Digital Evidence – Metadata.

What is and its use in courts.

By Er. Sandeep Suri, Advocate, Chandigarh

*The author is Managing Partner, **SUBROS and Associates**, Lawyers and Advocates, Chandigarh/Delhi and a qualified Electronics Engineer.*

WHAT IS METADATA

Unravelling the Mystery: Understanding Digital Evidence Metadata

HOW IS METADATA USED IN COURT

Metadata is both discoverable and admissible in court.

How Is Metadata Collected And Preserved As Evidence

What is forensic metadata and how is it used in court cases

How Is Forensic Metadata Collected And Analyzed

What Types Of Metadata Are Collected In Digital Forensics Investigations

Examples Of System Metadata

IN CONCLUSION

The Power of Metadata: How it Helps Solve Crimes and Protects Our Digital World

—-

The present is first in a series of Articles and Video casts dealing with Electronic evidence and its proof, Stay tuned!

Metadata can be used as evidence in both civil and criminal cases.

In this digital age, every piece of information we create and share leaves a digital footprint that can be used as evidence in investigations. Metadata, though not often considered by

the average user, plays a key role in digital evidence. It provides crucial details about the origin, creation, and transmission of digital files. In this article, we will explore the importance of metadata in digital evidence and how it helps solve crimes and protect our digital world.

Digital evidence, including metadata, can be used in criminal cases to corroborate and establish necessary elements of prosecution and defense cases. Electronic evidence provides unique information that may not otherwise be available in tangible form or from other sources. Metadata is a hidden, powerful component of electronic evidence that can be used to describe the characteristics, origins, usage, and validity of electronic evidence.

Metadata is information about data that can be used to describe the characteristics, origins, usage, and validity of electronic evidence. It can be hugely beneficial to legal professionals in painting a digital timeline of events. Metadata attaches to electronically stored information (ESI), making it useful for legal professionals to figure out the who, what, when and where of files. In litigation, metadata is evidence that describes the characteristics, origins, usage and validity of electronic evidence. As Metadata of electronic files it describes their unique characteristics, origins, etc. it can be used as evidence in court to authenticate electronic evidence and to prove the who, what, when, and where of files. It can also be used to show if a file has been tampered with or falsified. Missing metadata could prove that evidence has been altered or falsified.

However, metadata can also be misleading if there are inconsistencies or if it indicates that a file may have been tampered with. Therefore, it is important for legal professionals to spot metadata anomalies and ensure its reliability before using it as evidence in court.

If help of experts who understand the nuances of technology and law is to be used, then so be it.

WHAT IS METADATA

Unravelling the Mystery: Understanding Digital Evidence Metadata

Digital evidence metadata can be defined as the hidden data that resides within digital files, providing information about the file’s location, creation date, modification date, and other relevant data. It includes data that is automatically created by software or hardware, including cameras, smartphones, and computers. Despite its importance, metadata is often overlooked in digital investigations. However, it can be the difference between a successful investigation and a failed one.

Metadata is data that provides information about other data. It summarizes basic information about data, making it easier to find and work with particular datasets.

Metadata can be classified into different types based on their purpose. It can be divided into two categories: descriptive and technical. Descriptive metadata provides information

about the file content, such as the author, creation date, and keywords. Descriptive metadata describes a resource for purposes such as discovery and identification..

Technical metadata, on the other hand, provides technical information about the file, including the file format, resolution, and compression settings. Accessing and analyzing metadata requires specialized tools and expertise, and it is essential to preserve the integrity of the metadata in any investigation. Metadata can be applied to anything, including computer files, books, or pieces of art.

Uses of Metadata

Structural metadata indicates how compound objects are put together, for example, how pages are ordered to form chapters. Administrative metadata provides information to help manage a resource, such as when and how it was created, file type and other technical information, who can access it, and how long it should be kept. Metadata management strategies are used to improve data analytics, develop a data governance policy and establish an audit trail for compliance purposes. Without metadata, a dataset is incomprehensible; hence the importance of metadata in understanding datasets.

In summary, metadata is essential in providing context with details such as the source type owner and relationships to other datasets. It helps understand the relevance of a particular information / dataset and guides on how to use it.

