CHAPTER I

INTRODUCTION

The digital forensics community feels the urge to rapidly develop tools and techniques for capturing and analyzing physical memory content. This is motivated by the fact that physical memory may contain evidence that may not be found in any other source of digital evidence. The expected techniques will facilitate the investigation and analysis process and allow to reach more reliable conclusions. There has been a good attention paid to acquisition and analysis of physical memory in the past years. This paper explains the importance of the information that exists in memory for forensic investigators and introduces new approaches for the extraction and analysis of this information.

Forensic analysis of physical memory is gaining good attention from experts in the community especially after recent development of valuable tools and techniques. Investigators find it very helpful to seize physical memory contents and perform post-incident analysis of this potential evidence. So to extract the physical memory one must have access to the particular evidence system so if it is a password protected device, the memory dump of the particular digital evidence (laptops, computers..etc) can be used to obtain the passwords required.

CHAPTER II

LITERATURE REVIEW

Sarmoria and Chapin (2005) the *BodySnatcher* tool injects an independent acquisition operating system into the potentially compromised host operating system kernel. The injected operating system takes snapshots of the host operating system memory. These two techniques rely on preparing systems before any incident happens. The method of Carrier and Grand (2004) is among the few other hardware-based memory acquisition techniques that alter memory contents as little as possible. This method uses a PCI expansion card to dump the memory content to an external device.

The ManTech's Memory DD (MDD) (ManTech International Corporation) and Win32dd (Suiche) (2008)- Various software-based tools have been recently developed for memory acquisition. We can cite *WinEn* from Guidance Software which is part of EnCase Forensic version 6.11 and above (Guidance Software). This tool produces memory images with three different levels of compression that contain headers specific to EnCase which make the image hard to understand by other analysis tools tools generate raw images of memory contents.

Betz, (2005) launched MemParser which is a tool that loads a Windows memory dump, generates a list of active processes, and extracts information relating to a specific process. This tool is also able to dump the memory area allocated to a specific process. KnTList (Garner and R-Mora, 2007) is a command line tool that reconstructs the virtual address space of the system process and other processes. *PTFinder* is a proof-of-concept implementation (Schuster, 2006) providing the capability of revealing hidden and terminated processes and threads. In Carvey and Kleiman (2007), a tool developed in perl script, reads a windows crash dump file, finds structures, and translates virtual addresses (and pointers) to physical offsets within the dump file itself. This tool is available in the book'd DVD toolkit of Carvey and Kleiman (2007).

Zhao and Cao (2009)using *hiberfil.sys* (the hibernation file that contains a memory dump when the operating system hibernates), Windows crash dump file, pagefile, and direct memory access. Although, this work proposed to look for interesting patterns in the memory that may lead to sensitive information, it did not give valuable hints on how to obtain these patterns.One important contribution of this paper is leveraging this work by explaining the process of obtaining fingerprints and how it can be automated.

In a recently published research (Hejazi et al., 2008), S. M. Hejazi et al. paid attention to an important aspect of memory contents and proposed new methods for the extraction of executable and data files from physical memory images. Finally, A.R. Arasteh and M. Debbabi, in their paper (Arasteh and Debbabi, 2007), have paid attention to the analysis of memory stack and building a partial execution path for open processes. This has been achieved through combinational use of stack residues and process code extracted from memory contents. Section 6 of our paper augments this work by analyzing stack frames and extracting the sensitive parameters passed to functions.

CHAPTER III

AIM AND OBJECTIVE

Aim

To extract Passwords From “DUMP” files using WINHEX tool

Objectives

To know about the WINHEX tool, Study its features and try to extract Passwords from “DUMP” files

CHAPTER IV

MATERIALS AND METHODOLOGY

Materials required

- A working laptop
- Dump files from different sample Laptops of different companies and models
- A forensically licensed WINHEX tool

Methodology

Hypothesis

To see if sensitive data such as passwords can be extracted from computer 'Dump' files using a tool called 'WINHEX'

Why this acquisition?

Digital evidences are becoming more predominant to the society so acquisition of data from these evidences will prove to more important than material evidences. So in this project I'll try to recover a specific data from the digital evidence

Collection of data

I searched in my locality to find 10 different laptops with random company and model and collected the data from them

Then I did the research with the help of an external guide in my house

The research was completed within 15 days

Methods (acquiring dump file)

Laptop 1 : Lenovo B41

Step 1 Take FACEBOOK in Google Chrome and login using your credentials

Figure 1.1

Step 2 Login to your account and logout after a minute or two

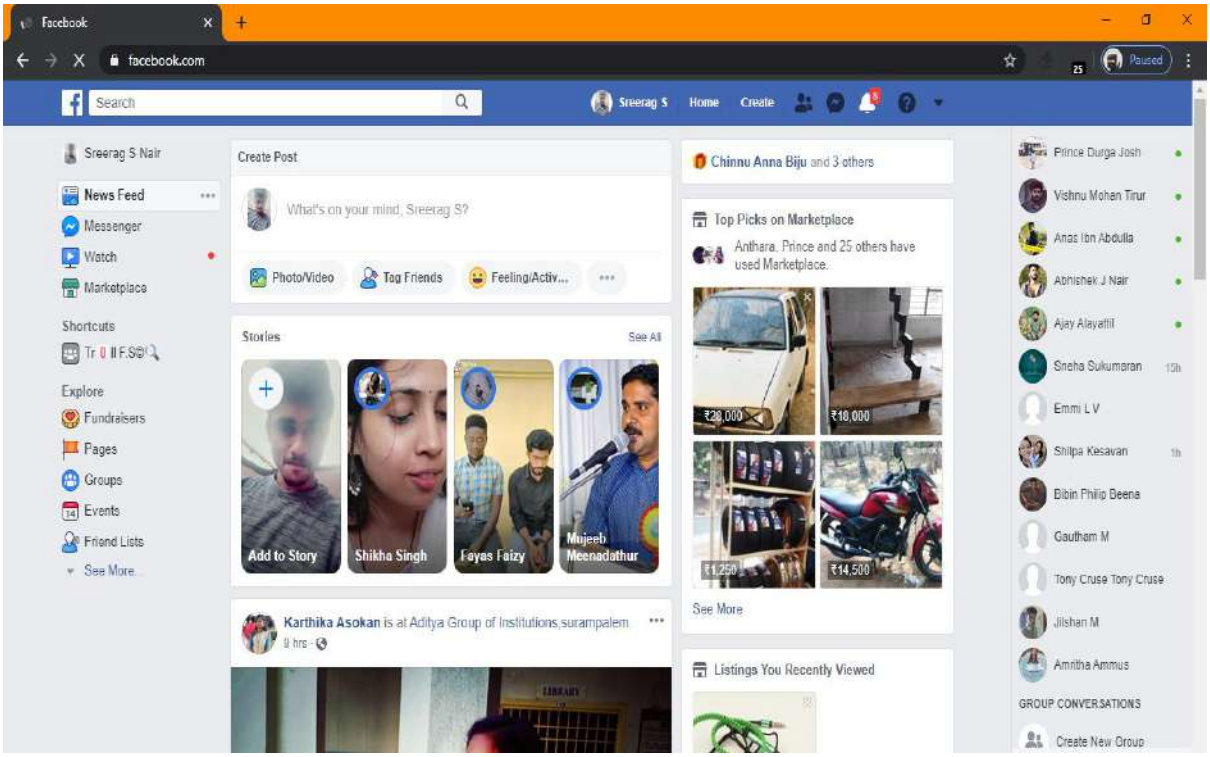


Figure 1.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

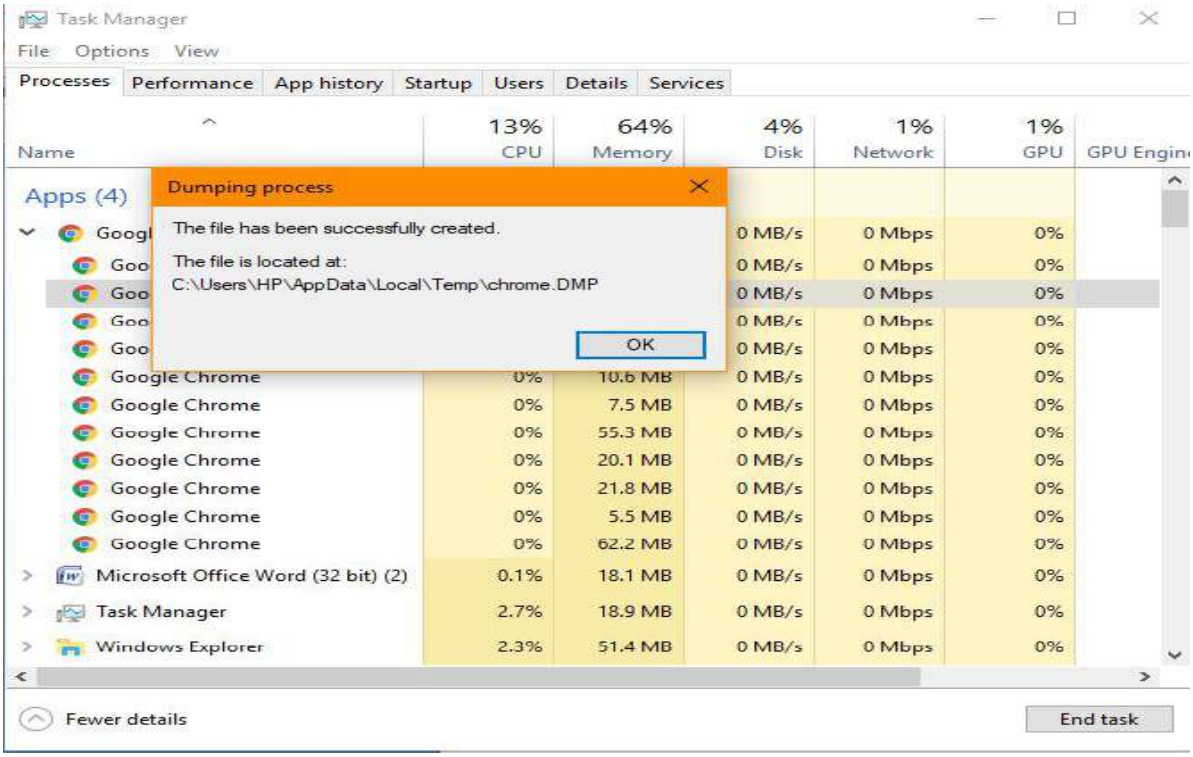


Figure 1.3

Step 4 Locate the Dumpfile in your PC

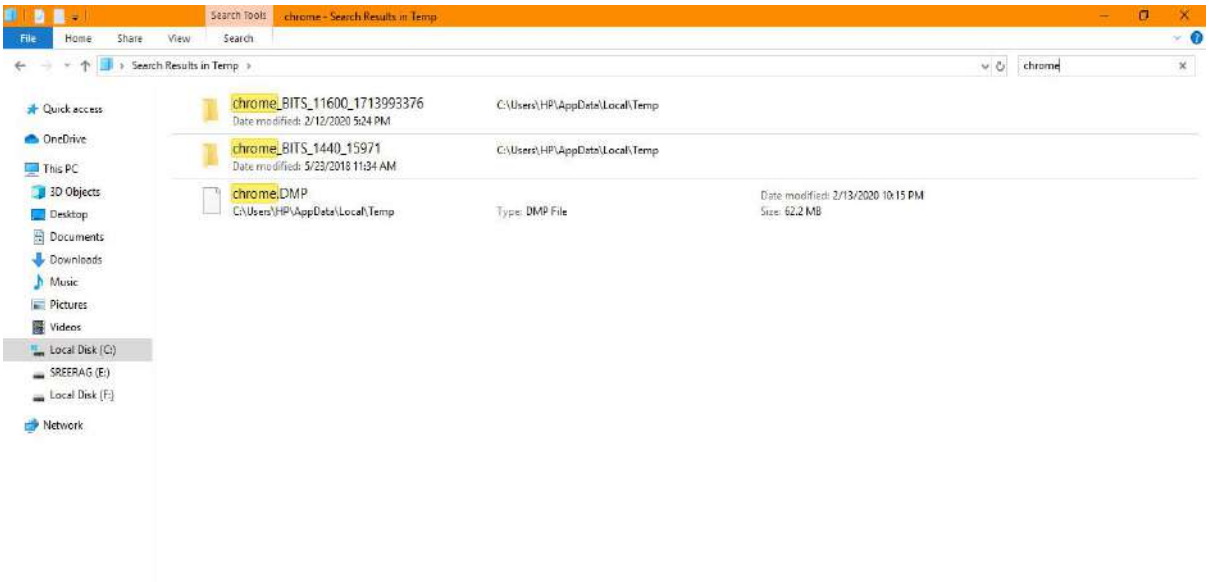


Figure 1.4

Step 5 Open the specific Dumpfile using WINHEX tool

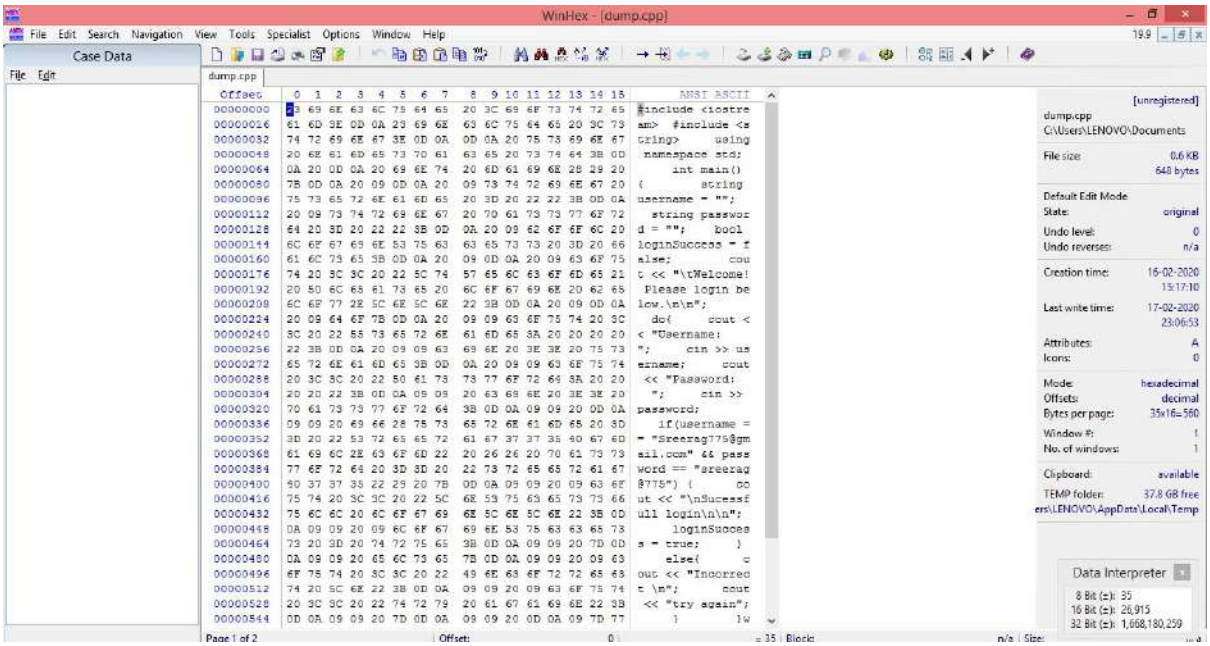


Figure 1.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

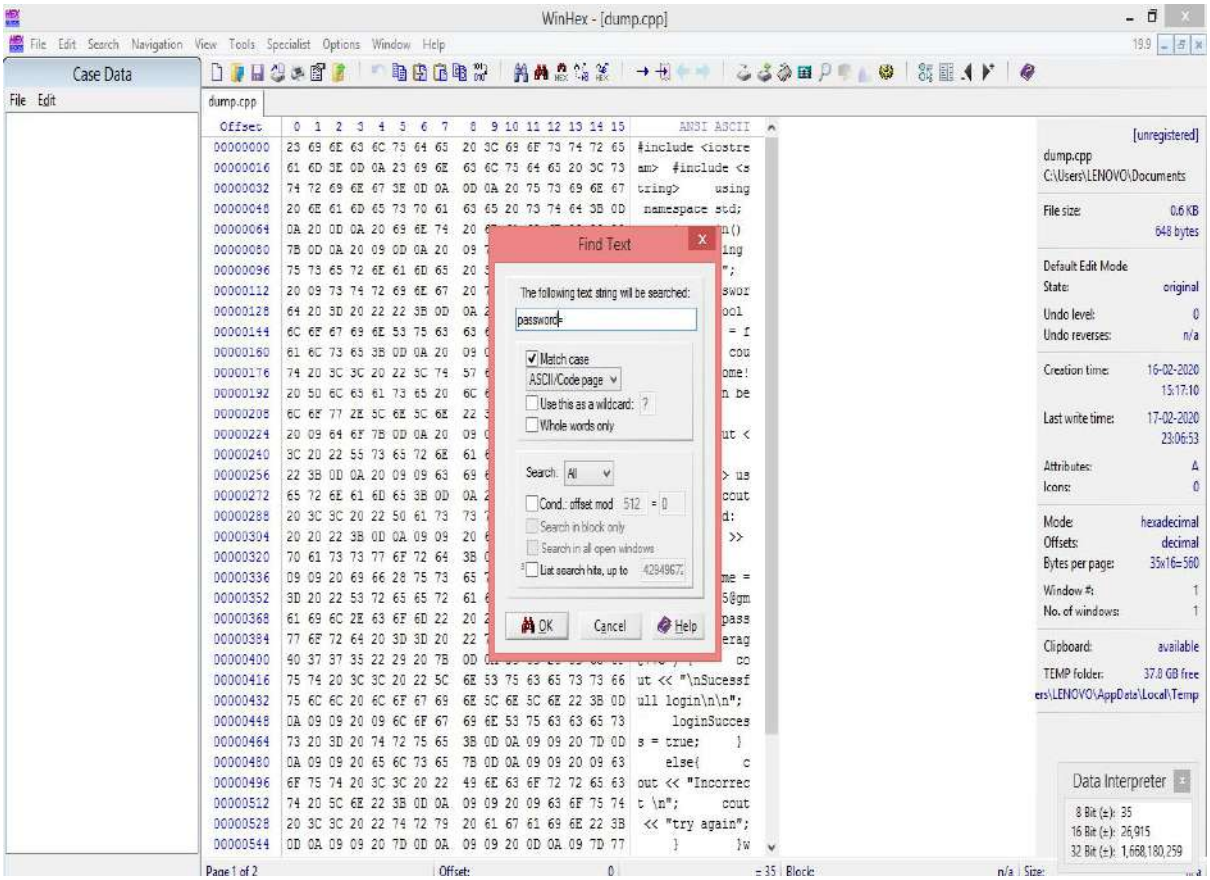


Figure 1.6

Step 7 Click on okay button to see the results.

