Big Windows Log Collection Tool v1.1

Table of Contents:

Revision History:

Revision	History	Author
1.0	Tool supports ET5x, VC80, TC70x	ECRT team
1.1	Added ET51/ET56 Entries	ECRT Team

Introduction:

Big Windows log collection tool collects the logs from Windows 10, Windows 8.1 and Windows 7 machines.
This tool helps to get logs from TC70x Windows 10, VC80 Windows 7/10, ET50/55, ET51/56 Windows 8.1/ Windows 10 OS.

Following are the steps to collect logs using this tool

1) Copy BigWindowsLogCollectionTool.exe to device.
2) Run tool with admin privileges.
3) Select required check boxes to collect logs and click on Collect Logs button to collect logs.
4) It will collect logs to Logs folder in system directory (Ex: C:\Logs)
5) Click on OK or Cancel button to close the UI.
6) Click on About button to get Tool Version details.

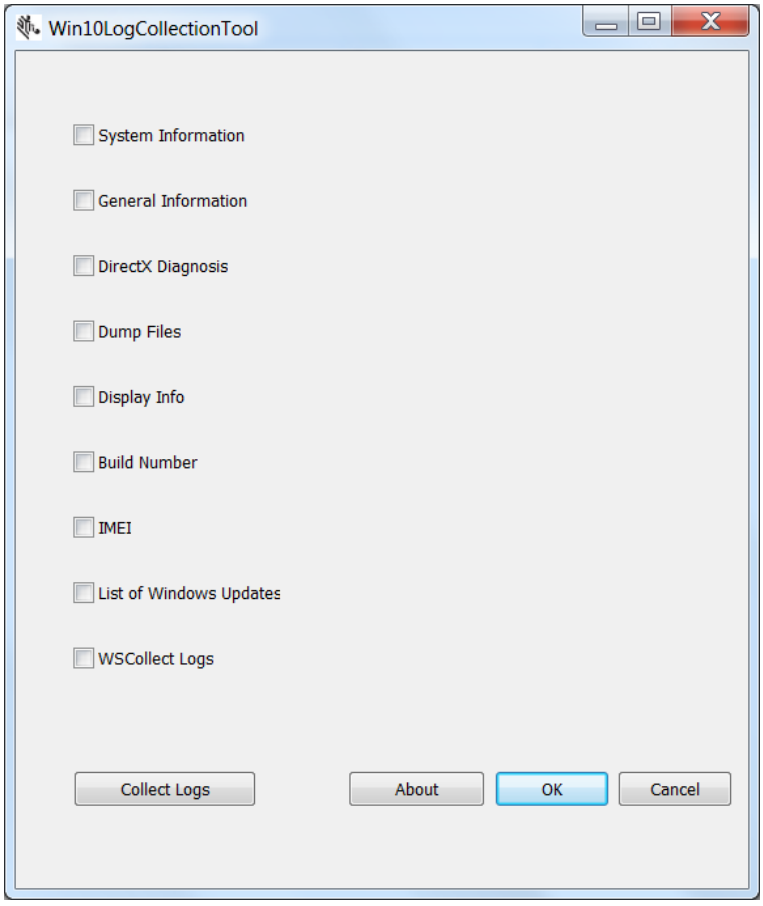


Figure (1): BigWindowsLogCollectionTool screenshot

Log Information:

Following are the list of logs this tool collects.

1. System Information:

This tool creates msinfo32.nfo file in system directory Logs folder (C:\Logs). MSINFO32 is Microsoft System Information tool.

Microsoft System Information tool collects system information, such as devices that are installed in your computer or device drivers loaded in your computer and provides a menu for displaying the associated system topics.

The information displayed in Microsoft System Information is divided into the following three categories:

- Hardware Resources
- Components
- Software Environment

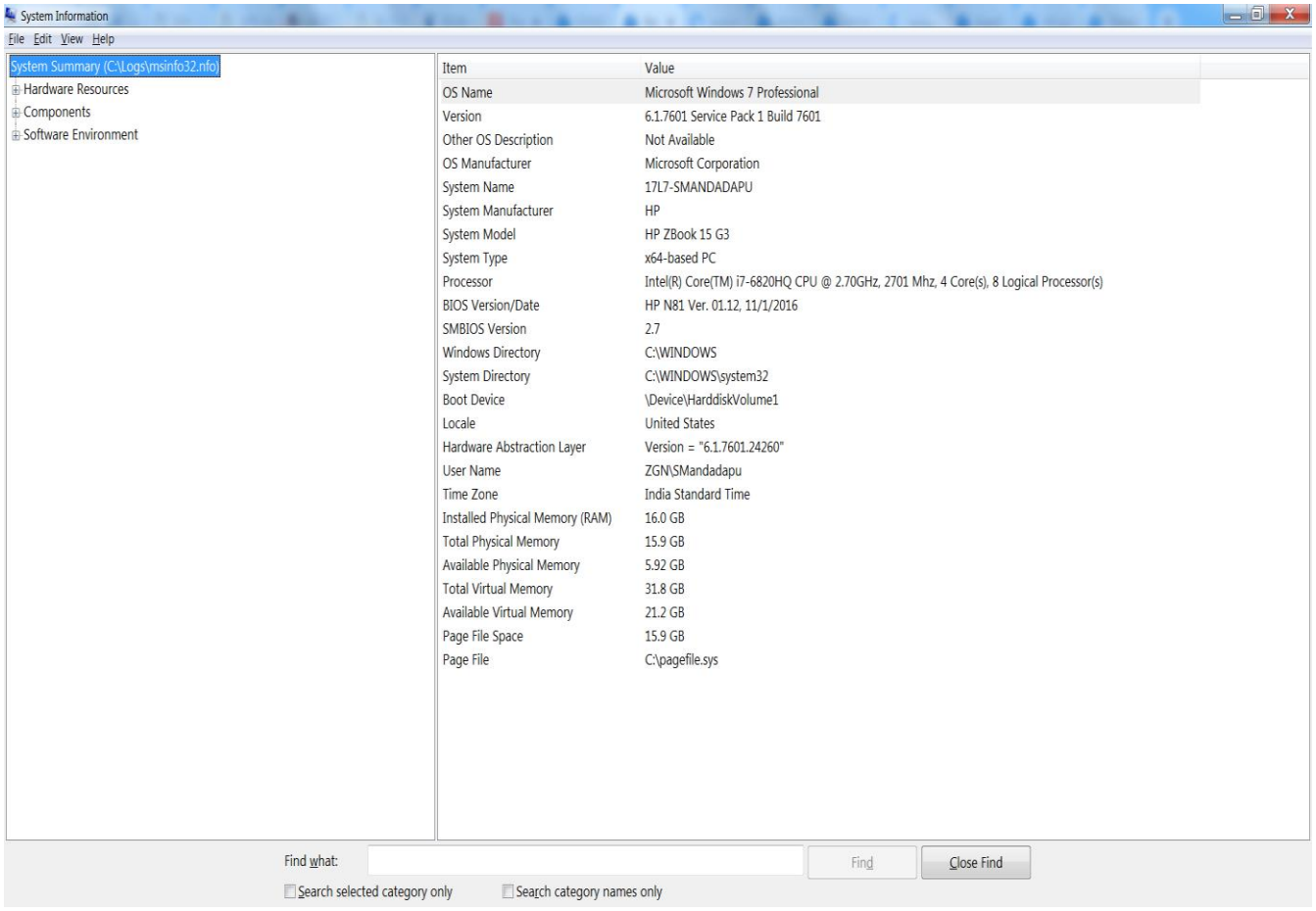


Figure (2): System Summary

System Summary:

The System Summary category provides a general file of your computer. This information includes:

- The version of Windows

- The version of Internet Explorer
- The type of central processing unit (CPU)
- The amount of memory and system resources
- Total and free hard disk space
- The file system for each partition

Use this information at the beginning of the troubleshooting process to develop a basic picture of the environment in which the issue occurs.

Hardware Resources:

The Hardware Resources category displays hardware-specific settings, such as assigned or used interrupt requests (IRQs), input/output (I/O) addresses, and memory addresses. The following list is the sub-categories included in the Hardware Resources category.

Conflicts/Sharing:

Lists the identified resource conflicts between Industry Standard Architecture (ISA) devices, and identifies resources shared by Peripheral Component Interconnect (PCI) devices. Use this information to help identify hardware conflicts.

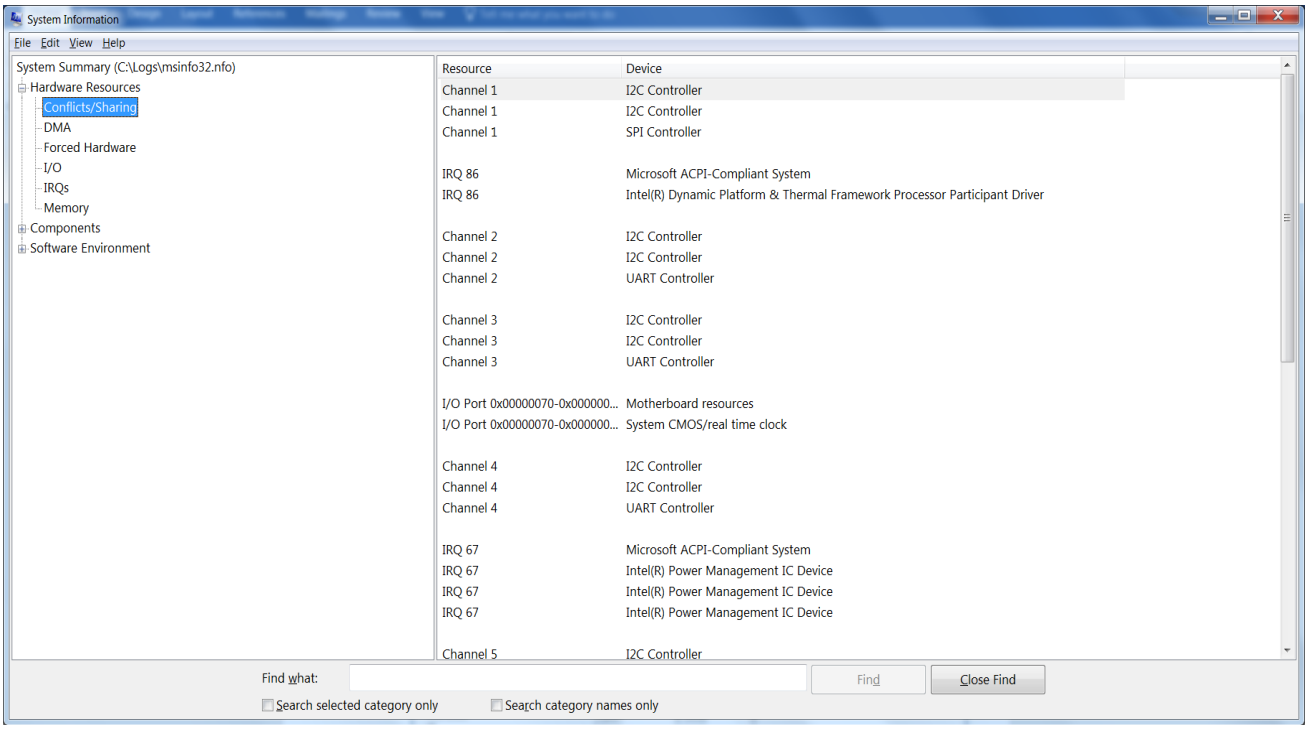


Figure (3): Conflicts/Sharing in Hardware Resources

DMA:

Reports the direct memory access (DMA) channels in use, the devices using them, and those that are free for use.

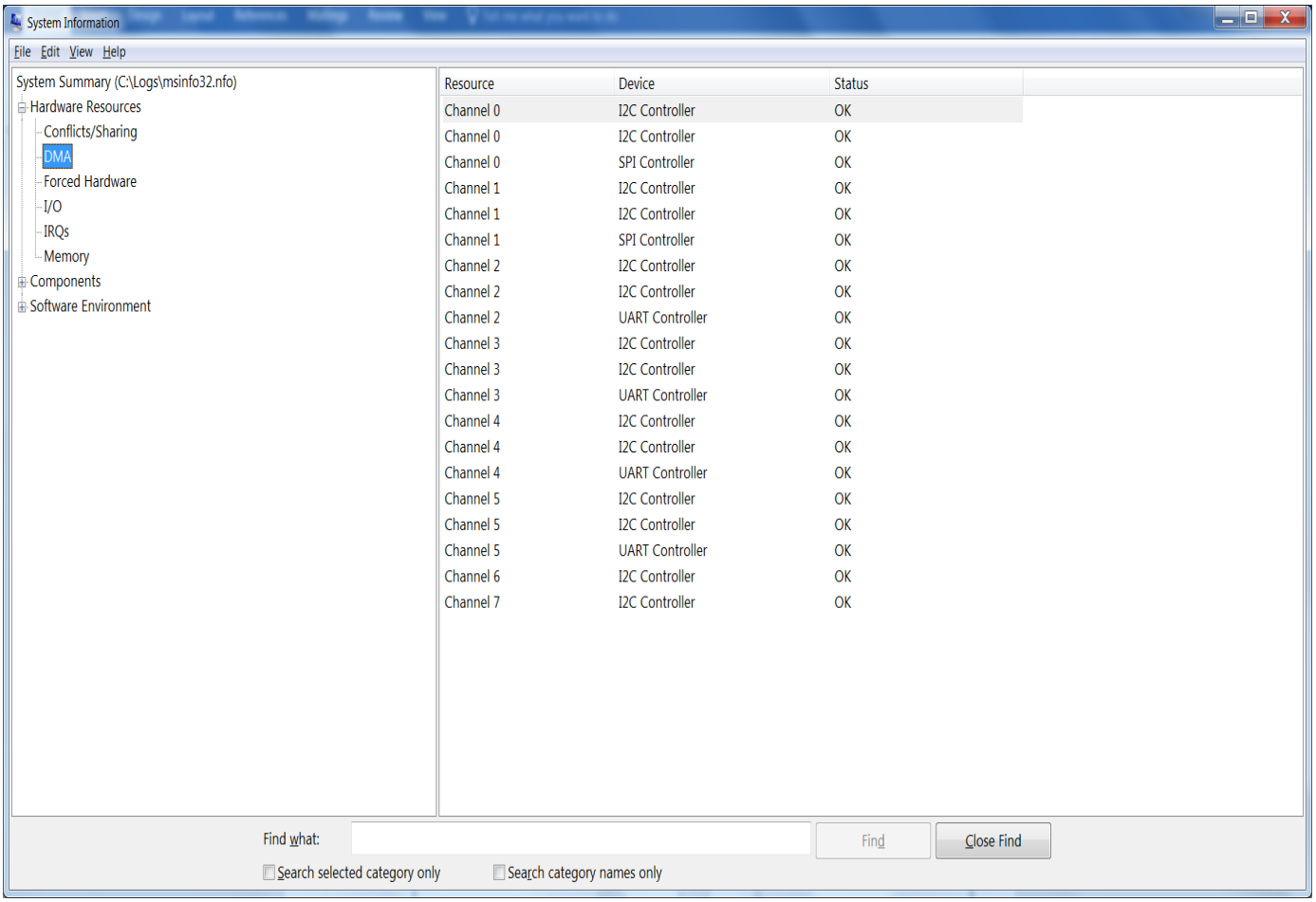


Figure (4): DMA in Hardware Resources

Forced Hardware:

Lists hardware devices in which the PnP configuration has been disabled and resource settings have been manually set to user-specified resources. Forced hardware would also apply to devices which do not participate in the PNP process such as legacy ISA devices. This information is useful when you want to troubleshoot Plug and Play resource conflicts.

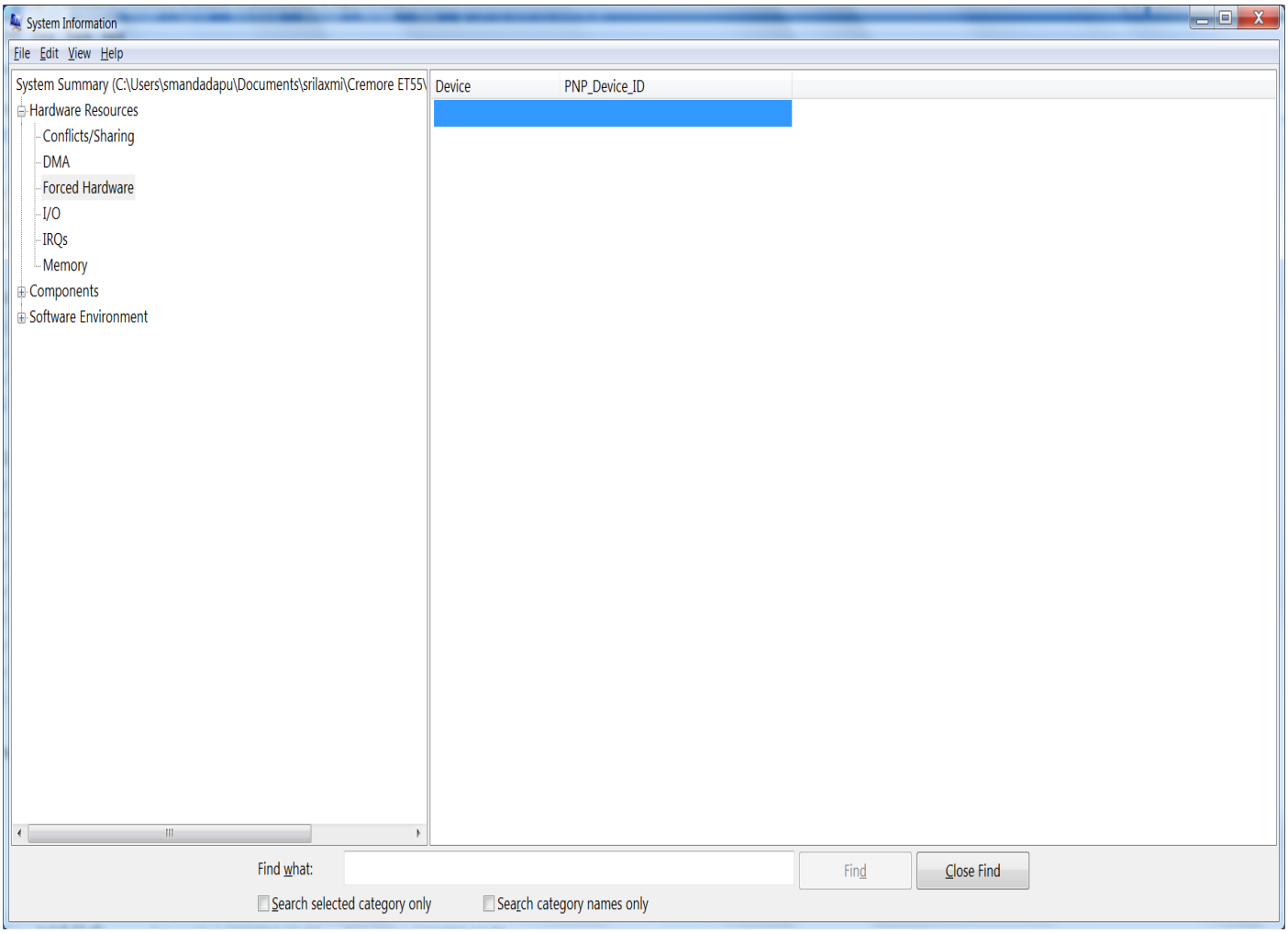


Figure (5): Forced Hardware in Hardware Resources

I/O:

Lists all I/O port ranges in use and the devices that are using each range.

