OSAC RESEARCH NEEDS ASSESSMENT FORM

Title of research need: Internet of Things, User Artifacts

Keyword(s): IoT, Connected Devices

Submitting subcommittee(s): Digital Evidence **Date Approved:** 12/12/2018

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

Background Information:

1. Description of research need:

As the use of connected technology devices increase, there is a need to establish a method for forensic examiners to capture user data from connected devices. The machine to machine communication provides unique challenges to forensic examiners. In addition to collecting historical information, it is imperative that the capture process stop potentially destructive processes from occurring. Additionally, much of the processing performed by an IoT device is completed by sending data to a cloud service or other external processing location. A library of file and artifact signatures, both for artifacts from device memory and for network traffic artifacts, would help to rapidly identify potential artifacts. As an example: It might be possible to carve Siri voice requests from network traffic, reconstruct the audio, and identify the corresponding returned text.

2. Key bibliographic references relating to this research need:

Internet of Things Forensics: Challenges and Case Study:
https://arxiv.org/ftp/arxiv/papers/1801/1801.10391.pdf

Internet of Things Forensics: Challenges and Approaches
https://www.researchgate.net/publication/259332114_Internet_of_Things_Forensics_Challenges_and_Approaches

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

Provide access to devices that currently do not have established forensics practices.

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

The ability to accurately identify, extract, and analyze IoT forensic artifacts, regardless of tool or source, would be improved.

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

Less time would be spent by agencies attempting to create one-off forensic processes when a new device was submitted for examination.

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

	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.

Approvals:

Subcommittee

Approval date: 12/12/2018

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

SAC

1. Does the SAC agree with the research need? Yes [x] No [ ]
2. Does the SAC agree with the status assessment? Yes [x] No [ ]

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

Approval date: 12/12/2018

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