

INFORMATION SECURITY STRATEGY DEVELOPMENT

**A password protection controls, risk management and digital
forensic investigation report**

Prepared by

Samuel Boadi Agyekum

London, United Kingdom

[Email](#) | [LinkedIn](#) | [GitHub](#)

Repository: github.com/agyekumboadi/information-security-strategy-playbook

Release tag: v1.0-verification-snapshot

Developed during MSc studies at Arden University (UK)

This report includes risk analysis, control mapping, implementation recommendations, and audit-ready evidence references.

Abstract

Password protection policy is a core mandate of every organisation seeking to protect service users and all necessary stakeholders. The purpose of this policy is to initiate and rollout measures for creating strong passwords, protecting them, how frequent users need to change them as well as ceasing loopholes for unauthorised intrusions. It is therefore essential for every organisation to put measures in place that can help minimise the vulnerabilities and attacks of a system. It also shows a forensic approach to recover deleted files and recover passwords using winhex tool.

Table of Contents

1.1 Password Protection Policy	4
1.2 Scenarios Associated With Corporate Passwords Being Compromised	5
1.2.1 Scenario 1	5
1.2.2 Scenario 2	6
1.2.3 Measures To Minimise Related Issues From Occurring	7
1.2.4 Defensive Measure To Block Unauthorised Access	8
2.0 Digital Forensics.....	9
2.1 Winhex Forensic Investigation	9
3.0 Conclusion.....	20
References	21

List Of Figures

Figure 1: Creating dump file	10
Figure 2: Locate the dump file	11
Figure 3: Click open to locate file via winhex	12
Figure 4: Open located file via winhex	13
Figure 5: Dump file data	14
Figure 6: File recovery type option	15

Figure 7: Selection of file type to be recovered	16
Figure 8: Recovery by header	17
Figure 9: Complete file recovery	17
Figure 10: Recovered files in Winhex folder	18
Figure 11: Simultaneous search button to recover password	19

List Of Abbreviations

Next-Generation Antivirus (NGAV)	8	Unique Quality Care (UQC)	4
Personal Protective Equipment (PPE)	5	Universal Serial Bus (USB)	4

1.1 Password Protection Policy

Password protection policy is a core mandate of every organisation seeking to protect service users and all necessary stakeholders (Shay *et al.*, 2016). The purpose of this policy is to initiate and rollout measures for creating strong passwords, protecting them, how frequent users need to change them as well as ceasing loopholes for unauthorised intrusions.

Unique Quality Care (UQC) is a private home care provider registered under the Care Quality Commission (CQC) under the Health and Care Act 2022. Services comprises of elderly and children care. Due to the delicate nature of the safety of clients which is the topmost priority of the company, safeguarding their personal information and type of care given is a paramount. Also, the work scope of employees regarding their personal data, and passwords used to access company resources are at the heart of the company.

In section 5 (IT Systems, Telephones and Monitoring) of the company's handbook, it shows in subsection 5.2.1 the Security scope of our System to mitigate information security breaches (Unique Quality Care Ltd., 2023, pp. 22-23). Employees are therefore urged in the handbook to adhere to these measures enumerated below;

- 1) An employee cannot make changes to pre-existing hardware or software unless authorised by management.

- 2) External devices such as Universal Serial Bus (USB) drives, external hard drives, and installation disks are not allowed to be attached to computers and printers unless permitted to do so and protected with password .
- 3) It is mandatory that employees take extra precautions and inform management when emails regarding the company are sent to them from unknown sources.
- 4) Employees are obliged to log out of computers and software such as the Birdie app (the application used by carers in the company to document care given to clients such as medication, health status, surroundings, and care assistance given) when left unattended.
- 5) Employees must protect their personal devices such as mobile phones, tablets and laptops with strong passwords.
- 6) If an employee's device is stolen or misplaced, he or she must inform management as soon as possible for the necessary measures to be taken.
- 7) Passwords of employees must not be shared amongst colleagues or third parties in quest of being busy, away from work, or after resignation.

1.2 Scenarios Associated With Corporate Passwords Being Compromised

Globus is a renowned company best-known for the manufacture of various protective clothing used at workplaces. Protective products that ensures adequate protection of hand, ear, eye, respiratory tract, head and body are the core values of the company. They are the sole distributors of Personal Protective Equipment (PPE) such as face masks, disposable gloves, aprons, head coverings, and shoe coverings to UQC. These PPEs help carers to ensure safety precautions at clients residence when carrying out their duties.

1.2.1 Scenario 1

Globus representatives who convey PPEs to UQC has established a strong relationship with staff members who work at the office. They seek opinions of products with regards to the type that best suites carers and enable a faster and effective workflow.

A typical scenario regarding password being compromised was a staff member at the accountancy section who watched a documentary of newly manufactured type of nose masks used in a hospital in the United States. She being in a hurry to share with the representative who delivers PPE's to the office, she made a copy of the video onto a flash drive and gave it to him to return it when next he brings a delivery. Unfortunately this flash drive had protected files of total amount of PPE's bought from Globus in 2022, total number of employees, salaries from January to August 2023, and their contracts with the company, and business negotiations made with clients relatives. Making matters worse, a pdf file named 'UQC_CODES' contained all passwords regarding the afore mentioned files and the company's bank account details. Since she had these files in the companies google drive account and had personal relationship with the delivery representative, it wasn't a major concern for her.

When he returned to the office the next time he brought consignments, he requested to use one of the computers at the office for a short while to assess the internet and check on a project Globus is about embarking. Due to the relationship existing between UQC and Globus, he was granted this opportunity. Since he now has access to almost all the passwords related to the company, he created a dummy cooperate email and forwarded previous transactions made to Globus, employees list and scanned bank cheques and receipts. Upon studying transaction history of and direct debits made, he went through the transaction history of UQC and succeeded in making a request worth about €2,500 to Globus in the name of the company with the accountant's cooperate email after accessing her cooperate password from the word document and made a bank transfer from the company's account through with the password. Unfortunately she does not use multi-factor authentication. Since he is in charge of deliveries to UQC, he got those items and sold to a different group at a cheaper price which later made the secretary lose her job and had to pay for the losses.