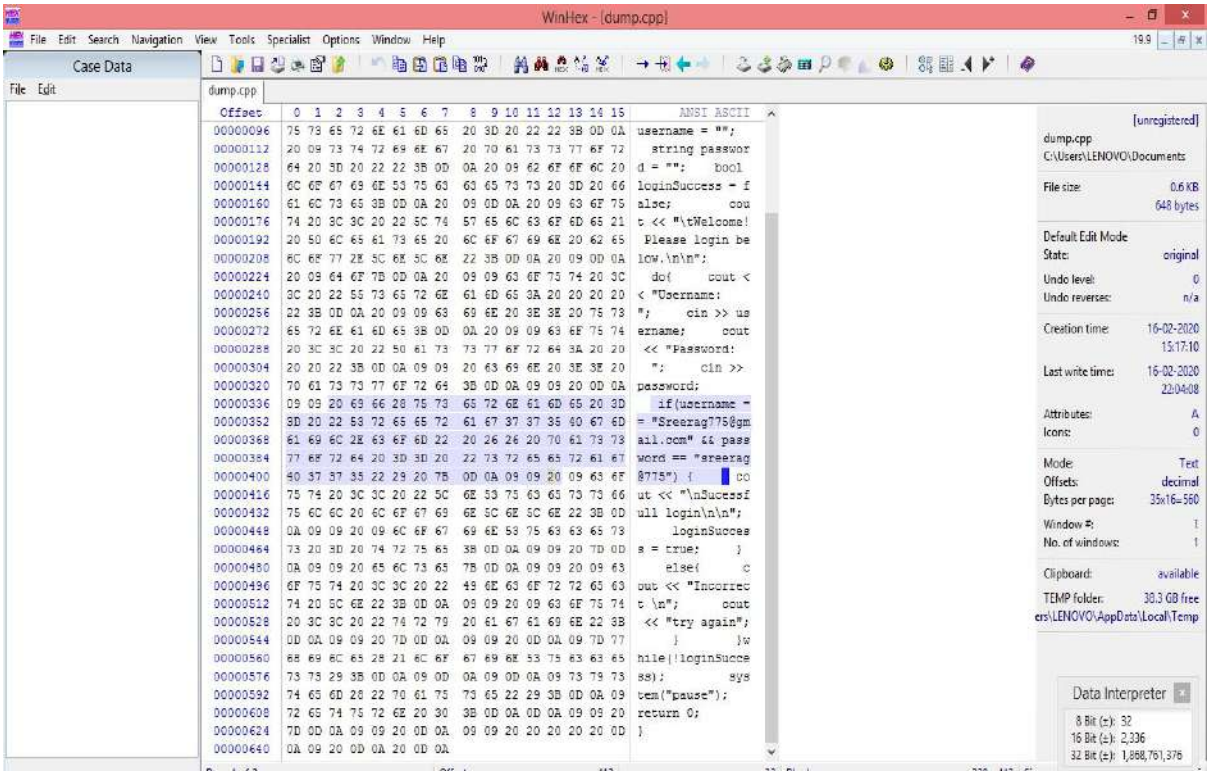


Figure 1.7

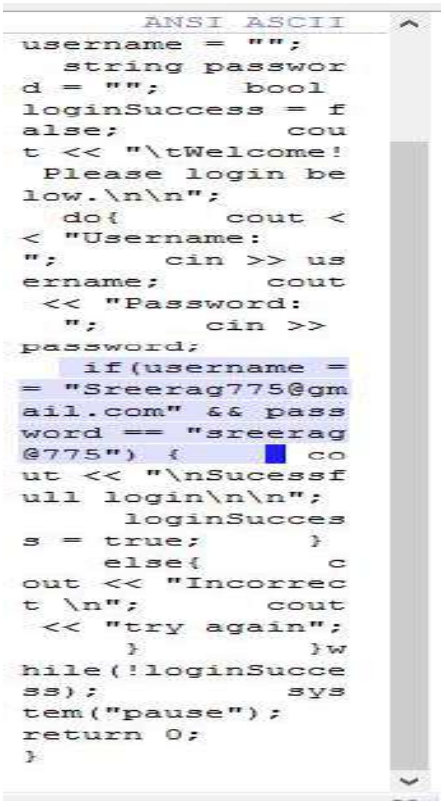


Figure 1.8

Laptop 2: Lenovo Ideapad

Step 1: Take FLIPKART in Google Chrome and login using your credentials

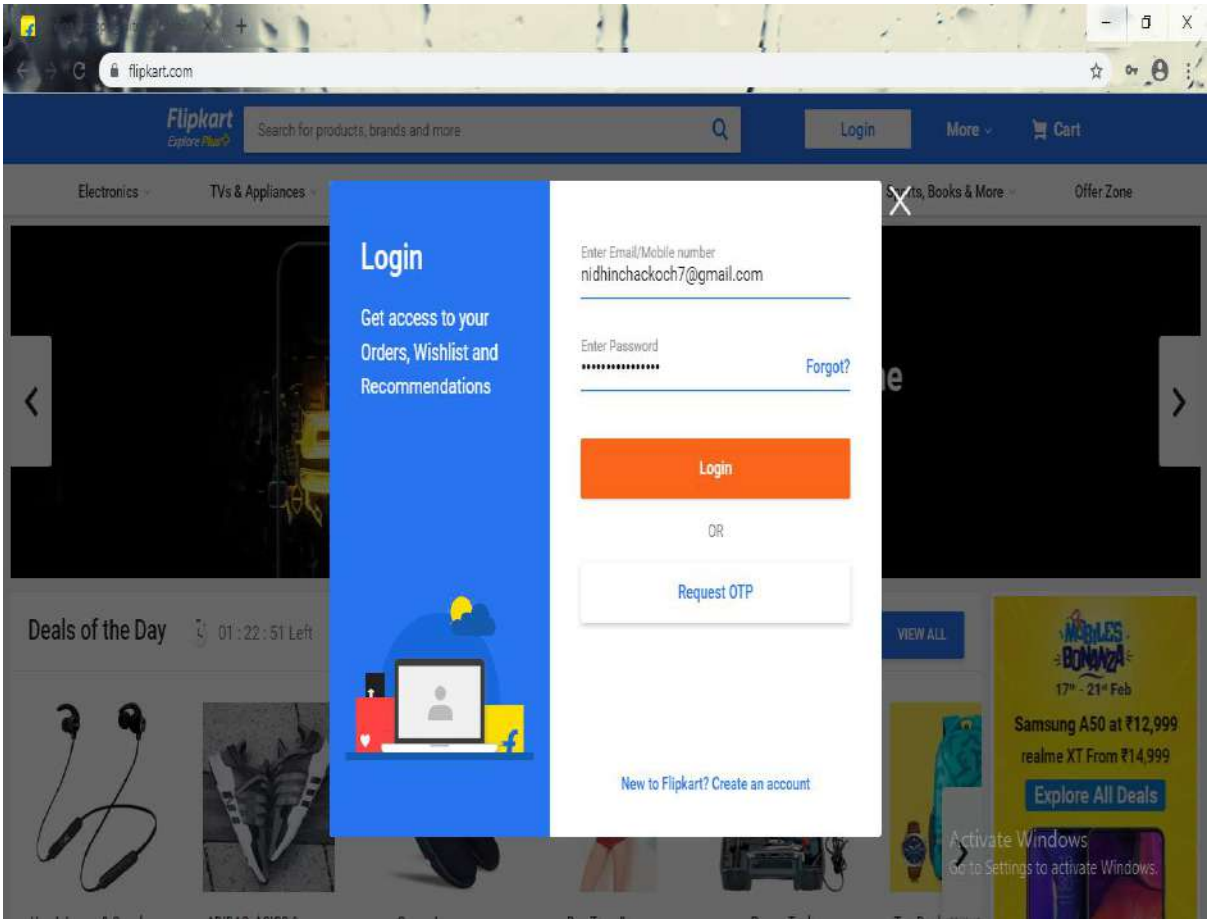


Figure 2.1

Step 2 Login to your account and logout after a minute or two

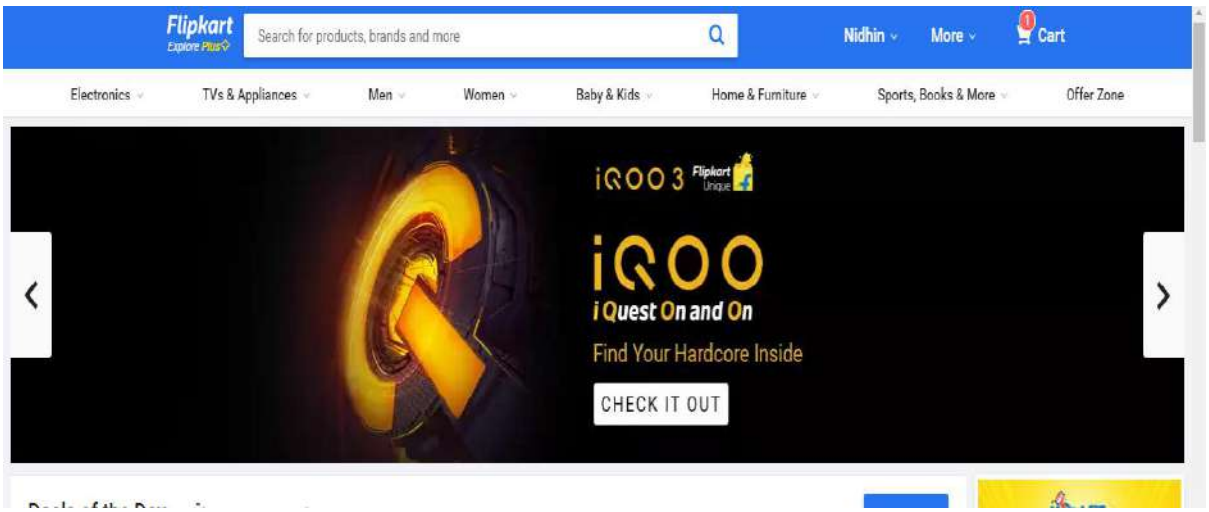


Figure 2.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

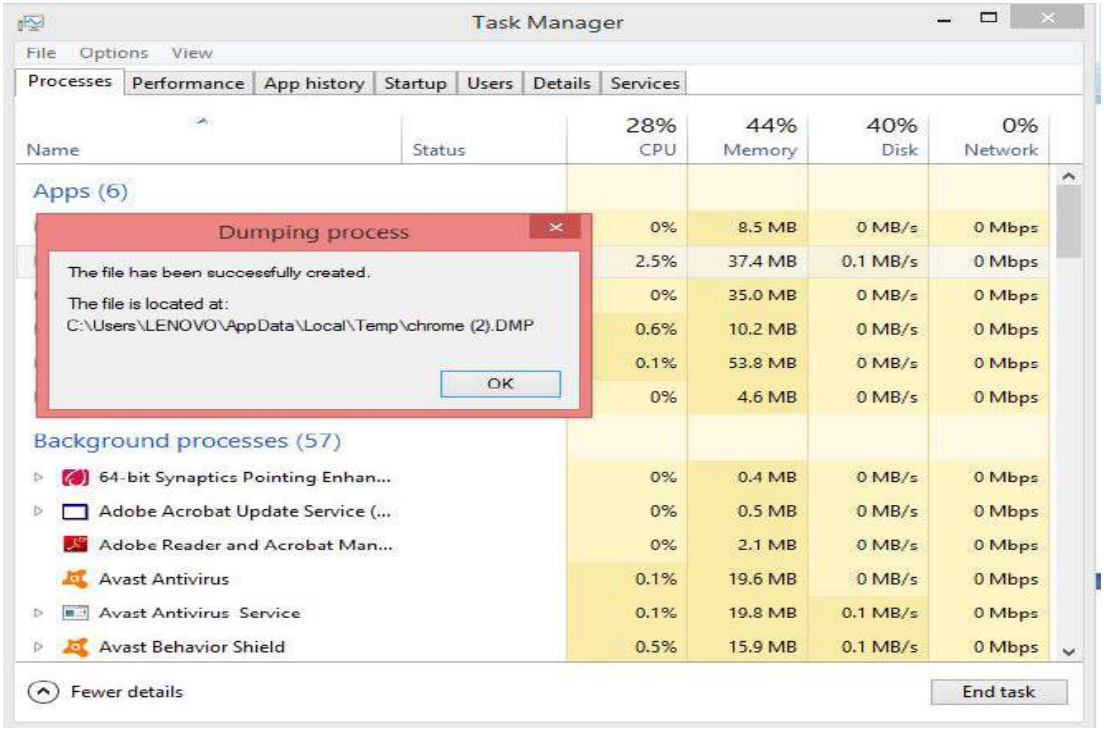


Figure 2.3

Step 4 Locate the Dumpfile in your PC

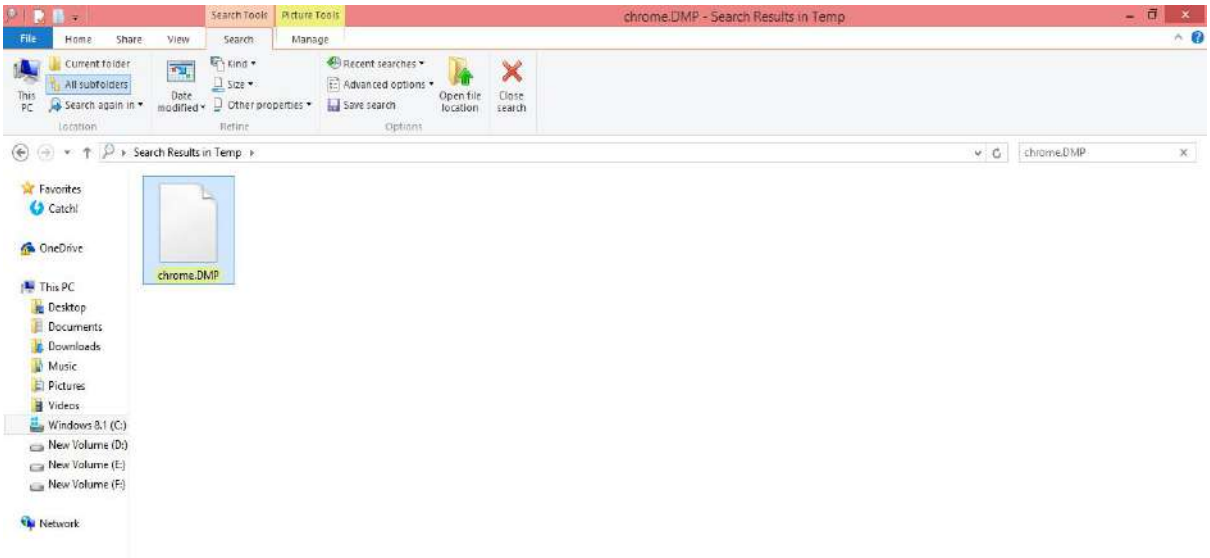


Figure 2.4

Step 5 Open the specific Dumpfile using WINHEX tool

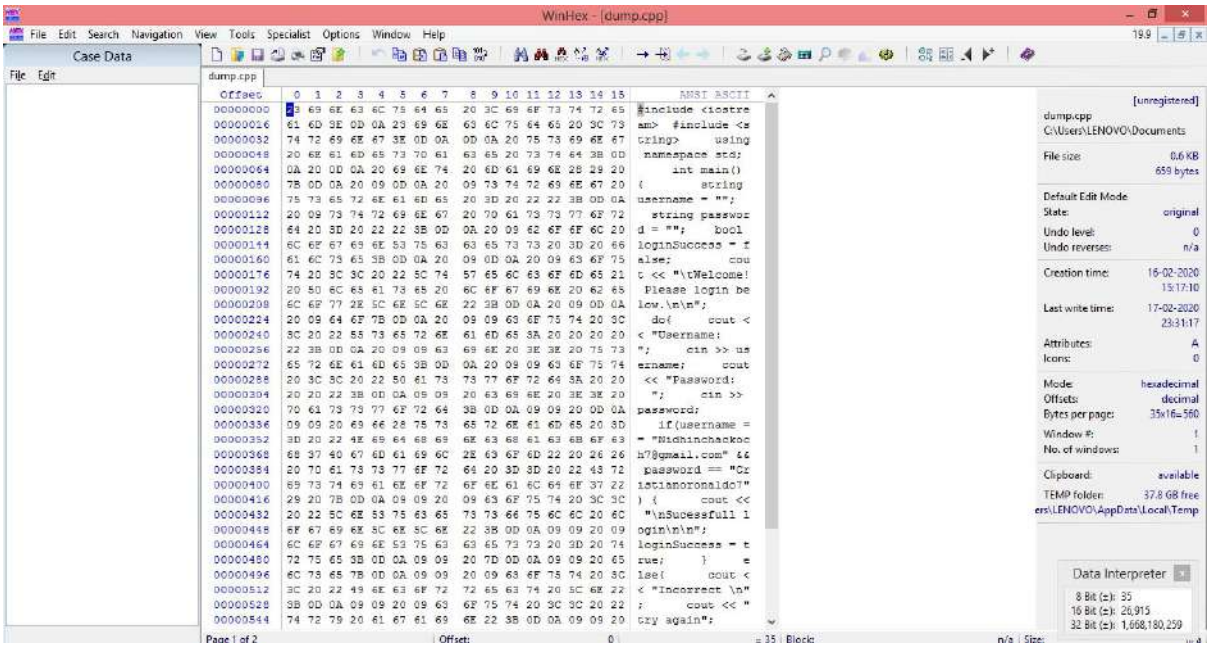


Figure 2.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

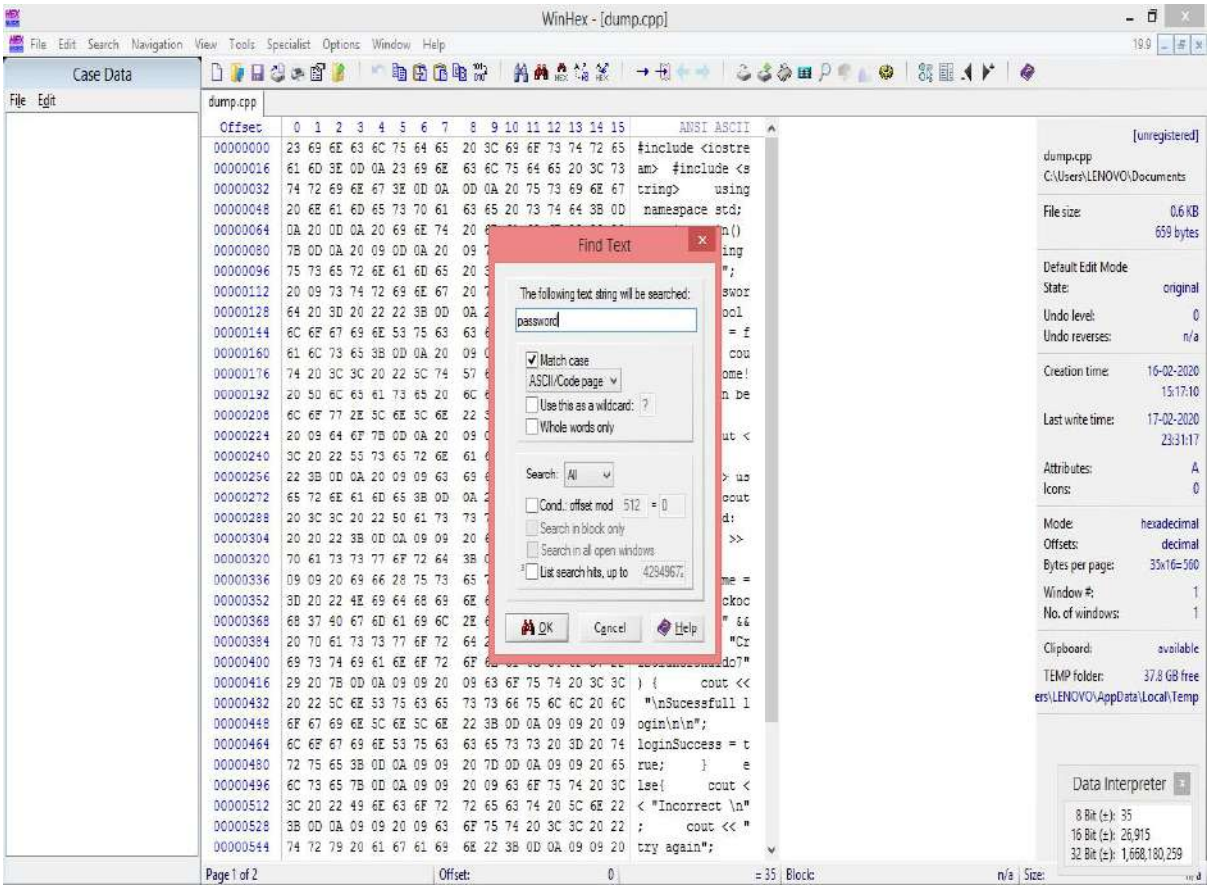


Figure 2.6

Step 7 Click on okay button to see the results.

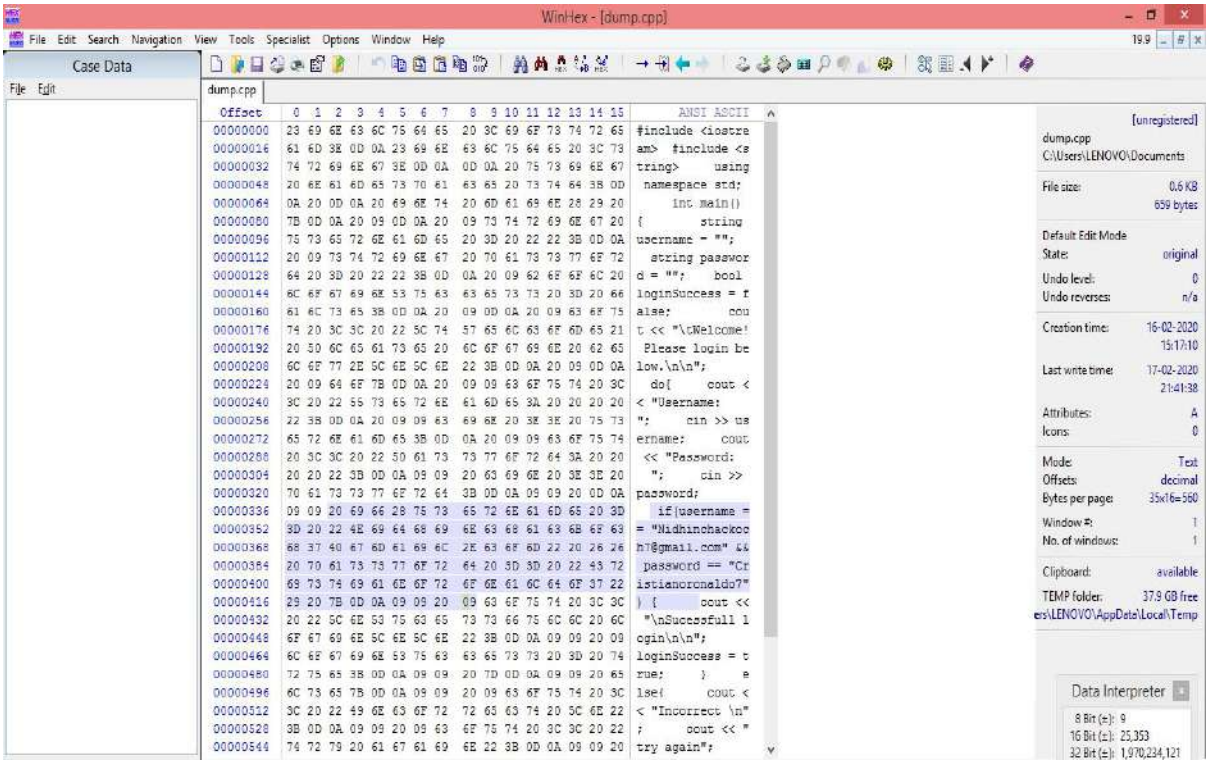


Figure 2.7

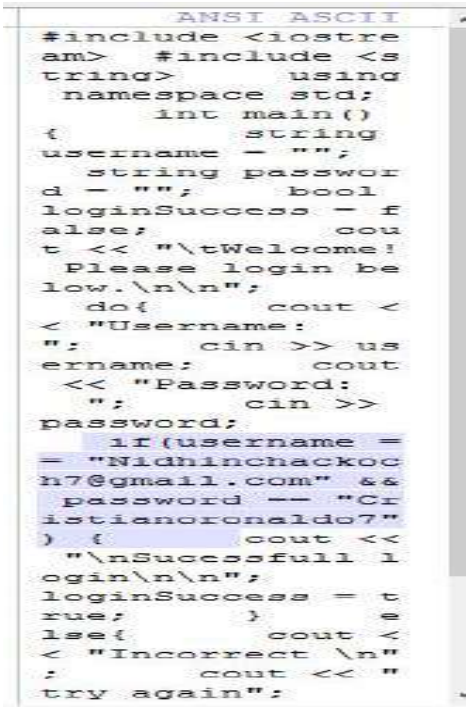


Figure 2.8

Laptop 3: HP 15 Ryzen

Step 1 Take FACEBOOK in Google Chrome and login using your credentials

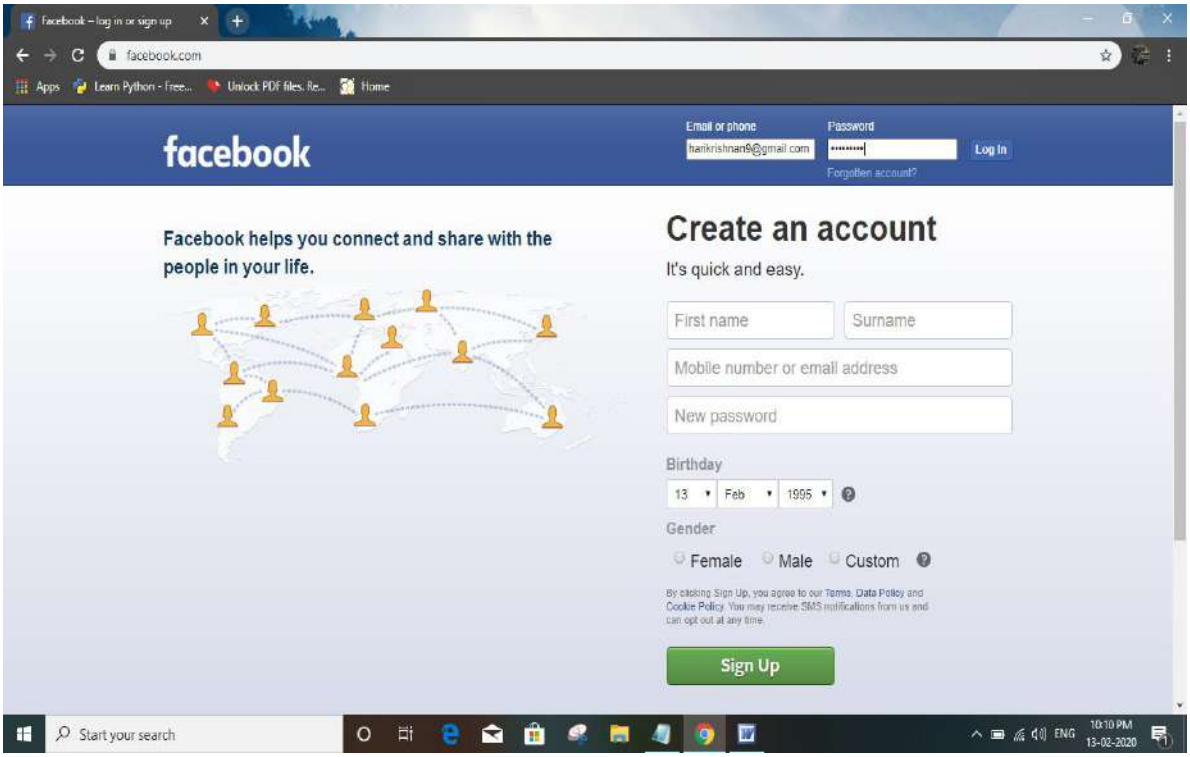


Figure 3.1

Step 2 Login to your account and logout after a minute or two

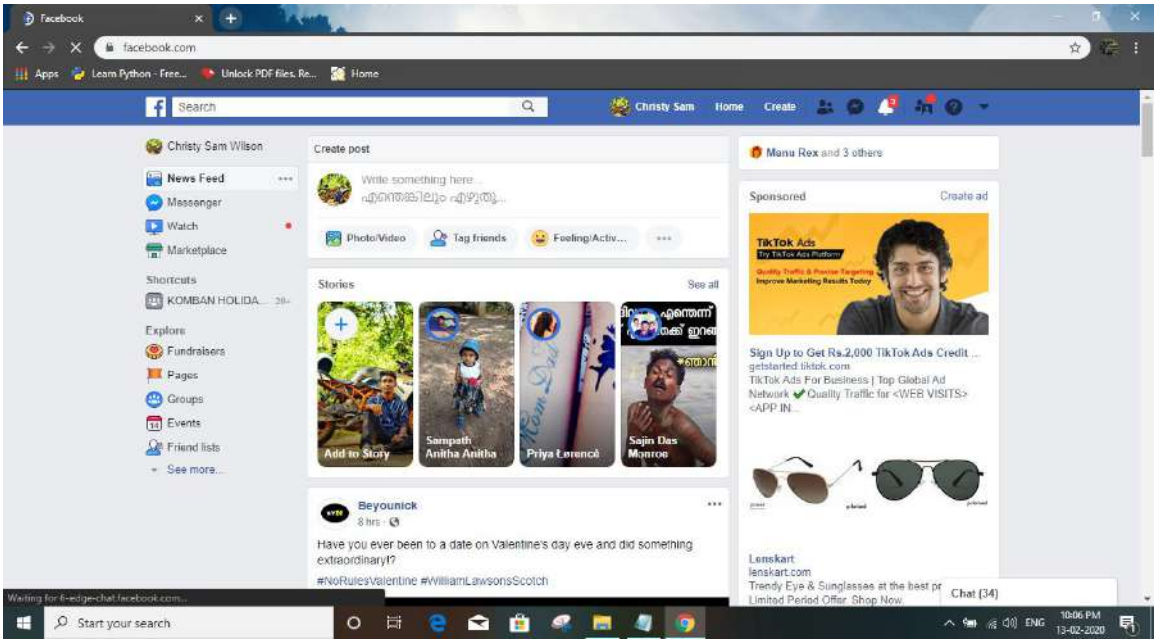


Figure 3.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on ‘Create Dump File’. Within a minute a Dumpfile will be created along with the file path

