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 ncludes 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 3

1.2 Scenarios Associated With Corporate Passwords Being Compromised 4

1.2.1 Scenario 1 4

1.2.2 Scenario 2 6

1.2.3 Measures To Minimise Related Issues From Occurring 6

1.2.4 Defensive Measure To Block Unauthorised Access 7

2.0 Digital Forensics 9

2.1 Winhex Forensic Investigation 9

3.0 Conclusion 19

References 19

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 ABC Homecare Ltd. [anonymised] (ABC) 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.

ABC Homecare Ltd. (anonymised) 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 (ABC Homecare Ltd.). 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 ABC. 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 ABC 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 'ABC_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 ABC 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 ABC 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 ABC, 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 (ABC Homecare Ltd.). 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 ABC, 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 (ABC Homecare Ltd.).

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**: ABC 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 ABC 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 ABC'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 conform 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

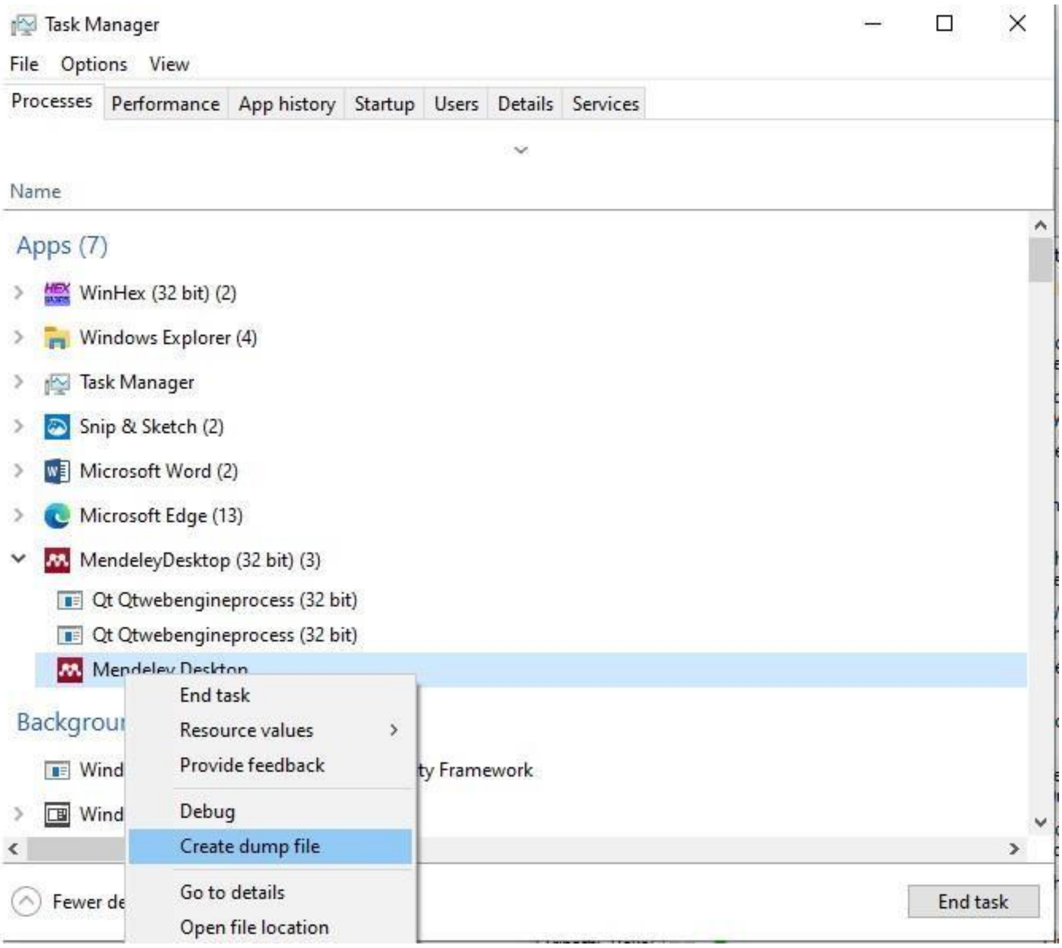
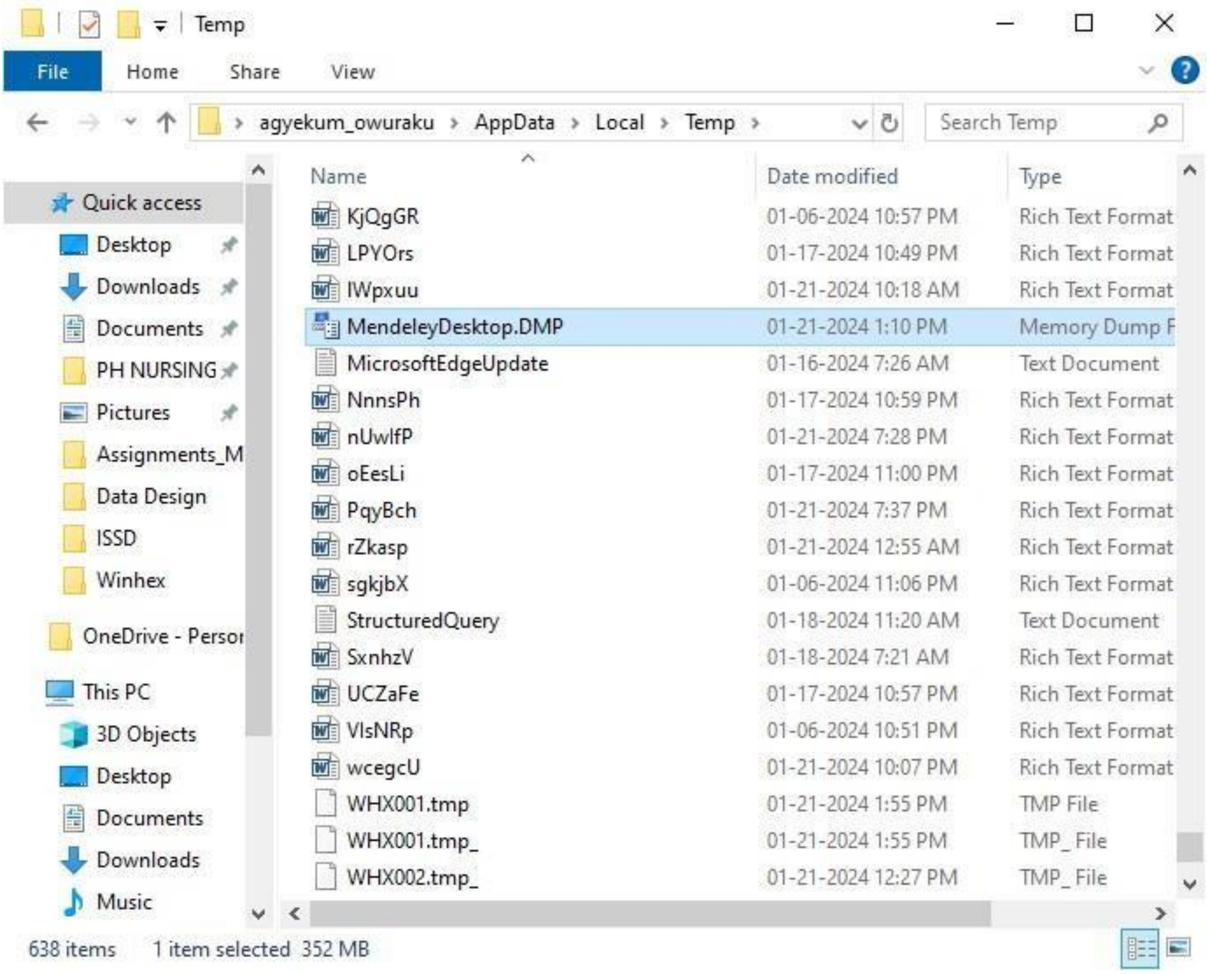


Figure 1: Creating dump file

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.



