Midterm Review

Two Parts to the Midterm

Online exam (on Blackboard)

Available starting 12 Oct

On Blackboard

Duration: ~ 1.5 hours

You will have 48-hour window to take it

Once started, clock starts running

 # Questions: ~20-25

Forensic Evaluation

Assigned after due date of Assign04b_rds (16 Oct)

Will perform forensic analysis of disk image

Duration: 5 days

Online Exam

Logistics

Nominal date:

Wednesday, 12 October

Question Types

Matching

Multiple Choice

Fill in the Blank

Fill in Multiple Blanks

Calculation

Online Exam

Reference Material

You are responsible for the following material:

Material in all lecture slides

Additional articles

E.g., “The Impact of Full Disk Encryption on Digital Forensics”

Nelson text:

Chapters 1-4

Chapter 5 (pp 195-203)

Carrier text:

Chapters 1-5

Online Exam

Topics

Topics Covered

- *Data Organization*
- *Digital Forensics Basics*
- *Computer Investigations*
  - Crime and Incident Processing
- *Forensic Laboratory and Investigator Certification*
- *Data Acquisition and Image Creation*
- *Mass Storage*
  - Rotating Magnetic Drives
  - SSD
- *Volumes and Partitions*
  - MBR
  - GPT

Online Exam

Data Organization

Binary, Decimal and Hex

Data sizes

Strings & Character Encoding

Data Structures

Flag Values

Reference:

Carrier Text: Chapter 2 / Data Organization section

Online Exam

Digital Forensics Basics

Digital forensics discipline

- *Know what (digital) forensics is*
- *Know what (digital) forensics isn't*

Related disciplines

Investigations triad

History of forensics

The law and digital forensics

Professional conduct

Types of forensic investigations

- *From Nelson text*
- *From lecture*

Online Exam

Computer Investigations

Investigation Procedure

- *Assess the case*
- *Plan investigation*
- *Secure evidence*
- *Gather evidence*
- *Analyze evidence*
- *Complete case*

Chain of custody

Acquiring digital evidence

Online Exam

Forensic Laboratory and Investigator Certification

Computer/digital forensic laboratory certification

- *ASCLD, others*

Computer/digital forensic investigator certification

- *IACIS, HTCN, others*

Internet Crime Complaint Center (IC^3)

Uniform Crime Reports (UCRs)

Forensic Laboratories

- *Home-based*
- *Mid-size*
- *Large/regional*

Forensic workstations

- *Needs and criteria (high level)*

Business case for developing a Forensics Lab

Online Exam

Data Acquisition and Image Creation

- Image formats suitable for evidence
  - *Raw (dd), .e01, AFF, etc.*
- Data acquisition
  - *Planning for image acquisition*
  - *Acquisition methods*
    - Local
    - Remote Network Acquisition
  - *Acquisition tools*
  - *Validating data acquisitions*
  - *RAID acquisitions*
  - *Tools*
- Hidden disk areas
  - *HPA*
  - *DCO*

Online Exam

Data Acquisition and Image Creation

Forensic images

- *Meaning and requirements for making forensic image*
- *Hash functions*
  - Which are used most commonly
  - Why two are used
- *Tools you know that are capable of making forensic images*
- *Forensic analysts should work from forensic copies, not originals*

Online Exam

Mass Storage

Microprocessor Architecture

- *IA32*

Hard Disk Drives

- *Hardware composition*
  - Platters, spindles, read/write heads, etc.
- *Magnetic storage*
- *Disk architectures*
  - ATA (PATA, SATA, ATAPI)
  - SCSI
- *Disk organization (physical formatting)*
  - Tracks, sectors, cylinders
- *Addressing*
  - CHS, Extended CHS
  - LBA
- *Locking/Unlocking ATA devices*

Online Exam

Mass Storage - continued

Solid State Drives (SSDs) (aka Flash)

- *History*
- *Basic hardware technology*
  - *NAND*
- *Data organization*
  - Pages, blocks, etc.
- *Advantages/disadvantages vs. HDDs*
- *Wear leveling*
  - Different strategies (dynamic/static)
- *Garbage Collection*
- *Key characteristics of SSDs*
  - Fast reads/slow writes/very slow erases
- *Error correcting*
- *SSD File Systems*
  - Mechanisms employed to offset SSD limitations
  - Effect of these mechanisms on digital forensic investigations

Online Exam

Volumes and Partitions

- BIOS
  - *Role in booting computer*
  - *Relationship to MBR (see below)*
- Volume
  - *How volumes relate to partitions*
  - *Linux vs. Windows*
  - *Volume spanning*
  - *Volume analysis*
    - Partitioning schemes
    - Overlays, detecting deleted partitions, etc.
- Partition
  - *How partitions relate to volumes*
  - *Partition tables*
    - MBR
    - GPT

Online Exam

Volumes and Partitions - continued

- MBR (detail)
  - *Different partition types*
  - *Limitations*
  - *MBR and the boot process*
    - Typical
    - Multiple OSs
    - Boot sector virus
  - *Tools to analyze*
- GPT
  - *Advantages over MBR*
  - *EFI vs. BIOS*
  - *GPT Volume Layout*
  - *GPT Partitions*
  - *Tools to analyze*

Forensic Analysis

Basics

Date available to students:

- *After Sunday, 16 October*

What you will receive

- *A scenario*
  - Posted on Blackboard
- *Raw disk image*
  - Uploaded to your student folder on the R: shared drive
  - It will be located in a folder called “Midterm”
  - Different students will receive different disk images

What you will submit

- *A single zip file containing*
  - A description of the artifacts you found, including how you found them (e.g., what tools you used, what options, where you looked, etc.)
  - The artifacts that you obtained from the disk image

You will have 5 days to complete it

Forensics Analysis

Scenario and Disk Image

The scenario will give you

- *Background*
- *Hints as to what to look for*

Tools you may have to use to forensically examine image

- *Autopsy*
- *Winhex*
- *FTK Imager*
- *OSForensics*
- *dd*
- *mmls*
- *Gpart*

Preparation

- *Assign04b_rds will give you good practice for this*
- *This forensic analysis will also be good prep for the forensic analysis portion of your final*

Forensics Analysis

Skills and Knowledge

Skills and knowledge you will need to analyze image

- *Tool use. E.g.,*
  - Know how to load in disk image
  - Know how to have tool interpret image as disk
- *Read hex dumps*
- *Interpret tool output*
- *Determine partitions*
  - MBR
  - GPT
  - Deleted
- *Analyze unallocated space*
- *Recover deleted files*
- *Extract artifacts from disk image*