The Design and Development of Hands-on Activities for Digital Forensics Education

Xinli Wang, Vijay Bhuse, and Sara Sutton

School of Computing

Grand Valley State University

Outline

- The problem and motivation
- Hands-on labs in three categories
  - Labs for tool use
  - Labs for knowledge reinforcement
  - Labs for mindset development
- A map to the CAE-CD outcomes
- Conclusion and future work

The Problem and Motivation

- We all know that hands-on activities are an important component for a digital forensics course.
- However, there is a lack of clear answers to the following questions:
  - What kinds of hands-on activities are needed for digital forensics education?
  - What are the educational objectives?
  - What are the specific learning outcomes from them?

Three Categories of Hands-on Activities (1 of 2)

- **Tool use:**
  - Students will learn how to use the tools that are used to complete the tasks for a digital forensic investigation through hands-on lab activities in this category.
- **Knowledge reinforcement**
  - Labs in this category are designed to reinforce the basic concepts and fundamental knowledge that are presented in class lectures.

Three Categories of Hands-on Activities (2 of 2)

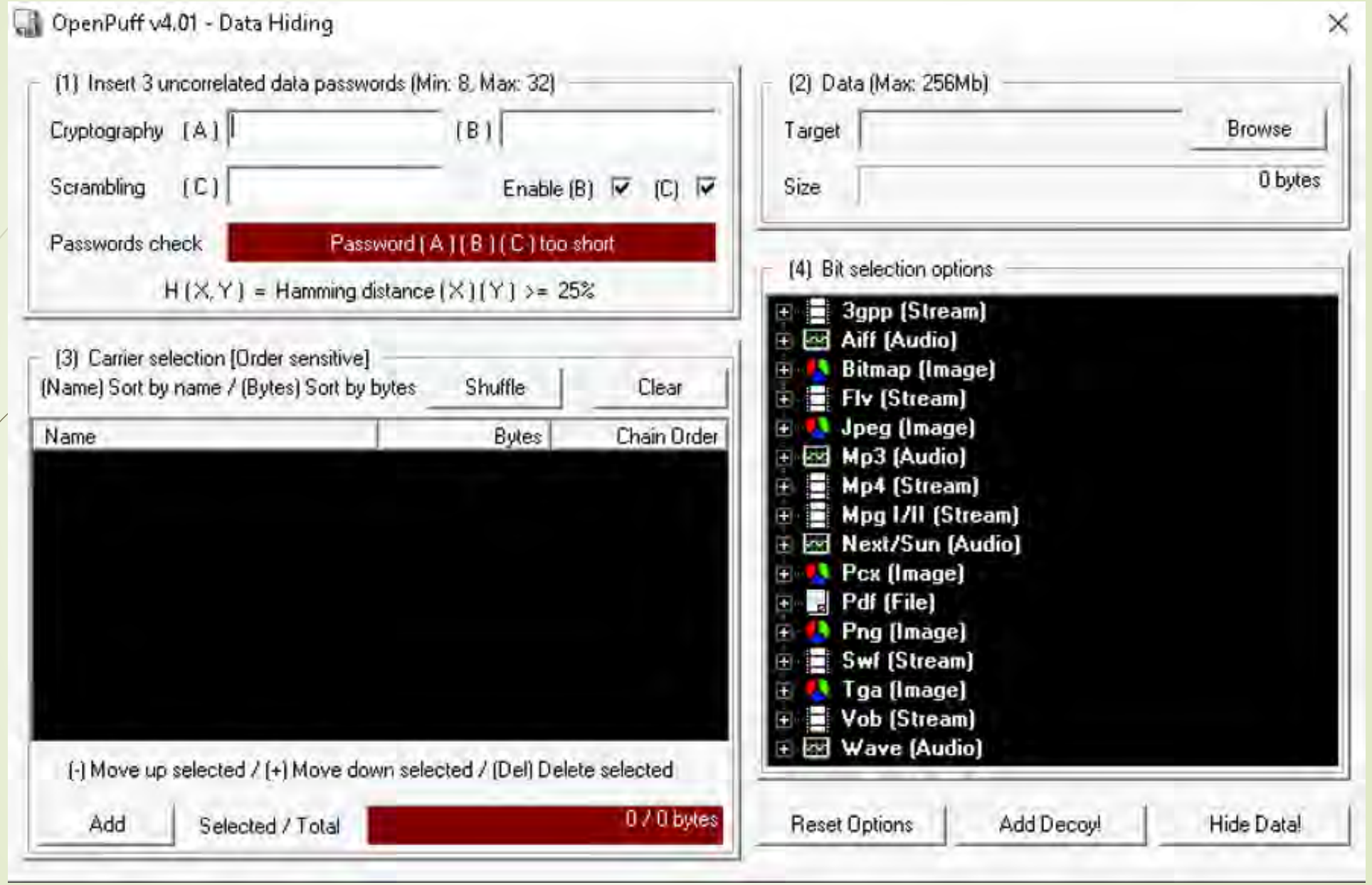
- **Mindset development:**
  - Hands-on activities in this category are designed to help students develop the mindsets that are needed for an effective digital forensic investigators.

