Digital Forensics Lab Report: 8

Date: 12-10-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

Aim/Purpose: Study of volatile memory forensics tools

Tool Names:

1. FTK Imager link :- https://go.exterro.com/l/43312/2022-08-23/f7rytx
2. WinHex link :- http://www.winhex.com/winhex/hex-editor.html

Step 1:- Download FTK Imager

- FTK Imager Download link :- https://go.exterro.com/l/43312/2022-08-23/f7rytx click on get free tool. It will ask to fill the form in order to get the software link.
- FTK Manager is a powerful tool that can be used to manage forensics investigations. It provides a user-friendly interface that makes it easy to search and analyze forensic data. FTK Manager can be used to investigate a wide range of crimes, including child pornography, terrorism, and espionage.
- WinHex is a hexadecimal editor for the Windows operating system. It is used for forensics, data recovery, low-level data processing, and IT security. It allows the user to view files in hexadecimal format.
- Add your details and click on Get Free Tool, you will receive then a mail containing a software link.

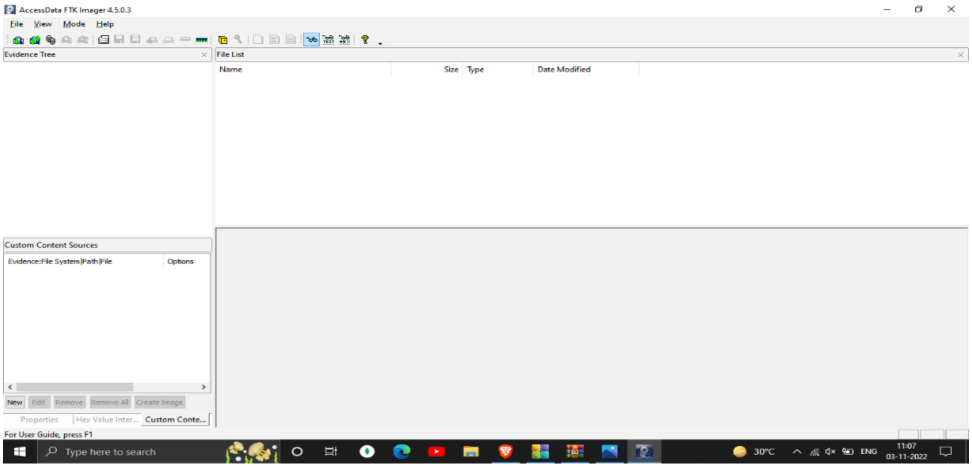
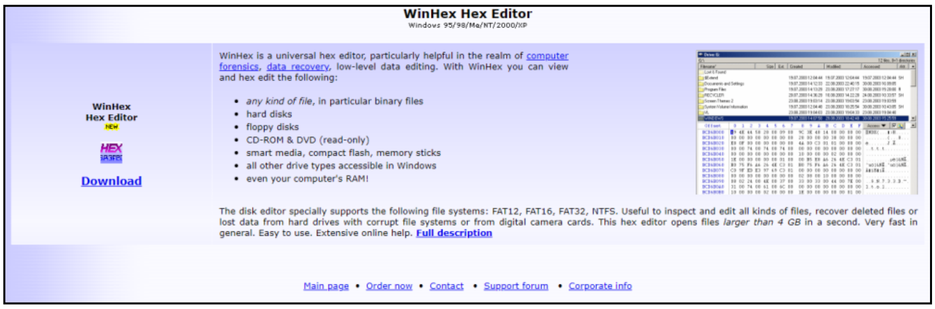


Figure 1 FTK Imager

Steps2: Download Winhex:

1. Visit http://www.winhex.com/winhex/hex-editor.html and click on Download.



WinHex Hex Editor
Windows 95/98/Me/NT/2000/XP

WinHex
Hex Editor
NEW

Download

WinHex is a universal hex editor, particularly helpful in the realm of computer forensics, data recovery, low-level data editing. With WinHex you can view and hex edit the following:

- *any kind of file*, in particular binary files
- hard disks
- floppy disks
- CD-ROM & DVD (read-only)
- smart media, compact flash, memory sticks
- all other drive types accessible in Windows
- even your computer's RAM!

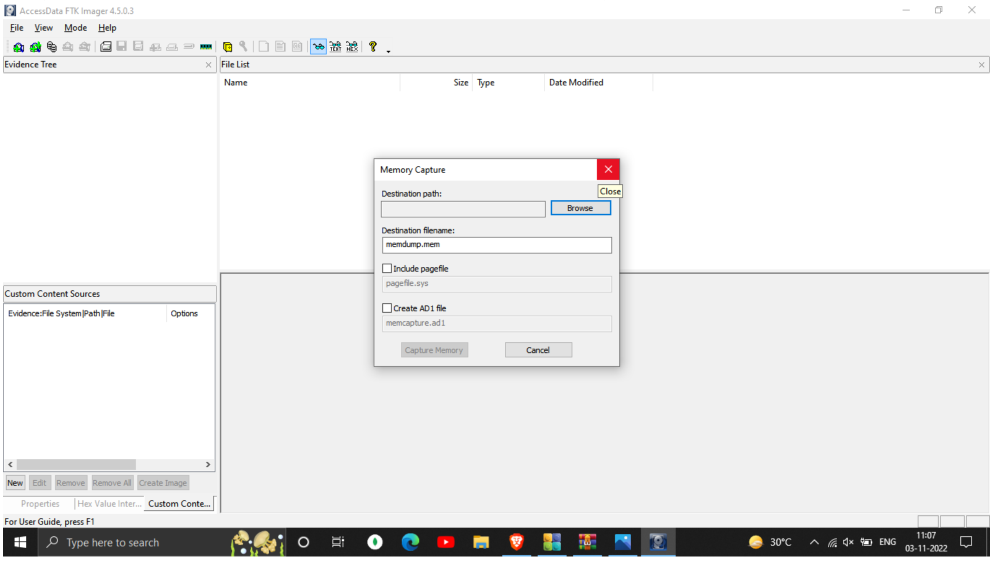
The disk editor specially supports the following file systems: FAT12, FAT16, FAT32, NTFS. Useful to inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards. This hex editor opens files *larger than 4 GB* in a second. Very fast in general. Easy to use. Extensive online help. **Full description**

Main page • Order now • Contact • Support forum • Corporate info

Figure 2 WinHex

Step 3: Make Image file in FTK imager Capture and open in Winhex.

