Dumbo v3.0

User Guide

6 July 2015

Table of Contents

1.0 Overview

The program is meant to be executed directly from a USB thumb drive, and requires being run as SYSTEM. Dumbo will log all actions, taken either automatically or manually, in a file called "log.txt" located in the same folder as the program's execution. Dumbo will also log all processes running at the start of its execution in a file called "proclist.txt" located in the same folder as the program's execution.

GUI.exe: Main executable for Dumbo v3.0. Requires being run as SYSTEM. If run as Administrator, the program will attempt to restart itself as SYSTEM. This file can be renamed as desired.

GUI.exe Command-Line Options:

- -n : do not take automatic actions on network or Bluetooth adapters

scanner.sys: Driver necessary for program to run correctly on 32 bit Windows XP. Driver will automatically be installed and removed, if necessary. Driver must be named "scanner.sys" and be located in the same folder as the main executable. The driver is not needed, and will not be installed, on any operating system other than 32 bit Windows XP.

wscupd.exe: Executable used to shutdown 32 bit operating systems. This file must be named "wscupd.exe" and be in the same folder as the main executable.

wermgr.exe: Executable used to shutdown 64 bit operating systems. This file must be named "wermgr.exe" and be in the same folder as the main executable.

2.0 Getting Started

2.1 Pre-Execution

Operating System Requirements:
Dumbo supports 32bit Windows XP, Windows Vista, and newer versions of Windows operating system. 64bit Windows XP, or Windows versions prior to XP, are not supported.

If run on an unsupported operating system, the program will not attempt to do any of its features. A warning will display, informing the user that the current operating system is not supported, and the program will exit after the message is accepted.

Execution Requirements:
Dumbo requires being run as SYSTEM. If the program is run with Administrator privileges, it will automatically attempt to restart itself as a SYSTEM process.

If Dumbo fails to restart itself as SYSTEM, or if the program was run as an unprivileged user, a warning will display, informing the user that Dumbo requires SYSTEM level execution, and the program will exit after the message is accepted.

2.2 Execution

- Run the program from a SYSTEM level cmd.exe shell
  - Add a '-n' switch to the command-line to prevent automatic actions on network and Bluetooth adapters
  - If run with Administrator privileges, the program will automatically attempt to restart itself as SYSTEM.
- A loading bar will appear as initialization occurs
- After loading, a new window will appear with the following four tabs:
  - System Info
  - Network
  - Camera & Microphone
  - Exit Options

2.2.1 System Info Tab

The "System Info" tab displays the following information:

- Computer Name
- Operating System and Service Pack
- Processor Architecture (x86 vs x64)
- Table of logical drive letters including the following details:
  - Free Space (MB)
  - Drive's Capacity (MB)

    - Percentage of free space remaining on drive
    - **Note**: The entries in this table are polled and updated every second.

This tab does not contain any interactive components.

2.2.2 Network Tab

The “Network” tab displays the following information:

- Table of network adapters including the following details:
    - Adapter Name (ex. “Local Area Connection”)
    - Device Name (ex. “Intel Gigabit Network Connection”)
    - Initial status of adapter, before program gained execution
    - Current status of adapter
- Inbound and outbound network traffic rates (KB/s)

Note: The information in the network adapter table, as well as the network traffic rates, are polled and updated every second.

Each row in the network adapter table is color-coded based on the adapter’s current status. The colors have the following statuses associated with them:

Color	Current Status
Green	Adapter is disabled
Orange	Adapter is enabled, but disconnected
Red	Adapter is connected
Gray	Status is unknown value

The Network tab has several interactive components. To selectively interact with a single network adapter, right-click an adapter in the table and select from the menu that appears. The selected adapter, for which the action would be applied to, will be highlighted blue in the table.

If Dumbo is ever unable to complete an action upon a network adapter, a warning message will be displayed to the user that the action failed.

2.2.3 Camera & Microphone Tab

The “Camera & Microphone” tab displays the following information:

- Number of camera devices detected
- Status of all microphones (muted or unmuted)
- Table of processes using the selected camera and their statuses
- Table of all files with write-permission detected and their statuses

A list of camera devices are displayed on the left by their unique device name. By default, the last camera detected is selected. The currently selected camera device is highlighted in blue and filters which processes and files with write-permission are displayed on the right of the screen. To ensure all files and processes are viewed and considered, the user must filter through all detected camera devices!

