U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND

DATA & ANALYSIS CENTER

CAPTURE THE FLAG 2.0

Dr. Oscar Perez, Stephen Cruz, Herandy Vazquez,
Juan Ulloa, Andrew Clanan, Salvador Melendez

15 JUL 2021

CODE OF ETHICS

- This workshop is intended to be an education tool to make students aware of the risks of electronic communications.
- The future of electronic communications has to be in charge of a cyber police with the highest standards of ethics.

- **What is ethics? moral principles that govern a person's behavior or the conducting of an activity. Always remember:**

WITH
GREAT
POWER COMES
GREAT
RESPONSIBILITY

WORKSHOP OBJECTIVES

Today, you will learn about:

✓***Social Engineering***

** Dumpster Diving*

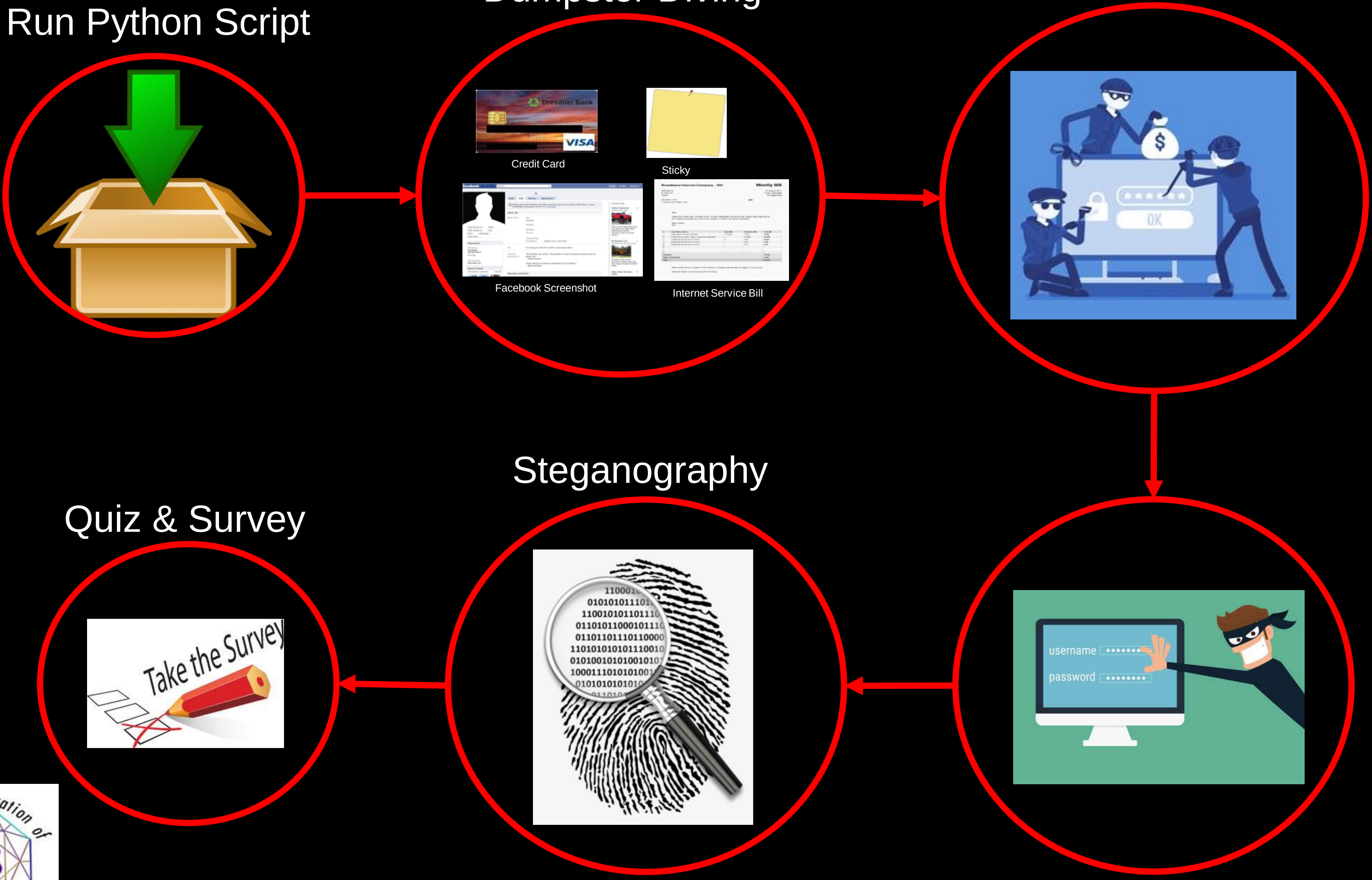
✓***Encryption***

** Encoding/Decoding (e.g. steganography)*
** Password Auditing (e.g .john)*

✓***Access Control***

** User/Admin Level (e.g. ssh)*

OVERVIEW



Download and Run Python Script

Dumpster Diving

[redacted]

Credit Card

Sticky

Facebook Screenshot

Internet Service Bill

Password Auditing

Access Control

Steganography

Quiz & Survey

DUMPSTER DIVING

WHAT?
Social Engineering technique used to gather Personal Identifiable Information (PII).

HOW?
Looking into the trash, websites, mailboxes, etc. and putting pieces together.

