

Background Activity Moderator (BAM)

The Bam key found in the SYSTEM hive at the

`"ControlSet001\Services\bam\"` key

Has a subkey of `"\UserSettings\"`

Which lists all the user SIDs in the current system.

| | | |
|--|-----|---------------------|
| ▼ bam | 6 | 2018-02-03 21:23:42 |
| ▼ UserSettings | 0 | 2018-02-22 23:05:35 |
| S-1-5-18 | 7 | 2018-02-25 12:42:20 |
| S-1-5-21-811833292-1881212584-745805... | 180 | 2018-02-25 13:13:05 |
| S-1-5-21-811833292-1881212584-745805238-1025 | 14 | 2018-02-22 23:10:53 |
| S-1-5-90-0-1 | 3 | 2018-02-24 15:03:51 |
| S-1-5-90-0-10 | 2 | 2018-02-01 20:44:23 |
| S-1-5-90-0-11 | 2 | 2018-01-10 08:43:08 |
| S-1-5-90-0-12 | 2 | 2018-01-10 08:43:08 |
| S-1-5-90-0-13 | 2 | 2018-01-10 08:43:08 |
| S-1-5-90-0-14 | 2 | 2018-01-10 08:43:08 |
| S-1-5-90-0-15 | 2 | 2018-01-10 08:43:08 |
| S-1-5-90-0-2 | 3 | 2018-02-24 19:39:12 |
| S-1-5-90-0-3 | 3 | 2018-02-24 21:10:08 |
| S-1-5-90-0-4 | 3 | 2018-02-25 08:32:35 |
| S-1-5-90-0-5 | 3 | 2018-02-22 18:47:30 |
| S-1-5-90-0-6 | 3 | 2018-02-22 20:06:33 |
| S-1-5-90-0-7 | 3 | 2018-02-22 23:03:31 |
| S-1-5-90-0-8 | 3 | 2018-02-22 23:10:54 |
| S-1-5-90-0-9 | 3 | 2018-02-22 23:11:23 |

Selecting a user's SID we see a list of paths and executables, not necessarily installed in Windows (eg AccesEnum.exe shown below, which is a command line utility):

| Value Name | Value Type | Data |
|---|------------|------------------|
| nt | nt | nt |
| Device\HarddiskVolume2\Forensic Tools\AccessEnum\AccessEnum.exe | RegBinary | EE-9E-3A-74-7... |
| Device\HarddiskVolume2\Forensic Tools\AmcacheParser\AmcacheParser... | RegBinary | 5E-72-9A-0C-5... |
| Device\HarddiskVolume2\Forensic Tools\CrowdResponse\CrowdRespons... | RegBinary | E9-E9-0B-94-D... |
| Device\HarddiskVolume2\Forensic Tools\CrowdResponse\CrowdRespons... | RegBinary | C7-E4-B7-FE-D... |
| Device\HarddiskVolume2\Forensic Tools\DCCode-v4.02a-build-4.02.0.930... | RegBinary | FE-06-AF-AA-1... |
| Device\HarddiskVolume2\Forensic Tools\esedatabaseview\ESEDatabase... | RegBinary | 09-2B-66-27-3... |
| Device\HarddiskVolume2\Forensic Tools\ForensicUserInfo.v1.0.5\Foren... | RegBinary | BC-E8-E0-19-1... |
| Device\HarddiskVolume2\Forensic Tools\JSONView\JSONView.exe | RegBinary | 54-A9-F9-9A-8... |

The value of the each of those is the time last executed (?) in Filetime (64bit little Endian) format:

| | |
|------------------|---|
| Decode Format: | Windows: 64 bit Hex Value - Little Endian |
| Example: | FF03D2315FE1C701 |
| Value to Decode: | EE9E3A747EADD301 |
| Date & Time: | Sat, 24 February 2018 14:47:55 UTC |

| Source date/times | Original | date | format |
|--------------------|--------------------|----------------------|----------|
| 0xEE9E3A747EADD301 | 0xEE9E3A747EADD301 | 24-Feb-18 2:47:55 pm | FileTime |

