Dumbo v3.0
User Guide
25 June 2015

CL BY: 2428190
DECL: 25X1; 25 June 2040
DRV: CIA NSCG MET S-06

Table of Changes

Date	Change Description	Authority

(U) Table of Contents

Dumbo User Guide

1.0 (U) Introduction

(S) Dumbo runs on a target to which we have physical access, mutes all microphones, disables all network adapters, suspends any processes using a camera recording device, and notifies the operator of any files to which those processes were actively writing so that they may be selectively corrupted or deleted.

1.1 (U) Requirement

(S) The Intelligence Community has identified the need (requirement 2015-OPS0001013) for a capability to suspend processes utilizing webcams and corrupt any video recordings that could compromise a PAG deployment.

1.2 (U) Purpose

(U) This User Guide describes how to use Dumbo v3.0.

2.0 (U) System Overview

(U) The tool is meant to be executed on a target machine directly from a USB thumb drive. The application requires being run as SYSTEM. Dumbo will log all actions taken either automatically, or manually by the operator, in a file called “log.txt” located in the same folder as the tool’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 tool’s execution.

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

GUI.exe Command-Line Options:

- -n : do not automatically disable network or Bluetooth adapters

scanner.sys: Driver necessary for tool 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 create a blue screen on 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 create a blue screen on 64 bit operating systems. This file must be named “wermgr.exe” and be in the same folder as the main executable.

3.0 (U) Getting Started

3.1 (U) Pre-deployment

Operating System Requirements:
(U) 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 tool will not attempt to do any of its features. A warning will display, informing the operator that the current operating system is not supported, and the tool will exit after the message is accepted.

Execution Requirements:
(U) Dumbo requires being run as SYSTEM. If the tool 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 tool was run as an unprivileged user, a warning will display, informing the operator that Dumbo requires SYSTEM level execution, and the tool will exit after the message is accepted.

3.2 (U) Deployment

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

3.2.1 (U) 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.

Link to view a screenshot of the System Info tab

3.2.2 (U) 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 Dumbo 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. There are three buttons located below the network traffic rates:

- **Disable All** – Attempts to disable all network adapters in the table
- **Restore Initial** – Reverts the adapters to their initial state (enabled or disable), as shown in the table, before Dumbo gained execution
- **Network Connections** – Opens the Control Panel view of network adapters

To selectively enable or disable 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 enable or disable a network adapter, a warning message will be displayed to the operator that the action failed.

Link to view a screenshot of the Network tab

3.2.3 (U) 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 operator 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 following options:

- **Show in Folder** –
- **Suspend / Resume** – Attempt to suspend the process, if it is running, or resume it if it is suspended
- **Terminate** – Terminates the process

If Dumbo fails to terminate a process, a warning will be displayed to the operator.

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 corrupted 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 corrupted, but still exists
Orange	The file has not been corrupted
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 the following options:

- **Show in Folder** – open the file's location in Explorer with the file selected
- **Corrupt –** Writes random data to the entirety of the file, corrupting it
- **Corrupt and Delete –** Writes random data to the file, then deletes it from the system
- **Corrupt All** – Attempts to corrupt all files that are visible in the table
  - Selecting this option will prompt a confirmation request

A deleted file (whose entry should be color-coded gray) cannot be "shown in folder". If Dumbo fails to corrupt or delete any file, a warning will be displayed to the operator.

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 and could be actively recording.

To restore the microphones to their previous unmuted/muted state, before Dumbo gained execution, click on the "Restore Initial" button. If all microphones were muted before Dumbo gained execution, clicking the button will not have any effect. If at least one microphone is unmuted, the button will change to a "Mute All" option.

If Dumbo fails to mute any microphone, a warning will be displayed to the operator.

Link to view a screenshot of the Camera & Microphone tab

3.2.4 (U) Exit Options Tab

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

- Exit Delay
- Blue Screen

Exit Delay

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

- **Restoration Time** – the time that network adapters, microphones, and suspended processes will be restored to their 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 target 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 operator 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 operator clicks the "Start Exit Delay" button, Dumbo will hide its window and wait the prescribed delay amount. If the operator closes ("X") the window at any time, Dumbo will wait the delay amount as well.