Name	Date modified	Type
KjQgGR	01-06-2024 10:57 PM	Rich Text Format
LPYOrs	01-17-2024 10:49 PM	Rich Text Format
IWpxuu	01-21-2024 10:18 AM	Rich Text Format
MendeleyDesktop.DMP	01-21-2024 1:10 PM	Memory Dump F
MicrosoftEdgeUpdate	01-16-2024 7:26 AM	Text Document
NnnsPh	01-17-2024 10:59 PM	Rich Text Format
nUwlfP	01-21-2024 7:28 PM	Rich Text Format
oEesLi	01-17-2024 11:00 PM	Rich Text Format
PqyBch	01-21-2024 7:37 PM	Rich Text Format
rZkasp	01-21-2024 12:55 AM	Rich Text Format
sgkjbX	01-06-2024 11:06 PM	Rich Text Format
StructuredQuery	01-18-2024 11:20 AM	Text Document
SxnhzV	01-18-2024 7:21 AM	Rich Text Format
UCZaFe	01-17-2024 10:57 PM	Rich Text Format
VlsNRp	01-06-2024 10:51 PM	Rich Text Format
wcegcU	01-21-2024 10:07 PM	Rich Text Format
WHX001.tmp	01-21-2024 1:55 PM	TMP File
WHX001.tmp_	01-21-2024 1:55 PM	TMP_ File
WHX002.tmp_	01-21-2024 12:27 PM	TMP_ File

638 items   1 item selected 352 MB

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.

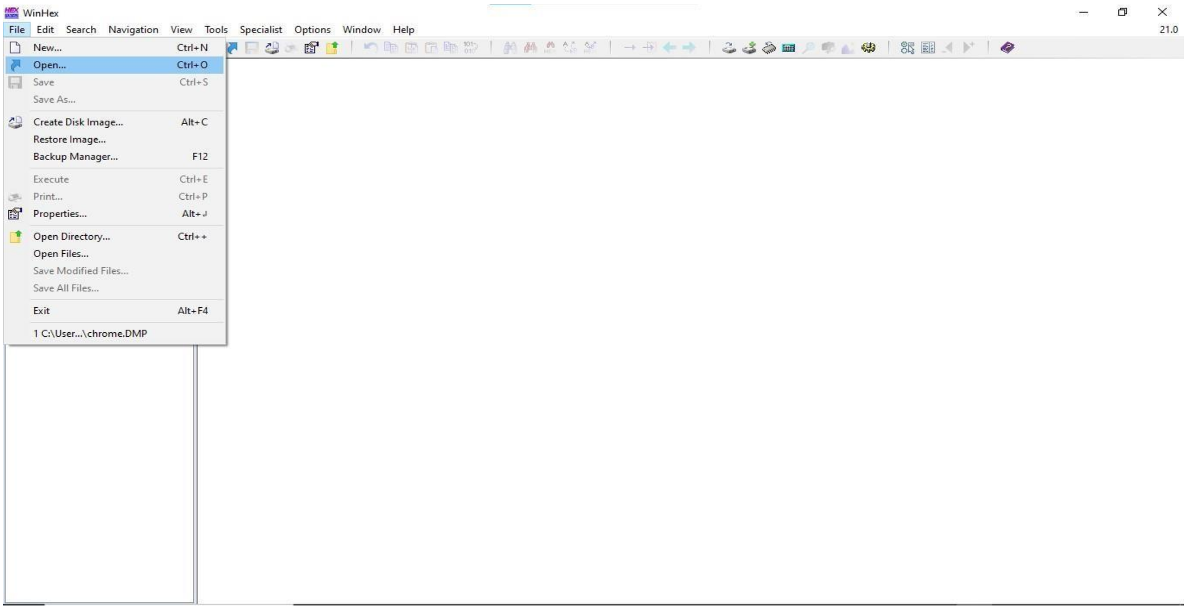
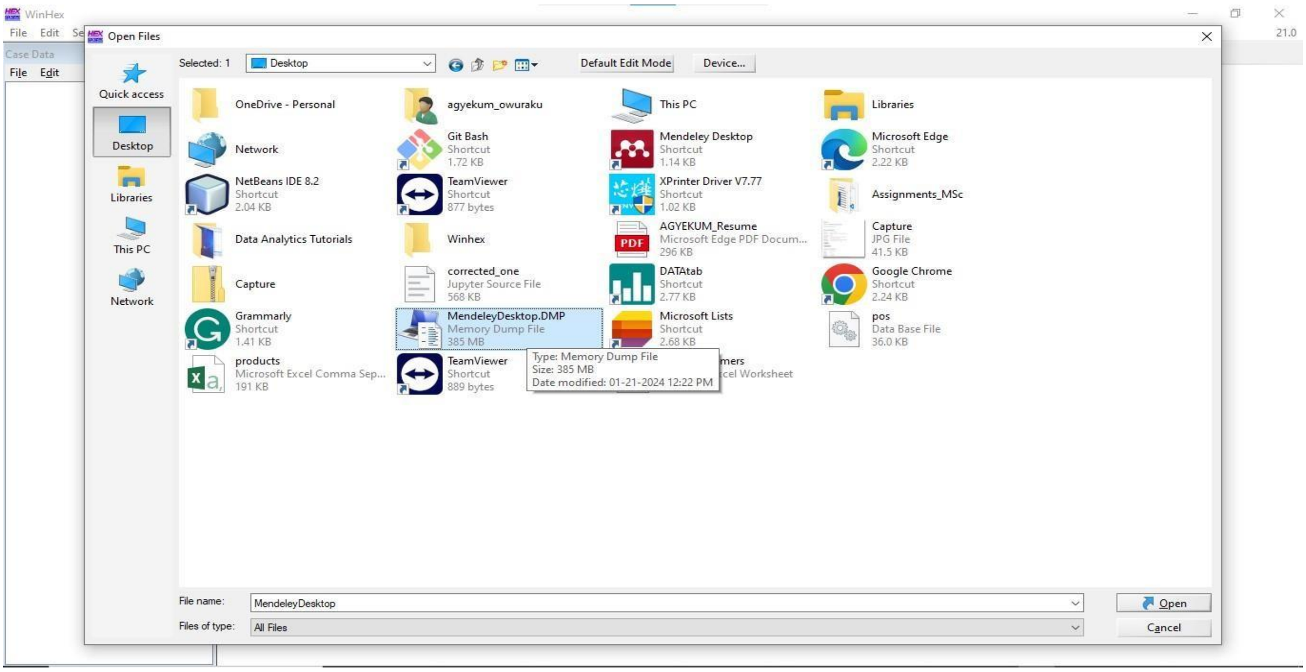


Figure 3: Click open to locate file via winhex


WinHex
File Edit Se
Case Data
File Edit
Open Files
Quick access
Desktop
Libraries
This PC
Network
Default Edit Mode
Device...
OneDrive - Personal
agyekum_owuraku
This PC
Libraries
Network
Git Bash Shortcut 1.72 KB
Mendeley Desktop Shortcut 1.14 KB
Microsoft Edge Shortcut 2.22 KB
NetBeans IDE 8.2 Shortcut 2.04 KB
TeamViewer Shortcut 877 bytes
XPrinter Driver V7.77 Shortcut 1.02 KB
Assignments_MSc
Data Analytics Tutorials
Winhex
AGYEKUM_Resume Microsoft Edge PDF Docum... 296 KB
Capture JPG File 41.5 KB
Capture
corrected_one Jupyter Source File 568 KB
DATAtab Shortcut 2.77 KB
Google Chrome Shortcut 2.24 KB
Grammarly Shortcut 1.41 KB
MendeleyDesktop.DMP Memory Dump File 385 MB
Microsoft Lists Shortcut 2.68 KB
pos Data Base File 36.0 KB
products Microsoft Excel Comma Sep... 191 KB
TeamViewer Shortcut 889 bytes
mers
cel Worksheet
Open
Cancel
21.0

