Hashing: Verifying Digital Evidence

Dr. Philip Craiger





Analyses? Not Yet...

- So we have a forensic image. Now what?
- Regardless of types of analyses we don't want to change anything on the image.
 - We can always verify by calculating a 'hash' of the evidence
 - A unique number based upon the contents of the file – MD5
 - » Message Digest 5, a 128-bit hash
 - SHA-1
 - » Secure Hash Algorithm -1 developed by NIST, 160-bit hash, government standard
 - SHA-2
 - » Family of hashes: 256, 384, 512-bit

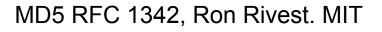




MD5 Cryptographic Hash

- The MD5 algorithm takes
 - as input a message of arbitrary length and
 - produces as output a 128-bit "fingerprint" or "message digest" of the input.
 - Likelihood of 'collision' = $\sqrt[1]{\sqrt{2^{128}}}$ = 1/2⁶⁴
- It is computationally infeasible to produce two messages
 - having the same message digest, or
 - to produce any message having a given prespecified target message digest.







MD5 Cryptographic Hash

- 'The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.'
- '... MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.'





.....

MD5 from Windows

- md5sum.exe -o d_drive.md5 \\.\D:
 - md5 drive d, output to file d_drive.md5
- md5sum.exe -c d_drive.img.md5
 - check d_drive.img.md5 against drive d





References

- Schulz & Shumway (2002). *Incident response*. New Riders.
- U.S. Secret Service (2000). Best Practices for Seizing Electronic Evidence. <u>http://www.cjtoday.com/pdf/7cjt0707.pdf</u>
- All the man files for dd, netcat, etc.



