The M365 Quirk: Unraveling the Mystery of QuickXor

Description

In the labyrinthine world of digital forensics and eDiscovery, there are often overlooked details that can significantly impact the defensibility and accuracy of evidence collection. One such detail lies hidden within Microsoftâ€™s M365 ecosystem, specifically within SharePoint and OneDrive: the hash type known as QuickXor.

What is QuickXor?

QuickXor is a hashing algorithm designed by Microsoft specifically for its M365 offerings, especially SharePoint and OneDrive. At its core, a hashing algorithm takes an input (or â€˜messageâ€™) and returns a fixed-size string, typically a sequence of numbers known as cryptographic hash algorithms. This string acts as a unique fingerprint for the given input[1].

QuickXor differentiates itself from more common hashing algorithms like SHA256 or MD5 in its efficiency and design. Built for speed and lower computational needs, QuickXor is adept at handling the vast, ever-evolving datasets associated with cloud storage. However, QuickXor is a non-cryptographic hash function designed for speed and efficiency rather than security and generates a hash by simply applying the XOR operation to the input data. While this means it is faster and less resource-intensive than cryptographic hashes, it is also less unique and more prone to collisions. It does not offer the same level of assurance that a cryptographic hash would and is, therefore, not as robust for forensic purposes where indisputable data integrity verification is critical.

The Role of QuickXor in M365

In platforms like OneDrive and SharePoint, data integrity and rapid access are paramount. QuickXor comes into play by offering a fast way to validate the integrity of files stored on these platforms. When a file is uploaded or modified, QuickXor generates a hash value for the file. This hash value is a unique

identifier, ensuring the file remains unchanged and undamaged during storage or transfer.

Following the Flock Off the Edge

Challenging Complacency in QuickXor Hash Validation

The hashing process is a cornerstone of evidence collection for digital forensic professionals. It ensures the collected data remains unaltered from its original state, offering a chain of custody and a measure of defensibility in legal settings.

However, thereâ€™s a blind spot. Many professionals, even those deeply embedded in digital forensics, are unaware of QuickXorâ€™s existence or need the tools and knowledge to work with it effectively. This unawareness stems from a few factors:

- **The ubiquity of Traditional Algorithms:** The dominance of established hashing algorithms like SHA256 and MD5 means that many tools and training programs are centered around them. This has inadvertently led to a lack of emphasis on non-cryptographic algorithms like QuickXor.
- **Assumptions about M365:** Thereâ€™s a prevailing assumption that global tech giants like Microsoft would employ universally recognized algorithms. This presumption can lead professionals astray when they need to account for specialized, in-house solutions.
- **Tool Limitations:** Many digital forensic tools on the market may not support or recognize QuickXor. Even if they do, thereâ€™s no guarantee they will handle it correctly, given its unique nature. Although QuickXor isnâ€™t as reliable as cryptographic hashing (e.g., MD5, SHA256), capturing what is available is critical.

A well-respected veteran digital forensics and eDiscovery software development company, Pinpoint Labs, has multiple tools that properly capture QuickXor values from Microsoftâ€™s servers and calculate and verify files collected from SharePoint and OneDrive sources. Additionally, Pinpoint Labs products provide a complete chain of custody and retain file timestamps and metadata.

Bridging the Knowledge Gap

The first step to addressing the QuickXor problem is awareness. By bringing this topic to the forefront, professionals can start to adapt their methodologies and tools.

For practitioners, itâ€™s essential to:

- **Update Training Programs:** Incorporate modules specifically addressing hashing algorithms and verification methods used in popular cloud storage services.
- **Choose the Right Tools:** Ensure that forensic tools, like those from Pinpoint Labs, are being used are QuickXor-compliant and can effectively handle M365 collections.
- **Engage with the Community:** Foster discussions, seminars, and workshops emphasizing the nuances of M365 collections and the role of QuickXor.

In the rapidly evolving realm of digital forensics, staying updated is a professional requirement and a mandate to ensure justice and accuracy. As Microsoftâ€™s M365 suite continues its ascendancy in the business world, understanding the intricacies of QuickXor becomes ever more crucial. Letâ€™s ensure weâ€™re not just collecting but collecting right.

---

1. For a deeper dive into hashing and its importance, refer to the National Institute of Standards and Technologyâ€™s (NIST) guidelines on cryptographic hash functions: NISTâ€™s Hash Functions.

Date
10/29/2025
Date Created
11/08/2023