Selected: 1 Desktop

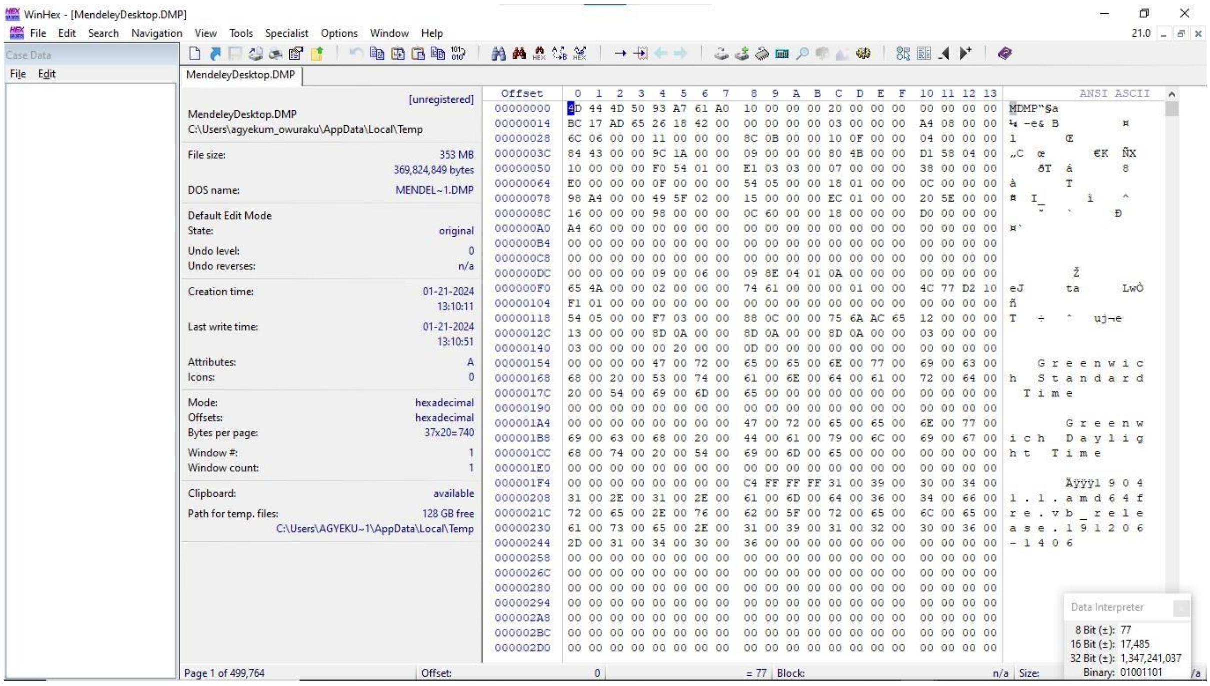
Type: Memory Dump File
Size: 385 MB
Date modified: 01-21-2024 12:22 PM

File name: MendeleyDesktop

Files of type: All Files

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.


WinHex - [MendeleyDesktop.DMP]
File Edit Search Navigation View Tools Specialist Options Window Help
21.0
Case Data
File Edit
MendeleyDesktop.DMP

[unregistered]
MendeleyDesktop.DMP
C:\Users\agyekum_owuraku\AppData\Local\Temp

File size: 353 MB
369,824,849 bytes
DOS name: MENDEL~1.DMP

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 01-21-2024 13:10:11
Last write time: 01-21-2024 13:10:51
Attributes: A
Icons: 0

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 37x20=740
Window #: 1
Window count: 1

Clipboard: available
Path for temp. files: 128 GB free
C:\Users\AGYEKU~1\AppData\Local\Temp

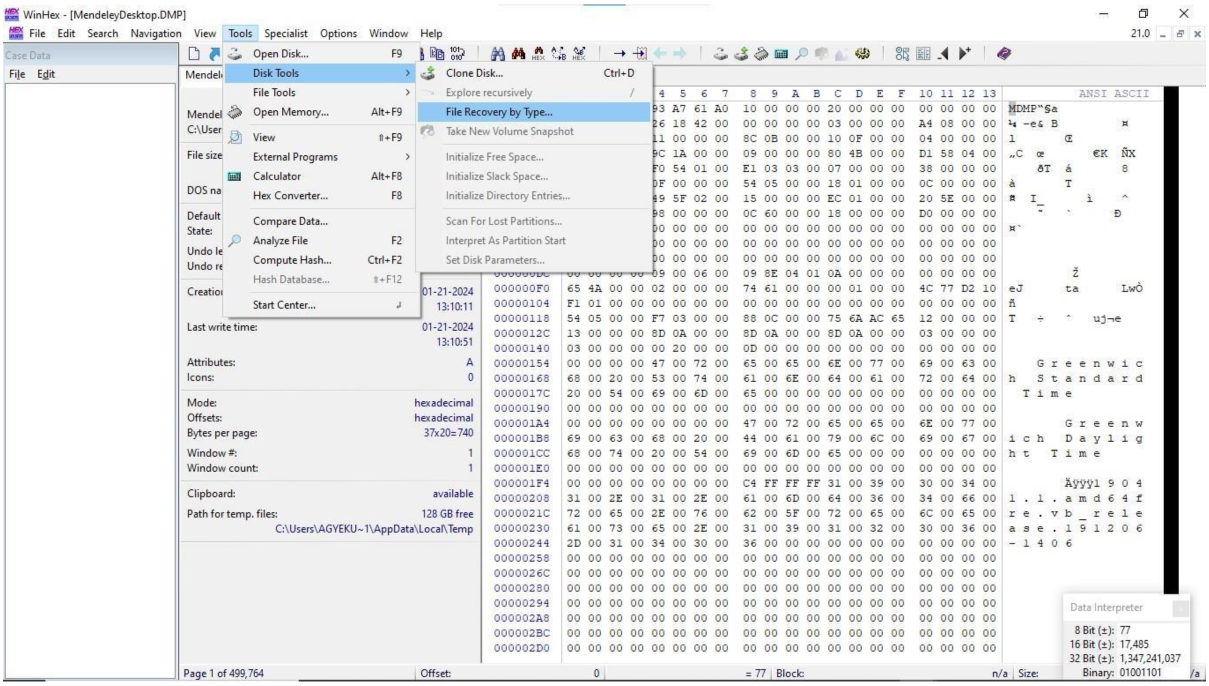
```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13         ANSI ASCII
00000000   4D 44 4D 50 93 A7 61 A0  10 00 00 00 20 00 00 00  00 00 00 00   MDMP"§a
00000014   BC 17 AD 65 26 18 42 00  00 00 00 00 03 00 00 00  A4 08 00 00   ¼ -e& B          ¤
00000028   6C 06 00 00 11 00 00 00  8C 0B 00 00 10 0F 00 00  04 00 00 00   l       Œ
0000003C   84 43 00 00 9C 1A 00 00  09 00 00 00 80 4B 00 00  D1 58 04 00   „C  œ       €K  ÑX
00000050   10 00 00 00 F0 54 01 00  E1 03 03 00 07 00 00 00  38 00 00 00       ðT  á       8
00000064   E0 00 00 00 0F 00 00 00  54 05 00 00 18 01 00 00  0C 00 00 00   à       T
00000078   98 A4 00 00 49 5F 02 00  15 00 00 00 EC 01 00 00  20 5E 00 00   ˜¤  I_      ì    ^
0000008C   16 00 00 00 98 00 00 00  0C 60 00 00 18 00 00 00  D0 00 00 00       ˜    `      Ð
000000A0   A4 60 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00   ¤`
000000B4   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000000C8   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000000DC   00 00 00 00 09 00 06 00  09 8E 04 01 0A 00 00 00  00 00 00 00            Ž
000000F0   65 4A 00 00 02 00 00 00  74 61 00 00 00 01 00 00  4C 77 D2 10   eJ      ta      LwÒ
00000104   F1 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00   ñ
00000118   54 05 00 00 F7 03 00 00  88 0C 00 00 75 6A AC 65  12 00 00 00   T   ÷   ˆ   uj¬e
0000012C   13 00 00 00 8D 0A 00 00  8D 0A 00 00 8D 0A 00 00  03 00 00 00
00000140   03 00 00 00 00 20 00 00  0D 00 00 00 00 00 00 00  00 00 00 00
00000154   00 00 00 00 47 00 72 00  65 00 65 00 6E 00 77 00  69 00 63 00       G r e e n w i c
00000168   68 00 20 00 53 00 74 00  61 00 6E 00 64 00 61 00  72 00 64 00   h   S t a n d a r d
0000017C   20 00 54 00 69 00 6D 00  65 00 00 00 00 00 00 00  00 00 00 00     T i m e
00000190   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000001A4   00 00 00 00 00 00 00 00  47 00 72 00 65 00 65 00  6E 00 77 00           G r e e n w
000001B8   69 00 63 00 68 00 20 00  44 00 61 00 79 00 6C 00  69 00 67 00   i c h   D a y l i g
000001CC   68 00 74 00 20 00 54 00  69 00 6D 00 65 00 00 00  00 00 00 00   h t   T i m e
000001E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000001F4   00 00 00 00 00 00 00 00  C4 FF FF FF 31 00 39 00  30 00 34 00           Äÿÿÿ1 9 0 4
00000208   31 00 2E 00 31 00 2E 00  61 00 6D 00 64 00 36 00  34 00 66 00   1 . 1 . a m d 6 4 f
0000021C   72 00 65 00 2E 00 76 00  62 00 5F 00 72 00 65 00  6C 00 65 00   r e . v b _ r e l e
00000230   61 00 73 00 65 00 2E 00  31 00 39 00 31 00 32 00  30 00 36 00   a s e . 1 9 1 2 0 6
00000244   2D 00 31 00 34 00 30 00  36 00 00 00 00 00 00 00  00 00 00 00   - 1 4 0 6
00000258   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
0000026C   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
00000280   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
00000294   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002A8   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002BC   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
```

