HEX EDITOR GUIDE

Link to online Hex Editor: https://hexed.it

Guide Outline

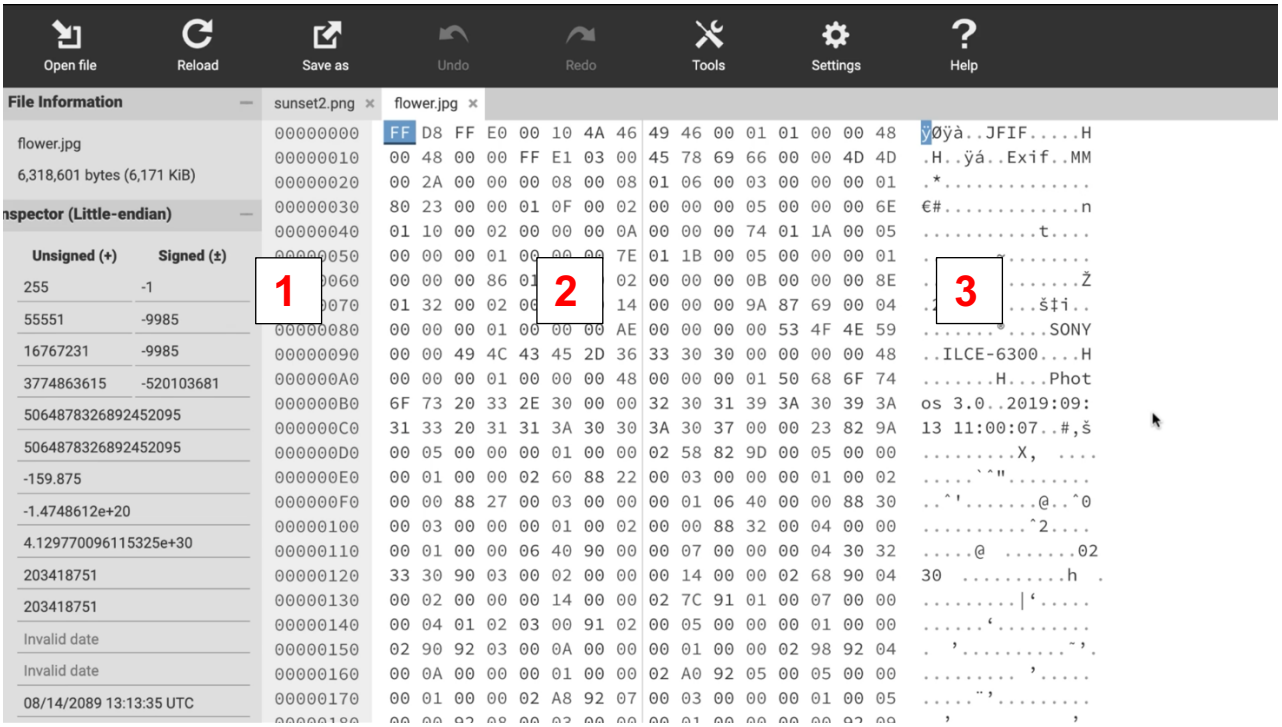
Hex Editor Overview

Visual Layout

The basic layout of a Hex Editor is usually divided into 3 sections:

1. Data Positions (Offsets)
2. Hex Columns – Bytes of data in hexadecimal format (1 pair characters = 1 byte)
3. Text Columns – Bytes of data in character encoding format (e.g. ASCII)

When you open a binary file, like an image (JPG, BMP, PNG) or even an executable (those are file that you can execute/run), it will look the this in a hex editor. You might recognize the Hexadecimal numbers (section 1) and ASCII characters (section 3) from SideQuest 0.



Let's Go Through The 3 Sections:

1 - Data Position

This is displayed as 8 hexadecimal digits. They represent the byte position, or "offset" showing you where the row of bytes is located within the file. If you move your cursor around on the data bytes, you'll often see your offset shown for easier locating.

For easier reading, the 8 digits are sometimes split with a colon ":"

0001:000F

Convert to decimal and you get 0x1000F = 65551. You're at byte #65551 in the file. You only need one "coordinate" for navigation in a file as it's just one long stream of numbers.