Open Magnet Ram capture and choose directory and file name and click on start



Memory Capture

Destination path:

Browse

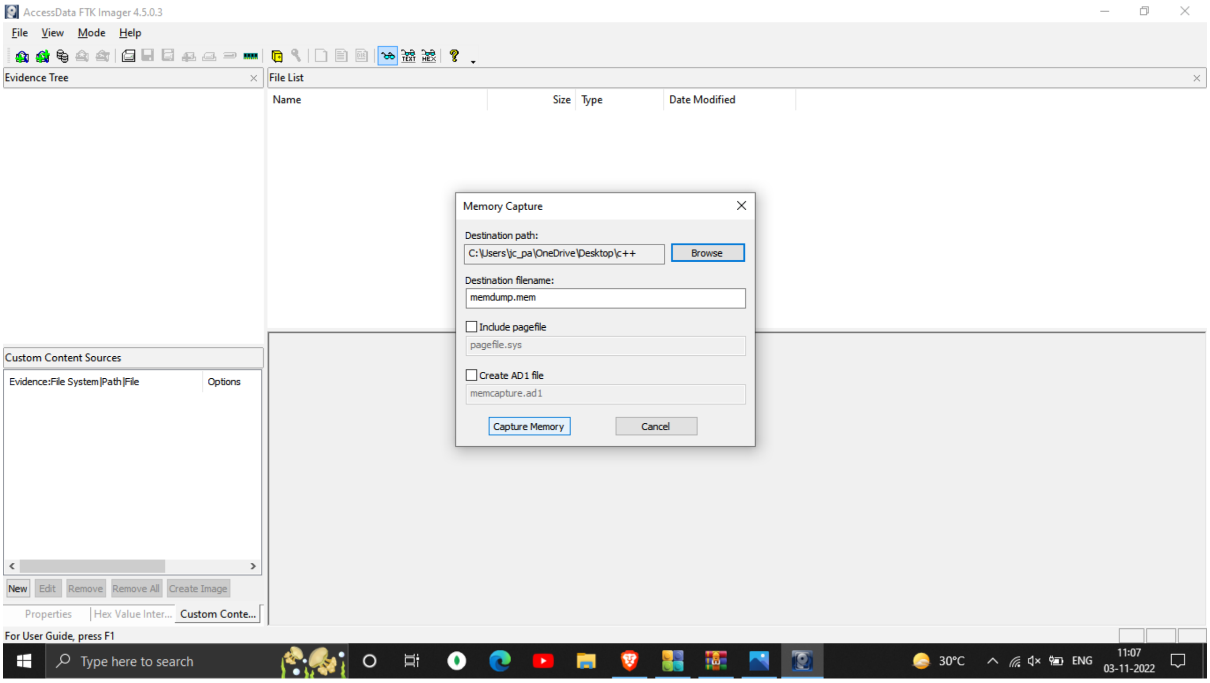
Destination filename:
memdump.mem

□ Include pagefile
pagefile.sys

□ Create AD1 file
memcapture.ad1

Capture Memory | Cancel

Figure 3 FTK Imager


AccessData FTK Imager 4.5.0.3
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Memory Capture
Browse
Capture Memory
Cancel
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
For User Guide, press F1

Destination path: C:\Users\c_pa\OneDrive\Desktop\c++

Destination filename: memdump.mem

□ Include pagefile: pagefile.sys

□ Create AD1 file: memcapture.ad1

Figure 4 FTK Imager

2. 0nce completed, a raw file will be created Now, open winhex and then open the created raw file

