Developing a Digital Forensics Curriculum

An Education Initiative for Digital Forensics Curriculum Standardization

Imani Palmer, Stefan Nagy, Roy Campbell, Masooda Bashir

ENGINEERING AT ILLINOIS
INFORMATIONTRUST INSTITUTE

Background

The growing role of digital evidence has created a demand for skilled digital forensics examiners. As that need has gone unfulfilled, a related demand has appeared: the need for a standardized digital forensics curriculum. While standards have been proposed by various organizations, widespread adoption has so far proved unsuccessful.

Goals

The Digital Forensics Education Initiative

- We are creating a scientifically grounded digital forensics curriculum consisting of an introductory course and an advanced course, with accompanying labs.
- We aim to distribute our curriculum materials to institutions around the world for use in their own digital forensics courses.

Research Plan

- We decided on a multidisciplinary approach to developing the lecture content and lab exercises.

Members of the Digital Forensics team

- The introductory course is a survey of interdisciplinary topics important to understanding digital forensics as a whole.
- The advanced course provides a more technical exploration of advanced computer and network forensics concepts.

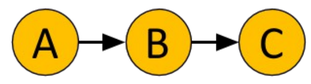
Fundamental Challenges

- **Key Challenge:** often, there is not a robust scientific basis for the way evidence is evaluated in digital forensics investigations.
- **Solution:** we decided it was necessary to educate students on scientific techniques applicable to digital forensics.

Scientific Model

The curriculum continually touches on the need to bring the rigor of the scientific method into the evaluation of evidence. Below is an example of material on logical reasoning covered in the courses.

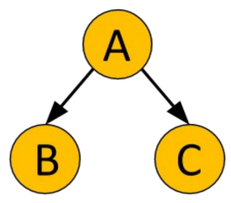
Serial Connection



$$P(A,B,C) = P(C|B)\,P(B|A)\,P(A)$$

If B is unknown, then A and C are dependent on each other. If B is known, then A and C are independent of each other. A and C are conditionally independent of each other given B.

Diverging Connection

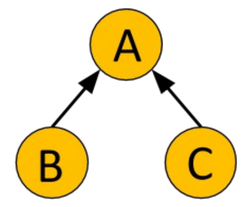


If B is known, then A and C are conditionally independent.

$$P(A,B,C) = P(C|B)\,P(A|B)\,P(B)$$

Converging Connection

If B is unknown, then A and C are independent. If B is known, A and C can influence each other.



$$P(A,B,C) = P(B|C,A)\,P(C)\,P(A)$$

Conclusion

To further the development of standards in digital forensics education, we are creating a two-course curriculum. We offered the introductory course in Fall 2013, and again in revised form in Fall 2014. This Spring, we are offering the pilot version of the advanced course. The materials have been designed by faculty from multiple disciplines and have been created in a modular and adaptable for use in institutions ranging from community colleges to traditional four-year universities.

Related Work:

1) A. Lang, M. Bashir, R. Campbell, and L. DeStefano, *Developing a New Digital Forensics Curriculum*, DFRWS (Digital Forensics Research Conference), Aug 3rd – 6th, 2014. Denver, CO
2) I. Palmer, S. Nagy, W. Morgan, J. Schipp, *ISLET: A Docker-Based Digital Forensics Course Environment* (in progress)