NAME: Megan Leonard

TODAY’S DATE: 3/12/2023

# ISEC 375 Homework 6

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

1. **[9 points]** You are making the forensic investigation of a live Linux system. You want to see the logon and logoff times of the suspect. The username of the suspect is john. Write down a single Linux command that will create an investigation file named john\_login.log showing login and logoff information of John.

$last john > /home/john\_login.log

The last command shows the last login and logout of users, so we specify the user john and the > is used to send the output of the command left of it into the right which is where we have the investigation file.

1. **[6 points]** If you are using a forensic tool that ignores inode 1 in the Linux file system, what action of the suspect may cause missing data during the data extraction process? What can be done to overcome this problem?

Inode 1 is used to contain bad blocks or bad sectors on the disk so by ignoring it, we ignore some possible important information as a block could be mase into a bad block to hide files and information we are looking for. To overcome this, we use the mke2fs command to create an ext2/3/4 file systems and then we can use the e2fsck to find the bad blocks. We use the

-c which locates any bad blocks and the -k which will help preserve any existing bad blocks and -L with a filename to save the bad blocks list to so it can be accessed even if the tool ignores the inode 1.

1. **[9 points]** What are four components that define the UNIX/Linux file system? What are the equivalents of these components in the NTFS file system? If you are investigating access and changes dates of the files in a hard drive with the Ext4 file system, which components of the filesystem are covered by your investigation?

The first component is the boot block which holds the bootstrap code for the Linux system. The NTFS equivalent would be the sector 0 and its master boot record. The second component I the superblock which manages the file system and tracks the inodes, available space, and specifies the disk geometry. Its NTFS counterpart would be the MFT or master file table. The third component is the inode blocks which are the first data following the superblock and are assigned to every file allocation unit. The NTFS component like this is the metadata. The fourth component is the data blocks which is where the directories and files are stored. NTFS uses clusters as an equivalent to this. Investigating changes in the fates of files would have us working in the inode blocks and the data blocks as we are dealing with the metadata changing of the specific files. We would also use the superblock to help locate where the changes took place.

1. **[6 points]** You are in a crime scene. There is a MacBook Pro computer. The computer is running and unlocked when you arrive at the crime scene. If you realize that the guest account is logged on to MacBook, what steps do you take in your investigation?

First, we can note that since there is a guest account, we will be working with Linux and not have to worry about macOS. We want to make sure to note any programs that are running and because we are working with apple technology, we have to start getting what data we can. Based on the apple site, files created by the guest account are only stored in temporary folders that are deleted upon logout so we would need to be able to copy these files. We want to make sure that it is powered securely and start copying the files and note any processes that are running at the time as closing the lid would shut down any nonessential processes. We also want to access the device settings to make sure that closing the lid will not log out the guest user. We can turn off sleep mode by going to energy saver and setting turn display off after to never. For the most part we want to make sure to mark everything that is active, keep the device from sleeping or shutting down, and copy any temporary files before we can move from the crime scene.