Hashes

A hash algorithm is a one way algorithm that creates a set-size unique output given a variable length input. Hashes have various applications and are used throughout many technologies. Basically, it is used to sign or verify data. Hashes can verify a download from the internet, ensure a file in a court case hasn’t been changed, follow data packets in internet traffic to ensure unchanged data transmission, or verify passwords on an internet server without storing the password in memory.

Not all hash algorithms are created equal

MDA-5 collision

Windows Powershell

Password storage – possibility to break them