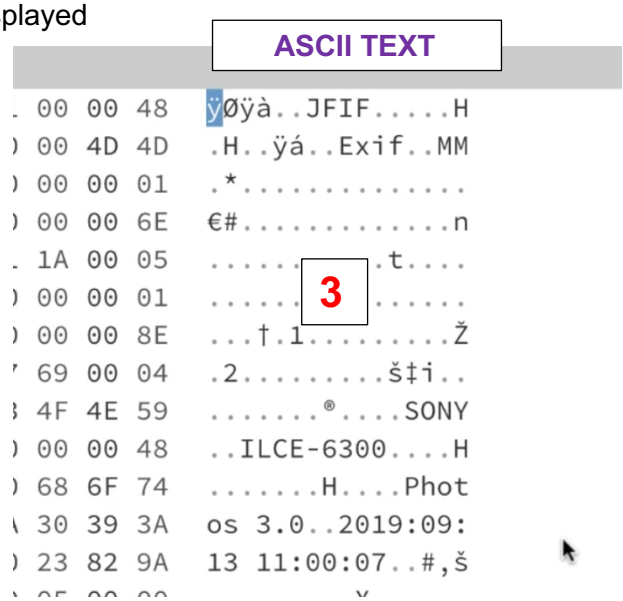
When you want to go to a certain position in the file, there's usually an option like "goto this offset" - very often the keyboard shortcut [Ctrl]+[G]

2 - Binary Data in Hexadecimal (Hex)

The middle section is the binary data as-is. Uninterpreted and just displayed byte-per-byte as a hex pair. If you see a "00" it means the number 0. If you see "FF" it's a full byte: 255.

3 - Binary Data In ASCII Character Encoding

Here you see each byte interpreted as a text character. Which text you'll see depends on the "character encoding". Non-printable characters are often displayed as dots "." – so it's easier to keep visual track when following byte positions.

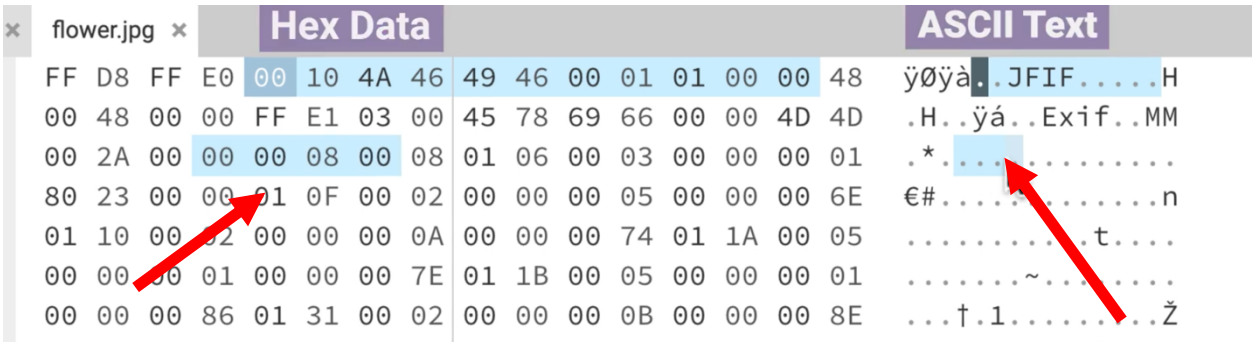


Some numbers are interpreted as alphanumeric characters. Don't be confused: they are not all real "text", but mere random characters. Their byte data is encoded numbers, so they are not meant to be displayed as characters. That's what makes viewing binary files as text so weird.

However, sometimes you will find real words, even whole chunks of readable text inside binary files. If you open a png file it will start with the letters "PNG" and a jpeg contains "JFIF" in its first bytes.

