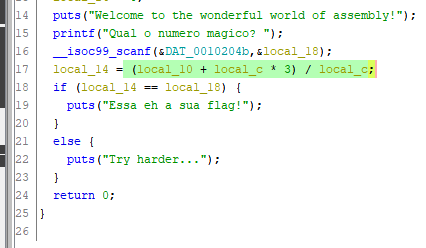
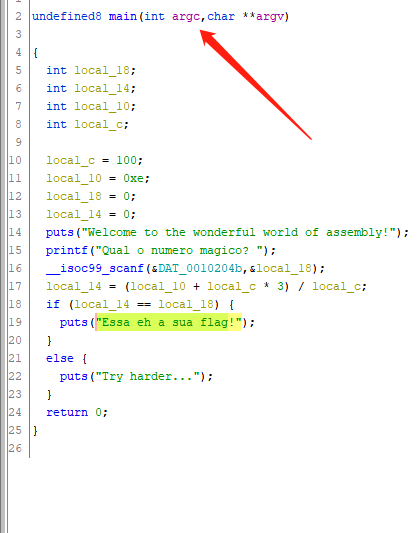
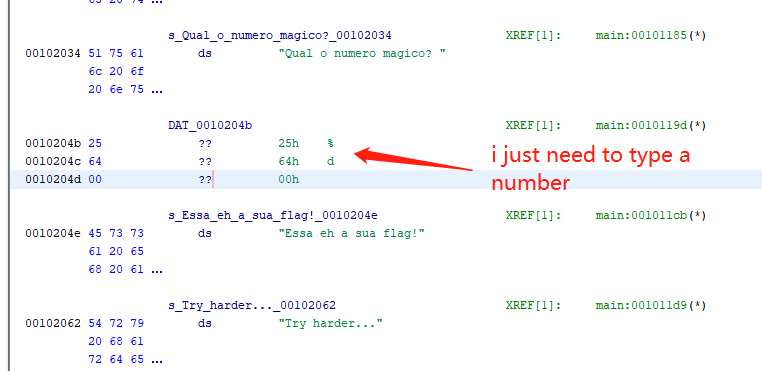
**CF assignment 10 \_\_A169180**

**2019/06/01**

**Zheng (Rio) Yin**

**Q1.**





C:\Users\10921\AppData\Local\Temp\WeChat Files\107484369427035268.pngFor how to get the password, u just need to type “3”. Cos the function is showed on pic 2.

There is a way we can abuse this code to accept a longer password. Give an example of a 12-character password that still provides us with a flag.

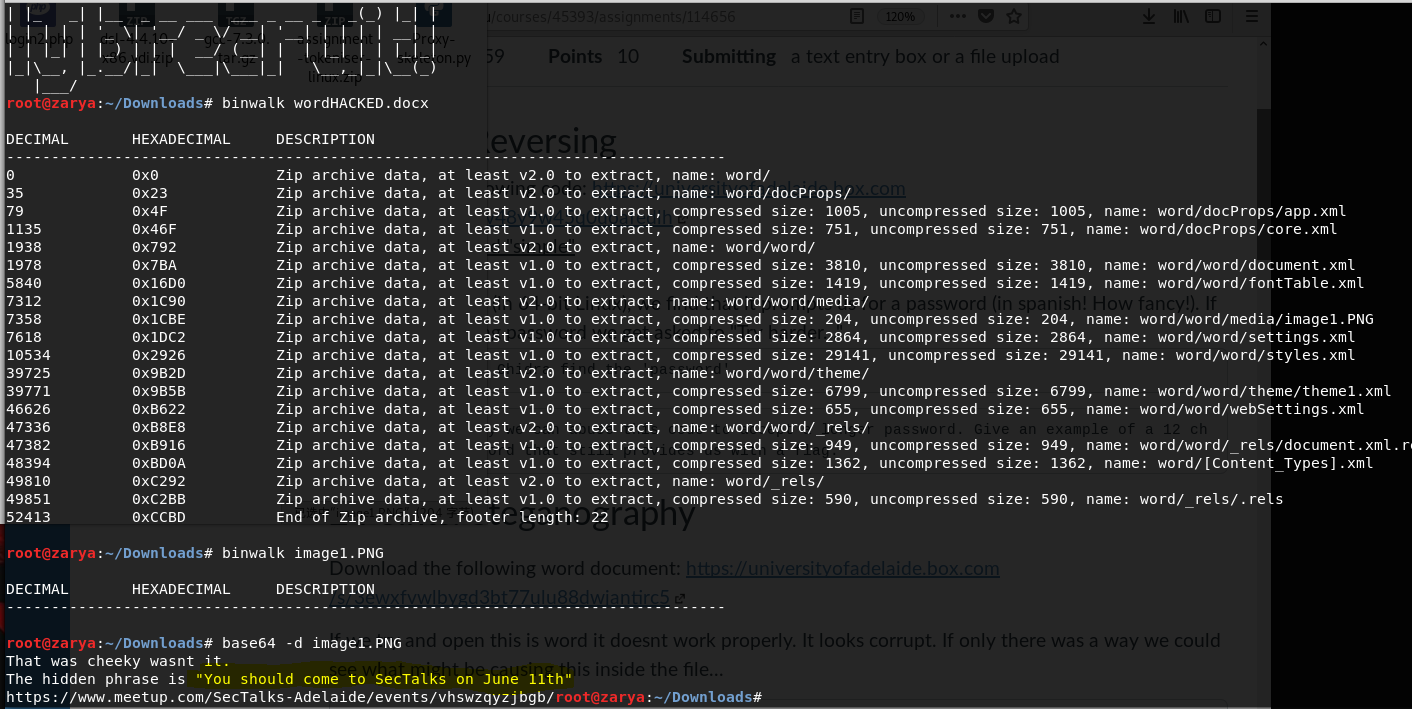
This program just scans first number. No matter how long remaining.

