

1.What is the difference between a binary file and a text file?

A.1

Binary file:

- File has sequence of bytes that represent custom data.
- These sequence of bytes are arranged in a format that stores necessary information for the application.
- File that can contain various types of data format for instance video, audio and images.
- It can be interpreted by appropriate program.
- If opened in text editor appears as garbled values with may be some readable parts.
- If header of binary file is erroneous, the file no more will be interpreted by the software program. Because that is where the content of file is recognized.

Text File:

- File has sequence of bytes that represent characters.
- Every line in file ends with EOL. and every file ends with EOF.
- File follows a charter encoding scheme that tell how the content is to be interpreted and what content is to be displayed.
- Two files in which it can be stored: .rtf and .txt. RTF contains text as well additional features like bold, italics and page formatting style.
- Error in text file can be shown when opened with a text editor.

2. What is the ELF FILE Format? 2. What is a hexdump?

A.2

ELF:

Executable and Linkable Format (ELF,Extensible Linking Format) is a common standard file format for executables, object code, shared libraries and core dumps. It is dependent on any particular processor or architecture. Allowing it to be adopted by many different operating systems on many different platforms.

Hex dump:

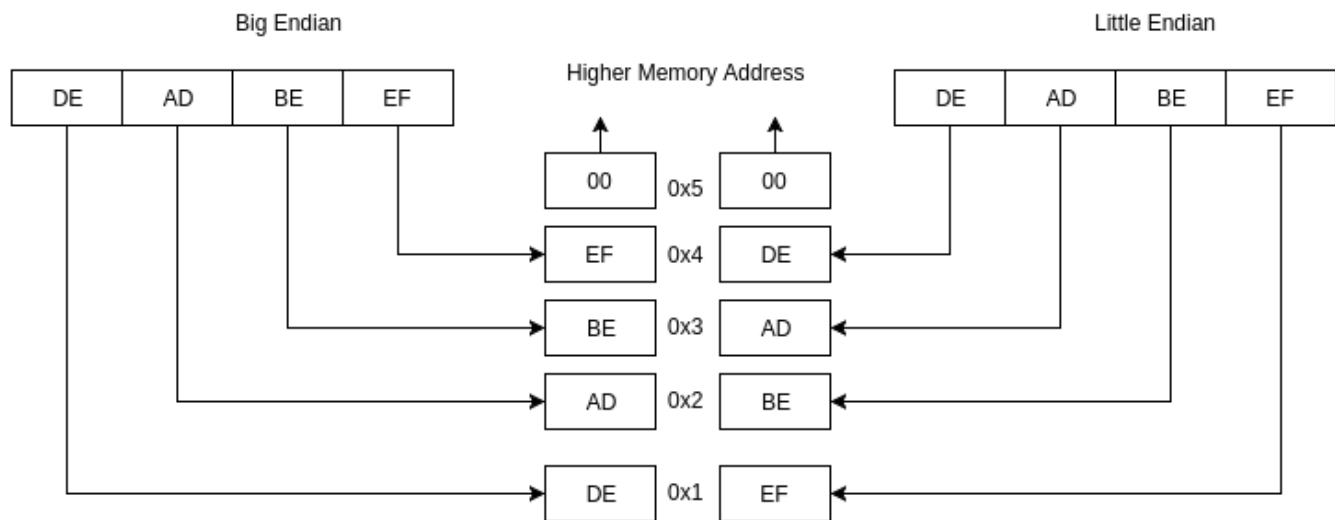
A hex dump is a hexadecimal view of computer data. Data can be from RAM or from a file or storage device. Used for debugging or for reverse engineering.

3. What kind of information is stored in a hexdump?

A.

Each byte is represented as a two-digit hexadecimal number. Hex dumps are commonly organized into rows of 8 or 16 bytes, sometimes separated by whitespaces. Some hex dumps have the hexadecimal memory address at the beginning or a checksum byte at the end of each line or both the information.

4. Diagrammatically represent how the hex characters “DEADBEEF” will be represented in Big Endian and Little Endian formats.



What does the strip command do?

strip command, program protection method. The strip command removes the symbol table and any debugging information from an executable.

Referred:

http://fileinfo.com/help/binary_vs_text_files

https://en.wikipedia.org/wiki/Hex_dump