Reading, Analyzing & Searching the Data

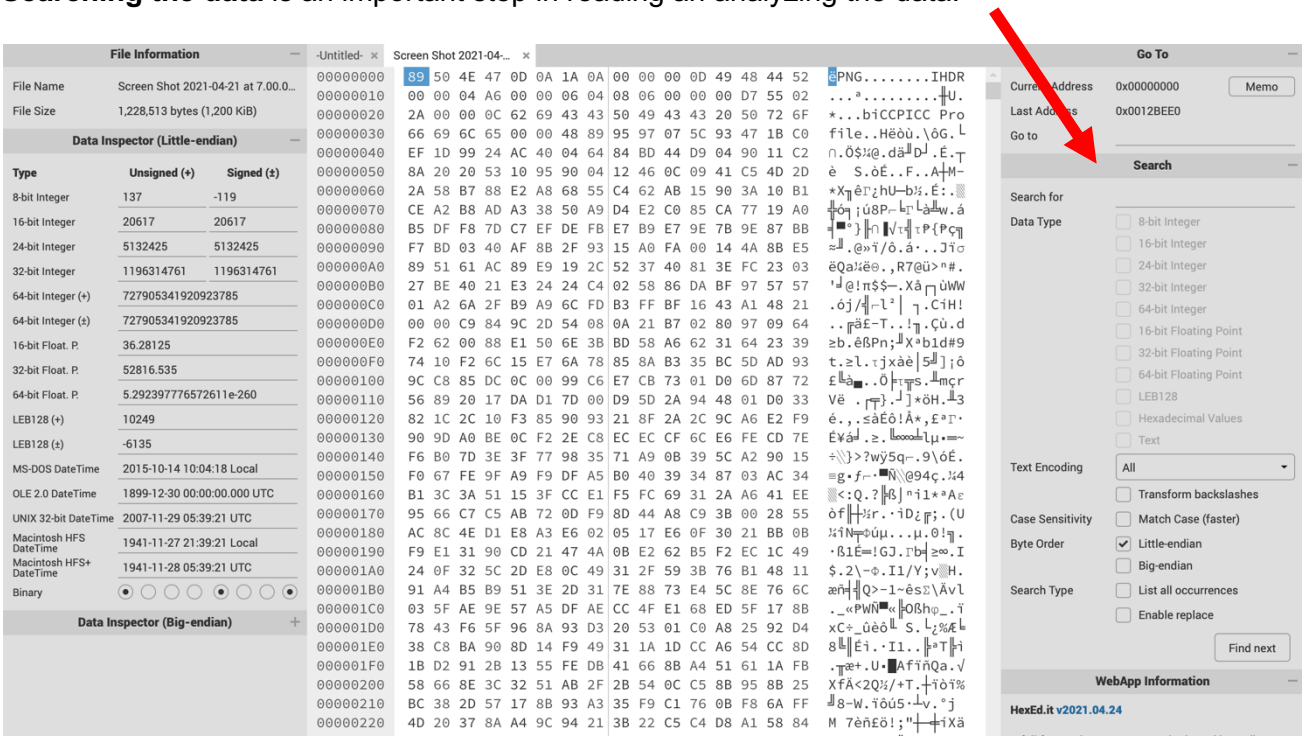
A hex editor has a cursor that can be moved by clicking with the mouse or using the cursor keys. You will see your cursor somewhere (not your mouse cursor, but a text cursor) that usually blinks or highlights a position in the file.



There should be 2 positions highlighted. They both show the same position in the file, but in 2 different views:

1. One in the Hex column
2. One in the ASCII text column

Searching the data is an important step in reading an analyzing the data.



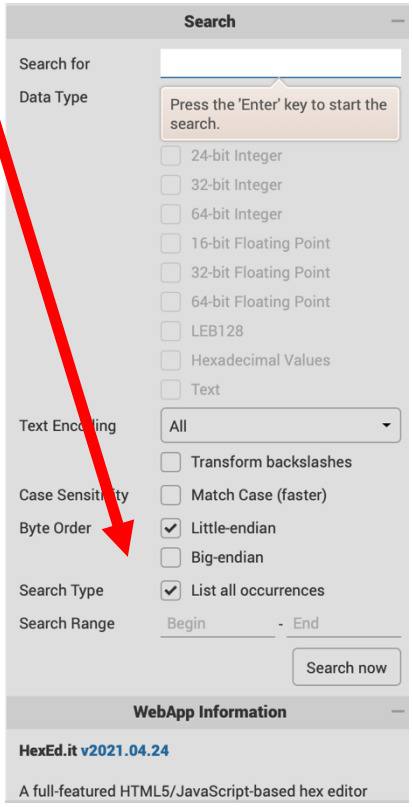
To do this:

- Use the search panel on the right side of the screen (you may have to expand the application window to reveal it.

- Make sure the following are checked off: Little-endian and List all occurrences
- You can use the shortcut keys for copy and paste to enter the Hex signature you are looking for in the search box.