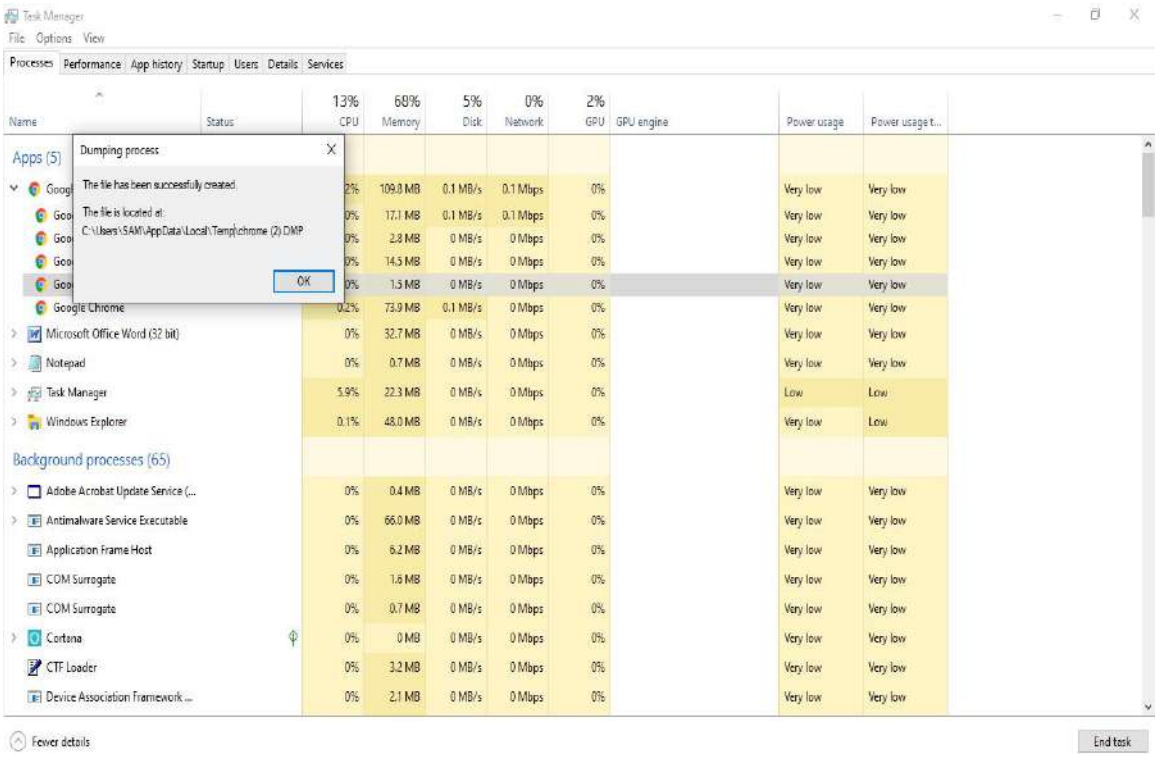


Figure 3.3

Step 4 Locate the Dumpfile in your PC

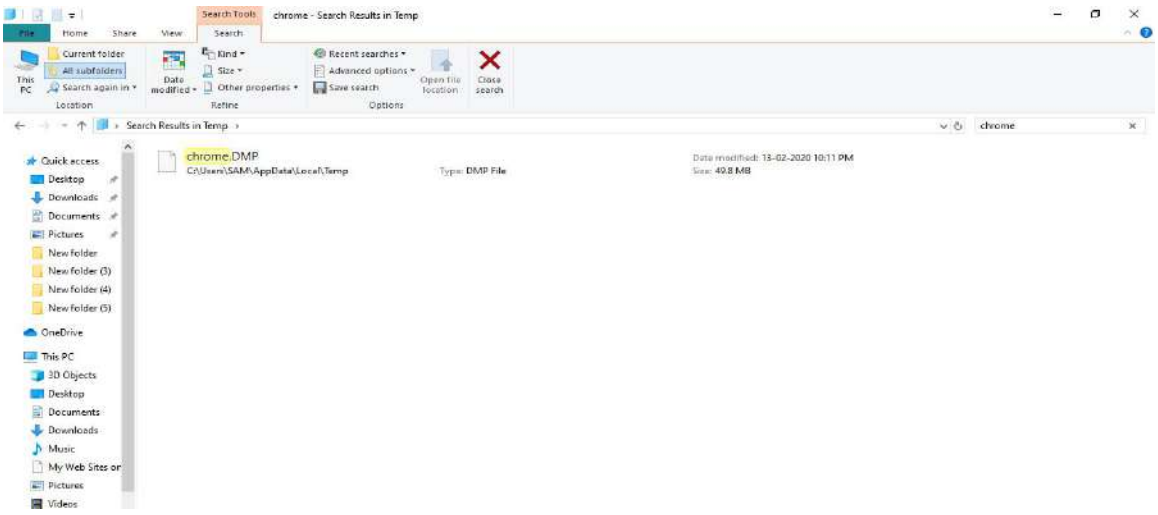


Figure 3.4

Step 5 Open the specific Dumpfile using WINHEX tool

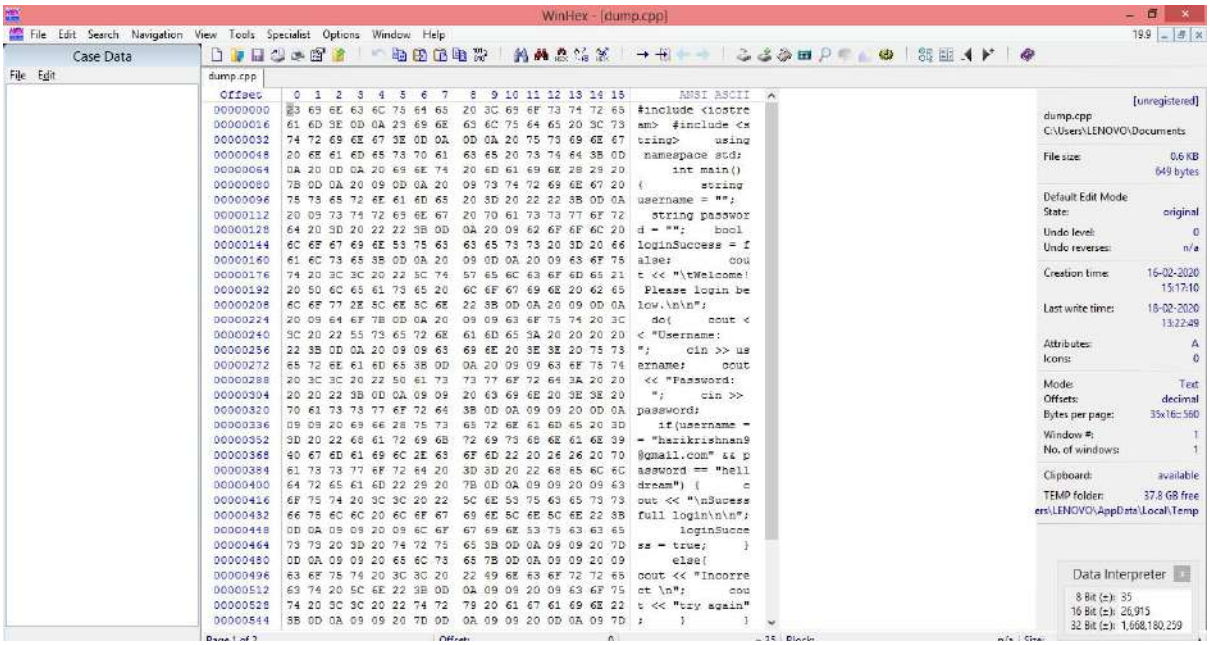


Figure 3.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

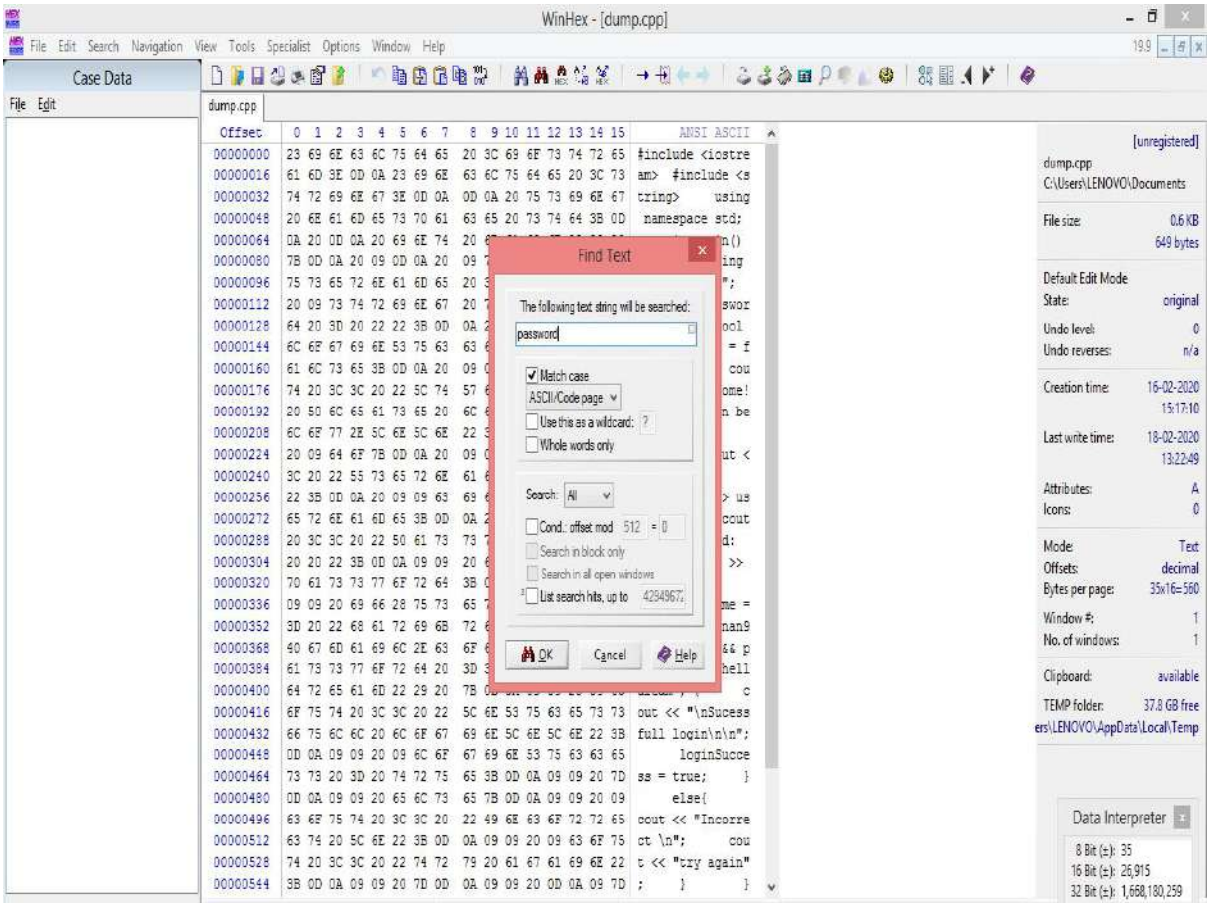


Figure 3.6

Step 7 Click on okay button to see the results

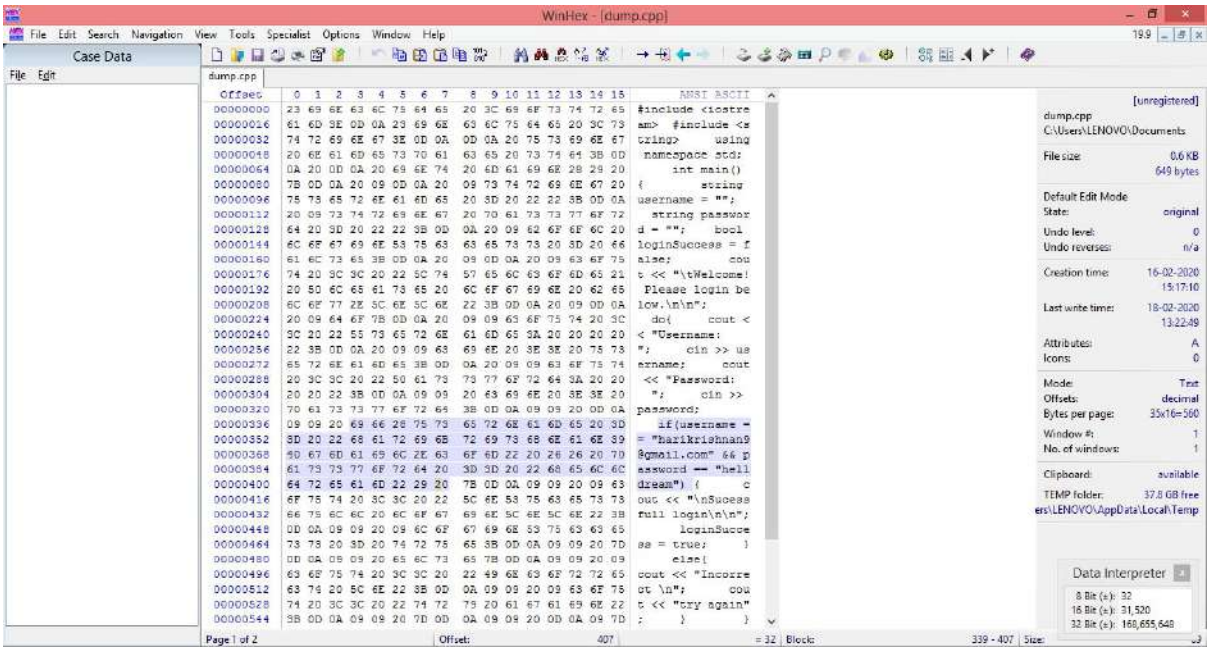


Figure 3.7

```
        ANSI ASCII
#include <iostre
am>   #include <s
tring>       using
 namespace std;
      int main()
{          string
username = "";
   string passwor
d = "";      bool
loginSuccess = f
alse;           cou
t << "\tWelcome!
 Please login be
low.\n\n";
   do{       cout <
< "Username:
";       cin >> us
ername;        cout
 << "Password:
  ";       cin >>
password;
    if(username =
= "harikrishnan9
@gmail.com" && p
assword == "hell
dream") {       c
out << "\nSucess
full login\n\n";
       loginSucce
ss = true;       }
      else{
cout << "Incorre
ct \n";       cou
t << "try again"
;       }          }
```

