BINUS UNIVERSITY DOCTORATE PROGRAM | Doctor of Computer Science

Framework to Ensure Digital Evidence Admissibility in Court

BACKGROUND

- *In 2012* more than 13,300 digital forensic examinations were conducted by CART (Computer Analysis and Response Team)
- Several Cases whereby a digital evidence was rejected due to integrity and authenticity problem
- Weakness in MD5 found in 2004 where a hash collision can be found
- Since then many methods are introduced to find collisions in a faster way

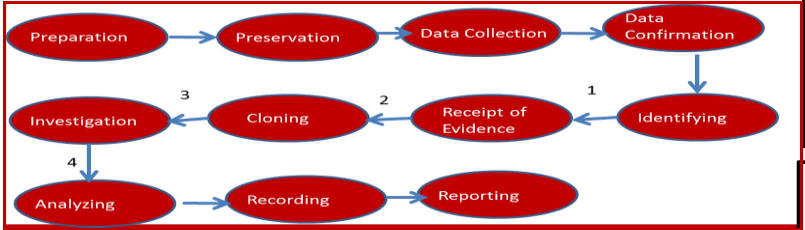
AIM

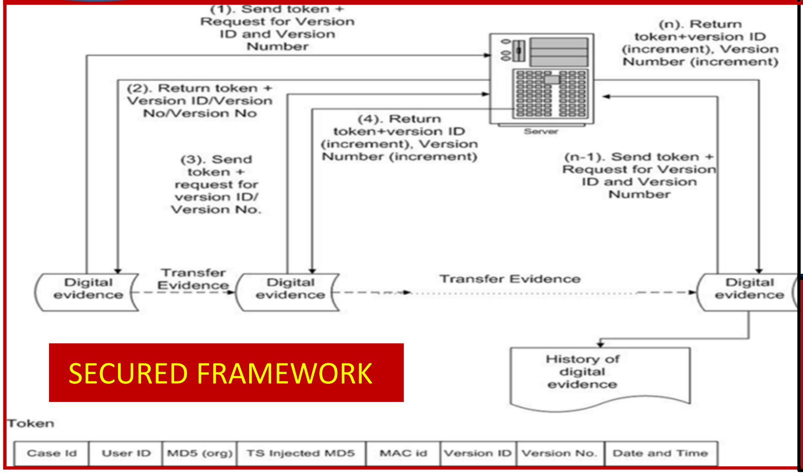
To ensure admissibility of Digital Evidence in court

OBJECTIVES

- To examine the effects of different Initial Values towards the creation of colliding files that would cause a compromise in the integrity of Digital Evidence
- To apply digital hashing with timestamp to reduce the creation of colliding files
- To develop a framework with the inclusion of digital hashing with timestamp to maintain evidence integrity and produce Digital Evidence confidence Level of Admissibility

POSSIBILITY of BREACH



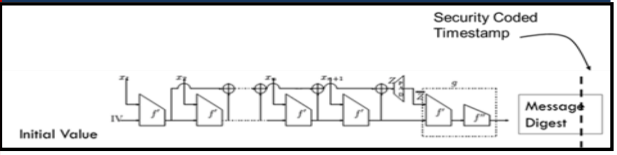

(1). Send token + Request for Version ID and Version Number
(n). Return token+version ID (increment), Version Number (increment)
(2). Return token + Version ID/Version No/Version No
(4). Return token+version ID (increment), Version Number (increment)
Server
(3). Send token + request for version ID/ Version No.
(n-1). Send token + Request for Version ID and Version Number
Digital evidence
Transfer Evidence
Digital evidence
Transfer Evidence
Digital evidence
History of digital evidence

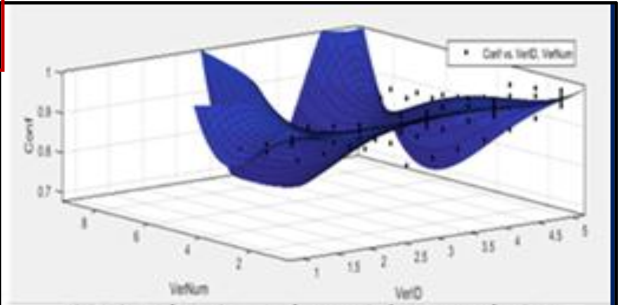
SECURED FRAMEWORK

Token

Case Id	User ID	MD5 (org)	TS Injected MD5	MAC id	Version ID	Version No.	Date and Time

Timestamp Injected Hash Function





3D Graph using Polynomial Interpolation

Confidence Level Formula:

$$f(x,y) = 1.429 - 0.2867y - 0.8045x + 0.4633x^2 + 0.589xy - 0.07297y^2 - 0.1059x^3 - 0.3557x^2y + 0.02145xy^2 + 0.2069y^3 + 0.008406x^4 + 0.08148x^3y + 0.00437x^2y^2 - 0.01083xy^3 - 0.0001982y^4 - 0.006413x^4y - 0.0009869x^3y^2 + 0.001117x^2y^3 + 0.0001334xy^4 - 0.000003783y^5.$$

CONCLUSION

- Using different IV, different prefix file and different size of file has no significant effect in the creation of a collision attack, as shown by the significant value being 0.415, 0.148 and 0.648 respectively, in which all are greater than α (0.05).
- With the MD chopping construction and the inclusion of timestamp into MD5 Algorithm, it is concluded that the creation of two colliding files has been suppressed.
- The proposed framework contains Timestamp Injected MD5 hash function and a procedure to handle evidence during investigation. History files can be used to trace the evidence back to the original document. The confidence level of the evidence admissibility as modelled into a 3D graph involving Confidence level of document including human interaction with the Digital Evidence as identified by Version ID and Version Number or the evidence.

RECOMMENDATIONS

- Timestamp Injected MD5 Hash function should use the birth date instead of the modification date, because the birthdate will never change. Further research on human trust and the effect of file changes on the modification of a few bits in a file can be incorporated it into the framework that would improve the Confidence Level of the Evidence Admissibility
- This framework should be tested and presented into real situation that involves all stakeholders, in this case, the investigators (police and private), lawyers, prosecutors and judges, to observe its viability

Name: Zulfany Erlisa Rasjid
Email: zulfany@binus.ac.id
Doctor Of Computer Science
Bina Nusantara University
Jakarta, Indonesia, 11480