CS 365: Digital Forensics
Spring 2020
Final Exam Review

Arun Dunna
adunna@cs.umass.edu

Revision 1.0 - April 28, 2020

1 Exam Format

- **Delivery Mechanism:** Gradescope exam
- **Duration:** 120 minutes
- **Availability:** May 1 00:00 - May 1 23:59 (EDT)
- **Question Format:** Multiple choice, short answer, and written response
- **Resources:** Open notes, **NO COLLABORATION**
- **Content Range:** All content from Lectures 15 through 24, and Assignments 5 and 6

2 Exam Contents

2.1 Lectures 15 and 16

- Structure of FAT filesystem
- Examples of boot sector contents, and know how to parse it given structure
- Endianness, and what the number in FATxx refers to
- What the FAT is and how it works
- What FAT clusters are and what they correspond to
- How to calculate maximum partition size of partition
- Reserved cluster values (FAT8, FAT12, FAT16, FAT32) and what they refer to
- How to parse FAT chains; what FAT fragmentation is and how it happens
- Directory entries and how to parse them; root directory and where it is stored; how subdirectories work
- File sizes and slack space relation

2.2 Lectures 17 and 18

- Differences between FAT and NTFS
- NTFS structure and how NTFS works
- How the MFT works and how to parse it
- How directories and subdirectories work in NTFS
- Be able to parse an NTFS filesystem given structures
- Role of data recovery in digital forensics

2.3 Lectures 19 and 20

- Why we care about malware in forensics
- Classes/types of malware that we covered
- Why permissions (and permission management) are important
- Role of operating system in malware
- Methods of obtaining malware
- Methods of detecting malware; methods of identifying malware
- How researchers reverse engineer malware (static/dynamic analysis)
- Malware defenses we discussed

2.4 Lectures 21 and 22

- Reasons why forensics varies between operating systems (both desktop and mobile)
- Roles that user authentication and automated encryption play between operating systems
- Importance of mobile forensics in modern society vs. (the still-important) desktop forensics
- Cloud infrastructure in mobile forensics

2.5 Lectures 23 and 24

- Role of biometrics authentication in law
- Role of biometrics in modern mobile forensics
- Process for biometric authentication/identification (including preprocessing, seeding, etc.)
- Examples of characteristics used in biometric authentication
- How biometrics can be applied to both digital forensics and real-time detection of crimes