Part 1:

Review the auth.log snippet and the contents of the ‘admin’ user directory.

**auth.log** - https://umd.box.com/s/fcn3rofylx6fg35o83j870w2w7jlthw3

**admin directory** - https://umd.box.com/s/fz511i74erti0cc2bdo59ilgv19cs995

1. Provide an explanation narrative of the attack that includes:

-based on the commands used, what actions or steps did they take?

-What did the person do or what were they attempting to accomplish?

-Provide a few screenshots with your name in original context

------------------------------

Part 2:

Use foremost (or another strictly file carving utility of your choosing) to analyze the disk image and perform file carving.

Disk Image:  
https://umd.box.com/s/f3uz9rfpcp073ih7zoaycccht47z8ob0

1. What files do you find?

2. What are the contents of the files?

3. What command or tool did you use to find the files?(Give lots of detail)

4. Provide a screenshot of your command/tool usage with your name on the command line and in original context (ex. working from a FolderName that is your name)