Labs for Tool Use (1 of 3)

- The tools we introduced in our labs include (1):
  - **FTK Imager:** to image a physical disk or a logical disk, dump a snapshot or RAM, overview an existing forensic image.
  - **Autopsy:** to investigate a digital forensic image of different systems, including Windows and Linux, and email and photographic investigation.
  - **Volatility:** to analyze a memory dump.

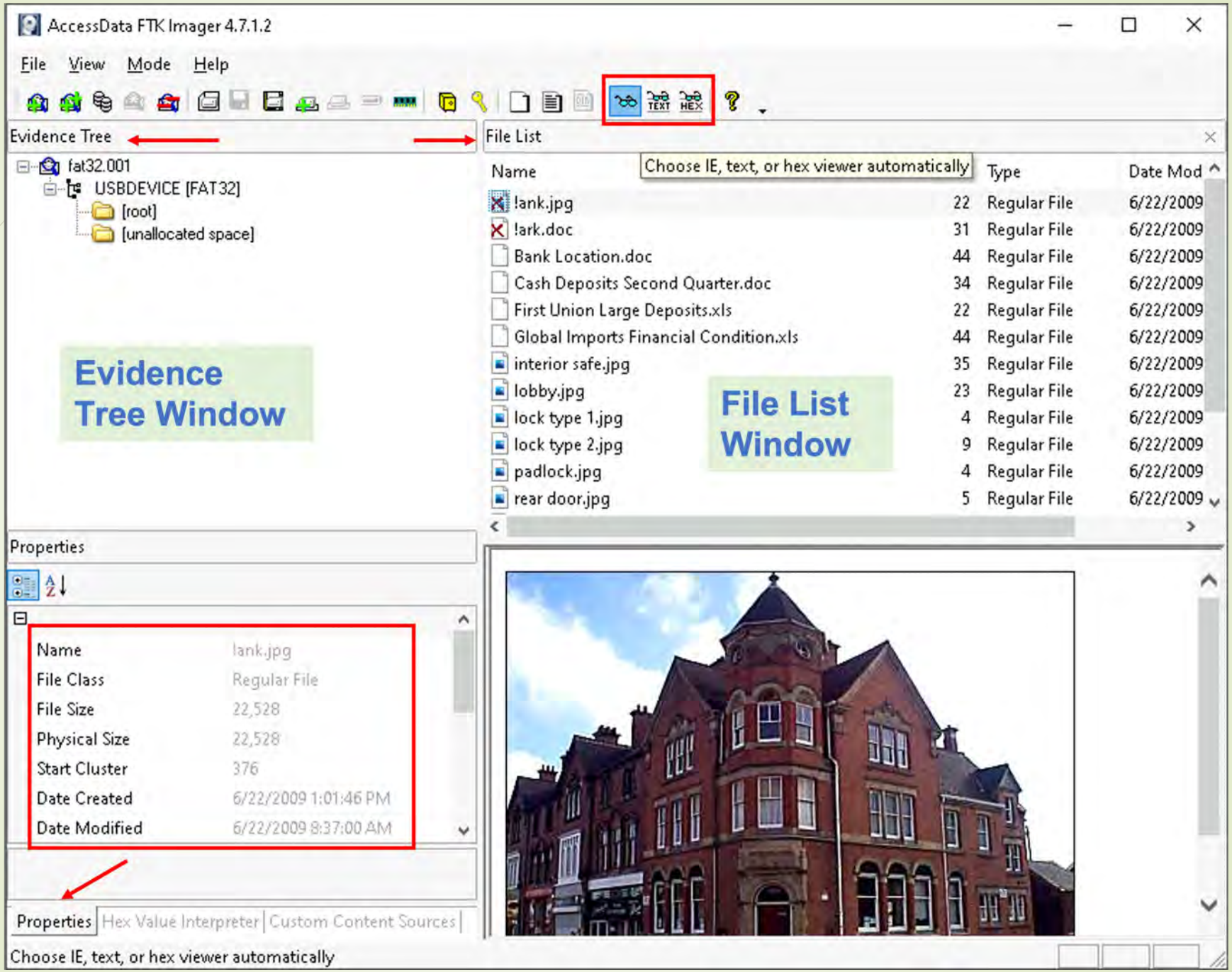
Labs for Tool Use (2 of 3)

- The tools we introduced in our labs include (2):
  - **Registry viewer:** to investigate Windows registry files.
  - **OpenPuff:** to investigate images files that has hidden data using steganographic techniques.
    - Very neat tool for educational purposes because it
      - Supports encryption methods.
      - Supports multiple file formats as carriers, including png, jpeg, etc.
      - Bit selection options.