HOW IS METADATA USED IN COURT

Metadata is both discoverable and admissible in court.

It is extremely useful for authenticating evidence because it often shows the author and creation date for files. Digital forensics experts use metadata to investigate cybercrime cases putting to use complex methods such as forensics and eDiscovery software to view metadata that is not readily available.

The key role of metadata in litigation is to prove the credibility of ESI (Electronically Stored Information). Modern cases rely heavily on data; therefore metadata can be vital in litigation. You can use metadata — such as file creation date — to prove or disprove a claim’s validity. A good example would be a doctor claiming they updated a record immediately after a medical process. However, the metadata shows they had not updated the file until a week later. Digital photographs can also contain GPS coordinates within their metadata, proving where someone took a photo. (How to obtain the same will be part of our video series!!!)

In the 2018 United States Supreme Court case of, ***Carpenter vs. the United States***, geolocation metadata gathered from cell towers was used as evidence in court. The case involved whether law enforcement officials needed a warrant to obtain cell phone location data from wireless carriers. The Supreme Court ruled that obtaining this data without a

warrant violated the Fourth Amendment. (The Fourth Amendment of the U.S. Constitution protects people from unreasonable searches and seizures by the government. It is the basis of the law regarding search warrants, stop-and-frisk, safety inspections, wiretaps, and other forms of surveillance. It also protects against arbitrary arrests.

How Is Metadata Collected And Preserved As Evidence

Metadata can often count as substantial evidence in modern cases. It attaches itself to all electronic files, leaving information that can help uncover details about a particular case and authenticate and interpret evidence. To ensure digital evidence can be used in court, data collections must be done correctly to avoid altering key information/metadata. It is data not only about the condition of files on the device but in cases about the device itself, and its appropriate preservation, collection, and production are continuing challenges in ESI's discovery process.

What is forensic metadata and how is it used in court cases

Metadata can be collected through complex methods such as forensics and eDiscovery software. Metadata can also be used as forensic evidence to help prove cases, solve crimes and assist in investigations. It can provide descriptive information about the piece of data collected such as time and GPS location where it was taken. Metadata is more than "data about data." It's often very useful evidence, and litigators will be more effective in discovery if they understand how metadata works.

Metadata is both discoverable and admissible in court. However, it may be necessary to retain an expert witness to authenticate metadata.

Properly preserved metadata can help uncover information about a particular case and authenticate evidence at trial. Unfortunately, like other forms of ESI (electronically stored information), it implicates a variety of new concerns too.

Metadata can be found in various forms, including descriptive, internal, and external metadata. Whereas as mentioned above, Descriptive metadata provides basic information about a file or piece of art, such as who created it and when it was created, Internal metadata is stored within the file itself and can be found in files like Word documents and Excel spreadsheets, External metadata includes information like the sender and subject of an email. (Do you know how a simple email can be provided? Keep a lookout for our video series on Digital Evidence, coming soon). It can also provide valuable information about the location and time a file was accessed.

Digital forensics experts use good practices to maintain the data integrity of suspected files while locating evidence using seizure, search, or retrieval techniques. The first step in this process is to perform a hash of the suspect files or media. A clean copy of the original data files is made called evidence media. Once this copy is made, a comparison of the hash shows whether any changes have been made to the original data files.

In summary, forensic metadata provides valuable information about electronic evidence

that can be used in court cases. It helps legal professionals figure out who created a file, when it was created or accessed, and whether it has been tampered with or falsified. Digital forensics experts use good practices to maintain data integrity while locating evidence using seizure, search, or retrieval techniques.

How Is Forensic Metadata Collected And Analyzed

Metadata is data and information that is part of or attached to some other more obvious piece of data. It can include the date that files were created, times at which edits to the original file were made, timestamps from the most recent access, and the GPS location of where it was taken eg photographs. Metadata can be used to help prove cases, solve crimes, and assist in other investigations. It is also used to authenticate documents and discover when files were created.