Data Interpreter
8 Bit (±): 77
16 Bit (±): 17,485
32 Bit (±): 1,347,241,037
Binary: 01001101

Page 1 of 499,764 | Offset: 0 | = 77 | Block: n/a | Size:

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.



Creation time: 01-21-2024 13:10:11
Last write time: 01-21-2024 13:10:51
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 37x20=740
Window #: 1
Window count: 1
Clipboard: available
Path for temp. files: 128 GB free
C:\Users\AGYEKU~1\AppData\Local\Temp

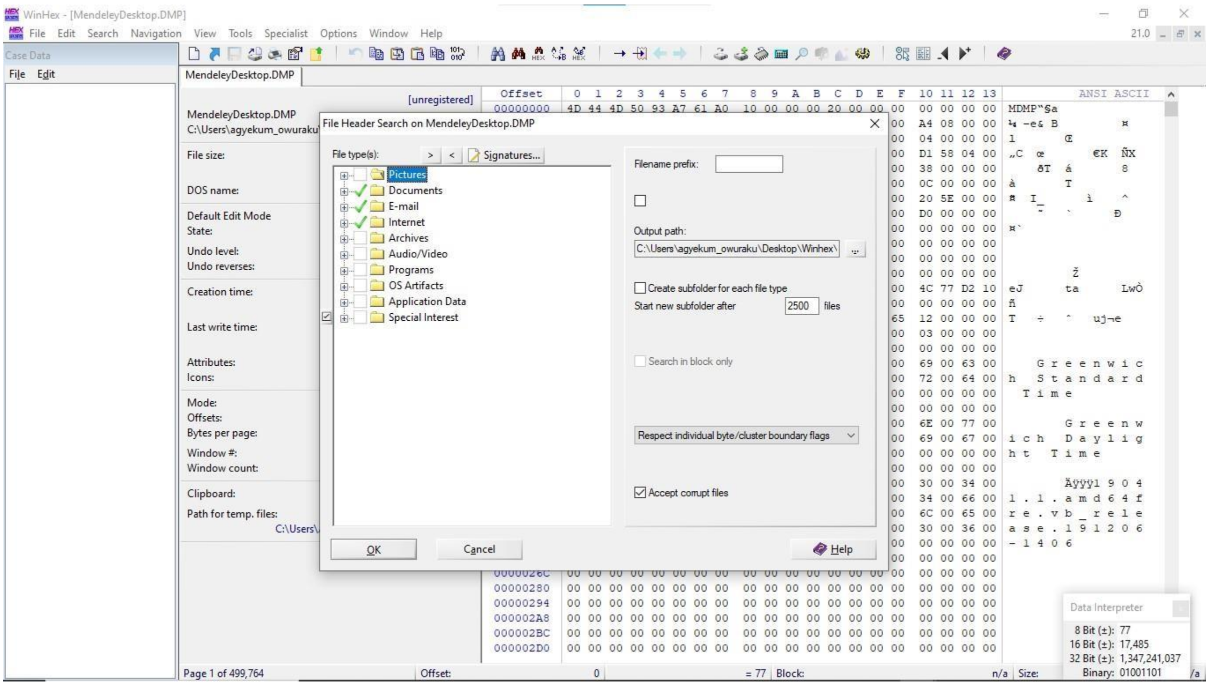
```
000000F0  65 4A 00 00 02 00 00 00  74 61 00 00 00 01 00 00  4C 77 D2 10  eJ      ta      LwÒ
00000104  F1 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00  ñ
00000118  54 05 00 00 F7 03 00 00  88 0C 00 00 75 6A AC 65  12 00 00 00  T  ÷   ˆ  uj¬e
0000012C  13 00 00 00 8D 0A 00 00  8D 0A 00 00 8D 0A 00 00  03 00 00 00
00000140  03 00 00 00 00 20 00 00  0D 00 00 00 00 00 00 00  00 00 00 00
00000154  00 00 00 00 47 00 72 00  65 00 65 00 6E 00 77 00  69 00 63 00      G r e e n w i c
00000168  68 00 20 00 53 00 74 00  61 00 6E 00 64 00 61 00  72 00 64 00  h   S t a n d a r d
0000017C  20 00 54 00 69 00 6D 00  65 00 00 00 00 00 00 00  00 00 00 00    T i m e
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000001A4  00 00 00 00 00 00 00 00  47 00 72 00 65 00 65 00  6E 00 77 00          G r e e n w
000001B8  69 00 63 00 68 00 20 00  44 00 61 00 79 00 6C 00  69 00 67 00  i c h   D a y l i g
000001CC  68 00 74 00 20 00 54 00  69 00 6D 00 65 00 00 00  00 00 00 00  h t   T i m e
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000001F4  00 00 00 00 00 00 00 00  C4 FF FF FF 31 00 39 00  30 00 34 00          Äÿÿÿ1 9 0 4
00000208  31 00 2E 00 31 00 2E 00  61 00 6D 00 64 00 36 00  34 00 66 00  1 . 1 . a m d 6 4 f
0000021C  72 00 65 00 2E 00 76 00  62 00 5F 00 72 00 65 00  6C 00 65 00  r e . v b _ r e l e
00000230  61 00 73 00 65 00 2E 00  31 00 39 00 31 00 32 00  30 00 36 00  a s e . 1 9 1 2 0 6
00000244  2D 00 31 00 34 00 30 00  36 00 00 00 00 00 00 00  00 00 00 00  - 1 4 0 6
00000258  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
0000026C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
00000280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
00000294  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002A8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002BC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
```

8 Bit (±): 77
16 Bit (±): 17,485
32 Bit (±): 1,347,241,037
Binary: 01001101

Page 1 of 499,764 | Offset: 0 | = 77 | Block: n/a | Size:

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 .