  Shortcut for Copy = [CTRL]+c / for mac users [Command]+c
  Shortcut for Paste = [CTRL]+p / for mac users [Command]+v

- Press “Enter” key to start the search



Editing Text

Data can be edited in a hex editor just like a normal text editor. You can edit the file by its **Hex value** or its ASCII **text character**. To do this use the mouse to click on a specific position in either column.

1. Position the cursor over the byte you want to edit, and type the value you want to change. In this Hex Editor it will **“overwrite**” the current bytes.
2. When the cursor is in the hexadecimal area, you have to enter byte values in hexadecimal notation.
3. When the cursor is in the ASCII text character area, you can enter regular characters just like a text editor.

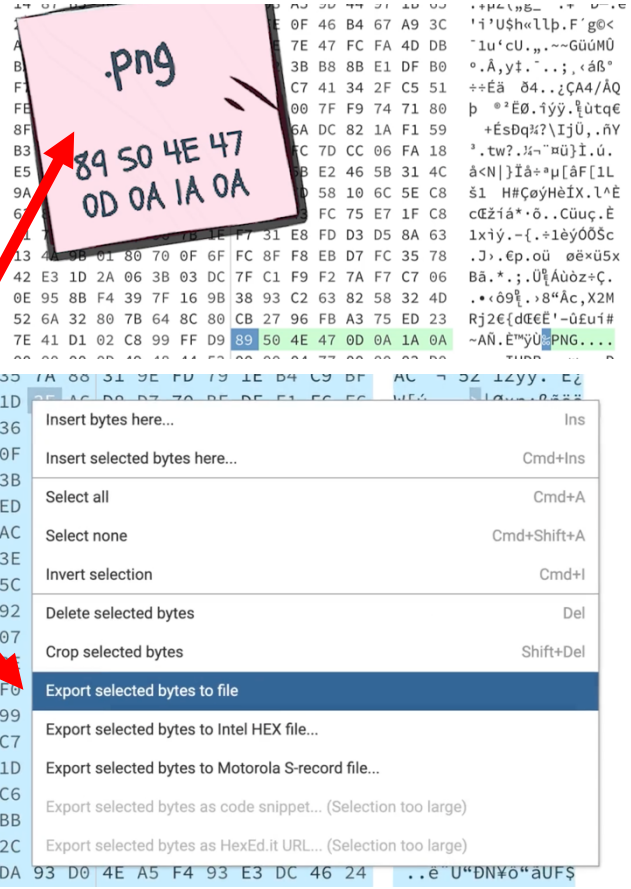
Some hex editors have an **Overwrite** mode and an **Insert** mode. In Overwrite mode, typing values on the keyboard just changes the existing byte values. In Insert mode, typing on the keyboard inserts new bytes into the file.

Data can also be edited by selecting a set of bytes to export out as a new file or delete. Selections are made just like a text editor:

1. click and drag the mouse over the bytes you want to select OR
2. hold the 'Shift' key while moving the cursor to the last byte you want to select
3. use the right click on your mouse to access options

Fixing Files Step-By-Step

- Check if file opens
- Make a note of the **File Extension**
- Using the File Signature Key make a note of its corresponding **File Signature (Hex Value and ASCII identifier)**
- Open online Hex Editor: https://hexed.it



If File Did Open – File is Embedded in Another File

1. Open file in Hex Editor
2. Look for the matching Hex Signature and ASCII identifier (these should correspond to the File Extension).
3. Search for another Hex Signature. If you find it make a note of its file extension.
4. To extract it highlight or select everything from this Hex Signature to the end of the document.
5. Right click and choose the option – Export selected bytes to file.
6. Save it to the desktop and add the File Extension that matches the Hex Signature.
7. Open file.

If File Did NOT Open –

Check to see if the Current File Extension is Incorrect

1. Open file in Hex Editor.
2. Figure out what type of file it may be based on Hex signature and ASCII identifier.
3. If the Hex and ASCII identifier match, the file has an incorrect file extension.
4. Add to the file's title the proper file extension based on Step 3.
5. Save file to desktop.
6. Open file.

Check to see if Hex Signature is Corrupted

1. Open file in Hex Editor.
2. Figure out what type of file it may be based on Hex signature and ASCII identifier.
3. If the Hex and ASCII identifier do not match which of these looks suspicious?
4. Replace (Overwrite) what you found with the correct Hex signature value.
5. Save file to desktop.
6. Open file.