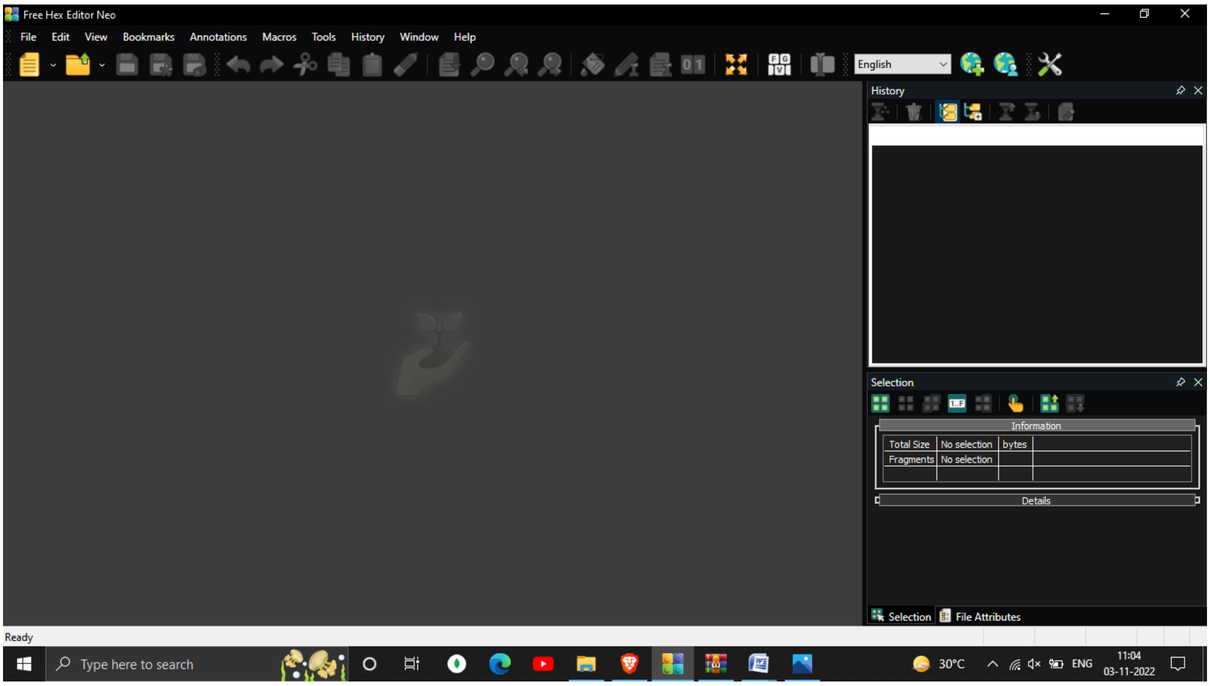
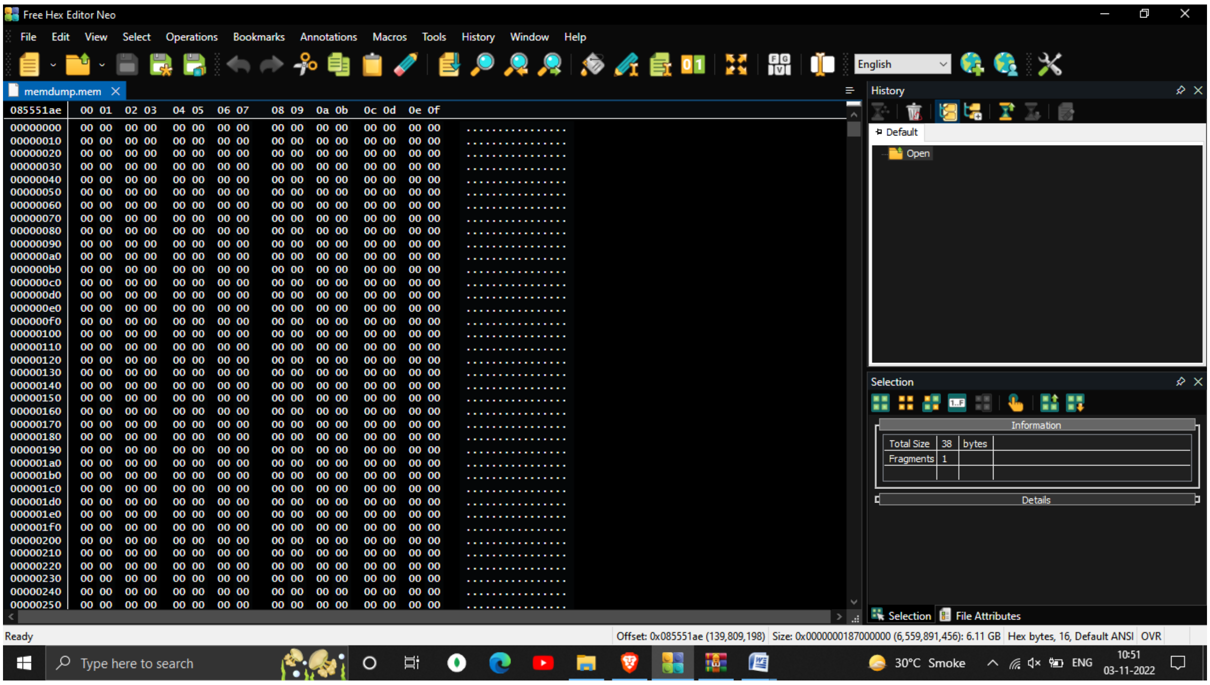

Free Hex Editor Neo
File Edit View Bookmarks Annotations Macros Tools History Window Help
English
History
Selection
Information
Total Size No selection bytes
Fragments No selection
Details
Selection File Attributes
Ready

Figure 5 WinHex

3. Import fie from which creating using FTK imager



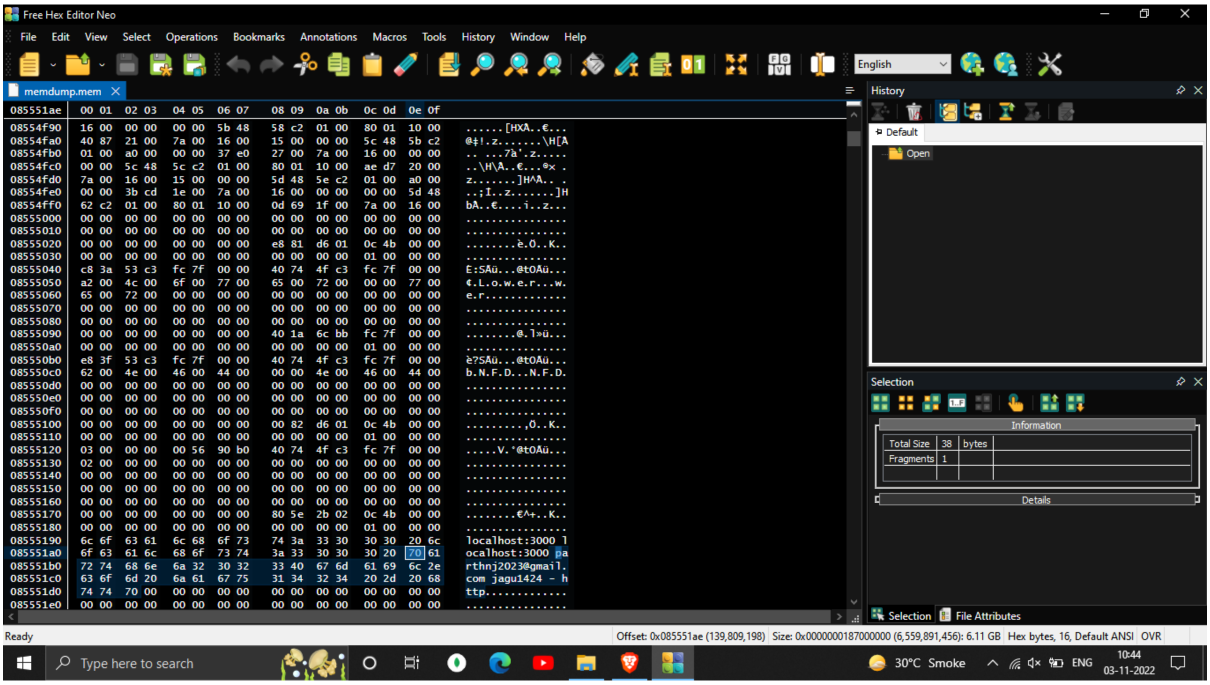
```
085551ae  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f
00000000  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000010  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000020  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000030  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000040  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000050  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000060  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000070  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000080  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000090  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000000a0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000000b0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000000c0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000000d0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000000e0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000000f0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000100  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000110  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000120  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000130  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000140  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000150  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000160  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000170  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000180  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000190  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000001a0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000001b0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000001c0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000001d0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000001e0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
000001f0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000200  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000210  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000220  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000230  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000240  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
00000250  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
```

