Peer Instruction for Digital Forensics

William E. Johnson, **Irfan Ahmed,** Vassil Roussev
Department of Computer Science
University of New Orleans

Cynthia B. Lee
Department of Computer Science
Stanford University

Peer Instruction

- Introduced by Eric Mazur, a physicist at Harvard University
- Tested and used in several scientific disciplines including
  - Physics,
  - Biology, and
  - Computer science
- Results of using peer instruction are promising
  - Improving student learning
  - Halving failure rates
  - Increasing student retention in their respective major

Peer Instruction in CS

- 6% higher grades on final exams over traditional lecture style
- 61% reduction in failure rates
  - Theory of Computation, and Computer Architecture
- 31% improvement in student retention
- Instructors find peer instruction effective
- Students recommend that more instructors should use peer instruction

Peer Instruction Methodology

- Pre-class preparation by students
  - Reading material
  - Quiz
- In Class, a topic is covered as
  - A question is asked to students
    - Conceptual
    - Multiple choice
  - Two to three minutes for reply
  - Group discussion of students
  - Students reply to the question again
  - Instructor may further discuss the answers

Iterative

Elements of a Peer Instruction Question

- Concept Trigger
- Presentation Type

Concept Trigger

- Provoke a student's thinking process
- Set the desired direction of peer discussion
- Examples: (Beatty *et al. [1]*)
  - Deliberate ambiguity
  - Trolling for misconceptions
  - Omit necessary information
  - Identify a set or subset
  - Compare and contrast
  - Trap unjustified assumptions

Question Presentation

- Putting concept and concept trigger together
  - Better presentation
  - Easier understanding
- Examples:
  - Scenario
  - Example
  - Diagram
  - Definitional
  - Feature

Example Question # 1
File Carving

In which of the following situations is file carving most effective?

a) The targeted drive is highly fragmented,
b) The targeted drive has been recently defragmented,
c) The system being used to examine the drive has low free space,
d) The system being used to examine the drive has high free space,
e) More than one of the above

Deconstruction # 1

- Concept Trigger
  - identify a set or subset
  - trolling for misconceptions
- Question Presentation
  - example

Example Question # 2

Forensic Artifacts

A USB drive with an unknown owner is found in a corporate setting. How might a forensic investigator typically determine whether that particular drive was plugged into any given Windows machine?

a) Examine all ntuser.dat files to determine if a user plugged it into the machine
b) Check the SYSTEM registry hive to see if it was plugged into that machine
c) Check the SOFTWARE registry hive to see if it has been used by any particular piece of software
d) More than one of the above
e) None of the above

Deconstruction # 2

- Concept Trigger
  - None of the above
  - Identify a set or subset
- Question Presentation
  - Scenario

