COMP 5350 / 6350 – Project #1

The first project for COMP 5350 / 6350 will focus on analysis of FAT16 and NTFS partitions and will require understanding of how to properly recover data from each.

Schedule:

Project #1 Assigned: 4 September
Project #1 Due: 8 October

Students Project Requirements:

Each team will be provided with a disk image that was collected from a laptop during a forensics investigation. This investigation will require you to critically evaluate and analyze digital artifacts on the laptop. The overall objective of this project is to recover data and determine if there is proof of criminal activity.

- ✓ Project1.dd

Part I: Technical Analysis

The first part of this project focuses on the technical analysis of the disk image where you will answer the following questions.

1) Specify the number and type of partitions on the disk image.
2) Specify the number of files, file names, and file size of each file on each partition.
3) Specify the starting and ending byte offset location of each file on each partition.
4) For each FAT partition explain the contents of the File Allocation Table and Root Directory.
5) For each NTFS partition specify which file attributes are associated with each file
6) Manually recover all files from each disk image. Note: You must show the step-by-step process for file recovery. Automated file recovery tools may not be used during this project!

Part II: Operational Analysis

The second part of this project is to "paint a picture" from the digital artifacts collected and analyzed. During this part of the project your team will answer the following questions:

1) What data hiding methods were used on this disk image?
2) What tools and / or applications were used to hide data?
3) Lastly, what was the ultimate objective of users of the laptop?

Final Report:

Each team will provide a final report that answers the questions from the grading rubric. The format of the final report will include the following sections:

1) Executive summary
2) Problem description
3) Description of analysis techniques utilized
4) Tables and screenshots
5) Conclusions and Recommendations

The purpose of this report is to show that effective analysis of each image was properly conducted. A single page report will not adequately answer all questions so be prepared to have an in-depth analysis and description of the methods you used to answer the questions.

Grading Rubric:

The grading rubric that will be used to grade each disk image will be based on the following criteria:

Activity	%
Specify number and type of partitions on the disk image	5%
List file status, filename, extension, attributes, and file sizes for each file on each partition	10%
Specify byte offset location for each file on each partition	15%
For FAT partitions generate a FAT	10%
Recover all files from each partition	25%
Describe data hiding methods used on partitions or files	15%
Describe what tools or applications were used to hide data	10%
Describe the ultimate objective of users of the laptop	10%
	100%

Project Grading:

Letter grades will be assigned based on a 10-point scale:

90 – 100 = A
80 - 89.9 = B
70 - 79.9 = C
60 - 69.9 = D
< 60 = F

Project Results							
Partition	Filename	Extension	Attribute	Status	Byte Offset	File Size	Recovery Command
FAT16	Image1	jpg	Archive	Deleted	1420342	20423	sudo dd if=Project1.dd of='Image1.jpg' bs=1 skip=1420342 count=20423 status=progress