Developing a New Digital Forensics Curriculum

By

Anthony Lang, Masooda Bashir, Roy Campbell and Lizanne Destefano

Presented At

The Digital Forensic Research Conference

DFRWS 2014 USA Denver, CO (Aug 3rd - 6th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Developing a New Digital Forensics Curriculum

Anthony Lang, **Masooda Bashir**,
Roy Campbell, Lizanne DeStefano
University of Illinois at Urbana Champaign
DFRWS 2014

Overview

- Undergraduate certificate program
- Self-contained curriculum package
  - Three courses: one basic, one advanced, one special topics
  - Hands-on lab exercises
  - Designed with express intent to distribute
- Covers all fundamental disciplines
  - Computer science, law, social science, psychology, and accounting
- Currently revising for institutional distribution

  http://publish.illinois.edu/digital-forensics/

Introduction

- Increased use of digital devices necessitates development of a standardized curriculum
- Field plays a major part of many investigations
- Still a new/rapidly-developing area of study
- Presents a challenging position for the education community

Perspectives on Curriculum Standards

- Establishment important for several reasons:
  - Provides means for validating qualifications
  - More efficient screening for expert witnesses
  - Simplifies evaluation of degree options
  - Increases employability for such degrees
- Spring 2013 workshop:
  - Findings indicate that adoption of curriculum hindered by practicality

Existing Curriculum Standards

These observations are by no means novel, and there have been concerted efforts from the digital forensics education community to establish standardized curriculum.

- The American Academy of Forensic Sciences (AAFS)
- Forensic Science Education Programs Accreditation Commission (FEPAC), published and offers accreditation based on, a standard that includes digital forensics
  - Forensic Science Education Programs Accreditation Commission (FEPAC – 2012)
  - Forensic Science Education Programs Accreditation Commission (FEPAC – 2014)

➢ However, only a few universities has adopted this standard and received their accreditation for digital forensics

Difficulty of Implementation

- Balancing training and education
- Textbook selection
- Finding qualified faculty
- Lab setup
- Selecting appropriate prerequisites
- Lack of curriculum standards

Our Digital Forensics Program

- Self-contained curriculum package
  - Instructor course content handbook
  - Lab exercises handbook
  - Presentation lecture slides
  - Remedial reading sources
  - Homework/exam question sets
- Topics organized by modules
  - Combined to form a coherent narrative

Program Goals

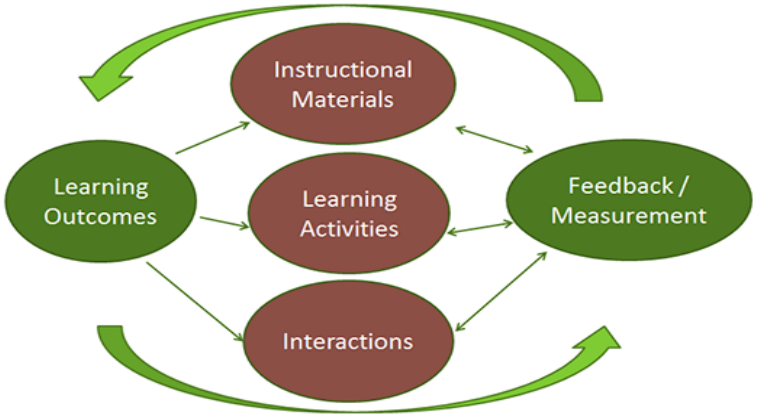
- Lower entry barrier for institutions
- Work toward curriculum standardization
- Provide educational introduction to the field
- Reflect all fundamental disciplines of the field
- Make curriculum accessible and useful

Introductory Course Development

- Curriculum objectives:
  - Focus on computer forensics, network forensics, and mobile device forensics
  - Provide relevant interdisciplinary perspectives
- Necessity of relying on up-to-date material
- Requiring knowledge prerequisites rather than course prerequisites

Pilot Course Design

- 16-week course consisting of:
  - Two 75-min lecture sessions per week
  - One 60-min lab session per week
- Course topics organized in modules:
  - Psychology, computer forensics, U.S. legal system, network forensics, law, fraud examination, and mobile device forensics and malware