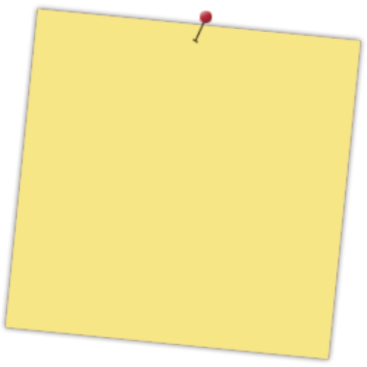
EXAMPLES OF DOCUMENTS:
Credit Card, Electricity Bill, Facebook Profile, Paper Notes.

DUMPSTER DIVING

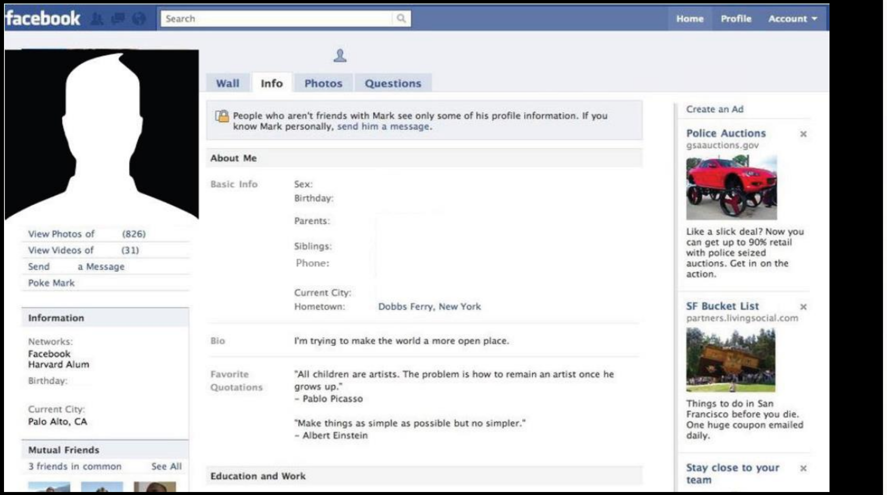
[redacted]

[redacted]

Credit Card



Sticky Note



People who aren't friends with Mark see only some of his profile information. If you know Mark personally, send him a message.

View Photos of (826)
View Videos of (31)
Send a Message
Poke Mark

Information

Networks:
Facebook
Harvard Alum
Birthday:

Current City:
Palo Alto, CA

Mutual Friends

3 friends in common See All

About Me

Basic Info	Sex:	
	Birthday:	
	Parents:	
	Siblings:	
	Phone:	
	Current City:	
	Hometown:	Dobbs Ferry, New York
Bio	I'm trying to make the world a more open place.	
Favorite Quotations	"All children are artists. The problem is how to remain an artist once he grows up." - Pablo Picasso "Make things as simple as possible but no simpler." - Albert Einstein	

Education and Work

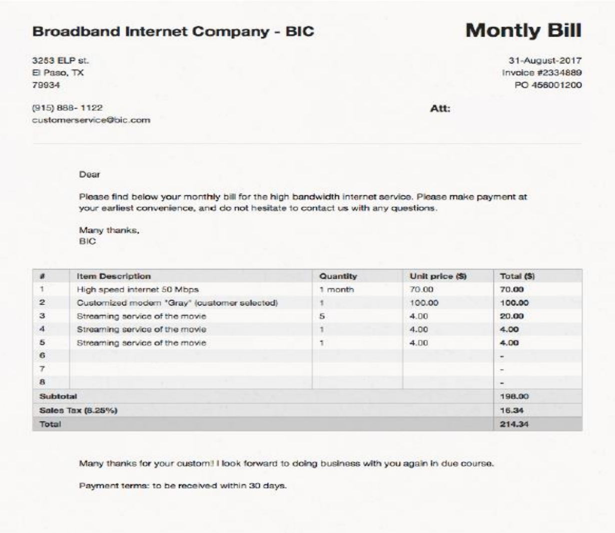
Create an Ad

Police Auctions
gsaauctions.gov
Like a slick deal? Now you can get up to 90% retail with police seized auctions. Get in on the action.

SF Bucket List
partners.livingsocial.com
Things to do in San Francisco before you die. One huge coupon emailed daily.

Stay close to your team

Facebook Screenshot



Broadband Internet Company - BIC

Montly Bill

3253 ELP st.
El Paso, TX
79934

(915) 888- 1122
customerservice@bic.com

31-August-2017
Invoice #2334889
PO 456001200

Att:

Dear

Please find below your monthly bill for the high bandwidth internet service. Please make payment at your earliest convenience, and do not hesitate to contact us with any questions.