File Header Search on MendeleyDesktop.DMP

File type(s):

- □ Pictures
- ✓ Documents
- ✓ E-mail
- ✓ Internet
- □ Archives
- □ Audio/Video
- □ Programs
- □ OS Artifacts
- □ Application Data
- □ Special Interest

Filename prefix:

□

Output path: C:\Users\agyekum_owuraku\Desktop\Winhex\

□ Create subfolder for each file type

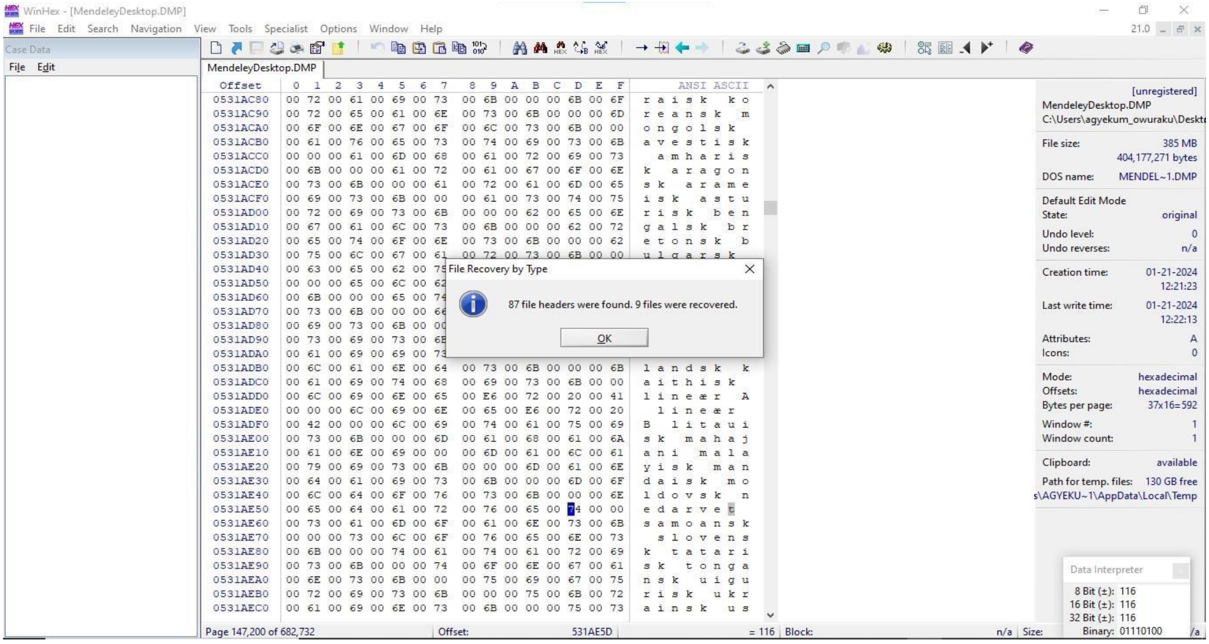
Start new subfolder after 2500 files

□ Search in block only

Respect individual byte/cluster boundary flags

☑ Accept corrupt files

Figure 7: Selection of file type to be recovered


WinHex - [MendeleyDesktop.DMP]
File Edit Search Navigation View Tools Specialist Options Window Help
21.0
Case Data
File Edit
MendeleyDesktop.DMP