Blue Screen

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

- **Crash Dump Setting** – informs the operator how much memory will be dumped in the event of a crash. Details on the possible options can be found below
- **Log Event** – If enabled, an entry that the system crashed will be created in the system's event log
- **Auto-Reboot** – If enabled, the system will automatically reboot after a crash. If disabled, the blue screen error message will remain on the screen until the system is manually rebooted.

Table of Crash Dump Settings		
Color	**Setting**	**Meaning**
Green	Disabled	No memory dump will occur on a crash
Yellow	Mini-dump	A minimal amount of memory is written to a file on crash
Orange	Kernel	All kernel memory is written on a crash (Default Value)
Red	Full	All memory is written to a file on crash

Note: The crash dump, log event, and auto-reboot settings are determined by reading registry values that are read only once, upon startup. Although unlikely, the system could have changed these values, but not have rebooted since the change. This would result in Dumbo reporting incorrect values.

(S) Note: Full crash dumps present a potential detection threat. Although it would be extremely difficult, a motivated actor could potentially attribute the blue screen to Dumbo, and subsequently reverse engineer the tool. Because of this, it is recommended that the blue screen exit option not be exercised on systems will a full crash dump setting enabled.

If the operator clicks the "Attempt Crash" button, the tool will ask for a confirmation. If confirmed, and Dumbo is able to create a blue screen crash scenario, the tool will exit and a blue screen should occur within 15 seconds.

If Dumbo is unable to create a blue screen crash scenario, a warning will be displayed to the operator that the attempt failed.

Link to view a screenshot of the Exit Options tab

3.3 (U) Logging Details

(U) Dumbo maintains a verbose log of all actions taken either automatically or manually by the operator. The log is stored in a file called "log.txt" and is located in the same directory as the tool'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 if the entry is good, bad, or simply informative. The following shows an example log excerpt:

```
[2015-06-24 20:10:17 UTC]         ==================== Started ====================
[2015-06-24 20:10:17 UTC] (INFO)  Operating System: Windows 7 Professional Service Pack 1
[2015-06-24 20:10:17 UTC] (INFO)  Computer Name: Example-PC
[2015-06-24 20:10:17 UTC] (INFO)  Computer Architecture: x64
[2015-06-24 20:10:17 UTC] (GOOD)  Disabled adapter: Local Area Connection
[2015-06-24 20:10:17 UTC] (GOOD)  Muted all microphones
[2015-06-24 20:10:17 UTC] (INFO)  Found a camera device, Friendly Name: Microsoft® LifeCam Cinema(TM)
[2015-06-24 20:10:18 UTC] (BAD)   Found a process using a camera! PID: 6020, Filename: C:\iSpy\iSpy.exe
[2015-06-24 20:10:18 UTC] (GOOD)  Suspended PID: 6020, Filename: C:\iSpy\iSpy.exe
[2015-06-24 20:10:18 UTC] (INFO)  Found a file with write-permission, Filename: C:\Recordings\video.mp4
[2015-06-24 20:10:23 UTC] (GOOD)  Corrupted file: C:\Recordings\video.mp4
[2015-06-24 20:10:23 UTC] (GOOD)  Deleted file: C:\Recordings\video.mp4
[2015-06-24 20:10:29 UTC] (INFO)  Began exit timer for 3 minutes
```

Dumbo's log is constantly appended to at the end of the file. If the tool is run on the same thumb drive, across multiple uses, without cleaning the log file, the log will maintain the entries from all uses.

3.4 (U) Additional Notes

Recording Software Crashes

(S) If Dumbo corrupts or deletes a file, the recording software using that file may crash upon being resumed. This is dependent on how the recording software handles the resulting error, and is impossible to detect beforehand.

Windows XP

(S) In order to function properly, Dumbo must install a device driver when running on Windows XP. Dumbo will handle this automatically, but the initialization process may take considerably longer to load in comparison to a user's experience with the tool on other operating systems.