Figure 3.8

Laptop 4: HP 14 Ryzen

Step 1 Take GMAIL in Google Chrome and login using your credentials

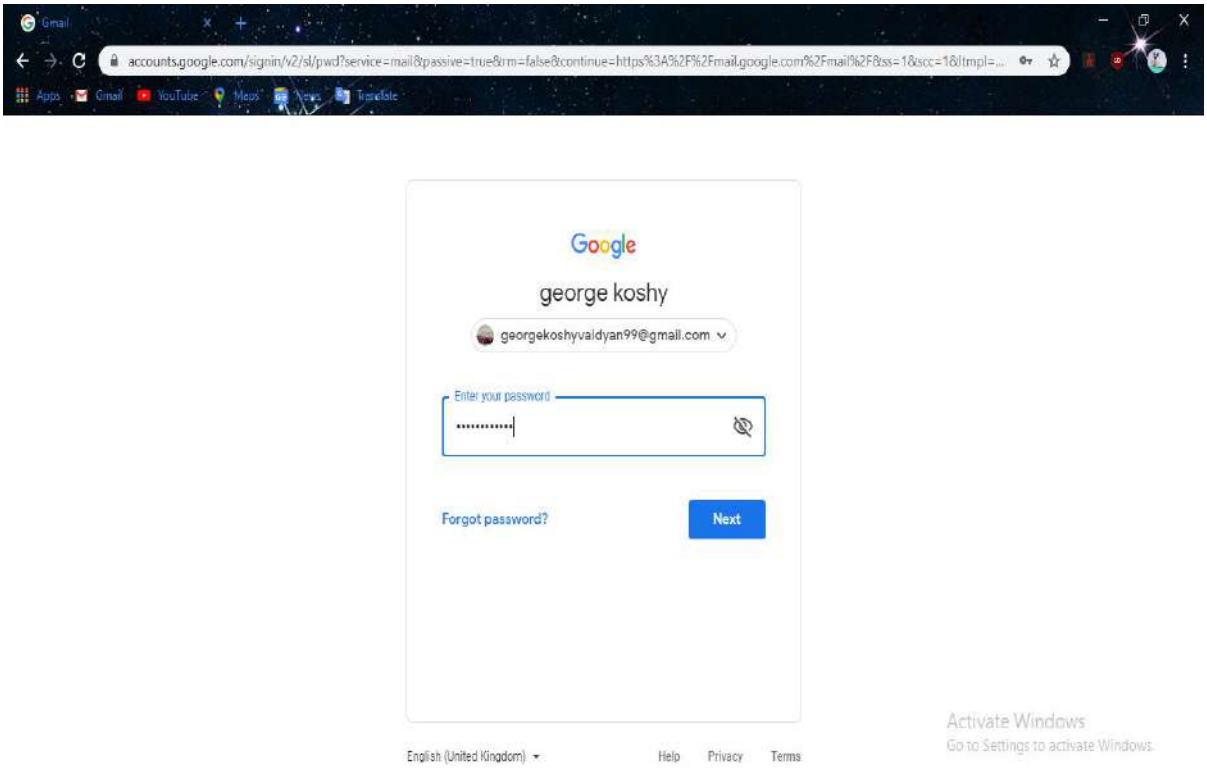


Figure 4.1

Step 2 Login to your account and logout after a minute or two

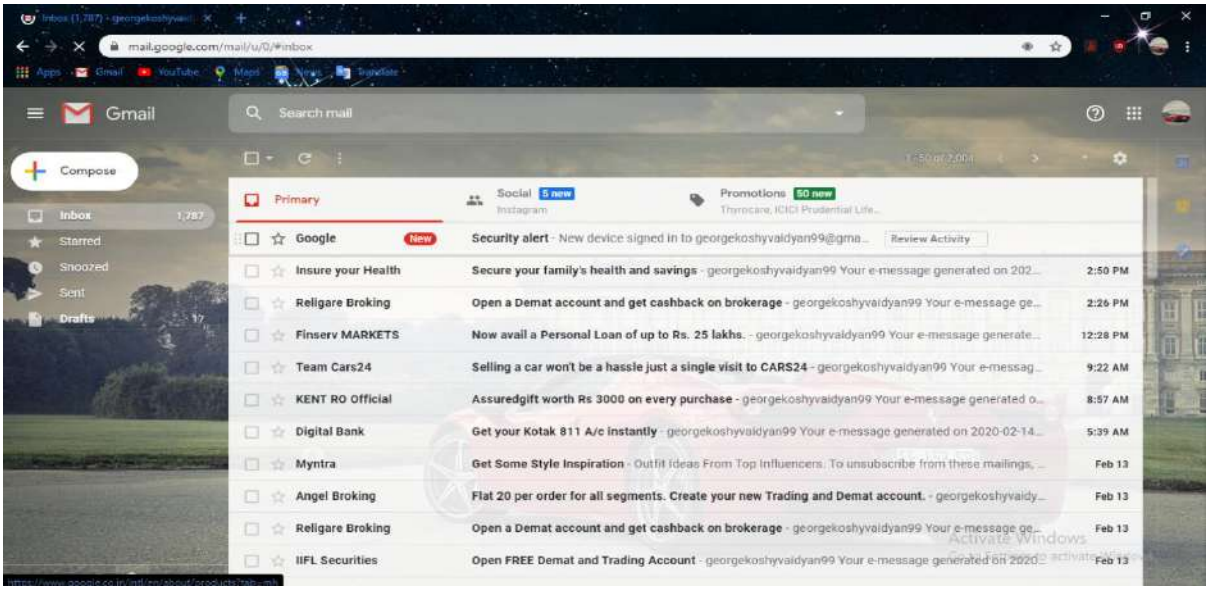


Figure 4.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

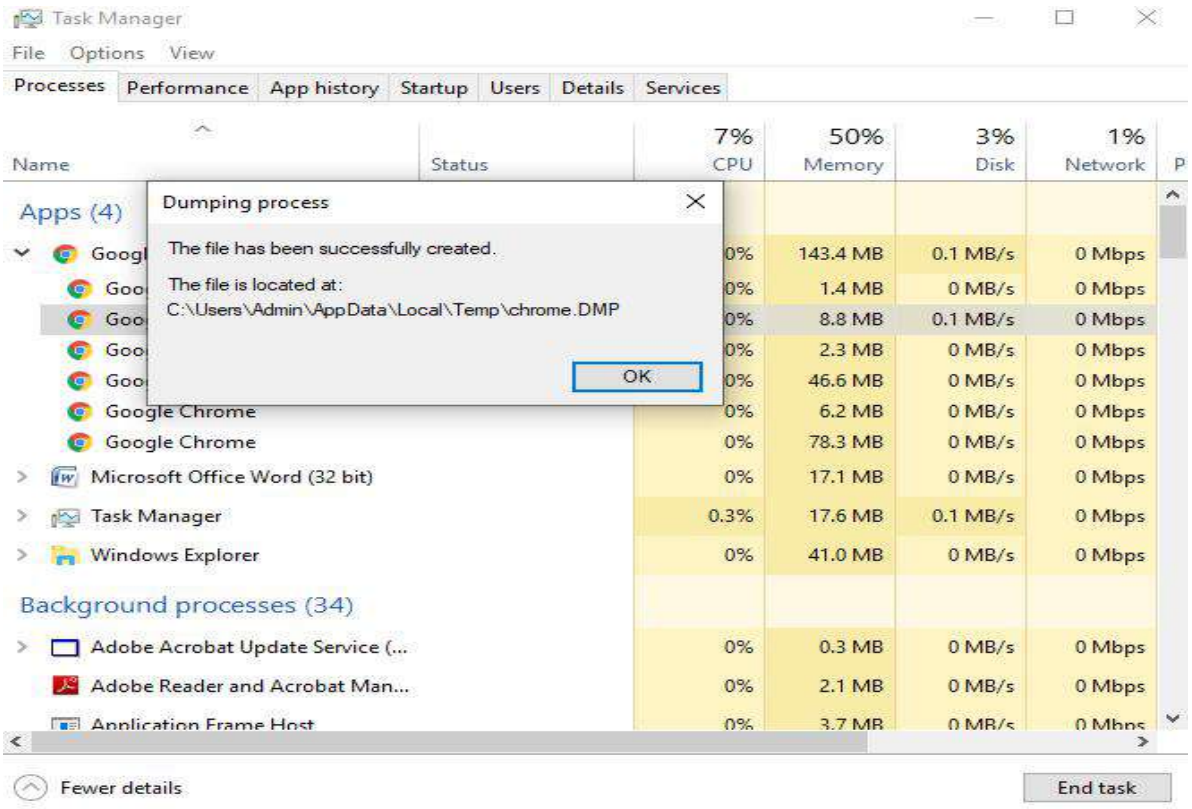


Figure 4.3

Step 4 Locate the Dumpfile in your PC

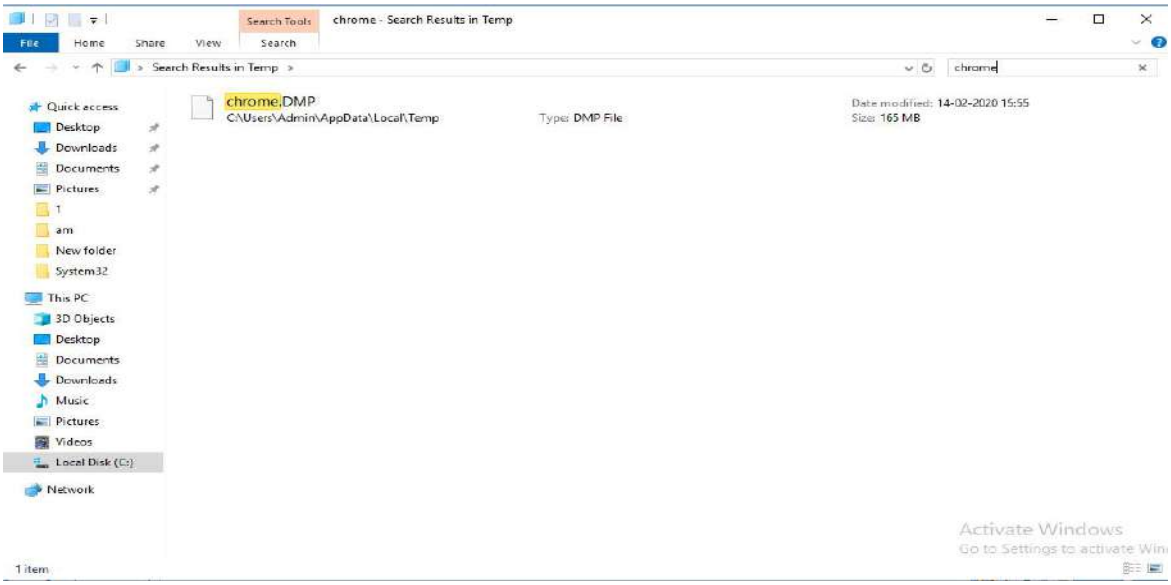


Figure 4. 4

Step 5 Open the specific Dumpfile using WINHEX tool

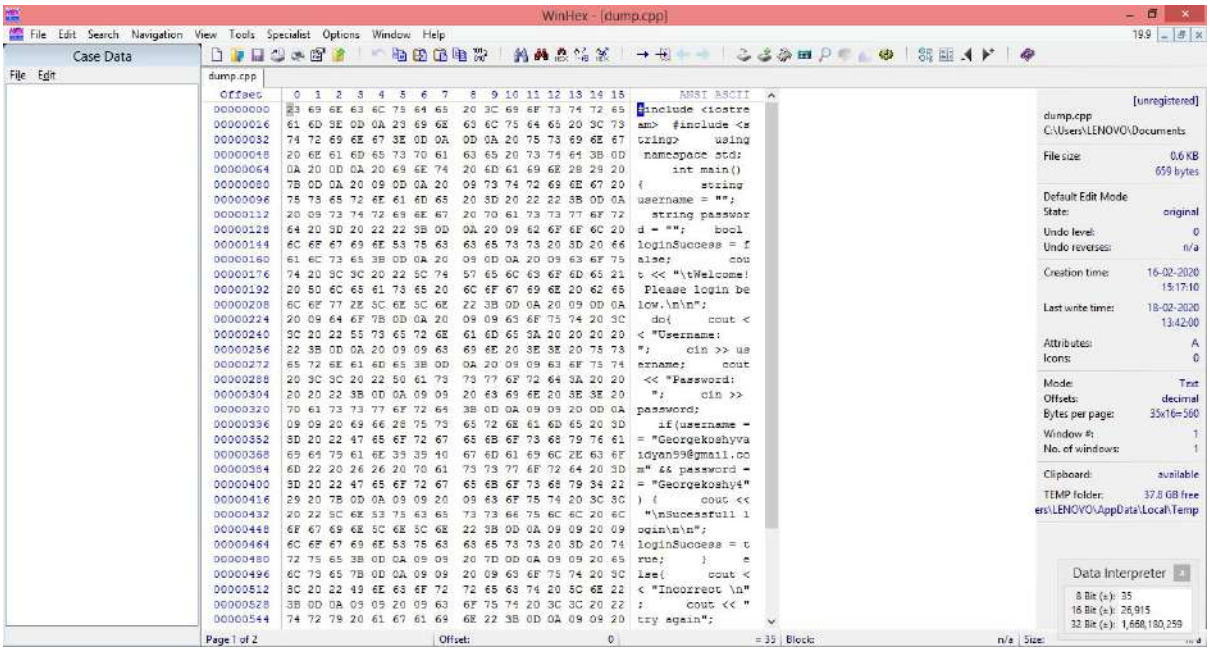


Figure 4.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

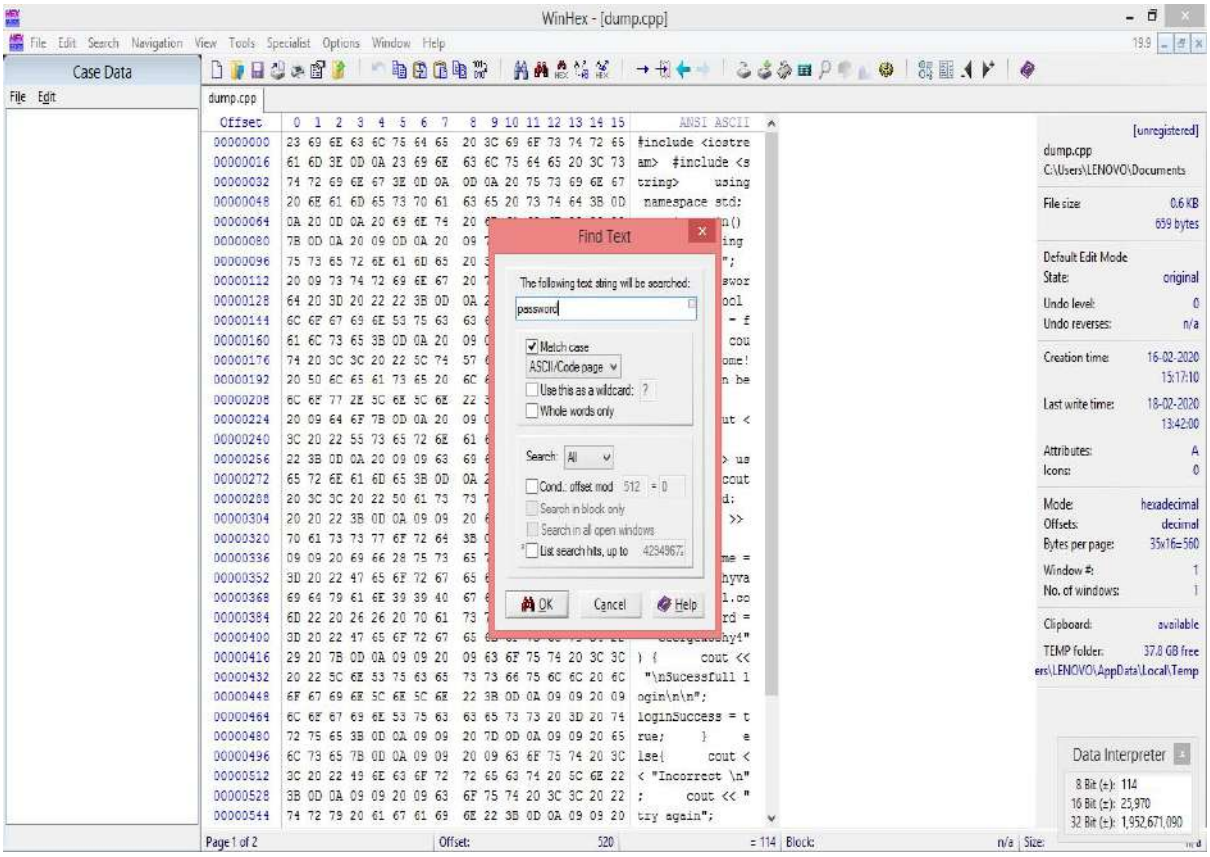


Figure 4.6

Step 7 Click on okay button to see the results

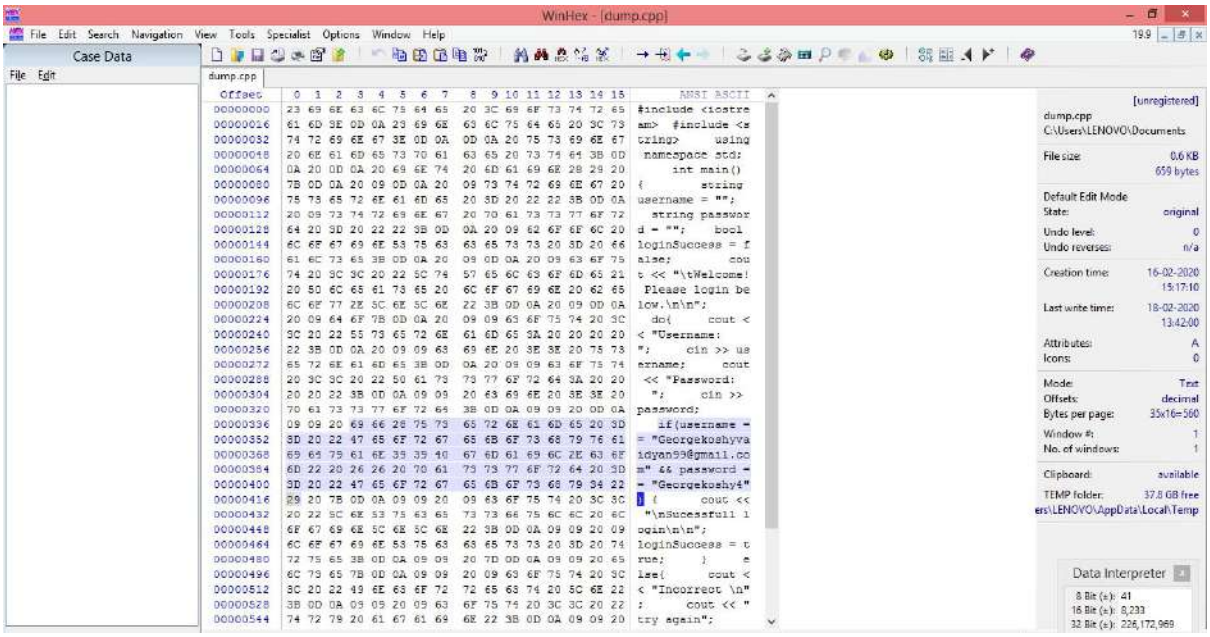


Figure 4.7

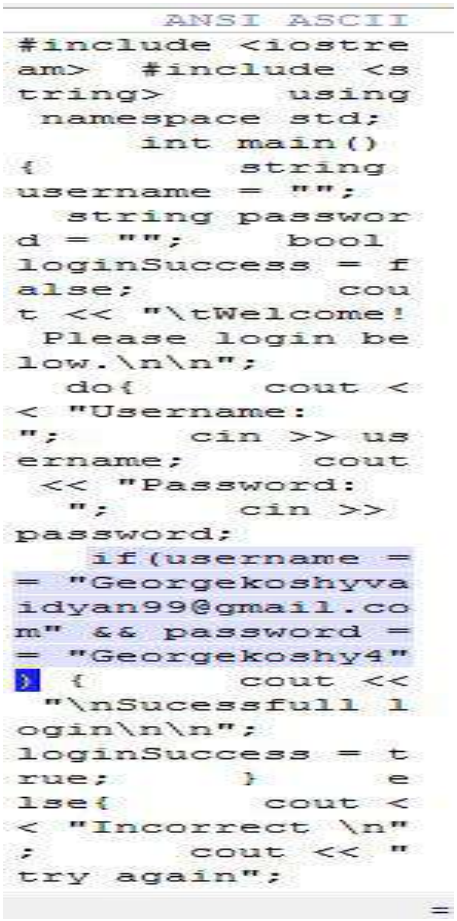


Figure 4.8

Laptop 5: Asus507

Step 1 Take GMAIL in Google Chrome and login using your credentials

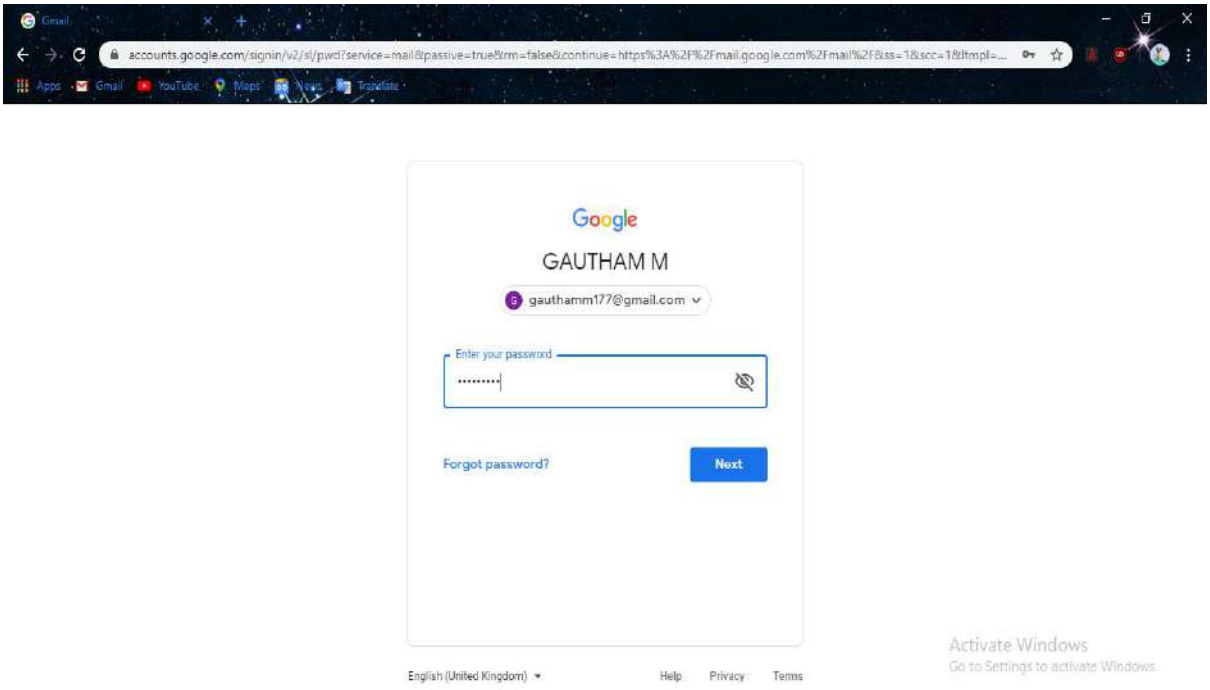


Figure 5.1

Step 2 Login to your account and logout after a minute or two

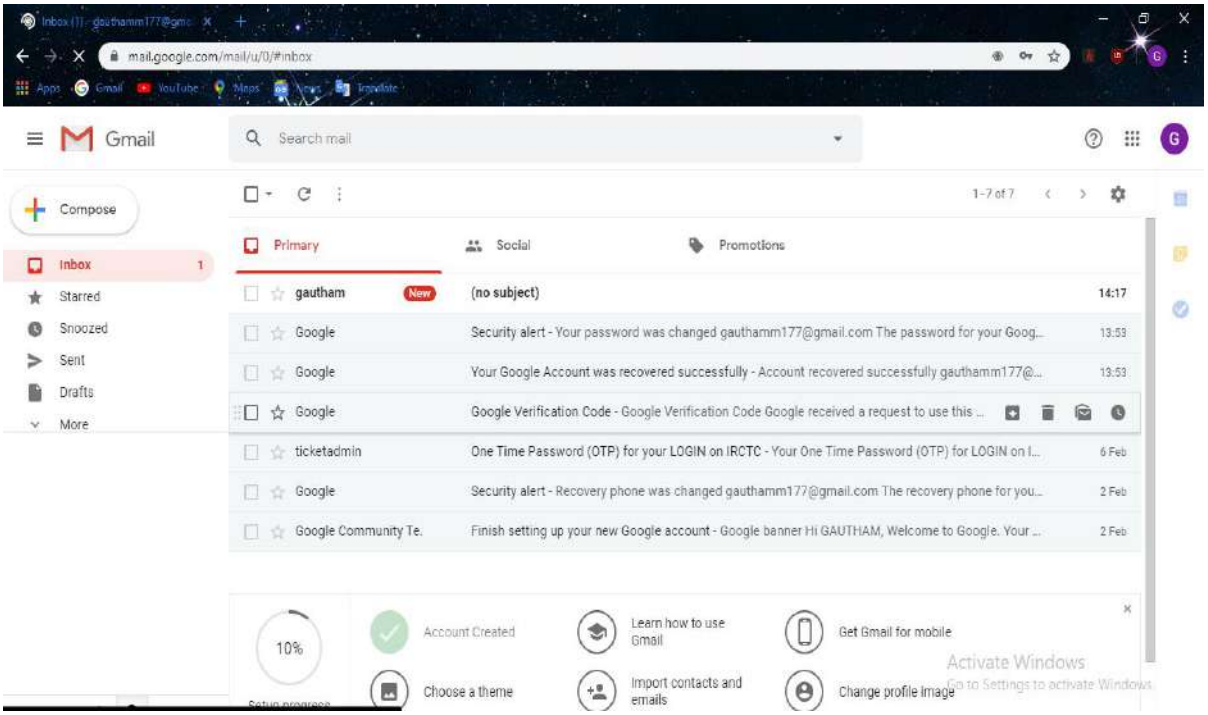


Figure 5.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on ‘Create Dump File’. Within a minute a Dumpfile will be created along with the file path