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
0531AC80  00 72 00 61 00 69 00 73  00 6B 00 00 00 6B 00 6F   r a i s k   k o
0531AC90  00 72 00 65 00 61 00 6E  00 73 00 6B 00 00 00 6D   r e a n s k   m
0531ACA0  00 6F 00 6E 00 67 00 6F  00 6C 00 73 00 6B 00 00   o n g o l s k
0531ACB0  00 61 00 76 00 65 00 73  00 74 00 69 00 73 00 6B   a v e s t i s k
0531ACC0  00 00 00 61 00 6D 00 68  00 61 00 72 00 69 00 73     a m h a r i s
0531ACD0  00 6B 00 00 00 61 00 72  00 61 00 67 00 6F 00 6E   k   a r a g o n
0531ACE0  00 73 00 6B 00 00 00 61  00 72 00 61 00 6D 00 65   s k   a r a m e
0531ACF0  00 69 00 73 00 6B 00 00  00 61 00 73 00 74 00 75   i s k   a s t u
0531AD00  00 72 00 69 00 73 00 6B  00 00 00 62 00 65 00 6E   r i s k   b e n
0531AD10  00 67 00 61 00 6C 00 73  00 6B 00 00 00 62 00 72   g a l s k   b r
0531AD20  00 65 00 74 00 6F 00 6E  00 73 00 6B 00 00 00 62   e t o n s k   b
0531AD30  00 75 00 6C 00 67 00 61  00 72 00 73 00 6B 00 00   u l g a r s k
0531AD40  00 63 00 65 00 62 00 75
0531AD50  00 00 00 65 00 6C 00 62
0531AD60  00 6B 00 00 00 65 00 74
0531AD70  00 73 00 6B 00 00 00 66
0531AD80  00 69 00 73 00 6B 00 00
0531AD90  00 73 00 69 00 73 00 6E
0531ADA0  00 61 00 69 00 69 00 73
0531ADB0  00 6C 00 61 00 6E 00 64  00 73 00 6B 00 00 00 6B   l a n d s k   k
0531ADC0  00 61 00 69 00 74 00 68  00 69 00 73 00 6B 00 00   a i t h i s k
0531ADD0  00 6C 00 69 00 6E 00 65  00 E6 00 72 00 20 00 41   l i n e æ r   A
0531ADE0  00 00 00 6C 00 69 00 6E  00 65 00 E6 00 72 00 20     l i n e æ r
0531ADF0  00 42 00 00 00 6C 00 69  00 74 00 61 00 75 00 69   B   l i t a u i
0531AE00  00 73 00 6B 00 00 00 6D  00 61 00 68 00 61 00 6A   s k   m a h a j
0531AE10  00 61 00 6E 00 69 00 00  00 6D 00 61 00 6C 00 61   a n i   m a l a
0531AE20  00 79 00 69 00 73 00 6B  00 00 00 6D 00 61 00 6E   y i s k   m a n
0531AE30  00 64 00 61 00 69 00 73  00 6B 00 00 00 6D 00 6F   d a i s k   m o
0531AE40  00 6C 00 64 00 6F 00 76  00 73 00 6B 00 00 00 6E   l d o v s k   n
0531AE50  00 65 00 64 00 61 00 72  00 76 00 65 00 74 00 00   e d a r v e t
0531AE60  00 73 00 61 00 6D 00 6F  00 61 00 6E 00 73 00 6B   s a m o a n s k
0531AE70  00 00 00 73 00 6C 00 6F  00 76 00 65 00 6E 00 73     s l o v e n s
0531AE80  00 6B 00 00 00 74 00 61  00 74 00 61 00 72 00 69   k   t a t a r i
0531AE90  00 73 00 6B 00 00 00 74  00 6F 00 6E 00 67 00 61   s k   t o n g a
0531AEA0  00 6E 00 73 00 6B 00 00  00 75 00 69 00 67 00 75   n s k   u i g u
0531AEB0  00 72 00 69 00 73 00 6B  00 00 00 75 00 6B 00 72   r i s k   u k r
0531AEC0  00 61 00 69 00 6E 00 73  00 6B 00 00 00 75 00 73   a i n s k   u s
```

File Recovery by Type

87 file headers were found. 9 files were recovered.

OK

[unregistered]
MendeleyDesktop.DMP
C:\Users\agyekum_owuraku\Deskt

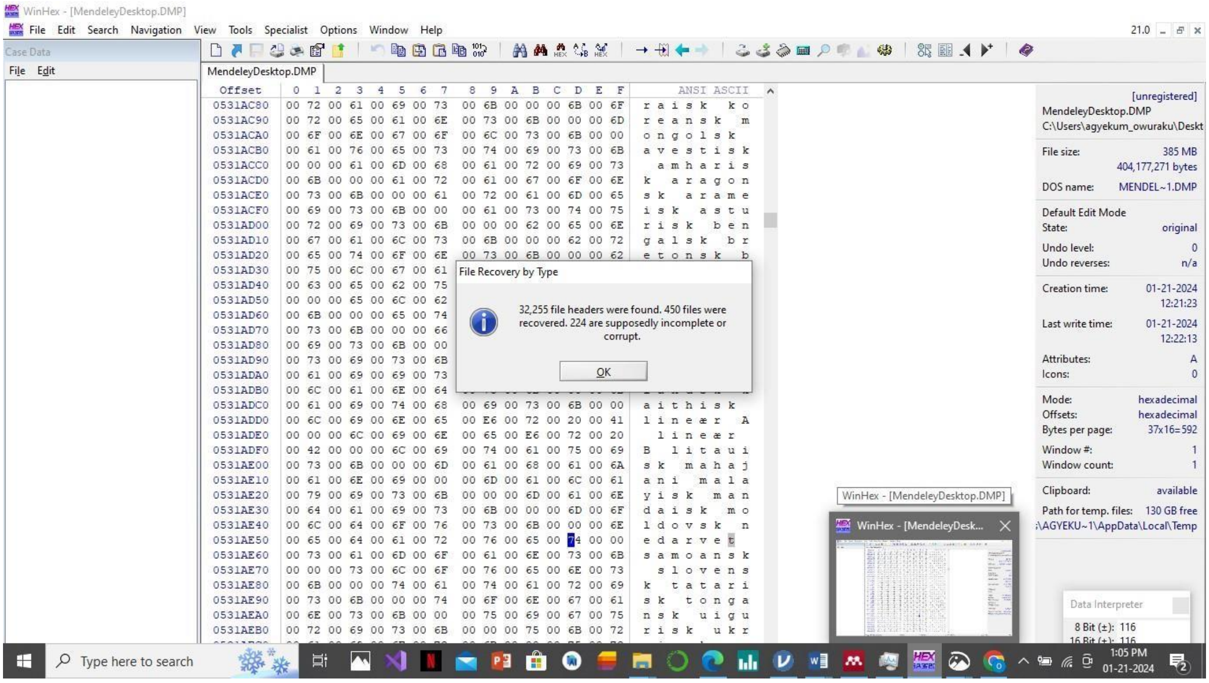
File size:	385 MB 404,177,271 bytes
DOS name:	MENDEL~1.DMP
Default Edit Mode State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	01-21-2024 12:21:23
Last write time:	01-21-2024 12:22:13
Attributes:	A
Icons:	0
Mode:	hexadecimal
Offsets:	hexadecimal
Bytes per page:	37x16=592
Window #:	1
Window count:	1
Clipboard:	available
Path for temp. files:	130 GB free

\AGYEKU~1\AppData\Local\Temp

Data Interpreter
8 Bit (±): 116
16 Bit (±): 116
32 Bit (±): 116
Binary: 01110100

Page 147,200 of 682,732 | Offset: 531AE5D | = 116 | Block: n/a | Size: n/a

Figure 8: Recovery by header


WinHex - [MendeleyDesktop.DMP]
File Edit Search Navigation View Tools Specialist Options Window Help
21.0
Case Data
File Edit
MendeleyDesktop.DMP
WinHex - [MendeleyDesktop.DMP]
WinHex - [MendeleyDesk...
Type here to search
1:05 PM
01-21-2024

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
0531AC80  00 72 00 61 00 69 00 73  00 6B 00 00 00 6B 00 6F   r a i s k   k o
0531AC90  00 72 00 65 00 61 00 6E  00 73 00 6B 00 00 00 6D   r e a n s k   m
0531ACA0  00 6F 00 6E 00 67 00 6F  00 6C 00 73 00 6B 00 00   o n g o l s k
0531ACB0  00 61 00 76 00 65 00 73  00 74 00 69 00 73 00 6B   a v e s t i s k
0531ACC0  00 00 00 61 00 6D 00 68  00 61 00 72 00 69 00 73     a m h a r i s
0531ACD0  00 6B 00 00 00 61 00 72  00 61 00 67 00 6F 00 6E   k   a r a g o n
0531ACE0  00 73 00 6B 00 00 00 61  00 72 00 61 00 6D 00 65   s k   a r a m e
0531ACF0  00 69 00 73 00 6B 00 00  00 61 00 73 00 74 00 75   i s k   a s t u
0531AD00  00 72 00 69 00 73 00 6B  00 00 00 62 00 65 00 6E   r i s k   b e n
0531AD10  00 67 00 61 00 6C 00 73  00 6B 00 00 00 62 00 72   g a l s k   b r
0531AD20  00 65 00 74 00 6F 00 6E  00 73 00 6B 00 00 00 62   e t o n s k   b
0531AD30  00 75 00 6C 00 67 00 61
0531AD40  00 63 00 65 00 62 00 75
0531AD50  00 00 00 65 00 6C 00 62
0531AD60  00 6B 00 00 00 65 00 74
0531AD70  00 73 00 6B 00 00 00 66
0531AD80  00 69 00 73 00 6B 00 00
0531AD90  00 73 00 69 00 73 00 6B
0531ADA0  00 61 00 69 00 69 00 73
0531ADB0  00 6C 00 61 00 6E 00 64
0531ADC0  00 61 00 69 00 74 00 68  00 69 00 73 00 6B 00 00   a i t h i s k
0531ADD0  00 6C 00 69 00 6E 00 65  00 E6 00 72 00 20 00 41   l i n e æ r   A
0531ADE0  00 00 00 6C 00 69 00 6E  00 65 00 E6 00 72 00 20     l i n e æ r
0531ADF0  00 42 00 00 00 6C 00 69  00 74 00 61 00 75 00 69   B   l i t a u i
0531AE00  00 73 00 6B 00 00 00 6D  00 61 00 68 00 61 00 6A   s k   m a h a j
0531AE10  00 61 00 6E 00 69 00 00  00 6D 00 61 00 6C 00 61   a n i   m a l a
0531AE20  00 79 00 69 00 73 00 6B  00 00 00 6D 00 61 00 6E   y i s k   m a n
0531AE30  00 64 00 61 00 69 00 73  00 6B 00 00 00 6D 00 6F   d a i s k   m o
0531AE40  00 6C 00 64 00 6F 00 76  00 73 00 6B 00 00 00 6E   l d o v s k   n
0531AE50  00 65 00 64 00 61 00 72  00 76 00 65 00 74 00 00   e d a r v e t
0531AE60  00 73 00 61 00 6D 00 6F  00 61 00 6E 00 73 00 6B   s a m o a n s k
0531AE70  00 00 00 73 00 6C 00 6F  00 76 00 65 00 6E 00 73     s l o v e n s
0531AE80  00 6B 00 00 00 74 00 61  00 74 00 61 00 72 00 69   k   t a t a r i
0531AE90  00 73 00 6B 00 00 00 74  00 6F 00 6E 00 67 00 61   s k   t o n g a
0531AEA0  00 6E 00 73 00 6B 00 00  00 75 00 69 00 67 00 75   n s k   u i g u
0531AEB0  00 72 00 69 00 73 00 6B  00 00 00 75 00 6B 00 72   r i s k   u k r
```

File Recovery by Type

32,255 file headers were found. 450 files were recovered. 224 are supposedly incomplete or corrupt.