Many thanks,
BIC

#	Item Description	Quantity	Unit price ($)	Total ($)
1	High speed internet 50 Mbps	1 month	70.00	70.00
2	Customized modem "Gray" (customer selected)	1	100.00	100.00
3	Streaming service of the movie	5	4.00	20.00
4	Streaming service of the movie	1	4.00	4.00
5	Streaming service of the movie	1	4.00	4.00
6				-
7				-
8				-
Subtotal				198.00
Sales Tax (8.25%)				16.34
Total				214.34

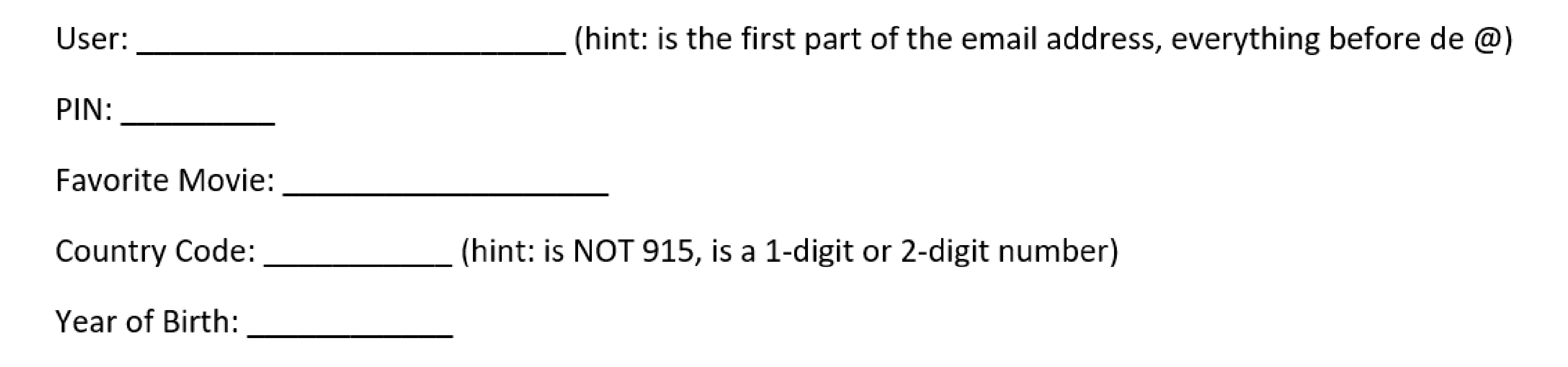
Many thanks for your custom!! I look forward to doing business with you again in due course.

Payment terms: to be received within 30 days.

Internet Service Bill

DUMPSTER DIVING

- By performing Dumpster Diving, you will get important personal identifiable information (PII) of a person.
- Write down on a paper the following information of the person you are investigating:



User: ___________________________ (hint: is the first part of the email address, everything before de @)

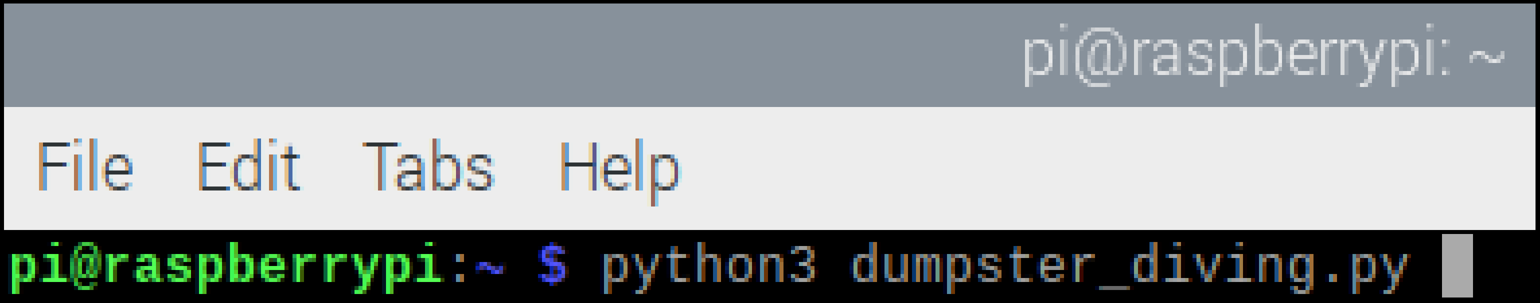
PIN: __________

Favorite Movie: ____________________

Country Code: ____________ (hint: is NOT 915, is a 1-digit or 2-digit number)