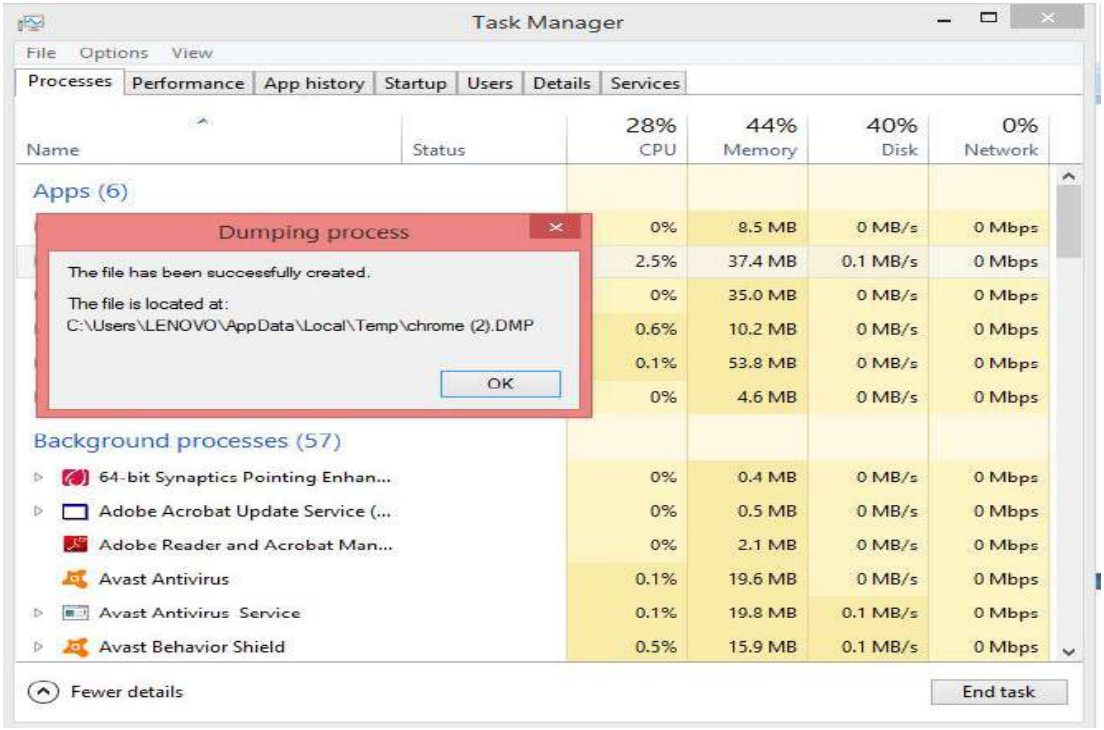


Figure 5.3

Step 4 Locate the Dumpfile in your PC

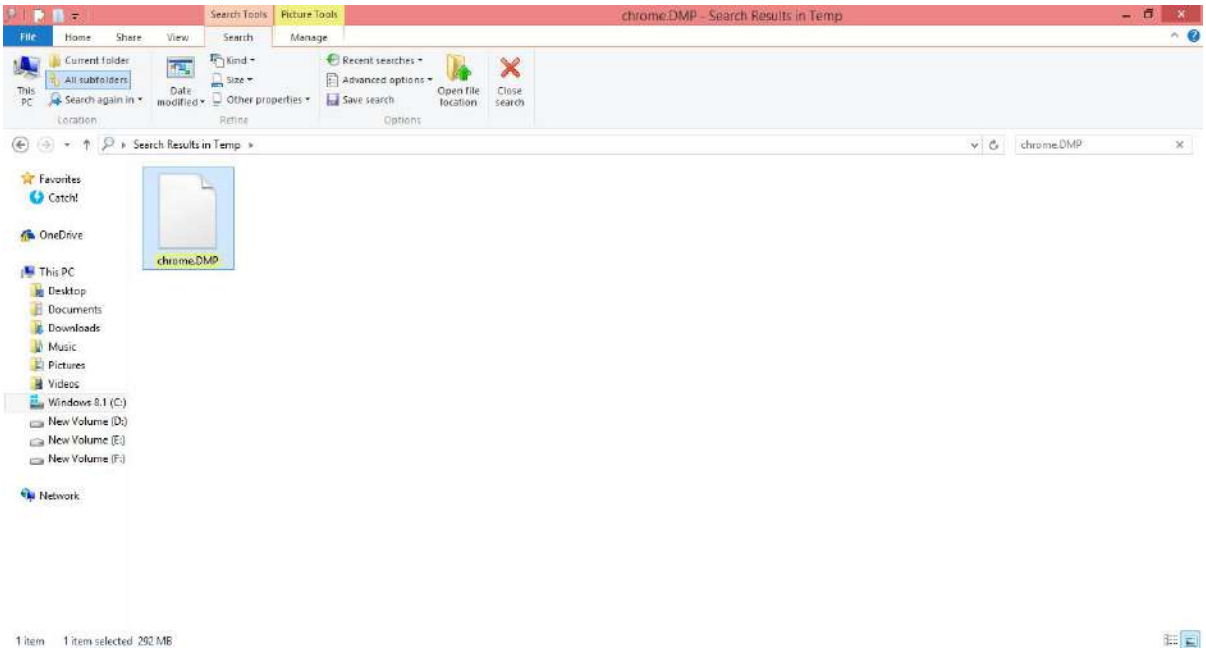


Figure 5.4

Step 5 Open the specific Dumpfile using WINHEX tool

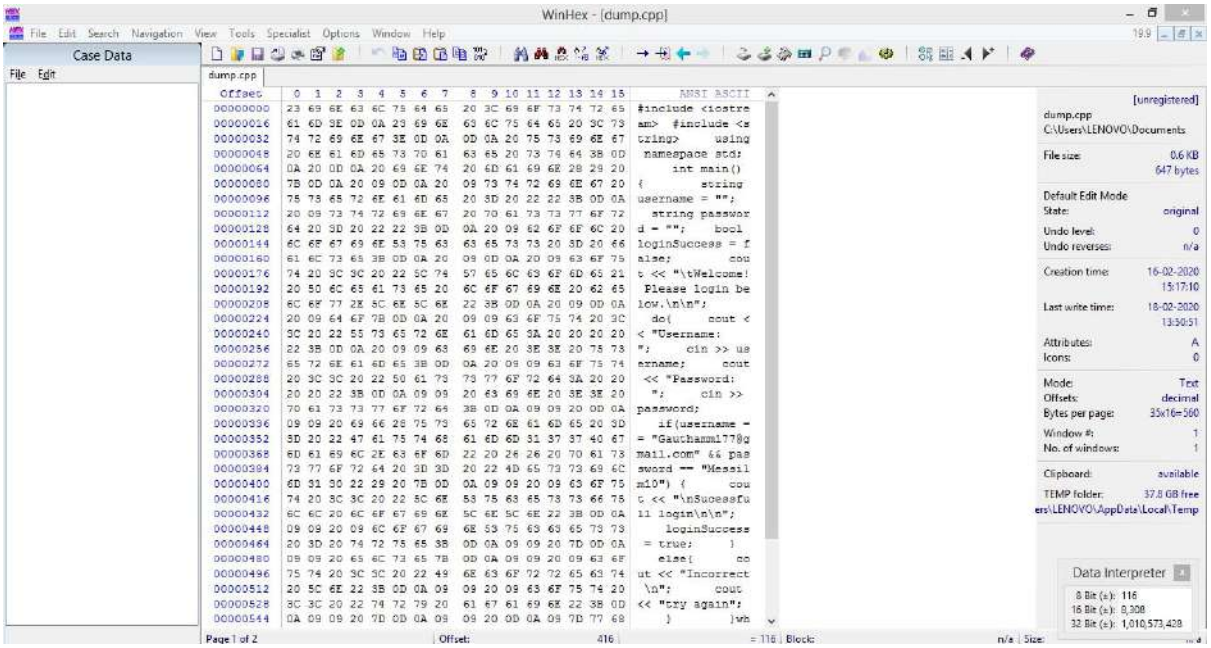


Figure 5.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

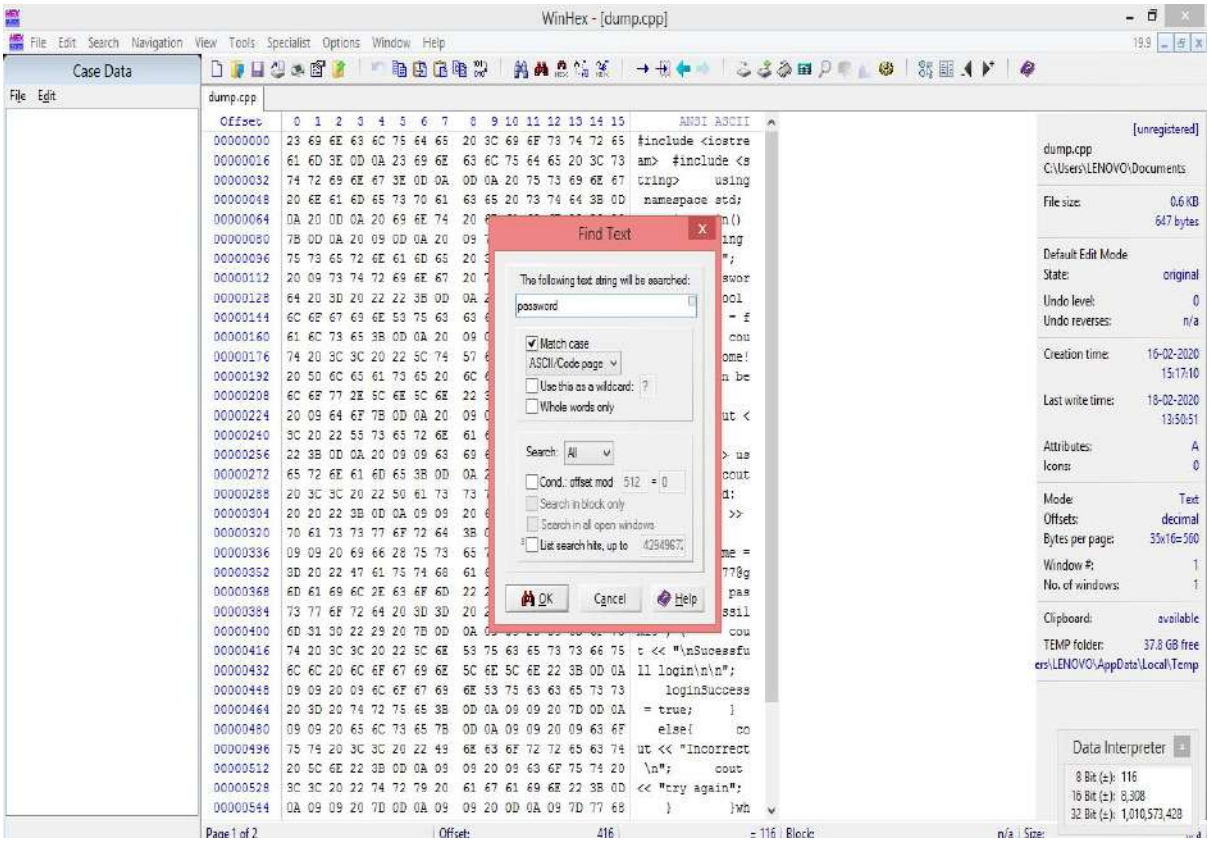


Figure 5.6

Step 7 Click on okay button to see the results

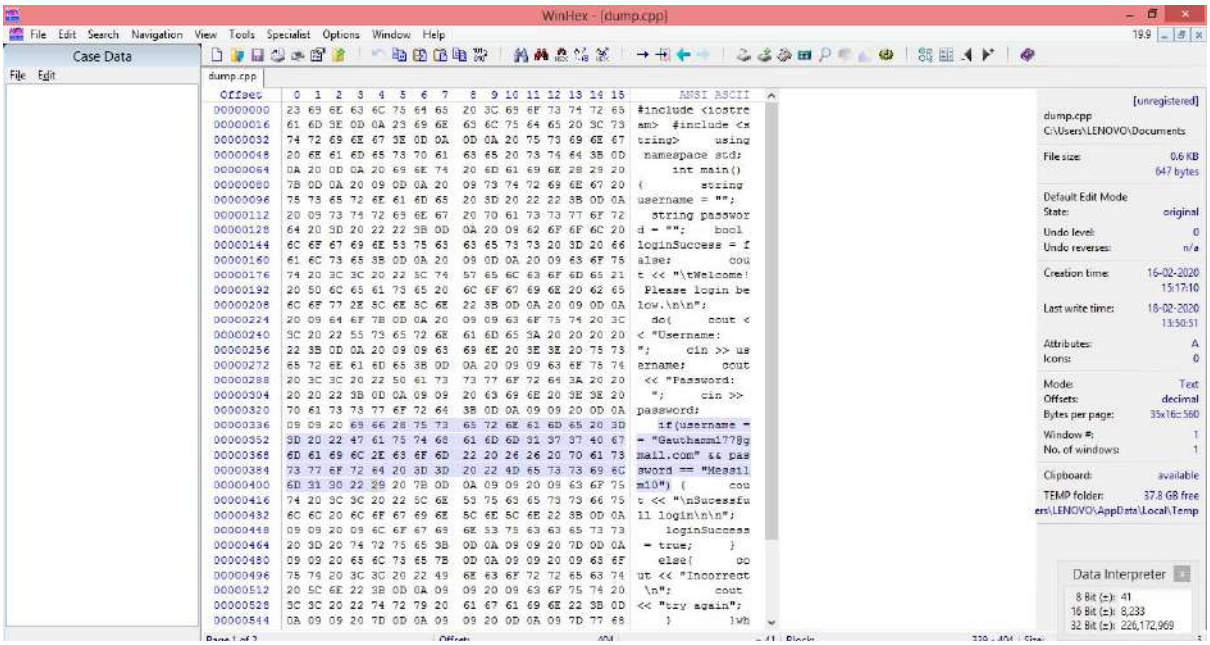


Figure 5.7

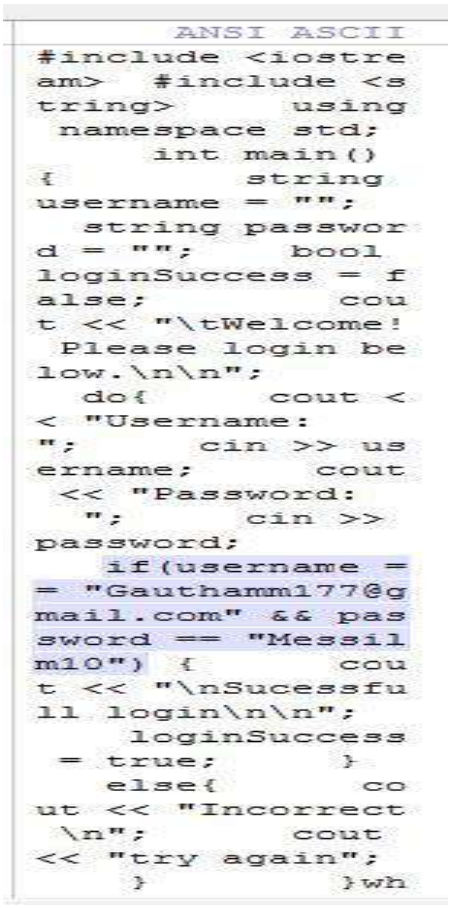


Figure 5.8

Laptop 6: Dell Inspiron 5755

Step 1 Take GMAIL in Google Chrome and login using your credentials

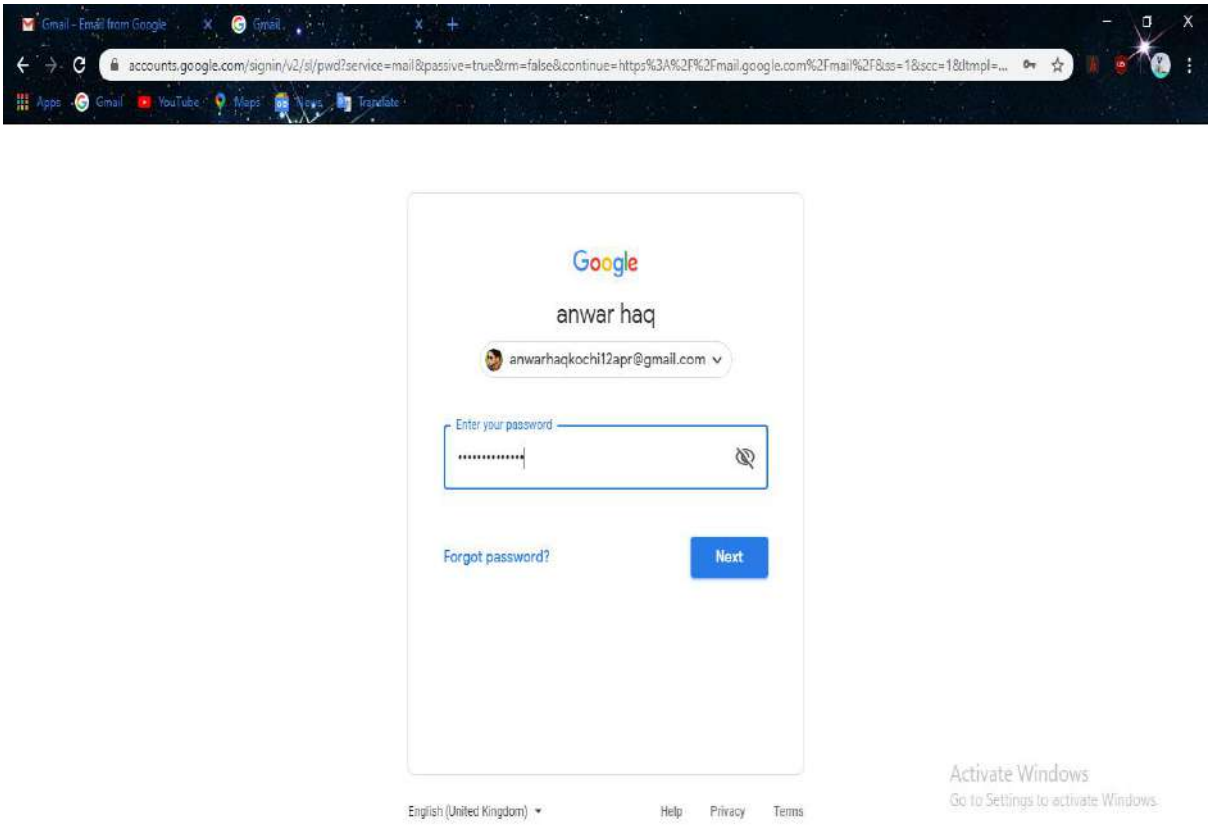


Figure 6.1

Step 2 Login to your account and logout after a minute or two

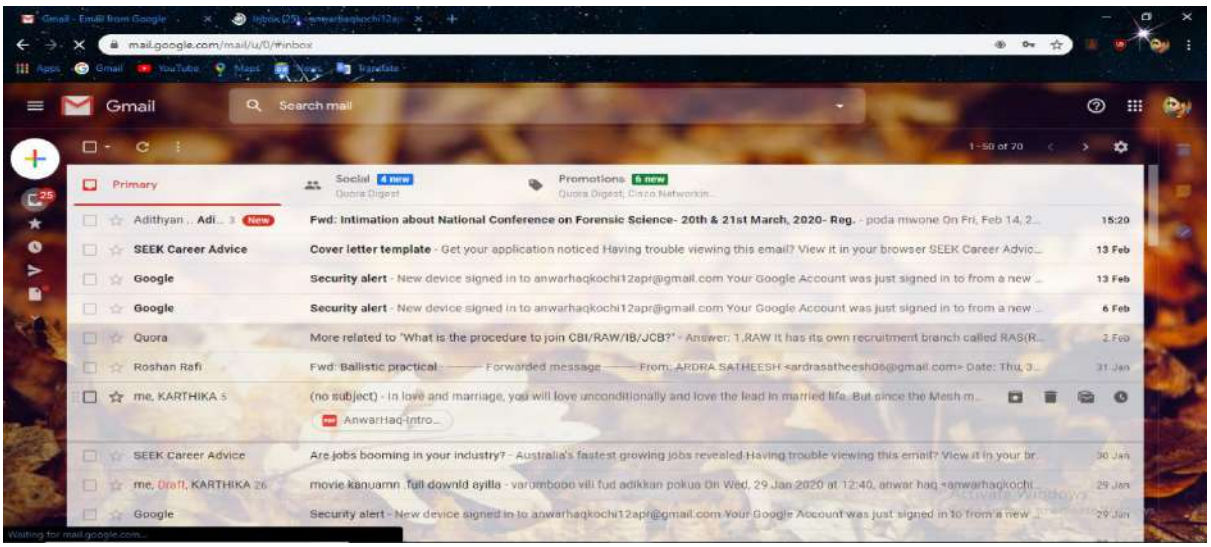


Figure 6.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

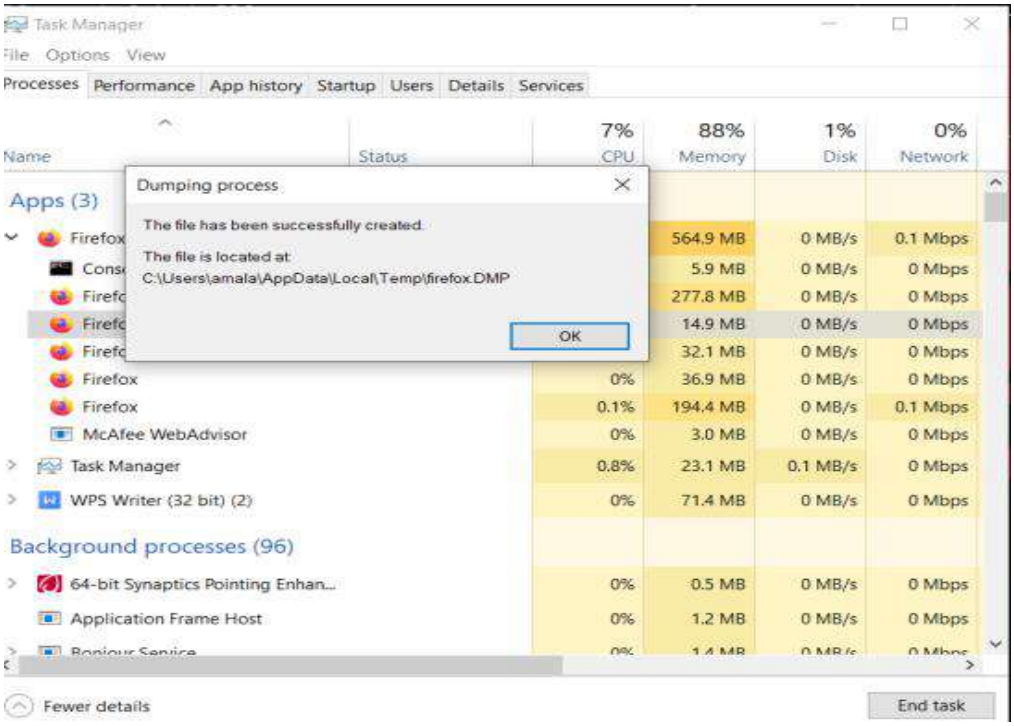


Figure 6.3

Step 4 Locate the Dumpfile in your PC

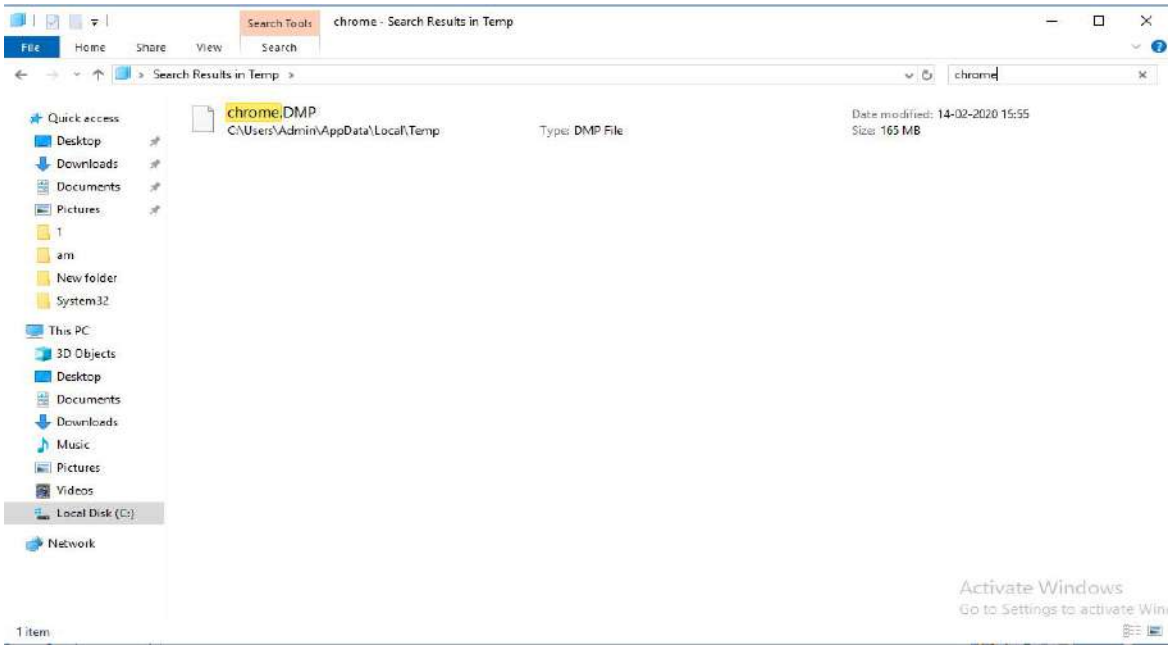


Figure 6.4

Step 5 Open the specific Dumpfile using WINHEX tool

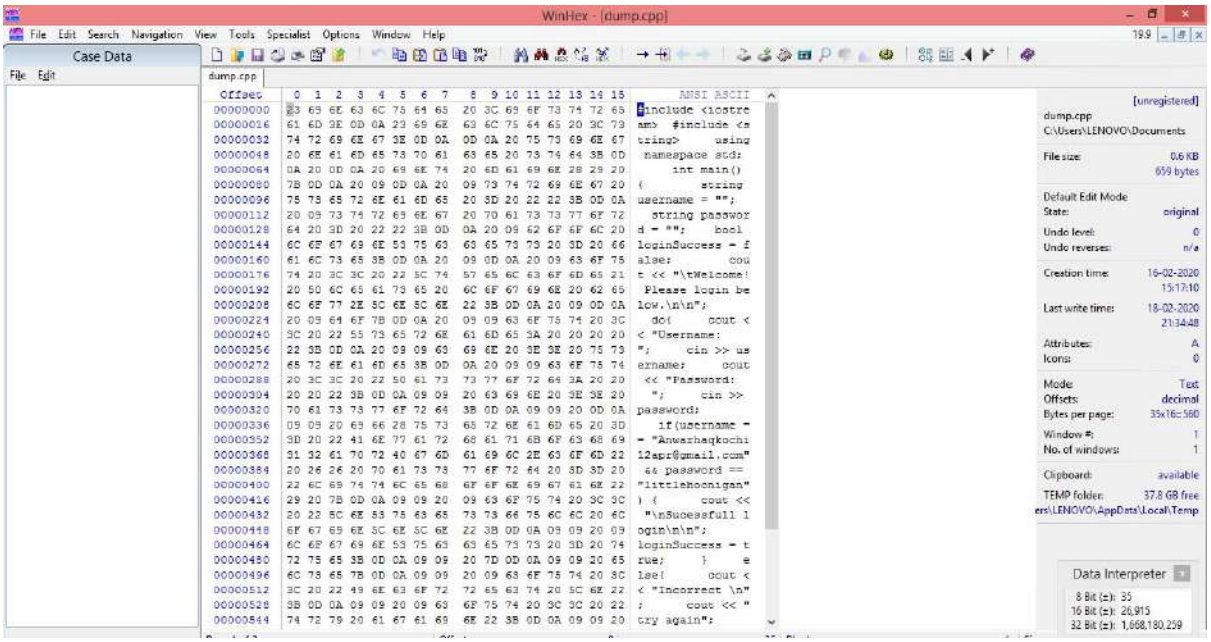


Figure 6.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

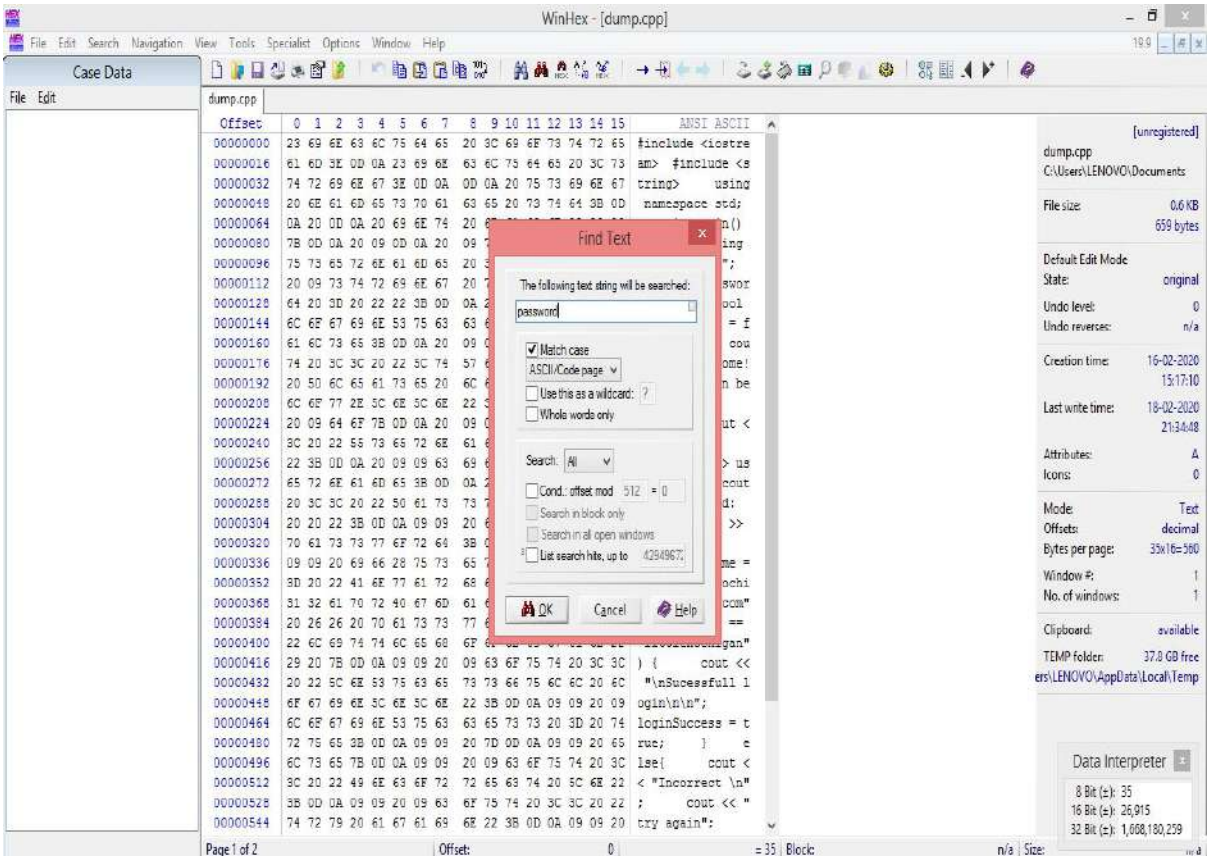


Figure 6.6

Step 7 Click on okay button to see the results

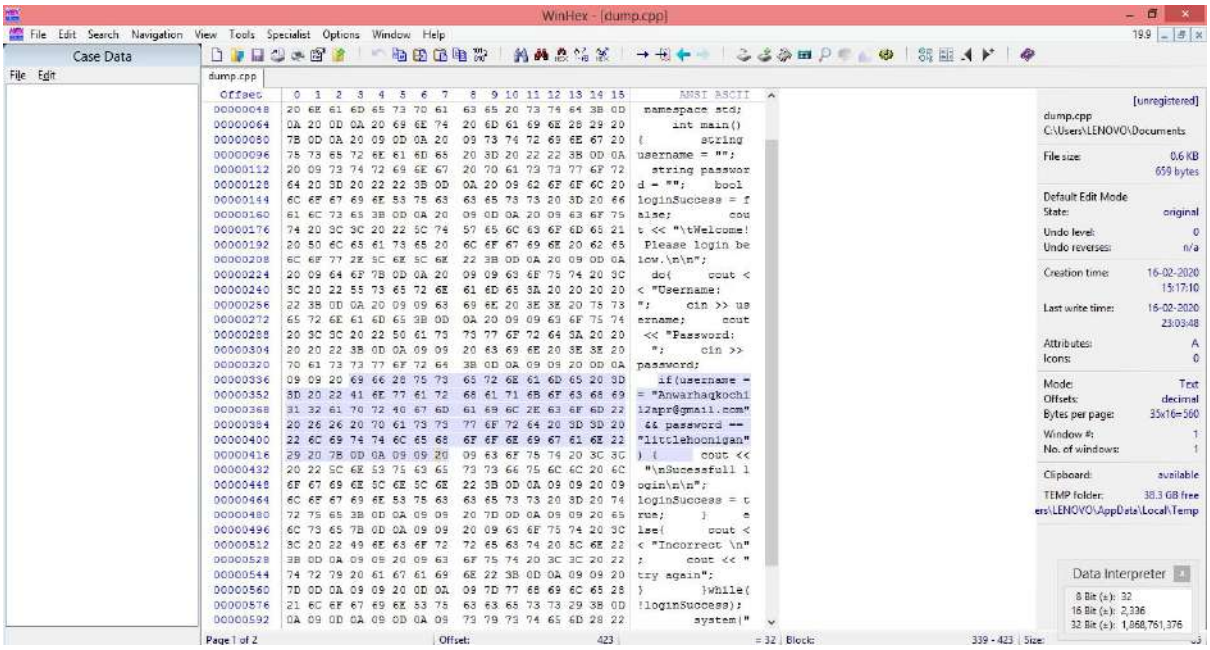


Figure 6.7

```
        ANSI ASCII
  namespace std;
       int main()
{          string
username = "";
   string passwor
d = "";      bool
loginSuccess = f
alse;          cou
t << "\tWelcome!
  Please login be
low.\n\n";
   do{       cout <
< "Username:
";      cin >> us
ername;      cout
  << "Password:
   ";       cin >>
password;
    if(username =
= "Anwarhaqkochi
12apr@gmail.com"
  && password ==
"littlehoonigan"
) {       cout <<
  "\nSucessfull l
ogin\n\n";
loginSuccess = t
rue;       }      e
lse{        cout <
< "Incorrect \n"
;       cout << "
try again";
}          }while(
!loginSuccess);
          system("
```

