Lab 10

CYL2002 Digital Forensics - Lab

Name : Mirza Humayun Masood(i22-1749)

Section : CY-A

Submitted to: Sir Ubaid Ullah

Department of Cyber Security BS(CY)

FAST-NUCES Islamabad

Password Cracking.

For this i actually first exported the office files from the autopsy

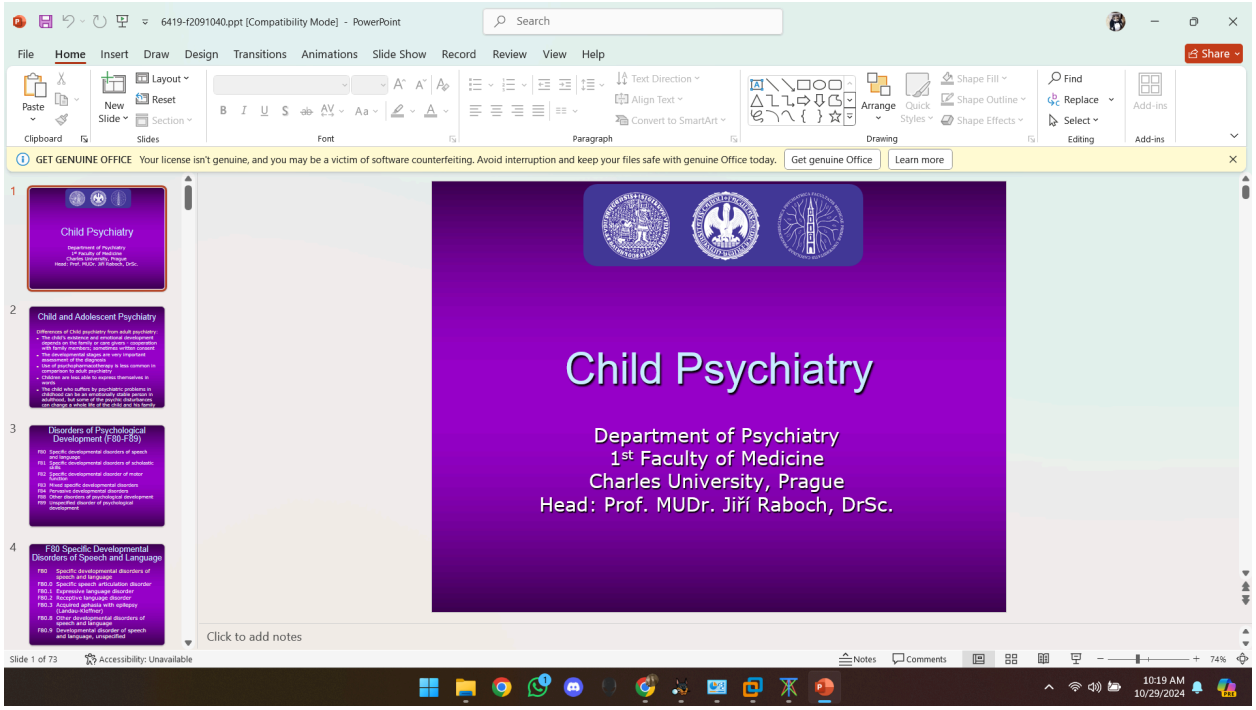
Name	S	C	O	Modified Time	Change Time
Paraphilias.ppt				2011-09-27 19:46:06 PKT	0000-00-00 00:00:0(
Assessment NCP.ppt				2011-09-27 19:40:12 PKT	0000-00-00 00:00:0(
f1581248.ppt			0	0000-00-00 00:00:00	0000-00-00 00:00:0(
Introduction.ppt				2011-09-27 19:42:58 PKT	0000-00-00 00:00:0(
General Psychopathology.ppt				2011-09-27 19:42:22 PKT	0000-00-00 00:00:0(
f0335328.ppt			0	0000-00-00 00:00:00	0000-00-00 00:00:0(
Biochemistry.ppt				2011-09-27 19:41:02 PKT	0000-00-00 00:00:0(
f2086048.ppt			0	0000-00-00 00:00:00	0000-00-00 00:00:0(
Child Psychiatry.ppt				2011-09-27 19:41:38 PKT	0000-00-00 00:00:0(