Pilot Class Topics, by Module

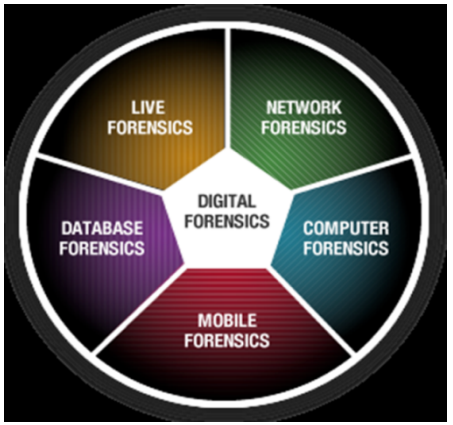
Define digital forensics and its subfields
Evidence handling/Scientific Method

Psychology

- Psychology of cyber crime
- Criminal profiling

Computer forensics

- Introduction to file systems
- NTFS analysis
- Deleted file recovery and file carving
- Windows Registry, log files, link files, Recycle Bin
- Web browser forensics, email forensics, EXIF



Pilot Class Topics (cont.)

U.S. legal system

- Disputes, courtroom workgroup, attorneys
- Judges, juries, legal process

Network forensics

- Networking fundamentals review
- Network evidence acquisition
- Protocol analysis, packet analysis, flow analysis
- Application protocols, statistical flow analysis
- Network intrusion detection and analysis

Law

- Fourth Amendment: reasonable expectation of privacy
- Warrant vs. subpoena, Federal Rules of Evidence
- Privacy laws, computer crime laws

Pilot Class Topics (cont.)

Fraud examination

- Introduction to fraud examination
- Characteristics and skills of a forensic accountant
- The nature and extent of fraud, Benford's Law

Mobile device forensics and malware

- Mobile device technology fundamentals
- Mobile device evidence extraction and analysis
- Mobile network evidence
- Legal and ethical considerations of interception
- Malware taxonomy, detection, and circumvention

Lessons from Pilot Course

1. Coordination between instructors/modules proved challenging
2. Differing understandings of the knowledge prerequisites among the professors/students
   - Wide range in levels of computer literacy
   - Some students struggled during lab exercises