Personal Security Products (PSPs)
(S) Kaspersky AV blocked the installation of the device driver necessary for Dumbo to function properly on XP. PSPs also often log processes that attempt to use a webcam, and Dumbo may cause interactive pop-up notifications altering the user that the tool is attempting to connect to the camera. Additionally, some PSPs were seen to prevent a fully functioning bluescreen exit option. Although no alerts were raised in this case, the exit functionality was blocked. Because of these potential hindrances, it is recommended that the operator consider disabling any PSP running on the target machine prior to running Dumbo. It is recognized that this choice has trade-offs, including that the system will explicitly log that the PSP was disabled, and should be considered on a case-by-case basis.

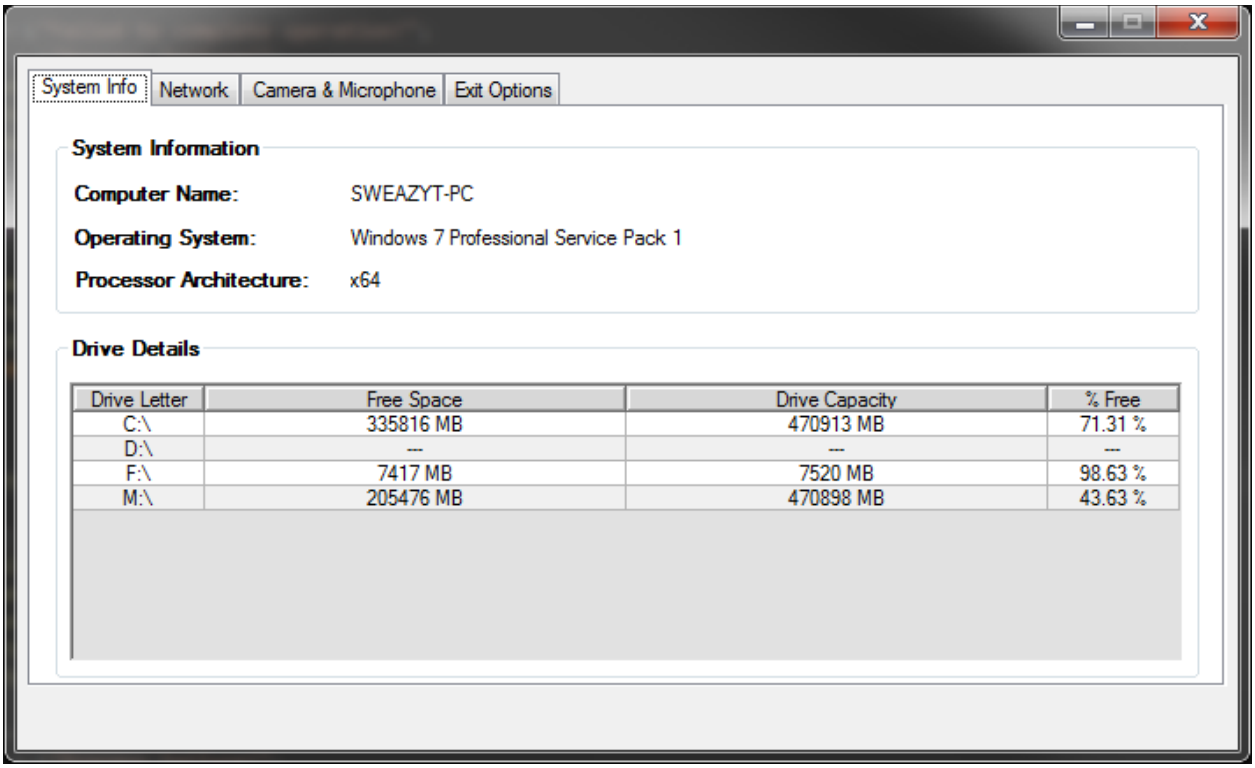
Camera Emulation
(S) Dumbo works by discovering which processes have access to the physical camera device and uses that information to corrupt video files. In some instances, programs emulate a camera input to other programs; such is the case with Fujitsu's YouCam.exe. When this occurs, YouCam.exe will have control of the actual webcam, and feed input to other processes that record images to files as needed. In this scenario, Dumbo will suspend YouCam.exe, but will not be able to detect the other processes to which YouCam.exe is feeding images. Although the camera will not be able to record additional frames, Dumbo will not be able to corrupt files that were being written to, as it is unaware of the processes writing the video files. If the operator sees a process using the camera device, but Dumbo detects no files being written, the operator should manually search for video files.