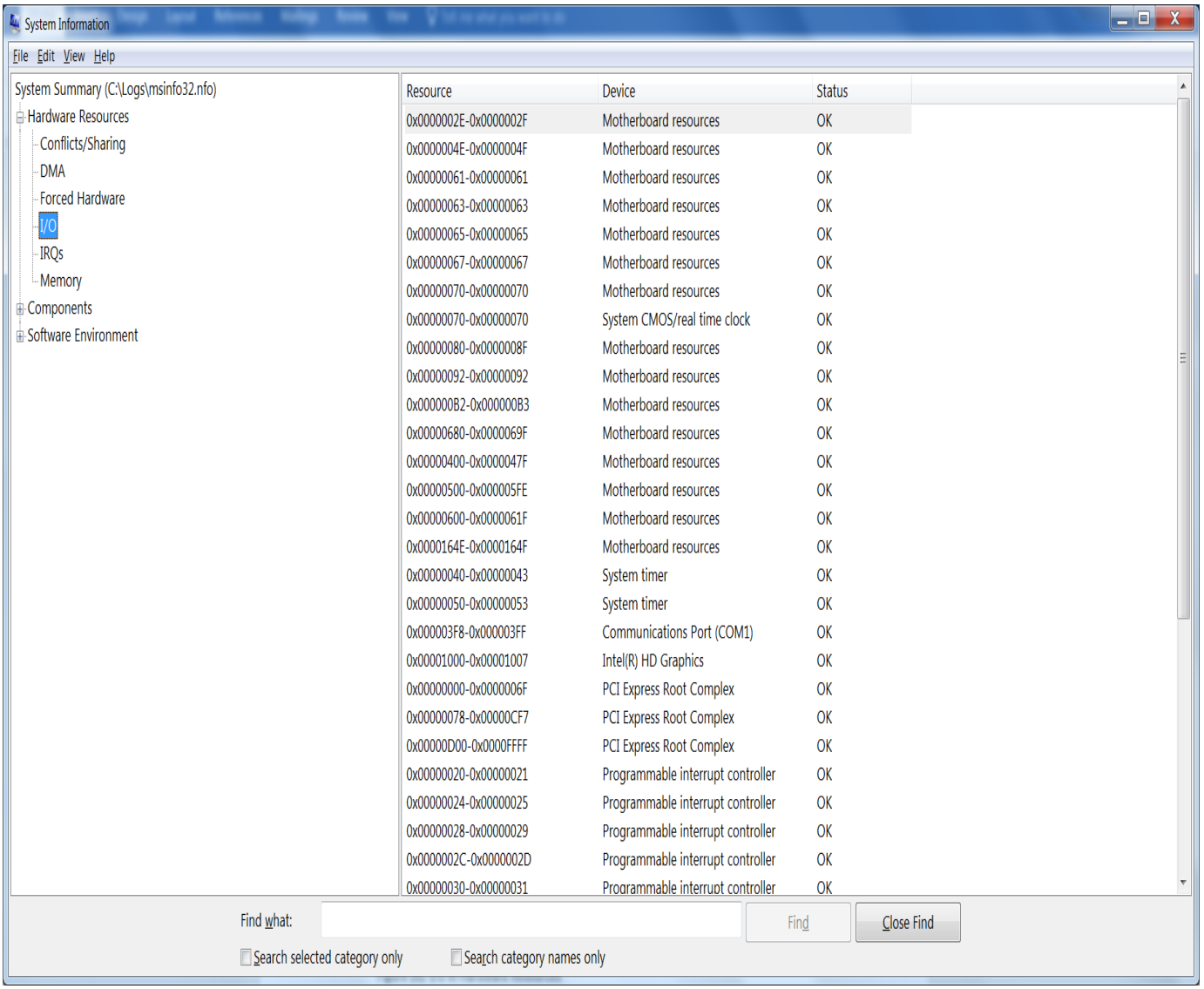


Figure (6): I/O in Hardware Resources

IRQs:

Summarizes IRQ usage, identifies the devices using the IRQs, and lists free IRQs.

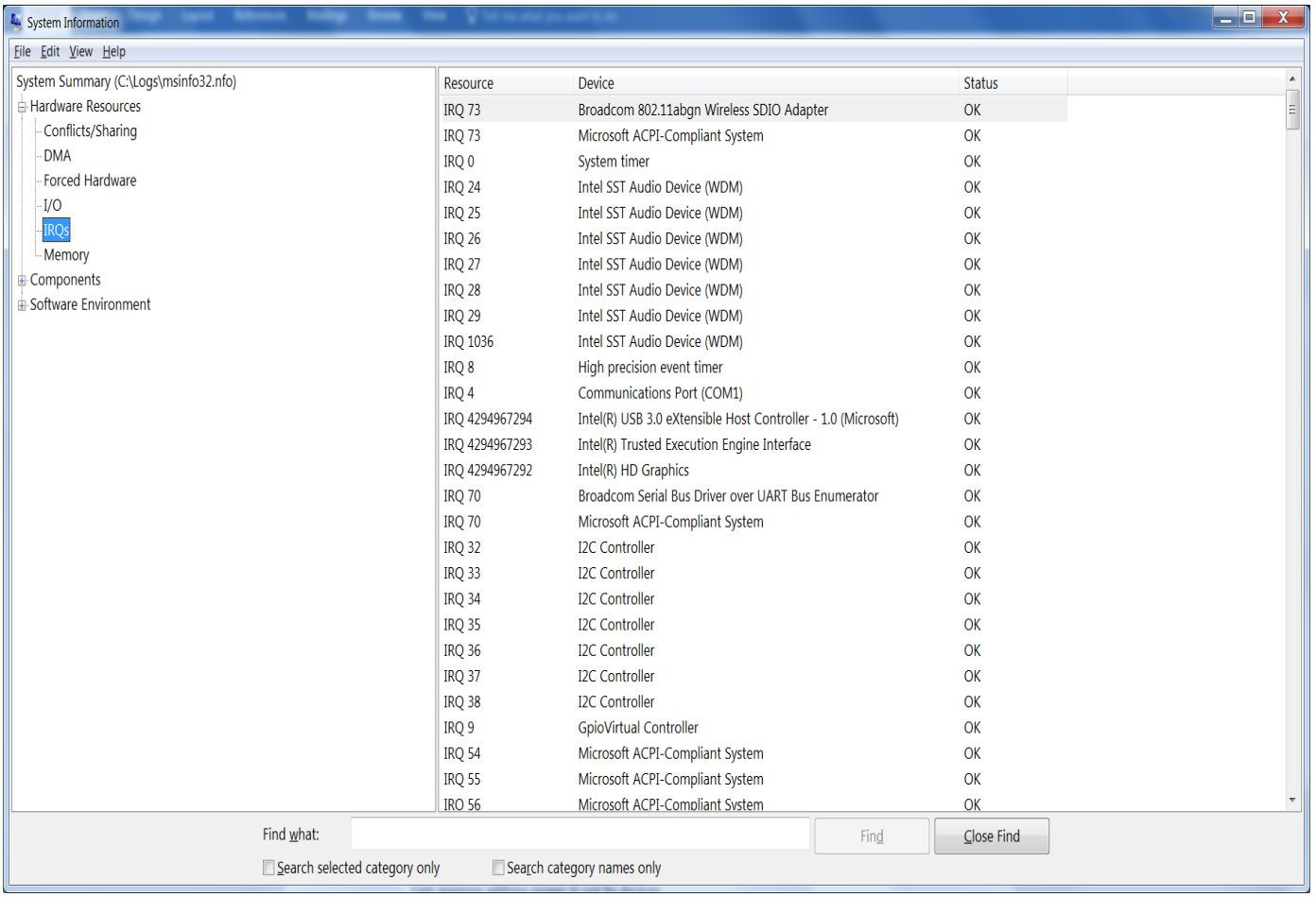


Figure (7): IRQs of Hardware Resources

Memory:

Lists memory address ranges in use by devices.

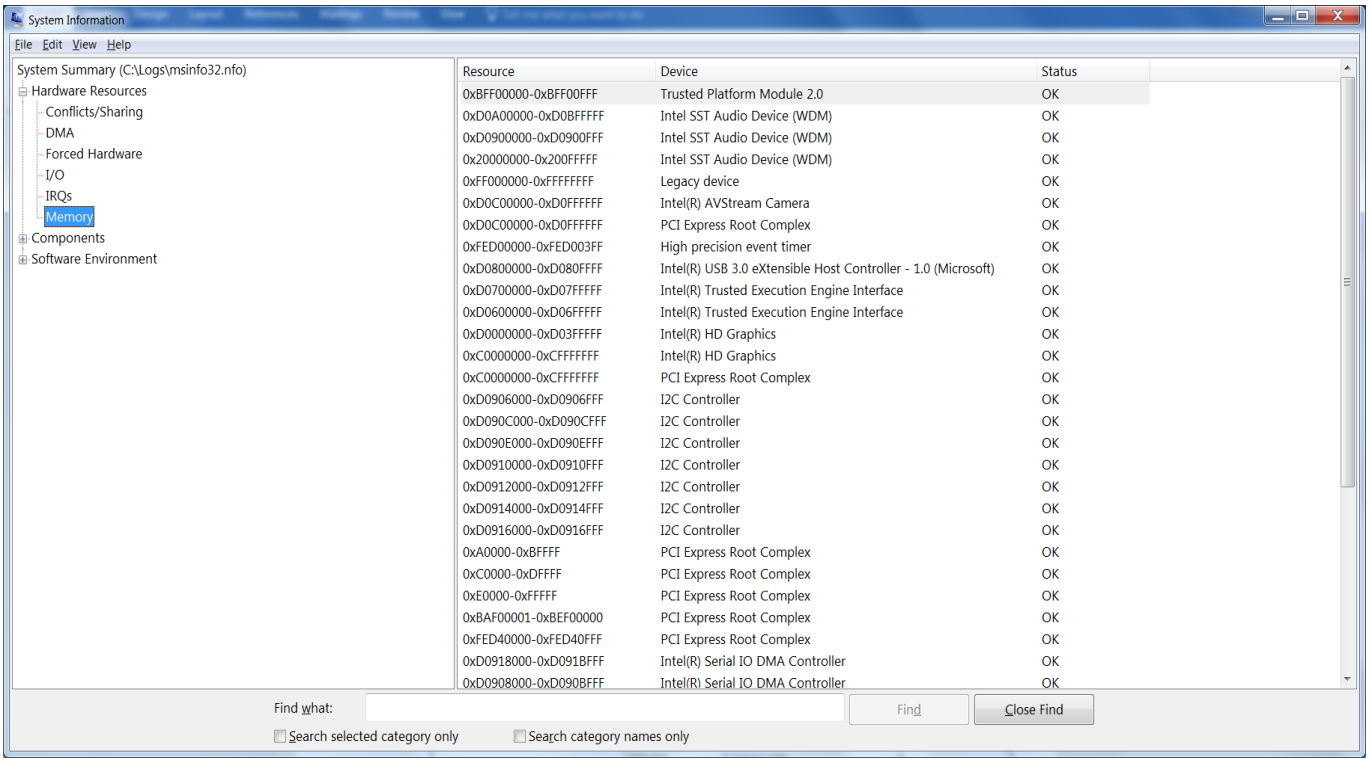


Figure (8): Memory of Hardware Resources

Components:

The Components category displays information about your Windows 98 system configuration. This includes the status of your device drivers, network components, and multimedia software. There is also a comprehensive driver history and a summary of devices that may not be working correctly. The following list is the sub-categories included in the Components category.

Multimedia:

Lists sound card and game controller information.

Multimedia - Audio:

Lists the audio codecs that are loaded.

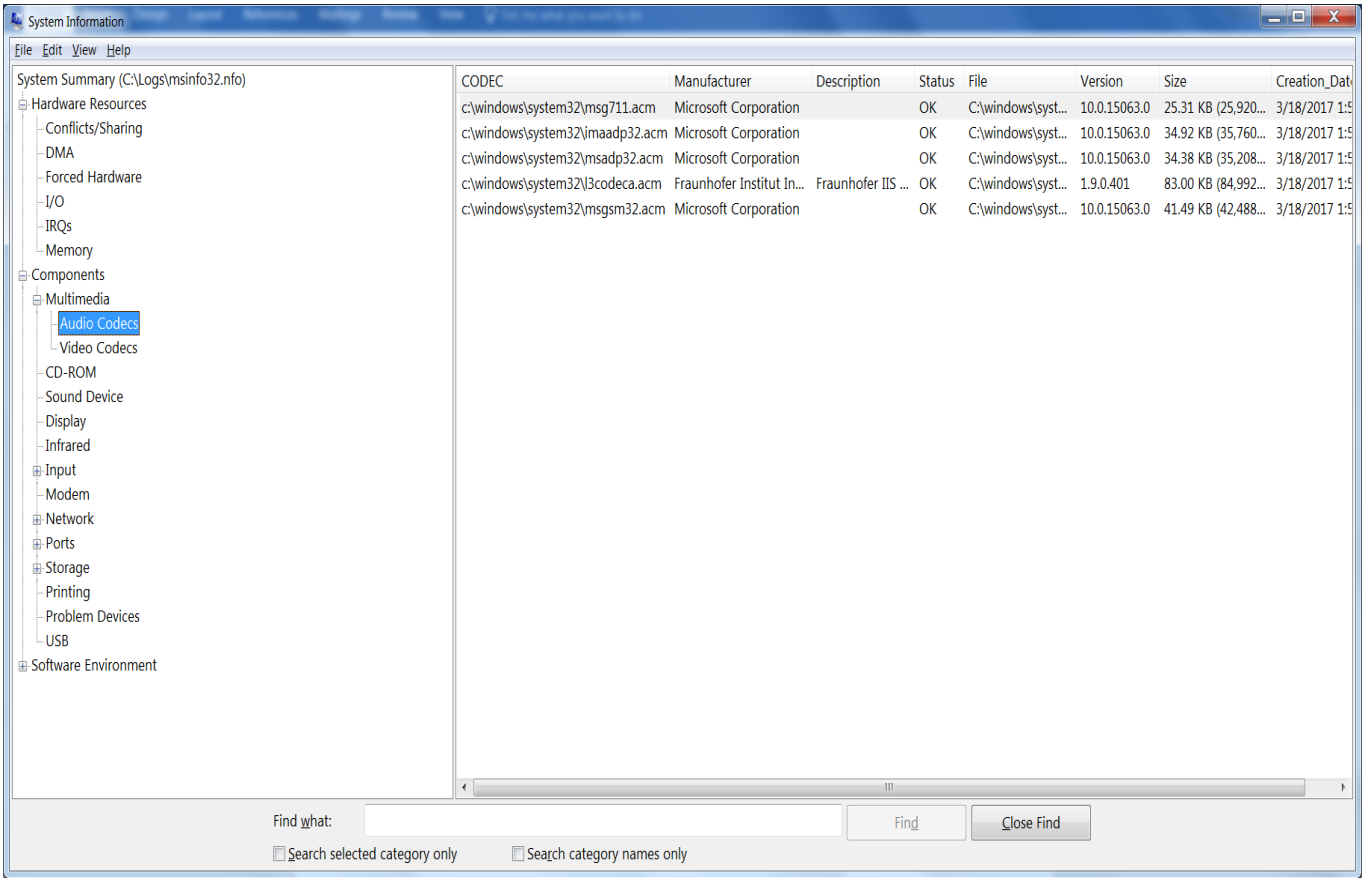


Figure (9): Audio Codecs of Multimedia

Multimedia - Video:

Lists the video codecs that are loaded.