This list also includes Windows apps. For example the last time MS Edge was executed was:

| | | |
|---|-----------|------------------|
| CAF9E577.Plex_aam28m9va5cke | RegBinary | BA-AE-CC-AB-... |
| Microsoft.AccountsControl_cw5n1h2bxyewy | RegBinary | 4B-82-DA-57-3... |
| Microsoft.LockApp_cw5n1h2bxyewy | RegBinary | BA-AE-CC-AB-... |
| Microsoft.MicrosoftEdge_8wekyb3d8bbwe | RegBinary | 87-7D-E4-96-3... |
| Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe | RegBinary | 54-C8-8E-EC-B... |
| Microsoft.Windows.Apprep.ChxApp_cw5n1h2bxyewy | RegBinary | 78-4D-56-B0-1... |
| Microsoft.Windows.CloudExperienceHost_cw5n1h2bxyewy | RegBinary | 89-91-2B-70-3... |
| Microsoft.Windows.Cortana_cw5n1h2bxyewy | RegBinary | F9-30-8D-38-3... |
| Microsoft.Windows.SecHealthUI_cw5n1h2bxyewy | RegBinary | E9-9A-4B-64-A... |
| Microsoft.Windows.ShellExperienceHost_cw5n1h2bxyewy | RegBinary | 08-79-F2-2D-1... |
| Microsoft.WindowsCalculator_8wekyb3d8bbwe | RegBinary | 42-38-EC-80-1... |
| Microsoft.WindowsCommunicationsApps_8wekyb3d8bbwe | RegBinary | CB-0F-43-D0-E... |
| Microsoft.WindowsStore_8wekyb3d8bbwe | RegBinary | 43-21-AF-38-3... |
| Microsoft.Xbox.TCUI_8wekyb3d8bbwe | RegBinary | 85-81-F1-0B-D... |

| Type viewer | Slack viewer |
|-------------|--|
| 00000000 | 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 |
| 00000011 | 87 7D E4 96 38 AE D3 01 00 00 00 00 00 00 00 01 |
| | 00 00 00 02 00 00 00 |

| | |
|------------------|------------------------------------|
| Value to Decode: | 877DE49638AED301 |
| Date & Time: | Sun, 25 February 2018 13:00:19 UTC |

So is it really the last executed time?

Let's check Notepad++:

| | | |
|--|-----------|---------------------------------|
| \\Device\\Harddisk\\Volume6\\Program Files (x86)\\Microsoft Office\\Office15\\EXCEL.EXE | RegBinary | F2-65-C7-A3-E8-AE-D3-01-00-0... |
| \\Device\\Harddisk\\Volume6\\Program Files (x86)\\Microsoft Office\\Office15\\OUTLOOK.EXE | RegBinary | 46-2F-EF-7D-EA-AE-D3-01-00-0... |
| \\Device\\Harddisk\\Volume6\\Program Files (x86)\\Microsoft Office\\Office15\\POWERPNT.EXE | RegBinary | D3-91-08-D4-EA-AE-D3-01-00-0... |
| \\Device\\Harddisk\\Volume6\\Program Files (x86)\\Microsoft Office\\Office15\\WINWORD.EXE | RegBinary | C6-62-F3-73-EA-AE-D3-01-00-0... |
| \\Device\\Harddisk\\Volume6\\Program Files (x86)\\Notepad++\\notepad++.exe | RegBinary | B1-17-2E-75-EA-AE-D3-01-00-0... |

Here we see the last time Notepad++ was executed:

| Dates and times | |
|------------------------------------|---------------------|
| DOS FAT Time/date (32 bit) | n/a |
| DOS FAT Date/time (32 bit) | n/a |
| Unix/Posix (32 bit) | 2032-04-19 02:36:33 |
| Windows FILETIME (64 bit) | 2018-02-26 10:13:33 |
| OLE 2.0 Date/time (64 bit) | 1899-12-30 00:00:00 |
| Windows SYSTEM Date/time (128 bit) | n/a |

Checking the prefetch file for Notepad++ "20180226105227_NOTEPAD++.EXE-58F9F447.pf" we see the LastRunTimes:

```

"LastRunTimes": [
  "/Date(1519639953612)/",
  "/Date(1519635526664)/",
  "/Date(1519567502155)/",
  "/Date(1519565819395)/",
  "/Date(1519552612642)/",
  "/Date(1519548852955)/",
  "/Date(1519470063868)/",
  "/Date(1519462959596)/"
]

```

Where the last one decoded is

| | |
|------------------|--|
| Decode Format: | Unix: Millisecond Value |
| Example: | 1176469232719 |
| Value to Decode: | 1519639953612 |
| Date & Time: | Mon, 26 February 2018 10:12:33.612 UTC |

So we see that there is a small difference of about a minute between the two times.

