OSAC Research Needs Assessment Form

Title of research need: Scientific Analysis of Hash Authentications

Keywords: Hash, MD5, SHA, digital forensic

Submitting subcommittee(s): Digital Evidence **Date Approved:** 2/9/16

(If SAC review identifies additional subcommittees, add them to the box above.)

Background information:

1. Description of research need:

Scientific study of the validity of utilizing hash computations on digitally stored information and their viability for use in authentication processes.
Uniqueness probability

2. Key bibliographic references relating to this research need:

NIST MD5 Standard
NIST SHA-1 Standard
NIST – NSRL Hashing algorithms and tests (zip) (2000/06/12)
NIST – NSRL White paper on Hash Algorithms Selection (2000/06/30)

3a. In what ways would the research results improve current laboratory capabilities?

The results would provide scientific validity studies to support the applicability of utilizing hash value comparisons to determine uniqueness, or known identification or evidence modification confirmation. (protection/security?) It would supply the scientific validity that does not currently exist in a citable form.

3b. In what ways would the research results improve understanding of the scientific basis for the subcommittee(s)?

The results would have a huge impact to the understanding and acceptance of an evidence protection and identification technique that currently is not supported by much scientific proof. It would provide confirmation of the validity of the technique and provide documented citable materials where little currently exists.

3c. In what ways would the research results improve services to the criminal justice system?

It would have a huge positive impact on the acceptance of what is the foundation of most digital forensic examinations by providing the scientific validity and documentation to support the foundational process of hashing.

4. Status assessment (I, II, III, or IV): I

	Major gap in current knowledge	**Minor** gap in current knowledge
No or limited current research is being conducted	**I**	**III**
Existing current research is being conducted	**II**	**IV**

This research need has been identified by one or more subcommittees of OSAC and is being provided as an informational resource to the community.

Subcommittee Approval date: 2/9/16

(Approval is by majority vote of subcommittee. Once approved, forward to SAC.)

SAC

1. Does the SAC agree with the research need? Yes ⊗ No ◯

2. Does the SAC agree with the status assessment? Yes ⊗ No ◯

If no, what is the status assessment of the SAC:

Approval date: 6/15/16

(Approval is by majority vote of SAC. Once approved, forward to NIST for posting.)