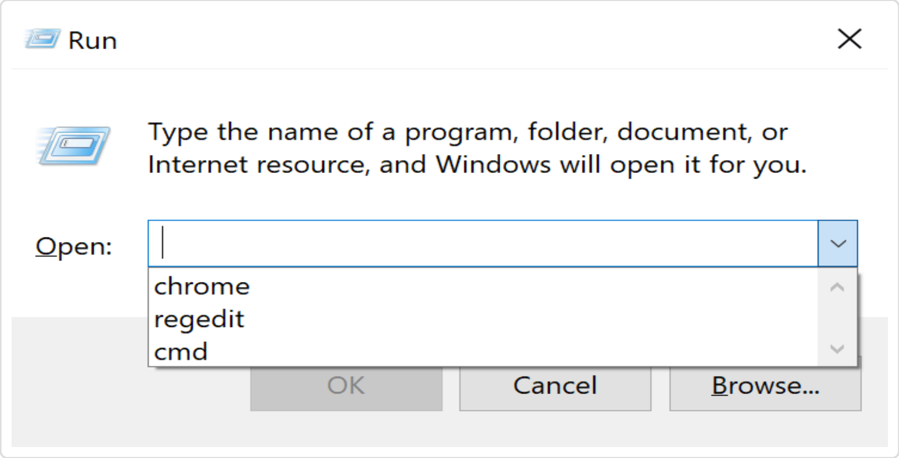
Blog >> Run MRU

Investigating Run MRU

29/04/2022 Friday

The Run utility on Windows Systems enables the user to directly open an application, folder or document. In Windows 10, the Run utility can be accessed by right-clicking on Start > Run or by using the keyboard shortcut Windows Key + R. As seen in the figure below, the Run utility includes a drop-down list that shows the last commands executed via the Run dialog.



Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open:

chrome
regedit
cmd

Items typed into the Windows Run dialog are recorded in the Registry under the RunMRU key. Deleting a value from RunMRU key will cause that entry to be removed from the history list of the Run utility. However, deleting the RunMRU key or any of its values does not remove the history list in Run utility immediately. The user has to close the Run window for the action to be effective.

Digital Forensics Value of Run MRU

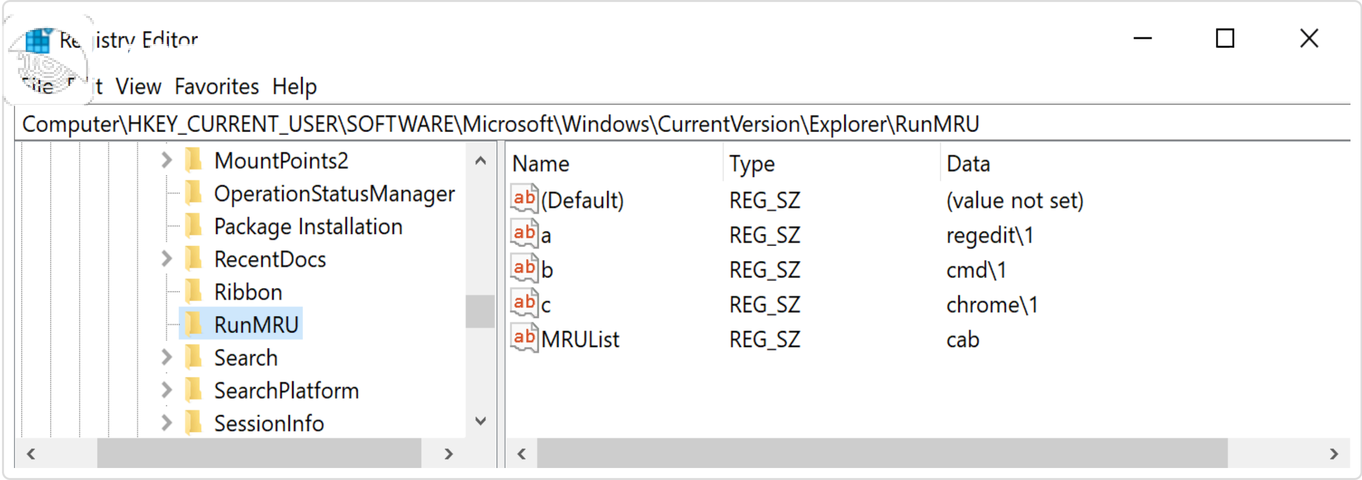
The information maintained in the RunMRU key may shed some light on the user's activity on the system. The Run MRU artifact is also used when suspecting an attack by a malicious actor as it can indicate the execution of a program or even a script on a device. In addition, this artifact proved to be helpful when investigating access to files and applications on removable storage devices or remote systems.