Figure 6.8

Laptop 7: Acer aspire 3

Step 1 Take GMAIL in Google Chrome and login using your credentials

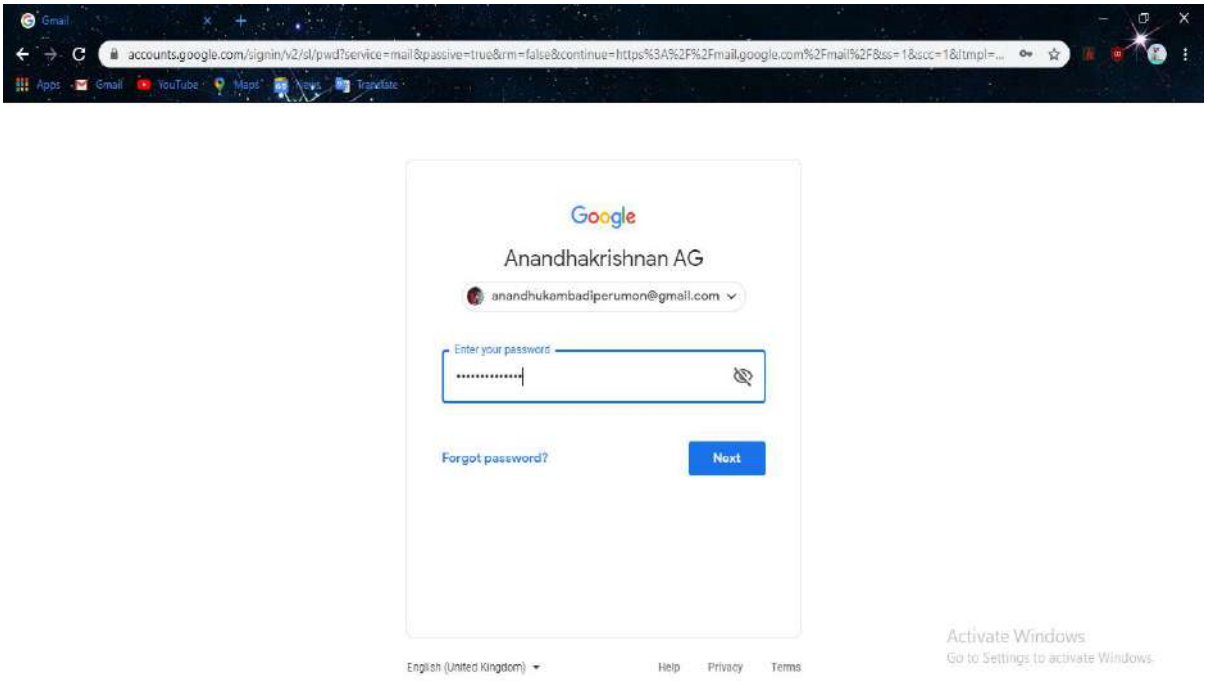


Figure 7.1

Step 2 Login to your account and logout after a minute or two

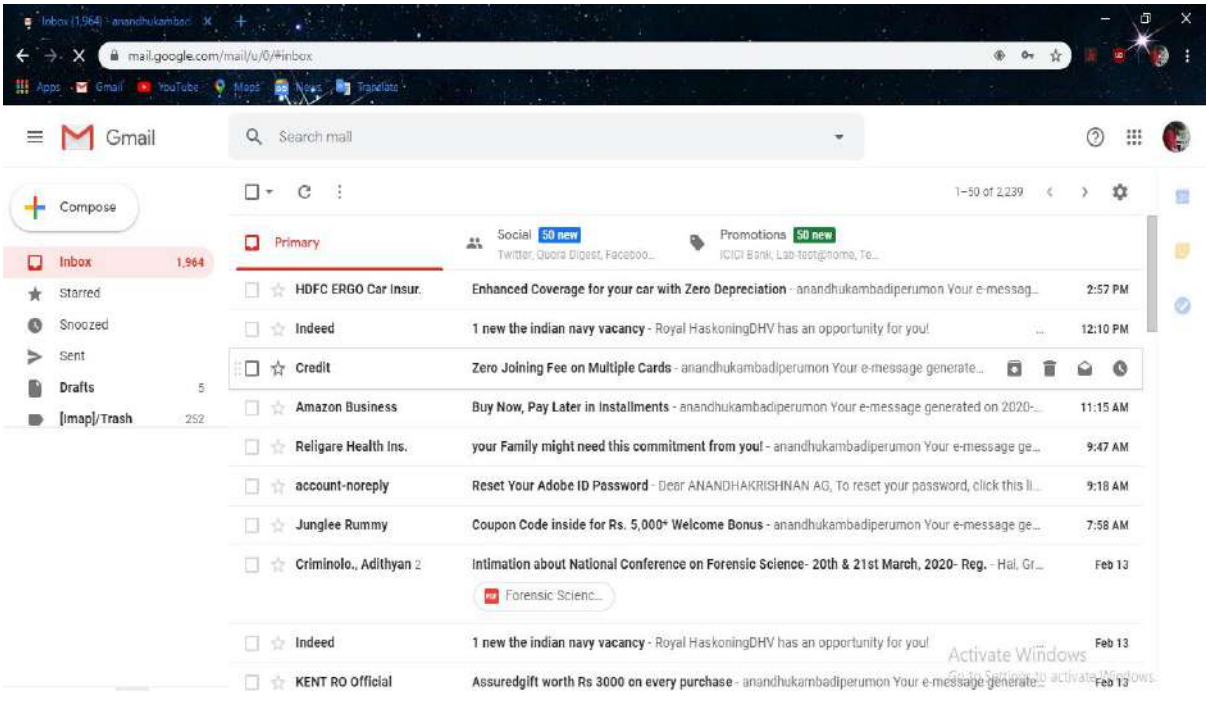


Figure 7.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

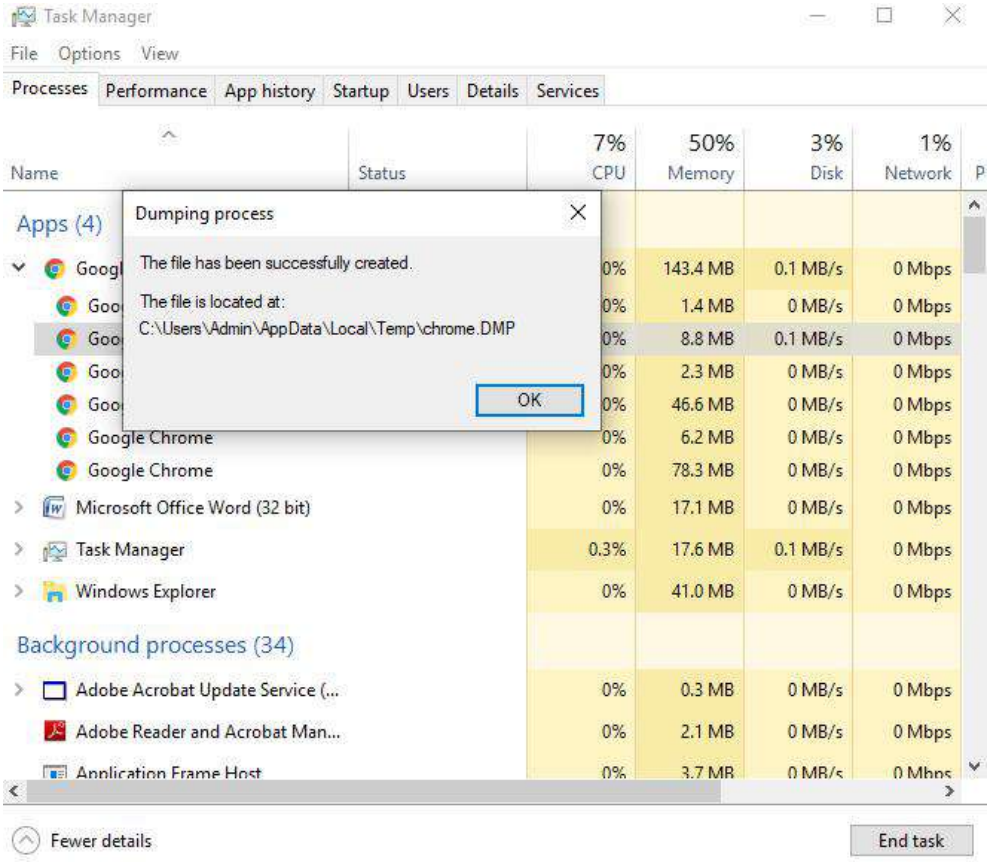


Figure 7.3

Step 4 Locate the Dumpfile in your PC

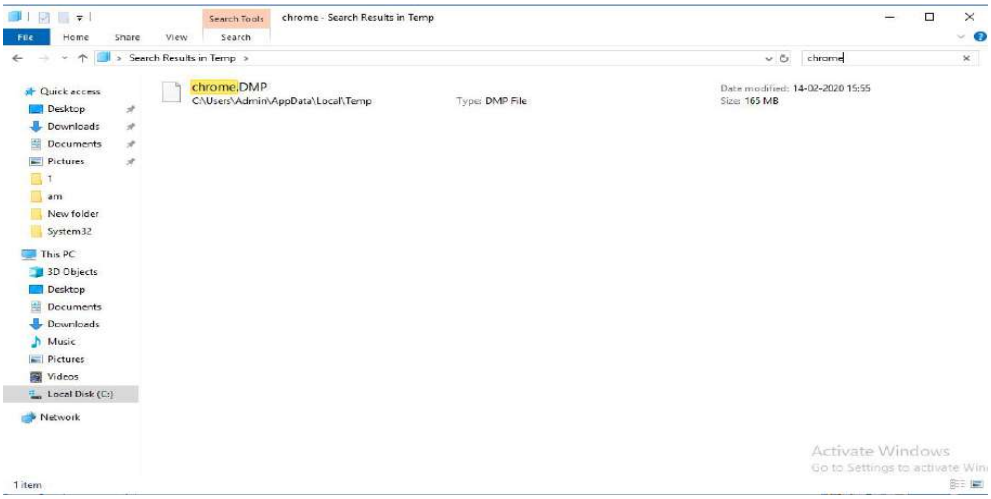


Figure 7.4

Step 5 Open the specific Dumpfile using WINHEX tool

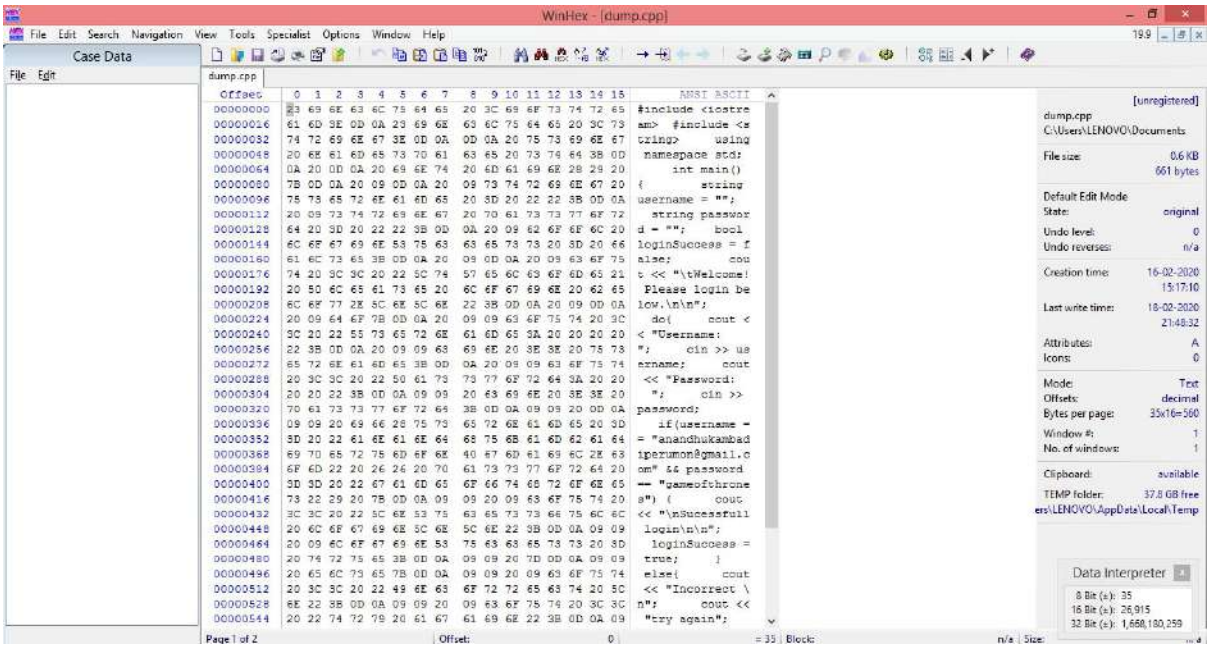


Figure 7.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

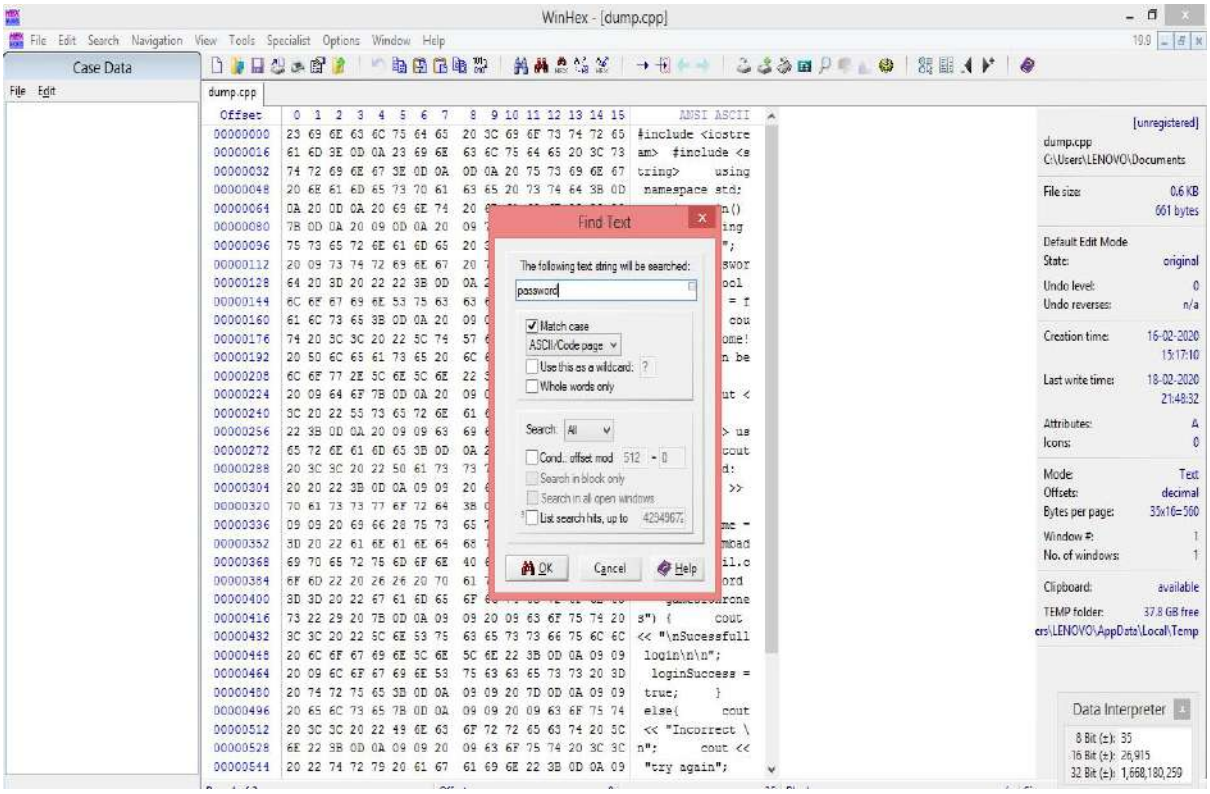


Figure 7.6

Step 7 Click on okay button to see the results

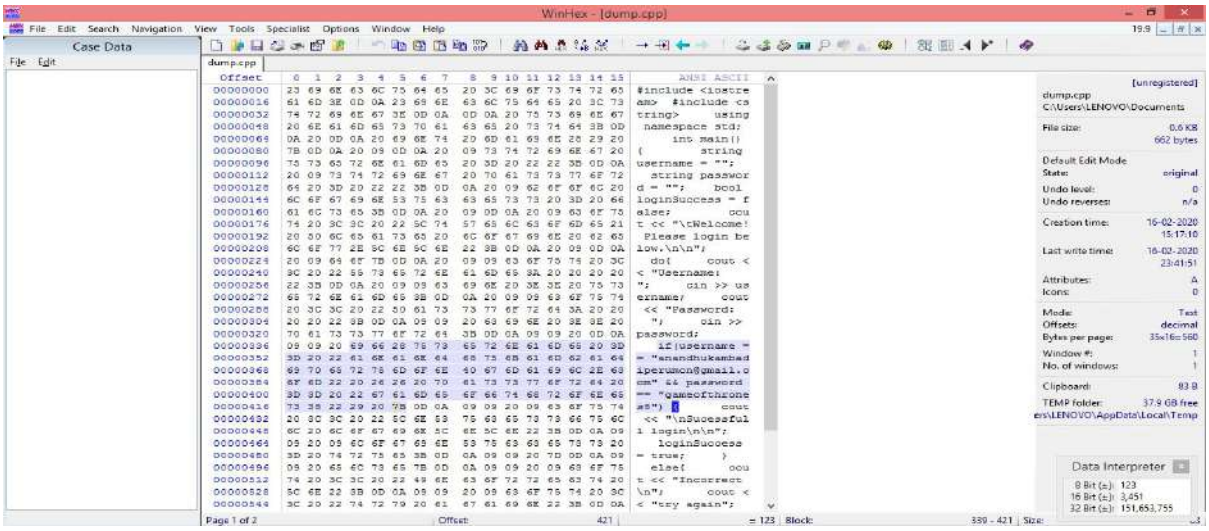


Figure 7.7

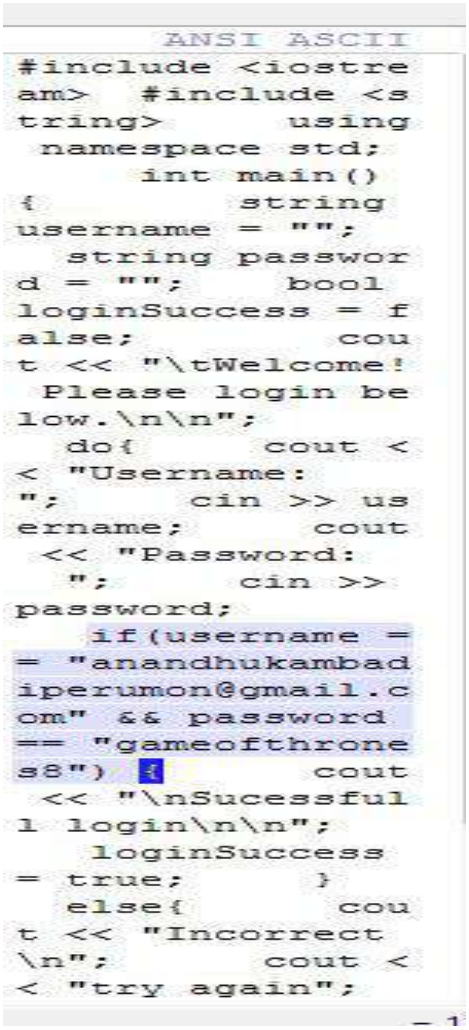


Figure 7.8

Laptop 8: Iball marvel 2

Step 1 Take FLIPKART in Google Chrome and login using your credentials

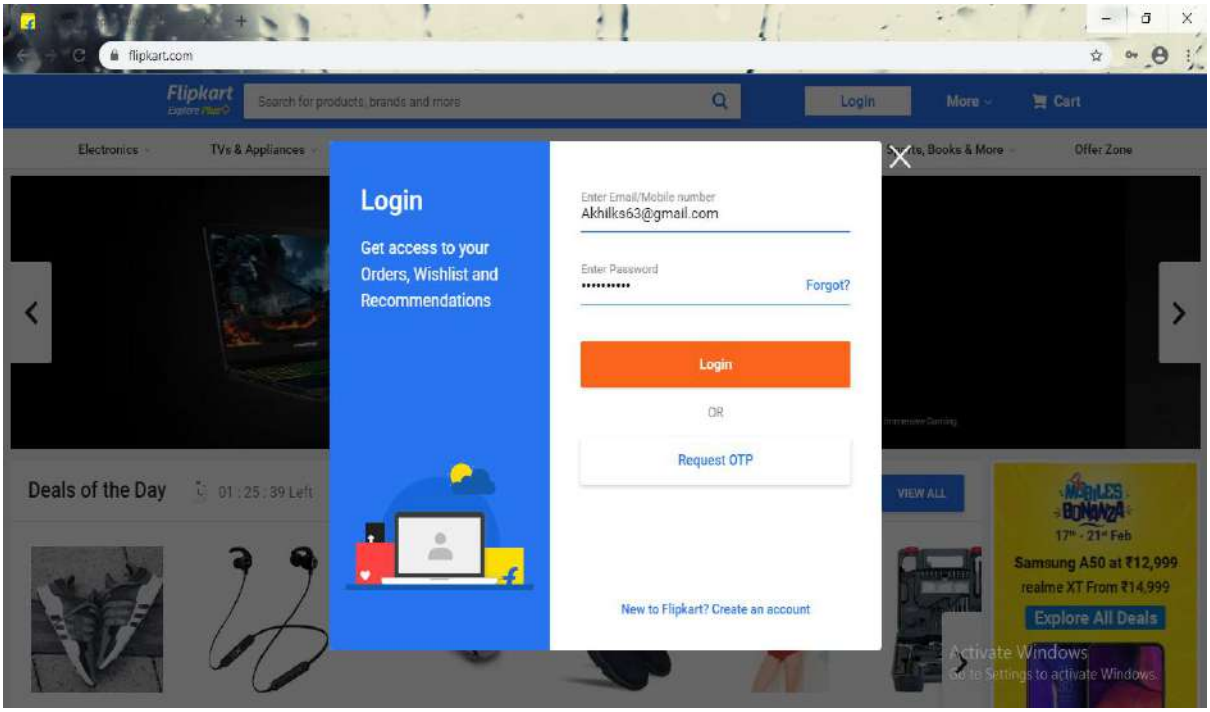


Figure 8.1

Step 2 Login to your account and logout after a minute or two

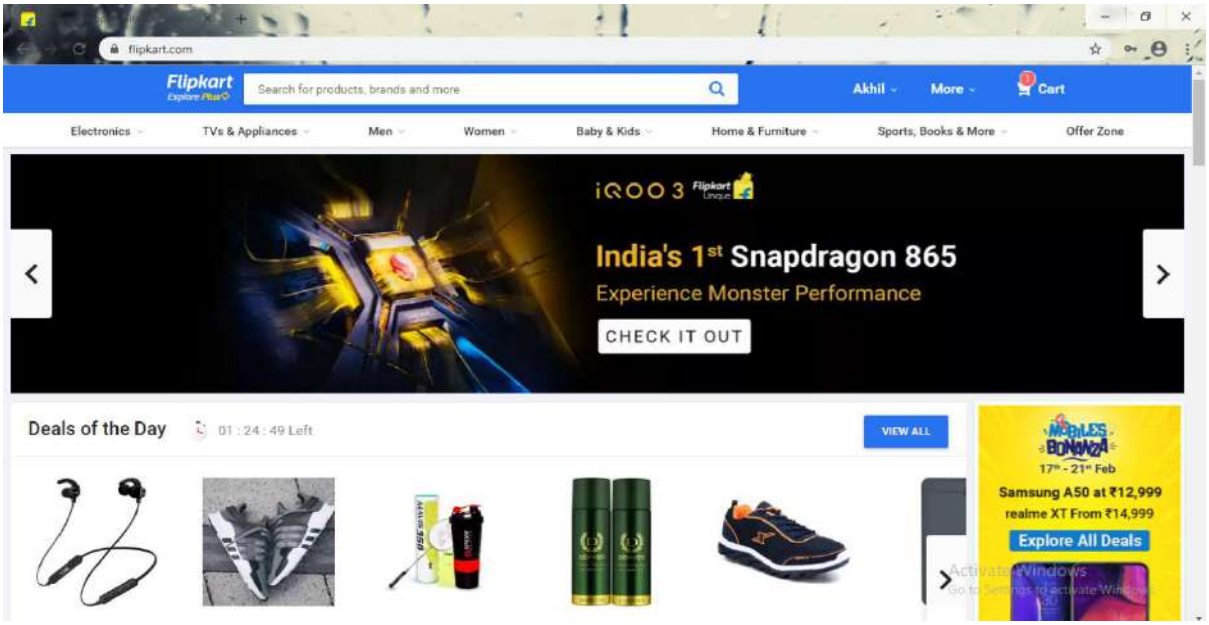


Figure 8.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

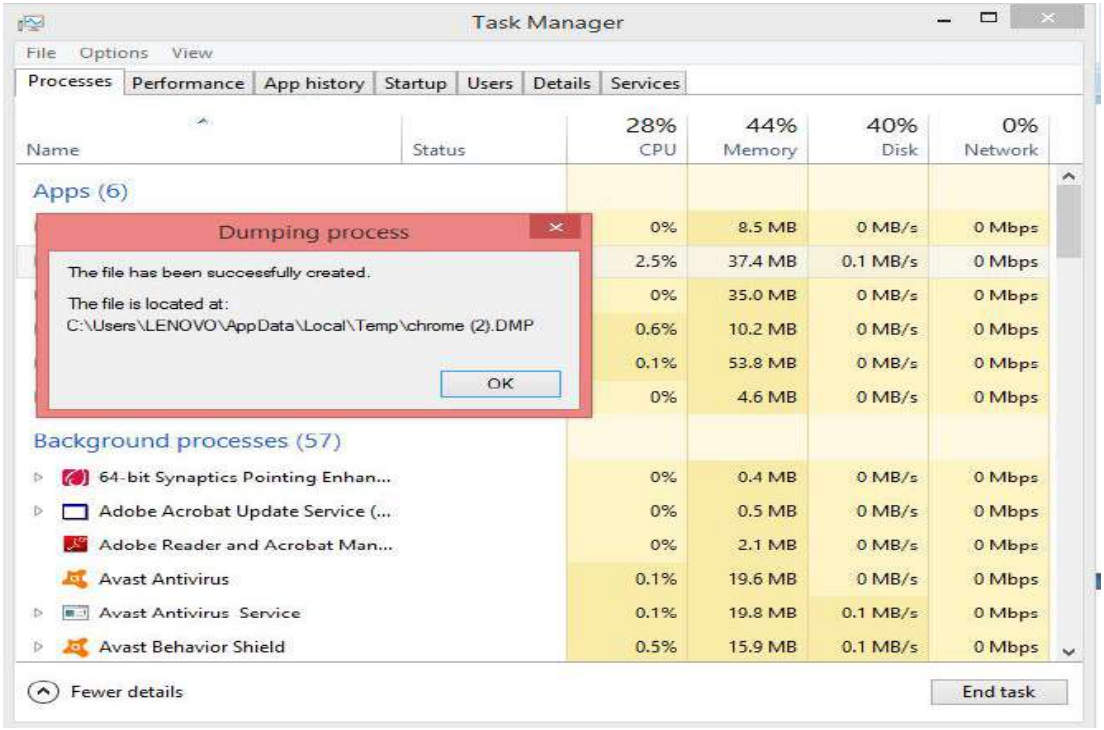


Figure 8.3

Step 4 Locate the Dumpfile in your PC

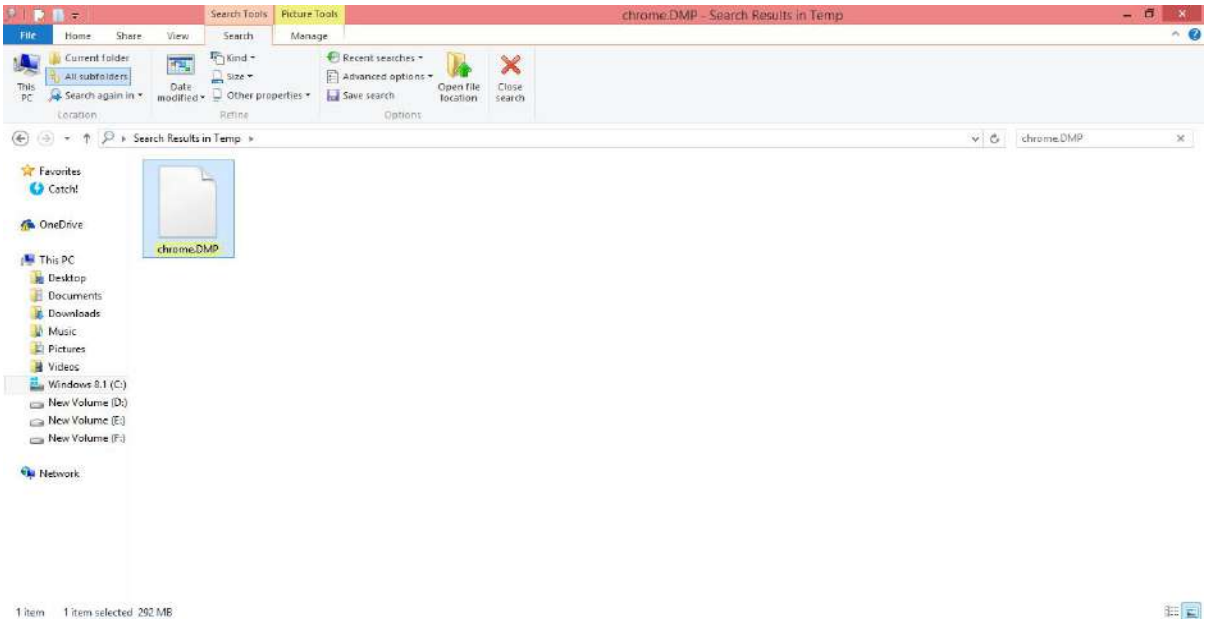


Figure 8.4