Previously Saved Files
(S) Dumbo has the capability to detect only files are were being written at the moment a recording program was suspended. Previously saved files such as earlier recordings or snapshot images will not be detected. If Dumbo detects a process using the camera, the operator should search around all reported files paths for potentially problematic prior recordings.

Recording Software Restarts
(S) In some instances, video recording software has the ability to detect it is not responding, and will restart itself; such is the case with iSpy.exe. When Dumbo detects a process using a camera device, it also claims control of the device. If the recording software were to restart itself, it would no longer be able to access the camera until Dumbo exits. In the case of iSpy, although the program may restart, it will be unable to record any additional frames; it will appear as if it was unable to access the camera, due to it already being in use.

4.0 (U) Sample Screenshots

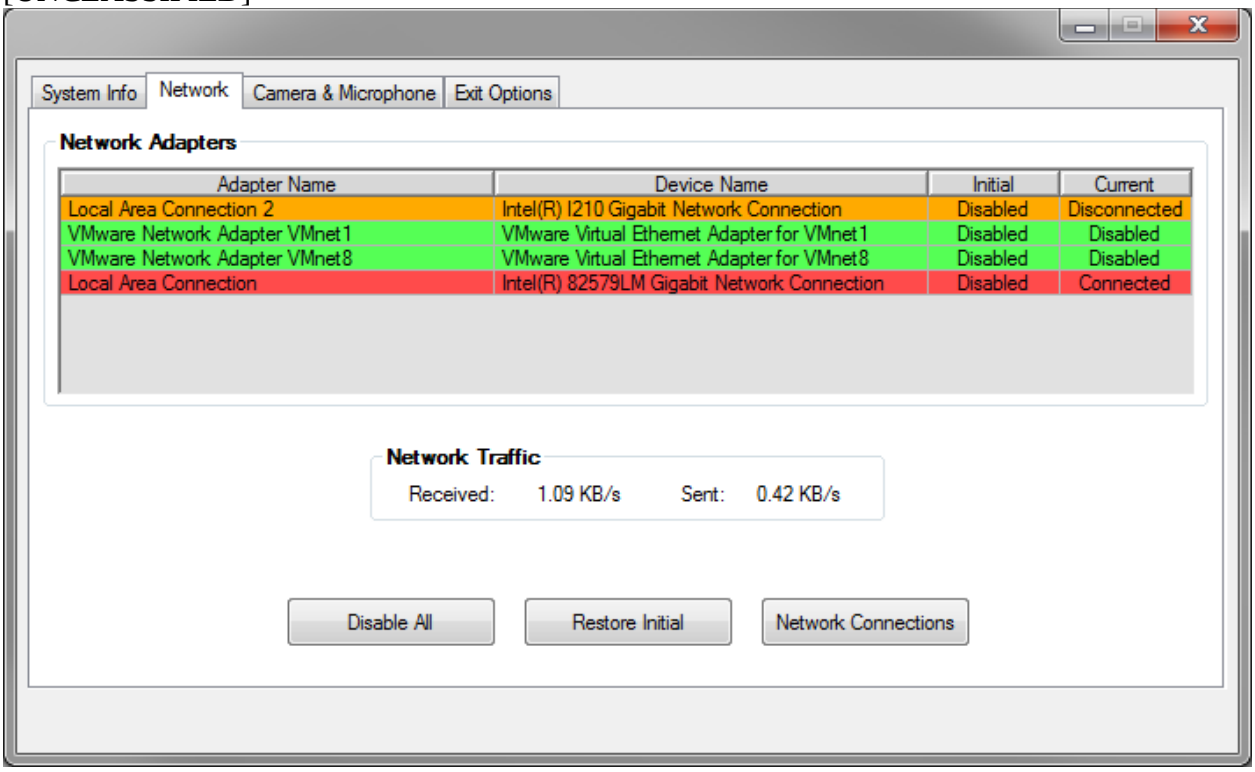
[UNCLASSIFIED]



[UNCLASSIFIED]

(U) This screenshot shows an example of the System Info tab. Basic system details are displayed on the top half of the tab, and logical drive information is displayed on the bottom. The “D” drive in the table is an empty CD-drive, and thus does not have any free space or capacity.