OK

[unregistered]
MendeleyDesktop.DMP
C:\Users\agyekum_owuraku\Deskt

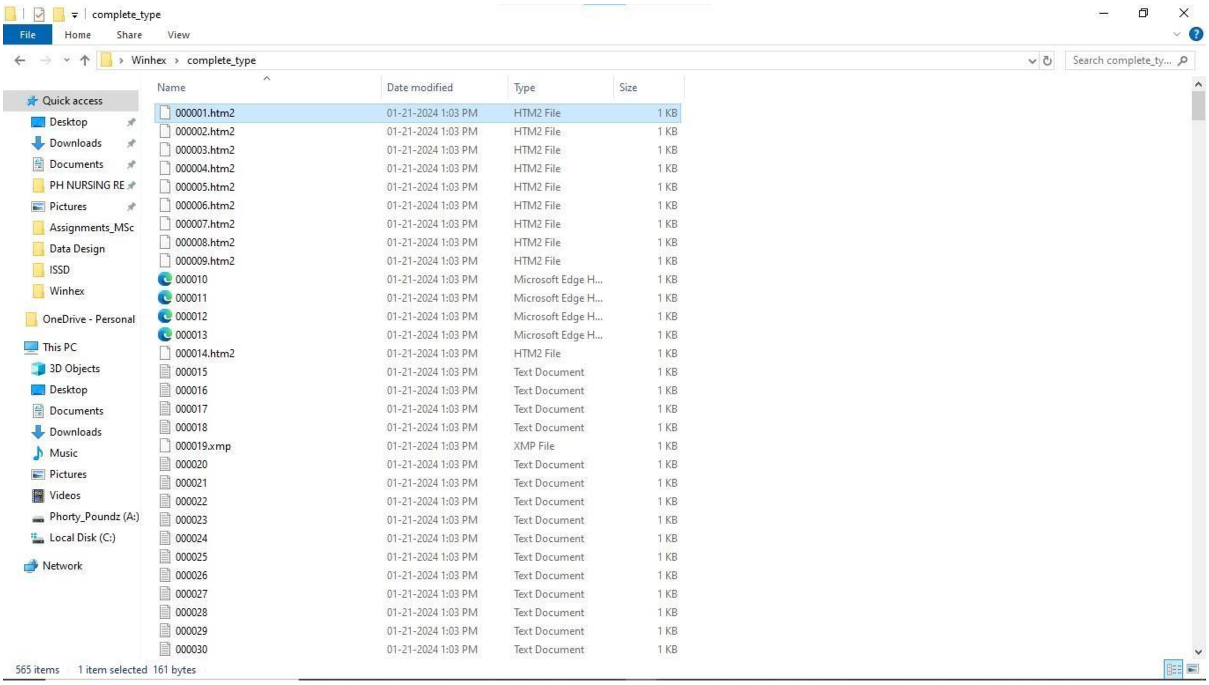
File size:	385 MB 404,177,271 bytes
DOS name:	MENDEL~1.DMP
Default Edit Mode State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	01-21-2024 12:21:23
Last write time:	01-21-2024 12:22:13
Attributes:	A
Icons:	0
Mode:	hexadecimal
Offsets:	hexadecimal
Bytes per page:	37x16=592
Window #:	1
Window count:	1
Clipboard:	available
Path for temp. files:	130 GB free

\AGYEKU~1\AppData\Local\Temp

Data Interpreter
8 Bit (±): 116

Figure 9: Complete file recovery

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



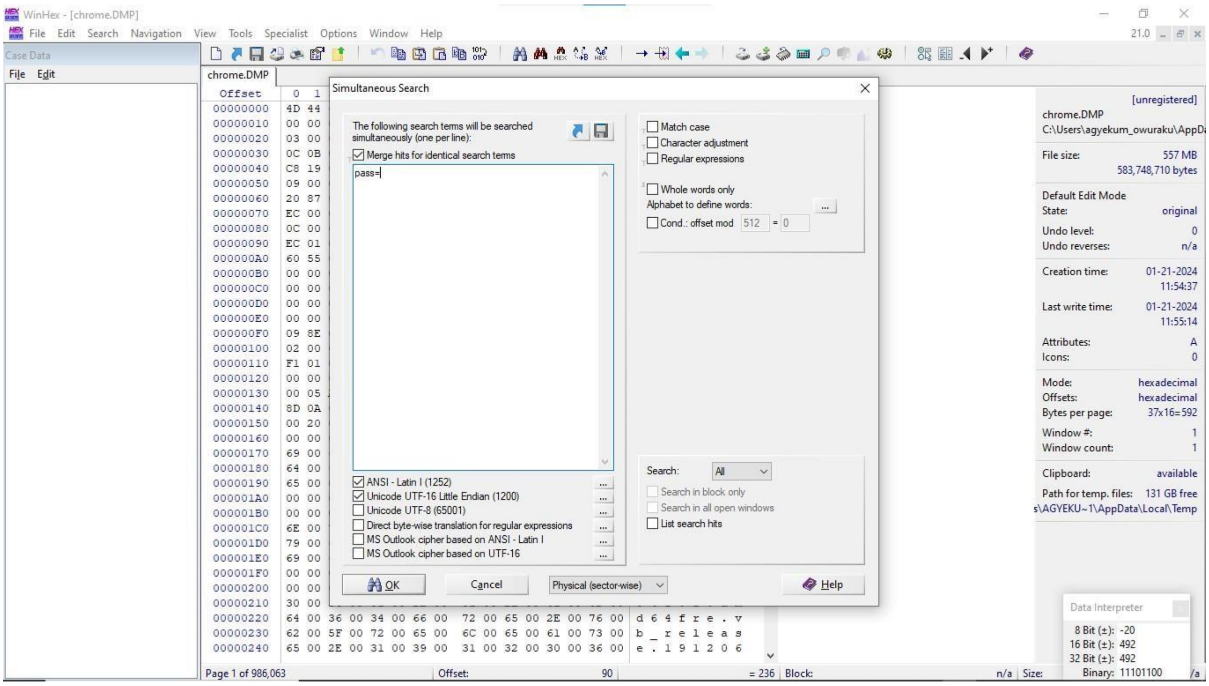
Name	Date modified	Type	Size
000001.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000002.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000003.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000004.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000005.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000006.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000007.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000008.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000009.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000010	01-21-2024 1:03 PM	Microsoft Edge H...	1 KB
000011	01-21-2024 1:03 PM	Microsoft Edge H...	1 KB
000012	01-21-2024 1:03 PM	Microsoft Edge H...	1 KB
000013	01-21-2024 1:03 PM	Microsoft Edge H...	1 KB
000014.htm2	01-21-2024 1:03 PM	HTM2 File	1 KB
000015	01-21-2024 1:03 PM	Text Document	1 KB
000016	01-21-2024 1:03 PM	Text Document	1 KB
000017	01-21-2024 1:03 PM	Text Document	1 KB
000018	01-21-2024 1:03 PM	Text Document	1 KB
000019.xmp	01-21-2024 1:03 PM	XMP File	1 KB
000020	01-21-2024 1:03 PM	Text Document	1 KB
000021	01-21-2024 1:03 PM	Text Document	1 KB
000022	01-21-2024 1:03 PM	Text Document	1 KB
000023	01-21-2024 1:03 PM	Text Document	1 KB
000024	01-21-2024 1:03 PM	Text Document	1 KB
000025	01-21-2024 1:03 PM	Text Document	1 KB
000026	01-21-2024 1:03 PM	Text Document	1 KB
000027	01-21-2024 1:03 PM	Text Document	1 KB
000028	01-21-2024 1:03 PM	Text Document	1 KB
000029	01-21-2024 1:03 PM	Text Document	1 KB
000030	01-21-2024 1:03 PM	Text Document	1 KB

565 items 1 item selected 161 bytes

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.