In section 5, subsection 5.2.1 of the company's handbook as stated in section 1.1 of this document above, it states that No external devices or equipment should be attached to our computers or computer equipment without the prior approval of management – if you are permitted to use a memory stick this should be password protected (Unique Quality Care Ltd., 2023, pp. 22-24). This was a breach of information security systems stated in the employee handbook that caused the company a substantial amount to a third party agent from Globus.

1.2.2 Scenario 2

An employee who was an operations officer and a personal assistant to the general manager resigned when he had to further his education at the masters level. During his days at UQC, he took charge of all meetings scheduled for the manager, rota implementation for employees using backend of the birdie app, and errands regarding transactions on behalf of the company, meeting relatives of clients for negotiations and meetings with the birdie company in charge of the mobile application.

When he was about leaving, he deliberately kept login details to all software systems, previous rotas schedules, and made copies of all transactions made during her time as an employee. With an intention of foreseeing workflow at the office in real time, he installed Anydesk (a remote desktop software for collaborative work, copied the auto generated ID, login and password of the software to help him access all resource at the comfort of his home. After opening the password protected files he sent out copies of all resources to a friend who wants to start a care company with a dummy cooperate email created with the managers cooperate account since he knows her login details.

In section 5, subsection 5.2.3 of the company's handbook as stated in section 1.1 of this study above, it states emphatically that, passwords are confidential and must not be given to another person without prior permission from management. If you are preparing to leave your position with this Company for any reason (for example because you have resigned), you must make any passwords used in the course of your employment known to a manager (Unique Quality Care Ltd., 2023, pp. 22-24).

In view of this scenario, the employee deliberately went contrary to the password policy after resigning from the company which is a breach of the information security policy stated within the employee handbook which was made available to him before the commencement of his contract with the company.

1.2.3 Measures To Minimise Related Issues From Occurring

It is required of every organization to put measures in place that can help minimise the vulnerabilities and attacks of a system (Campbell *et al.*, 2006). These policies ensure the safety of the system and the users who are major stakeholders of the entire organization. The following measures can be factored into the password protection policy to reduce the aforementioned scenarios from occurring:

- 1) **Saving sensitive files in organisation's cloud storage rather than portable devices:** In scenario one for instance, if the file was saved onto a cloud based platform rather than the flash drive, the secretary would have saved herself from the company's cooperate password being exposed to Globus delivery representative.
- 2) **Establishing password guidance for service users:** UQC must educate employees on usage of passwords across platforms such as social media. Many people for the sake of forgetfulness tend to use same passwords across almost all platforms they may sign up to. Employees must be educated on bad password practices such as simple phrases like 'mynameisamuel', 'icareaboutyou' and the likes (AlFayyadh *et al.*, 2011).
- 3) **Prohibition of common and easier phrasal passwords:** implementation of uppercase, numeric, and special characters can be a requirement to minimise passwords being compromised easily.
- 4) **Implementing ex-employee password surveillance in scope of work:** In scenario 2 for instance, if password of ex-employee was deleted from the system, he would not have gotten access to the companies sensitive data which can put the company's integrity at stake. It is therefore an essential part for UQC to back up and delete sensitive details such as passwords of former employees and also restrict access to companies digital resources
- 5) **Educating employees to keep company's password private and secured:** employees often give out cooperate passwords to fellow employees, friends, or relatives they trust in order to access certain resources at odd times. This can sometimes be compromised without the third parties notice. It is be difficult to retrieve sometimes as a result of the impact involved.

1.2.4 Defensive Measure To Block Unauthorised Access

Defensive measures to curb issues of this sort requires comprehensive effort and guidelines that should be a priority to every organization. Below are some measures that can block unauthorised access within UQC's working environment.

- **Adapting to an Endpoint Security Strategy:** this encompasses each user's device such as mobile devices and computers and other devices connected on a network to prevent unauthorised access.

Packet-filtering firewall can be used to assess inflow and outflow packets such as IP addresses and port numbers which conforms to the network layer of the OSI model (a structural framework used to elaborate the activities of a network system). It is simple to implement, has less impact on network activity and less costly to undertake.

The Next-Generation Antivirus (NGAV) software which is an endpoint security system can easily detect third party intrusions and could have detected the ex-employee's access to the company's resources.

- **Monitoring users activities and scope of work:** this is an important strategy to prevent intrusion. monitoring unusual activities within a system is a good way of noticing abnormalities that has occurred (Bhuyan *et al.*, 2022). If structures were put in place at the office for instance, when the flash drive was inserted, the system would have notified the administrator at the end point of the network. On the birdie application for instance, if a carer enters a drug which is not part of the administered drug to that client, the system should notify management of an abnormality unless it is an drug added unto the system by management. If a carer's password is entered more than 5 times, the application should log him or her out, unless password is changed by the carer via email recovery password procedure.
- **Establishing a multi-Factor Authentication for devices:** the company must establish a twofactor or multifactor authentication for employees through authentication platforms such as google authenticator (Feruza & Kim, 2007). Employees will need to authorise login through this process if activity is paused for about 30 minutes. This will help employees and management minimise attacks by third parties.
- **Use of strong password and file encryption:** establishing passwords with combination of special characters, numbers and encrypting files sent through emails and saved in the cloud minimises risk of an attack.

2.0 Digital Forensics

Digital forensic is the process used by legal professionals to identify, gather and investigate reports obtained from electronic data (Irons *et al.*, 2014). It is mostly used within investigative departments such as cyber security units, law court, banking sector and the likes. With the help of specialised forensic tools such as Wireshark, Volatility, Autopsy and the likes, these investigations are carried out with results that goes a long way to mitigate societal issues and improve human activities.

