# CS 365: Digital Forensics
# Spring 2020
# Exam #2 Review

Arun Dunna
adunna@cs.umass.edu

Revision 1.0 - March 18, 2020

## 1 Exam Format

- **Delivery Mechanism:** Moodle Exam module
- **Duration:** 60 minutes
- **Availability:** March 24 00:00 - March 24 23:59 (EDT)
- **Question Format:** Multiple choice, short answer, and written response
- **Question Count:** TBD
- **Resources:** Open notes, **NO COLLABORATION**
- **Content Range:** All content from Lectures 9 through 14, and Assignment 4

## 2 Exam Contents

### 2.1 Lectures 9, 10, and 11

- Structure of Internet (Clients, servers, packets, routers, DNS)
- Layers 1 - 4 of the OSI model, and familiarity with 5 - 7
- Basics of IPv4 address structure (hierarchy address scheme, valid ranges of octets)
- Splitting data among packets and reassembling data from packets
- Basic idea behind packet structures (header and payload; know examples of content in header)
- TCP/IP model in contrast to OSI model
- IPv4, IPv6, and TCP packet structures
- Why important to monitor network data
- Types of network forensics: active monitoring, and analysis of captured traffic; how each is done, reasons for each, and tradeoffs for each
- Sources of data used in analysis
- Common sources of evidence seen during (1) reconnaissance by attackers, and (2) actual attacks by attackers
- Content from written portion in Assignment 4

## 2.2 Lectures 12, 13, and 14

- Examples of storage technologies
- Differences and tradeoffs between storage technologies with and without moving parts
- Purpose of disk imaging, difference between hashing and checksums, and how to check integrity of images in different situations (checking copies vs. checking for malicious intent)
- Physical disk structure (cells and sectors)
- Logical disk structure (blocks, partitions, and volumes)
- Covered errors (physical/logical bad sectors, component failure, filesystem-level logical errors, firmware-level logical errors), and how they can be resolved (if they can)
- Definition of boot sector
- Structures of MBR and GPT, and differences between them
- How/why GPT offers redundancy of its header data and partition table
- How more than 4 partitions can be created in an MBR scheme
- Why filesystems are used, the basics of what each filesystem needs to keep track of in order to be a filesystem, and examples of extra features some modern filesystems may offer
- Examples of file metadata that most modern filesystems maintain
- Basic concept behind how the table in FAT works