e.g. 3asdaadsfasdfsa

e.g. 3dfbhfdbfvfsathynujmhnb

e.g. 3tenfgklcujniomwerbergfdvdc

**Q2.**



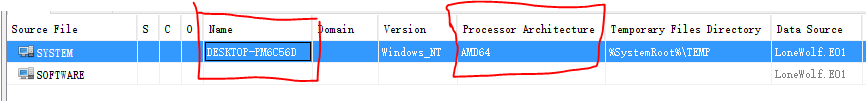
**Q3.**

**(1) What was the main users Windows Username? and other email/s used for cloud services?**

Main user: **jcloudy**



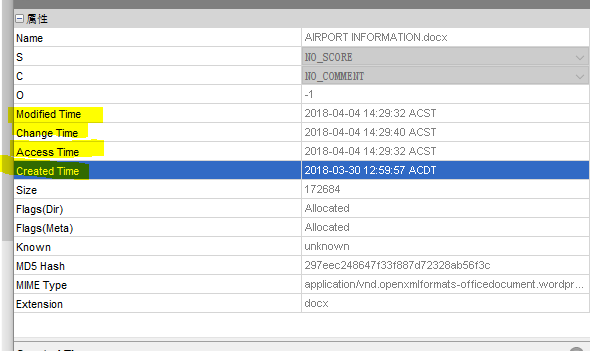
**(2) What is the Processor Architecture and computer name?**



**(3) What is an LNK file? What does it do? Give an example from the provided image?**

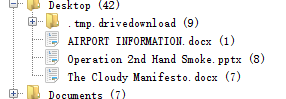
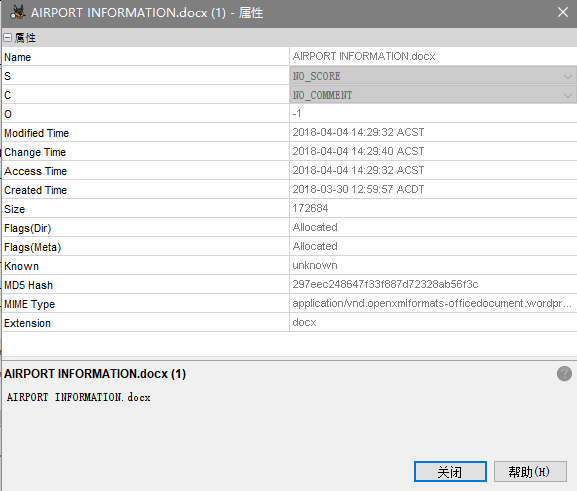
**LNK is a file extension for a shortcut file used by Microsoft Windows to point to an executable file. LNK stands for Link.**