Year of Birth: _____________

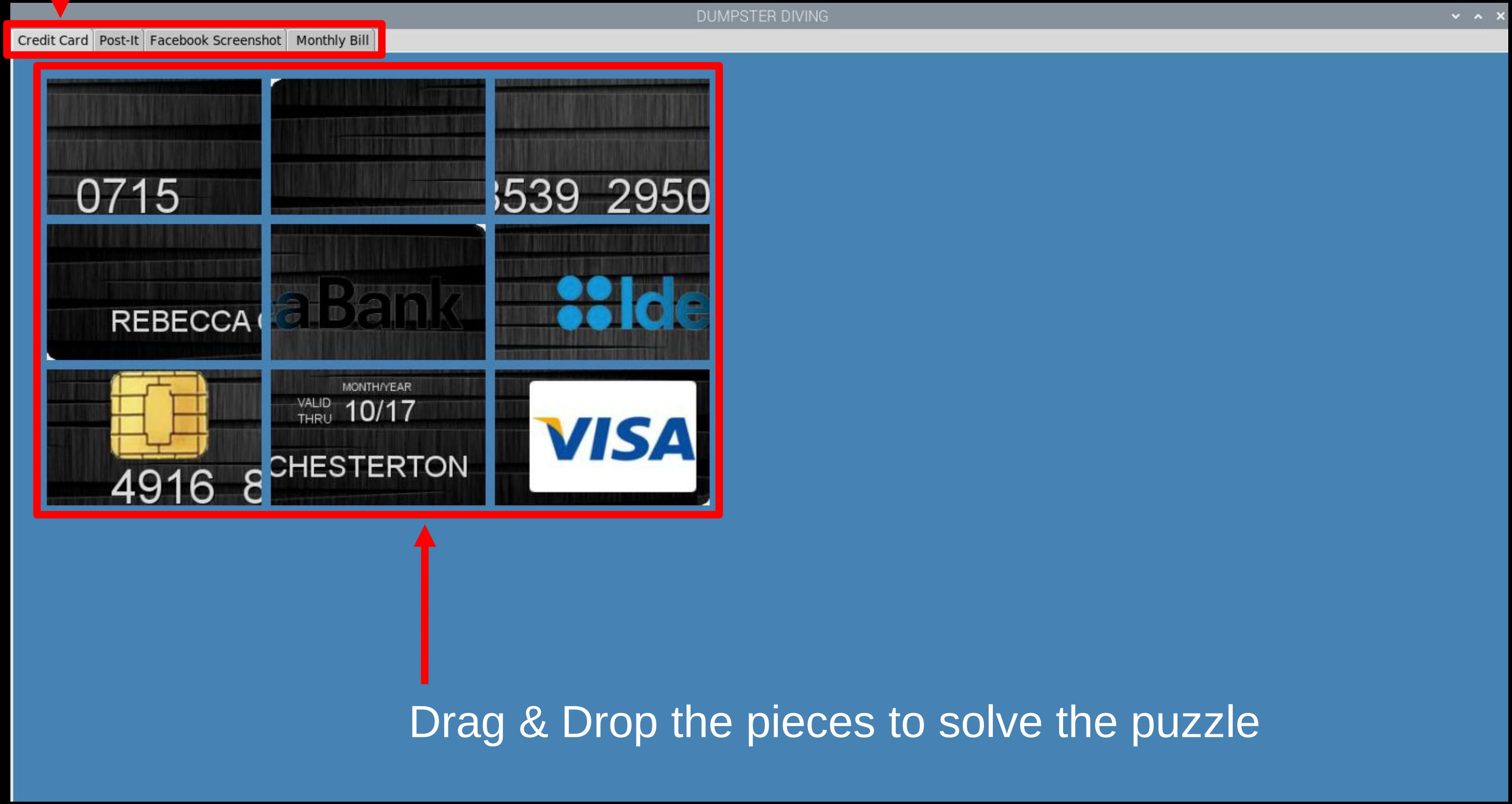
Dumpster Diving Command



```
pi@raspberrypi:~ $ python3 dumpster_diving.py
```

DUMPSTER DIVING

4 Tabs → 1) Credit Card, 2) Post-It, 3) Facebook Profile, and 4) Monthly Bill



Drag & Drop the pieces to solve the puzzle

PASSWORD AUDITING

WHAT?

Is the process of guessing a password by hashing different words and comparing those hashes against the hash to be guessed.

HOW?

Using John The Ripper (john for short)

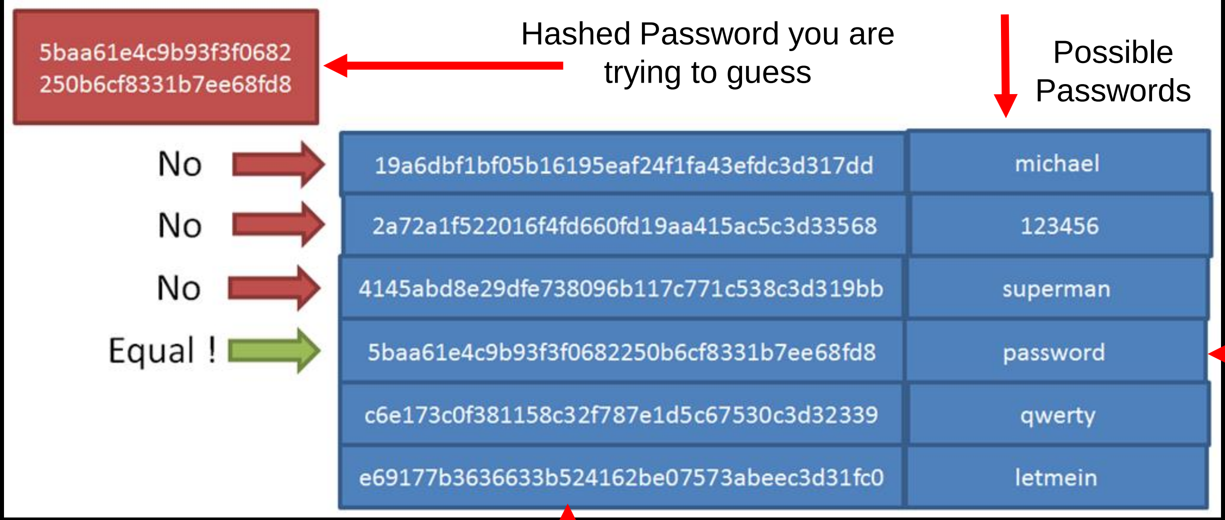
Command:

```
john --wordlist=cracking_wordlist.txt shadow
```

John The Ripper

List of possible dictionary words to hash and compare against the hashes inside the “shadow” file