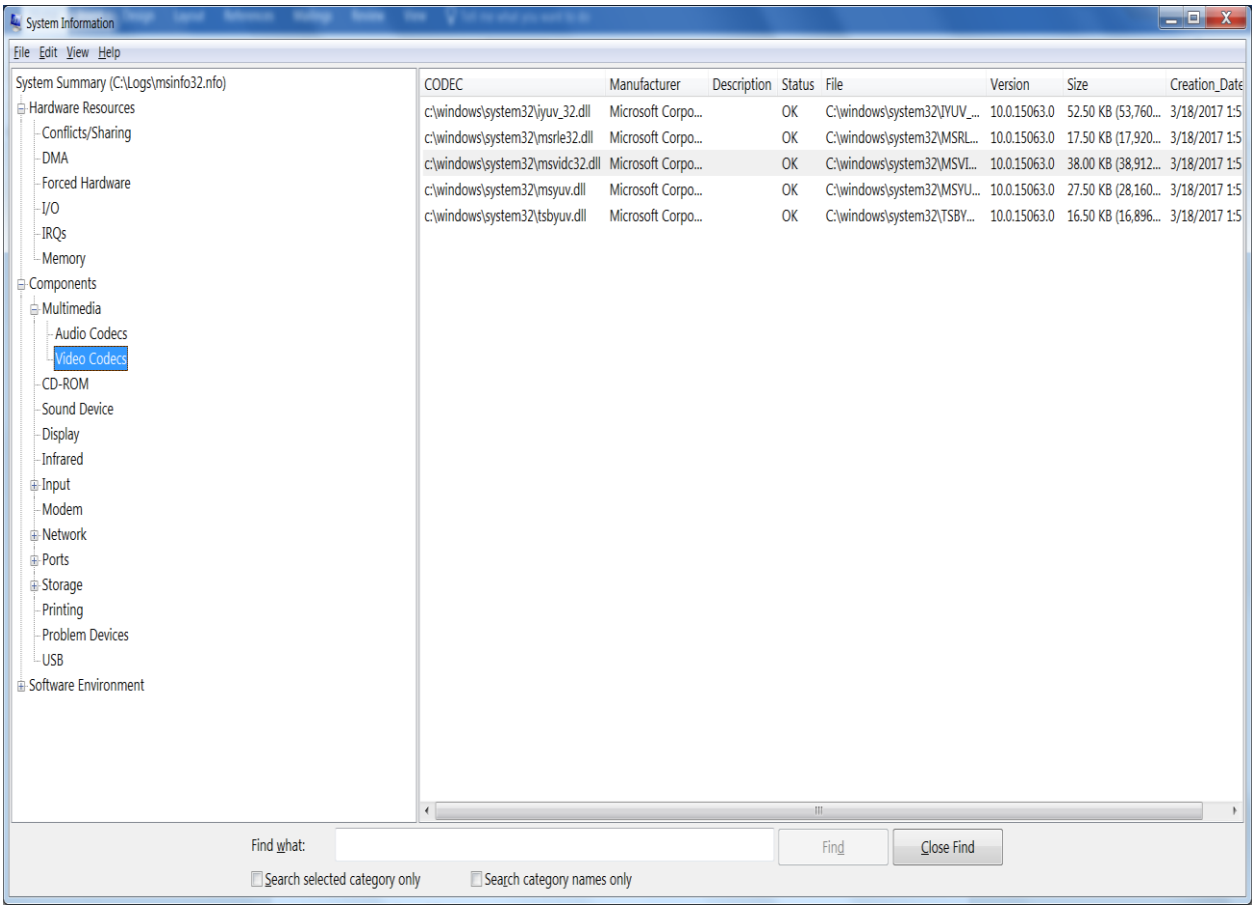


Figure (10): Video Codecs of Multimedia

Multi-media - CD-ROM:

Lists the drive letter and model of your CD-ROM drive. If a data CD-ROM is in the drive, Microsoft System Information also performs a data transfer test.

Sound Device:

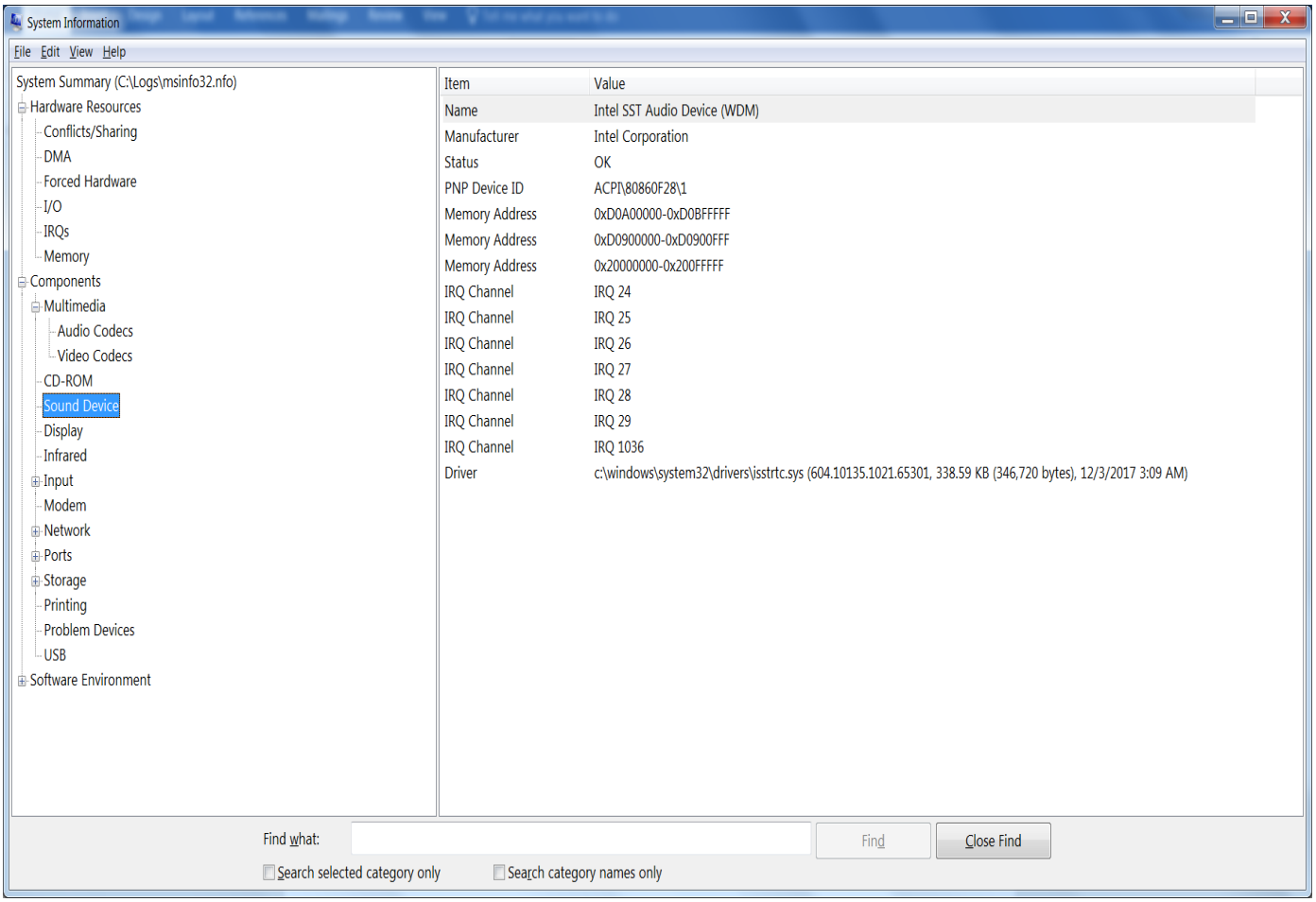


Figure (11): Sound Device of Multimedia

Display:

Lists video card and monitor information.

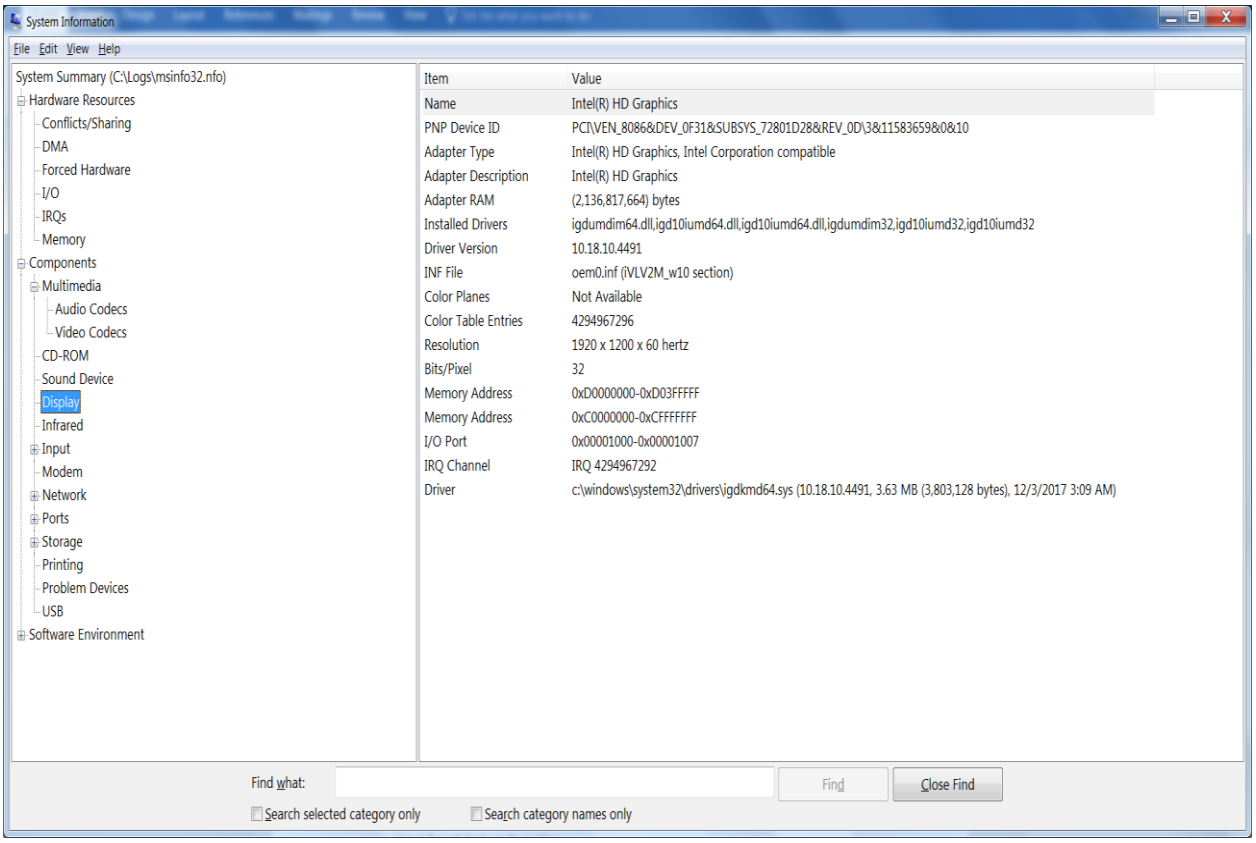


Figure (12): Display of Multimedia

Infrared:
Lists Infrared device information.

Input:
Lists keyboard and mouse information.

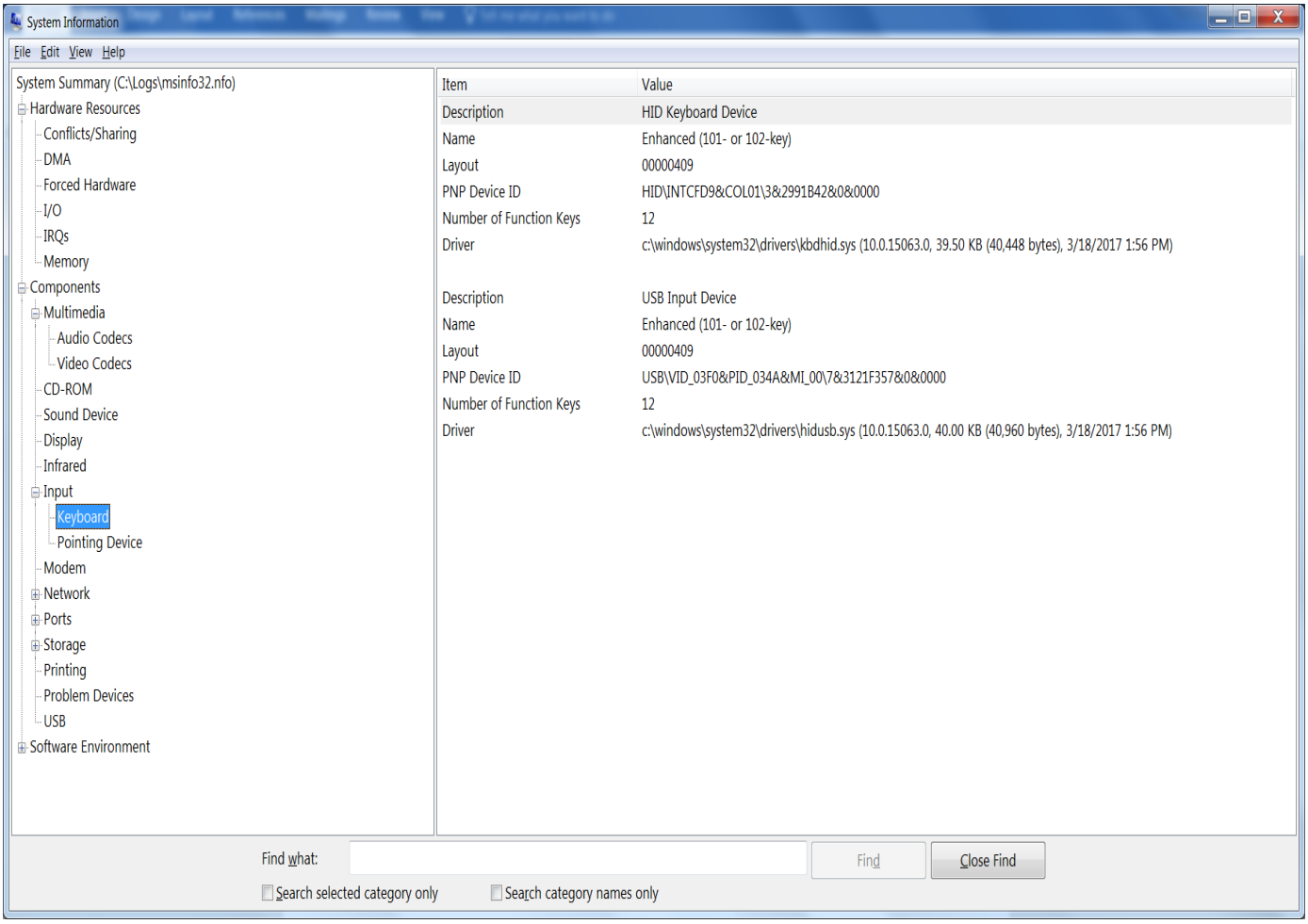


Figure (13): Keyboard of Input

Miscellaneous:
Lists information about any miscellaneous components.

Modems:
Lists modem information.

Network:
Lists network adapter, client, and protocol information.

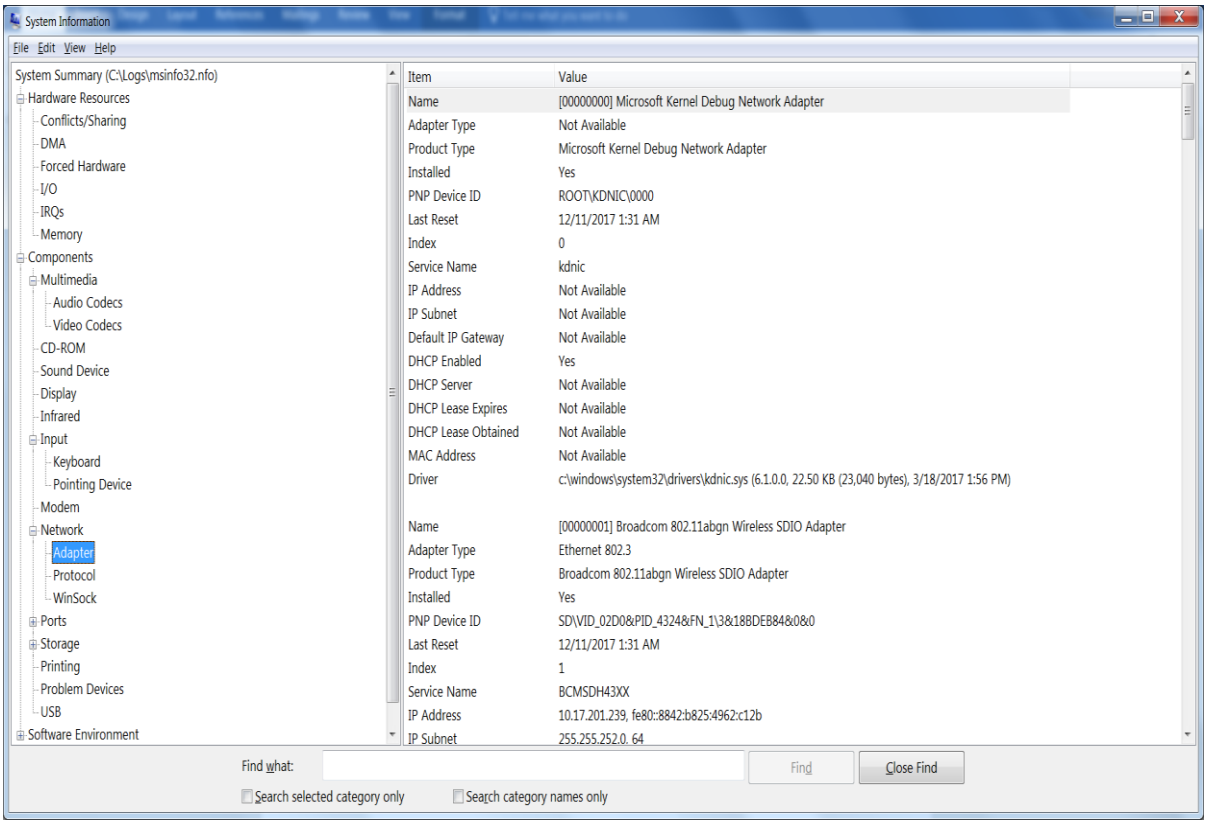


Figure (14): Adapter of Network

Network - Winsock:

Lists Winsock version, description, and status information.