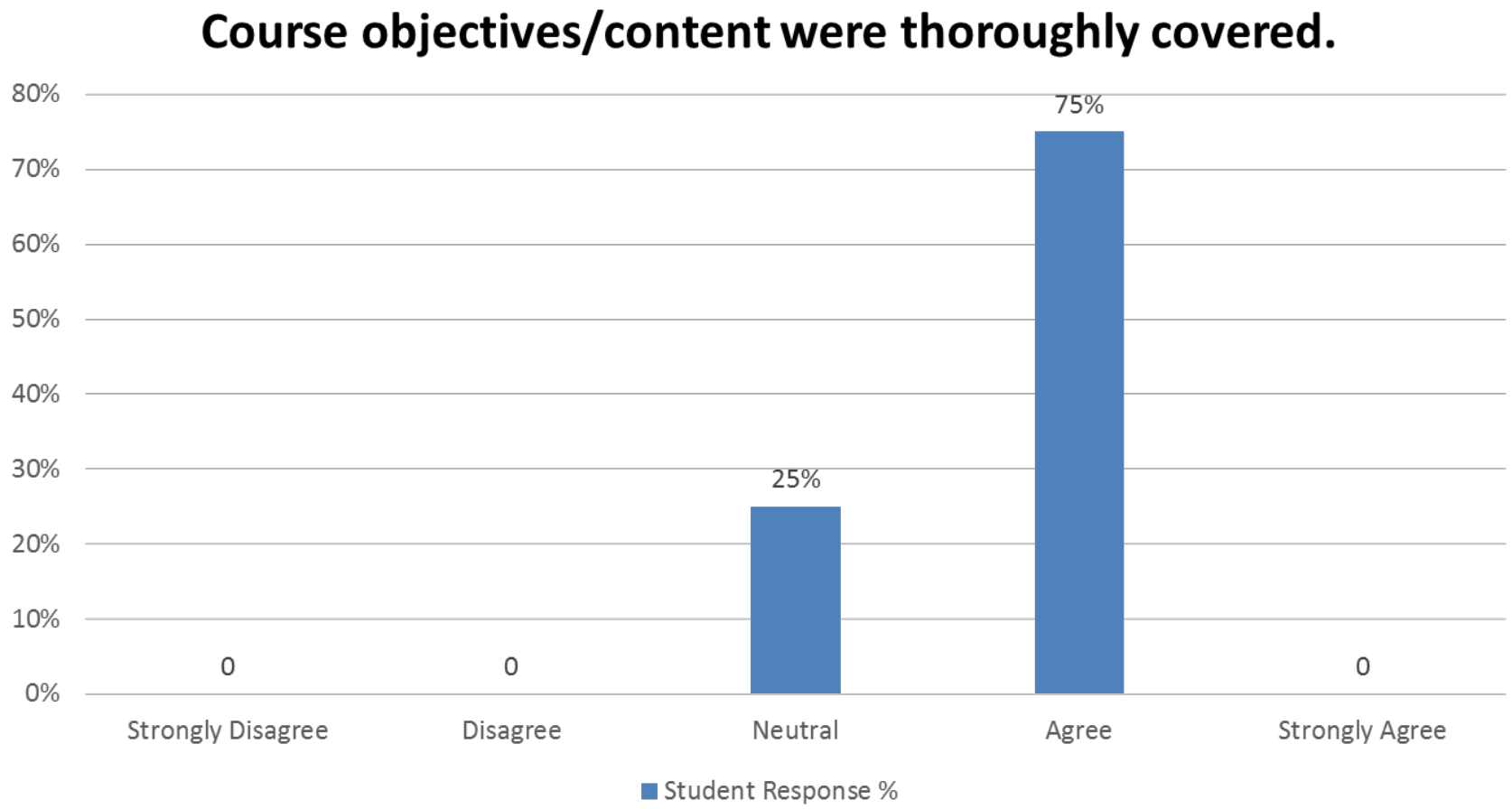
Lessons from Pilot Course

3. Enrollment consisted mainly of Computer Science and Law students
   - Law students had difficulty with technical aspect compared to Computer Science students
   - Decision to shift focus to investigative and evidentiary complexities
   - Lab modules revised to include more teamwork between Law and Computer Science students