OpenPuff v4.01 - Data Hiding
(1) Insert 3 uncorrelated data passwords (Min: 8, Max: 32)
Cryptography [A]
[B]
Scrambling [C]
Enable (B)
(C)
Passwords check
Password [A] [B] [C] too short
H(X,Y) = Hamming distance [X] [Y] >= 25%
(2) Data (Max: 256Mb)
Target
Browse
Size
0 bytes
(3) Carrier selection [Order sensitive]
(Name) Sort by name / (Bytes) Sort by bytes
Shuffle
Clear
Name
Bytes
Chain Order
(-) Move up selected / (+) Move down selected / (Del) Delete selected
Add
Selected / Total
0 / 0 bytes
(4) Bit selection options
3gpp (Stream)
Aiff (Audio)
Bitmap (Image)
Flv (Stream)
Jpeg (Image)
Mp3 (Audio)
Mp4 (Stream)
Mpg I/II (Stream)
Next/Sun (Audio)
Pcx (Image)
Pdf (File)
Png (Image)
Swf (Stream)
Tga (Image)
Vob (Stream)
Wave (Audio)
Reset Options
Add Decoy!
Hide Data!

Labs for Tool Use (3 of 3)

- The main educational objectives of the labs in this category are to help students help student learn how to use common forensic tools to examine a dataset and understand the functions the tools provide.
  - Link is given and ask students to download and install the current version of tools.
  - Step-by-step instructions are given.
  - Screenshots with highlighted marks are used to show students what can be found and from where they can be seen.


AccessData FTK Imager 4.7.1.2
File View Mode Help
Evidence Tree
fat32.001
USBDEVICE [FAT32]
[root]
[unallocated space]
Evidence Tree Window
File List
Choose IE, text, or hex viewer automatically
Name Type Date Mod
!ank.jpg 22 Regular File 6/22/2009
!ark.doc 31 Regular File 6/22/2009
Bank Location.doc 44 Regular File 6/22/2009
Cash Deposits Second Quarter.doc 34 Regular File 6/22/2009
First Union Large Deposits.xls 22 Regular File 6/22/2009
Global Imports Financial Condition.xls 44 Regular File 6/22/2009
interior safe.jpg 35 Regular File 6/22/2009
lobby.jpg 23 Regular File 6/22/2009
lock type 1.jpg 4 Regular File 6/22/2009
lock type 2.jpg 9 Regular File 6/22/2009
padlock.jpg 4 Regular File 6/22/2009
rear door.jpg 5 Regular File 6/22/2009
File List Window
Properties
Name !ank.jpg
File Class Regular File
File Size 22,528
Physical Size 22,528
Start Cluster 376
Date Created 6/22/2009 1:01:46 PM
Date Modified 6/22/2009 8:37:00 AM
Properties Hex Value Interpreter Custom Content Sources
Choose IE, text, or hex viewer automatically

