**1. What specific behaviors of this machine make booting normally a bad idea?**

**There is an anti-theft system that asks for a password before booting the operating system. If an incorrect password (evidence 1.0) is detected, the hard drive will purge itself (evidence 1.1) making it impossible to get into (evidence 1.2). As forensic investigators, we must find a backdoor to get around the anti-theft system.**

**2. What operating system does the suspect use?**

**The suspect is using "4.13.0-21-genertic #24-Ubuntu" (evidence 2.0).**

**3. What is the username of the account typically used by the suspect?**

**The username of the account typically used by the suspect is "Leslie Nielson" (evidence 3.0). The suspect also uses the online alias "Artemis" (evidence 3.1).**

**4. Any indication that the suspect shared the company secrets with other individuals?**

**There is indication that the suspect has shared the company secrets.**

**- There is a hidden message in 1.jpg which contains an internal SDSC email telling Alex to dump Bungle stock (evidence 4.0).**

**- A top secret SDSC memo was leaked (evidence 4.1), we believe by the suspect because a file on their device named "secret\_exe" had the password to unlock the SDSC memo (evidence 4.2).**

**- A top secret SDSC ledger was also leaked (evidence 4.3), which we also believe the suspect provided because a file on their device named "contract.mp3" had the password to unlock the ledger (evidence 4.4).**

**5. Reconstruct the timeline of actions by the suspect that may be relevant**

**6. Anything else on the computer that would imply the suspect had malicious intents in using this computer?**

**7. Any suspicious-looking encrypted files on the machine? Attach decrypted contents (if possible) as evidence and briefly describe how you obtained the contents.**

**There is a zipped file called "secrets.zip", which using password "6f7y**

**(evidence 7.0), contained**

**- 1.jpg, which contained an internal SDSC email (evidence 4.0)**

**- 2.jpg, which when renamed to 2.zip contained two more files "good\_advice.png" and "plan.png" (evidence 7.2)**

**- contract.mp3, which when analyzed through a sonic visualizer revealed a message "PP4m#36ajK1mu" (evidence 4.4)**

**- secret\_exe, which we discovered plain text "the password is "ke9dtcesm6f"" (evidence 4.2)**

**8. Did the suspect try to delete any files before their arrest? Please attach the name(s) of the file(s) and any indications of their contents that you can find.**

**The suspect tried to delete the folder "finished" and files ".chat.log.swx", "insurance.txt", and "planning.png"**

**- We found the folder "finished" (evidence 8.0) which contained many images as well as multiple files**

**- "finished" contained a document that would eventually be "insurance.txt" (evidence 8.1)**

**- We recovered ".chat.log.swx" (evidence 8.2) using Autopsy**

**- We found "planning.png" in 2.jpg from part 7 (evidence 7.2, 8.3).**

**The suspected deleted the contents from "bash\_history" (evidence 5.5)**

**9. List all other secrets, and other findings.**

**217 Possible Zip Bombs: Using Autopsy, we were alerted to 217 possible zip bombs (evidence 9.0)**

**Leslie's Ubuntu Password: Used John the Ripper to find the password "copper" (evidence 9.1)**

**info.pdf password: Inside the recovered chat log (evidence 8.2), we got a link to a password protected pdf. We cracked the pdf, discovering password "beacon" (evidence 9.2)**

**Agent user: We used a python script (agent.py) to brute force https://weratepups.xyz in order to find the agent user, 86753, to real a concealed chat (evidence 9.3)**

**RSA Public key: found in id\_rsa (evidence 9.4) in order to confirm our identity in the conconcealed chat**

**insurance.txt: Discovered the members of The Collective when recovered the folder "finished" (evidence 8.1)**

**Employee Badge: There is a SDSC Auditor - All Access employee badge (evidence 9.5)**

**10.**

**a. What does this file indicate? (Be specific)**

**This file indicates that the user running SDSC’s website was trying to log in to a machine that it did not have credentials for. They were using port 22 which is the ssh port, and so were tring to get remote access to root on sshd, CRON (a time-based job scheduler), tty1 (text only terminal) and PAM (pluggable authentication module). They successfully gained access to root and changed the password to “chauthtok” after finding user ‘nefarious’**

**b. Can you attribute this behavior to a specific program?**

**This auth.log suggests that the suspect was trying to brute force a password. This suggests a program such as THC-HydrU or Hydra5-4, both of which can use a dictionary attack to crack SSH passwords.**