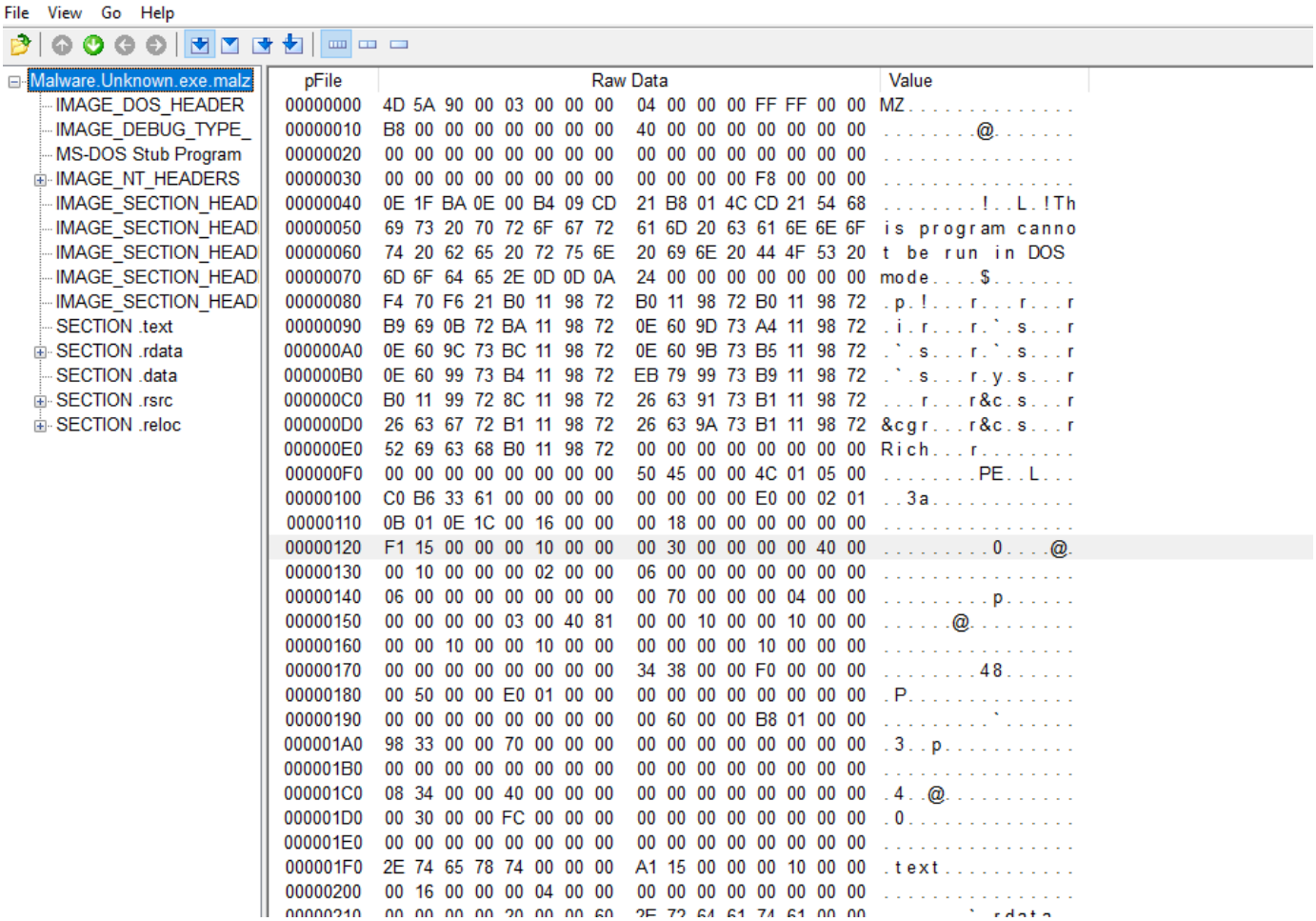
Analyzing the import Address Table (PE View)

Analyzing the import Address Table (PE View)

PE : Portable Executable

It is nothing more than a **gigantic array of bytes**, which will be our **Malware**