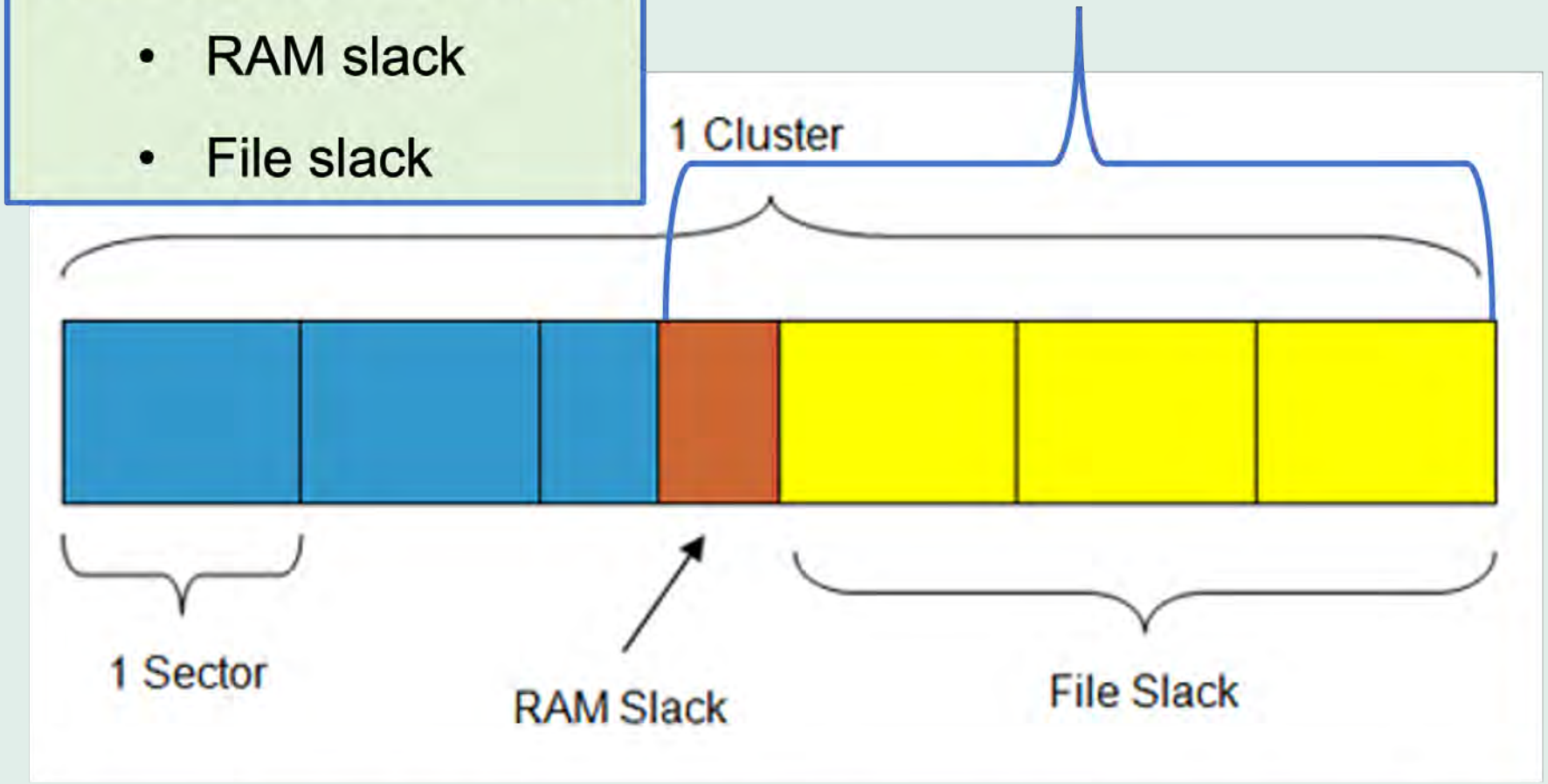
Labs for Knowledge Enforcement

- The main educational objective of the labs in this category is to help students gain in-depth understanding of essential concepts and fundamental knowledge that are presented in class lectures.
- One way to develop such labs is to ask informative results after related information has been observed.
- For example: $Drive\ Slack = RAM\ Slack + File\ Slack$
- When observed sizes of a sector and a cluster, along with physical and logical/real size of the file, ask for RAM slack and file slack.

Slack space/Drive slack:

- RAM slack
- File slack

Slack space/drive slack



Why RAM Slack? When a file is written to a disk, the writing is done sector by sector from RAM to disk.

Hands-on Activities for Mindset Development

- The mindset they need:
  - Analytic thinking
  - Technical curiosity
  - Objectivity
  - Patience and persistence
  - Ethical mindset
  - Self-learning
  - Etc.

The main educational objectives are to help students develop the mindsets.

Two subcategories:

Case studies – teamwork.

Course projects teamwork, 4 – 6 weeks.

A Map to the CAE-CD Outcomes (1 of 3)

Labs for tool use:

- “Use one or more common digital forensics tools, such as EnCase, FTK, ProDiscover, Xways, SleuthKit.”
- “Students will be able to understand how to acquire a forensically sound image.”

A Map to the CAE-CD Outcomes (2 of 3)

Labs for knowledge reinforcement:

- “Describe what can/cannot be retrieved from various Operating Systems.”
- “Describe the methodologies used in host forensics.”

Samples of Students' Feedback

"The course presented ideas in lectures then allowed us to work through a real-world example. I felt like I learned when I completed labs, and they made me think."

"The project is the perfect way to utilize what we learned in class as well as incorporate other forensic tools that we learned outside of class. Overall, it is fun to create the evidence."

Conclusion

- We have proposed to design and develop hands-on activities in three categories for digital forensics education for meeting the needs by an effective digital forensic investigator, including tool use, knowledge reinforcement, and mindset development.
- The development of these exercises has been briefly described in each category.
- The educational objectives and learning outcomes of these hands-on activities map to the CAE-CD outcomes very well.

End of the Lecture