Step 5 Open the specific Dumpfile using WINHEX tool

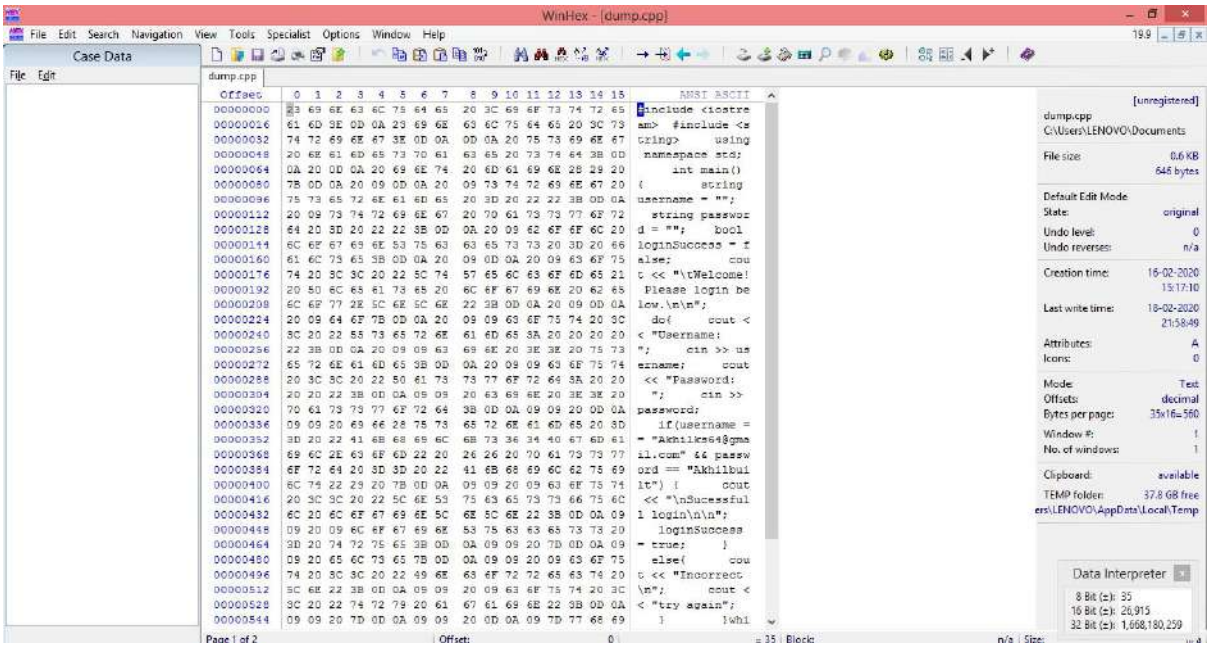


Figure 8.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

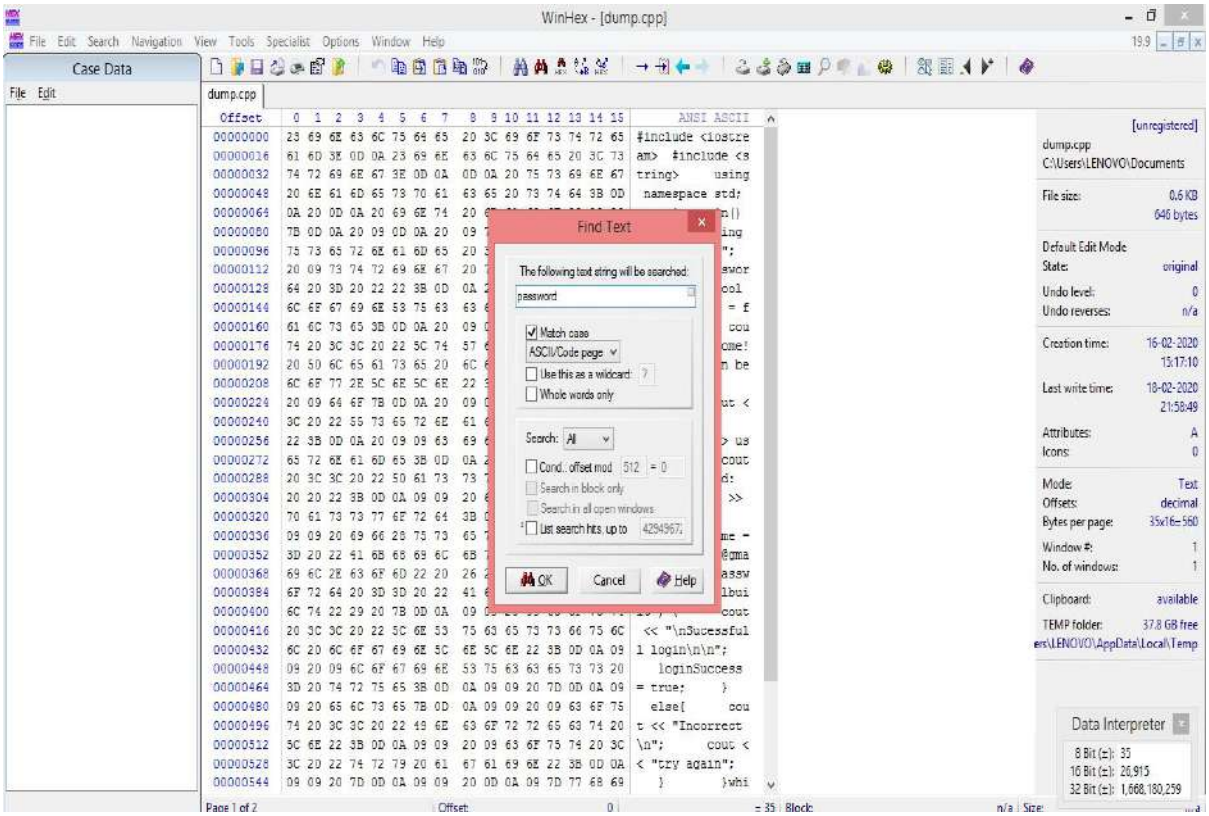


Figure 8.6

Step 7 Click on okay button to see the results

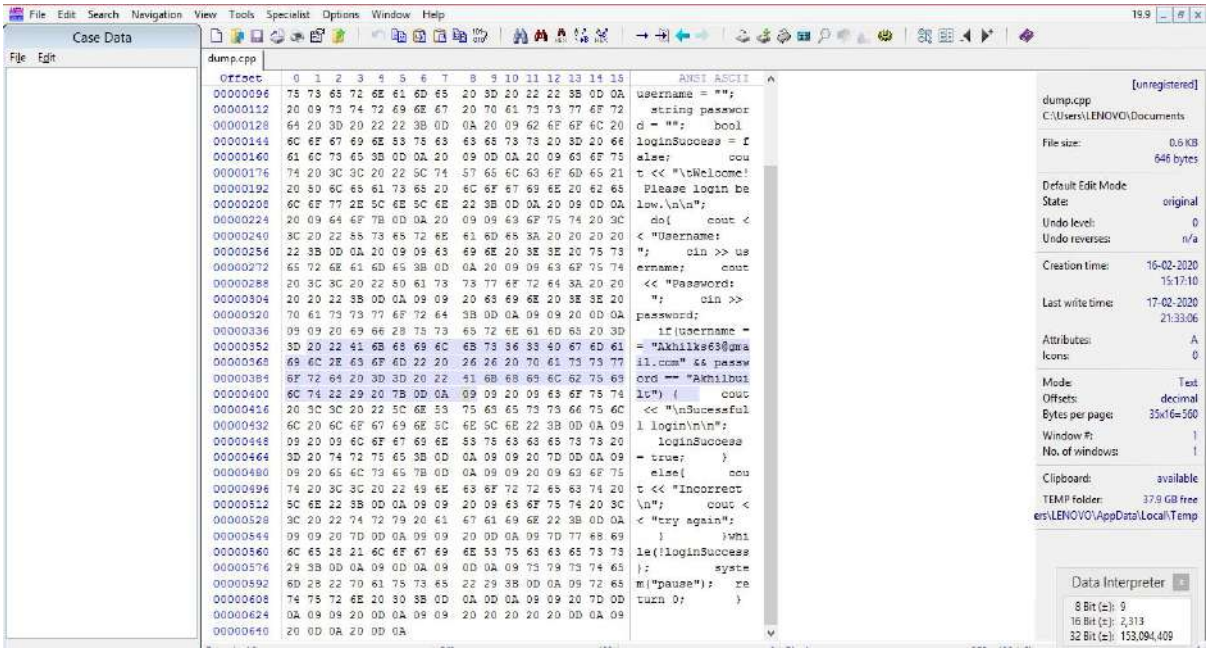
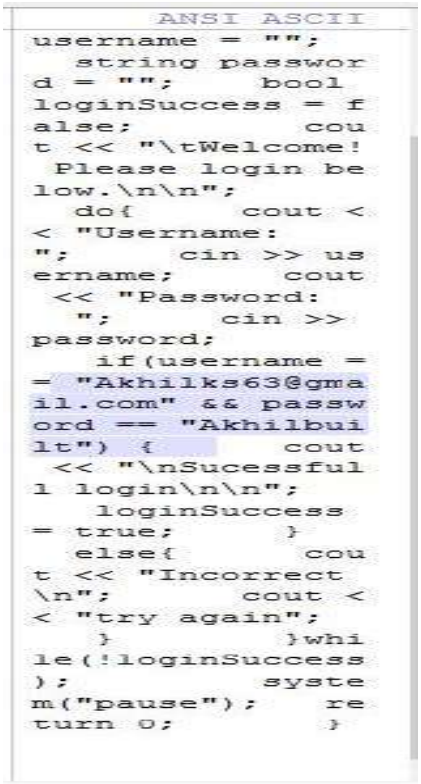


Figure 8.7



```
      ANSI ASCII
username = "";
   string passwor
d = "";     bool
loginSuccess = f
alse;          cou
t << "\tWelcome!
 Please login be
low.\n\n";
   do{      cout <
< "Username:
";      cin >> us
ername;      cout
 << "Password:
  ";      cin >>
password;
    if(username =
= "Akhilks63@gma
il.com" && passw
ord == "Akhilbui
lt") {      cout
 << "\nSucessful
l login\n\n";
    loginSuccess
= true;      }
   else{       cou
t << "Incorrect
\n";      cout <
< "try again";
    }          }whi
le(!loginSuccess
);          syste
m("pause");    re
turn 0;         }
```

Figure 8.8

Laptop 9: Acer aspire 5s

Step 1 Take GMAIL in Google Chrome and login using your credentials

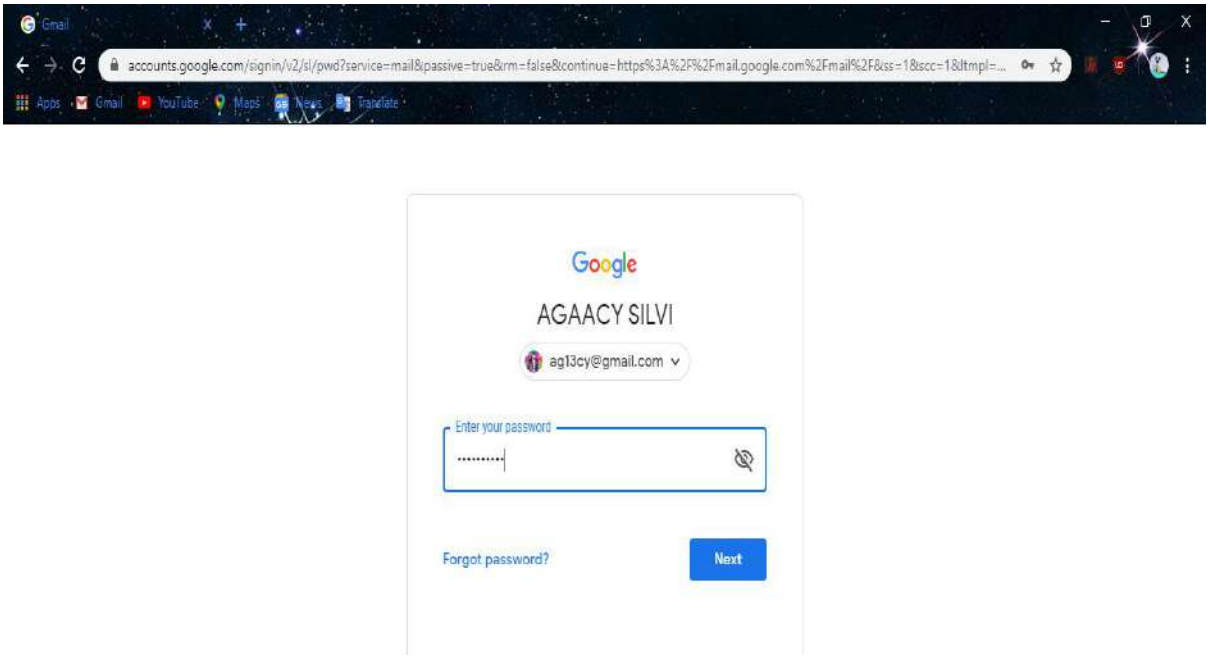


Figure 9.1

Step 2 Login to your account and logout after a minute or two

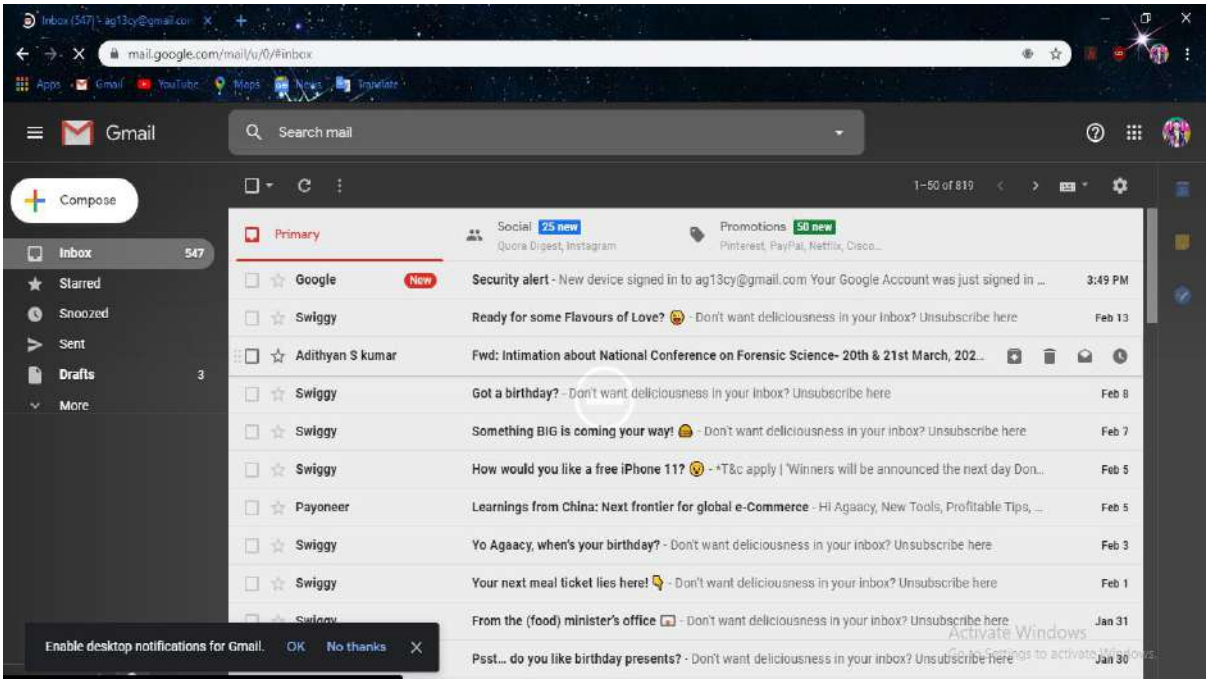


Figure 9.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on 'Create Dump File'. Within a minute a Dumpfile will be created along with the file path