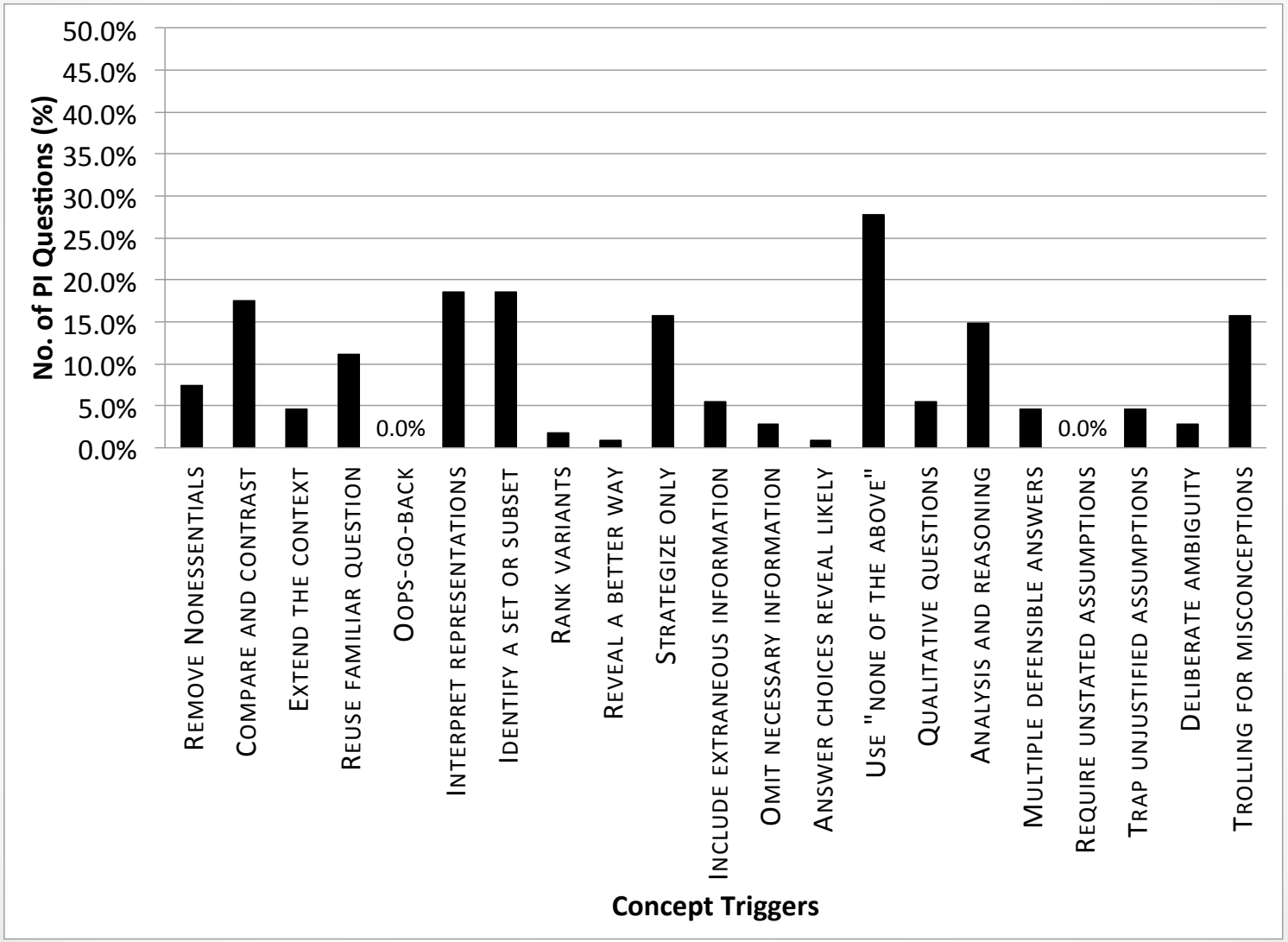
Analysis of Questions

- Developed 108 questions for digital forensics

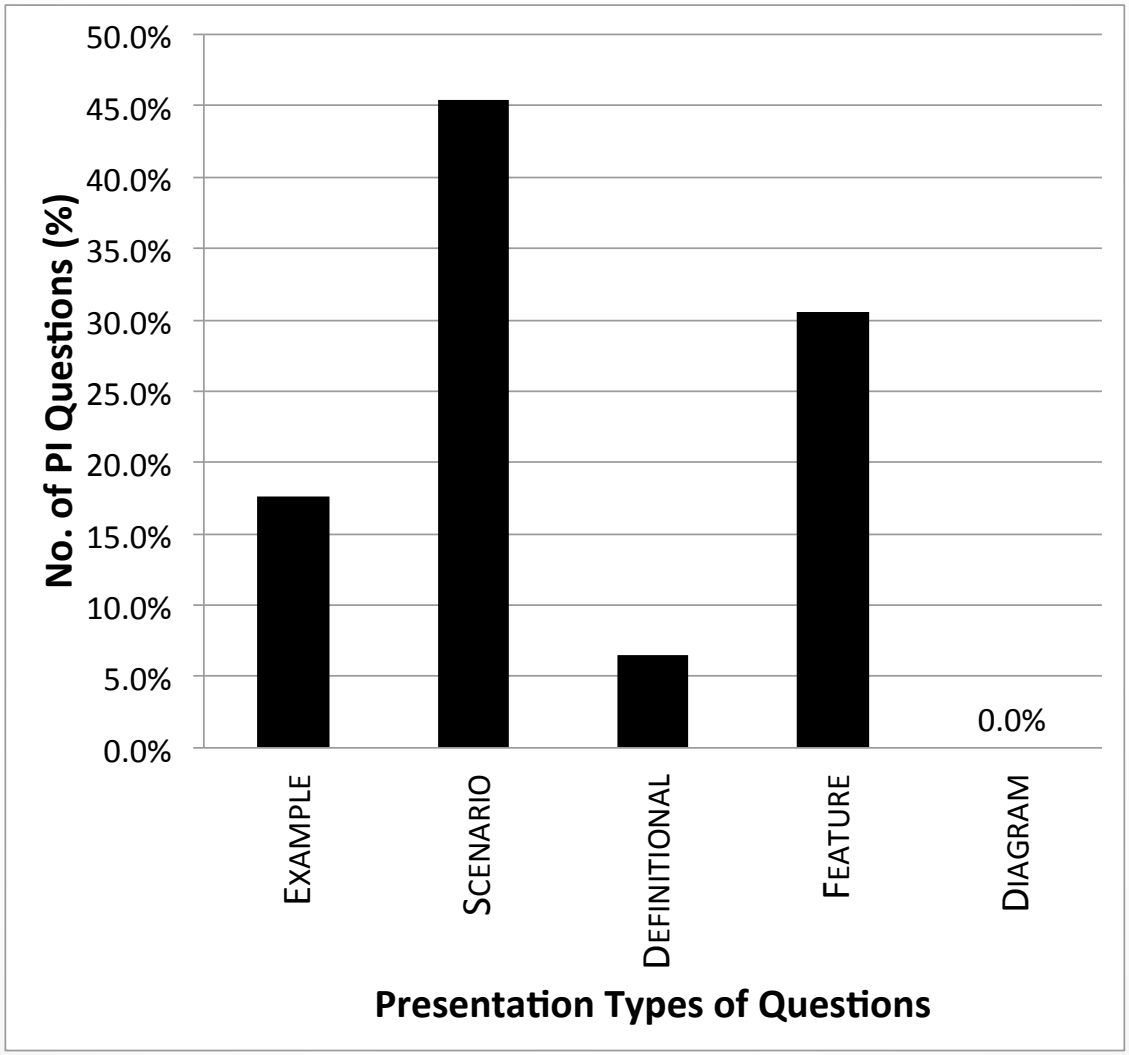
Topics	# of Questions
Introduction to Computer Forensics	31
Windows Registry	10
Forensic Artifacts	24
File Systems	11
Live Forensics	24
File Carving	8

- Goal of Analysis is to identify concept triggers and presentation types in the questions

