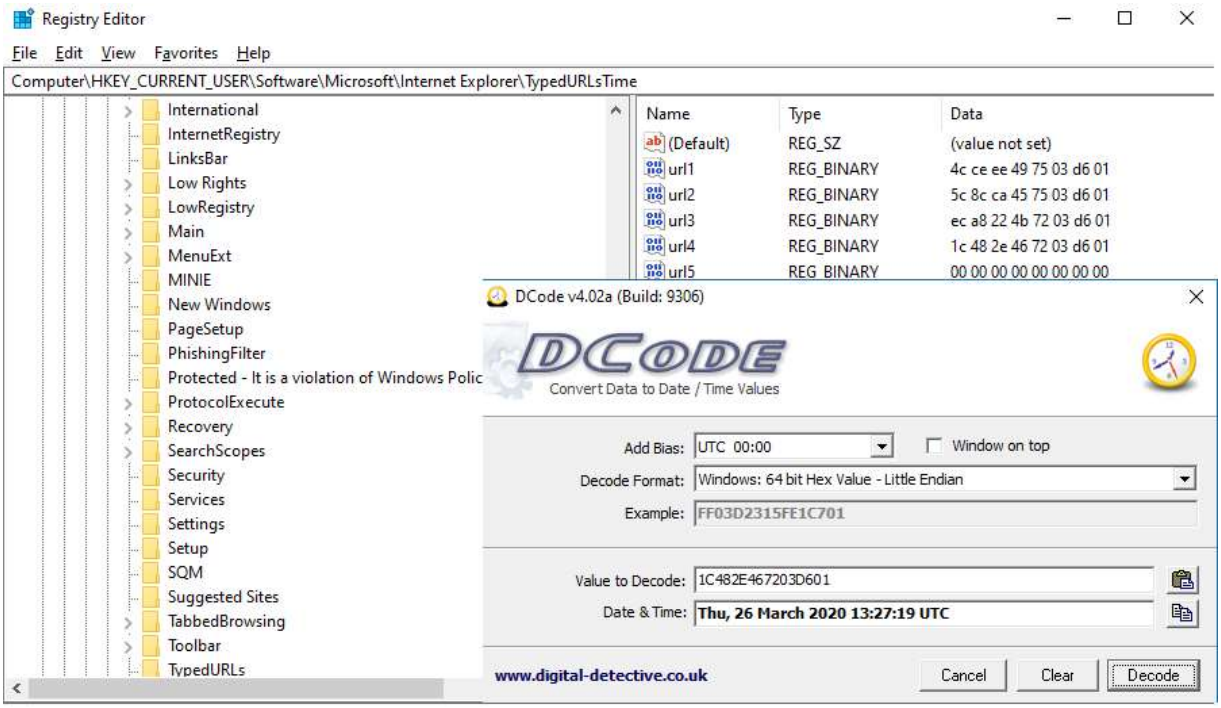


Figure 14- Here we can see values in TypedURLsTime and the decoding of time with DCode tool.

If we want to look for browser history for Microsoft Edge, we can find it HKEY_CURRENT_USER…[4]

Use case: *user activity, evidence of access.*

USER SEARCH HISTORY IN SEARCH BAR: key values are located in ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> **WordWheelQuery**

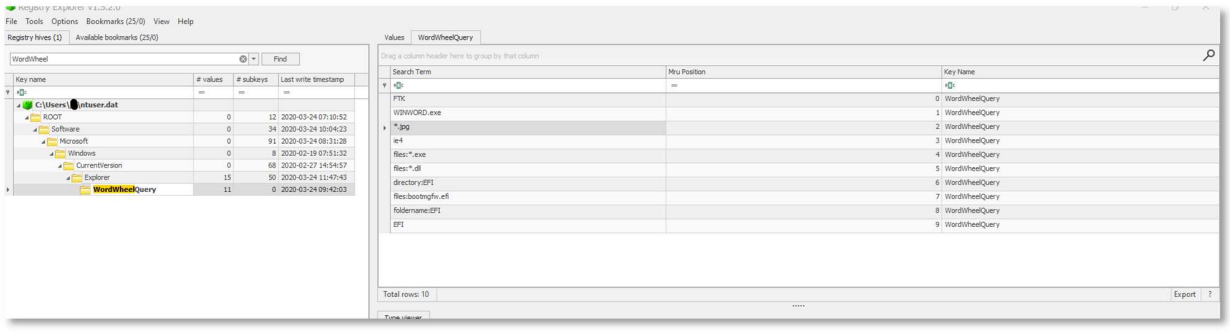


Figure 15 - Expressions user typed in search bar.

