# Fields Associates
Litigation Consultants

Speak directly to a qualified member of staff
**0845 301 5778**


Within the world of digital forensics, metadata is a term that is used frequently and, whilst you may be unfamiliar with why this is or precisely what it is, it consistently provides important information that is used to obtain insights and formulate robust arguments. But what exactly is it?

In simplistic terms, metadata is data about data. To put it another way, it is information about key files that can be used to construct compelling narratives. A skilled forensicist can use metadata to determine when a file was created, who created it, the number of times it has been and when it was modified, if it has been printed, whether an individual has deleted it and much more. Such information is vital as it can allow legal individuals to build a plausible course of events and disprove or cast significant doubt over presumptions in accordance with their requirements.

Metadata is equally useful within the field of electronic discovery. By analysing metadata, it is possible to glean a significantly better understanding of which data, being stored by a company or institution, is likely to be of high-value and which is of less importance. Consider, for example, a file that has been accessed several-thousand times by multiple individuals employed by the same company. It is only logical to conclude that said file is likely to have high importance and is worthy of preserving. In comparison, files that are very rarely accessed are, of course, less likely to possess value. It would be possible to determine the value of various electronic files by interviewing staff or reviewing the files themselves, but reviewing metadata is a highly-efficient and much more cost-effective means of identifying data that is valuable and worth protecting on a long-term basis.

Key to successfully analysing the metadata held on a device are the tools that a forensicist employs. Metadata must be extracted before it can be analysed and specialist niche software must be utilised as a result. Unfortunately, much of the software that is widely used will extract metadata from only certain file types and will ignore others in spite of the fact that it is likely that this data will contain information that is just as revealing as that which is held in more common file types such as word documents or images. It is therefore essential that, before seeking the help of a forensicist, that you ensure that they will be able to extract all rather than just some of the metadata held on the device in question. It should also be noted that extracting and analysing the data can, depending on the volume of data available, be a time-consuming process.

Ultimately, the process of analysing metadata is essential to forming the exact and precise narrative needed in order to obtain a conviction or acquittal. It is, and will forever be, an essential part of digital forensics.