Total Size | 38 | bytes
Fragments | 1

Ready   Offset: 0x085551ae (139,809,198) Size: 0x0000000187000000 (6,559,891,456): 6.11 GB Hex bytes, 16, Default ANSI OVR

Figure 6 WinHex

4. Findings:
1. Found Gmail id and password :-



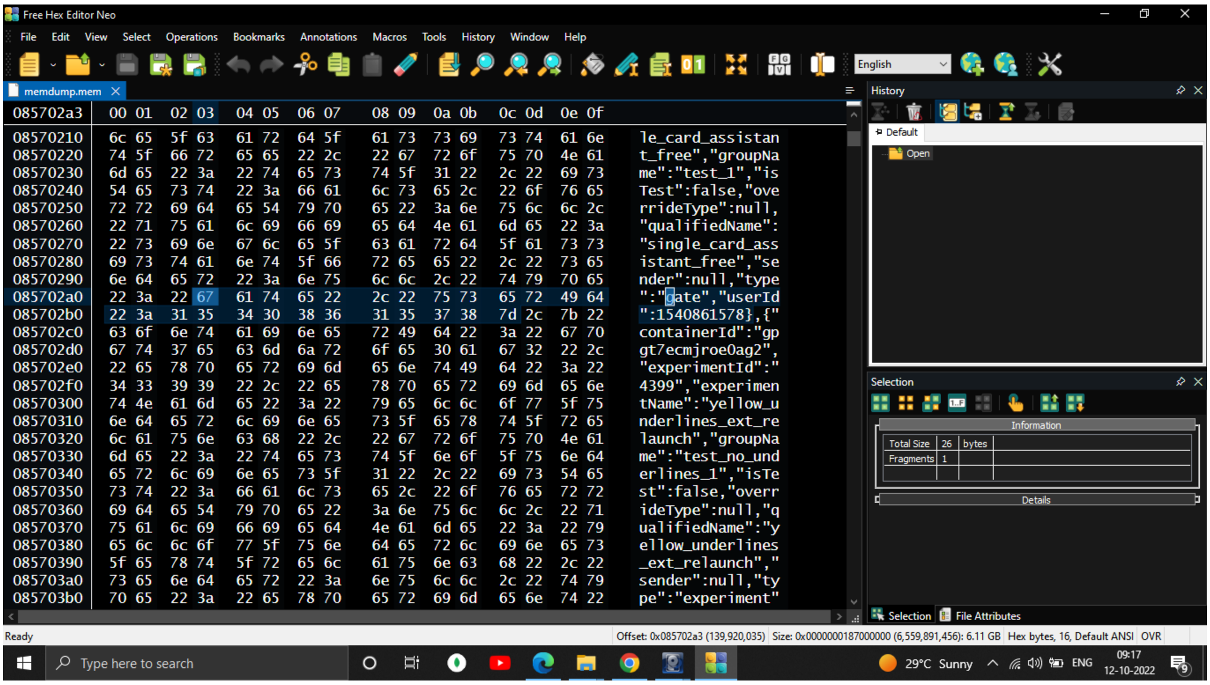
```
085551ae  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f
08554f90  16 00  00 00  00 00  5b 48   58 c2  01 00  80 01  10 00   ......[HXÂ..€...
08554fa0  40 87  21 00  7a 00  16 00   15 00  00 00  5c 48  5b c2   @‡!.z.......\H[Â
08554fb0  01 00  a0 00  00 00  37 e0   27 00  7a 00  16 00  00 00   .. ...7à'.z.....
08554fc0  00 00  5c 48  5c c2  01 00   80 01  10 00  ae d7  20 00   ..\H\Â..€...®× .
08554fd0  7a 00  16 00  15 00  00 00   5d 48  5e c2  01 00  a0 00   z.......]H^Â.. .
08554fe0  00 00  3b cd  1e 00  7a 00   16 00  00 00  00 00  5d 48   ..;Í..z.......]H
08554ff0  62 c2  01 00  80 01  10 00   0d 69  1f 00  7a 00  16 00   bÂ..€....i..z...
08555000  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555010  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555020  00 00  00 00  00 00  00 00   e8 81  d6 01  0c 4b  00 00   ........è.Ö..K..
08555030  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
08555040  c8 3a  53 c3  fc 7f  00 00   40 74  4f c3  fc 7f  00 00   È:SÃü...@tOÃü...
08555050  a2 00  4c 00  6f 00  77 00   65 00  72 00  00 00  77 00   ¢.L.o.w.e.r...w.
08555060  65 00  72 00  00 00  00 00   00 00  00 00  00 00  00 00   e.r.............
08555070  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555080  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555090  00 00  00 00  00 00  00 00   40 1a  6c bb  fc 7f  00 00   ........@.l»ü...
085550a0  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
085550b0  e8 3f  53 c3  fc 7f  00 00   40 74  4f c3  fc 7f  00 00   è?SÃü...@tOÃü...
085550c0  62 00  4e 00  46 00  44 00   00 00  4e 00  46 00  44 00   b.N.F.D...N.F.D.
085550d0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
085550e0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
085550f0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555100  00 00  00 00  00 00  00 00   00 82  d6 01  0c 4b  00 00   .........‚Ö..K..
08555110  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
08555120  03 00  00 00  00 56  90 b0   40 74  4f c3  fc 7f  00 00   .....V.°@tOÃü...
08555130  02 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555140  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555150  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555160  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555170  00 00  00 00  00 00  00 00   80 5e  2b 02  0c 4b  00 00   ........€^+..K..
08555180  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
08555190  6c 6f  63 61  6c 68  6f 73   74 3a  33 30  30 30  20 6c   localhost:3000 l
085551a0  6f 63  61 6c  68 6f  73 74   3a 33  30 30  30 20  70 61   ocalhost:3000 pa
085551b0  72 74  68 6e  6a 32  30 32   33 40  67 6d  61 69  6c 2e   rthnj2023@gmail.
085551c0  63 6f  6d 20  6a 61  67 75   31 34  32 34  20 2d  20 68   com jagu1424 - h
085551d0  74 74  70 00  00 00  00 00   00 00  00 00  00 00  00 00   ttp.............
085551e0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
```