Forensic metadata is collected by performing a hash of suspect files or media, which creates a clean ‘sanitized’ copy of the original data files. This new copy is called evidence media. Computer forensic experts are trained to locate evidence utilizing seizure, search, or retrieval while maintaining the “data integrity” of suspected files. Metadata analysis involves interrogating data and providing evidence that can support a court case. It can also be used to search through large amounts of data quickly and pinpoint relevant ones for an eDisclosure or eDiscovery process. Additionally, computer forensic experts use their skills to spot inconsistencies in digital files caused by criminals attempting to cover their tracks by modifying metadata.

Metadata is critical in digital forensics because it provides an abundant source of information regarding everything from authenticating documents to discovering when files were created. Digital forensics experts may gather metadata evidence by browsing web search history, website title and URL, browser used, time on websites.

Digital forensic experts use metadata to help put together a timeline of events by analyzing how and when an individual interacts with a computer program to create, modify or copy files.

In digital forensics investigations, metadata analysis is used to understand the history of a particular electronic file. Digital forensics computer experts analyze file metadata to help put together a timeline of events. They use metadata necessary to fully understand electronic evidence such as Excel workbooks. For example, they can see formulas used to calculate numbers in an Excel workbook. This information helps them understand how and when an individual interacts with a computer program to create, modify, print or copy.

Metadata can be found in various digital formats such as documents, spreadsheets, images, videos, audio files, web pages and other computer files.

It allows investigators to follow a digital trail by reviewing digital data and their metadata to look for evidence that can support a court case. It can also be used to authenticate documents and discover when files were created.

The most basic metadata includes the date that files were created, times at which edits to the original file were made, timestamps from the most recent save and GPS location where it was taken.

However, even this basic metadata can be misinterpreted and often misunderstood. For example, the file creation date/time is not necessarily when that particular file was first written but rather when it was first written to the storage media we see it on.

In conclusion, system metadata is collected in digital forensics investigations by analyzing digital data and their metadata. Metadata provides information about electronic files such as when they were created, modified and accessed. Digital forensic experts use metadata analysis to authenticate documents and discover when files were created. They also use it to help put together a timeline of events by analyzing how individuals interact with computer programs.

What Types Of Metadata Are Collected In Digital Forensics Investigations

It can be categorized in various ways, including system metadata which is automatically generated by a computer system, application metadata which is created by an application, and user-generated metadata which is created by the user.

Metadata can provide an abundant source of information regarding authentication of documents, discovering when files were created, and assessing the legitimacy and efficacy of files derived from other sources.

In digital forensics investigations, commonly used computer metadata evidence includes browsing metadata such as web search history, website title and URL, browser used, time on websites; file system metadata such as file creation date/time; document properties such as author name; email headers such as sender address; image properties such as camera model and GPS location; and hash values for comparison. Metadata can be used to help prove cases, solve crimes, assist in timeline analysis, authenticate documents, assess the legitimacy of files derived from other sources, and more.

EXAMPLES OF SYSTEM METADATA

System metadata is automatically generated by a computer system and includes information such as a document’s title, author, date, time of creation, and the dates on which it was modified. Examples of administrative metadata include location information, acquisition information, and digitization selection criteria. Technical metadata is information that shows how metadata behaves or system functions. Such metadata includes software and hardware documentation, technical digitization information such as formats, scaling routines, and compression ratios. Technical metadata also involves tracking of system response.

In conclusion

The Power of Metadata: How it Helps Solve Crimes and Protects Our Digital World

Metadata plays a crucial role in digital investigations, helping to solve crimes and protect our digital world. In criminal investigations, metadata can provide investigators with vital information about the origin of a file, its creation date, and the devices used to create it. This information can help to identify suspects, provide alibis, and establish timelines, all of which are critical in solving crimes.

In addition to its role in investigations, metadata plays a significant role in protecting our digital world. It can be used to monitor and track the spread of malware and viruses, identify and prevent cyber attacks, and provide evidence in cases of intellectual property theft. Metadata can also help to ensure the authenticity and integrity of digital files, providing a means to verify that a file has not been tampered with or altered.

In conclusion, metadata is a critical component of digital evidence, providing valuable information about the origin, creation, and transmission of digital files. Its importance in digital investigations cannot be overstated, and its role in protecting our digital world is becoming increasingly important. As digital technology continues to evolve, it is essential that we understand the power of metadata and the role it plays in our digital lives.