2.1 Winhex Forensic Investigation

Winhex is a forensic inspection tool used for data recovery, advance file editing and password recoveries (Casey, 2004). This tool will be used recover files from computer and results the results will be shown in snapshots as shown in the figures below:

a) Recovered deleted files:

To begin with, a dump file will be create with the help of the task manager as shown in figure 1

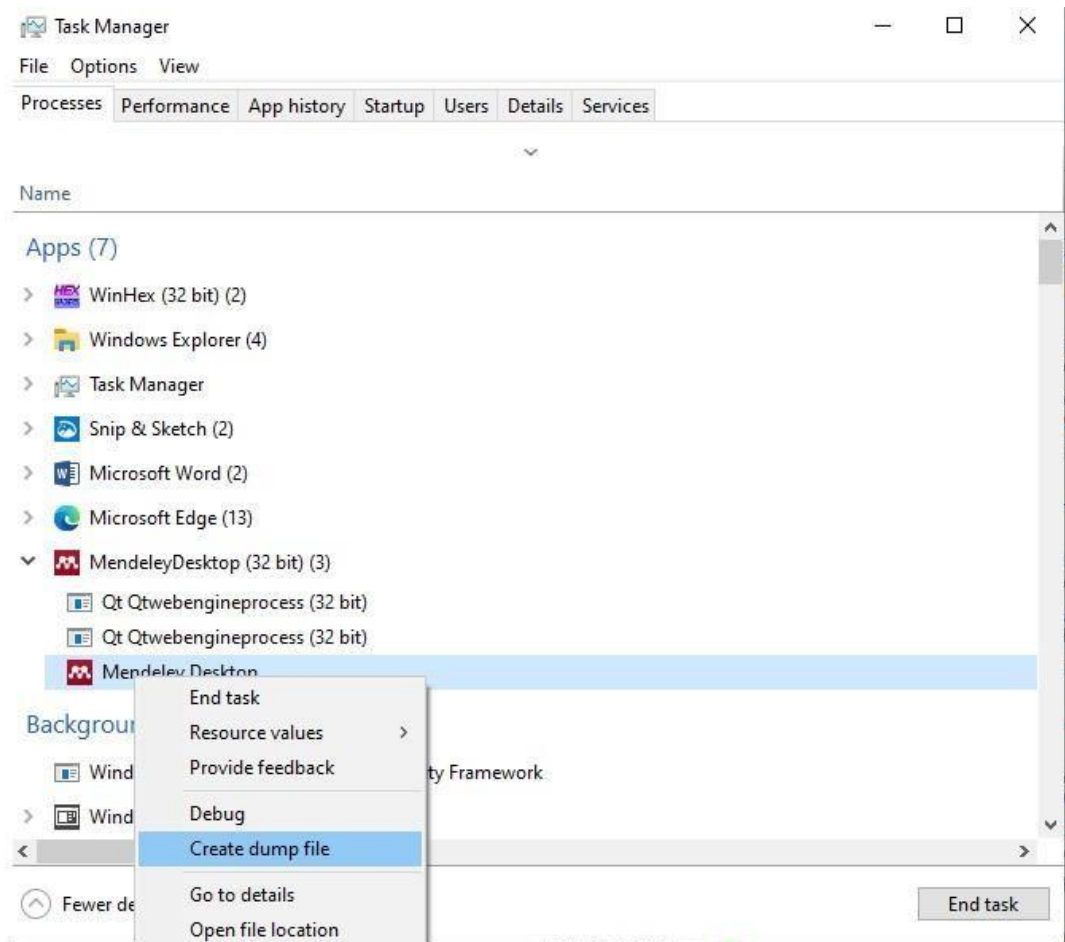


Figure 1: Creating dump file

Also, the file path of the dump file will be located as shown in figure 2. In order not to forget the path, user can create a folder on desktop or choose any appropriate location for the file.

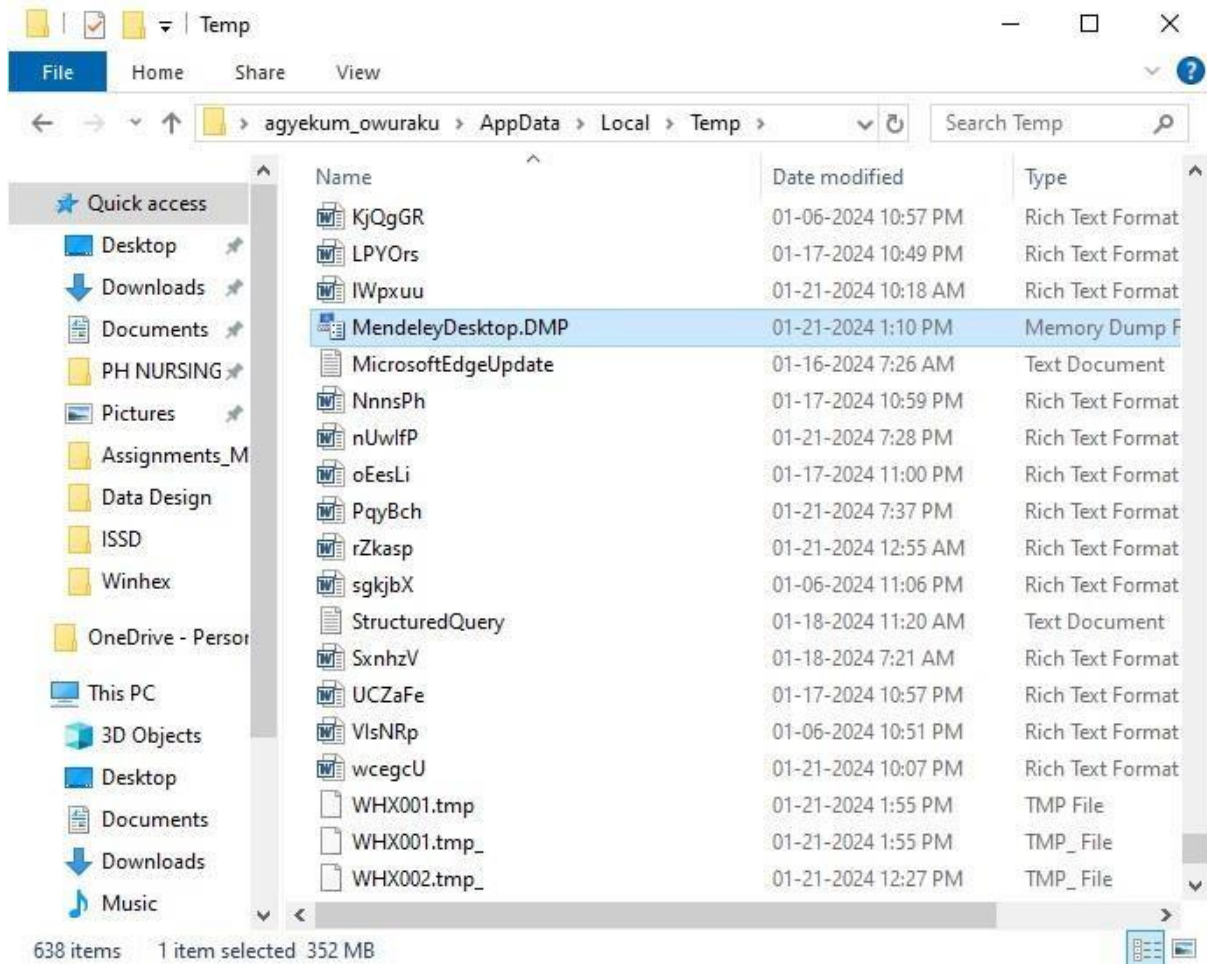


Figure 2: Locate the dump file

Again, by installing winhex via web browser, launch winhex application and open the dump file as shown in figure 3 and 4.

