Volume-10| Issue-12| 2022 Research Article

IN COMPUTER SYSTEMS SEARCHING FOR WAYS TO IMPROVE THE EFFECTIVENESS OF VARIOUS TOOLS THAT DETECT CORRUPTED FILES

https://doi.org/10.5281/zenodo.7487649

Gafurov A.A
Qilichev E.J
**1 "Cybersecurity Center" State Unitary Enterprise, Head of UZSERT Department, Uzbekistan*
**2Master's degree, Faculty of Cyber-Security,Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan*

Abstract:. While the technology of computers has enabled consumers to communicate with people from around the world in the blink of an eye, all internet users will eventually face a situation in which they will have to deal with data or file corruption. In such circumstances, a particular video, image, or PDF file will essentially be rendered unusable or unreadable, causing a great level of stress and frustration to the individual that was looking to send or receive the said file. However, while file and data corruption are extremely common occurrences, many people may be unaware of the root causes that can lead to such corruption. As is the case with any other complex issue or problem, file and data corruption can result from a number of different factors, ranging from hard drive issues to technical problems.

Keywords:.... Physical hardware issues, power, malware infections, failed software, Cyber-security, bad program

Received: 22-12-2022
Accepted: 22-12-2022
Published: 22-12-2022

About: FARS Publishers has been established with the aim of spreading quality scientific information to the research community throughout the universe. Open Access process eliminates the barriers associated with the older publication models, thus matching up with the rapidity of the twenty-first century.

Introduction. Physical hardware issues are one of the primary factors that can result in data and file corruption. While hard drives, motherboards, central processing units or CPUs, and computer storage data allow computers to function in an effective and efficient manner, these components can break down from wear and tear in the same way that any other physical tool would. To this point, when a hard drive within a computer system crashes, the data that was held within the said computer can become corrupted. Alternatively, a failing motherboard within a computer can also cause data and file corruption within the system. Another factor that can result in file and data corruption within a particular computer system are power issues. To illustrate this point further, some users will shut down their computers by taking the plug out of the electrical outlet. While such practices may seem to be harmless on a surface level, they go against the electrical designs of the vast majority of computer systems. As such, shutting down a computer suddenly can also lead to file and data corruption, as the various files within the computer that were open when the shutdown occurred may not have been properly closed within the hard drive on the computer. As cybercrime can result in a number of adverse effects and consequences for online users, ranging from identity theft to financial loss, such actions can also cause files and data within a computer to become corrupted. With this being said, many cybercriminals will use malware infections in an attempt to retrieve various forms of personal information from online users, whether this is in the form of social security numbers, debit and credit

card numbers, or email addresses login credentials, among a host of others. In the process of trying to steal personal information from consumers, the files and data within the computers said consumers use can become corrupted. Bad program exits are another major factor that can lead to file and data corruption. As users will undoubtedly have a number of programs open when using their respective computers, failing to shut these programs down correctly can result in file correction. For example, a user may be using multiple programs within their computer when a power outage occurs due to inclement weather within the community they reside in. As the user in question did not have time to properly close the various programs they were using on their computer when the power outage occurred, the said user could find that the files within their computer were corrupted as a result. A final root cause of file and data corruption is failed software. Generally speaking, software failure is defined as the inability of a computer program to continue processing due to erroneous logic. This failure is typically caused by incorrect file system recovery within a particular computer, but also can occur as a result of resource conflicts between the operating and file systems within a computer. Irrespective of how a software program fails, such failures can lead to data and file corruption, as any work that a user when doing within the software program that failed will effectively be damaged. Despite the difficulties that online users may face when having their files or data corrupted, there are remedies available to mitigate the situation.

Materials. An online user's data or files have become corrupted as a result of hard drive issues, said user can perform a disk check on their hard drive. During this disk check, any bad sectors or issues within the hard drive may be repaired, and the user will then be able to access the files and data that had been corrupted. Conversely, as it pertains to preventative measures, users can also save all of their files via a backup on their hard drive, or to an external hard drive that can be accessed in the event that a computer becomes damaged beyond repair. In this way, online users can ensure that their files and data remain intact, even if the data within their computer becomes corrupted for any rhyme or reason.

Methods. This paper reveals that the most existing surveys in this area are either outdated or fail to provide a holistic view of the problem, since they usually focus on a specific subset of the standard

Results. Your Windows system is running slow or acting strangely, it may be difficult to pinpoint exactly what is causing it. It could be that you have picked up some malware or a virus, or it could be that some of your systems files are corrupted and so are unable to perform as they should.