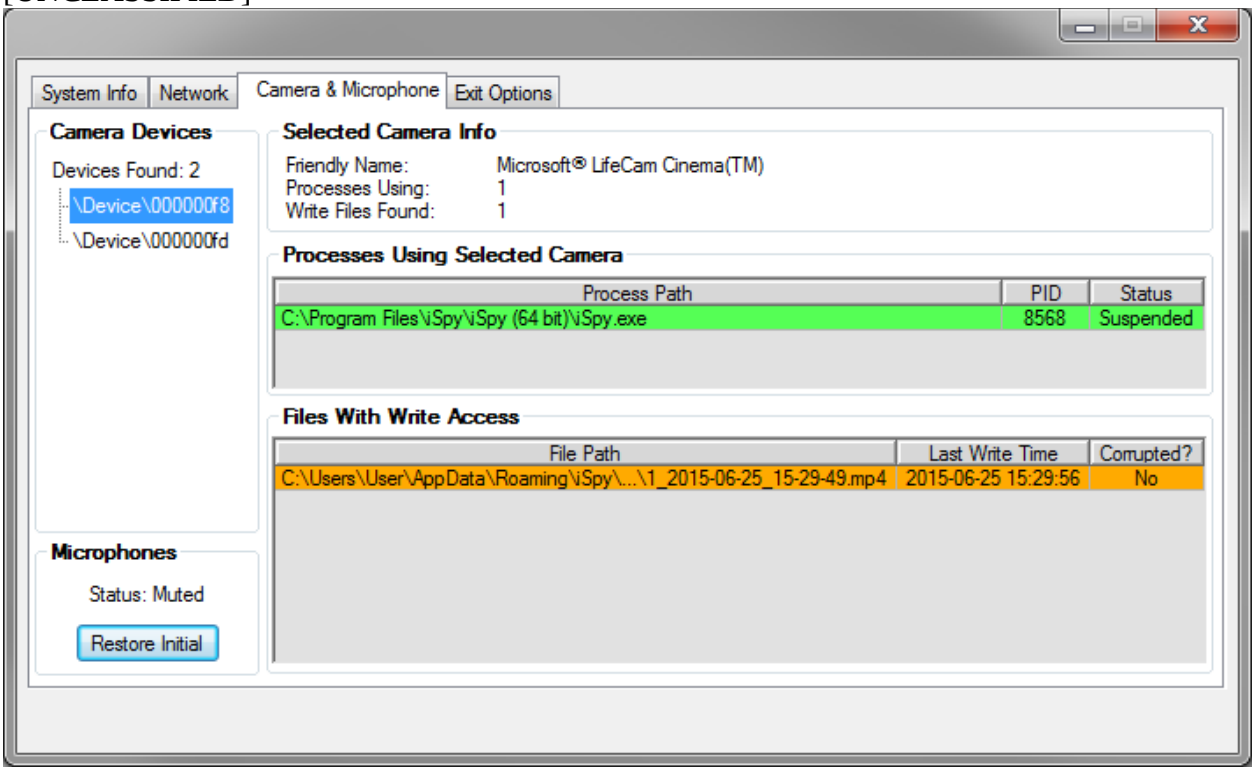
[UNCLASSIFIED]



[UNCLASSIFIED]

(U) This screenshot shows an example of the Network tab. The “Local Area Connection 2” adapter is an enabled Ethernet adapter that does not have a cable plugged into it; thus the adapter is in a ‘disconnected’ state. Both “VMware” adapters are disabled. The “Local Area Connection” adapter is enabled and connected. Because at least one adapter is connected, network traffic is able to flow, as shown by the traffic rate displays.