Total Size | 38 | bytes
Fragments | 1

Ready   Offset: 0x085551ae (139,809,198) Size: 0x0000000187000000 (6,559,891,456): 6.11 GB Hex bytes, 16, Default ANSI OVR

Figure 7 WinHex (Found :- Gmail ID and Password)

2. Found gate website account



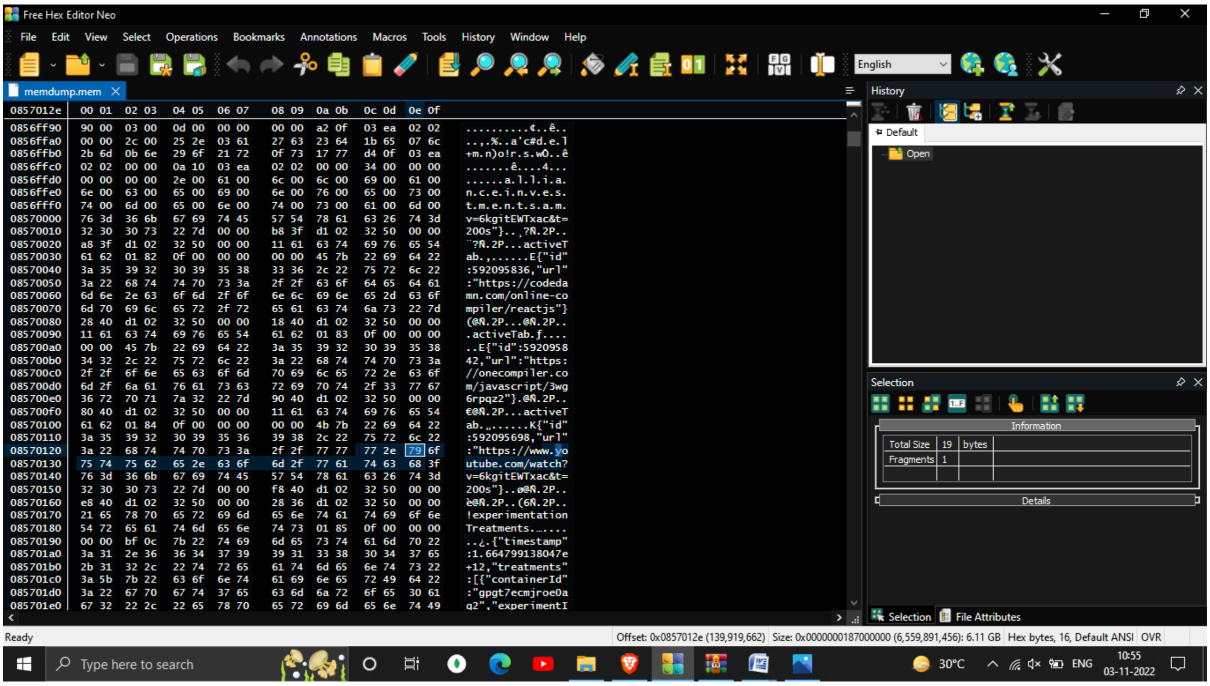
```
085702a3  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f

08570210  6c 65  5f 63  61 72  64 5f   61 73  73 69  73 74  61 6e   le_card_assistan
08570220  74 5f  66 72  65 65  22 2c   22 67  72 6f  75 70  4e 61   t_free","groupNa
08570230  6d 65  22 3a  22 74  65 73   74 5f  31 22  2c 22  69 73   me":"test_1","is
08570240  54 65  73 74  22 3a  66 61   6c 73  65 2c  22 6f  76 65   Test":false,"ove
08570250  72 72  69 64  65 54  79 70   65 22  3a 6e  75 6c  6c 2c   rrideType":null,
08570260  22 71  75 61  6c 69  66 69   65 64  4e 61  6d 65  22 3a   "qualifiedName":
08570270  22 73  69 6e  67 6c  65 5f   63 61  72 64  5f 61  73 73   "single_card_ass
08570280  69 73  74 61  6e 74  5f 66   72 65  65 22  2c 22  73 65   istant_free","se
08570290  6e 64  65 72  22 3a  6e 75   6c 6c  2c 22  74 79  70 65   nder":null,"type
085702a0  22 3a  22 67  61 74  65 22   2c 22  75 73  65 72  49 64   ":"gate","userId
085702b0  22 3a  31 35  34 30  38 36   31 35  37 38  7d 2c  7b 22   ":1540861578},{"
085702c0  63 6f  6e 74  61 69  6e 65   72 49  64 22  3a 22  67 70   containerId":"gp
085702d0  67 74  37 65  63 6d  6a 72   6f 65  30 61  67 32  22 2c   gt7ecmjroe0ag2",
085702e0  22 65  78 70  65 72  69 6d   65 6e  74 49  64 22  3a 22   "experimentId":"
085702f0  34 33  39 39  22 2c  22 65   78 70  65 72  69 6d  65 6e   4399","experimen
08570300  74 4e  61 6d  65 22  3a 22   79 65  6c 6c  6f 77  5f 75   tName":"yellow_u
08570310  6e 64  65 72  6c 69  6e 65   73 5f  65 78  74 5f  72 65   nderlines_ext_re
08570320  6c 61  75 6e  63 68  22 2c   22 67  72 6f  75 70  4e 61   launch","groupNa
08570330  6d 65  22 3a  22 74  65 73   74 5f  6e 6f  5f 75  6e 64   me":"test_no_und
08570340  65 72  6c 69  6e 65  73 5f   31 22  2c 22  69 73  54 65   erlines_1","isTe
08570350  73 74  22 3a  66 61  6c 73   65 2c  22 6f  76 65  72 72   st":false,"overr
08570360  69 64  65 54  79 70  65 22   3a 6e  75 6c  6c 2c  22 71   ideType":null,"q
08570370  75 61  6c 69  66 69  65 64   4e 61  6d 65  22 3a  22 79   ualifiedName":"y
08570380  65 6c  6c 6f  77 5f  75 6e   64 65  72 6c  69 6e  65 73   ellow_underlines
08570390  5f 65  78 74  5f 72  65 6c   61 75  6e 63  68 22  2c 22   _ext_relaunch","
085703a0  73 65  6e 64  65 72  22 3a   6e 75  6c 6c  2c 22  74 79   sender":null,"ty
085703b0  70 65  22 3a  22 65  78 70   65 72  69 6d  65 6e  74 22   pe":"experiment"
```