Then went to kali, and used crunch to generate a password file, then used john to extract the hashes of the ppt file, and then used john to see the password.
I found a handful of passwords like.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist="three_letter_wordlist.txt" hash.txt
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (oldoffice, MS Office ≤ 2003 [MD5/SHA1 RC4 32/64])
Remaining 6 password hashes with 6 different salts
Cost 1 (hash type [0-1:MD5+RC4-40 3:SHA1+RC4-40 4:SHA1+RC4-128 5:SHA1+RC4-56]) is 3 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
eno              (5431-f1512576.ppt)
one              (1301-General   Psychopathology.ppt)
rim              (6418-f2086048.ppt)
rod              (1311-Personality Disorders.ppt)
xyz              (6419-f2091040.ppt)
5g 0:00:00:00 DONE (2024-10-29 01:14) 250.0g/s 878800p/s 3643Kc/s 3643KC/s yge..zzz
Warning: passwords printed above might not be all those cracked
Use the "--show --format=oldoffice" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Lets use the password to see the content of one file.



So these are just slides.

Now to work on pdf.

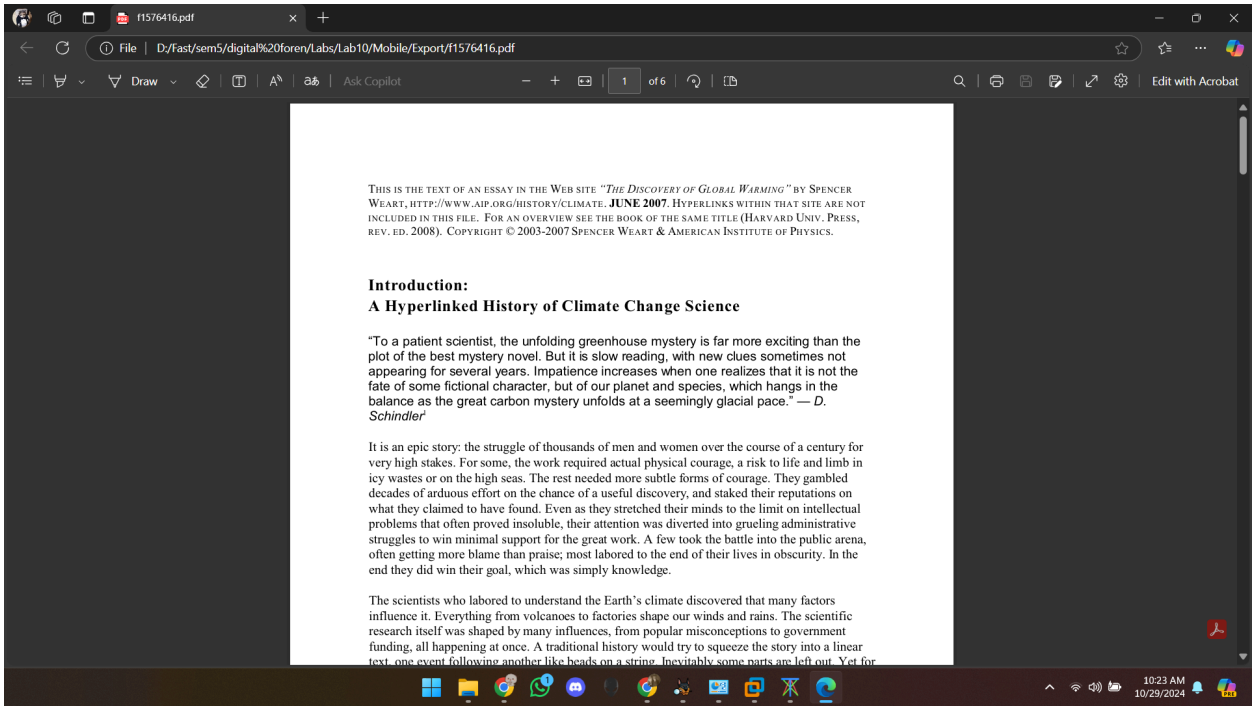