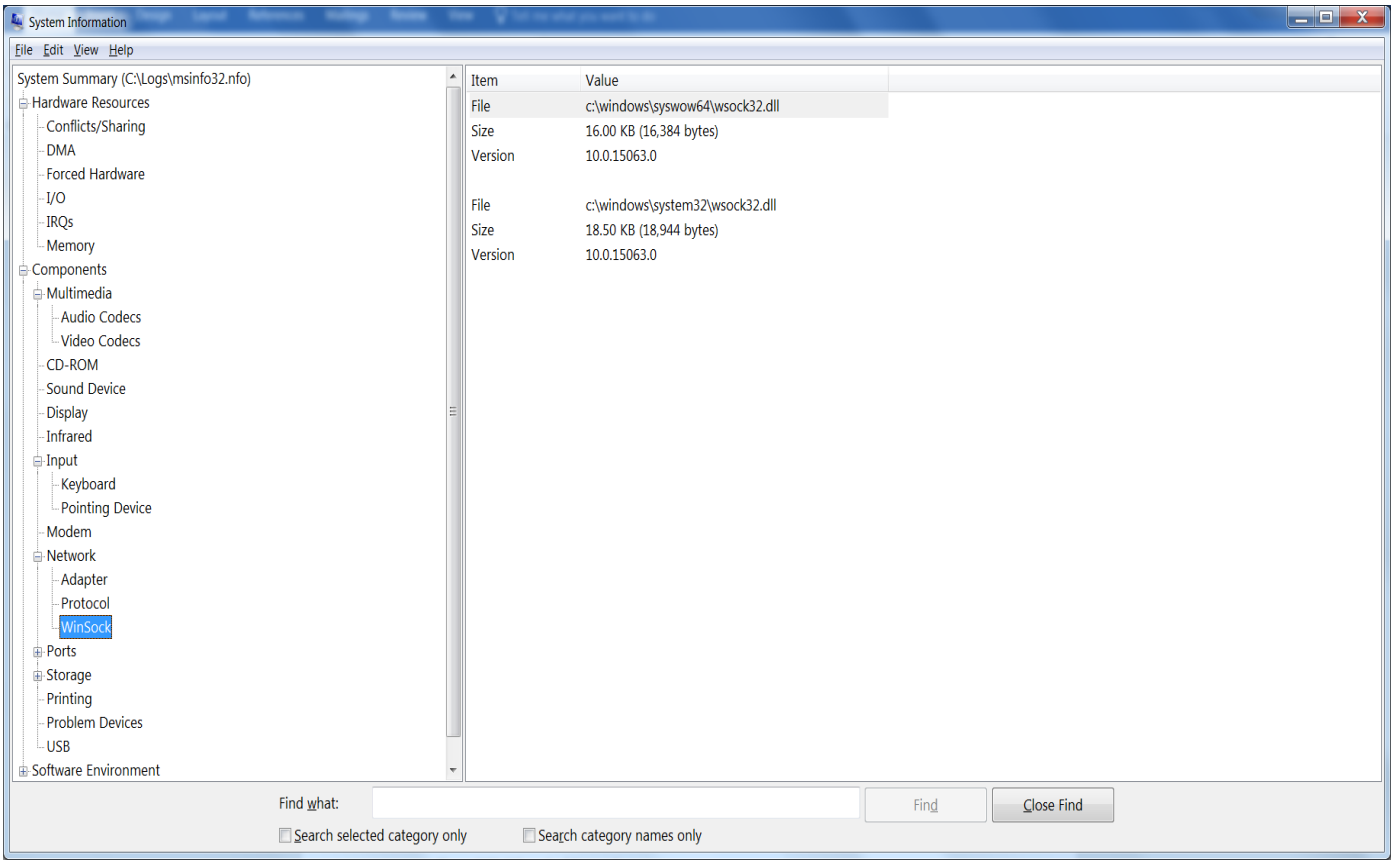


Figure (15): Winsock of Network

Ports:
Lists serial and parallel port information.

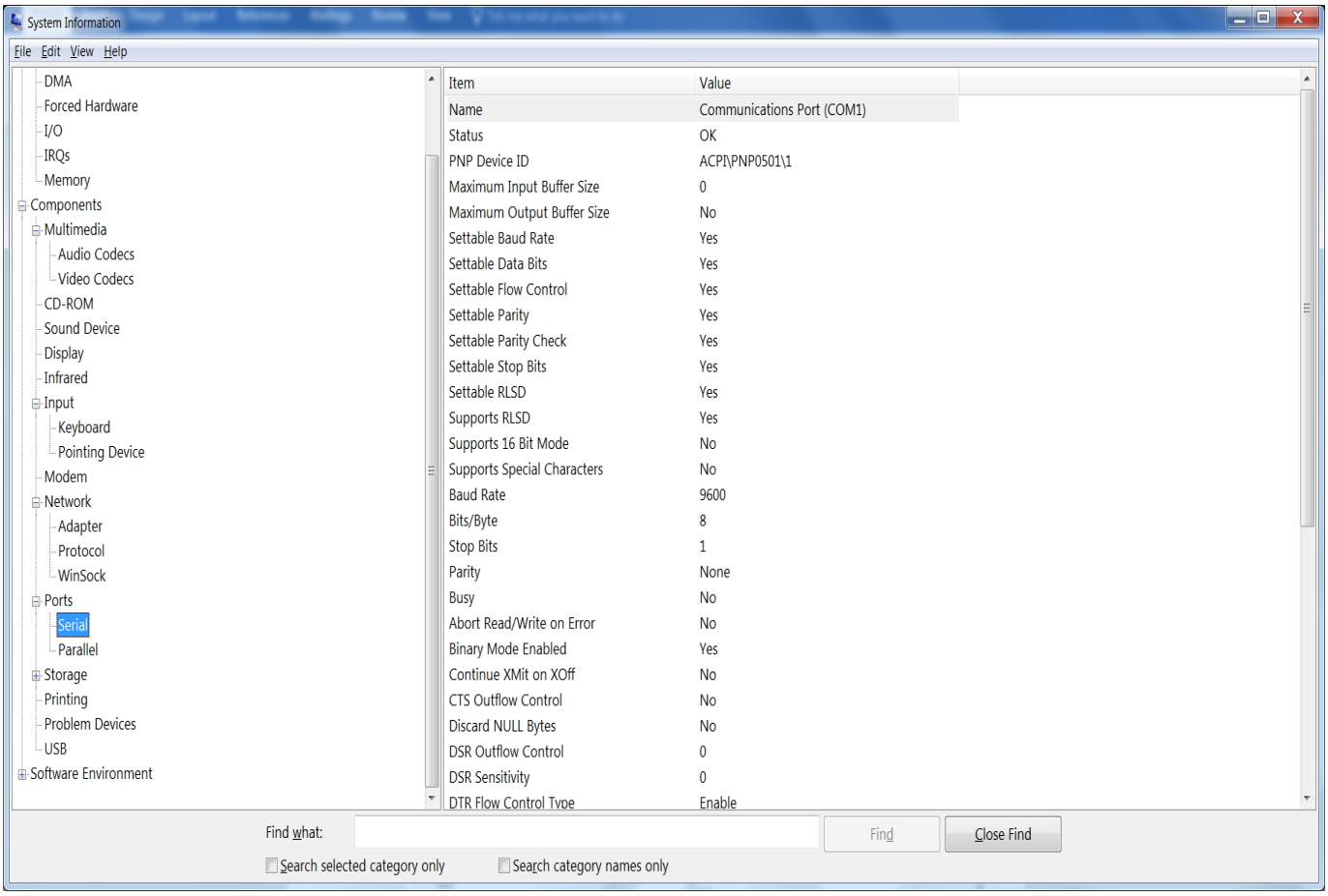


Figure (16): Serial Port

Storage:

Lists information about hard disks, floppy drives, removable media, and controllers.

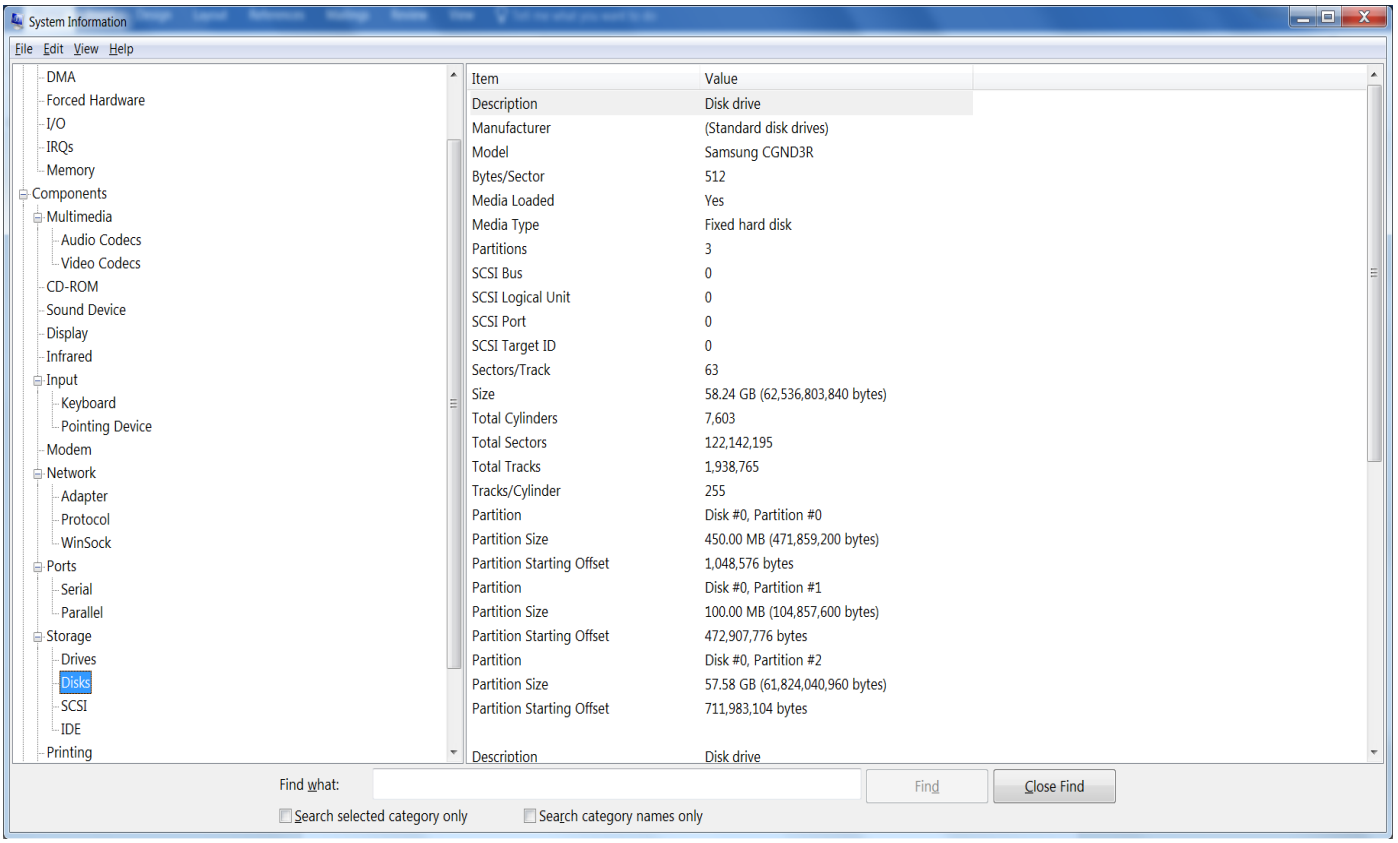


Figure (17): Disks storage

Printing:

Lists installed printers and printer drivers.

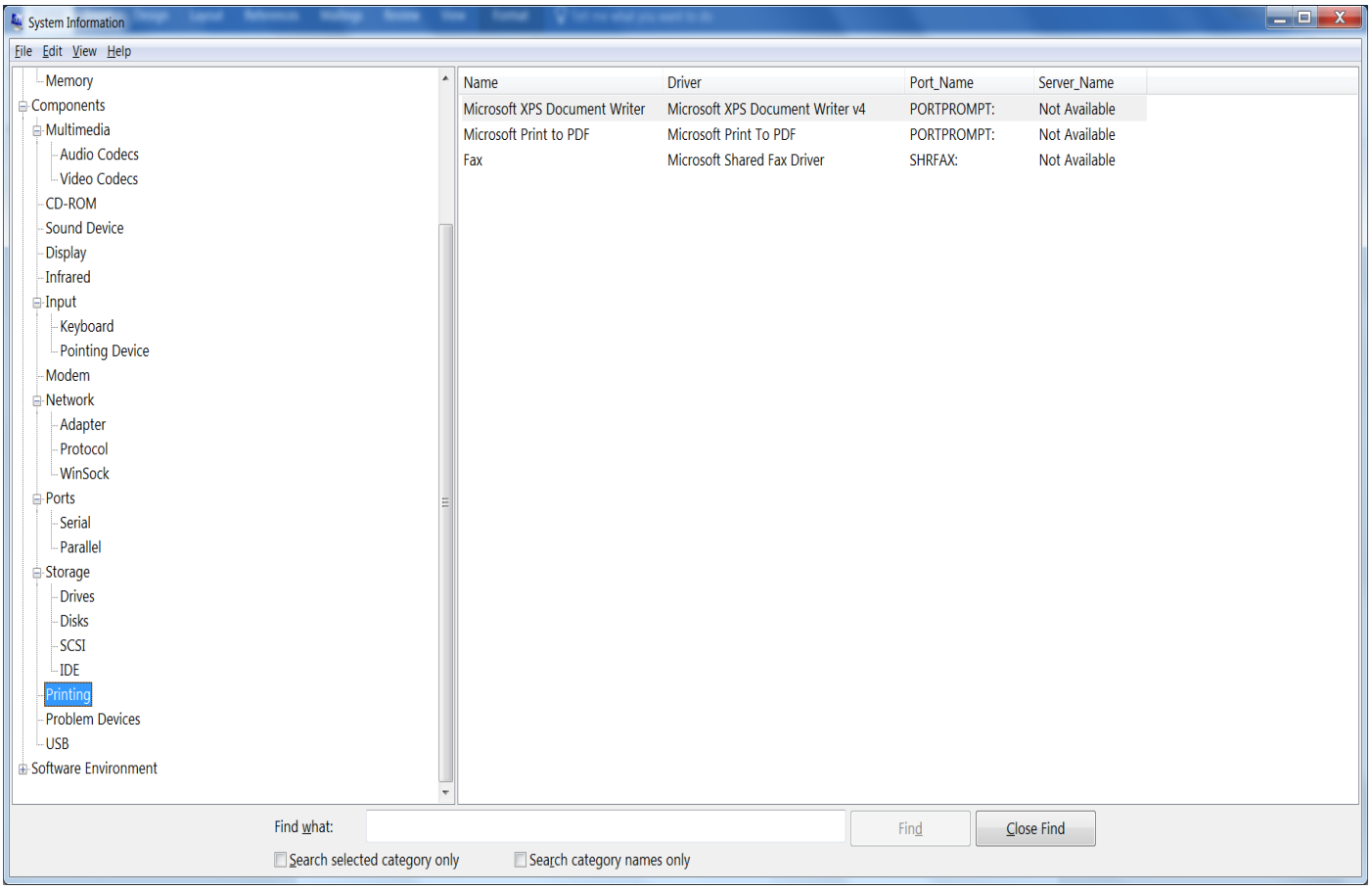


Figure (18): Printing

Problem Devices:
Lists devices with issues. Lists each device that is flagged in Device Manager and displays the corresponding status information.

USB:
Lists Universal Serial Bus (USB) controllers and drivers that are installed.

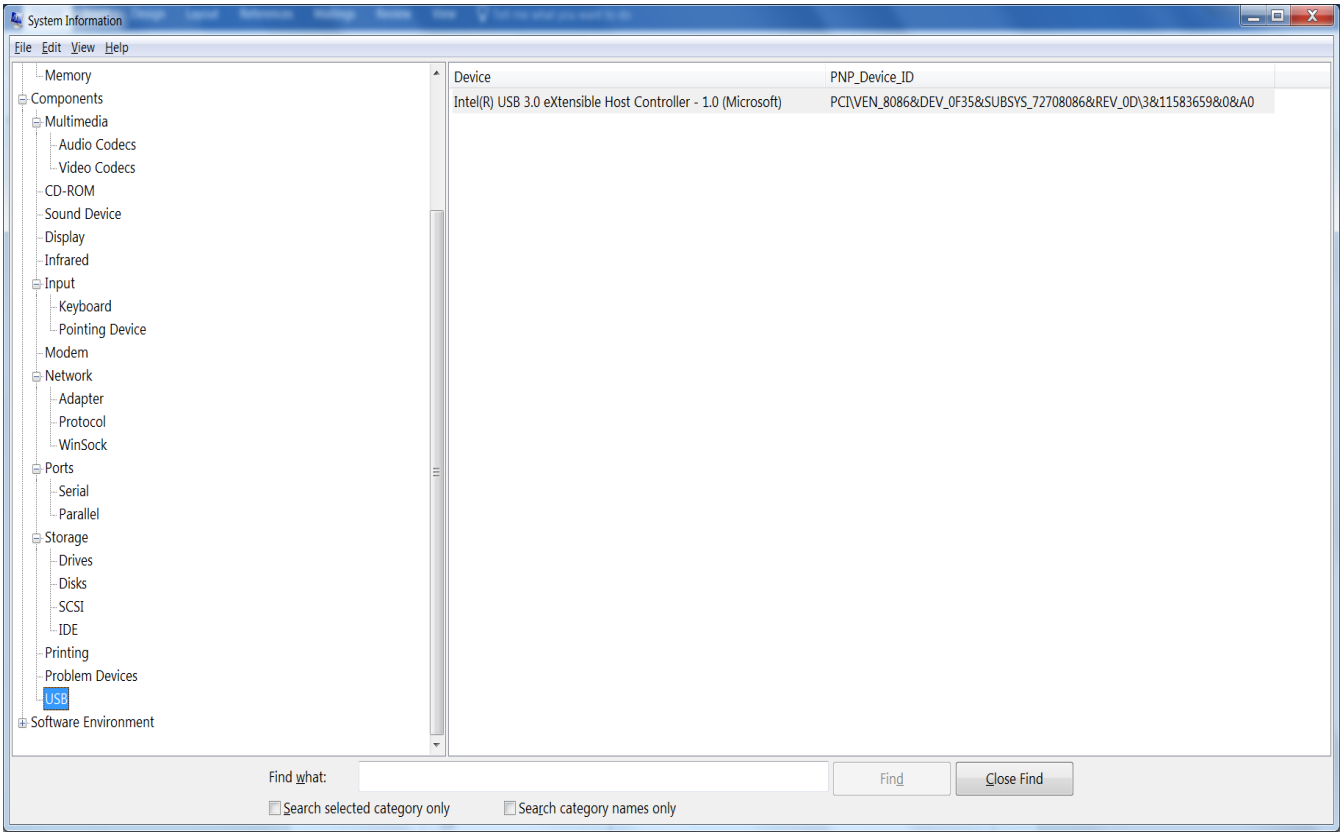


Figure (19): USB

History:
Lists complete driver history, or the history for the last seven days. This may be useful for tracking changes to your computer's configuration.