Processes Using Selected Camera Table

This table contains the following information:

- Path to the process' binary
- Process Unique Identifier (PID)
- Status of the process (Running, Suspended, or Terminated)

Entries in the "Processes" table are color-coded with the following scheme:

Color	Meaning
Green	The process is currently suspended
Red	The process is running
Gray	The process has been terminated, and the PID is no longer valid

The "Processes" table is interactive. The currently selected entry in the table is highlighted blue. Right-clicking an entry in the table will display a menu with the several options.

Files with Write-Access Table

This table contains the following information:

- Path to the file
- Last time the file's been written to
  - ISO 8601 format (Year-Month-Day 24Hour:Minutes:Seconds)
- If the file has ever been modified by this instance of Dumbo (Yes/No)

Entries in the "Files" table are color-coded with the following scheme:

Color	Meaning
Green	The file has been modified, but still exists
Orange	The file has not been modified
Gray	The file has been deleted, and the path is no longer valid

The "Files" table is interactive. The currently selected entry in the table is highlighted blue. Right-clicking an entry in the table will display a menu with several options.

A deleted file (whose entry should be color-coded gray) cannot be "shown in folder".

Microphones Section

The microphone section is located in the bottom left corner of the "Camera & Microphone" tab. This section displays whether all microphones are muted, or if at least one microphone is unmuted.

2.2.4 Exit Options Tab

The "Exit Options" tab is broken into two subsections, based on the desired exiting method

Exit Delay

The "Exit Delay" subsection of the Exit Options tab displays the following information:

- **Restoration Time** – the time that the system will be restored to its original status. This time is calculated by adding the system's current time and the number of minutes to delay.
    - **Note:** Since the restoration time is dependent on the system's clock, if the system has an incorrect time setting, the restoration time will be incorrect as well.
- **Delay Timer** – the number of minutes to delay before restoring the system to its original state. The default value is 7 minutes.

An user may adjust the default delay time by clicking the up or down arrows next to the box, manually enter a value, or by using the mouse-wheel if the box has focus. The maximum delay time is 99 minutes, and the minimum time is 0 minutes (no delay).

If the user clicks the "Start Exit Delay" button, Dumbo will hide its window and wait the prescribed delay amount. If the user closes ("X") the window at any time, Dumbo will wait the delay amount as well.

Shut Down

The other subsection of the Exit Options tab displays how much memory will be written before shutdown, if an entry in the system event log will be created, and if the system will automatically reboot.

Table of Shut Down Color Codes	
Color	**Meaning**
Green	No memory will be written
Yellow	A minimal amount of memory is written
Orange	All kernel memory is written
Red	All memory is written

Note: It is recommended that the shutdown exit option not be exercised on systems with a full setting enabled.

If the user clicks the button to initiate this exiting method, the program will ask for a confirmation. If confirmed, and Dumbo is successful, the program will exit and a shutdown should occur within 15 seconds.

If Dumbo is unsuccessful, a warning will be displayed to the user that it failed.

2.3 Logging Details

Dumbo maintains a verbose log of all actions taken either automatically or manually by the user. The log is stored in a file called "log.txt" and is located in the same directory as the program's execution. For the log to be maintained, the thumb drive Dumbo is executed from must remain plugged into the system throughout the duration of the operation. Dumbo will not report failed logging attempts if the drive is removed.

All logging entries are preceded by an ISO 8601 UTC timestamp, ex.:

```
[Year-Month-Day Hour:Minutes:Seconds UTC]
```

Logging entries are also preceded by a header labeling the sentiment of the log entry. Dumbo's log is constantly appended to at the end of the file. If the program is run on the same thumb drive, across multiple uses, without cleaning the log file, the log will maintain the entries from all uses.

2.4 Additional Notes

In some instances, programs emulate a camera input to other programs; such is the case with Fujitsu's YouCam.exe. When this occurs, YouCam.exe will have control of the actual webcam, and feed input to other processes as needed. In this scenario, Dumbo may not output meaningful details related to files.

Dumbo has the capability to detect only files are were being written at the moment of its execution. Previously saved files will not be detected.

If another program attempts to use a camera while Dumbo is running, it will not function properly due to the camera already being in use.