Final Exam Review

Cyber Forensics, Fall 2022

Final Exam Description and Breakdown

Exam Process

The final exam will consist of two parts:

Part 1: Online exam

Part 2: Forensic Lab

Part 1 and Part 2 will each contribute 50% toward the overall final exam score

Online Exam

The final exam will consist of a timed exam, taken and graded on Blackboard

You will have a 36-hour window to take the exam

Date range: December 7-8, 2022

Online Exam

Number of Questions: ~30

Question Types:

- *Fill in the blank*
- *Fill in multiple blanks*
- *Short answer*
- *Matching*
- *Multiple Choice (single and multiple answer)*

Forensic Lab Exam

You will have to perform a forensic investigation

Inputs:

- Case Description
- Digital images (logical &/or physical)

You must submit a single Zip file that contains:

- Short write-up describing your investigation
- Forensic report
  - *A template will be provided*
- Extracted evidence

Grade will be based on:

The degree to which you met the success criteria associated with the Case Description

Quality of your investigation write-up

Quality of your forensic report

Following the provided instructions

Forensic Exam

Will be primarily focused on investigations at the application level

Email

Database

Social Media (e.g., chats)

May involve both computer and mobile device images

May require database extraction and recovery

Forensic Exam

The forensic exam will be made available early next week:

Monday, December 5 (~evening)

You will have ~5 days to complete the analysis and submit your results

Online Exam Process

Online Exam Process

You must complete the exam once you start.

You cannot pause the entire exam and complete it at a later time.

You will have 120 minutes to complete the exam from the time you begin.

At the end of the 120 minutes, if you have not submitted your exam, Blackboard will automatically submit it for you.

Online Exam Process

You can begin taking the exam on Wednesday, 7 December (time tba)

Once you begin, you will have 120 minutes to complete the exam. If you have not finished at that point, the test will be submitted for you.

When you are finished, review all your answers, then SAVE and then **SUBMIT** your exam.

Online Exam Process

Recommendation: First go through all the questions as follows:

1. *Answer all questions, even if you have to guess at or are uncertain of some of the answers*
2. *Note the question numbers for which you guessed at or are uncertain of the answers*
3. *After you complete answering all the questions, return to the questions you noted, review them, and change your answers as needed.*

Answers to Questions: Follow the instructions given in the question

*Answers are case **in**sensitive, so either upper or lower case is OK for a correct answer*

But misspelled answers that would be accepted as correct might be graded as incorrect if an upper-case letter is used. Follow the instructions given in the question.

Online Exam Process

Misspellings & Typos:

Please check your answers for spellings and typos.

While I review the automated scores to account for spellings and typos, I can't catch all of them

Save and Submit:

*After you're through taking the test, please make sure that you **Save** and **Submit** your test*

Don't forget to do this. While Blackboard will automatically submit your test, you will be ensured that every answer has been processed if you submit manually.

Online Exam Topics

FAT

Understand how FAT files systems are organized

Understand about the tables and metafiles in FAT

Understand about allocation of space and what keeps track of it

Know what TSK tools might be used to discover the contents of metadata files and tables

Be able to identify the partition boot sectors

NTFS

There will be one or more questions on NTFS

Know the goals of NTFS

Understand about cluster size containment compared to FAT

Know what contains the essential information about an entire NTFS partition

Carrier's definition of essential largely is the location and size of items

Understand about ***$MFT***, ***MFT***, and ***$MFT***

Know what the following means

$MFT{MFT[$MFT…]}

NTFS

Understand about the metadata MFT entries

e.g., What is MFT metadata record #0

Both Carrier and Nelson discuss MFT metadata tables

You don't need to memorize the MFT metadata entry names

Where is the allocation status of clusters contained?

File attributes

Understand about the location of file attributes

What are the two parts of an attribute?

ExtX

There will be questions on the ExtX file systems

- *Understand the layout and structure of ExtX file systems*
- *Understand blocks, superblocks, block groups, etc.*
- *Understand about thenumber of blocks and block groups*
- *Understand what is contained in the various blocks of a block group*

Allocation Strategies

Given a file to save into a specific file system, be able to place the file

Understand about the 3 types of allocation strategies

See

Lecture 8b slides (NTFS), topic "Allocation Algorithms"

Carrier, Chapter 8, Section entitled "Allocation Strategies"

SleuthKit & Linux Tools

There will be one or more questions on TSK and Linux tools

Understand and recognize the use of a few Sleuthkit tools such as

mmls

istat

fsstat

Understand and recognize the use of a few Linux distro tools

Forensic Suites

There will be questions on Forensic Suite tools

- *The focus will be on Autopsy*
  - The capabilities we reviewed, including, but not limited to
    - *How to create a case, add a data source and perform an analysis*
    - *Specialized viewers, e.g.,*
      - Communications Viewer
      - Timeline Viewer
    - *Extracting and recovering artifacts*
    - *Tagging for inclusion into HTML reports that can be included in an overall report template*
    - *Extending the capability of Autopsy using ingest modules*
- *There may be limited questions on*
  - OSForensics
  - FTK Imager

File Carving

One or more questions may be asked on the topic of File Carving

We covered this in more depth in the second half of this semester

Know (not exhaustive)

How different Operating Systems determine file types

Different techniques associated with file carving

Different file carving tools (both Windows and Kali Linux)

e.g., scalpel

Alternate Data Streams

There may be one or more questions on Alternate Data Streams (ADS')

You will need to know (not exhaustive)

- *What file system this pertains to*
- *How to set one up*
- *Limitations*
- *How to send files with ADS' intact across the internet or to other file systems*

Email Forensics

There will be one or more questions on Email Forensics

Understand client/server email architecture

Understand types of crimes involving emails

Privacy and Email investigations

Know what is most forensically interesting with regard to emails when doing an investigation. E.g.,

Know what can be found on the client

Know what can be found on the server

Email headers

Logs (Which ones? Where?)

Forensic Linguistics

There will be one or more questions on Forensic Linguistics

Understand what it is

Understand how it relates to email and social media investigations

Know the four Forensic Linguistic categories

Specifically know which category is most relevant to Email and Social Media Forensics

Know the primary specialties in Forensic Linguistics

Know what they are

Know which are more readily accepted in the court of law

Understand limitations

Email Forensics

Understand how to trace an email to determine its origin

- *Know important logs on Unix email servers*
- *Microsoft Outlook files*
- *Microsoft Exchange Server files*
- *Where to find messages locally for web-based email systems*

Forensic Tools for Email Investigations

- *Specialized tools (recognize, don't need to memorize)*
- *Hex Editor (when is it useful?)*

Recovering Email files

Social Media Forensics

There will be one or more questions on Social Media Forensics

Importance of Social Media Forensics

Types of crimes that involve Social Media

Role of mobile devices in social media forensics

Where most of the social media forensic information lies on mobile devices

Status of social media forensic tools

Anti-forensics

One or more questions will be asked on this topic

Know what this term means

Be able to give examples of this in the cyber forensics area (including database forensics)

Be prepared to give an examples of a tool that has some anti-forensic support

Mobile and Database Forensics

There will be one or more questions on Mobile and Database Forensics

Review the lecture for today's class

Go over Chapter 12 in your Nelson text

SQLite Database structure

SQLite Database file recovery

Database Forensics

Types of forensic data that can be recovered from SQLite databases (e.g., deleted tables, unallocated space, etc.)

Understand how this could apply to recovering forensic data from a smartphone

You will be expected to be familiar with the database forensics tools used in class today and in Assign06c_s

Strengths/weaknesses

Anti-forensic support

SQLite Forensic Corpus

Know what this is and how its structured

Understand its usefulness