At the NTuser.dat hive

“Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{E0325B96-8E38-472E-8985-BF103644A570}” key, the LastAccessedTime is 131641135535970000

| | | |
|------------------|----------|--|
| AppId | RegSz | {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Notepad+... |
| AppPath | RegSz | C:\Program Files (x86)\Notepad++\notepad++.exe |
| LastAccessedTime | RegQword | 131641135535970000 |
| LaunchCount | RegDword | 4 |

Which decodes to the same date/time as the Prefetch:

| | |
|----------------------------|---------------------|
| Unix/Posix (32 bit) | 2013-04-21 03:02:40 |
| Windows FILETIME (64 bit) | 2018-02-26 10:12:33 |
| OLE 2.0 Date/time (64 bit) | 1899-12-30 00:00:00 |

Similarly WINWORD, right above notepad++, has a value of ‘C6-62-F3-73-EA-AE-D3-01’

| Dates and times | |
|----------------------------|---------------------|
| DOS FAT Time/date (32 bit) | n/a |
| DOS FAT Date/time (32 bit) | 2029-06-06 14:31:38 |
| Unix/Posix (32 bit) | 2031-08-24 09:32:54 |
| Windows FILETIME (64 bit) | 2018-02-26 10:13:31 |
| OLE 2.0 Date/time (64 bit) | 1899-12-30 00:00:00 |

And the respective prefetch “20180226105236_WINWORD.EXE-CFE28797.pf” has a last run time of:

| | |
|------------------|--|
| Value to Decode: | 1519639928431 |
| Date & Time: | Mon, 26 February 2018 10:12:08.431 UTC |

And the same applies to NTuser.dat’s key of

Software\Microsoft\Windows\CurrentVersion\Search\RecentApps\{CF0E3775-86D6-4C41-AA89-761E587E42D5}\LastAccessedTime which has a value of 131641135284310000

| | | |
|------------------|----------|--|
| AppId | RegSz | {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Microsoft... |
| AppPath | RegSz | C:\Program Files (x86)\Microsoft Office\Office15\WINW... |
| LastAccessedTime | RegQword | 131641135284310000 |
| LaunchCount | RegDword | 15 |

| | |
|----------------------------|---------------------|
| Unix/Posix (32 bit) | 2005-04-30 09:29:20 |
| Windows FILETIME (64 bit) | 2018-02-26 10:12:08 |
| OLE 2.0 Date/time (64 bit) | 1899-12-30 00:00:00 |

Also with a small a difference of a minute and a few seconds.

What I deduce from this is that BAM might take from seconds to a few minutes (depending on system load ?) to update these entries.

The BAM entries are updated when Windows boots (or shuts down ?), after the programs/apps were executed, as seen from the last write timestamps of the SYSTEM hive:

| | | | |
|---|-------------------|-----|---------------------|
| ▼ | ROOT | 0 | 2018-02-26 10:19:48 |
| > | ActivationBroker | 0 | 2017-10-29 12:42:08 |
| ▼ | ControlSet001 | 0 | 2018-02-07 10:52:46 |
| > | Control | 12 | 2018-02-26 10:19:53 |
| > | Enum | 139 | 2018-02-07 09:12:48 |
| > | Hardware Profiles | 0 | 2018-02-26 10:19:48 |
| > | Policies | 0 | 2018-02-07 08:15:31 |
| ▼ | Services | 0 | 2018-02-26 10:16:42 |

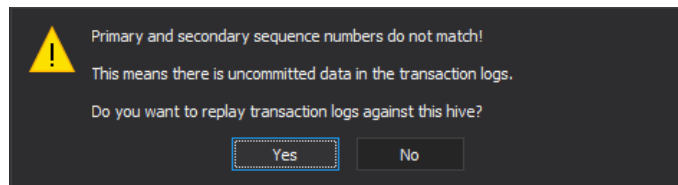
And of the bam\UserSettings\{userSID} key:

| | | | |
|---|---|-----|---------------------|
| ▼ | bam | 6 | 2018-02-03 21:23:42 |
| ▼ | UserSettings | 0 | 2018-02-22 23:05:35 |
| > | S-1-5-18 | 7 | 2018-02-26 10:16:49 |
| > | S-1-5-21-811833292-1881212584-745805... | 160 | 2018-02-26 10:19:57 |