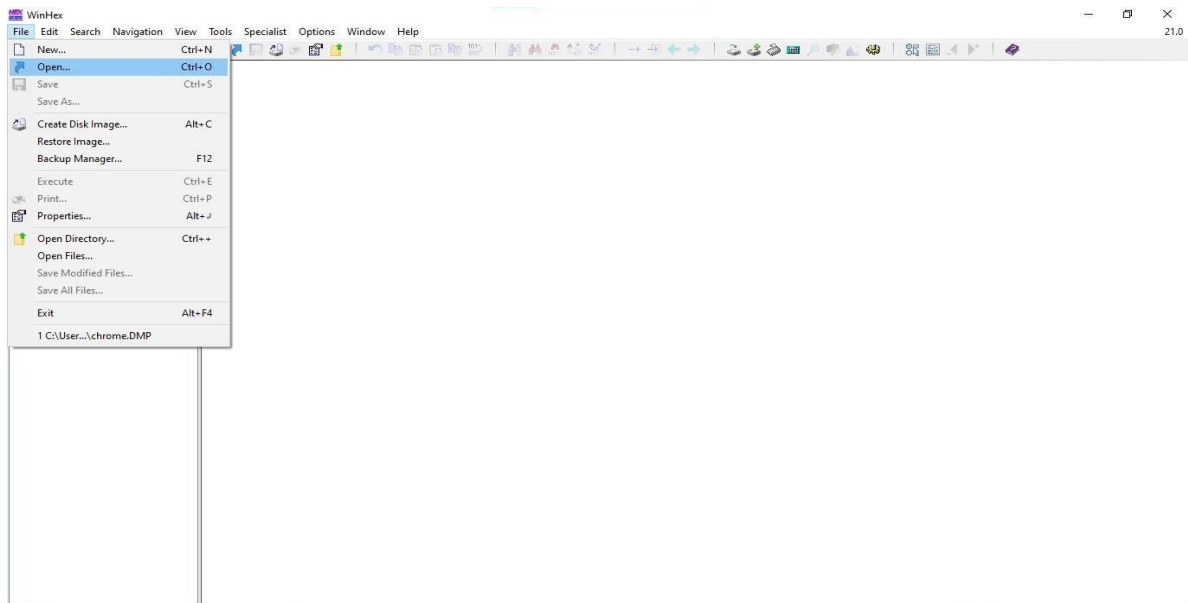


Figure 3: Click open to locate file via winhex

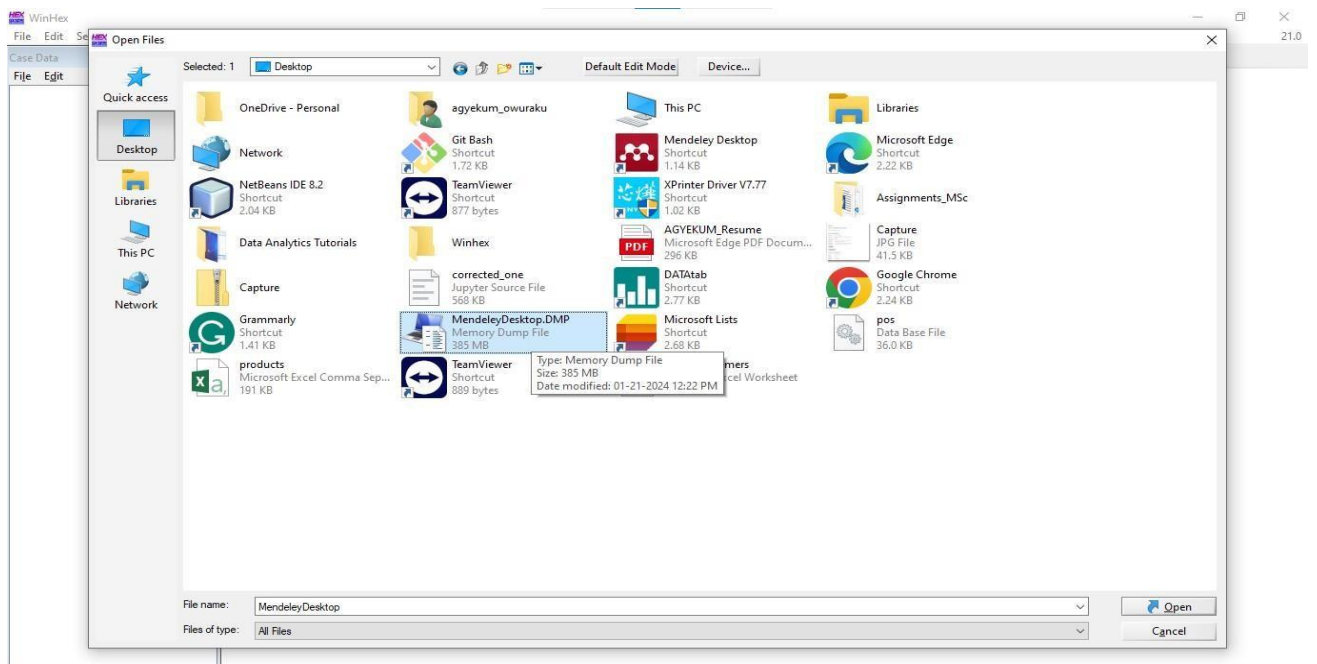
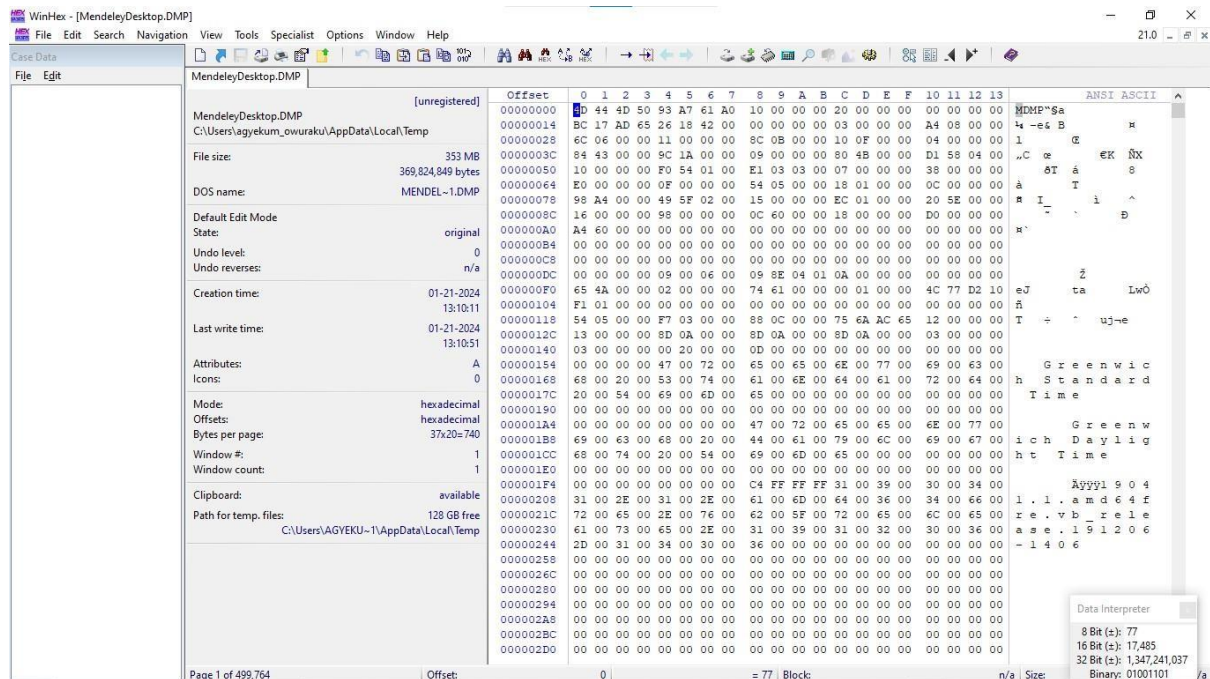