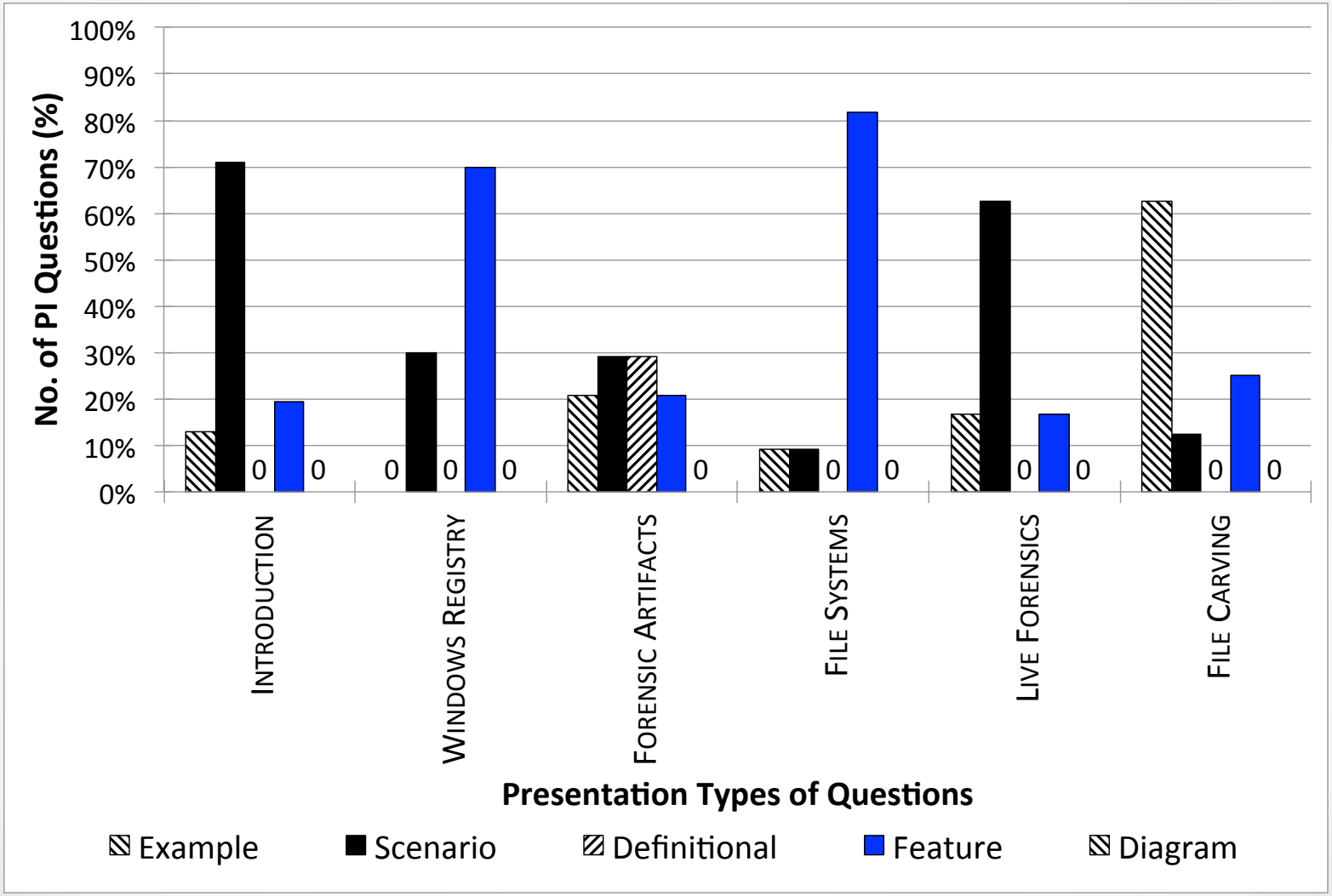
Concept Trigger



Presentation types



Presentation-types & Topics



Workshop

- ***Topic:*** Computer forensics
- ***Participants:*** 12 undergrad students
- ***Topics covered:***
  - Introduction to Computer Forensics
  - File Systems
  - File Carving
  - Windows Registry
- ***Duration:*** 4 hours

