HEX Explained

In the context of digital forensics and the FAT (File Allocation Table) file system, HEX typically refers to hexadecimal representation. Hexadecimal is a numeral system that uses a base of 16, which makes it particularly useful in digital forensics for representing binary data in a more human-readable form.

Hexadecimal is just another way of counting, like the numbers you already know. Normally, we use ten digits (Decimal): 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. But in hexadecimal, we use sixteen different digits instead of ten. So, besides the regular numbers, we also use the letters A, B, C, D, E, and F.

Think of it like this:

- In our normal counting, we go from 0 to 9, and then when we run out of digits, we add one to the next place. For example, when you count to 9, the next number is 10, and then 11, 12, and so on.
- In hexadecimal, we go from 0 to F (which is 15 in regular numbers), and then we add one to the next place. So, when you count in hexadecimal, it looks like 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10, 11, and so on.

This way of counting is very useful in computer programming and when working with things like file systems (like FAT) because it is a convenient way to represent binary data (0s and 1s) in a more human-readable format.

So, to sum it up, hexadecimal is just a different way to count, using numbers and letters, and it helps us work with computers and data more easily.

In a FAT file system, HEX can be important for several purposes:

1. **File Data Representation**: The content of files and the file system structure itself are stored in binary format. Hexadecimal representation helps forensic analysts view and interpret the binary data more easily. They can examine the HEX values to understand the structure of the file system and recover data or investigate potential anomalies.
2. **Hexadecimal Editor/Viewer**: Forensic analysts often use hexadecimal editors or viewers to inspect the raw data on storage media. These tools allow them to view the contents of a disk or a specific file in HEX format, which is useful for detecting hidden or deleted data, file headers, and other structures within the file system.
3. **File Signature Analysis**: HEX is used to identify file types and signatures. Each file type has a unique HEX signature or header that allows forensic tools and analysts to recognize and

categorize different types of files. This is crucial for file recovery and analysis (Explained further below).

4. **Carving and Recovery**: In data recovery and forensic investigations, HEX is important for file carving. This process involves searching for file headers and footers in raw binary data to recover files that may have been deleted or lost. HEX values are used to identify the beginning and end of file structures.

5. **Data Integrity Checks**: HEX values can be used to perform integrity checks on the file system and its data. Comparing HEX values of files or sectors to expected or known values can help identify data corruption, tampering, or inconsistencies.

6. **Error Analysis**: When analysing a FAT file system for errors or inconsistencies, HEX can be used to examine the values stored in the File Allocation Table (FAT). Changes to HEX values in the FAT can indicate potential file system errors or tampering.

In summary, HEX, in the context of FAT file system forensics, refers to the hexadecimal representation of binary data. Forensic analysts use HEX values to investigate, recover, and analyse data from storage media while looking for file structures, signatures, anomalies, and data integrity issues. It plays a significant role in file system analysis and recovery efforts in digital forensics.

File Signature Analysis is a fundamental concept in digital forensics and data recovery. It involves using hexadecimal (HEX) values or binary patterns at the beginning of a file (often referred to as a "file signature" or "magic number") to identify and categorize different types of files. Here is a more detailed explanation with examples:

1. **File Signatures (Magic Numbers)**: A file signature, or magic number, is a unique sequence of bytes at the beginning of a file that indicates the file's format or type. These signatures are typically in hexadecimal format. Different file formats have distinct signatures, and these signatures are recognized by forensic tools to determine the file type.

2. **Identifying File Types**: By analysing the HEX values at the beginning of a file, forensic analysts can determine the file type. For example, a PDF file might start with the HEX values "25 50 44 46" (which represents "%PDF"), while a JPEG image file may begin with "FF D8 FF E0" or "FF D8 FF E1." These unique HEX patterns help identify the file format.

  - Example 1: A JPEG file often starts with the HEX values "FF **D8** FF E0" Start of Image (SOI marker).
  - Example 2: A PNG file typically begins with "89 50 4E 47 0D 0A 1A 0A" (signature of a PNG file).

3. **File Recovery**: File signature analysis is crucial for file recovery because even if file system metadata (e.g., file names and locations) is lost or damaged, the file signatures remain intact. Forensic tools use these signatures to locate and extract files from storage media.

4. **Analysis and Categorization**: In digital forensics, once the file types are identified through file signature analysis, forensic analysts can categorize and organize files based on their types. This is especially important when dealing with large volumes of recovered data.

   - For instance, identifying and categorizing image files, document files, or executable files allows investigators to focus on specific types of evidence or relevant information.

5. **Data Carving**: File signature analysis is essential for a process known as "data carving." Data carving involves scanning raw disk images or unallocated disk space to locate and extract files solely based on their signatures. This can be useful in recovering deleted or partially overwritten files.

   - For example, if a digital forensics tool encounters the PDF file signature "%PDF" within a raw data stream, it knows that it has located the start of a PDF file and can then extract and reconstruct the entire file.

In summary, file signature analysis using HEX values is a critical technique in digital forensics for identifying, categorizing, and recovering files from storage media. Each file format has a unique HEX signature or magic number that helps forensic tools and analysts recognize the file type, even when other file system metadata is missing or damaged. This process is instrumental in evidence recovery and analysis during forensic investigations.

Common file signatures or magic numbers:

1. JPEG Image:

   - Magic Number: FF D8 FF
   - Description: Identifies JPEG image files.

HEX Explained

2. PNG Image:
   - Magic Number: 89 50 4E 47 0D 0A 1A 0A
   - Description: Identifies Portable Network Graphics (PNG) image files.
3. GIF Image:
   - Magic Number: 47 49 46 38 37 61
   - Description: Identifies Graphics Interchange Format (GIF) image files.
4. PDF Document:
   - Magic Number: 25 50 44 46 2D
   - Description: Identifies Adobe PDF documents.
5. ZIP Archive:
   - Magic Number: 50 4B 03 04
   - Description: Identifies ZIP archives, used for compression and packaging files.
6. Microsoft Word (DOCX):
   - Magic Number: 50 4B 03 04
   - Description: Identifies Microsoft Word documents in the newer Office Open XML format.
7. MP3 Audio:
   - Magic Number: 49 44 33
   - Description: Identifies MP3 audio files.
8. Microsoft Office Documents (DOC, XLS, PPT):
   - Magic Numbers: Varies depending on the specific format (e.g., DOCX, XLSX).
   - Description: Identifies various Microsoft Office document formats.
9. HTML Document:
   - Magic Number: 3C 21 44 4F 43 54 59 50 45 20
   - Description: Identifies HTML documents.

10. Executable Files (Windows PE):
    - Magic Number: 4D 5A
    - Description: Identifies Windows Portable Executable (PE) files, including executables and dynamic link libraries.
11. Unix Executable Files:
    - Magic Number: 7F 45 4C 46
    - Description: Identifies Unix or Linux executable files.

These magic numbers are essential for file identification and are used by software to determine how to interpret and handle files. They play a crucial role in file format recognition and validation.