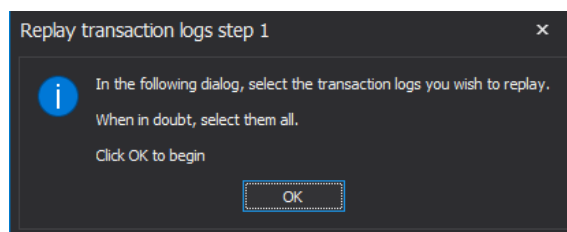
Update 5 March 2018:

The release of [Registry Explorer](#) 1.0 by Eric Zimmerman, allows to load the uncommitted data contained in the registry transaction logs (.LOG1 and .LOG2).

So loading the SYSTEM hive gives this message:



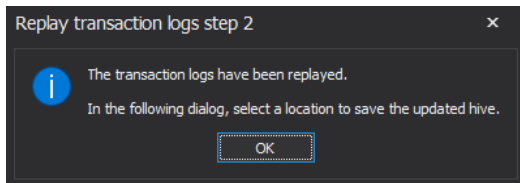
And selecting Yes:



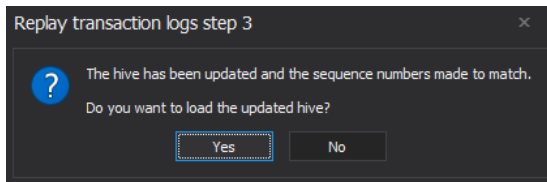
*Note: If exporting these files with FTK imager, you may need to change their attributes with the attrib -H -S *.* from a command console.*

We can pick the two LOG files:





After saving the updated SYSTEM hive, we now are asked if we want to load it:



Let's check the FTK imager in the Bam key's user settings in the updated SYSTEM hive. It has a UTC execution time of:

| | |
|--|---------------------|
| Microsoft.Windows.Common-UI\Winlogon\Exec | 2018-03-05 08:24:07 |
| \Device\HarddiskVolume6\Program Files\AccessData\FTK Imager\FTK Imager.exe | 2018-03-05 08:24:45 |
| \Device\HarddiskVolume2\Forensic Tools\RegistryExplorer_RECnd\RegistryExplorer.exe | 2018-03-05 08:24:07 |

Checking the Prefetch for FTK Imager

| | |
|--------------|-----------------------|
| LastRunTimes | 8 |
| | \Date(1520238284184)\ |
| | \Date(1520148351195)\ |
| | \Date(1520083764426)\ |

we see a last run time of 1520238284184 which translates to (UTC):

| Original | date | format |
|---------------|----------------------|-------------------|
| 1520238284184 | 05-Mar-18 8:24:44 am | Unix milliseconds |

So we see there is now a difference of 1 second in the two execution times.

So what is BAM?

Bam is a service that Controls activity of background applications. This service exists in Windows 10 only after Fall Creators update - version [1709](#) (needs checking when it was first introduced).

For example a machine running Windows 10 version 15063 (as seen at the Software hive's key "Microsoft\Windows NT\CurrentVersion")

| | | |
|---------------------------|----------|--|
| BuildLabEx | RegSz | 15063.0.amd64fre.rs2_release.170317-1834 |
| CompositionEditionID | RegSz | Core |
| CurrentBuild | RegSz | 15063 |
| CurrentBuildNumber | RegSz | 15063 |
| CurrentMajorVersionNumber | RegDword | 10 |
| CurrentMinorVersionNumber | RegDword | 0 |

Does not have a Bam service listed in "ControlSet001\Services\" at the System hive

| | | |
|----------------|----|---------------------|
| > b06bdrv | 8 | 2017-07-30 07:38:09 |
| > BasicDisplay | 7 | 2017-07-30 08:04:33 |
| BasicRender | 7 | 2017-07-30 08:04:01 |
| BattC | 1 | 2017-07-30 07:38:09 |
| bcmfn2 | 8 | 2017-07-30 07:38:09 |
| > BDESVC | 10 | 2017-07-30 08:25:14 |
| Beep | 6 | 2017-07-30 07:38:09 |