Total Size 26 bytes
Fragments 1

Ready Offset: 0x085702a3 (139,920,035) Size: 0x0000000187000000 (6,559,891,456): 6.11 GB Hex bytes, 16, Default ANSI OVR

Figure 8 WinHex (Found :- gate website and account)

3. Find YouTube website



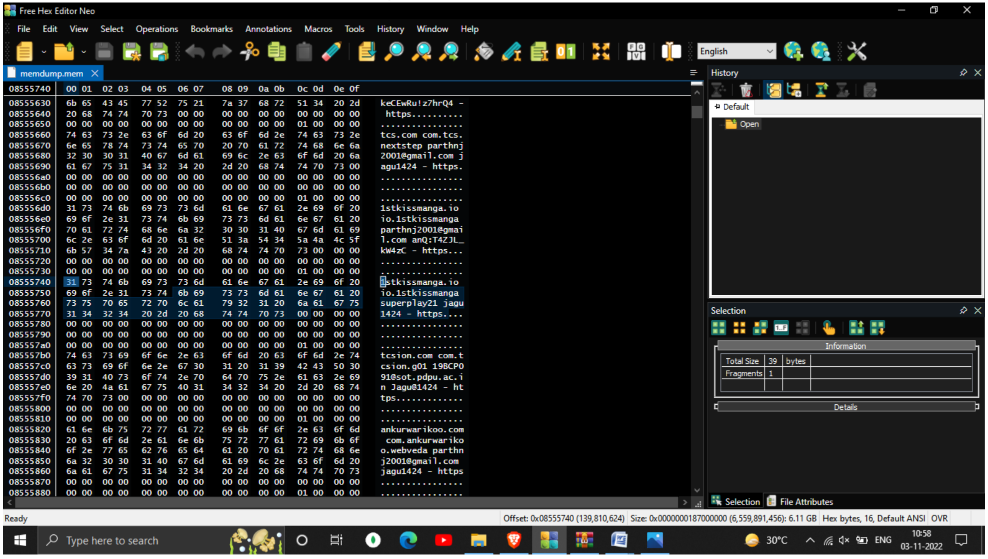
```
0857012e  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f

0856ff90  90 00  03 00  0d 00  00 00   00 00  a2 0f  03 ea  02 02   ..........¢..ê..
0856ffa0  00 00  2c 00  25 2e  03 61   27 63  23 64  1b 65  07 6c   ..,.%..a'c#d.e.l
0856ffb0  2b 6d  0b 6e  29 6f  21 72   0f 73  17 77  d4 0f  03 ea   +m.n)o!r.s.wÔ..ê
0856ffc0  02 02  00 00  0a 10  03 ea   02 02  00 00  34 00  00 00   .......ê....4...
0856ffd0  00 00  00 00  2e 00  61 00   6c 00  6c 00  69 00  61 00   ......a.l.l.i.a.
0856ffe0  6e 00  63 00  65 00  69 00   6e 00  76 00  65 00  73 00   n.c.e.i.n.v.e.s.
0856fff0  74 00  6d 00  65 00  6e 00   74 00  73 00  61 00  6d 00   t.m.e.n.t.s.a.m.
08570000  76 3d  36 6b  67 69  74 45   57 54  78 61  63 26  74 3d   v=6kgitEWTxac&t=
08570010  32 30  30 73  22 7d  00 00   b8 3f  d1 02  32 50  00 00   200s"}..¸?Ñ.2P..
08570020  a8 3f  d1 02  32 50  00 00   11 61  63 74  69 76  65 54   ¨?Ñ.2P...activeT
08570030  61 62  01 82  0f 00  00 00   00 00  45 7b  22 69  64 22   ab.‚......E{"id"
08570040  3a 35  39 32  30 39  35 38   33 36  2c 22  75 72  6c 22   :592095836,"url"
08570050  3a 22  68 74  74 70  73 3a   2f 2f  63 6f  64 65  64 61   :"https://codeda
08570060  6d 6e  2e 63  6f 6d  2f 6f   6e 6c  69 6e  65 2d  63 6f   mn.com/online-co
08570070  6d 70  69 6c  65 72  2f 72   65 61  63 74  6a 73  22 7d   mpiler/reactjs"}
08570080  28 40  d1 02  32 50  00 00   18 40  d1 02  32 50  00 00   (@Ñ.2P...@Ñ.2P..
08570090  11 61  63 74  69 76  65 54   61 62  01 83  0f 00  00 00   .activeTab.ƒ....
085700a0  00 00  45 7b  22 69  64 22   3a 35  39 32  30 39  35 38   ..E{"id":5920958
085700b0  34 32  2c 22  75 72  6c 22   3a 22  68 74  74 70  73 3a   42,"url":"https:
085700c0  2f 2f  6f 6e  65 63  6f 6d   70 69  6c 65  72 2e  63 6f   //onecompiler.co
085700d0  6d 2f  6a 61  76 61  73 63   72 69  70 74  2f 33  77 67   m/javascript/3wg
085700e0  36 72  70 71  7a 32  22 7d   90 40  d1 02  32 50  00 00   6rpqz2"}.@Ñ.2P..
085700f0  80 40  d1 02  32 50  00 00   11 61  63 74  69 76  65 54   €@Ñ.2P...activeT
08570100  61 62  01 84  0f 00  00 00   00 00  4b 7b  22 69  64 22   ab.„......K{"id"
08570110  3a 35  39 32  30 39  35 36   39 38  2c 22  75 72  6c 22   :592095698,"url"
08570120  3a 22  68 74  74 70  73 3a   2f 2f  77 77  77 2e  79 6f   :"https://www.yo
08570130  75 74  75 62  65 2e  63 6f   6d 2f  77 61  74 63  68 3f   utube.com/watch?
08570140  76 3d  36 6b  67 69  74 45   57 54  78 61  63 26  74 3d   v=6kgitEWTxac&t=
08570150  32 30  30 73  22 7d  00 00   f8 40  d1 02  32 50  00 00   200s"}..ø@Ñ.2P..
08570160  e8 40  d1 02  32 50  00 00   28 36  d1 02  32 50  00 00   è@Ñ.2P..(6Ñ.2P..
08570170  21 65  78 70  65 72  69 6d   65 6e  74 61  74 69  6f 6e   !experimentation
08570180  54 72  65 61  74 6d  65 6e   74 73  01 85  0f 00  00 00   Treatments.…....
08570190  00 00  bf 0c  7b 22  74 69   6d 65  73 74  61 6d  70 22   ..¿.{"timestamp"
085701a0  3a 31  2e 36  36 34  37 39   39 31  33 38  30 34  37 65   :1.664799138047e
085701b0  2b 31  32 2c  22 74  72 65   61 74  6d 65  6e 74  73 22   +12,"treatments"
085701c0  3a 5b  7b 22  63 6f  6e 74   61 69  6e 65  72 49  64 22   :[{"containerId"
085701d0  3a 22  67 70  67 74  37 65   63 6d  6a 72  6f 65  30 61   :"gpgt7ecmjroe0a
085701e0  67 32  22 2c  22 65  78 70   65 72  69 6d  65 6e  74 49   g2","experimentI
```