Figure 4: Open located file via winhex

At this stage, open the dump file to display the offset and data within the dump file where offset represents the number of bytes at the entry point of the string as shown in figure 5.



The screenshot shows the WinHex application window titled 'WinHex - [MendeleyDesktop.DMP]'. The left pane displays file metadata for 'MendeleyDesktop.DMP' (unregistered), including file size (353 MB), DOS name (MENDEL-1.DMP), and creation/last write times. The main pane shows a hex dump with columns for offset (0 to 13) and data. The right pane shows the ASCII interpretation of the data, which includes the string 'Mendeley Desktop' and other text. A 'Data Interpreter' window is open at the bottom right, showing the binary data in a structured format.

Figure 5: Dump file data

Furthermore, click on disk tools and open file recovery by type to select the types of files to be recovered.

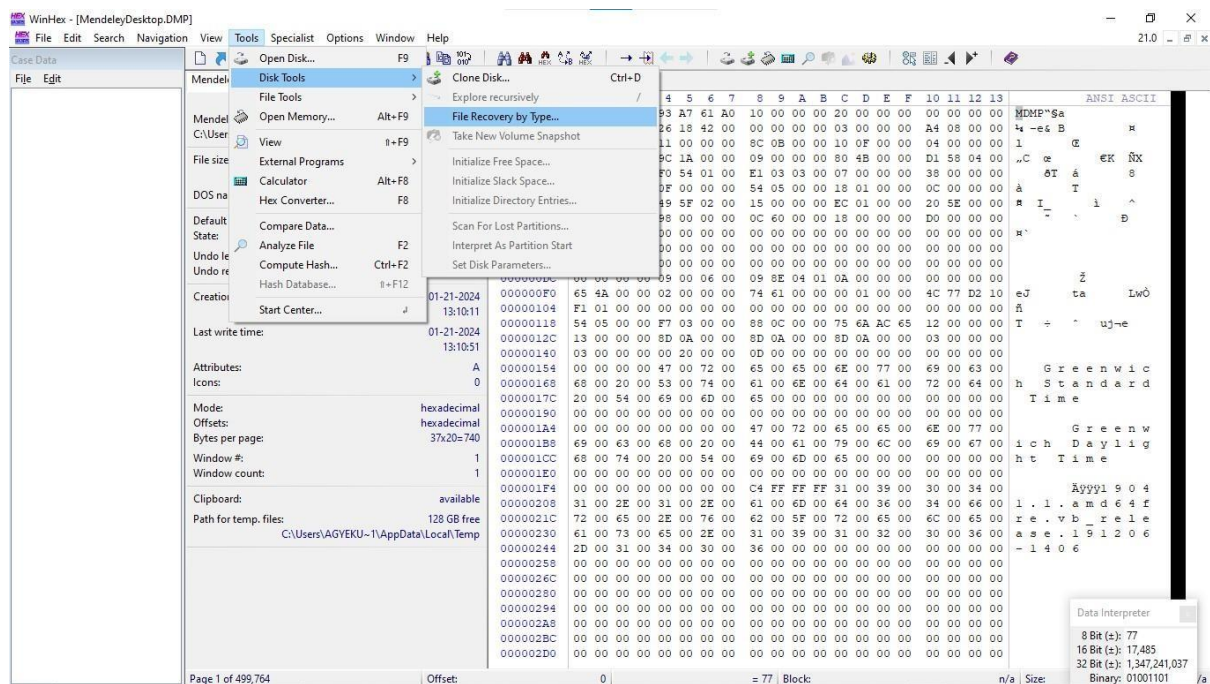


Figure 6: File recovery type option

Select the type of files. In this investigation, documents, emails, and internet files is selected shown in figure 7 and has been recovered successfully as shown in figure 8 and 9 which shows a recovery by header and a complete recovery respectively .