So i used john to extract the hash then did the same to see the password of the file.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ pdf2john f1576416.pdf > pdfhash.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist="three_letter_wordlist.txt" pdfhash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 2 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tip              (f1576416.pdf)
1g 0:00:00:00 DONE (2024-10-29 01:22) 100.0g/s 1318Kp/s 1318Kc/s 1318KC/s tie..tnb
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$
```

The content of the file is given below.



THIS IS THE TEXT OF AN ESSAY IN THE WEB SITE *"THE DISCOVERY OF GLOBAL WARMING"* BY SPENCER WEART, HTTP://WWW.AIP.ORG/HISTORY/CLIMATE. **JUNE 2007**. HYPERLINKS WITHIN THAT SITE ARE NOT INCLUDED IN THIS FILE. FOR AN OVERVIEW SEE THE BOOK OF THE SAME TITLE (HARVARD UNIV. PRESS, REV. ED. 2008). COPYRIGHT © 2003-2007 SPENCER WEART & AMERICAN INSTITUTE OF PHYSICS.

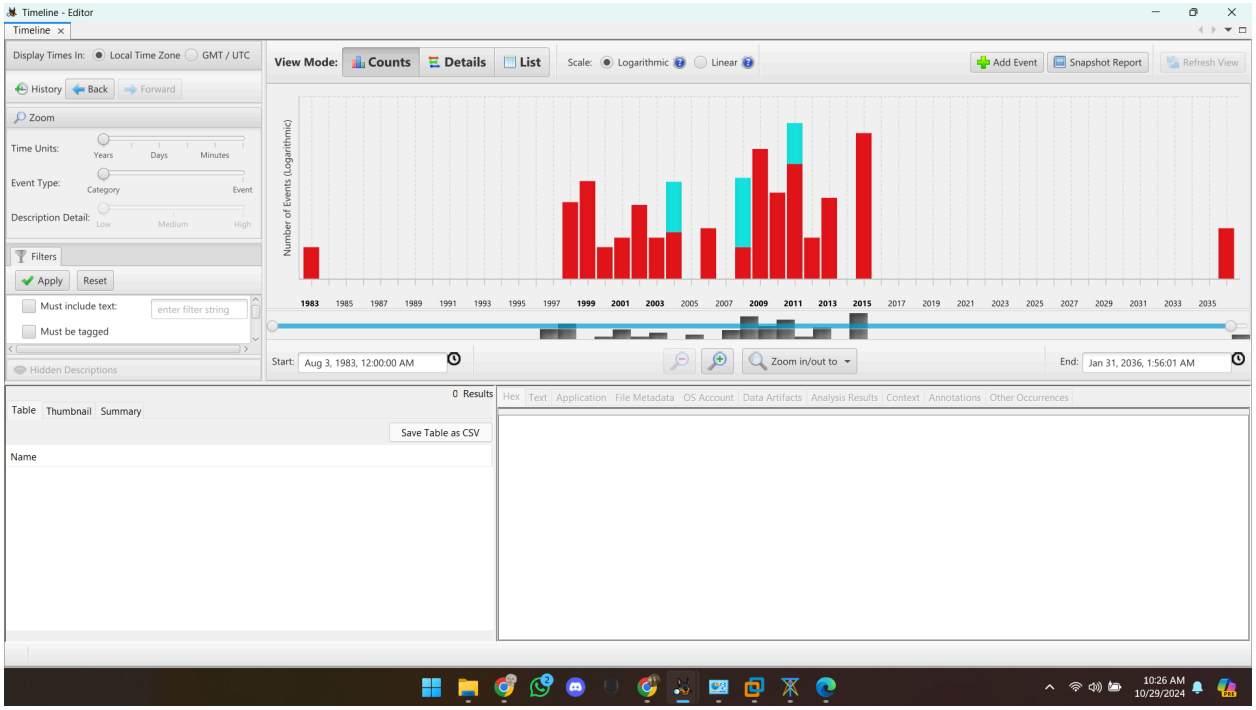
Introduction:
A Hyperlinked History of Climate Change Science

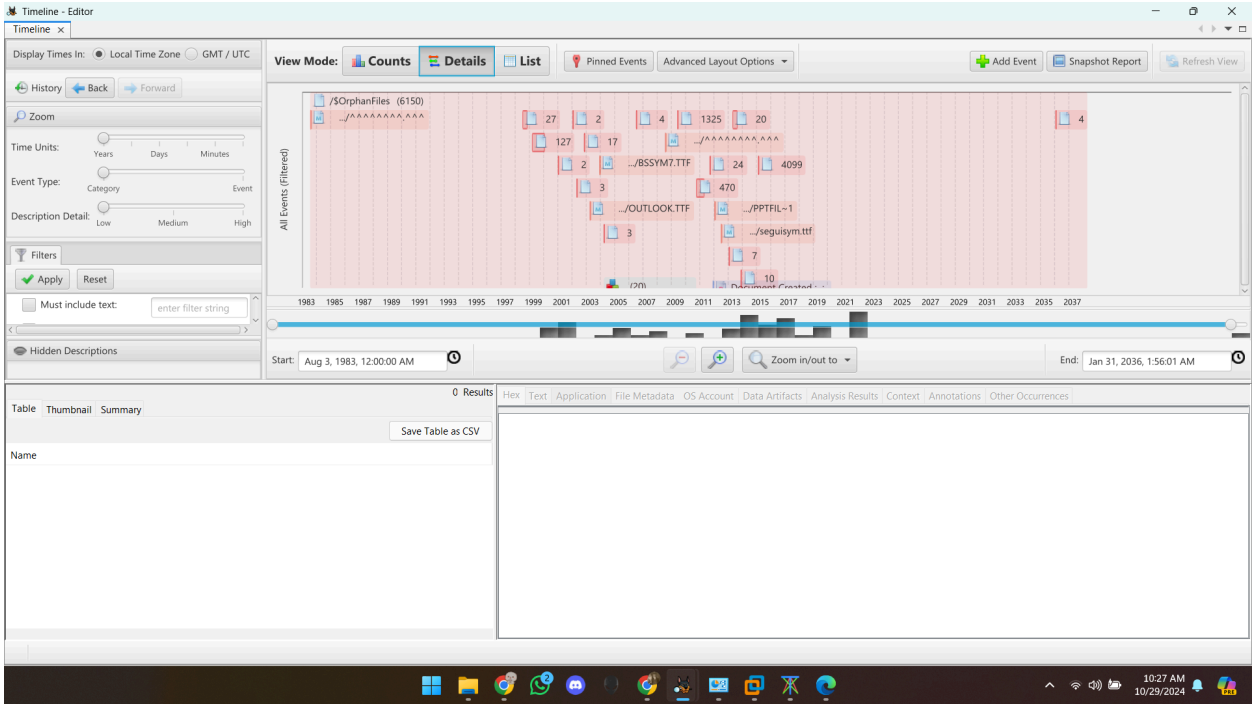