Total Size 19 bytes
Fragments 1

Ready Offset: 0x0857012e (139,919,662) Size: 0x0000000187000000 (6,559,891,456): 6.11 GB Hex bytes, 16, Default ANSI OVR

Figure 9 WinHex (Found :- Youtube)

4. Manga read website (1stkissmanga.io)



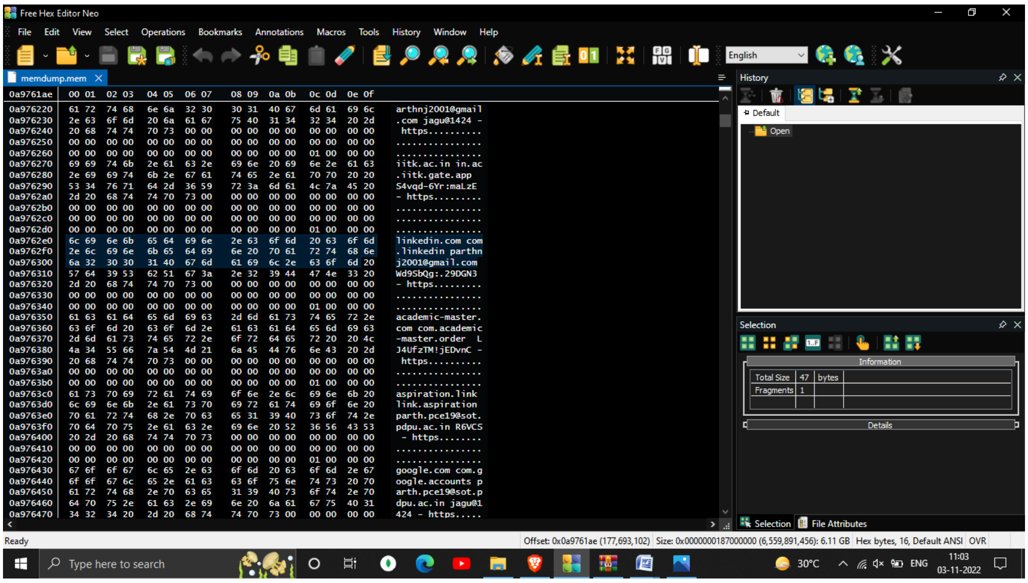
```
08555740  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f
08555630  6b 65  43 45  77 52  75 21   7a 37  68 72  51 34  20 2d   keCEwRu!z7hrQ4 -
08555640  20 68  74 74  70 73  00 00   00 00  00 00  00 00  00 00    https..........
08555650  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
08555660  74 63  73 2e  63 6f  6d 20   63 6f  6d 2e  74 63  73 2e   tcs.com com.tcs.
08555670  6e 65  78 74  73 74  65 70   20 70  61 72  74 68  6e 6a   nextstep parthnj
08555680  32 30  30 31  40 67  6d 61   69 6c  2e 63  6f 6d  20 6a   2001@gmail.com j
08555690  61 67  75 31  34 32  34 20   2d 20  68 74  74 70  73 00   agu1424 - https.
085556a0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
085556b0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
085556c0  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
085556d0  31 73  74 6b  69 73  73 6d   61 6e  67 61  2e 69  6f 20   1stkissmanga.io
085556e0  69 6f  2e 31  73 74  6b 69   73 73  6d 61  6e 67  61 20   io.1stkissmanga
085556f0  70 61  72 74  68 6e  6a 32   30 30  31 40  67 6d  61 69   parthnj2001@gmai
08555700  6c 2e  63 6f  6d 20  61 6e   51 3a  54 34  5a 4a  4c 5f   l.com anQ:T4ZJL_
08555710  6b 57  34 7a  43 20  2d 20   68 74  74 70  73 00  00 00   kW4zC - https...
08555720  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555730  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
08555740  31 73  74 6b  69 73  73 6d   61 6e  67 61  2e 69  6f 20   1stkissmanga.io
08555750  69 6f  2e 31  73 74  6b 69   73 73  6d 61  6e 67  61 20   io.1stkissmanga
08555760  73 75  70 65  72 70  6c 61   79 32  31 20  6a 61  67 75   superplay21 jagu
08555770  31 34  32 34  20 2d  20 68   74 74  70 73  00 00  00 00   1424 - https....
08555780  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555790  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
085557a0  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
085557b0  74 63  73 69  6f 6e  2e 63   6f 6d  20 63  6f 6d  2e 74   tcsion.com com.t
085557c0  63 73  69 6f  6e 2e  67 30   31 20  31 39  42 43  50 30   csion.g01 19BCP0
085557d0  39 31  40 73  6f 74  2e 70   64 70  75 2e  61 63  2e 69   91@sot.pdpu.ac.i
085557e0  6e 20  4a 61  67 75  40 31   34 32  34 20  2d 20  68 74   n Jagu@1424 - ht
085557f0  74 70  73 00  00 00  00 00   00 00  00 00  00 00  00 00   tps.............
08555800  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555810  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
08555820  61 6e  6b 75  72 77  61 72   69 6b  6f 6f  2e 63  6f 6d   ankurwarikoo.com
08555830  20 63  6f 6d  2e 61  6e 6b   75 72  77 61  72 69  6b 6f    com.ankurwariko
08555840  6f 2e  77 65  62 76  65 64   61 20  70 61  72 74  68 6e   o.webveda parthn
08555850  6a 32  30 30  31 40  67 6d   61 69  6c 2e  63 6f  6d 20   j2001@gmail.com
08555860  6a 61  67 75  31 34  32 34   20 2d  20 68  74 74  70 73   jagu1424 - https
08555870  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
08555880  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
```