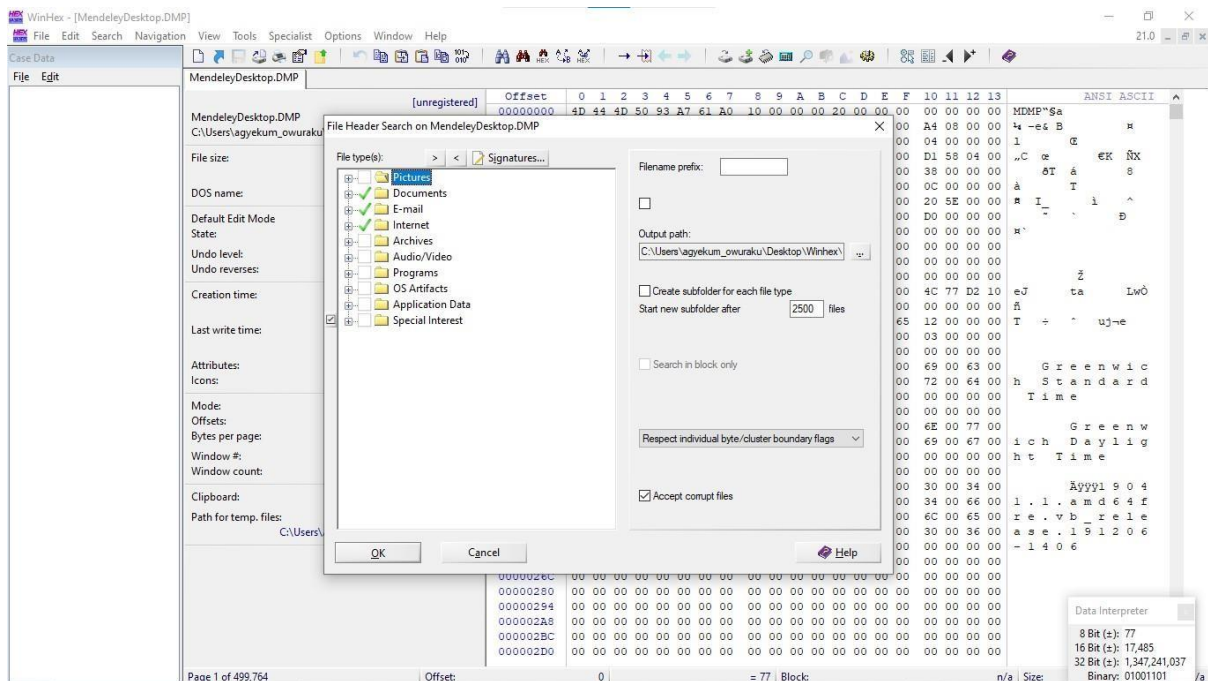


Figure 7: Selection of file type to be recovered

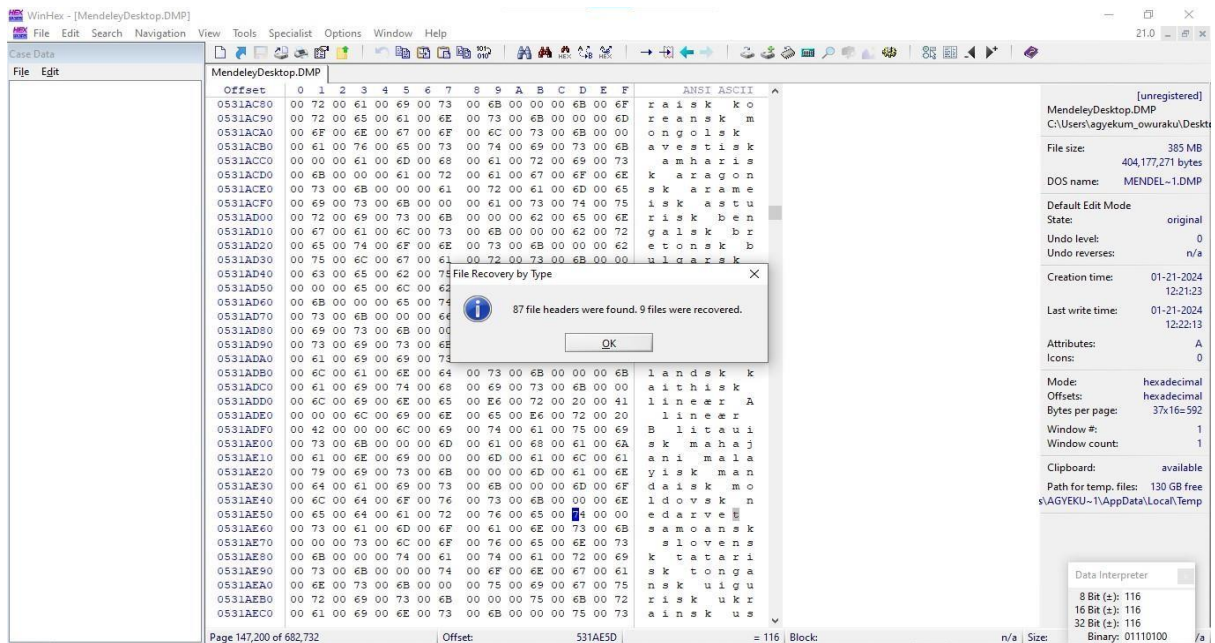


Figure 8: Recovery by header

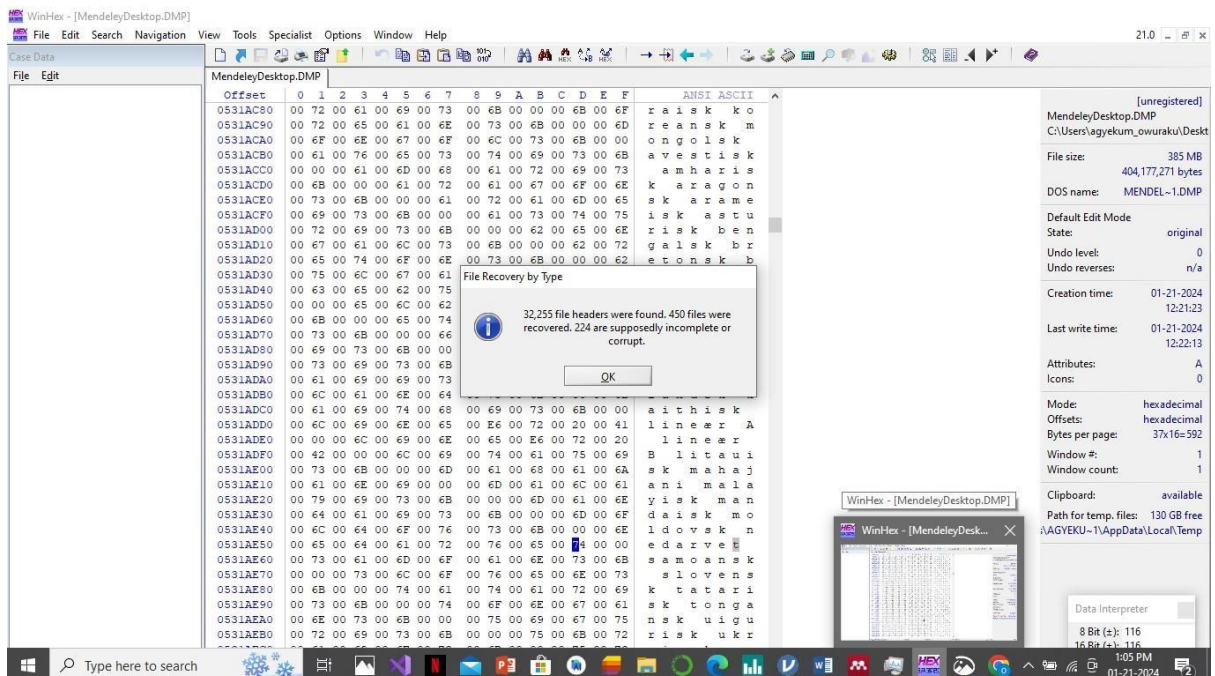


Figure 9: Complete file recovery

Finally the files are recovered in the winhex folder created at the start of the investigation

