NAME: Megan Leonard

TODAY’S DATE: 2/26/2023

# ISEC 375 Homework 5

Answer the following questions based on your reading of the textbook, the module key points, and the instructor’s presentation this week.

1. **[3 points]** A hard drive has 40 logical platters, 16,384 cylinders, and 63 sectors per track. A sector has 4096 bytes. What is the size of the disk in Gigabytes?

40 platters = 80 heads as heads are 2 per platter.

Tracks = cylinders x platters = 16,384 x 40 = 655,360 tracks.

63 sectors per track so total sectors = 63 x 655,360 = 41,287,680 sectors total.

Each sector has 4096 bytes so total bytes = 41,287,680 x 4096 = 169,114,337,280 bytes.

Going with the book’s conversion of 1,000 bytes = 1kilobyte, we get 169,114,337.28 kilobytes. Then 1,000 kilobytes to 1 megabyte so we get 169,114.33728 or 169,114.34 MB.

1,000MB = 1 Gigabyte so we get 169.11434 or 169.11 GB

1. **[3 points]** If you are suspicious about an image file with a "bmp" extension, what do you do to ensure that it is an original bmp image or an executable file that the attacker changed its extension to avoid the suspicion.

To ensure that it is an original bmp image or executable file, we will check the file over in the hex editor where we can check the header value and identify the file type.

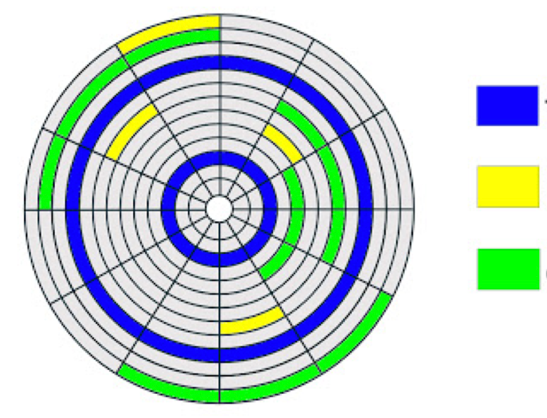
1. **[6 points]** You have a search warrant for a company employee suspected of downloading and storing video files containing child abuse. You entered into the office room of the suspect and seized his computer. His desktop computer is on and running the Windows 7 operating system. Full disk BitLocker encryption is enabled on the computer. So you are making a live data acquisition. When you uncover the case of the computer to note all the hard drives and also models of them, you see that there is only one Seagate 500 GB internal hard drive. When you double click "my computer" icon, you can see C, D, and E drives with sizes of 10 GB, 100 GB, and 140 GB, respectively. You realize that there is a missing 250 GB disk space. You think that video files might be stored in this hidden space. What is the name of this hidden space? Please write the steps you perform as a forensics investigator to access the hidden space.

The hidden space is called hidden partitions or voids as they are gaps between the partitions on a disk. To start, as this is a company employee, we will get the pass code for bit locker from tech support so that we can get past bitlocker. To find the hidden partition, we will access the partition table in the Master Boot Record within sector 0 of the disk drive. We can use WinHex to determine the offset between the first partition and use that to locate where the hidden partitions are located so we can access it without it being reformatted. We will make sure to take note of the location of the hidden partition so we do not have to search for it again and we create a copy of the hidden partition so we can have better access.

1. **[3 points]** What happens when you delete a file in a FAT32 file system?

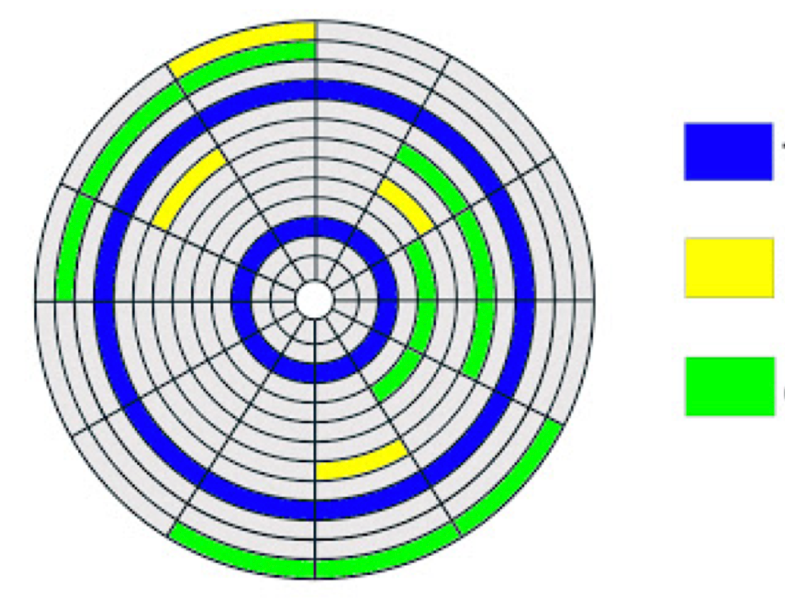
When a file in a FAT32 file system is deleted, the directory entry will be marked as a deleted file with the HEX E5 character replacing the first letter of its name. The FAT chain is then set to 0 while the data found in the file will remain on the disk drive. The disk area of the deleted file then becomes unallocated disk space so it can receive new data.

1. **[3 points]** You see a fictitious head of a hard drive below. What do blue, yellow, and green areas represent? Assume that, the hard drive has a Microsoft-compliant file structure.



The yellow area represents sectors within the hard drive. The green is used to represent clusters. The blue represents tracks within the hard drive.

1. **[6 points]** Let's assume that yellow areas of below head represent recently deleted files. Blue and green areas represent occupied space. Gray areas represent empty spaces. Let's also assume that the size of each small tile is 5 Megabytes. You have a file with a capacity of 30 Megabytes. You will copy the file from your USB thumb drive to the hard drive. The starting cluster is shown with the red small lightning symbol. Copy operation will be performed clock-wise on the same track. Please put a cross sign to the tiles on which file will be copied. At the end of the copy operation, can it be said that the file became fragmented?





The file will become fragmented as it is separated in half when being saved following the clock-wise pattern, starting at the indicated spot of the lightning bolt.

1. **[3 points]** What is a resident file in the NTFS file system?

A resident file is a file that contains 512 bytes or less and can be found stored in the master file table.

1. **[3 points]** Which information below is not stored in Windows Registry?
2. Hardware configuration information
3. User account information
4. Network connections
5. Log files
6. File type and file extension information