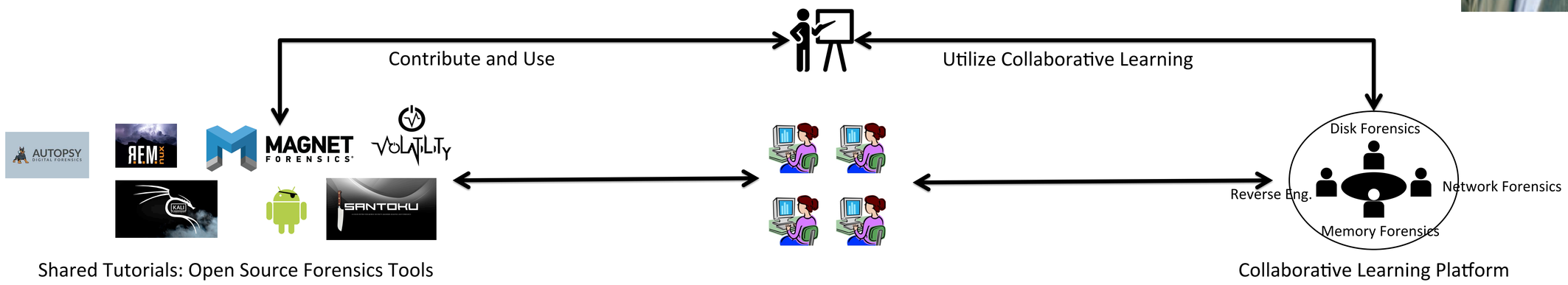
SaTC: EDU: Improving Student Learning and Engagement in Digital Forensics through Collaborative Investigation of Cyber Security Incidents and Simulated Capture-the-Flag Exercises

Akbar Siami Namim (Texas Tech University)

http://www.myweb.ttu.edu/asiamina/research_files/SaTC-EDU-DigitalForensics.html



Key Problems and Challenges:

- Teaching digital forensics requires extensive development of hands-on experiences and instructional modules
- There is no educational support for instructors
- It is hard and time consuming to develop course modules and lab materials for digital forensics
- There is no platform for sharing such teaching materials
- There is no platform for collaborative learning

Scientific Impact:

- Advance pedagogy and education of digital forensics
- Identify educational challenges related to teaching digital forensics
- Compare open-source digital and mobile forensics tool
- Identify the pros/cons of different dynamic and static analysis tools targeting digital and mobile forensics

Solution:

- Establish a public repository and platform for instructors to share their educational modules and lab materials
- Develop an educational platform for collaborative learning focusing on digital forensics and incident responses
- Develop online tutorials, instructional modules, hands-on experiences, and training videos on well-known and widely used forensics open source digital and mobile tools

Impact on Society:

- Make the shared repository publicly available for promoting cyber security
- Enable users to be aware of different types of malware
- Helps users discover different channels of attacks malware developers utilize
- The materials can be utilized as a self-learning course

Impact on Education and Outreach:

- Promote cyber security education
- Support pedagogy and education of digital forensics and malware analysis
- Support instructors with teaching artifacts and enable them to shair their lab materials
- Promote collaborative learning and team work

Quantify Potential Impact:

- Over 40 open source tools have been identified
- Over 10 training modules will be developed for each topic targeting different aspects of digital forensics such as 1) Disk, 2) Memory, 3) Network, 4) Mobile, and 5) Reverse Engineering

Award ID#: 1821560