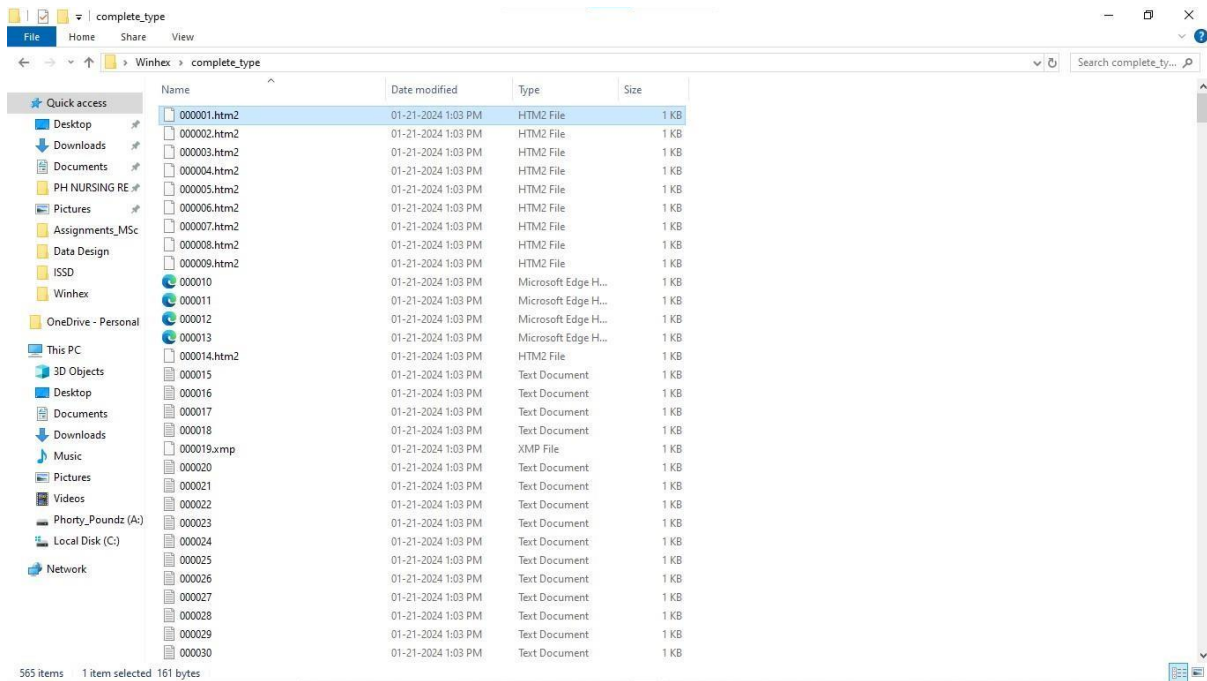


Figure 10: Recovered files in Winhex folder

b) Recovered password:

After recovering deleted files the next is recovering password which will be achieved with the simultaneous search button and passing the 'pass=' function as shown in figure 11 to recover password.