"To a patient scientist, the unfolding greenhouse mystery is far more exciting than the plot of the best mystery novel. But it is slow reading, with new clues sometimes not appearing for several years. Impatience increases when one realizes that it is not the fate of some fictional character, but of our planet and species, which hangs in the balance as the great carbon mystery unfolds at a seemingly glacial pace." — *D. Schindler*[1]

It is an epic story: the struggle of thousands of men and women over the course of a century for very high stakes. For some, the work required actual physical courage, a risk to life and limb in icy wastes or on the high seas. The rest needed more subtle forms of courage. They gambled decades of arduous effort on the chance of a useful discovery, and staked their reputations on what they claimed to have found. Even as they stretched their minds to the limit on intellectual problems that often proved insoluble, their attention was diverted into grueling administrative struggles to win minimal support for the great work. A few took the battle into the public arena, often getting more blame than praise; most labored to the end of their lives in obscurity. In the end they did win their goal, which was simply knowledge.

The scientists who labored to understand the Earth's climate discovered that many factors influence it. Everything from volcanoes to factories shape our winds and rains. The scientific research itself was shaped by many influences, from popular misconceptions to government funding, all happening at once. A traditional history would try to squeeze the story into a linear text, one event following another like beads on a string. Inevitably some parts are left out. Yet for

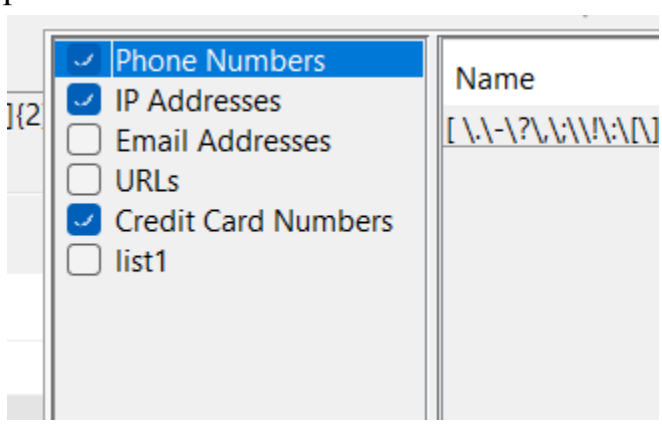
For timeline as we can use autopsy's timeline feature.





Credit Card, Phone Number, Ip address.

I used the keyword search module, and checked the credit card, ip address and phone numbers.



So after running it gave this output

Single Regular Expression Search (0)	0
Email Addresses (502)	1
IP Addresses (544)	1
Phone Numbers (142)	1

Ip addresses.

List Name	Files with Hits
0.0.0.0 (11)	11
0.1.0.2 (3)	3
0.1.2.3 (24)	24
0.1.2.4 (2)	2
0.1.2.5 (2)	2
0.1.3.4 (5)	5
0.1.4.5 (5)	5
0.1.4.7 (4)	4
0.1.5.6 (4)	4
0.1.6.7 (4)	4

0.1.2.4 (2)

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Con