System:
Lists information about your computer's Basic Input / Output System (BIOS), motherboard, and other system devices.

NOTE: You may choose to view Basic Information, Advanced Information, or History if the component has a device driver.

Software Environment:

The Software Environment category displays the software loaded in your computer's memory.

Drivers - Kernel Drivers:
Lists kernel-mode (ring 0) device drivers that are loaded.

Drivers - MS-DOS Drivers:
Lists real-mode device drivers that are loaded.

Drivers - User-Mode Drivers:
Lists user-mode (ring 3) device drivers that are loaded.

16-bit Modules Loaded:
Lists 16-bit system-level dynamic link libraries (.dll) and programs that are loaded. This may be useful for debugging software issues, such as application fault errors.

32-bit Modules Loaded:
Lists 32-bit system-level DLLs and programs that are loaded. This may be useful for debugging software issues, such as application fault errors.

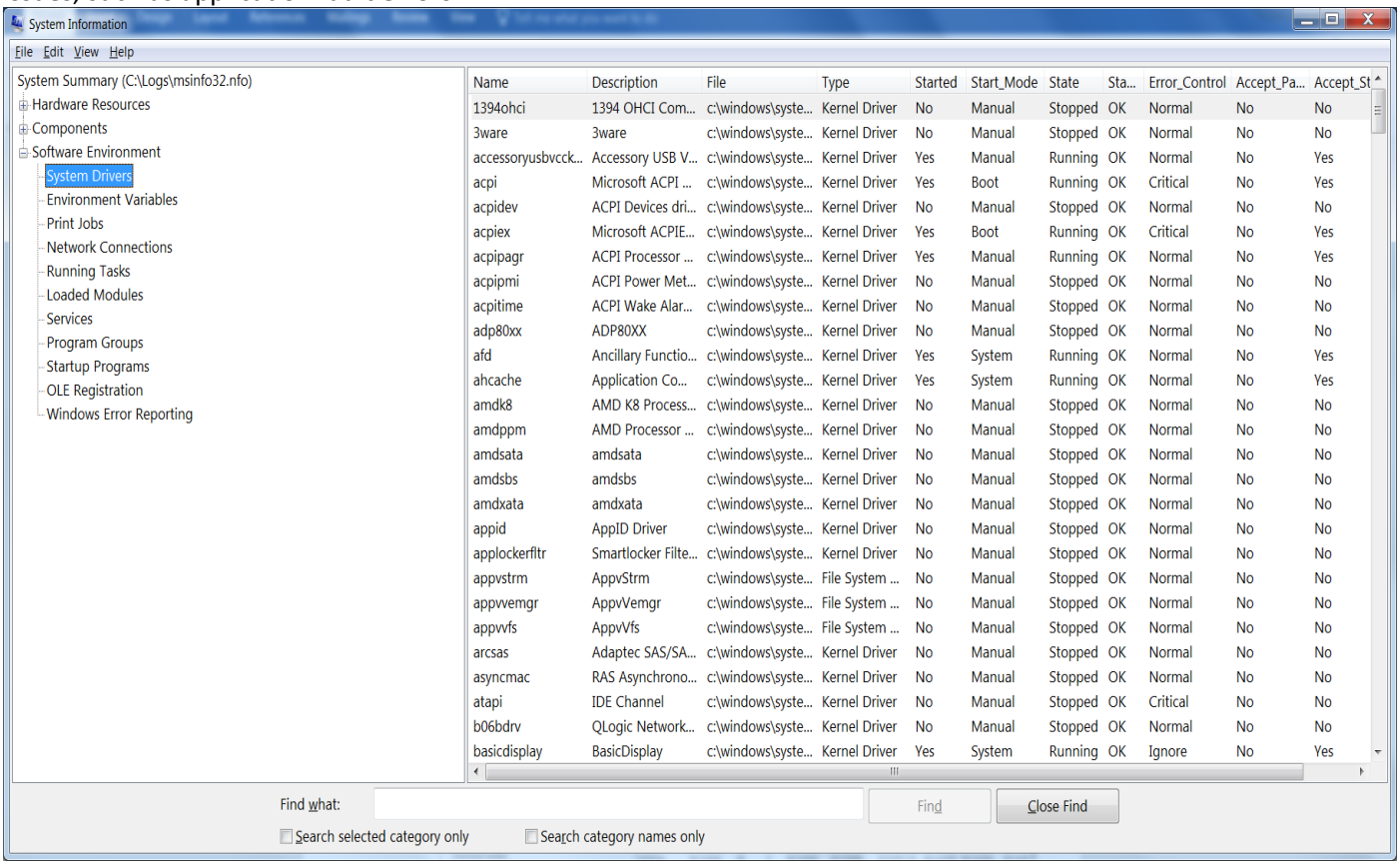


Figure (20): System Drivers

Running Tasks:

Lists the currently running executable files or programs. This provides a comprehensive view of the processes running on your computer.

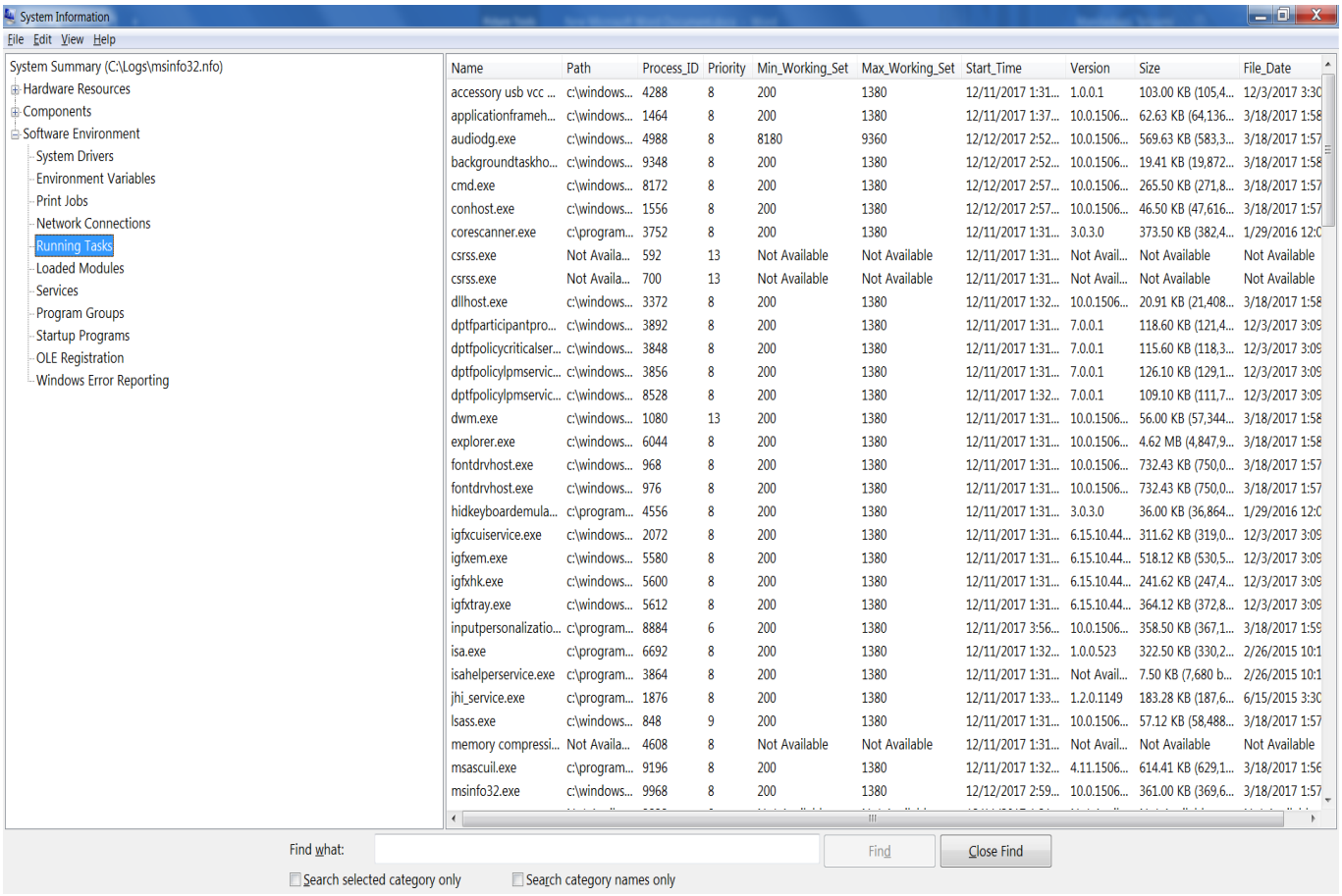


Figure (21): Running tasks of Software Environment

Startup Programs:

Lists programs started automatically either from the registry, the Startup folder, or the Win.ini file.

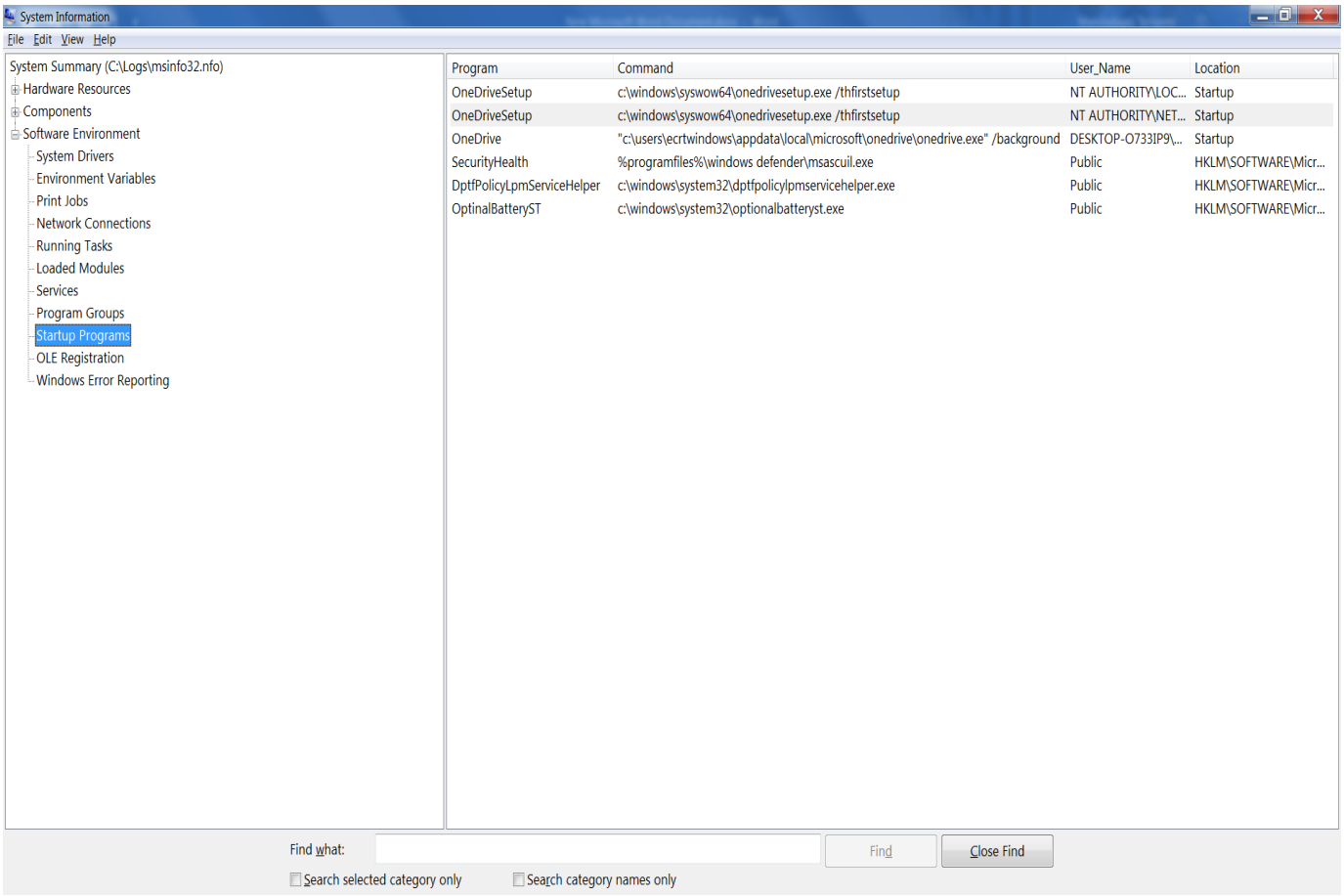


Figure (22): Startup Programs of Software Environment

System Hooks:
Lists programs that are resident in memory and hook system calls.

OLE Registration - INI File:
Lists OLE file associations controlled by various .ini files.

OLE Registration - Registry:
Lists OLE file associations that are controlled by the Registry.

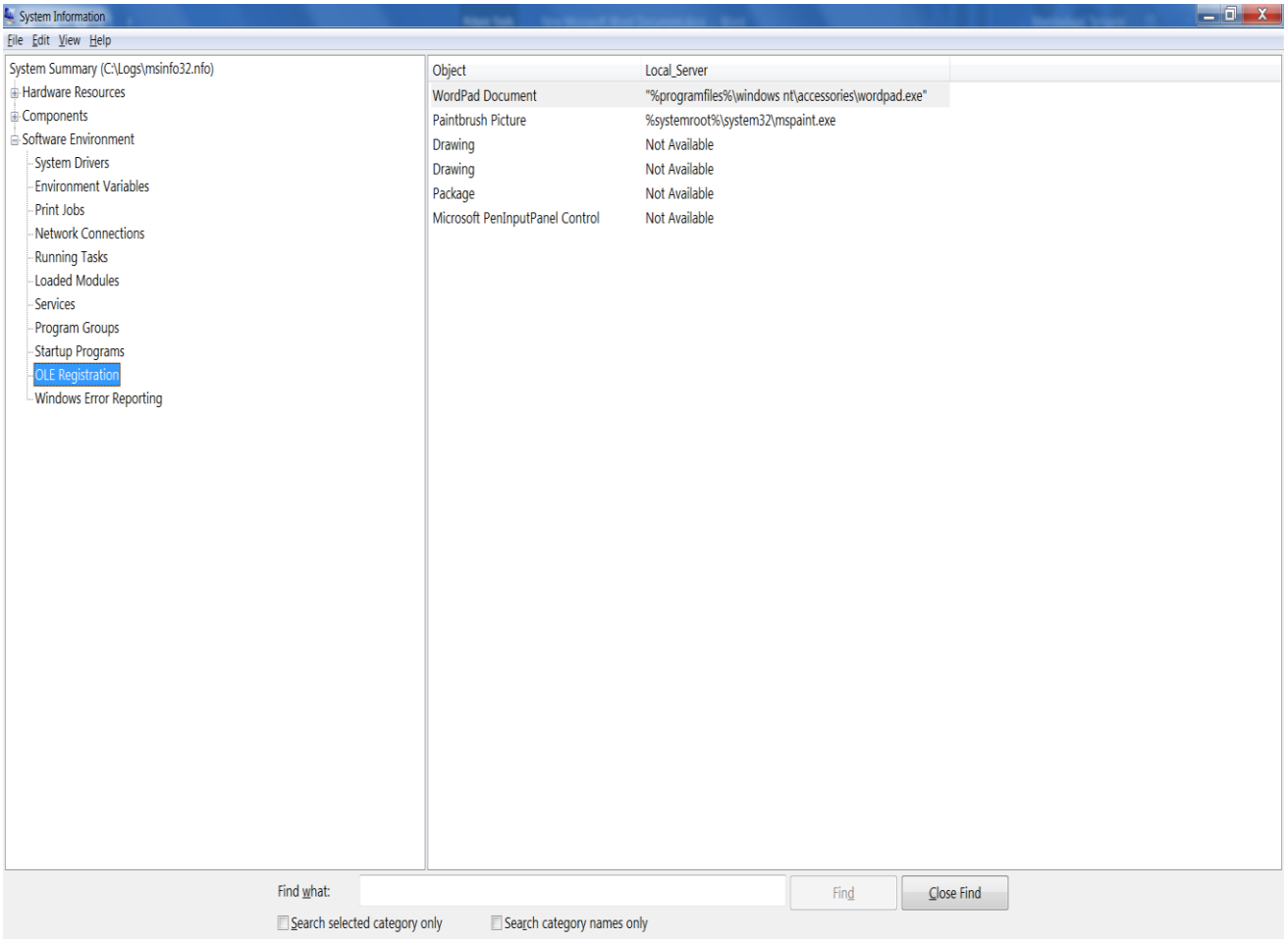


Figure (23): OLE Registration

Services:

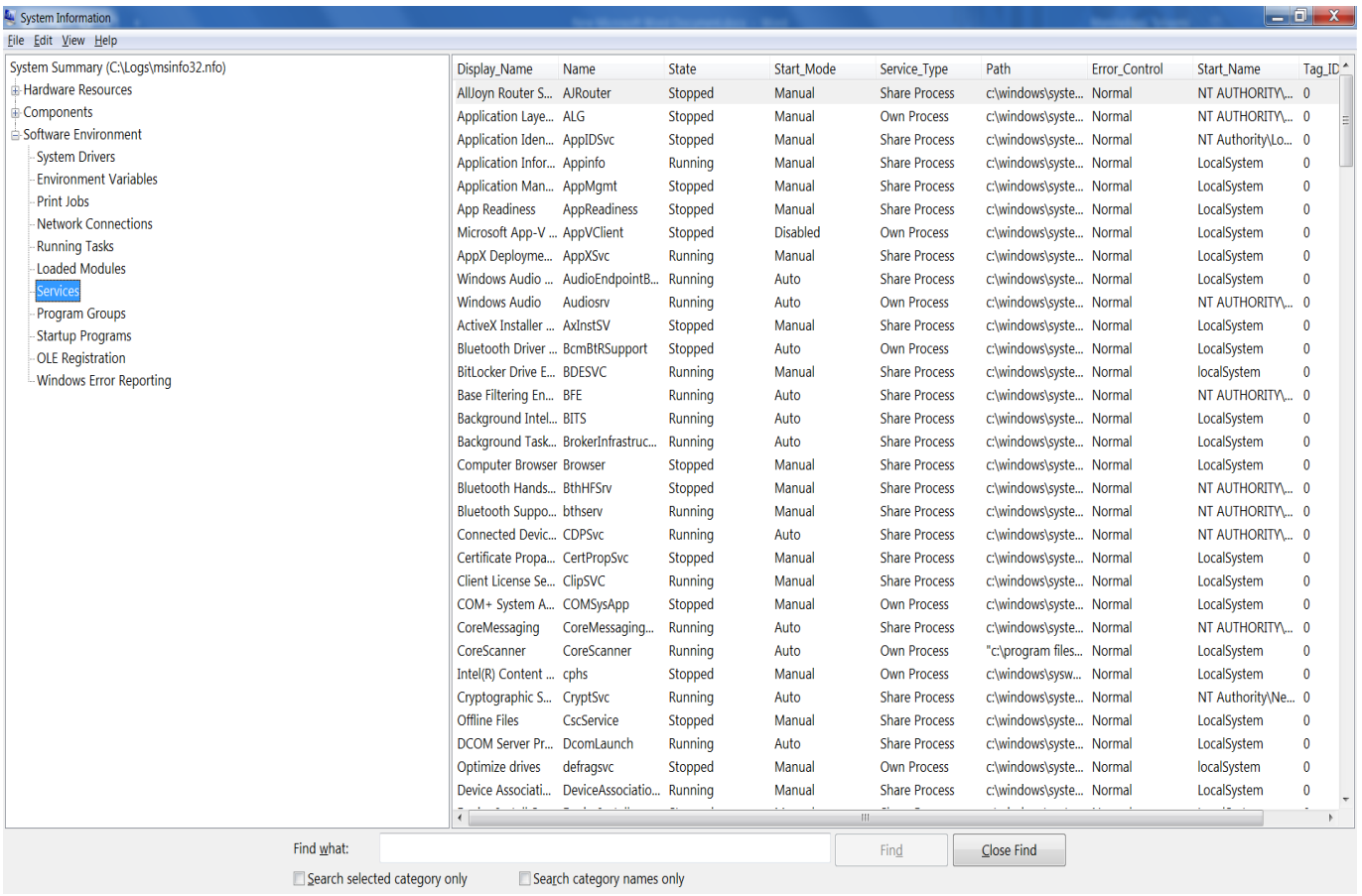


Figure (24): Services of Software Environment

NOTE: Hardware information is not available in Safe Mode. While Microsoft System Information can be run in Safe Mode, it is limited to displaying information about system components and the software environment.

When you want to troubleshoot issues with Windows 98, Microsoft recommends you start with the Microsoft System Information tool. To reduce the time needed to start other troubleshooting or system tools, you can start the following programs from the Tools menu in Microsoft System Information:

- Windows Report Tool
- Update Wizard Uninstall
- System File Checker
- Signature Verification Tool
- Registry Checker
- Automatic Skip Driver Agent
- Dr. Watson

- System Configuration Utility
- Scandisk
- Version Conflict Manager

2. General Information:

- **Windows updates:**

  Collects the windows update files.

  Windows updates is a Microsoft service, which automates downloading and installing software updates over the internet. The service delivers software updates for Windows, as well as the various Microsoft antivirus products, including Windows Defender and Microsoft Security Essentials.

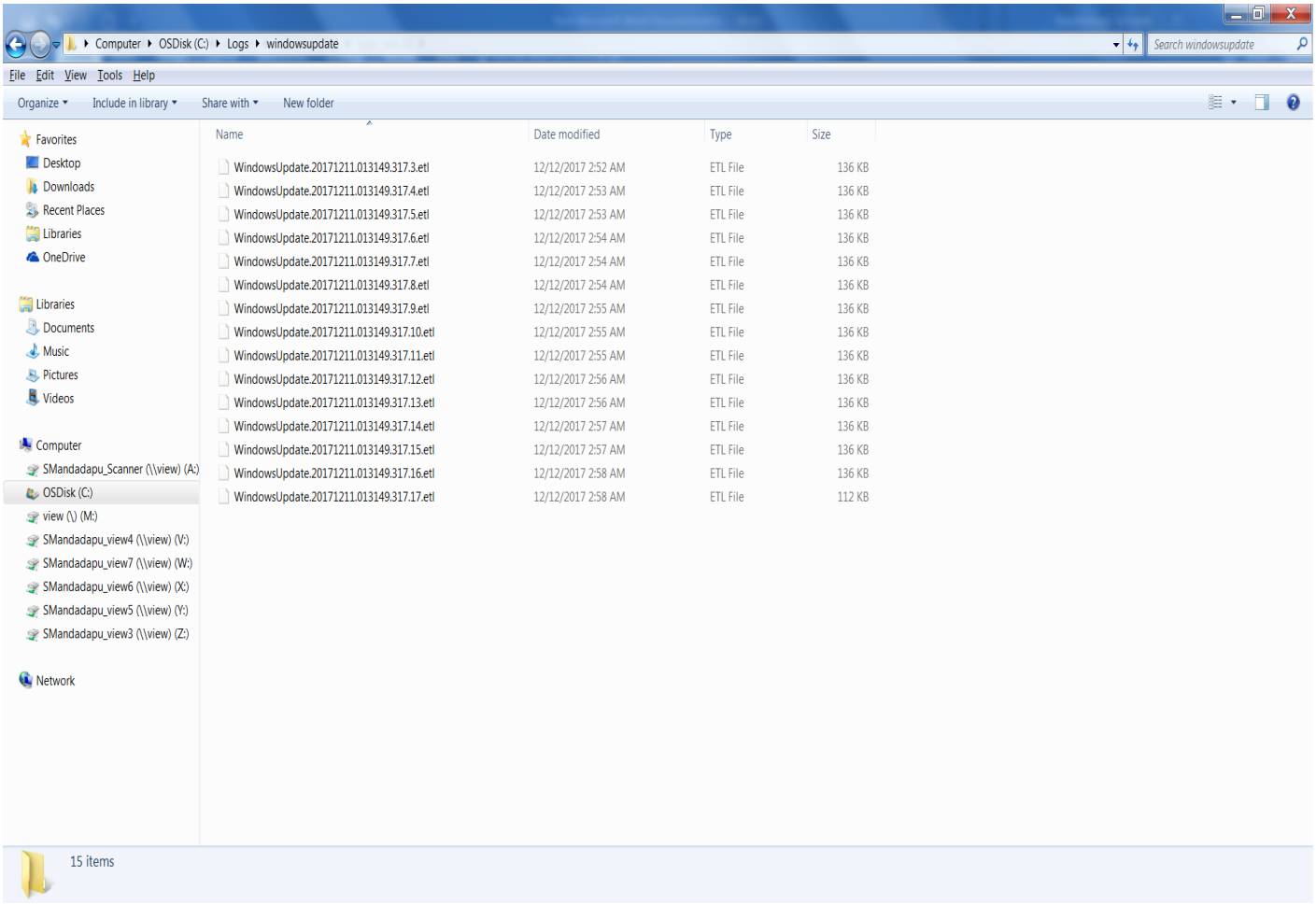


Figure (25): Windows Updates in General Information

- **Inf:**
  SetupAPI logs information about device installation in a plain-text log file that you can use to verify the installation of a device and to troubleshoot device installation problems. If a signing problem exists, SetupAPI will log information about the signing problem in the log file. The name of this log file is SetupAPI.dev.log, and it is located, by
  default, in the Windows INF file directory (%SystemRoot%\inf).

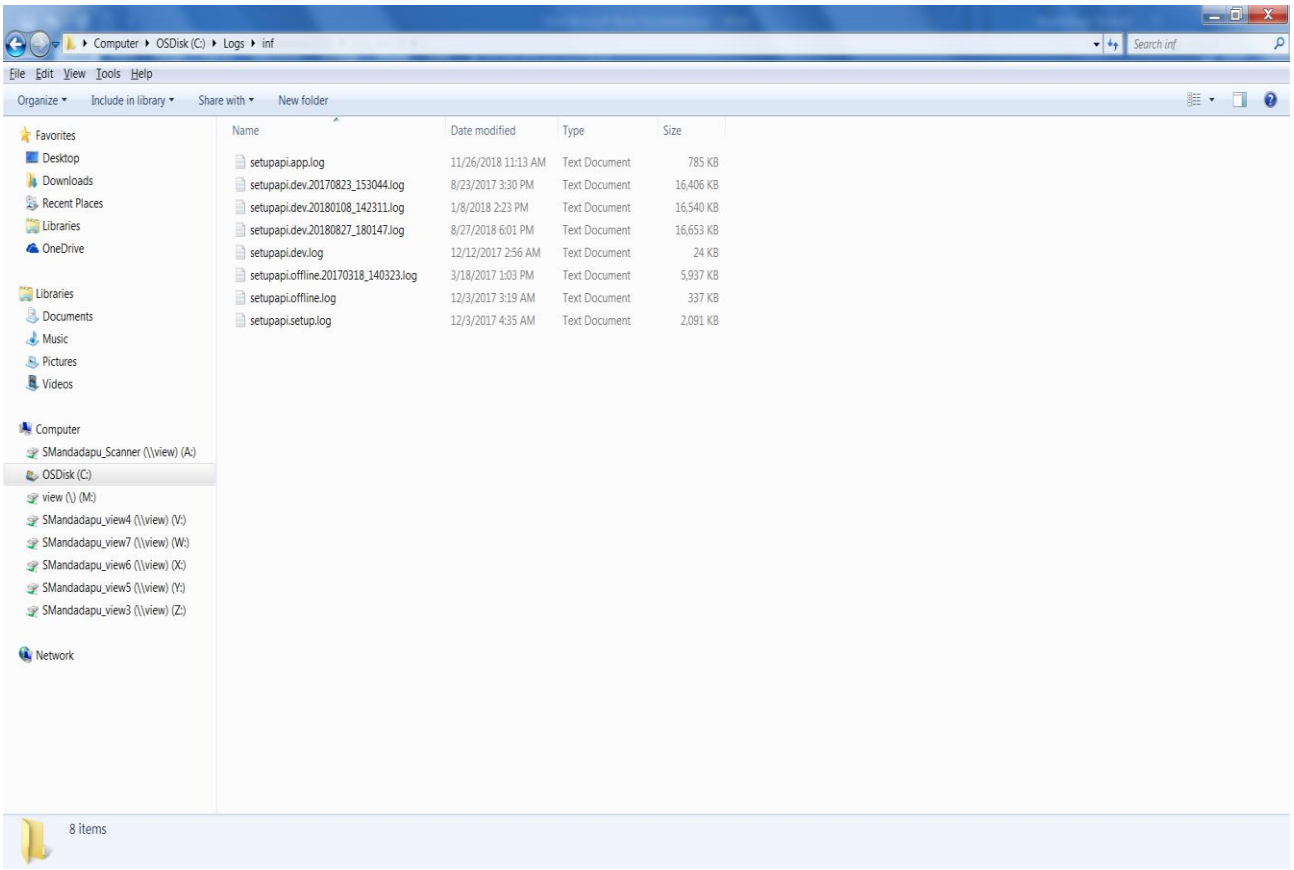


Figure (26): Inf folder

- **Panther:**
  Windows Setup creates log files for all actions that occur during installation. If you are experiencing problems installing Windows, consult the log files to troubleshoot the installation. Windows Setup includes the ability to review the Windows Setup performance events in the Windows Event Log viewer. This enables you to more easily review the actions that occurred during Windows Setup and to review the performance statistics for different parts of Windows Setup.

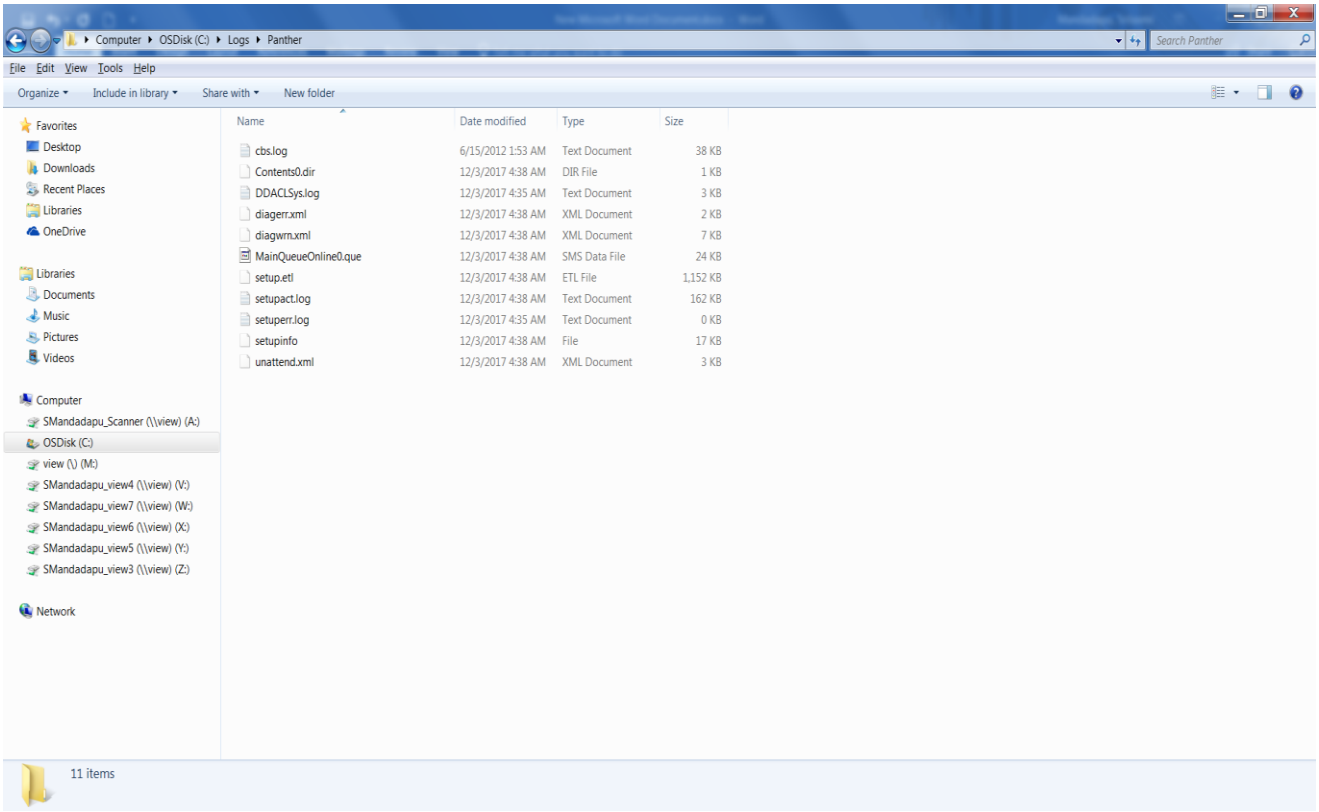


Figure (27): Panther folder

- **Winsxs:**
  Windows uses a system folder called WinSxS to store files that are needed for your Windows installation, as well as backups or updates to those files.

- **CBS:**
  CBS stands for component-based servicing. CBS.log is a file which include logs about components when they get installed or uninstalled during updates.
  If you want to check these files, they are located at %windir%\Logs\CBS\
  You will see two files in CBS folder, one is CBS.log and the other is CBS.persist.log.
  CBS.persist.log is the older of these two and is generated when the CBS.log is around 35-40 MB.
  Persist log folder can easily be dumped.