There are dozens of reasons why your Windows files or system files might become corrupted, but among the most common are:

Sudden power outage

Power surge

Complete system crash

Mismatched versions

Updating errors

Fortunately, if you find yourself on the receiving end of any of these issues, there are steps you can take to fix them yourself using the System File Checker or the DISM (Deployment Image Servicing and Management) tools that are already pre-installed on your Windows operating system. Also, if you'd like to go beyond these basic tools, we offer reliable IT support in London for individuals and SMEs.

What does it mean if a file is corrupted?

A corrupted file is one that is damaged, and does not perform properly. This can apply to any type of file, from program files to system files and all types of documents. Just about everybody has probably had an issue with a corrupted file at some point in time. In many cases it can be resolved with a simple re-boot of your system, but sometimes the issues are more complex.

Every file on your computer has a particular structure and content. When this information is in the right place and arranged properly, the file will work as normal. However, if the wrong information is written into a file, or if the right information is written in the wrong place, it will affect the way the data is used and displayed. A corrupted file may not open at all, or it may appear scrambled and unreadable. This does not always indicate that the core program is corrupted, however – such as might be the case, for example, when a Microsoft Word file will not open, but all other files of the same type remain unaffected.

Application programs and operating systems may also develop corrupted files, which would then affect the use of items that depend on these programs to open or operate them.

How does a Windows file become corrupted?

File corruption usually occurs when there is a problem during the 'save' process. If your computer crashes, if there is a power surge or if you lose power, the file being saved will likely be corrupted. Damaged segments of your hard drive or damaged storage media may also be a potential culprit, as can be viruses and malware.

What to do if you encounter a corrupted file

If you have a file that you cannot open or suspect is corrupted for any reason, there are a few easy things you can do before you dive into anything too complex. First, try to open the file on another device or computer. If the file opens fine on another device, it is possible that the first computer has some corrupted system files you will need to address.

If the file still won't open on the second device or computer, consider deploying a file recovery program like Recuva, DMDE or the open source app PhotoRec. Most of these programs have a free version available that delivers pretty good results, locating the corrupted files, then recovering and repairing them if they can. Depending on your specific file recovery needs, there are plenty more applications to choose from, both paid and free. Start with the free version to see how deep your issues really are, and go from there. You will find that even files that you have written off completely, such as those that have been accidentally erased from a hard drive, removable drive or other storage device might be recoverable. It's certainly worth a try.

What are Windows System Files?

A Windows system file is seen by the operating system as being instrumental to the function of the system itself. They contain code that tells the computer how to respond and process commands. Moving them, deleting them or altering them in any way has the potential to cause widespread system failure or general instability.

Most system files use a .sys extension, but this is not a hard and fast rule. Other system files could include extensions like .dll, .pcf, .idx, .so, .dat, and others.

As an added layer of protection against deletion or unwitting alteration, these files might have 'hidden' attributes, or they may be 'read-only'. This is to prevent accidents from happening, as one click in the wrong direction can have catastrophic effects. These files will not be displayed in normal system searches, purely as a precautionary measure – just one more reminder that you shouldn't be messing around with these files in the first place!

Where are Windows system files stored?

Windows system files are stored in various places on your Windows operating system. Some are located in the Windows file system itself, and some will be in your program files. The primary folder (C drive on most Windows systems) also uses and stores several system files, including System Recovery and system volume information.

It is important to note that you cannot delete a system file that Windows is actively using. These files are locked and cannot be changed in any way. You might also find that there are duplicates of some systems files; these consist of previous versions and backups.

You can, however, unhide the hidden system files if you need to do so. Follow these steps to show all hidden files, folders and drives in a Windows system:

Go to COMMAND PROMPT

click on CONTROL FOLDERS

click on VIEW

select "SHOW HIDDEN FILES, FOLDERS AND DRIVES"

deselect "HIDE PROTECTED OPERATING SYSTEM FILES"

click OK

Once you complete this process, you will find that the files, folders and drives in question will all be dimmed, which means you won't likely be able to do anything with these files even though they are visible. Again, this is to protect the integrity of your operating system. While it is possible to toggle the attribute option for any file whether it is integral to system operations or not, it is never recommended. That being said, it is a handy trick to have up your sleeve, just in case your computer is affected by a particular virus – one that toggles the system attribute in order to hide all of your files, not just the system files. In this situation, it is perfectly safe to run these commands in order to locate and recover your files.

Using the system file checker (SFC) tool

The system checker file tool (also known as SFC) is a standard utility on all Windows systems. It scans your system to locate, repair and replace corrupted or altered files. If one of your system files has been modified or damaged, it will automatically update it to a clean version.

When to use the SFC

If your Windows system is running extremely slow, is buggy or blue-screening, if your apps are crashing and nothing seems to be working as it should, the SFC might be able to fix it. Running the SFC should be step one in your troubleshooting process. Even if it doesn't work, you will be able to confirm immediately whether or not it is your system files that are causing the problems.

Running the SFC command

Note: You can only run the SFC command from an administrator command prompt window. When you choose Command Prompt from the Start menu, you will see the option to run as an admin. For earlier versions of Windows, right-click Command Prompt and it will give you the admin option.

Type this into the command prompt window and hit enter:

sfc /scannow

Your scan may take several minutes to complete. Do not close the command prompt window while the scan is underway. Once the scan is complete, you will receive a message letting you know if Windows was able to fix your corrupt system files or not. It will also let you know whether or not it found any corrupted files at all.

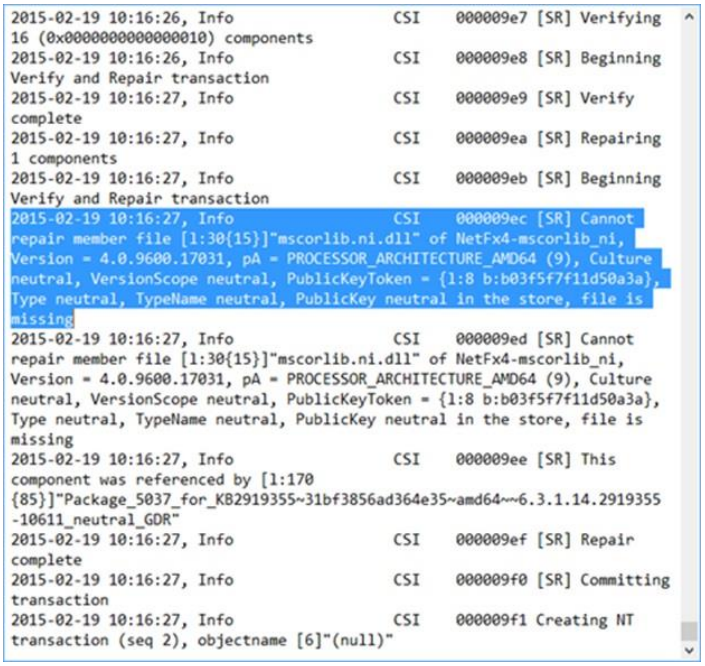
If the resulting message tells you that the SFC could not repair your corrupted Windows files, you can try rebooting your computer in safe mode. You can do this by holding the SHIFT key down during the restart. For Windows 7 or earlier versions, hold the F8 key during reboot. Once you have restarted in safe mode, run the SFC again.

You can also attempt to repair or replace the corrupted files manually. In this case, you would locate the corrupted files in the SFC process details and then manually replace the file with a good copy or a backup.

To locate the corrupted files, access the CBS.Log. you will find it at:

C:\Windows\Logs\CBS\CBS.log

Open the log file, and navigate to the corrupted files. Scroll down towards the end of the log, and look for entries that begin with “cannot repair member file”, as in this image:



Copy the message from the log and paste it into a search engine to locate specific information on how to fix your file.

Repairing corrupted Windows files with the DISM

The Deployment Image Servicing and Management tool should be your next line of defence, in case the SFC does not turn up any culprits.

Depending on how complex your issues are, you may think that it would be easier to reinstall Windows from scratch. The caveat here would be that you will then have the task of re-installing drivers, software and updates. So in all likelihood, running the DISM would make things easier, faster and less stressful.

To run DISM, enter this command into the Power Shell:

Dism /Online /Cleanup-Image /RestoreHealth

Once the command is running, it may take some time to complete. It is not unusual for it to seem to get stuck along the way, so be patient. Once complete, the log will either show that the files have been fixed, or it will show the errors it discovered. If there is an error, you will proceed to the next step, which is restoring the Windows disc image.

At this point, you will need to insert your installation media, which could be a DVD or a USB drive. If you do not have the physical media required, you will need to download the latest version of your Windows ISO and right click to MOUNT. This is in order to have a source to repair the corrupted files, and will replace only those files that need to be fixed, leaving the rest of your file system intact.

Once you have done this, run the appropriate DISM command, which can be found here.

As with the previous operation, this may take a while to complete. If all goes well, you will receive this message: "restoration operation completed" which would indicate mission accomplished.

At this point, you should run the SFC one more time to repair any lingering issues.

Professional file repair apps

If you are a developer, or if you run an office with several workstations, you might want to consider investing in a file repair app. Some of the top rated data recovery applications include:

Data Rescue PC4: compatible with SSD and RAID, and works on crashed and even erased drives.

Kroll Ontrack: Reviewers are impressed by how fast and easy-to-use it is, and how effective it is in recovering and repairing Microsoft Office files in particular.

Stellar Data Recovery: delivers one of the highest and most predictable recovery rates in its class. Following these security practices can help you reduce the risks associated with malicious code: Install and maintain antivirus software. Antivirus software recognizes malware and protects your computer against it. Installing antivirus software from a reputable vendor is an important step in preventing and detecting infections. Always visit vendor sites directly rather than clicking on advertisements or email links. Because attackers are continually creating new viruses and other forms of malicious code, it is important to keep your antivirus software up-to-date. Use caution with links and attachments. Take appropriate precautions when using email and web browsers to reduce the risk of an infection. Be wary of unsolicited email attachments and use caution when clicking on email links, even if they seem to come from people you know. (See Using Caution with Email Attachments for more information.)

Block pop-up advertisements. Pop-up blockers disable windows that could potentially contain malicious code. Most browsers have a free feature that can be enabled to block pop-up advertisements. Use an account with limited permissions. When navigating the web, it's a good security practice to use an account with limited permissions. If you do become infected, restricted permissions keep the malicious code from spreading and escalating to an administrative account. Disable external media AutoRun and AutoPlay features. Disabling AutoRun and AutoPlay features prevents external media infected with malicious code from automatically running on your computer. Change your passwords. If you believe your computer is infected, change your passwords. This includes any passwords for websites that may have been cached in your web browser. Create and use strong passwords, making them difficult for attackers to guess. (See Choosing and Protecting Passwords and Supplementing Passwords for more information.) Keep software updated. Install software patches on your computer so attackers do not take advantage of known vulnerabilities. Consider enabling automatic updates, when available. (See Understanding Patches and Software Updates for more information.)

Back up data. Regularly back up your documents, photos, and important email messages to the cloud or to an external hard drive. In the event of an infection, your information will not be lost. Install or enable a firewall. Firewalls can prevent some types of infection by blocking malicious traffic before it enters your computer. Some operating systems include a firewall; if the operating system you are using includes one, enable it. (See Understanding Firewalls for Home and Small Office Use for more information.)

Use anti-spyware tools. Spyware is a common virus source, but you can minimize infections by using a program that identifies and removes spyware. Most antivirus software includes an anti-spyware option; ensure you enable it.

Monitor accounts. Look for any unauthorized use of, or unusual activity on, your accounts—especially banking accounts. If you identify unauthorized or unusual activity, contact your account provider immediately.

Avoid using public Wi-Fi. Unsecured public Wi-Fi may allow an attacker to intercept your device's network traffic and gain access to your personal information.

Conclusion. In this paper we had surveyed an overview of techniques and tools for detecting and analyzing the malware. In particular, a light has been thrown on various tools available for malware detection, memory forensics, packet analysis, scanners/sandboxes, reverse engineering, debugging, and website analysis. Since most of the existing surveys usually focus on a specific subset of the standard, this paper provides a thorough study of tools for detecting and analyzing malware with a clear understanding of domain specific analysis.

REFERENCES:

1. S. K. Talukder, M. I. I. Sakib, and M. M. Rahman, "Model for egovernment in bangladesh: A unique id based approach," in 2020 International Conference on Informatics, Electronics Vision (ICIEV), May 2020, pp. 1–6.

2. S. Talukder and B. Carbunar, "When friend becomes abuser: Evidence of friend abuse in facebook," in Proceedings of the 9th ACM Conference on Web Science, ser. WebSci '17. New York, NY, USA: ACM, June 2021. [Online]. Available: http://doi.acm.org/10.1145/3091478.3098869

3. S. K. Talukder, M. I. I. Sakib, and M. M. Rahman, "Digital land management system: A new initiative for bangladesh," in 2019 International Conference on Electrical Engineering and Information Communication Technology, April 2019, pp. 1–6.

4. S. Talukder, I. I. Sakib, F. Hossen, Z. R. Talukder, and S. Hossain, "Attacks and defenses in mobile ip: Modeling with stochastic game petri net," in 2019 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE, 2019, pp. 18–23.