File that contains the hashes to crack



Hashed Password you are trying to guess

5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8

Possible Passwords

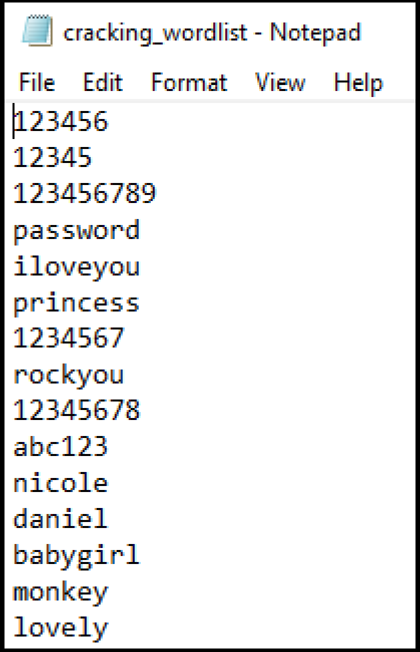
No	19a6dbf1bf05b16195eaf24f1fa43efdc3d317dd	michael
No	2a72a1f522016f4fd660fd19aa415ac5c3d33568	123456
No	4145abd8e29dfe738096b117c771c538c3d319bb	superman
Equal !	5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8	password
	c6e173c0f381158c32f787e1d5c67530c3d32339	qwerty
	e69177b3636633b524162be07573abeec3d31fc0	letmein

This password matches the hash!

Possible Hashes

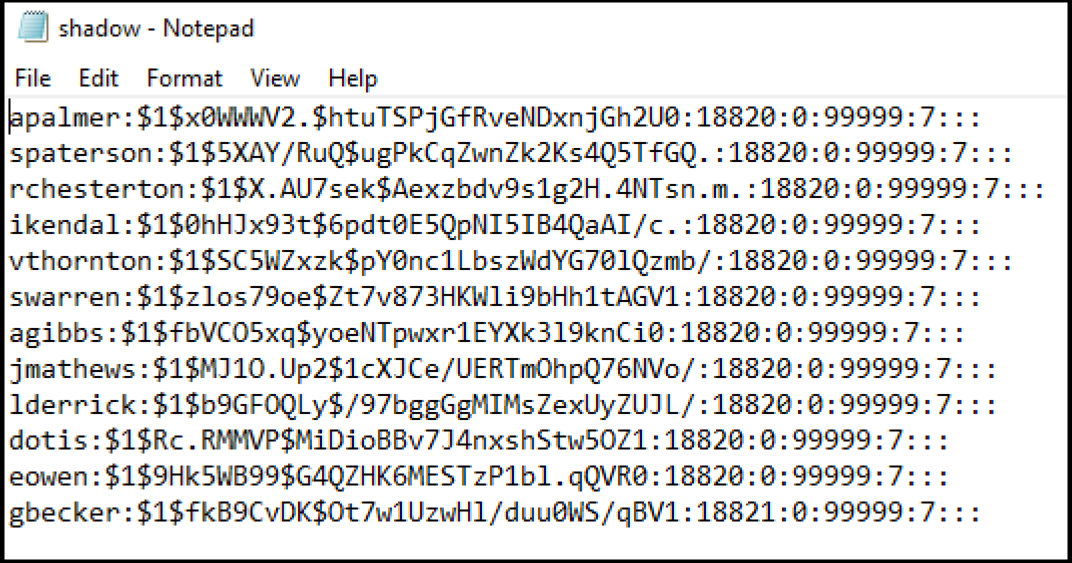
PASSWORD AUDITING

Wordlist



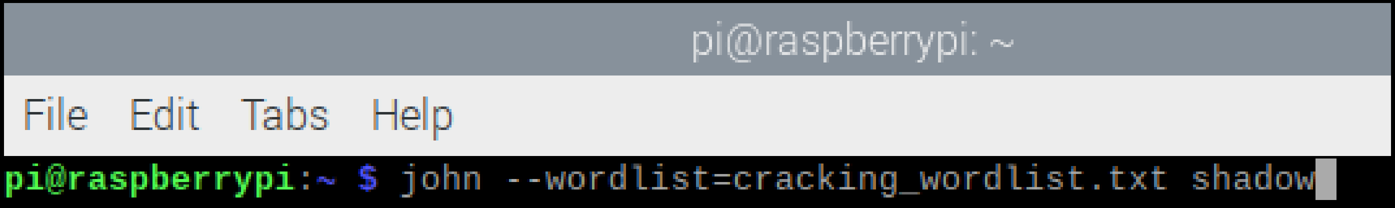
```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
```

Shadow File



```
apalmer:$1$x0WWWV2.$htuTSPjGfRveNDxnjGh2U0:18820:0:99999:7:::
spaterson:$1$5XAY/RuQ$ugPkCqZwnZk2Ks4Q5TfGQ.:18820:0:99999:7:::
rchesterton:$1$X.AU7sek$Aexzbdv9s1g2H.4NTsn.m.:18820:0:99999:7:::
ikendal:$1$0hHJx93t$6pdt0E5QpNI5IB4QaAI/c.:18820:0:99999:7:::
vthornton:$1$SC5WZxzk$pY0nc1LbszWdYG701Qzmb/:18820:0:99999:7:::
swarren:$1$zlos79oe$Zt7v873HKWli9bHh1tAGV1:18820:0:99999:7:::
agibbs:$1$fbVCO5xq$yoeNTpwxr1EYXk319knCi0:18820:0:99999:7:::
jmathews:$1$MJ1O.Up2$1cXJCe/UERTmOhpQ76NVo/:18820:0:99999:7:::
lderrick:$1$b9GFOQLy$/97bggGgMIMsZexUyZUJL/:18820:0:99999:7:::
dotis:$1$Rc.RMMVP$MiDioBBv7J4nxshStw5OZ1:18820:0:99999:7:::
eowen:$1$9Hk5WB99$G4QZHK6MESTzP1bl.qQVR0:18820:0:99999:7:::
gbecker:$1$fkB9CvDK$Ot7w1UzwHl/duu0WS/qBV1:18821:0:99999:7:::
```