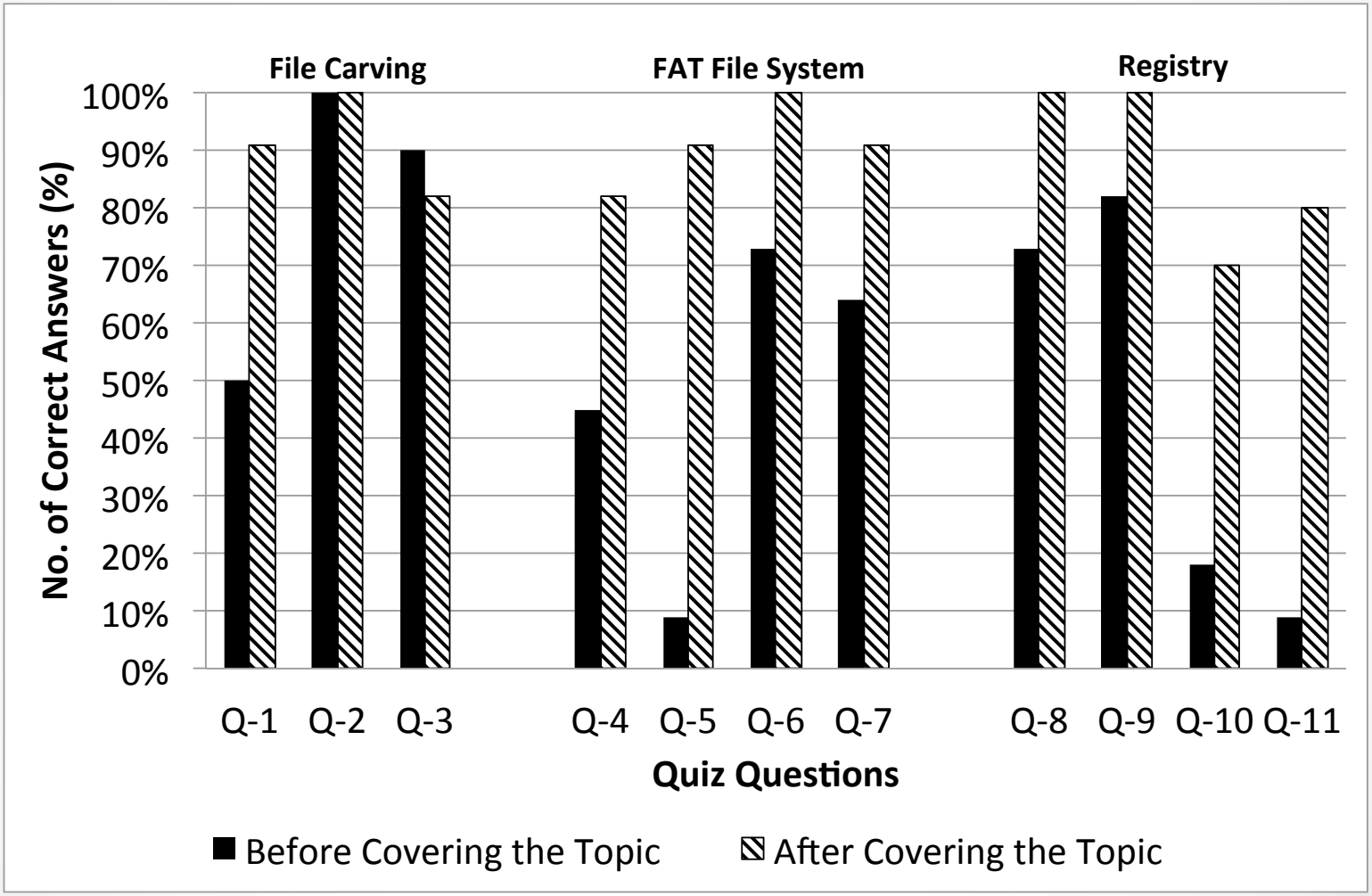
Pre-workshop Activities

- ***Advertisement***
  - Email is sent out to UNO CS Undergrad students
  - Registration form
- ***Reading Material:*** Students asked to read some material on workshop topics
  - Windows registry
  - File carving and
  - FAT32 and NTFS file systems
- ***Pre-workshop quiz***
  - Students are asked to complete a quiz on the reading material
  - Ensures that students read the material