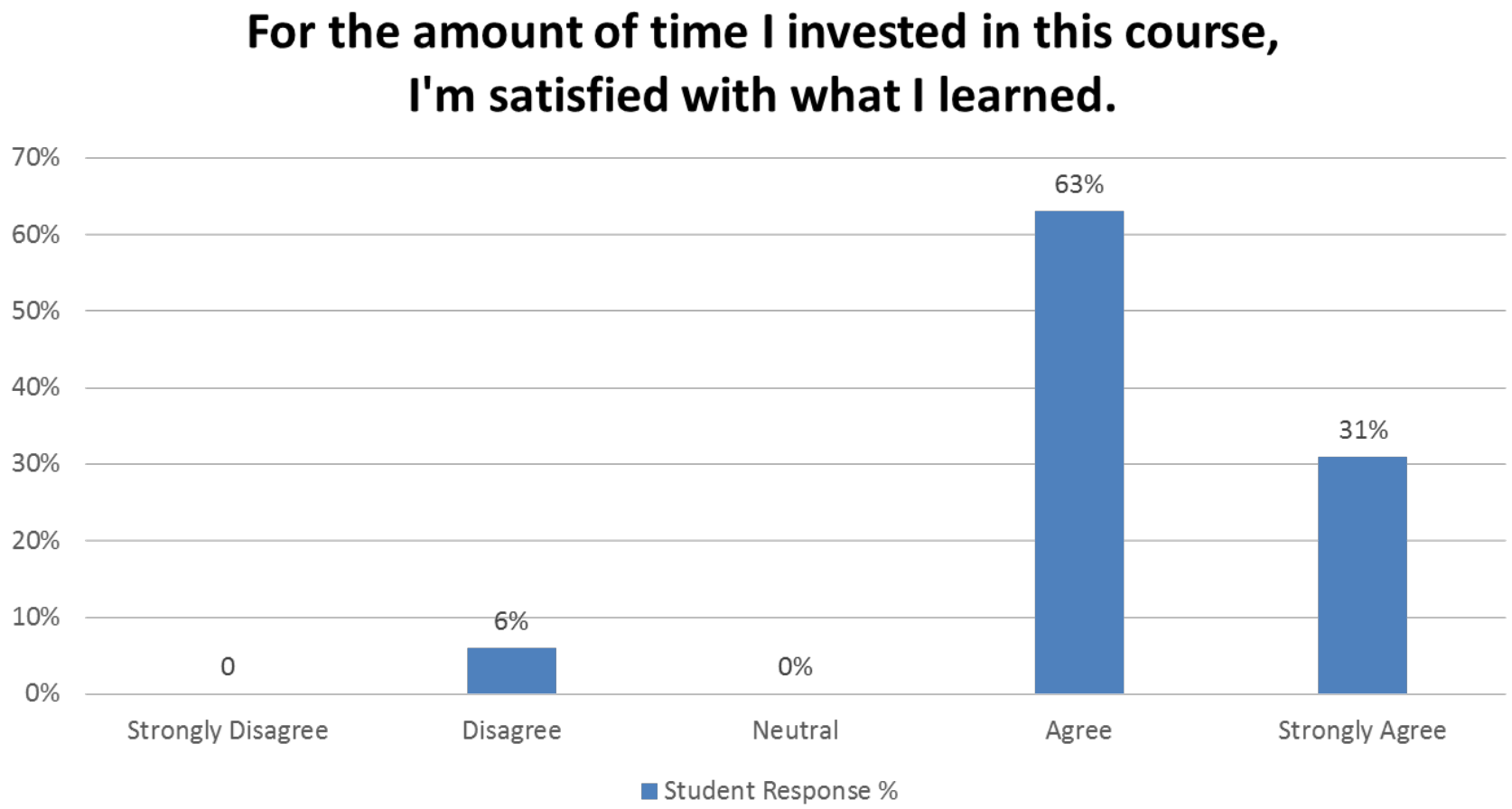
Evaluation Methodology

- Illinois Science, Technology, Engineering, and Mathematics Education Initiative (I-STEM)
- Evaluation intended to provide feedback on implementation and efficacy of curriculum
- Evaluators collected data using the following:
  1. Three student surveys: pre, mid, and end-course
  2. Course and lab section observations
  3. Mid and end focus groups with students

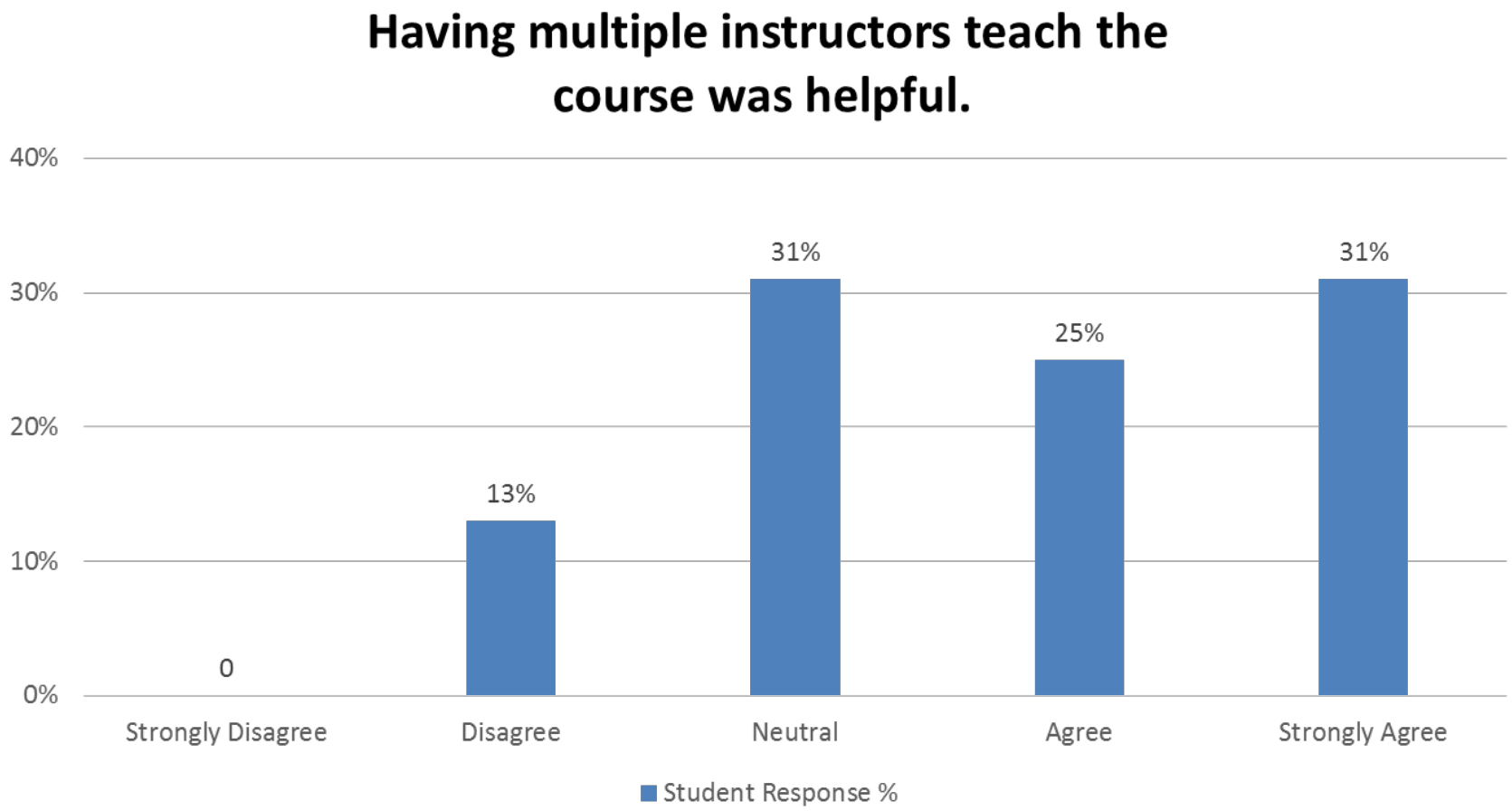
Student Feedback Summary



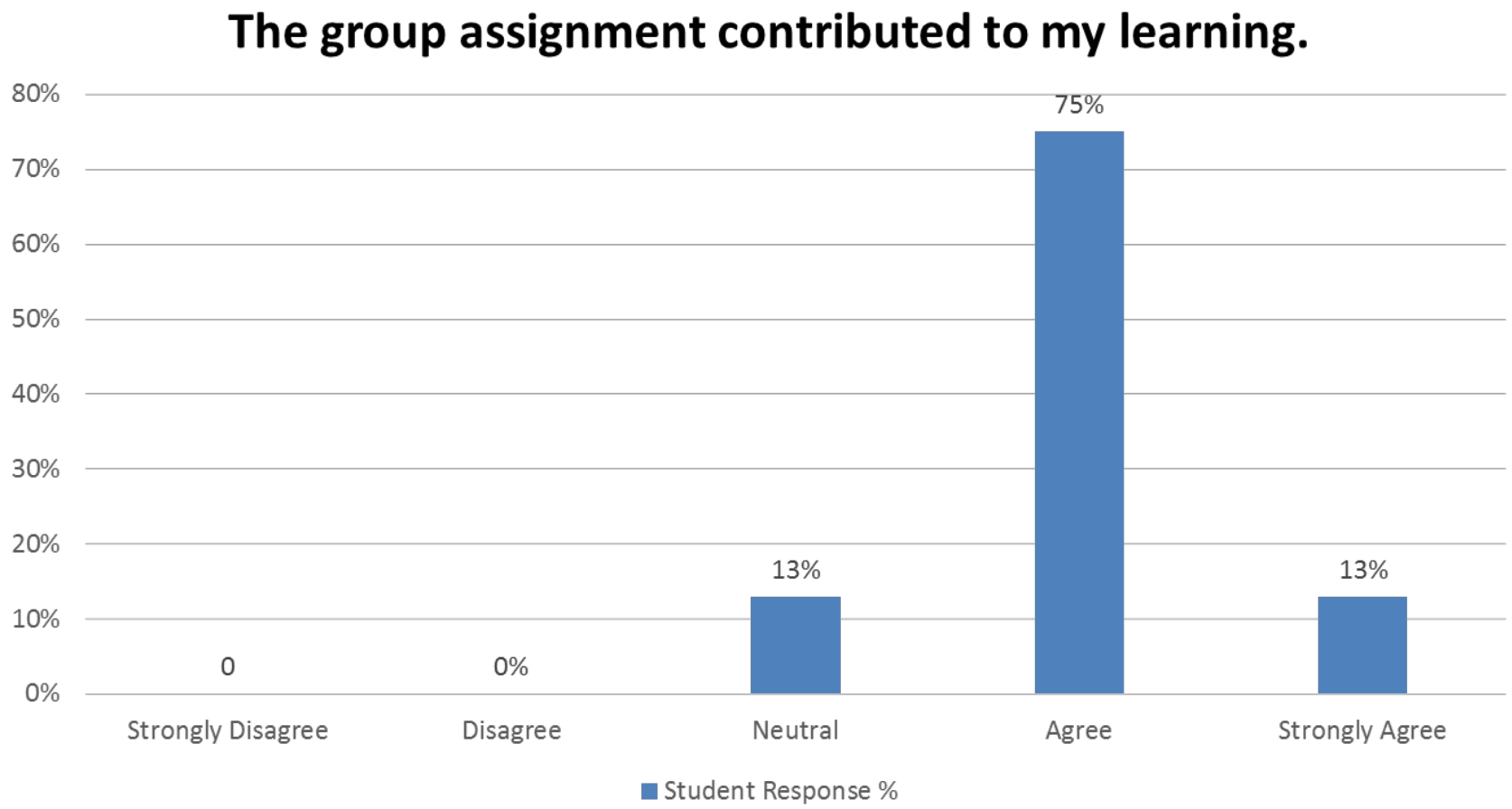
Student Feedback Summary



Student Feedback Summary



Student Feedback Summary

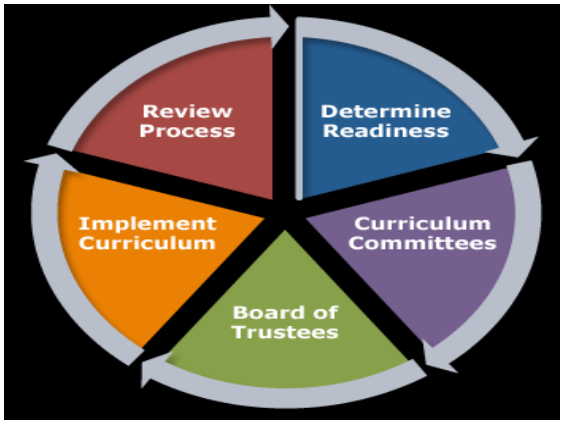


Student Feedback Summary

- Students felt there was a lack of communication among the instructors
- Topics felt out of place and did not fit together
- Suggested using a single, long-term case study
- Potential benefit of glossary of technical terms

Revisions

- Incorporating a fictitious case study that advances as the course progresses
- Changing order of modules
  - Non-technical material before technical material
  - Highlight wider social impact of the field
  - Other modules will be ordered to best fit



Revisions (cont.)

- Four changes to address computer literacy
  1. Extend focus on investigations, evidence analysis, and group activities to earlier parts of course
  2. Offer students a primer on technical fundamentals
  3. Quick-reference glossary of terminology
  4. Prerequisite quiz for completion before course enrollment

Conclusions and Future Work

- Alpha version of curriculum package available in Summer 2014
- Welcome any feedback from education, research, and professional communities
- Dedicated Workshop Aug 7, 2014 - DFRWS
- Developing curriculum for advanced course to be piloted at UIUC in Spring 2015

http://publish.illinois.edu/digital-forensics/

Acknowledgments

We would like to acknowledge the attendees of the 2013 Digital Forensics Curriculum Standards (DFCS) workshop for their engaging discussions and invaluable feedback.

This work was supported by the National Science Foundation under Grant No. DUE-1241773.

Questions?

mnb@illinois.edu