WinHex - [chrome.DMP]

Simultaneous Search

The following search terms will be searched simultaneously (one per line):

☑ Merge hits for identical search terms

pass=

☑ ANSI - Latin I (1252)
☑ Unicode UTF-16 Little Endian (1200)
☐ Unicode UTF-8 (65001)
☐ Direct byte-wise translation for regular expressions
☐ MS Outlook cipher based on ANSI - Latin I
☐ MS Outlook cipher based on UTF-16

☐ Match case
☐ Character adjustment
☐ Regular expressions
☐ Whole words only
Alphabet to define words:
☐ Cond.: offset mod 512 = 0

Search: All
☐ Search in block only
☐ Search in all open windows
☐ List search hits

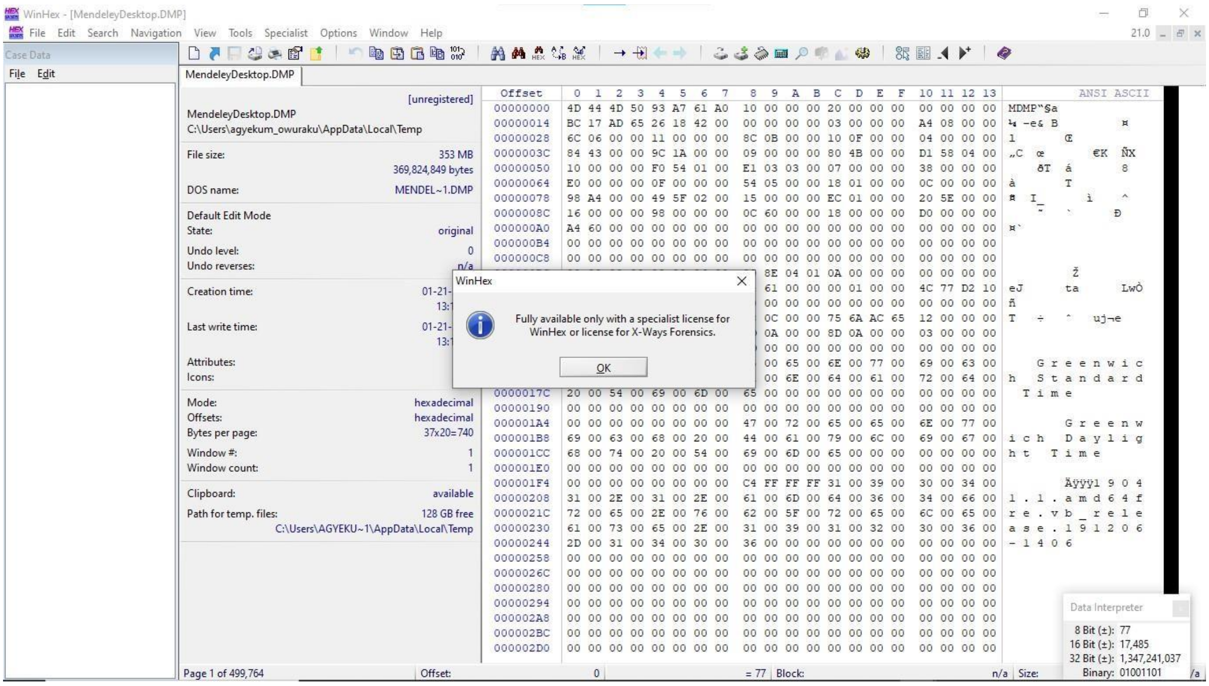
Physical (sector-wise)

chrome.DMP
C:\Users\agyekum_owuraku\AppD
File size: 557 MB
583,748,710 bytes
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 01-21-2024 11:54:37
Last write time: 01-21-2024 11:55:14
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 37x16=592
Window #: 1
Window count: 1
Clipboard: available
Path for temp. files: 131 GB free
s\AGYEKU~1\AppData\Local\Temp

Page 1 of 986,063 Offset: 90 = 236 Block: n/a Size:

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.



WinHex - [MendeleyDesktop.DMP]

File Edit Search Navigation View Tools Specialist Options Window Help
21.0
Case Data
File Edit
MendeleyDesktop.DMP

[unregistered]

MendeleyDesktop.DMP
C:\Users\agyekum_owuraku\AppData\Local\Temp

File size: 353 MB
369,824,849 bytes

DOS name: MENDEL~1.DMP

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 01-21-
13:1

Last write time: 01-21-
13:1

Attributes:
Icons:

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 37x20=740

Window #: 1
Window count: 1

Clipboard: available

Path for temp. files: 128 GB free
C:\Users\AGYEKU~1\AppData\Local\Temp

```
  Offset   0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F  10 11 12 13      ANSI ASCII
00000000  4D 44 4D 50 93 A7 61 A0  10 00 00 00 20 00 00 00  00 00 00 00  MDMP"§a
00000014  BC 17 AD 65 26 18 42 00  00 00 00 00 03 00 00 00  A4 08 00 00  ¼ -e& B      ¤
00000028  6C 06 00 00 11 00 00 00  8C 0B 00 00 10 0F 00 00  04 00 00 00  l      Œ
0000003C  84 43 00 00 9C 1A 00 00  09 00 00 00 80 4B 00 00  D1 58 04 00  „C  œ      €K  ÑX
00000050  10 00 00 00 F0 54 01 00  E1 03 03 00 07 00 00 00  38 00 00 00      ðT  á      8
00000064  E0 00 00 00 0F 00 00 00  54 05 00 00 18 01 00 00  0C 00 00 00  à      T
00000078  98 A4 00 00 49 5F 02 00  15 00 00 00 EC 01 00 00  20 5E 00 00  ˜¤  I_      ì    ^
0000008C  16 00 00 00 98 00 00 00  0C 60 00 00 18 00 00 00  D0 00 00 00     ˜    `      Ð
000000A0  A4 60 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00  ¤`
000000B4  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000000C8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
                                      8E 04 01 0A 00 00 00  00 00 00 00              Ž
                                      61 00 00 00 01 00 00  4C 77 D2 10  eJ      ta      LwÒ
                                      00 00 00 00 00 00 00  00 00 00 00  ñ
                                      0C 00 00 75 6A AC 65  12 00 00 00  T   ÷   ˆ   uj¬e
                                      0A 00 00 8D 0A 00 00  03 00 00 00
                                      00 00 00 00 00 00 00  00 00 00 00
                                      00 65 00 6E 00 77 00  69 00 63 00     G r e e n w i c
                                      00 6E 00 64 00 61 00  72 00 64 00  h   S t a n d a r d
0000017C  20 00 54 00 69 00 6D 00  65 00 00 00 00 00 00 00  00 00 00 00    T i m e
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000001A4  00 00 00 00 00 00 00 00  47 00 72 00 65 00 65 00  6E 00 77 00          G r e e n w
000001B8  69 00 63 00 68 00 20 00  44 00 61 00 79 00 6C 00  69 00 67 00  i c h   D a y l i g
000001CC  68 00 74 00 20 00 54 00  69 00 6D 00 65 00 00 00  00 00 00 00  h t   T i m e
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000001F4  00 00 00 00 00 00 00 00  C4 FF FF FF 31 00 39 00  30 00 34 00          Äÿÿÿ1 9 0 4
00000208  31 00 2E 00 31 00 2E 00  61 00 6D 00 64 00 36 00  34 00 66 00  1 . 1 . a m d 6 4 f
0000021C  72 00 65 00 2E 00 76 00  62 00 5F 00 72 00 65 00  6C 00 65 00  r e . v b _ r e l e
00000230  61 00 73 00 65 00 2E 00  31 00 39 00 31 00 32 00  30 00 36 00  a s e . 1 9 1 2 0 6
00000244  2D 00 31 00 34 00 30 00  36 00 00 00 00 00 00 00  00 00 00 00  - 1 4 0 6
00000258  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
0000026C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
00000280  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
00000294  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002A8  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002BC  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
000002D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  00 00 00 00
```

WinHex

Fully available only with a specialist license for WinHex or license for X-Ways Forensics.

Data Interpreter
8 Bit (±): 77
16 Bit (±): 17,485
32 Bit (±): 1,347,241,037
Binary: 01001101

Page 1 of 499,764 | Offset: 0 | = 77 | Block: n/a | Size:

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. 114128.

Feruza, 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.