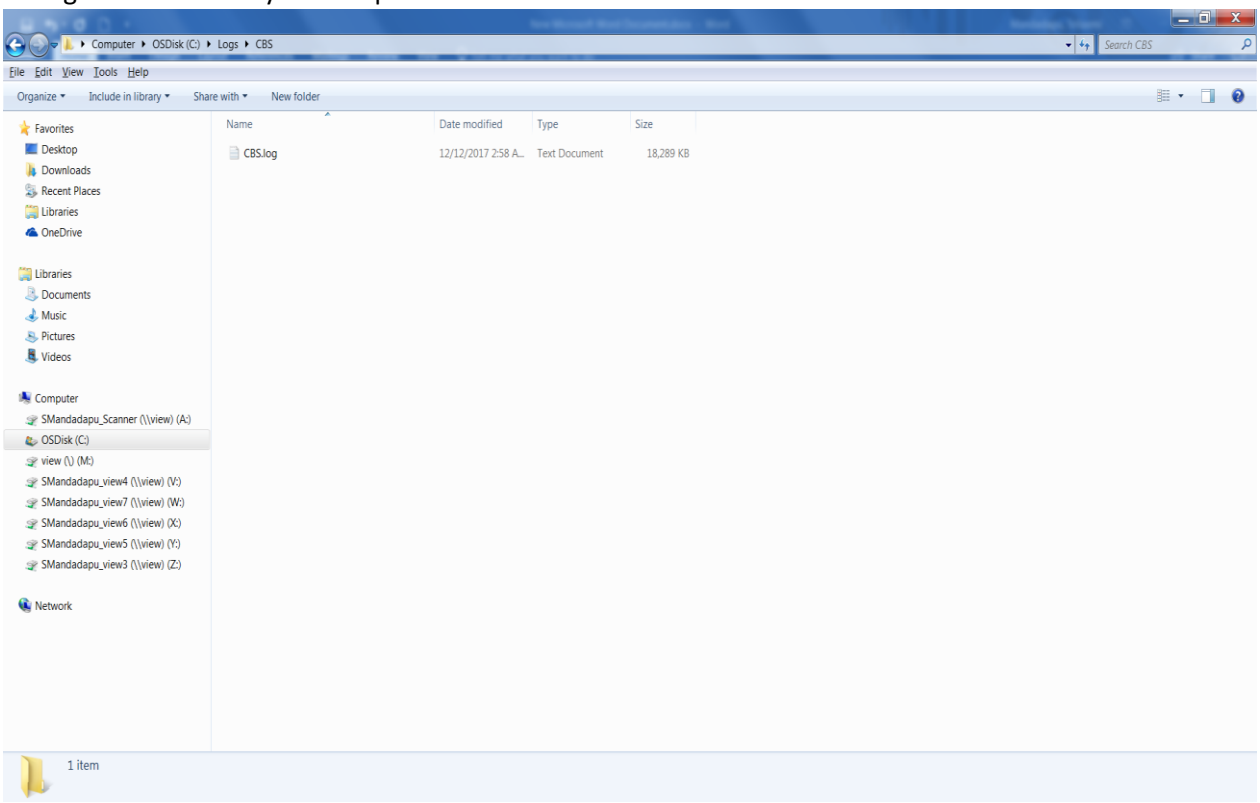


Figure (28): CBS Log

- **DISM:**
  The Deployment Image Servicing and Management (DISM) tool is the primary tool for all offline-servicing tasks. DISM runs from a command prompt from Windows PE or a running Windows operating system. If a failure occurs when executing a DISM command, the tool will provide an immediate response, and log the issue in the DISM.log file. The Session.xml file is a transaction log file that captures all servicing activities on the target operating system. The Session.xml file can be used in conjunction with the DISM.log file to determine points of failures and the required servicing activity.

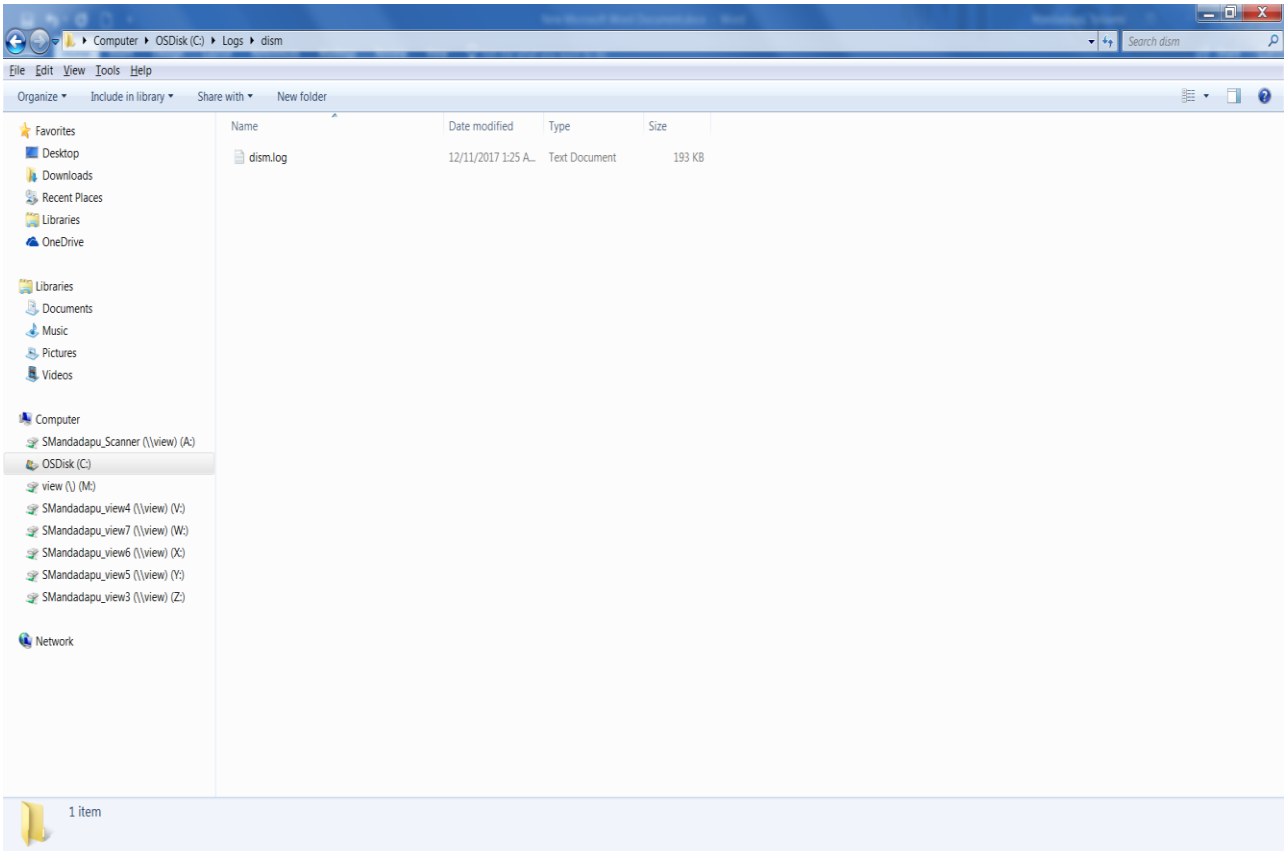


Figure (29): DISM Log

- **System restore:**
  System Restore is a feature in Microsoft Windows that allows the user to revert their computer's state (including system files, installed applications, Windows Registry, and system settings) to that of a previous point in time, which can be used to recover from system malfunctions or other problems. System restore related logs will be available in event log and in windows\logs\systemrestore folder.

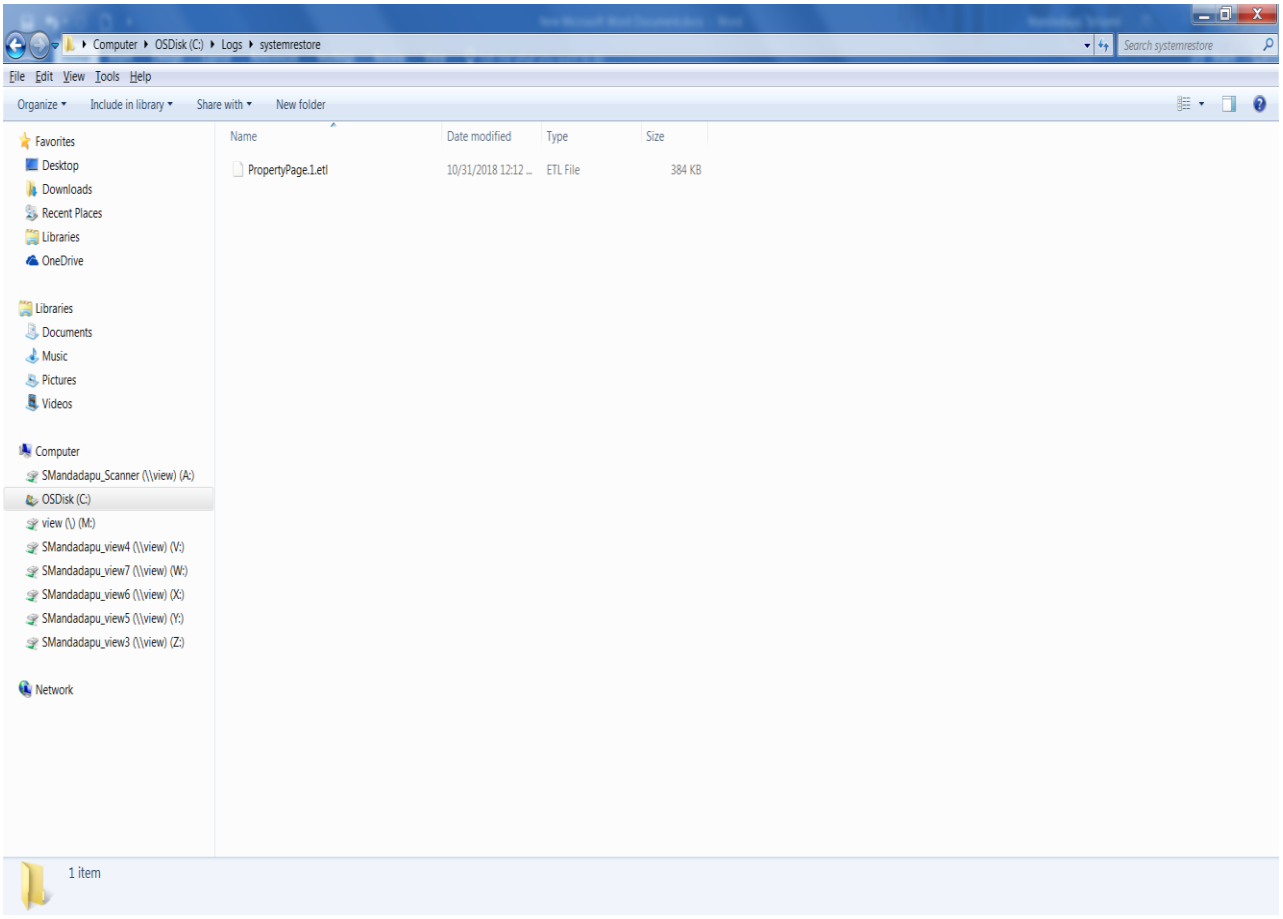


Figure (30): System Restore Folder

- **Pbr:**
  Windows 8 includes a feature called Push-Button Reset that gives you options for returning your PC to a known configuration. You can use this to recover from a problem, or to return it to the factory state. This can be handy if you are selling a PC, or giving it to another member of the family and want to give them a fresh start.
  Push Button Reset provides two options:
    - Refresh your PC without affecting your files
    - Remove everything and reinstall Windows

- **Windows Events:**
  The Windows event log is a detailed record of system, security and application notifications stored by the Windows operating system that is used by administrators to diagnose system problems and predict future issues.
  Application Log: Any event logged by an application. These are determined by the developers while developing the application. Eg.: An error while starting an application gets recorded in Application Log.
  System Log: Any event logged by the Operating System. E.g.: Failure to start a drive during startup is logged under System Logs

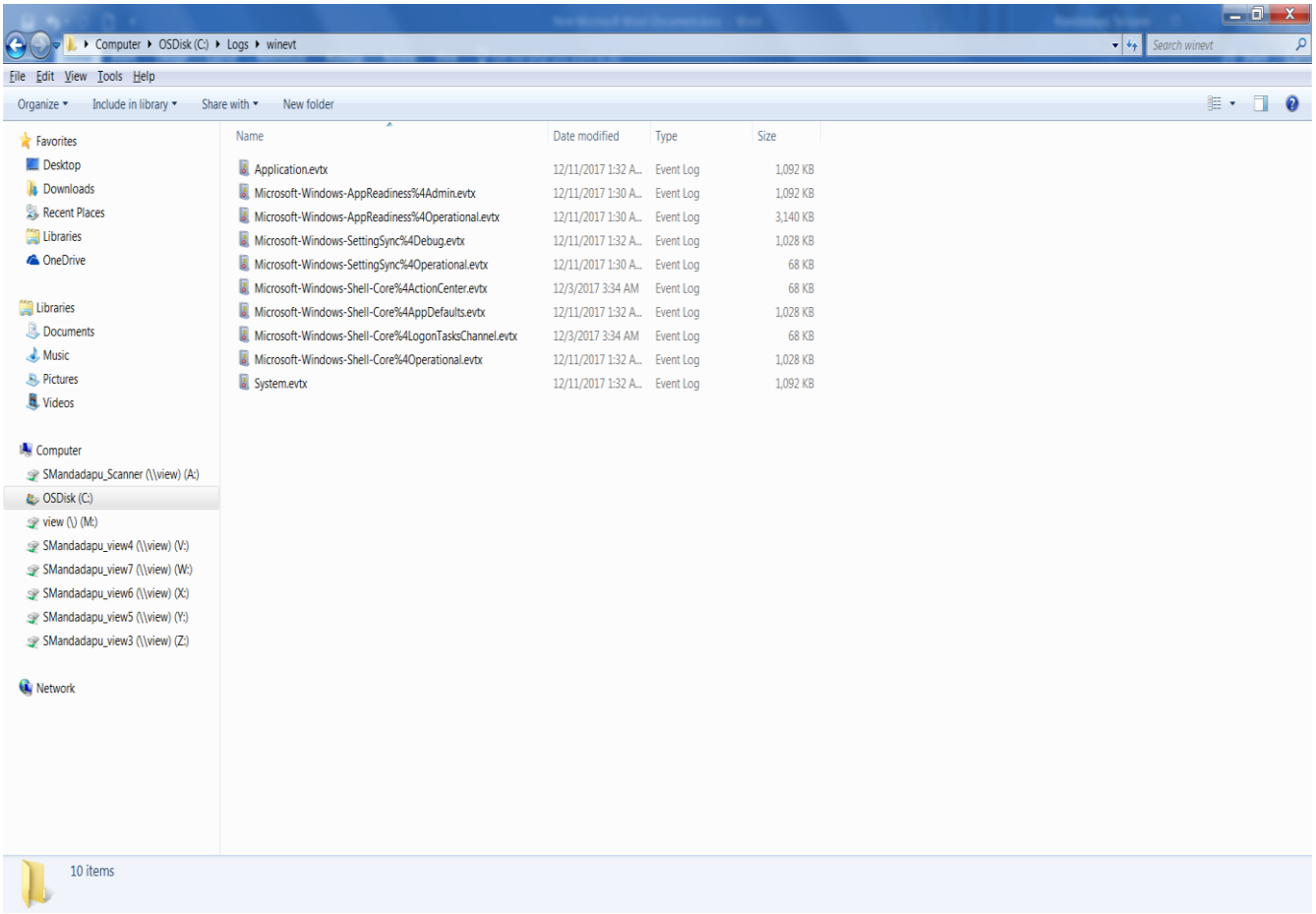


Figure (31): Windows Events

3. DirectX Diagnosis:

DxDiag ("DirectX Diagnostic Tool ") is a diagnostics tool used to test DirectX functionality and troubleshoot video- or sound-related hardware problems. DirectX Diagnostic can save text files with the scan results.

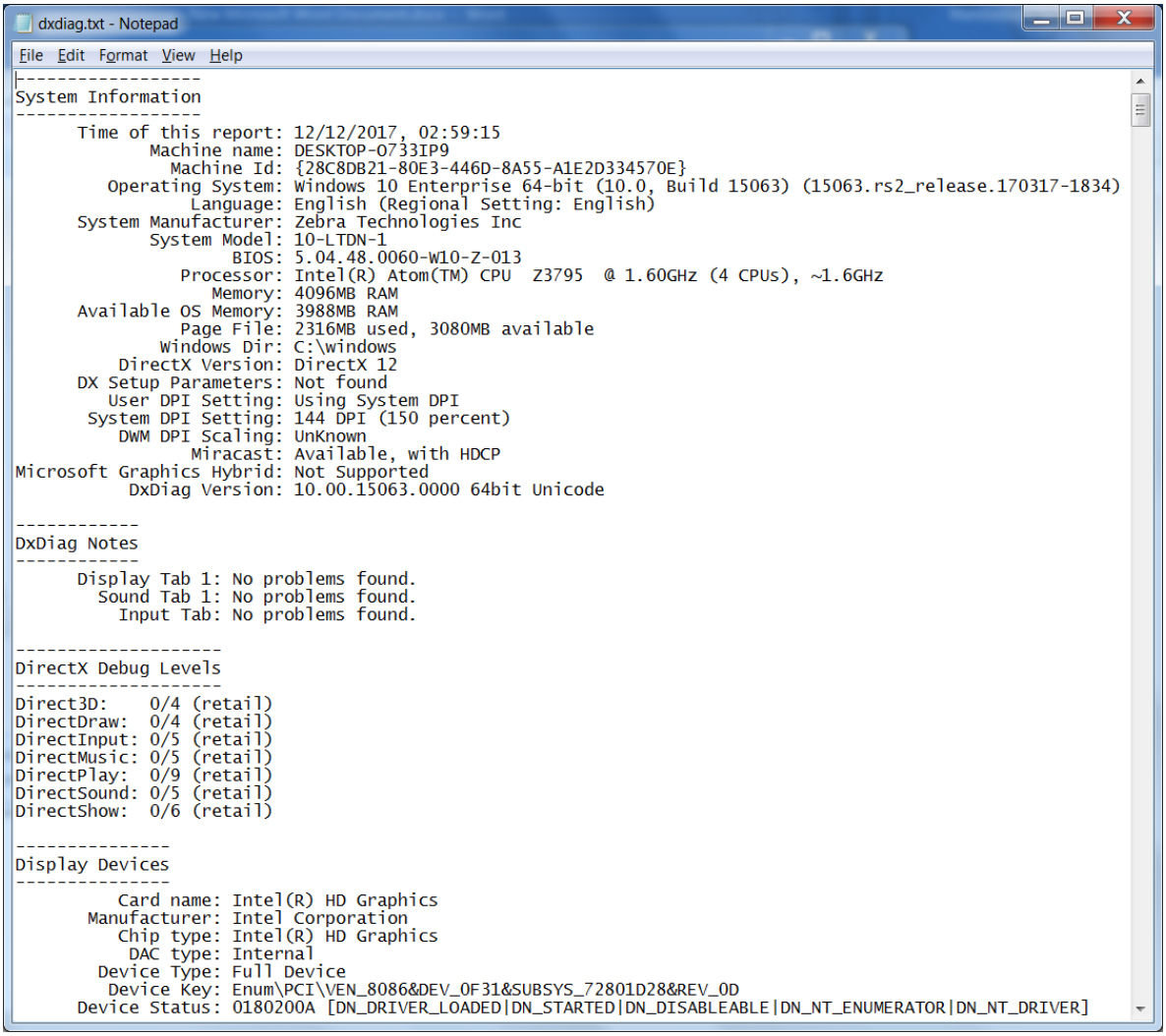


Figure (32): Direct Diagnosis dxdiag.txt file

4. Dump Files:

A DMP file is a file that contains data "dumped" from a program's memory space. It is often created when a program has an error or crashes and may also be saved by the program "Savedump.exe" on the first reboot after a crash. DMP files are usually named "Memory.dmp."