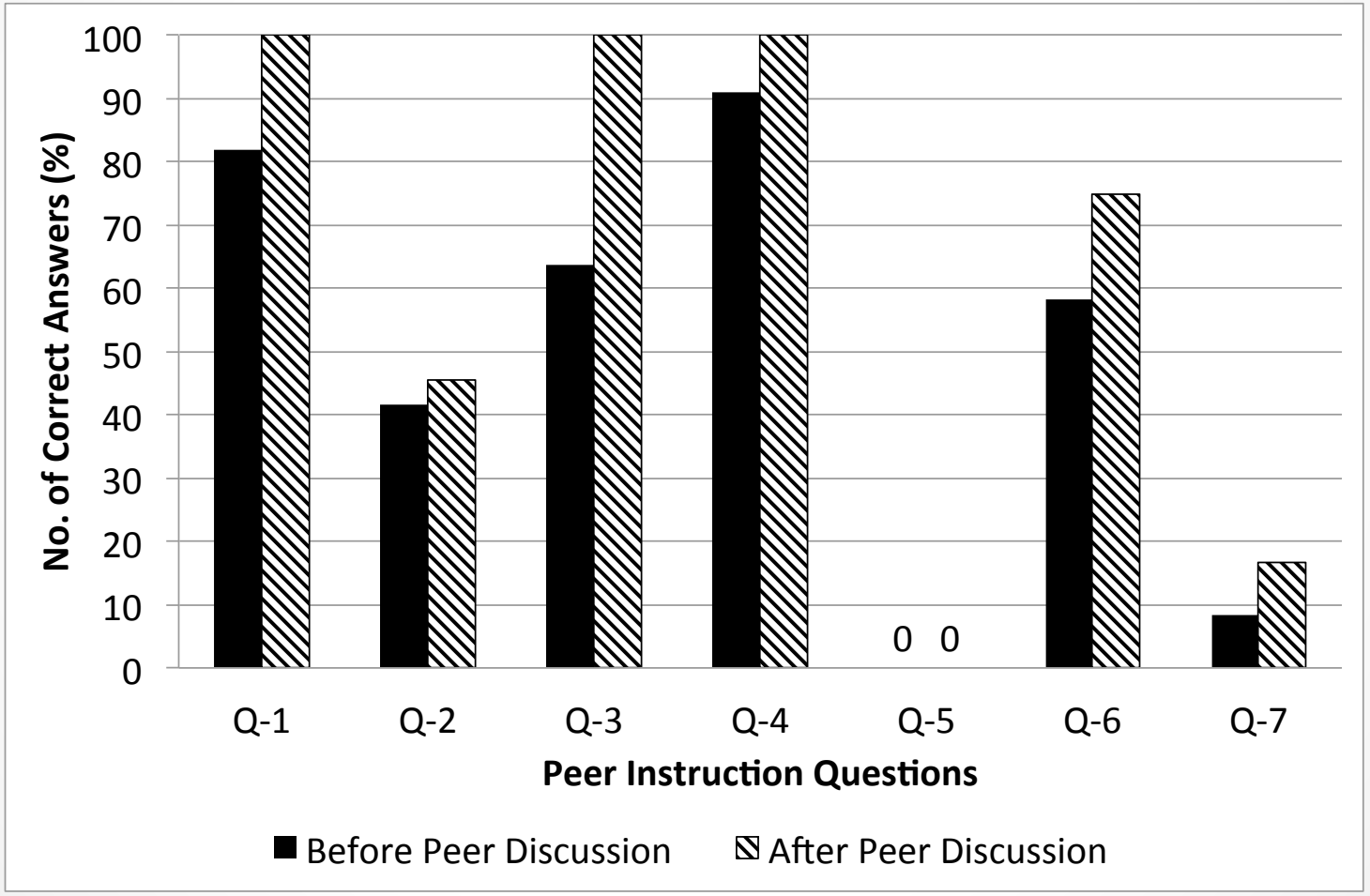
Evaluation

- Quizzes
  - Three quizzes: Carving, FAT, and Registry.
  - Each quiz is taken *before* and *after* the material is covered
- Survey on Peer Instruction Experience

Quiz Results



Peer Instruction Results



Question 5

- Originally worded "File carving is the most effective in which one or more of the following scenarios?"
  - A. Drive is highly fragmented
  - B. Drive is recently defragmented
  - C. System used to examine drive has low space
  - D. System used to examine drive has high space
  - E. More than one of the above

The question targets "**misconception**" about defragmentation, causing incorrect answers

Conclusion

- 108 peer instruction questions with variety of concept triggers
- Example and scenario based questions are often used
- Four-hour long workshop is used to test a subset of questions
  - The participants show positive response for peer instruction and clicker survey
  - The learning gain evaluated via quiz and peer instruction questions are 34% and 13%
  - 91% would recommend that other instructors use peer instruction

Please send me any questions at irfan@cs.uno.edu