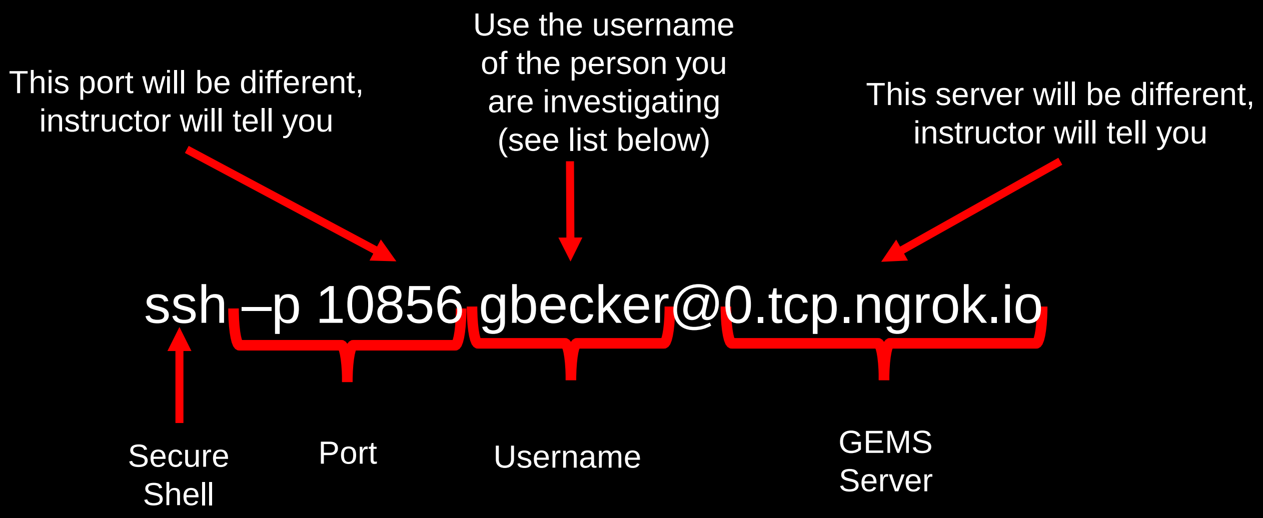
john Command



```
pi@raspberrypi:~ $ john --wordlist=cracking_wordlist.txt shadow
```

ACCESS CONTROL

– Establish a SSH connection to the GEMS server:



This port will be different, instructor will tell you

Use the username of the person you are investigating (see list below)

This server will be different, instructor will tell you

```
ssh –p 10856 gbecker@0.tcp.ngrok.io
```

Secure Shell

Port

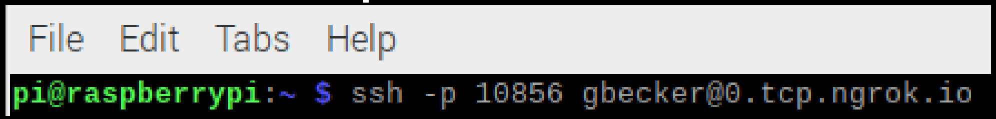
Username

GEMS Server

Possible Usernames (check which one belongs to the person your are investigating):

- gbecker
- apalmer
- spaterson
- rchesterton
- ikendal
- vthornton
- swarren
- agibbs
- jmathews
- lderrick
- dotis
- eowen