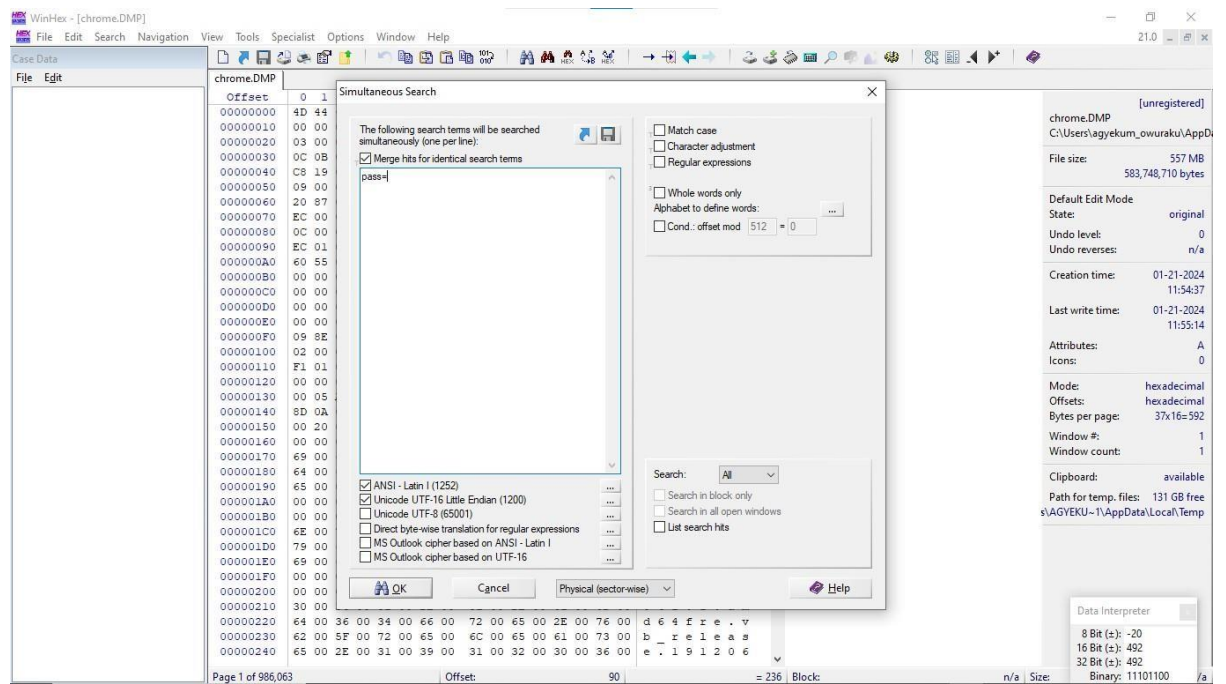
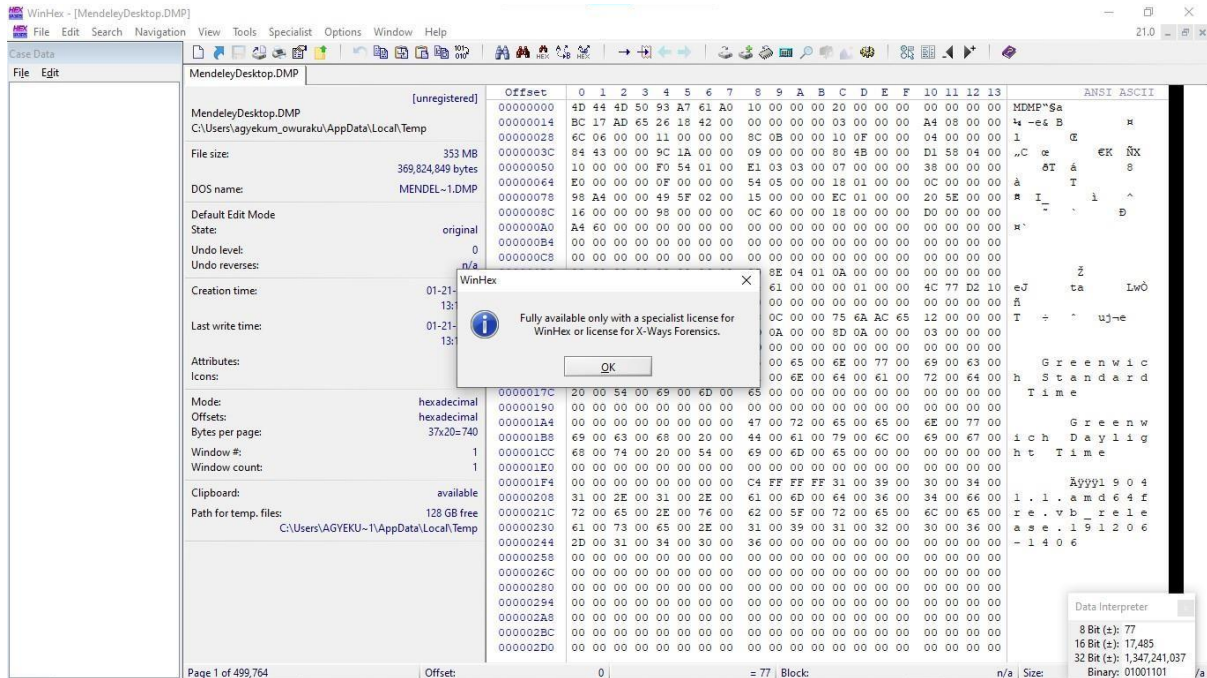


Figure 11: Simultaneous search button to recover password

In order to recover password, a winhex specialist license is needed to achieve this goal due to security permissions. After obtaining the licence, the same procedure will is used.



3.0 Conclusion

It is the core duty of every organisation to lay out proper structures to mitigate intrusion from thirdparties. Although some occurrences are not deliberate, measures are needed to factor these occurrences which serves as a wakeup call to employees and organisations at large.

References

AlFayyadh, B., (2011). Improving Usability of Password Management with Standardized Password Policies. *Queensland University of Technology. Australia.*

Available from: https://sarssi2012.greyc.fr/wp-content/uploads/SAR-SSI-2012_p3845_AlFayyadh.pdf
[Accessed: 22 January 2024].

Bhuyan, F. A., Lu, S., Reynolds, R., Zhang, J. and Ahmed, I., (2022). A Security Framework for Scientific Workflow Provenance Access Control Policies. *IEEE Transactions on Services Computing*, 15(1), pp. 97-109.

Campbell, J., Kleeman, D. and Ma, W., (2006). Password composition policy: Does enforcement lead to better Password Choices?. *In: ACIS 2006 Proceedings - 17th Australasian Conference on Information Systems*. Adelaide: Australia, Available from: <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1064&context=acis2006> [Accessed: 22 January 2024].

Casey, E., (2004). Tool review—WinHex. *Digital Investigation* [online], 1, pp. 114-128.

Feruzi, S. and Kim, P. T., (2007). IT Security Review: Privacy, Protection, Access Control, Assurance and System Security. *International Journal of Multimedia and Ubiquitous Engineering* [online], 2(2), pp.17-32.

Irons, A. and Lallie, H., (2014). Digital Forensics to Intelligent Forensics. *Future Internet* [online], 6(3), pp. 584–596.

Shay, R., Komanduri, S., Durity, A., Huh, P., Mazurek, M., Segreti, S., Ur, B., Bauer, L., Christin, N. and Cranor, L., (2016). Designing password policies for strength and usability. *ACM Transactions on Information and System Security* [online], 18(4). pp. 1-34.

Unique Quality Care Ltd., (2023). *Employee handbook*. Cuffley: Unique Quality Care Ltd.