**A4**

**Prob1**

**A screenshot of a computer

Description automatically generated with medium confidence**

**Graphical user interface, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

## Questions:

1. In Digital Forensics why are hash values calculated for files? **1pt**

**Can be compared agains known file hashes to possibly determin what a file is.**

1. Name 2 other existing hashing algorithm, other than **md5** or **sha256**? **2pts**

**- sum32**

**- CRC32**

* 1. Is there a reason why you would choose **sha512** over **sha256** or **md5?**

**Sha512 is a more complex and more secure algorithm**

* 1. What is one cost associated with using one algorithm over another? *Cost here implies a negative impact.* **1pt**
     + **A more complex algorithm such as sha512 is more secure but more computationally expensive to perform**
     + **A less complex algorithm such as MD5 is less secure but faster to perform**
     + **Balancing act between security and resource cost.**

1. Why are file extensions not a good way of knowing the true nature (**type**) of the file? **1pt**

**file extensions can be changed to anything and may not represent the contests of the file**

1. Other than file extensions or hashes, what other methods that can be used to determine if a file is unique or is correctly identified? **1pt**

**File magic number can be checked to determin file type**

**Hexdump file and analyze the contents.**

1. Explain why an analyst should **NOT** use the original suspected folder to perform analysis? **1pt**

**You want to make sure you do not accidently change something in the original folder so you always have the original files.**

**Prob 2**

**Text

Description automatically generated**

**Text

Description automatically generated**

## Questions

1. What improvement(s) to the password policy would you suggest to this company?

**They should improve the hashing algorithm, each user appears to have at least 2 million 8 digit password solutions.**

1. As the Security Analyst on staff what improvements would you make if you noticed a user having many failed attempts?

**By reducing the number of attempts between lock outs and lengthening the lockouts (possibly exponentially) we could introduce a minor inconvenience to a normal user but make brute force attacks impractical.**

1. What is a brute-force attack?

**Trying every possible solution in a logical order.**

* 1. What would you use as criteria to determine if the user’s account is being hacked using brute-force?

**Number of attempts and any pattern in the passwords or order including known wordlists**.

* 1. Now that you know what brute-force attack means; name at least 2 other techniques that an attacker could use?

**Phishing**

**Social engineering**

**Physical access**

* 1. As a penetration tester, how would you avoid being noticed by the system administrator, while performing your penetration testing?

**If it was possible to get access to a password file and test aginst the hashes outside the targets system.**