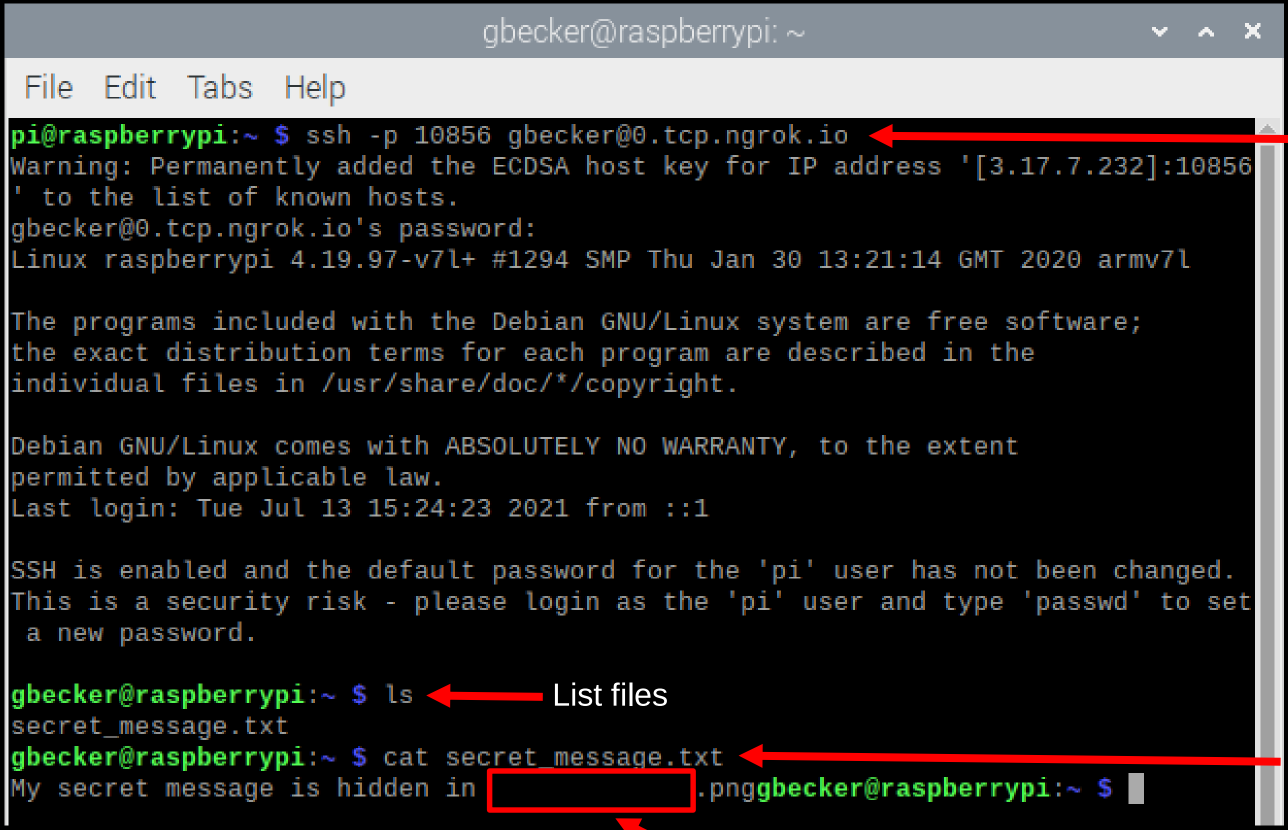
Example Command:



```
pi@raspberrypi:~ $ ssh -p 10856 gbecker@0.tcp.ngrok.io
```

ACCESS CONTROL

- After you establish the SSH connection, list files using ls
- If you find the file “secret_message.txt”, use the cat command to see its contents
- Write down the name of the image with the secret message, you will need it



```
pi@raspberrypi:~ $ ssh -p 10856 gbecker@0.tcp.ngrok.io
Warning: Permanently added the ECDSA host key for IP address '[3.17.7.232]:10856
' to the list of known hosts.
gbecker@0.tcp.ngrok.io's password:
Linux raspberrypi 4.19.97-v7l+ #1294 SMP Thu Jan 30 13:21:14 GMT 2020 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 13 15:24:23 2021 from ::1

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
 a new password.

gbecker@raspberrypi:~ $ ls
secret_message.txt
gbecker@raspberrypi:~ $ cat secret_message.txt
My secret message is hidden in [redacted].pnggbecker@raspberrypi:~ $
```

ssh connection

List files

See contents of file

Name of image with secret message

STEGANOGRAPHY

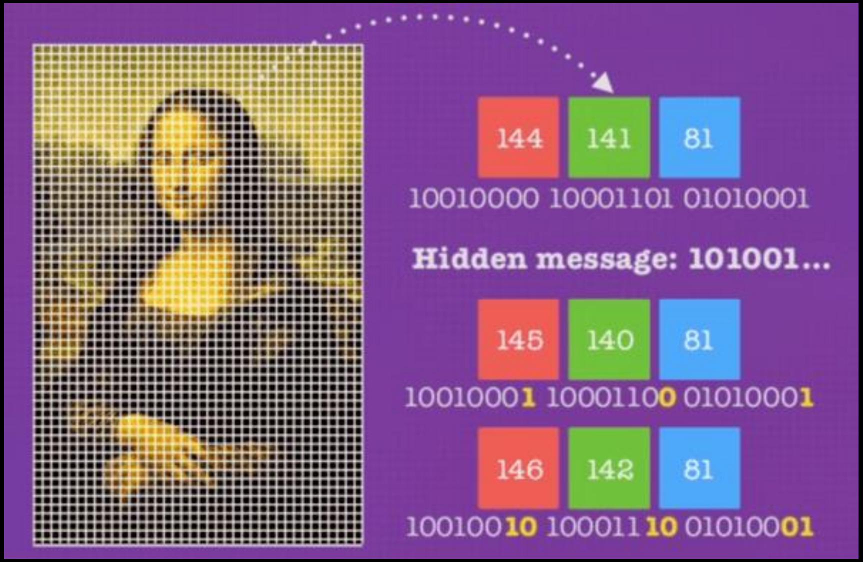
What?

- A technique used to hide data within an ordinary file (e.g. image, sound, text, etc.) to keep information secret from a naked eye.

