CS 365: Digital Forensics
Spring 2020
Exam #1 Review

Arun Dunna
adunna@cs.umass.edu

Revision 1.0 - February 14, 2020

1 Exam Format

- **Duration:** 75 minutes
- **Question Format:** Multiple choice, short answer, and written response; no coding questions
- **Question Count:** 20 - 25 questions
- **Resources:** No notes; we will provide relevant tables where needed
- **Content Range:** All content from Lectures 1 through 8, and Assignments 2 and 3

2 Exam Contents

2.1 Lectures 1, 2, and 3

- Goal of forensics, and how digital forensics differs from traditional forensics
- Basics of digital forensics process models
- Locard's Exchange Principle
- Two main types of evidence, and examples
- Federal Rules of Evidence
- Types of reasoning (abduction, induction, deduction) and flaws with each
- Types of forensic investigations
- Little vs. Big Endian
- ASCII representation
- Purpose of hashing

2.2 Lectures 4 and 5

- Carving ASCII text
- Covered aspects of Unicode and UTF-8
- Encoding and decoding UTF-8 given code points or encoded text
- Searching for a given code point, and carving UTF-8 text
- Bit manipulations

2.3 Lectures 6, 7, and 8

- File formats and file extensions
- Definition of metadata, and covered methods of distinguishing metadata from file data
- Tradeoffs with each method of distinguishing metadata from file data
- Definitions of file headers and footers, and understanding of how to use them to identify files given the header/footer bytes
- Parsing file headers/footers given the format specifications of the header/footer, such as the WAV format
- Parsing EXIF metadata by hand given tables of tag IDs and tag formats, but not necessarily the rest of the EXIF format specifications for reference