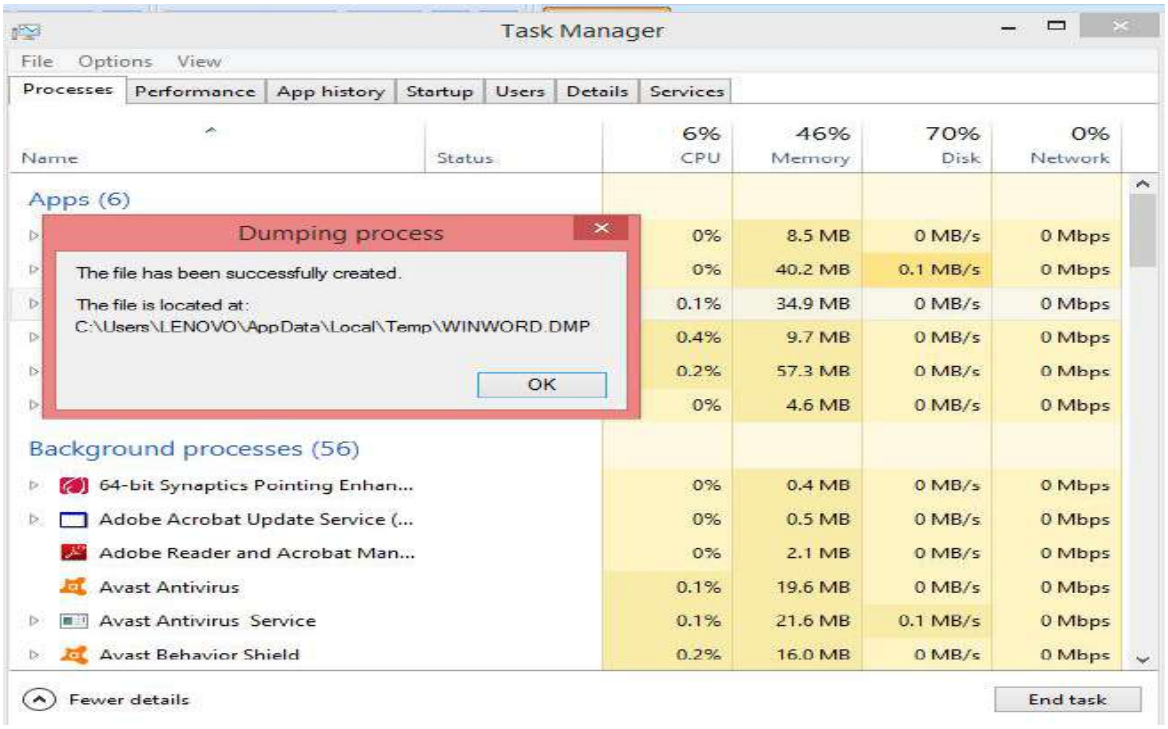


Figure 9.3

Step 4 Locate the Dumpfile in your PC

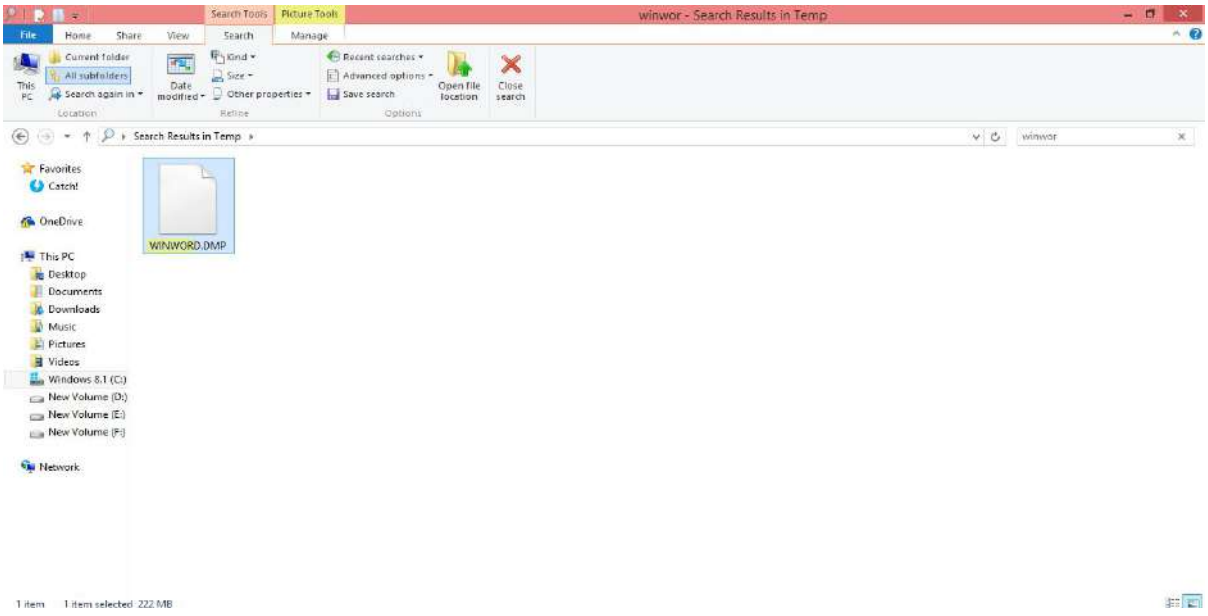


Figure 9.4

Step 5 Open the specific Dumpfile using WINHEX tool

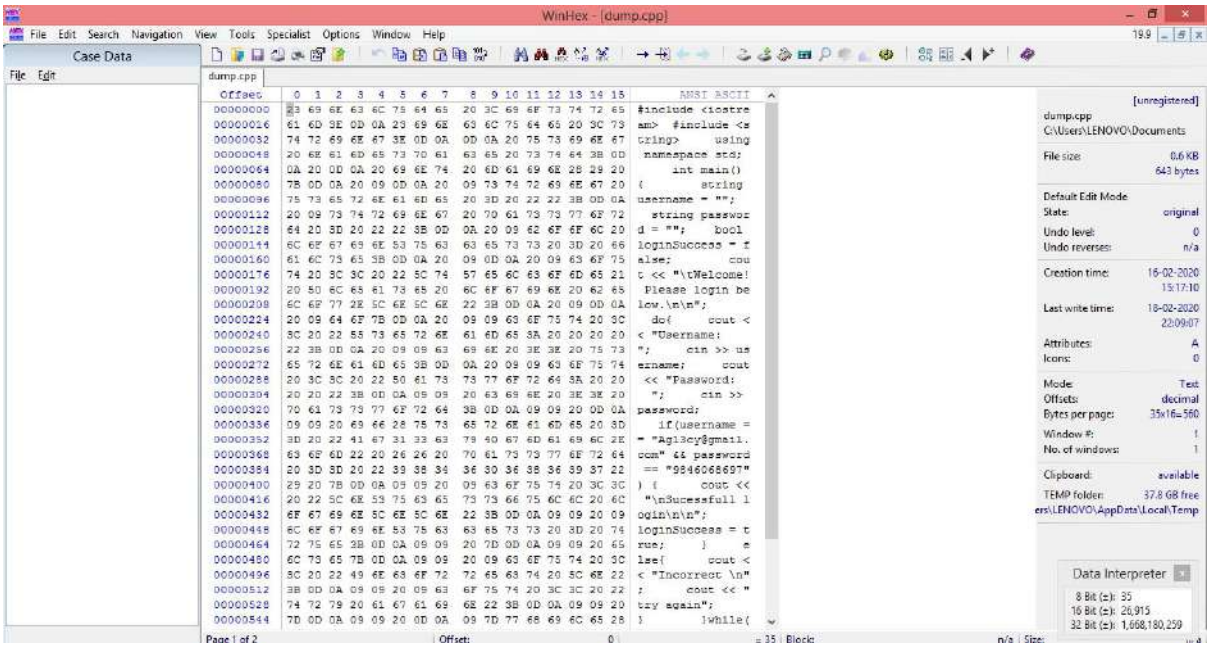


Figure 9.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

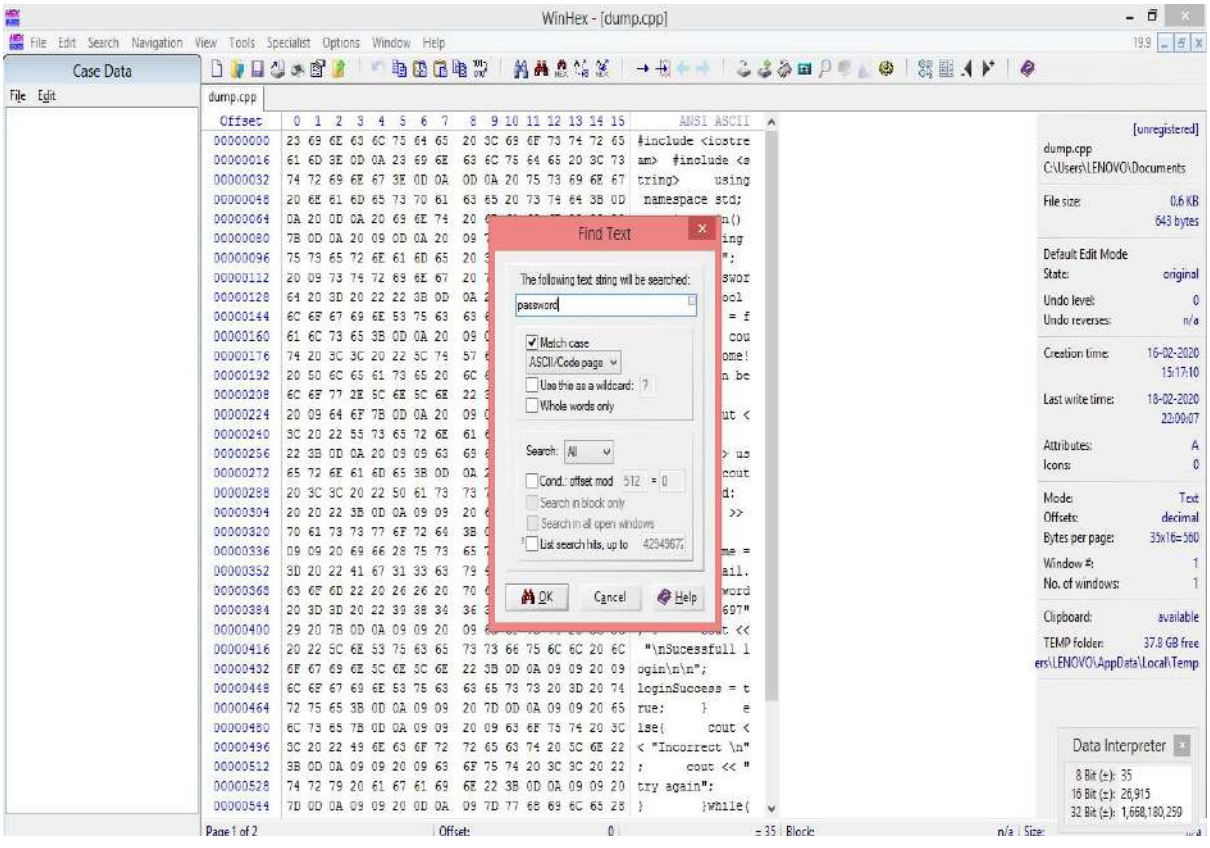


Figure 9.6

Step 7 Click on okay button to see the results

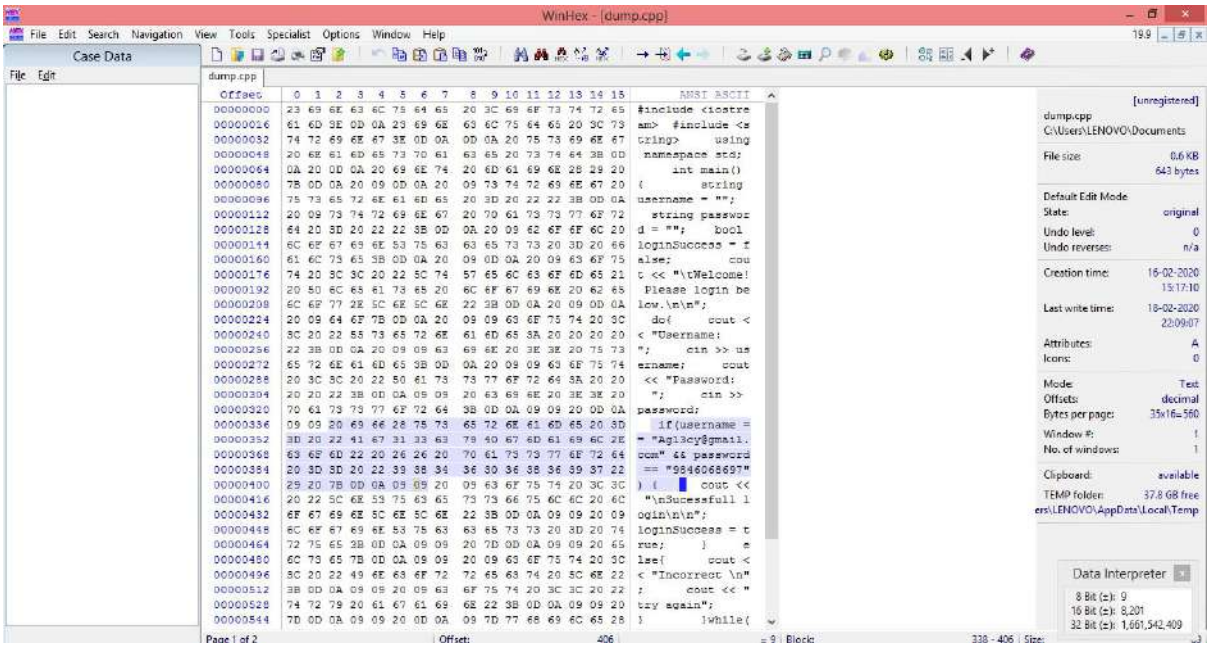


Figure 9.7

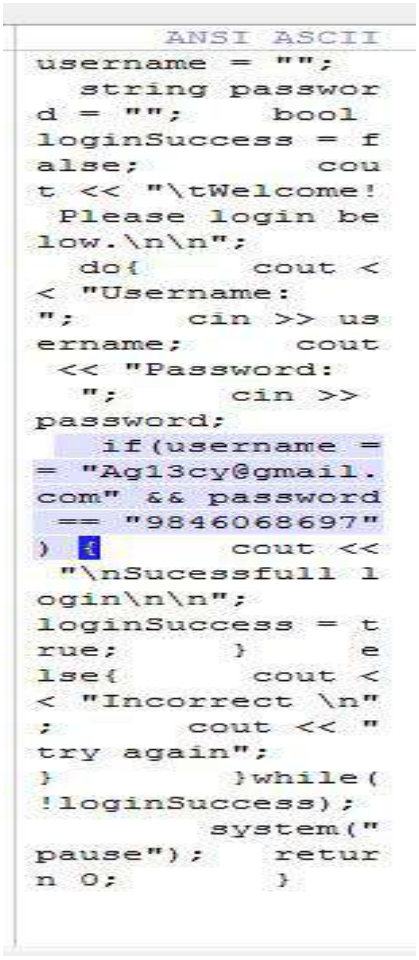


Figure 9.8

Laptop 10: Lenovo v145

Step 1 Take FLIPKART in Google Chrome and login using your credentials

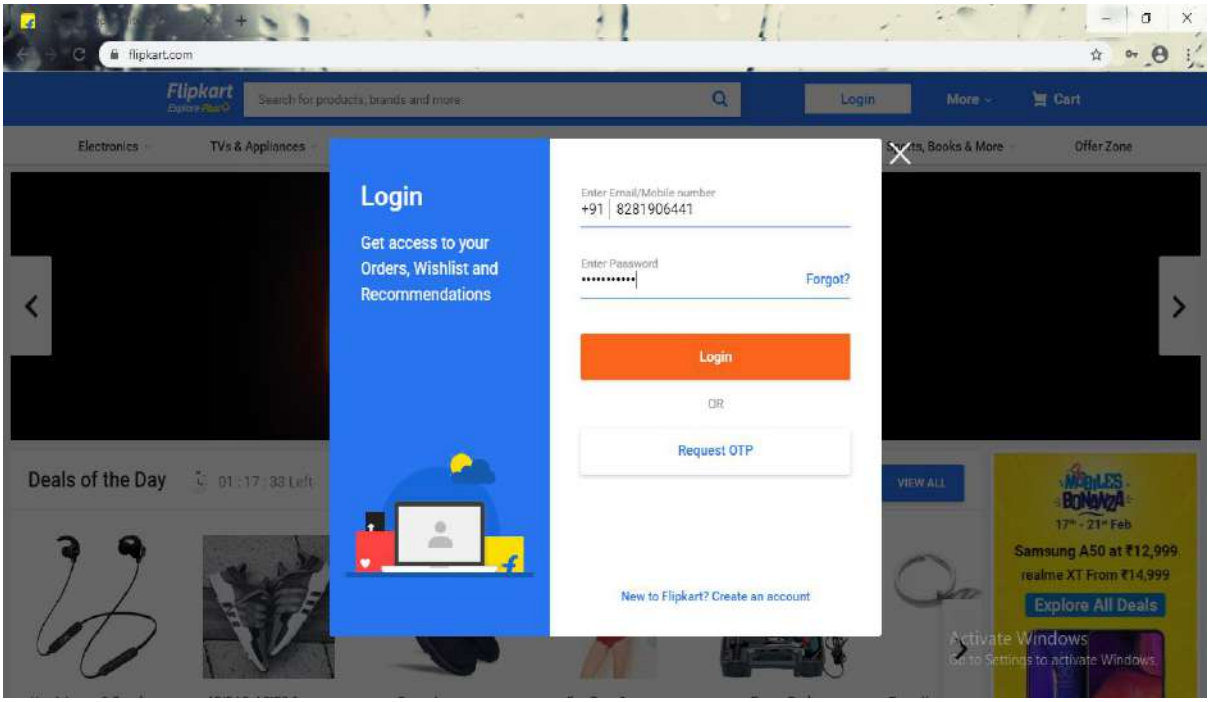


Figure 10.1

Step 2 Login to your account and logout after a minute or two

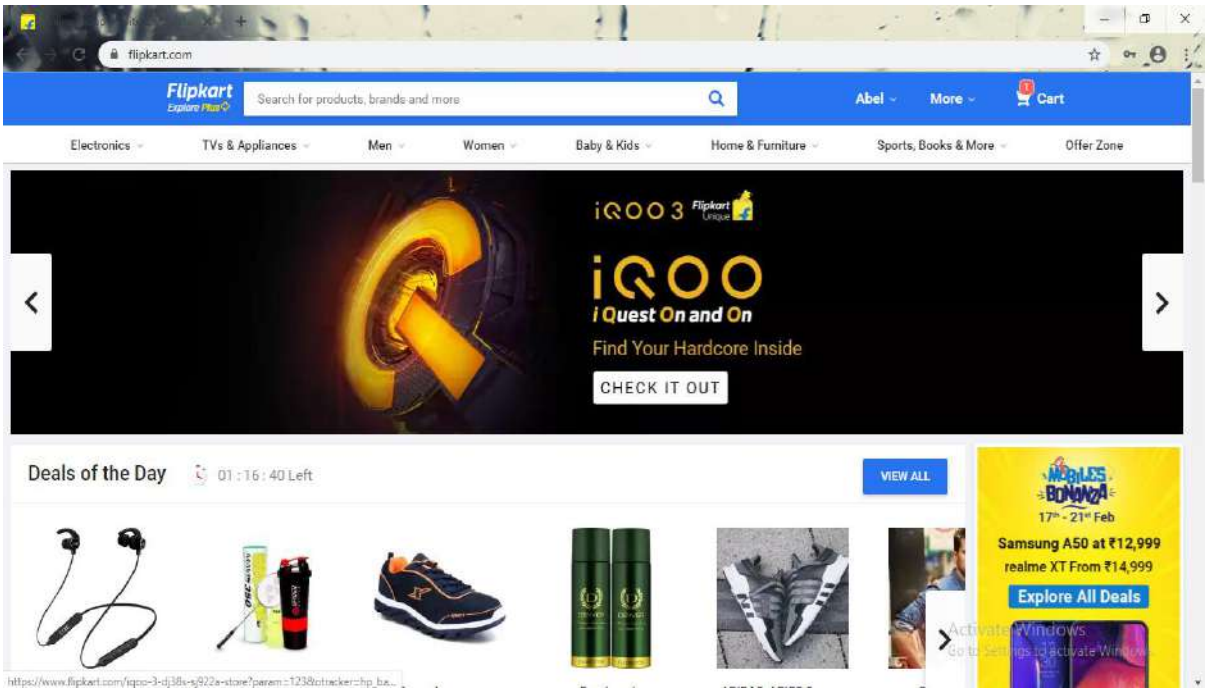


Figure 10.2

Step 3 After logging out open task manager which can be found on the bottom toolbar of the particular system. From the application Right click on Google chrome App and click on ‘Create Dump File’. Within a minute a Dumpfile will be created along with the file path

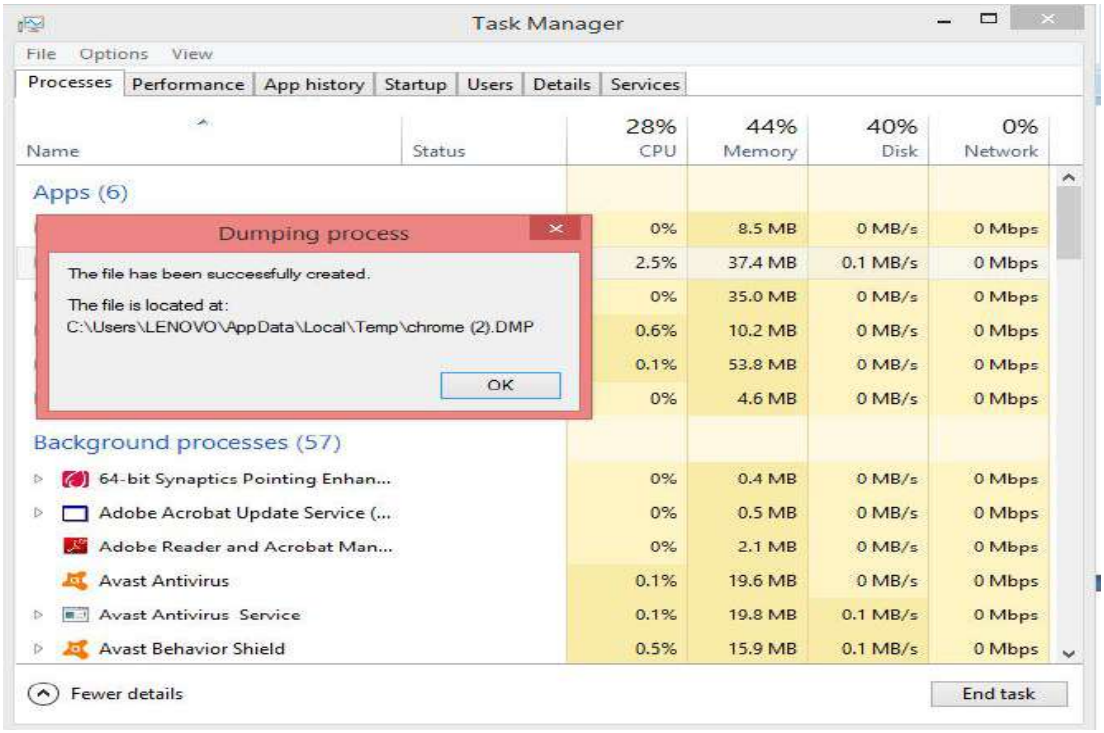


Figure 10.3

Step 4 Locate the Dumpfile in your PC

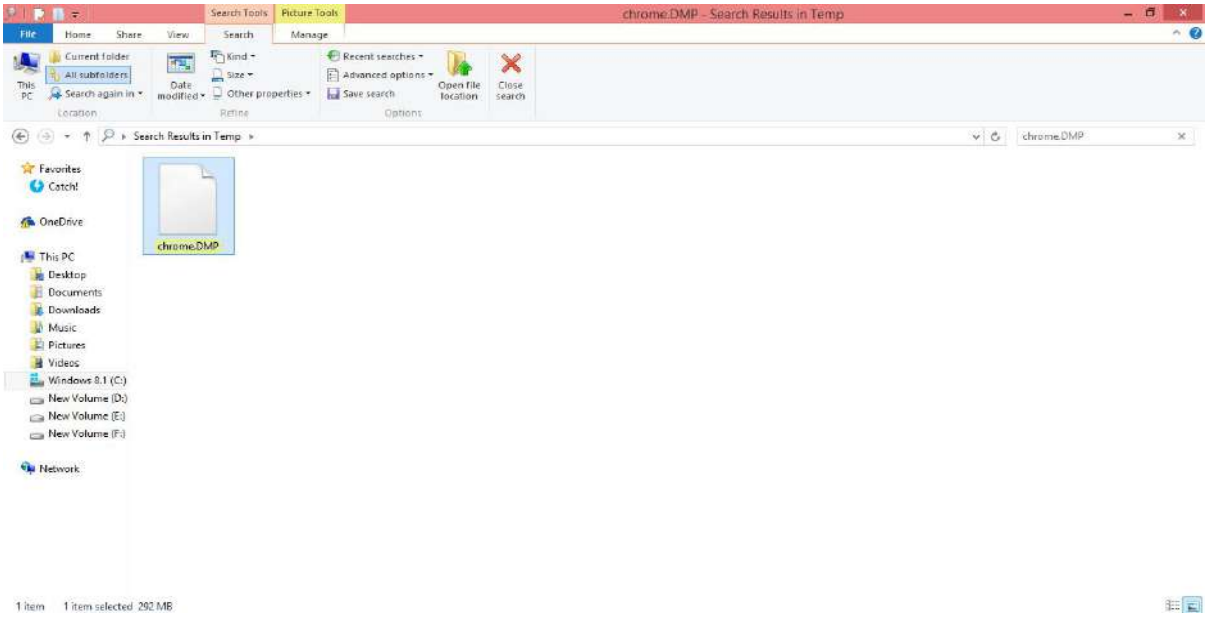


Figure 10.4

Step 5 Open the specific Dumpfile using WINHEX tool

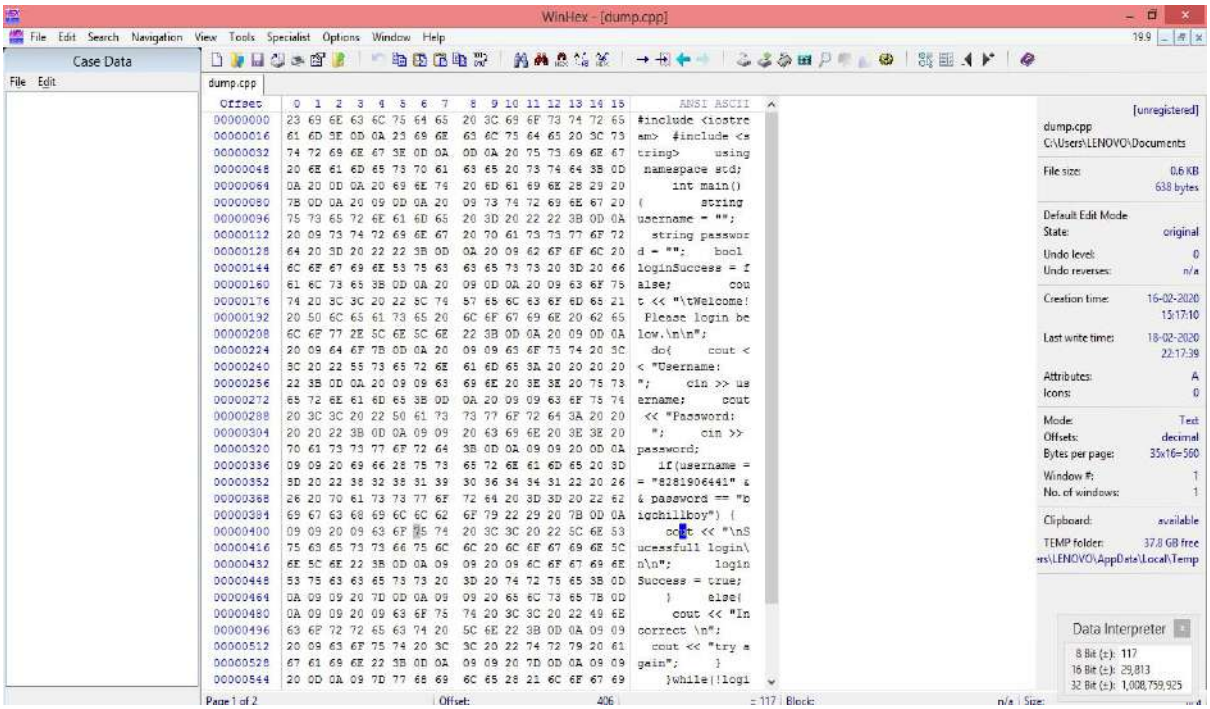


Figure 10.5

Step 6 Click on find text option which can be found on the top bar of the WINHEX tool and type in “password = “

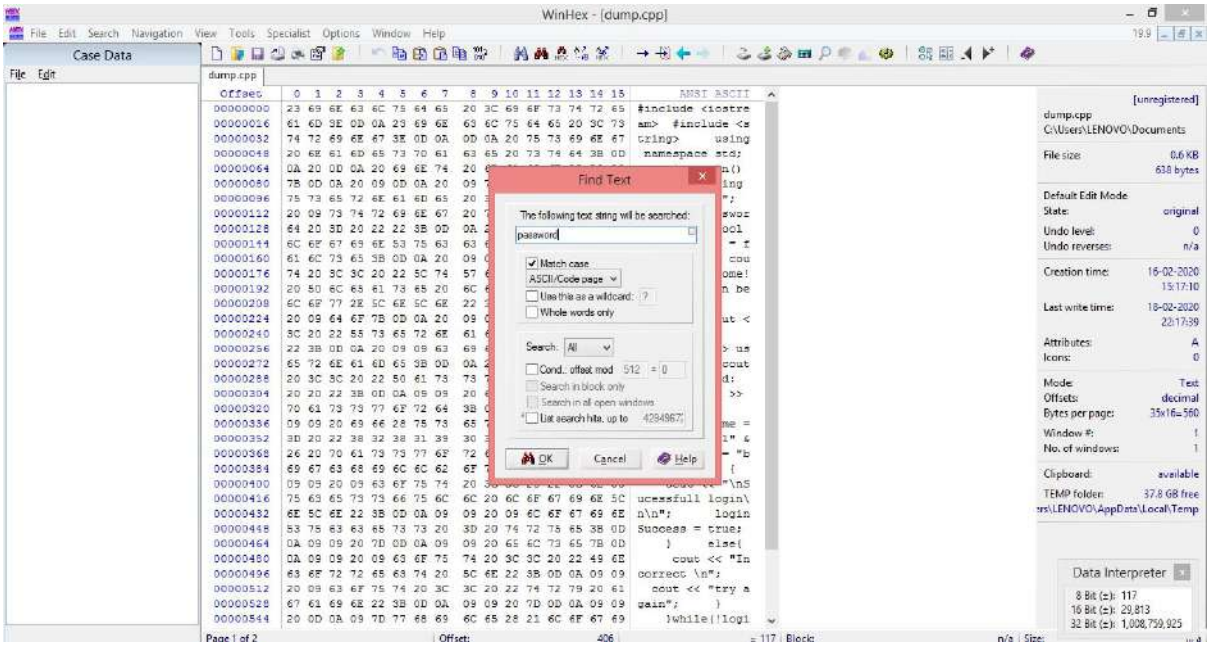


Figure 10.6

Step 7 Click on okay button to see the results

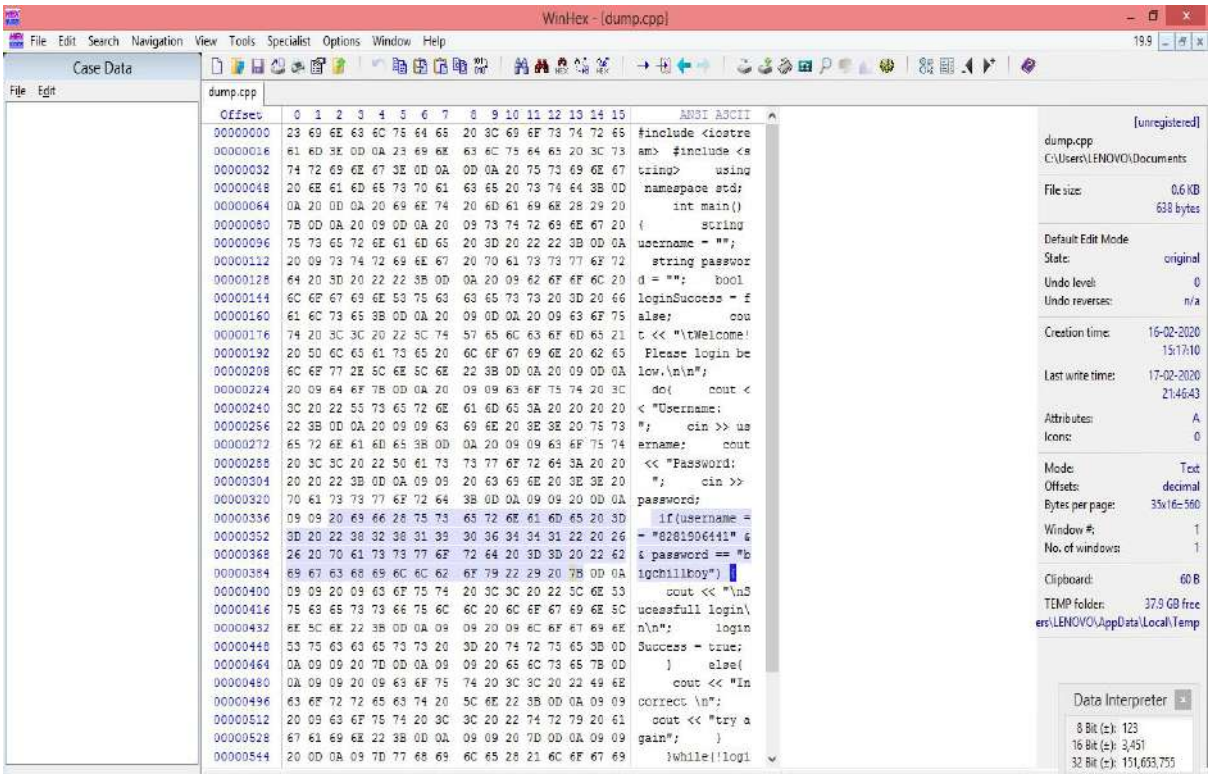


Figure 10.7

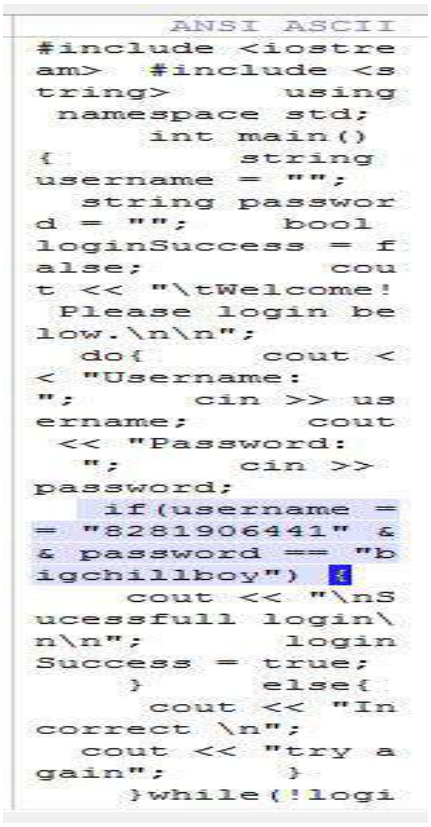


Figure 10.8

CHAPTER V

RESULTS AND CONCLUSION

RESULTS:-

Observation Table

Owner name	Laptop company	Model	Password Extraction Successful?	Time Taken for extraction	The user id and Password
Sreerag	Lenovo	B41	Yes Facebook password was extracted	5 minutes	User id: Sreerag775@gmail.com Password Sreerag@775
Nidhin	Lenovo	Ideapad S145	Yes Flipkart id and password extracted	7minutes	User id: Nidhinchackoch7@gmail.com Password: Cristianoronaldo7
Hari	HP	15 Ryzen	Yes Facebook id and password extracted	5minutes	User id: Harikrishnan9@gmail.com Password:helldream
George	HP	14 Ryzen	Yes Gmail id And password extracted	5minutes	User id: Georgekoshyvaidhyan99@gmail.com Password:Georgekoshy4
Gautham	Asus	X507	Yes Gmail id and password extracted	6minutes	Userid: Gauthamm177@gmail.com Password:Messilm10
Anwar	Dell	Inspiron 5755	Gmail id and password extracted	5minutes	Userid: Anwarhaqkochi12apr@gmail.com Password:littlehoonigan
AG	Acer	Aspire 3	Gmail id and password extracted	6 minutes	Userid: anandhukambadiperumon@gmail.com Password:gameofthrones
Akhil	Iball	Marvel 2	Flipkart id and passwordextracted	4minutes	Userid: Akhilks63@gmail.com Password:Akhilbuilt
Agacy	Acer	Aspire 5s	Gmail id and password extracted	5minutes	Userid: Ag13cy@gmail.com Password:9846068697
Abel	Lenovo	V145	Flipkart id and password extracted	7minutes	Userid: 8281906441 Password:bigchillboy

Calculation

Average time taken for extraction = The mean of the time taken for extraction

5+7+5+5+6+5+6+4+5+7/10= 55/10 =**55minutes**

The Password extraction was done successfully in 10 random laptops and the average time taken for the extraction of Password is **5.5minutes.**

CHAPTER VI

REFERENCES

https://www.sciencedirect.com/science/article/pii/S1742287609000474

http://www.x-ways.net/winhex/manual.pdf

https://searchoracle.techtarget.com/answer/Extracting-data-from-dmp-file

https://www.quora.com/How-can-I-extract-ressources-of-a-DMP-file-in-Windows

https://cqureacademy.com/blog/forensics/memory-dump-analysis

https://wikileaks.org/hbgary-emails//fileid/57220/15931

https://documentation.help/WinHex-X-Ways/topic39.htm

https://www.digital-detective.net/datadump/

https://en.wikipedia.org/wiki/WinHex

https://en.wikipedia.org/wiki/Core_dump