Total Size 39 bytes
Fragments 1

Ready   Offset: 0x08555740 (139,810,624) Size: 0x0000000187000000 (6,559,891,456): 6.11 GB Hex bytes, 16, Default ANSI OVR

Figure 10 WinHex (Found :- 1stkissmanga)

5. LinkedIn



```
0a9761ae  00 01  02 03  04 05  06 07   08 09  0a 0b  0c 0d  0e 0f
0a976220  61 72  74 68  6e 6a  32 30   30 31  40 67  6d 61  69 6c   arthnj2001@gmail
0a976230  2e 63  6f 6d  20 6a  61 67   75 40  31 34  32 34  20 2d   .com jagu@1424 -
0a976240  20 68  74 74  70 73  00 00   00 00  00 00  00 00  00 00    https..........
0a976250  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
0a976260  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
0a976270  69 69  74 6b  2e 61  63 2e   69 6e  20 69  6e 2e  61 63   iitk.ac.in in.ac
0a976280  2e 69  69 74  6b 2e  67 61   74 65  2e 61  70 70  20 20   .iitk.gate.app
0a976290  53 34  76 71  64 2d  36 59   72 3a  6d 61  4c 7a  45 20   S4vqd-6Yr:maLzE
0a9762a0  2d 20  68 74  74 70  73 00   00 00  00 00  00 00  00 00   - https.........
0a9762b0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
0a9762c0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
0a9762d0  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
0a9762e0  6c 69  6e 6b  65 64  69 6e   2e 63  6f 6d  20 63  6f 6d   linkedin.com com
0a9762f0  2e 6c  69 6e  6b 65  64 69   6e 20  70 61  72 74  68 6e   .linkedin parthn
0a976300  6a 32  30 30  31 40  67 6d   61 69  6c 2e  63 6f  6d 20   j2001@gmail.com
0a976310  57 64  39 53  62 51  67 3a   2e 32  39 44  47 4e  33 20   Wd9SbQg:.29DGN3
0a976320  2d 20  68 74  74 70  73 00   00 00  00 00  00 00  00 00   - https.........
0a976330  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
0a976340  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
0a976350  61 63  61 64  65 6d  69 63   2d 6d  61 73  74 65  72 2e   academic-master.
0a976360  63 6f  6d 20  63 6f  6d 2e   61 63  61 64  65 6d  69 63   com com.academic
0a976370  2d 6d  61 73  74 65  72 2e   6f 72  64 65  72 20  20 4c   -master.order  L
0a976380  4a 34  55 66  7a 54  4d 21   6a 45  44 76  6e 43  20 2d   J4UfzTM!jEDvnC -
0a976390  20 68  74 74  70 73  00 00   00 00  00 00  00 00  00 00    https..........
0a9763a0  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
0a9763b0  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
0a9763c0  61 73  70 69  72 61  74 69   6f 6e  2e 6c  69 6e  6b 20   aspiration.link
0a9763d0  6c 69  6e 6b  2e 61  73 70   69 72  61 74  69 6f  6e 20   link.aspiration
0a9763e0  70 61  72 74  68 2e  70 63   65 31  39 40  73 6f  74 2e   parth.pce19@sot.
0a9763f0  70 64  70 75  2e 61  63 2e   69 6e  20 52  36 56  43 53   pdpu.ac.in R6VCS
0a976400  20 2d  20 68  74 74  70 73   00 00  00 00  00 00  00 00    - https........
0a976410  00 00  00 00  00 00  00 00   00 00  00 00  00 00  00 00   ................
0a976420  00 00  00 00  00 00  00 00   00 00  00 00  01 00  00 00   ................
0a976430  67 6f  6f 67  6c 65  2e 63   6f 6d  20 63  6f 6d  2e 67   google.com com.g
0a976440  6f 6f  67 6c  65 2e  61 63   63 6f  75 6e  74 73  20 70   oogle.accounts p
0a976450  61 72  74 68  2e 70  63 65   31 39  40 73  6f 74  2e 70   arth.pce19@sot.p
0a976460  64 70  75 2e  61 63  2e 69   6e 20  6a 61  67 75  40 31   dpu.ac.in jagu@1
0a976470  34 32  34 20  2d 20  68 74   74 70  73 00  00 00  00 00   424 - https.....
```

Total Size 47 bytes
Fragments 1

Ready   Offset: 0x0a9761ae (177,693,102) Size: 0x0000000187000000 (6,559,891,456): 6.11 GB Hex bytes, 16, Default ANSI OVR

Figure 11 WinHex (Found :- LinkedIn)

Analysis:

1. We are using FTK imager to Capture memory and then using Win Hex to find data.

Conclusion:

1. We are using FTK imager to capture memory
2. We are using Win Hex to find data from FTK imager data may include like Gmail account and password , YouTube watch video other website password or other person phone number.