Digital Investigation 12 (2015) 53–65

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

# Forensic implications of System Resource Usage Monitor (SRUM) data in Windows 8

Yogesh Khatri*

*163 South Willard Street, P O Box 670, VT 05402-0670, USA*

ARTICLE INFO

*Article history:*
Received 5 March 2014
Received in revised form 16 December 2014
Accepted 15 January 2015
Available online 11 February 2015

*Keywords:*
System Resource Usage Monitor
SRUM
Windows 8
Forensics
Process metrics

ABSTRACT

The Microsoft Windows 8 operating system has a newly added feature to track system resource usage, specifically process and network metrics over time. Process related information such as process owner, CPU cycles used, data bytes read/written, and network data (sent/received) are continuously recorded by a mechanism called System Resource Usage Monitor (SRUM). This paper describes the SRUM mechanism, its databases, Windows registry entries, data logging, and potential uses in a forensic examination. Prior to this applied research, no tools were available to parse the SRUM data to a usable format. As part of this paper, two scripts have been developed to aid forensic examiners who would want to read, parse, and decode this information from a forensic disk image.

© 2015 Elsevier Ltd. All rights reserved.

## Introduction

System Resource Usage Monitor (SRUM) is a new technology that made its debut in Windows 8. SRUM tracks process and network statistics over time in a database. The information collected by SRUM includes process details, user details, CPU cycles, and network data sent or received by a particular process. Only a limited amount of this information is available to the end user – the bulk of the SRUM database is not displayed. Windows 8.1 which released in October 2013 continued to use this technology and expanded upon it.

SRUM offers forensic examiners an historical view into past system usage on a computer. From a forensic examiner's point of view, this database can be immensely useful in tracing user activity and linking process, user and network activity together. This paper examines SRUM databases, exposes the locations of these databases, the types of data stored, the formats and some working details of SRUM. A practical guide to extracting and decoding this data is included in this paper. A limited analysis and interpretation of this data is presented to demonstrate its usefulness in a forensic investigation. This includes tracking processes in ways previously not possible, linking of process to network activity and tracking external or deleted processes. This new data has immediate applications in the incident response space as it can provide evidence of data copying, estimate the amount of ex-filtrated data from a computer at the same time tying it down to a specific user, process and time period.

## Research methods

As of writing this paper, there are no existing works or published literature on SRUM. The SRUM feature is new in Windows 8 and, currently, there is no Microsoft documentation detailing the inner workings of SRUM. The research method used in this work for studying SRUM involved observation and experiment. Several experiments were conducted to study the SRUM mechanism as a black box. These are detailed in Section Experiments below.

Primarily two versions of Windows were studied, Windows 8 and Windows 8.1. Four test computers were

* Tel.: +1 626 344 9189.
*E-mail address:* yogesh@swiftforensics.com.

http://dx.doi.org/10.1016/j.diin.2015.01.002
1742-2876/© 2015 Elsevier Ltd. All rights reserved.

utilized which included a mix of laptops, desktops and virtual machines. On each test system, a baseline was taken, and then all test results were observed using forensic software, including EnCase and Autopsy. In addition, SRUM databases from several other personal computers were collected and analyzed to evaluate the consistency of the data structures observed during experimentation, and to validate the conclusions outlined here.

## System Resource Usage Monitor

System Resource Usage Monitor (SRUM) is integrated into the new Diagnostic Policy Service (DPS). DPS enables problem detection, troubleshooting, and resolution for Windows components according to Microsoft (Microsoft, Diagnostic Policy Service, 2009). This service is enabled by default and configured to start automatically upon system startup on all Windows versions, including Enterprise versions. Internally, the system uses a number of extensions to monitor process, network, and energy resources. Table 1 lists the extensions, associated DLL files and GUIDs that represent them. These GUIDs are the same on any Windows 8 or 8.1 systems.

'Windows Network Connectivity' (ncuprov.dll) has been added in Windows 8.1 and was not present earlier in Windows 8.

### *Data collection and update frequency*

Process related data and network usage associated with processes are logged by SRUM. These data are collected for all desktop applications, system utilities, services, as well as Windows Store (Metro) Apps (Microsoft, Meet Windows Store Apps).

The process related information collected by SRUM includes full process path, process owner (user that launched the process), metrics for I/O data (bytes read & written in foreground/background), CPU cycle utilization (foreground/background), context switches, process network utilization (data uploaded/downloaded), and Windows Push Notifications (Notification type and data payload size). Network connectivity is also tracked, i.e. the start time and amount of time the computer system was connected to a network. Windows also tracks the type of network, whether it is metered (3G, 4G …) or non-metered (Ethernet or Wi-Fi) (Microsoft, Metered Internet connections: FAQ). On laptops and mobile devices, SRUM also collects system transition state and battery related information such as designated capacity, full charge capacity and available charge.

**Table 1**
SRUM extensions, associated GUIDs and DLL files.

| SRUM extension | GUID | DLL in System32 |
|---|---|---|
| Windows Network Data Usage Monitor | {973F5D5C-1D90-4944-BE8E-24B94231A174} | nduprov.dll |
| Windows Push Notifications (WPN) SRUM Provider | {d10ca2fe-6fcf-4f6d-848e-b2e99266fa86} | wpnsruprov.dll |
| Application Resource Usage Provider | {d10ca2fe-6fcf-4f6d-848e-b2e99266fa89} | appsruprov.dll |
| Windows Network Connectivity Usage Monitor | {DD6636C4-8929-4683-974E-22C046A43763} | ncuprov.dll |
| Energy Usage Provider | {fee4e14f-02a9-4550-b5ce-5fa2da202e37} | energyprov.dll |

However, not all process or network related details are collected. Process details such as the command line arguments, DLL information, resource handles, thread information, or files accessed are not recorded by SRUM. Furthermore, network endpoint details like IP addresses, computer names, protocols or port numbers are not collected.

While SRUM continuously collects data on a running system, it only periodically updates the SRUM database. This update period is one hour by default. On any Windows 8 system, the default setting is to write out information at 30 min after every hour (example: 4:30, 5:30, 6:30 …) unless a shutdown occurs, which triggers an immediate update of the SRUM.

### *Viewing SRUM data on windows*

On a running Windows 8 system, SRUM data is viewable under Task Manager's 'App History' tab (Gear, 2013). However the view is very limited and most of the collected data are not shown, it is only an abridged summary of the SRUM database contents. For example, individual application runs are not displayed in the Task Manager view, only cumulative statistics are shown. In addition, application names shown in the Task Manager view are not those of the executable files, instead the 'File Description' strings from version information are used. Applications are tracked by their full path on disk, so two copies of the same application running from different locations will be shown separately. Application details for deleted executables and those that can no longer be found in their original location are grouped together under the name 'Uninstalled processes'. As most program installers extract and run from temporary locations such as %temp%, these also find themselves in this category as they are deleted from their temporary locations post install.

Details such as timestamps, application paths, and deleted application names are not on display. To obtain these details, it is necessary to read the data directly from the SRUM database and the Windows registry.

### *Retention*

The SRUM service typically retains data for at least one month. This retention can be witnessed in Task Manager's App History tab which shows the starting date from which history has been displayed. However, much older entries are frequently found in the SRUM database. Users can also manually purge the collected data using the option 'Delete usage history' from the Task Manager as seen in Fig. 1. However, this delete operation does not purge all information from the SRUM database. In experiments, even when the delete operation was selected, much of the data

Download English Version:

https://daneshyari.com/en/article/457798

Download Persian Version:

https://daneshyari.com/article/457798

Daneshyari.com