[UNCLASSIFIED]



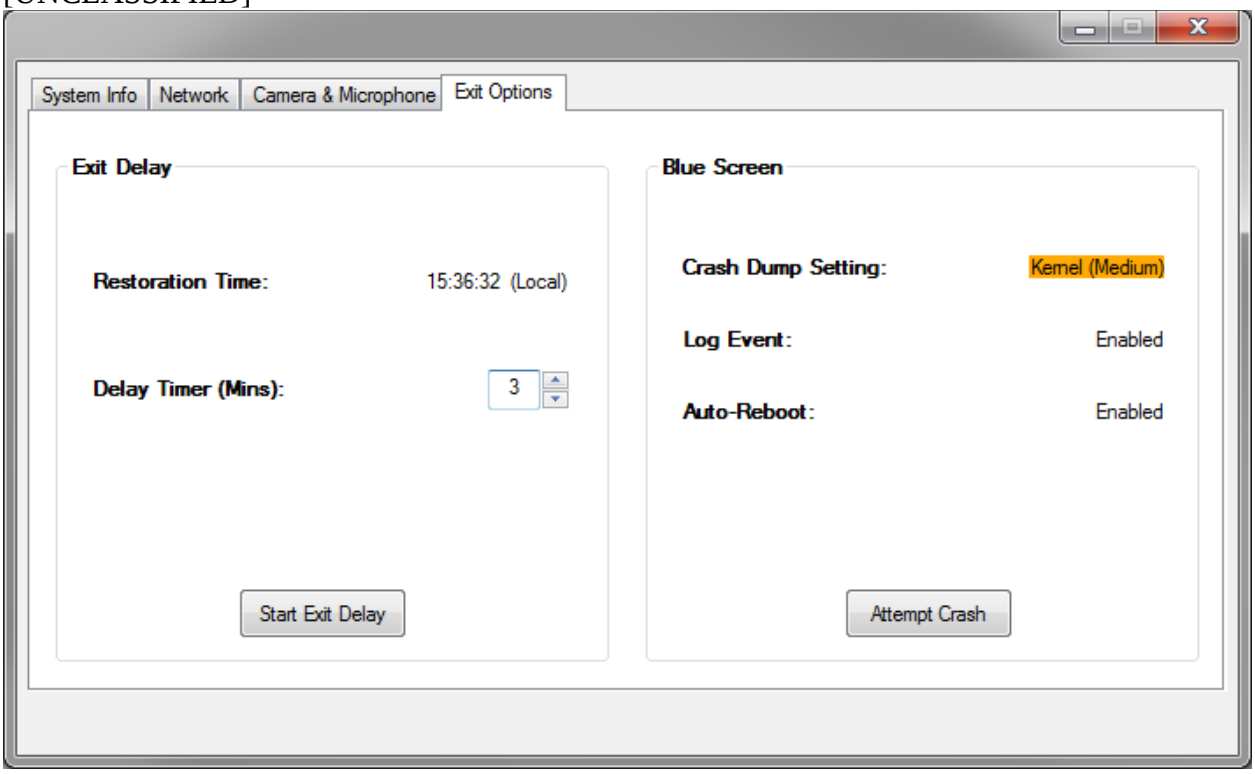
[UNCLASSIFIED]

(U) This screenshot shows an example of the “Camera & Microphone tab”. In this instance, there were two camera devices connected to the target system. The camera with device name “\Device\000000f8” is currently selected, and shows that a single process was using the device. The “Files” table shows that one file was being written to at the time Dumbo suspended the process. If multiple processes were using the camera device, all of the files with write-access found across the multitude of processes would be shown in the table.

(S) The last write time is shown to be a recent time, and is likely a suspect file that should be corrupted or deleted. The “.mp4” file extension is a known video format, and is another clue this file should not be left on disk.

(U) The screenshot also shows that all microphones are currently muted.

[UNCLASSIFIED]



[UNCLASSIFIED]

(U) This screenshot shows an example of the “Exit Options” tab.

(S) Because the crash dump setting isn’t a “Full” memory dump, this system represents a reasonable candidate on which to cause a blue screen. See the note in the “Exit Options” tab regarding the potential risk associated with a full memory crash dump.