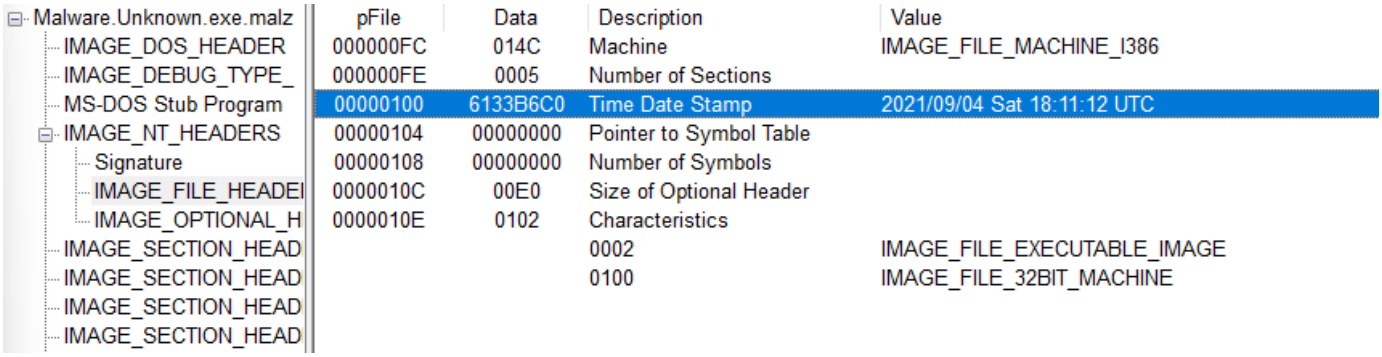
In PE view you can see **Pfile(Address)** ,**Raw Data** , **Actual value**.



This **MZ** The two starting byte will give you the idea what this file is.

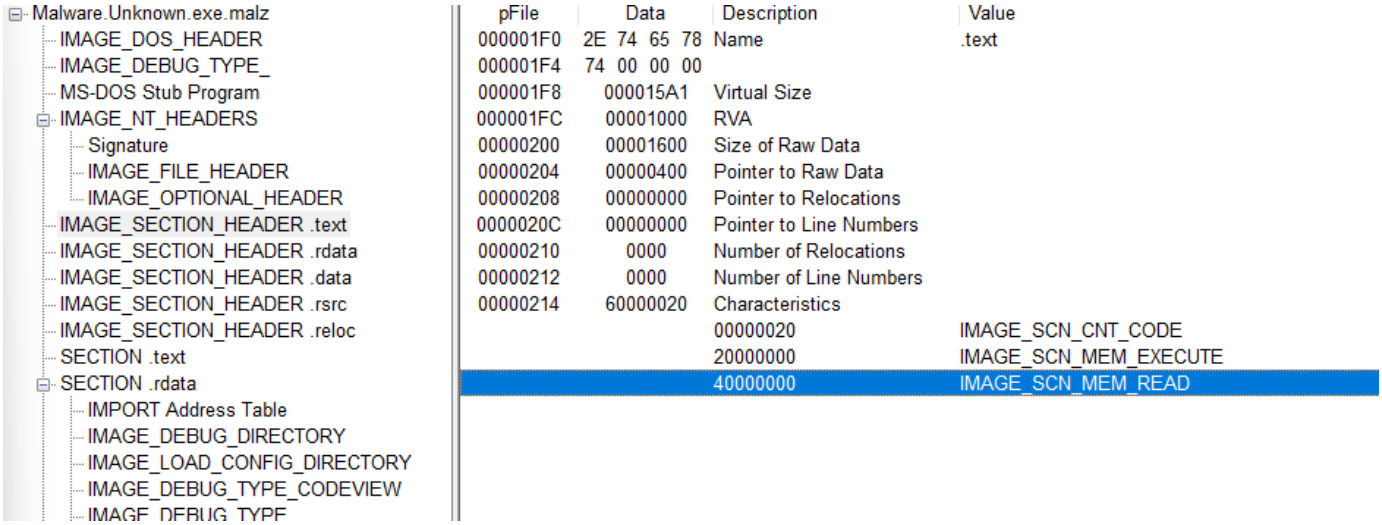
`IMAGE_FILE_HEADER` under `Image section` will have the **time stamp** which can be correct or incorrect.

The malwares compiled with Borland Delphi Compiler Will always have a timestamp of 1992



Now , Take a good look at `IMAGE_FILE_HEADER .text` Here we can see the **virtual size** and **size of raw data** , it will be in Hex ,So use a calculator to compare their size

If **Virtual size is** > **Size of raw data** then we may be dealing with a `packed binary`.



One of the Important Info We can get in `IMPORT Address Table` Under `SECTION .rdata`
To Understand this we have to understand **Windows API** .

- Dont forgot procmon,procwatch,proc explore (John.H)
- always open three of them for use
- regshot learn about about
    - To caputure wht registry changed and can compare
- cscript.exe run .js file in cmd