We can see the service status with the sc command:

```
C:\WINDOWS\system32>sc query bam

SERVICE_NAME: bam
        TYPE               : 1  KERNEL_DRIVER
        STATE                : 4  RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE   : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

```
C:\WINDOWS\system32>sc qc bam
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: bam
        TYPE               : 1  KERNEL_DRIVER
        START_TYPE          : 1  SYSTEM_START
        ERROR_CONTROL       : 1  NORMAL
        BINARY_PATH_NAME    : system32\drivers\bam.sys
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : Background Activity Moderator Driver
        DEPENDENCIES        :
        SERVICE_START_NAME  :
```

The bam.sys driver is found in the “%WinDir%\system32\drivers” folder.

In the COMPONENTS registry hive at the

“DerivedData\Components\amd64_microsoft-windows-b..ndactivitymoderator_31bf3856ad364e35_10.0.16299.192_none_e2a8303682e9dcc6”

key, we can see some more info on the bam.sys driver:

| | | | |
|--|-----------|--------------------|-------------|
| c1cbf7c3cd7a7..b24bec58e1_31bf3856ad364e35_10.0.16299.192_21f3221b1cde9375 | RegBinary | | |
| CF | RegDword | 2048 | |
| fibam.sys | RegDword | 65 | |
| identity | RegBinary | 4D-69-63-72-6F-... | 00-35-00 |
| S256H | RegBinary | FC-14-27-94-49-... | 61-00-5A-00 |

| Type viewer | Slack viewer |
|-------------|---|
| 00000000 | 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 |
| 00000012 | 4D 69 63 72 6F 73 6F 66 74 2D 57 69 6E 64 6F 77 73 2D |
| 00000024 | 4D 6F 64 65 72 61 74 6F 72 2C 20 43 75 6C 74 75 72 65 |
| 00000036 | 3D 6E 65 75 74 72 61 6C 2C 20 56 65 72 73 69 6F 6E 3D |
| 00000048 | 31 30 2E 30 2E 31 36 32 39 39 2E 31 39 32 2C 20 50 75 |
| 0000005A | 62 6C 69 63 48 65 79 54 6F 6B 65 6E 3D 33 31 62 66 33 |
| 0000006C | 38 35 36 61 64 33 36 34 65 33 35 2C 20 50 72 6F 63 65 |
| 0000007E | 73 73 6F 72 41 72 63 68 69 74 65 63 74 75 72 65 3D 61 |
| 00000090 | 6D 64 36 34 2C 20 76 65 72 73 69 6F 6E 53 63 6F 70 65 |
| 000000A2 | 3D 4E 6F 6E 53 78 53 |

Microsoft-Windows-BackgroundActivityModerator, Culture=neutral, Version=10.0.16299.192, PublicKeyToken=31bf3856ad364e35, ProcessorArchitecture=amd64, versionScope=NonSxS

Similarly in the Amcache hive at:

"\\InventoryDriverBinary\\c:/windows/system32/drivers/bam.sys"

| | | |
|-------------------------|----------|--|
| DriverChecksum | RegDword | 105414 |
| DriverCompany | RegSz | Microsoft Corporation |
| DriverId | RegSz | 00004bf81bb5a8e2bf36bcc6137033293c5f719cb... |
| DriverInBox | RegSz | 1 |
| DriverIsKernelMode | RegSz | 1 |
| DriverLastWriteTime | RegSz | 01/01/2018 12:51:59 |
| DriverName | RegSz | bam.sys |
| DriverPackageStrongName | RegSz | |
| DriverSigned | RegSz | 1 |
| DriverTimeStamp | RegDword | 2422666894 |
| DriverType | RegDword | 8650778 |
| DriverVersion | RegSz | 10.0.16299.192 |
| ImageSize | RegDword | 81920 |
| Inf | RegSz | |
| Product | RegSz | Microsoft® Windows® Operating System |
| ProductVersion | RegSz | 10.0.16299.192 |
| Service | RegSz | bam |
| WdfVersion | RegSz | |

Happy hunting :)