5. Display Info:

Logs display information to a file.

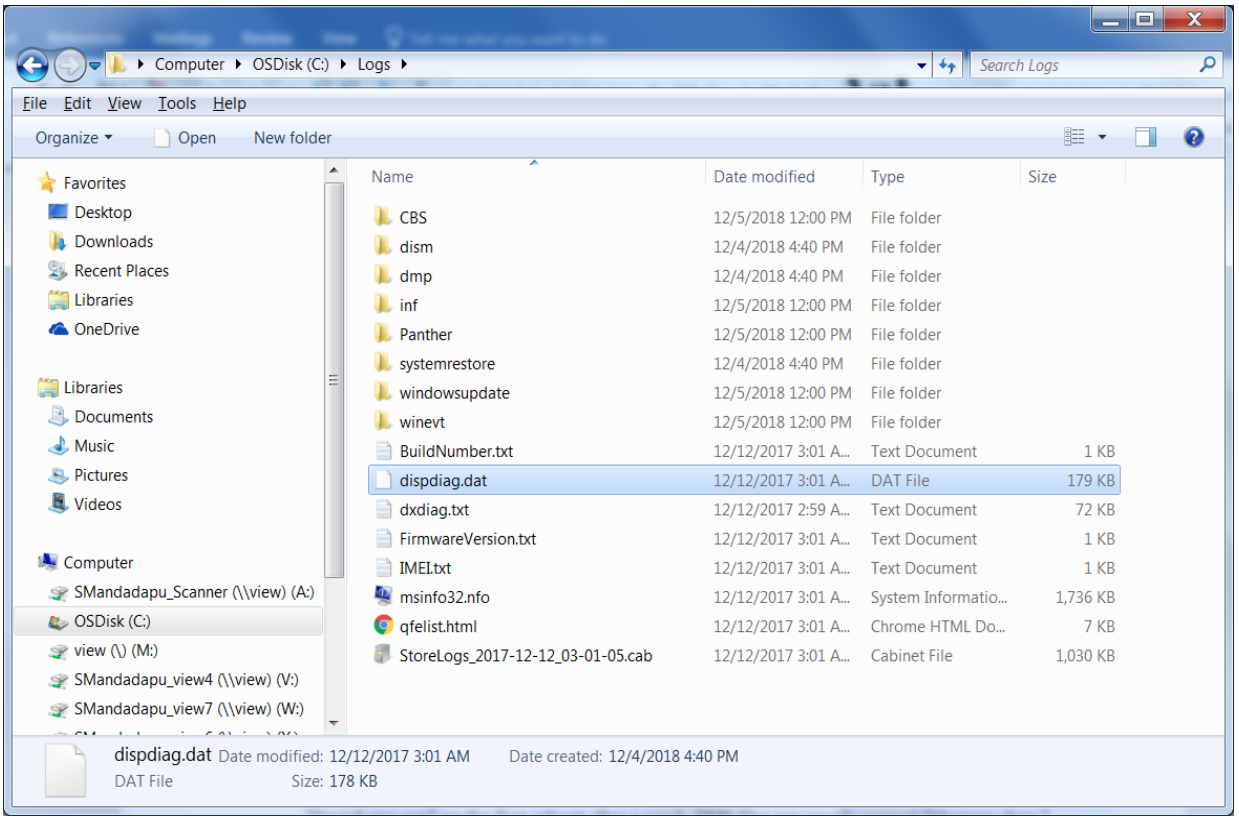


Figure (33): Display Info dispdiag.dat file

6. Build Number:

BuildLabEx: Provides the Windows update version
EditionID: Provides Edition (Professional or Enterprise) information of the Windows
ProductName: Provides Product name of the Windows (Windows 10 Enterprise)

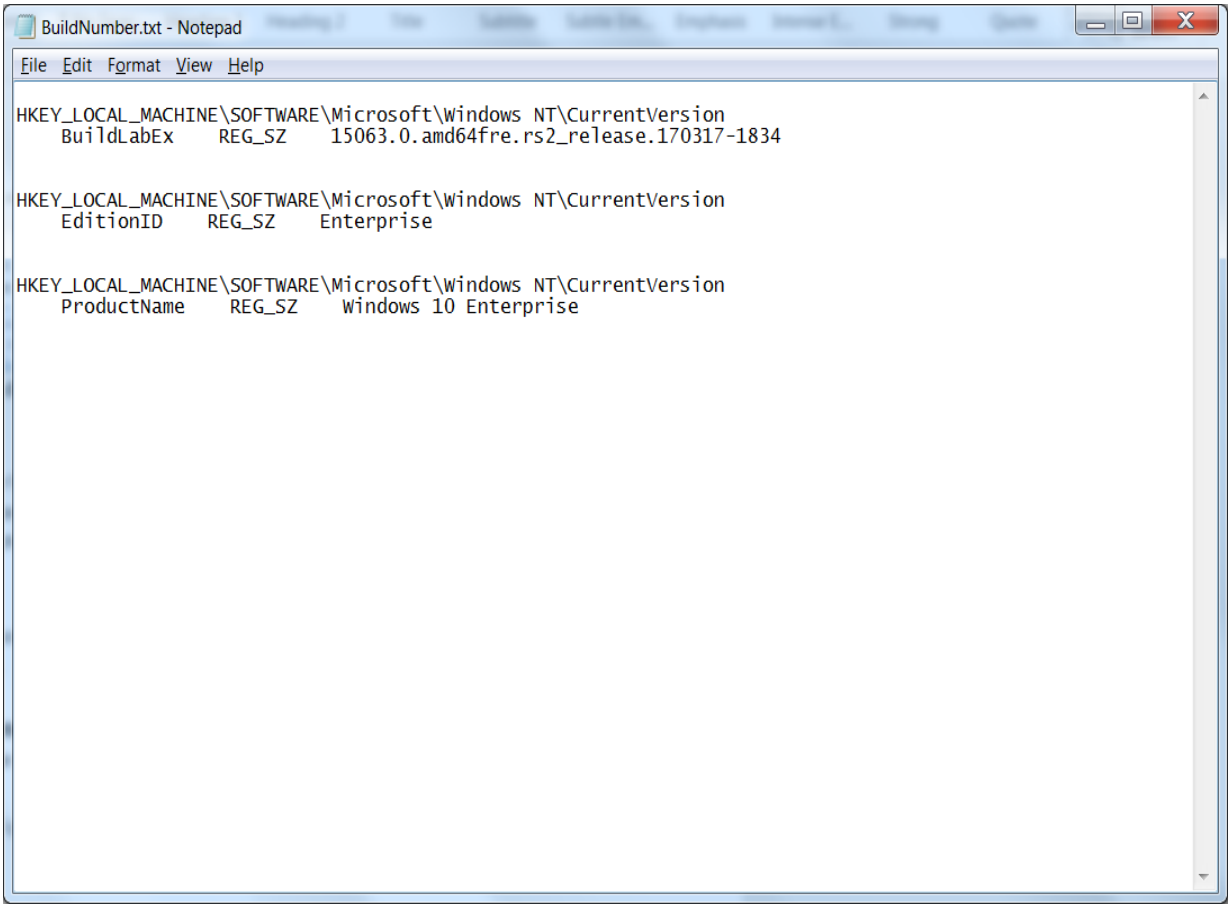


Figure (34): BuildNumber.txt file

7. IMEI:

Netsh mdn show interface will show the information about list of Mobile broadband interfaces available on the system.

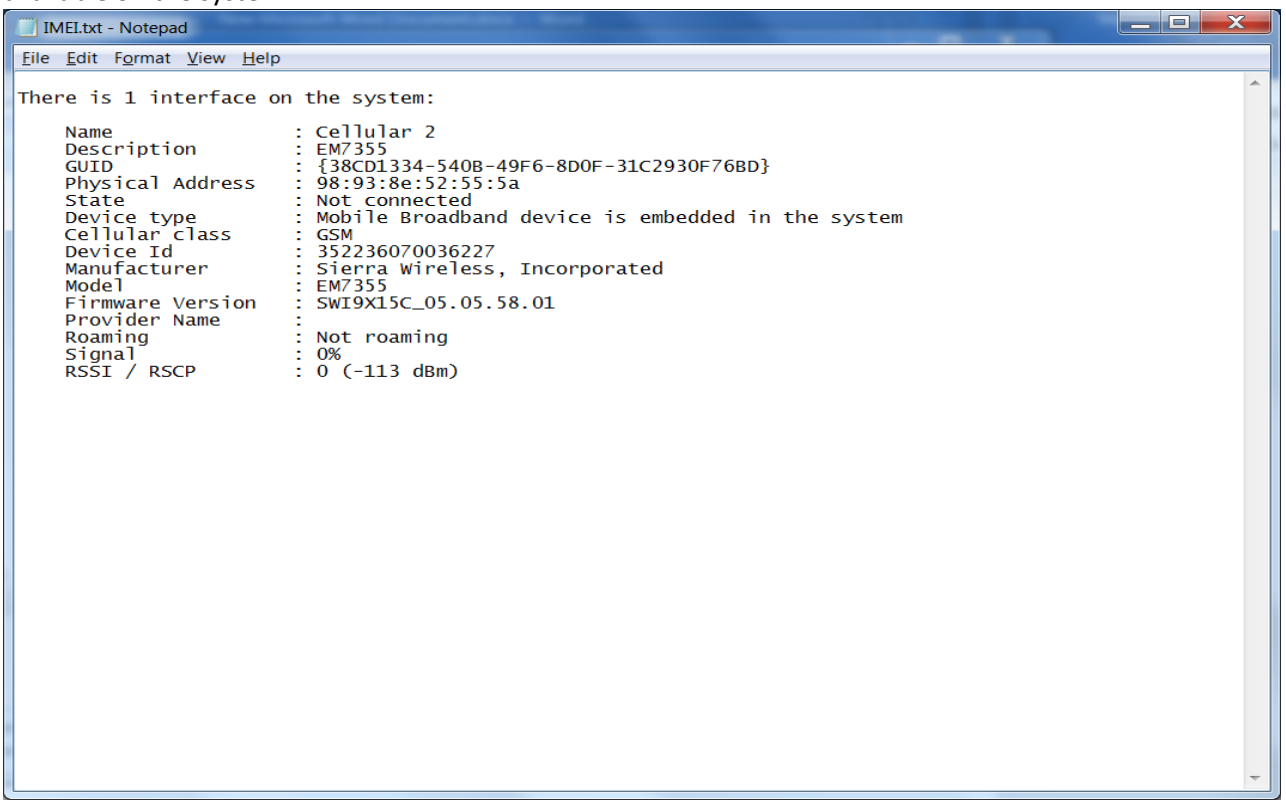
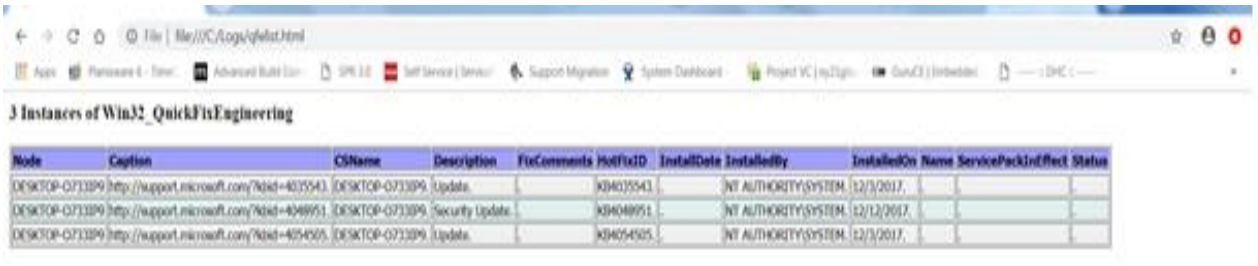


Figure (35): IMEI.txt file

8. List of Windows Updates:

Wmic qfe list will provide the list of all installed Microsoft and software updates.



3 Instances of Win32_QuickFixEngineering

Node	Caption	CSName	Description	FixComments	HotFixID	InstallDate	InstalledBy	InstalledOn	Name	ServicePackInEffect	Status
DESKTOP-G7133P9	http://support.microsoft.com/?kbid=4035543	DESKTOP-G7133P9	Update		KB4035543		NT AUTHORITY\SYSTEM	12/3/2017			
DESKTOP-G7133P9	http://support.microsoft.com/?kbid=4048951	DESKTOP-G7133P9	Security Update		KB4048951		NT AUTHORITY\SYSTEM	12/12/2017			
DESKTOP-G7133P9	http://support.microsoft.com/?kbid=4054505	DESKTOP-G7133P9	Update		KB4054505		NT AUTHORITY\SYSTEM	12/3/2017			

Figure (36): List of Windows Updates qfelist.html file

9. WSCollect Logs:

Collects few logs from system and saves it as cab file. It collects few windows updates and events.

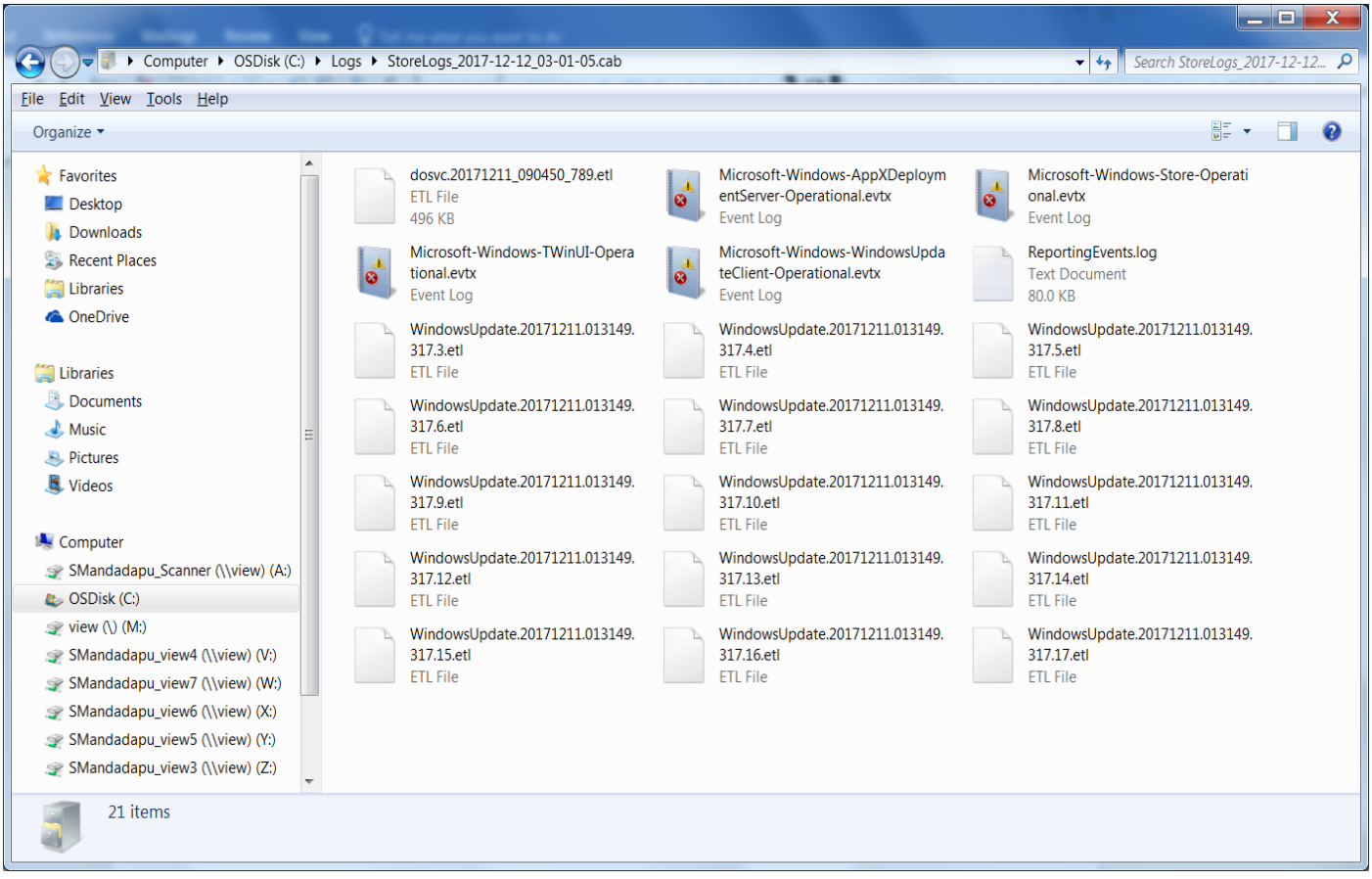


Figure (37): WSCollect Logs cab file