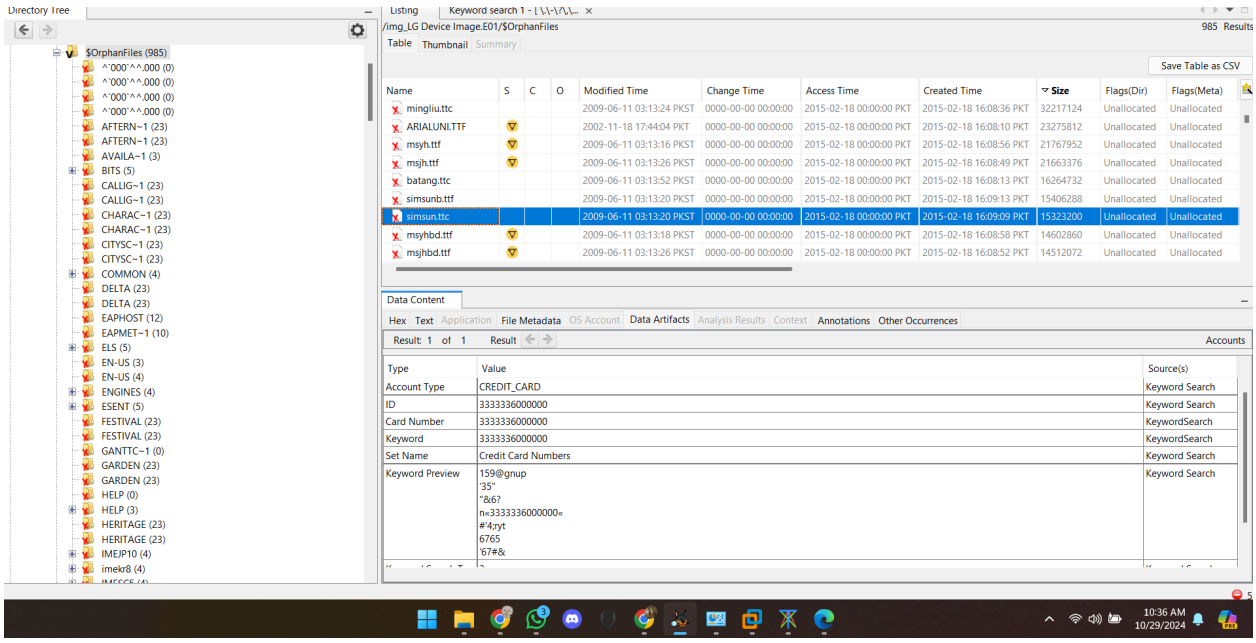
Phone numbers.

List Name	Files with Hits
(415) 961-8830 (7)	7
350 500 1000 (6)	6
350 556 1000 (6)	6
500 333 1000 (6)	6
500 444 1000 (6)	6
500 500 1000 (6)	6
556 333 1000 (6)	6
584 556 1015 (6)	6
667 333 1000 (6)	6
667 667 1000 (6)	6

Data Content

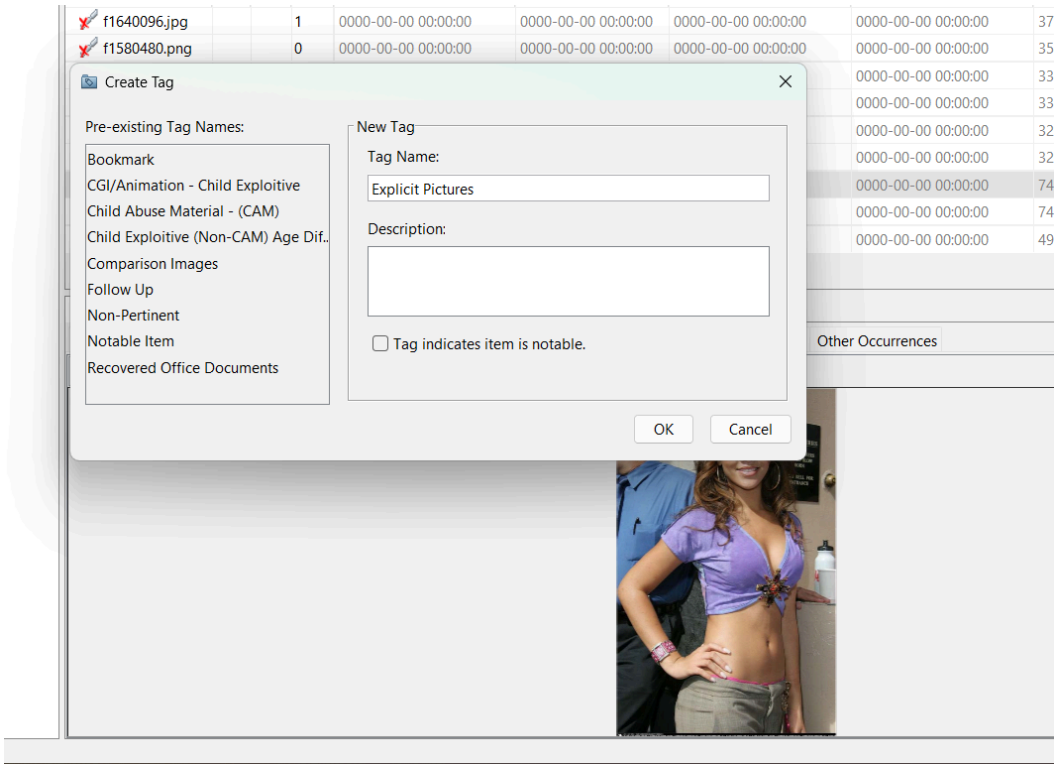
Hex | Text | Application | File Metadata | OS Account | Data Art

For Credit Card



Photos

For Explicit pictures i have generated a tag



And will tag every explicit picture in that.

Name	S	C	O	Modified Time	Change Time	Access Time
f1575680.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1575840.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1580384.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1649600.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1649504.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1580256.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1575968.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1648576.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0
f1648480.jpg			0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:0