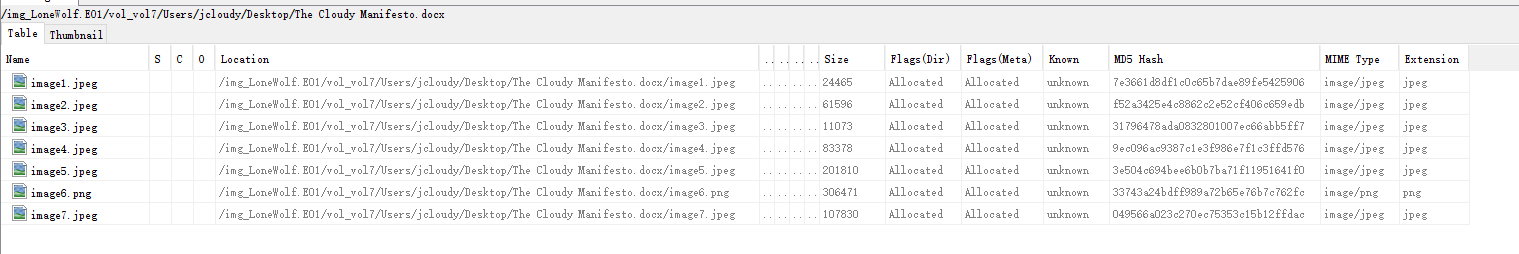


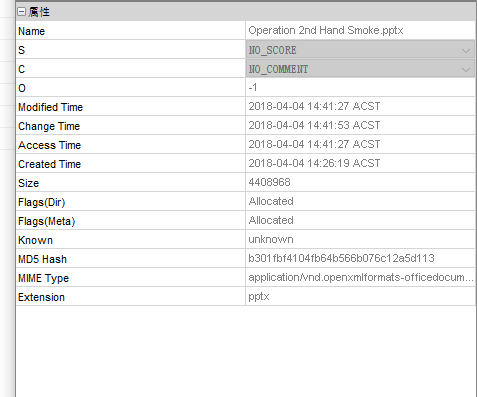
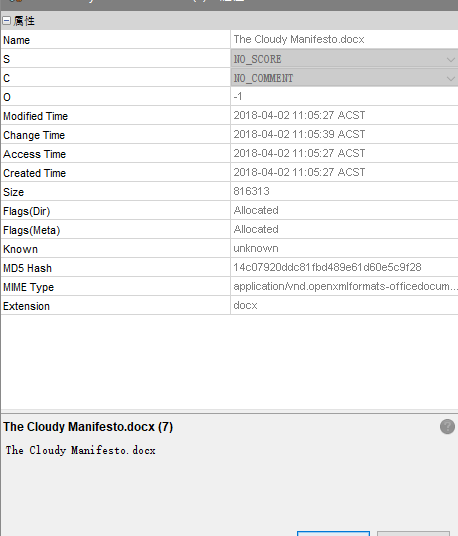
**(4) Windows has 3 different time stamps in each files metadata, what are they, and how are they different?**

**It’s created time (when this file created), access time (when this file accessed) and created time (when this file created)**.

**(5) The user had lots of files on their desktop, what evidence can be found in this folder to help the investigators?**





For the document <<airport information.docx>>:

* American airlines unfinished payment.
* Dulles Airport traffic info.

For the document <<Operation 2nd Hand Smoke.pptx>>:

* “Town Hall For Our Lives” speech event time and google map reality marked.
* Route from the airport to the speech location.
* Place of stay.
* Detail of air tickets.

For the document <<The cloudy Manifesto.docx>>:

* Actions, believe that the government cannot protect the peoples.

**(6) What went on? From all the documents we found can you put together the plans that the suspect wanted to carry out? Remember to stick to the facts only as a forensic expert it's not up to us to tell the story, just present the facts in an unbiased way. Please summarize what we know in a paragraph.**

After i analysis the timeline, suspects searched those things:

“Can I sync a file to multiple cloud storage locations?”

“cloud storage solutions”

“amazon cloud storage”

“can I use amazon s3 for free”

“sync amazon s3 from desktop”

“tntdrive”

“shooting range”

“just how easy is it to buy an illegal gun”

“new phones and map of gun free zones”

“democratic offices in DC”----“430 south capitol street”

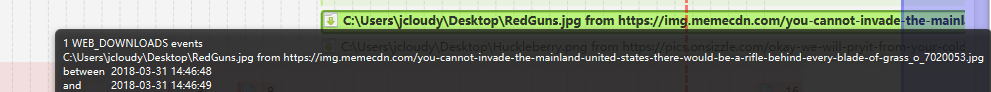
“police response times by zip code”

“which state has the worst police response times”

“how to use google docs as chat”







Timeline should like:

