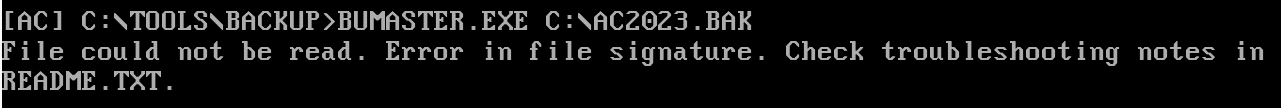
Learning Objectives

* Experience how to navigate unfamiliar legacy system.
* Learn about DOS and its connection to its contemporary, the windows command prompt.
* Discover the significance of file signatures and magic bytes in data recovery and file system analysis.

**What is MS-DOS?**

The disk operating system was a dominant operating system during the early days of personal computing. MS tweaked a DOS variant and rebranded it as MS-DOS, which later served as the groundwork for their graphical extension, the initial version of Windows OS. The fundamentals of file management, directory structures, and command syntax in DOS have stood the test of time and can be found in the command prompt and PowerShell of modern-day Windows Systems.

The goal for this task is to restore the AC2023.BAK file found in the root directory using the backup tool found in C:\TOOLS\BACKUP directory, the tool is called BUMASTER.exe.

A screen shot of a computer

Description automatically generatedKnowing this, I can view the readme.txt file using the type command.

I need to view the first couple of bytes and determine if they contain “41 43”.

**CheatSheet**

|  |  |  |
| --- | --- | --- |
| File Format | Magic Bytes | ASCII representation |
| PNG image file | 89 50 4E 47 0D 0A 1A 0A | %PNG |
| GIF image file | 47 49 46 38 | GIF8 |
| Windows and DOS executables | 4D 5A | MZ |
| Linux ELF executables | 7F 45 4C 46 | .ELF |
| MP3 audio file | 49 44 33 | ID3 |

What are file signatures/Magic bytes?

File signatures, commonly referred to as magic bytes are specific byte sequences at the beginning of a file that identify or verify its content type and format. These bytes often have corresponding ASCII characters, allow for easier human readability when inspected. The identification process helps software applications quickly determine whether a file is in a format they can handle, aiding operational functionality and security measures.

In cybersecurity, file signatures are crucial for identifying file types and formats. This is encountered during malware analysis, incident response, network traffic inspection, web security checks, and forensics.

Quickly creating a c program, using Borland Turbo C Compiler. Run using “TC <filename>”.

A computer screen with text

Description automatically generated

A screen shot of a computer

Description automatically generatedWhen inside, press ALT+C to get to the compile tab.

A screenshot of a computer

Description automatically generatedThen go to “Build All” option and select it.

Now Edit it.

A screen shot of a computer

Description automatically generatedNotice the following ASCII characters “MZ”, in the initial sequence of characters & symbols.

A screen shot of a computer

Description automatically generatedThese are the magic bytes of the file. Looking back at the cheatsheet above, MZ stands for Microsoft Executable. Knowing this I can view the AC2023.BAK which previously didn’t open.

The beginning of the sequence doesn’t show anything other than 2 ‘X’s.

**Question 1) How large (in bytes) is the AC2023.BAK file?**



**Answer**: 12,704 bytes.

**Question 2) What is the name of the backup program?**

A screenshot of a computer

Description automatically generatedLocated in C:\TOOLS\BACKUP, and contained within the file README.txt.

**Answer**: BackupMaster3000.

**Question 3) What should the correct bytes be in the backup’s file signature to restore the backup properly?**

A close up of a sign

Description automatically generatedAs previously stated, the file should contain a different pair of characters, that aren’t XX. Reading the trouble shooting, it mentioned that the file must contain “41 43” hex values respectively. I quickly went to convert hex to human readable and found the value to be “AC”.



**Answer**: 41 43

**Question 4) What is the flag after restoring the backup successfully?**

Using MS-DOS editor to modify the file.

A screenshot of a computer

Description automatically generatedThen using the command ALT + F (f = file) to save.

A black background with white text

Description automatically generatedThen finally running the command.

**Answer**: THM{0LD\_5CH00L\_C00L\_d00D}