Location of Run MRU Artifact

RunMRU key is located at: **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**

Structure of Run MRU Artifact

RunMRU key contains multiple values that are named for lowercase letters. These values store the commands that a user run using the Run utility. The first value added is named "a", the second value is named "b", then, "c" and so on. However, the names of the values do not always reflect the order in which the commands were typed into the Run box. This information is maintained in the "MRUList" value which is a string that lists the order in which each value beneath the RunMRU key was last accessed. For instance, in the figure below, the first letter listed in the MRUList is "c". The value named "c" stores the command "chrome" which means that the most recent command typed into the Run box is "chrome".



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

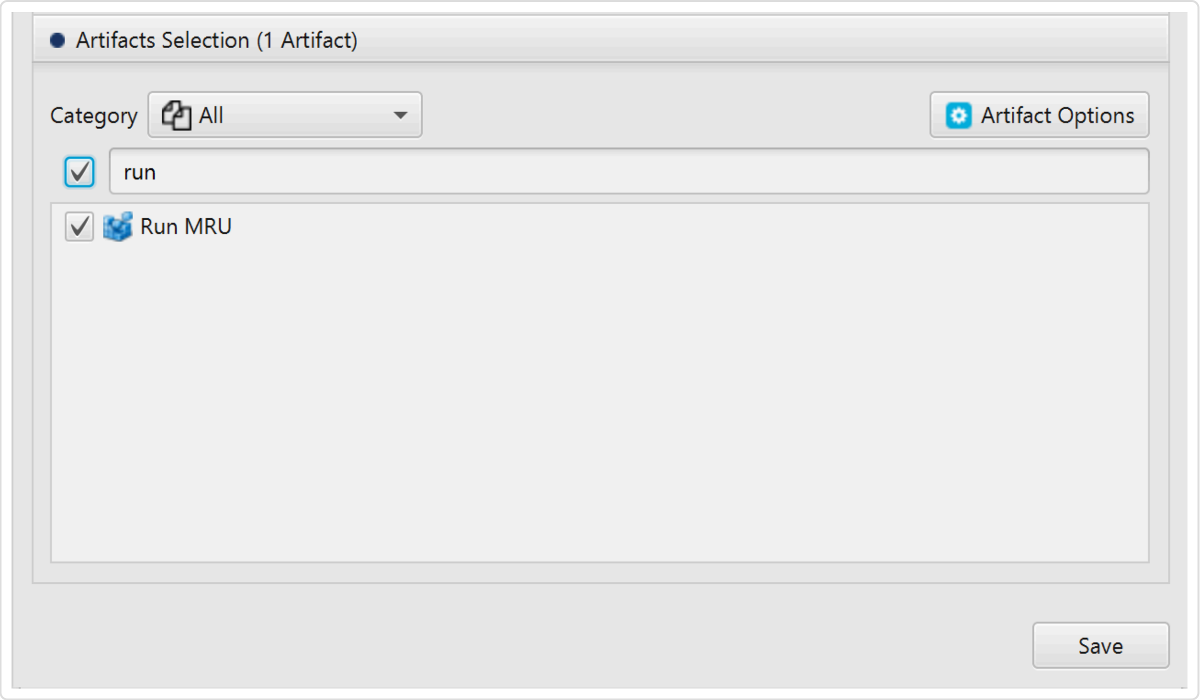
Name	Type	Data
(Default)	REG_SZ	(value not set)
a	REG_SZ	regedit\1
b	REG_SZ	cmd\1
c	REG_SZ	chrome\1
MRUList	REG_SZ	cab

Free Version
Try

Analyzing Run MRU Artifact with ArtiFast Windows

This section discusses how to use ArtiFast Windows to analyze Run MRU artifact from Windows machines and what kind of digital forensics insight we can gain from the artifact.

After you have created your case and added evidence for the investigation, at the Artifacts Selection phase, you can select Run MRU Artifact:

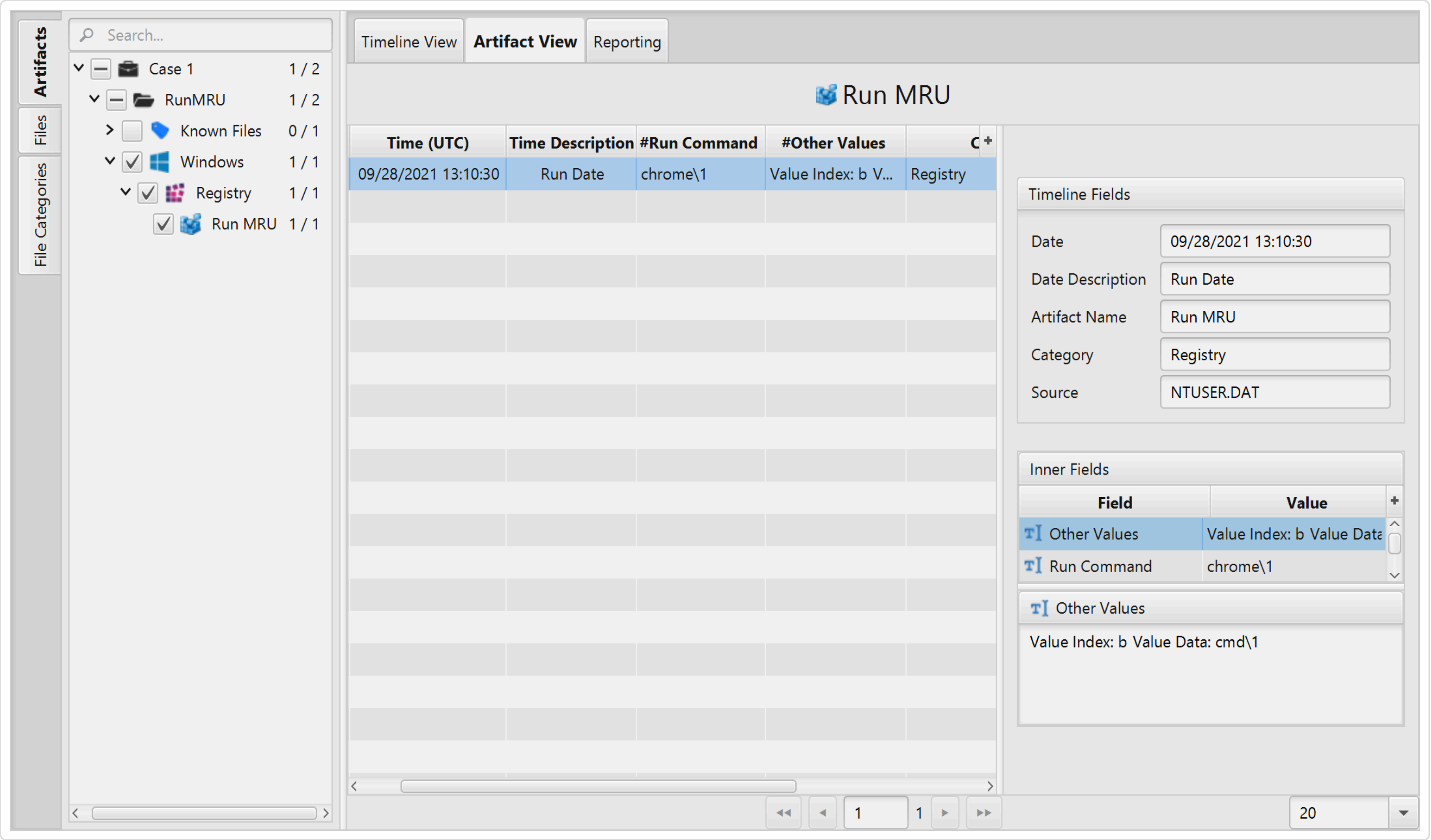


● Artifacts Selection (1 Artifact)

Category: All

☑ run

☑ Run MRU



- Case 1 1 / 2
  - RunMRU 1 / 2
    - □ Known Files 0 / 1
    - ☑ Windows 1 / 1
      - ☑ Registry 1 / 1
        - ☑ Run MRU 1 / 1

Time (UTC)	Time Description	#Run Command	#Other Values	C
09/28/2021 13:10:30	Run Date	chrome\1	Value Index: b V...	Registry

Timeline Fields

Date	09/28/2021 13:10:30
Date Description	Run Date
Artifact Name	Run MRU
Category	Registry
Source	NTUSER.DAT

Inner Fields

Field	Value
Other Values	Value Index: b Value Data
Run Command	chrome\1

Other Values

Value Index: b Value Data: cmd\1

Once ArtiFast parser plugins complete processing artifacts for analysis, it can be reviewed via “Artifact View” or “Timeline View”, with indexing, filtering, and searching capabilities. Below is a detailed description of Run MRU artifact in ArtiFast Windows.

Run MRU Artifact

- **Run Command** - The last command string that the user inserted in the Windows Run utility.
- **Run Date** - The date and time the RunMRU key was last modified.
- **Other Values** - The other values inserted in the Windows Run utility.

For more information or suggestions please contact: asmaa.elkhatib@forensafe.com

FORENSAFE

- About Us
- ArtiFast
- Contact
- Artifacts
- Buy Now

- Try
- Events
- Resources
- Blog
- Artifact Parser Library

New York - USA
575 Underhill Blvd. Suite 209
Syosset, NY 11791 USA

Copyright © 2024 Forensafe - All Rights Reserved.