4 HKEY_CURRENT_USER\Software\Classes\Local_Settings\Software\Microsoft\Windows\CurrentVersion\Ap

Skilled threat actor will usually not search for files through graphical interface or by typing into Explorer search bar. Therefore, we should not expect to find evidence of malicious behavior here when dealing with advanced attacker.

Use case: *it can help us gain insight in user behavior during investigation of disgruntled employee or insider threat.*

Applets: key values are located at ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> **Applets**

This key holds evidence of execution, access time and path of files access by specific applets. Let us take a look at RegEdit and WordPad applets as an example.

Regedit – Last Key shows the last opened key with regedit.exe. Changing this value will make the next instance of regedit start on modified key.

WordPad – Recent File List key holds paths to WordPad files saved by user on the system.

pContainer\Storage\microsoft.microsoftedge_8wekyb3d8bbwe\Children\001\Internet Explorer\DOMStorage

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

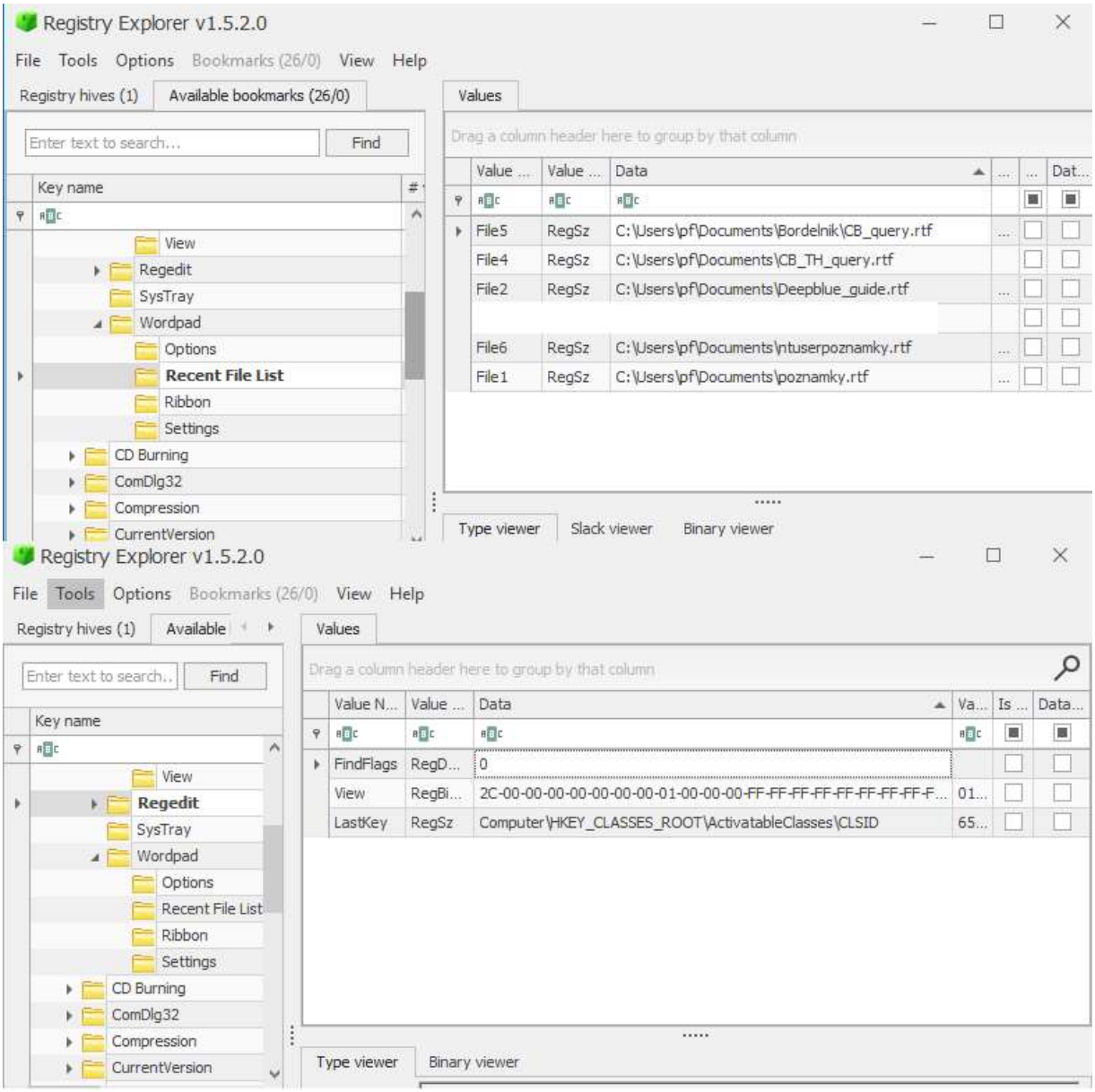


Figure 16-Last accessed files in WordPad and last accessed key through RegEdit.

Use case: *evidence of execution, user activity.*

RECENTLY OPENED DOCUMENTS: ROOT -> Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> **RecentDocs**

We can find information on what files and folders user accessed and when. However, we cannot trust the time indications in this key unless we verify it from another source (image of disk, logs, other registry hives).

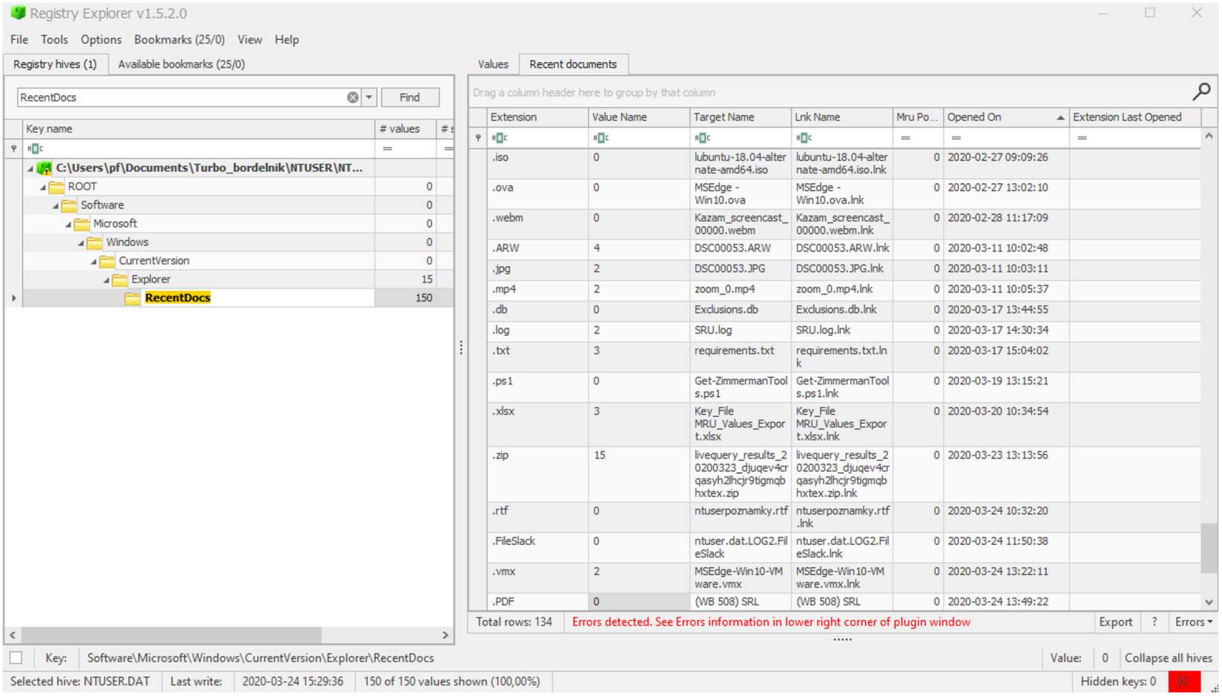


Figure 17- Recently opened documents with first and last accessed time.

Use case: *finding out if user opened malicious file or accessed sensitive documents. We can find evidence of execution for files accessed on network share or removable media.*

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

PROGRAMS THAT RUN ON STARTUP FOR CURRENT USER: Software -> Microsoft -> Windows -> CurrentVersion -> **Run**

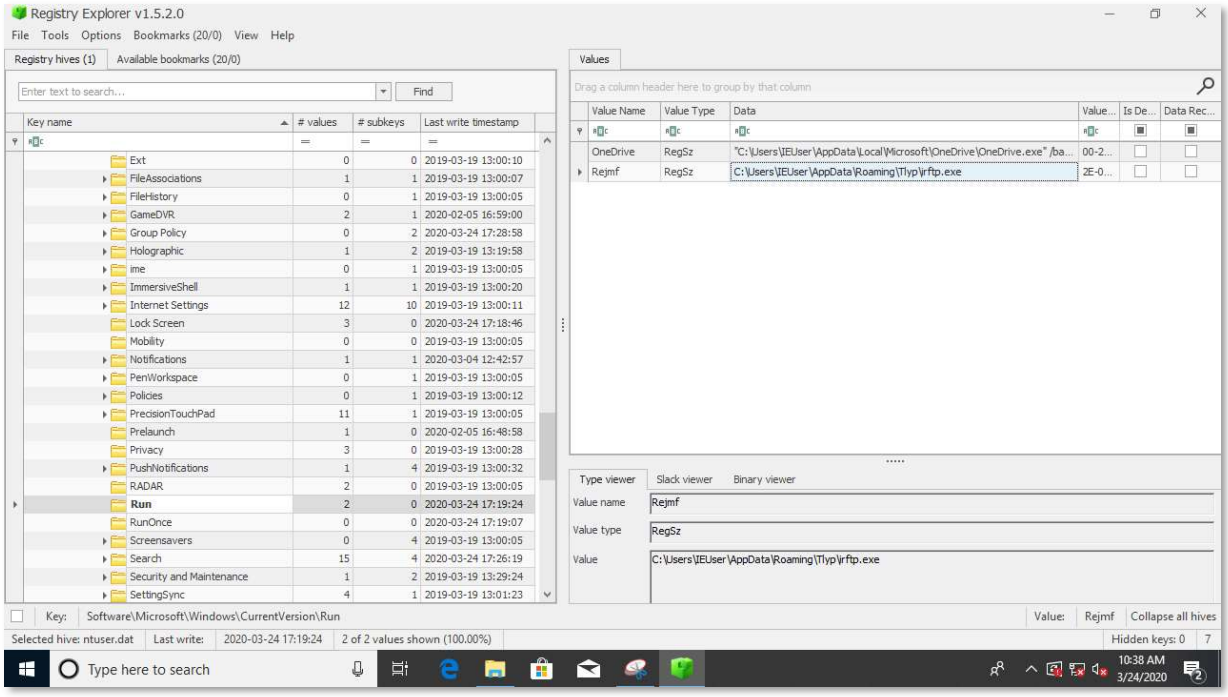


Figure 18- Here we can see startup entry created by Dridex malware.

We can find path to executables or files that run on startup of user whose NTUSER hive we are investigating.

Use case: *good place to look for persistence created by PUA, trojans or malwares running under permissions of that user.*

CONNECTED PRINTER DEVICES: *key value is located ROOT ->* Software -> Microsoft -> Windows NT -> CurrentVersion -> **Devices**

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com

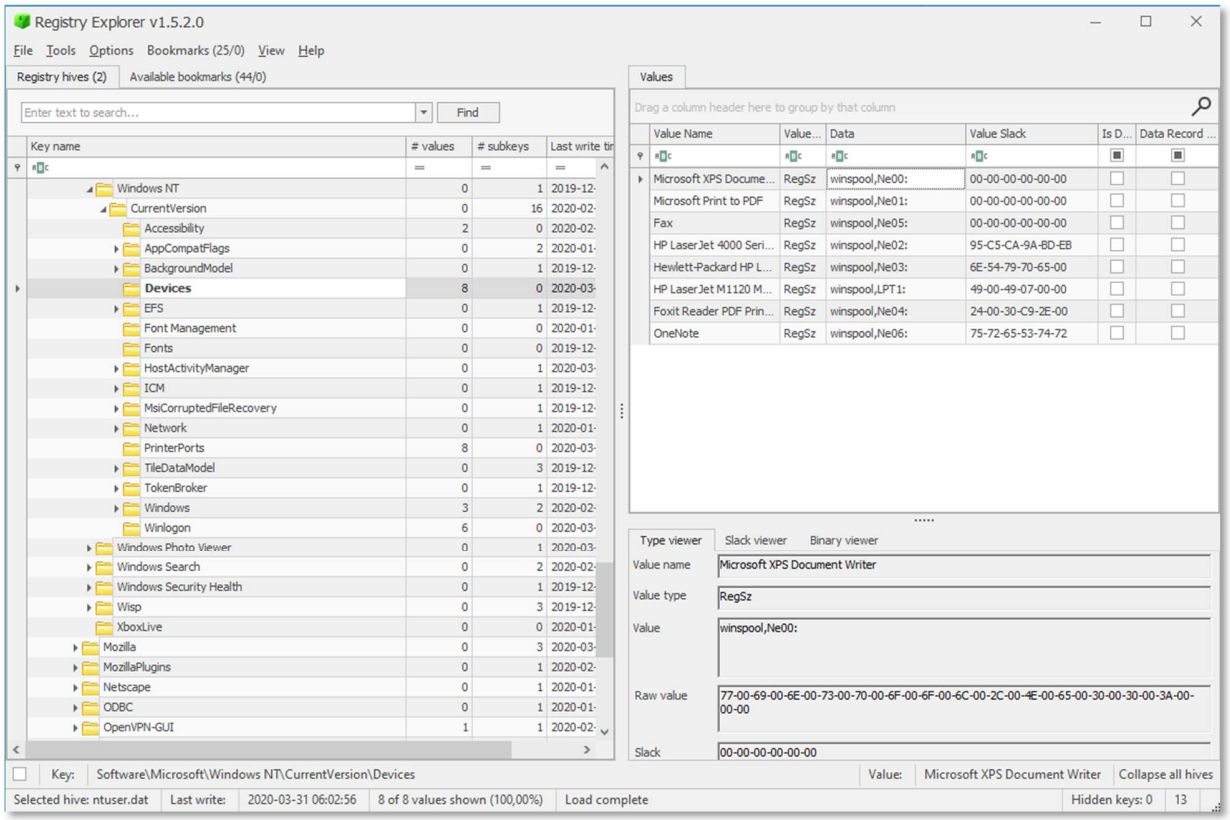


Figure 19- List of printers that were connected to this device.

We can find list of currently active drivers loaded by Device Manager. If we want to find history of USB's connected to this workstation at some point, we need to look into SYSTEM\....\USBSTOR [5]hive key.

Use case: secondary or tertiary source of forensic artifacts.

[5] HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

******

Additional information sources:

https://www.dfir.training/resources/downloads/windows-registry

https://ad-pdf.s3.amazonaws.com/UserAssist%20Registry%20Key%209-8-08.pdf

https://www.nirsoft.net/utils/iehv.html

244 Fifth Avenue, Suite 2035, New York, NY 10001
LIFARS.com (212) 222-7061 info@lifars.com