- Steganography can be combined with Encryption to provide more security

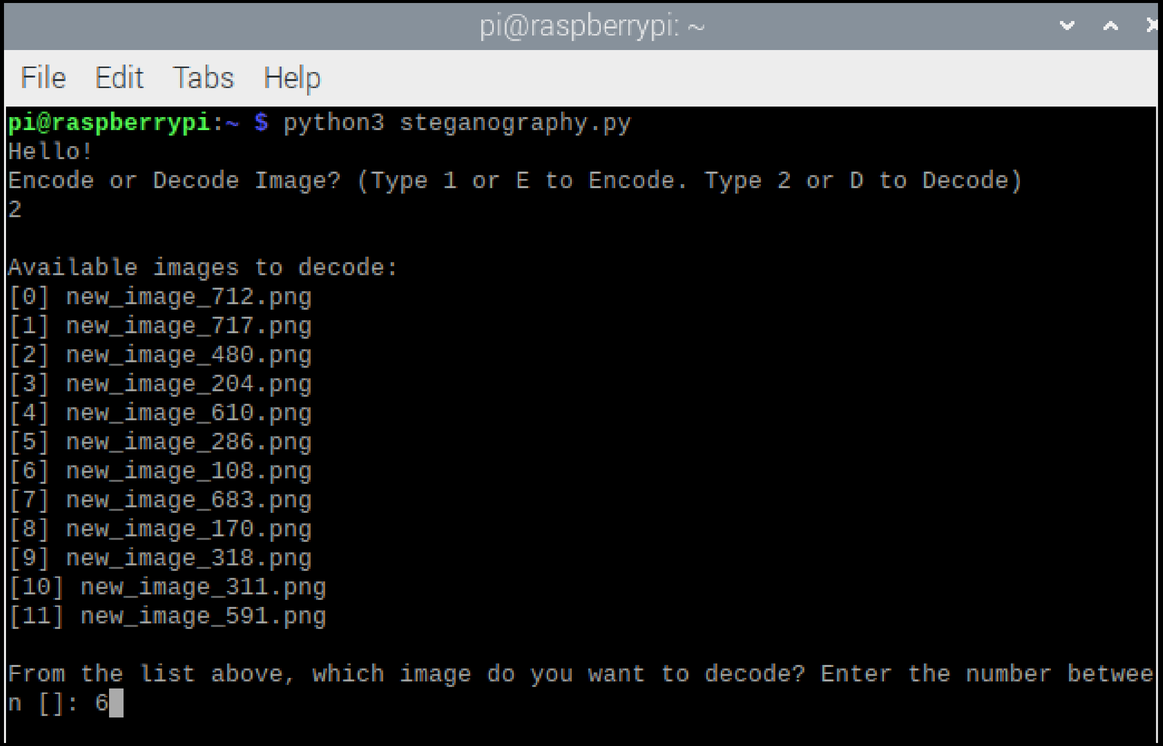
Steganography on Images.

- Each pixel in the image has colors defined in RGB (Red, Green, Blue) format → Color intensity ranges from 0 to 255



STEGANOGRAPHY

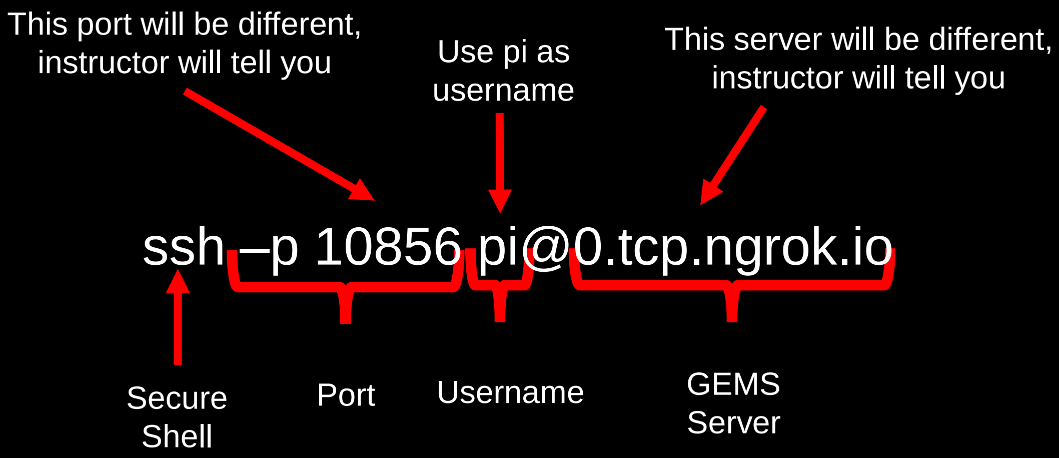
- You will be prompted if you want to “Encode” or “Decode”.
    - Type “1” or “E” or “e” to Encode
    - Type “2” or “D” or “d” to Decode
- Type 2, hit enter, then type the NUMBER between brackets, hit enter
- Write down the secret message that belongs to the person you are investigating.



```
pi@raspberrypi:~ $ python3 steganography.py
Hello!
Encode or Decode Image? (Type 1 or E to Encode. Type 2 or D to Decode)
2

Available images to decode:
[0] new_image_712.png
[1] new_image_717.png
[2] new_image_480.png
[3] new_image_204.png
[4] new_image_610.png
[5] new_image_286.png
[6] new_image_108.png
[7] new_image_683.png
[8] new_image_170.png
[9] new_image_318.png
[10] new_image_311.png
[11] new_image_591.png

From the list above, which image do you want to decode? Enter the number betwee
n []: 6
```

ACCESS CONTROL

- Establish a SSH connection to the GEMS server



This port will be different, instructor will tell you

Use pi as username

This server will be different, instructor will tell you

ssh –p 10856 pi@0.tcp.ngrok.io

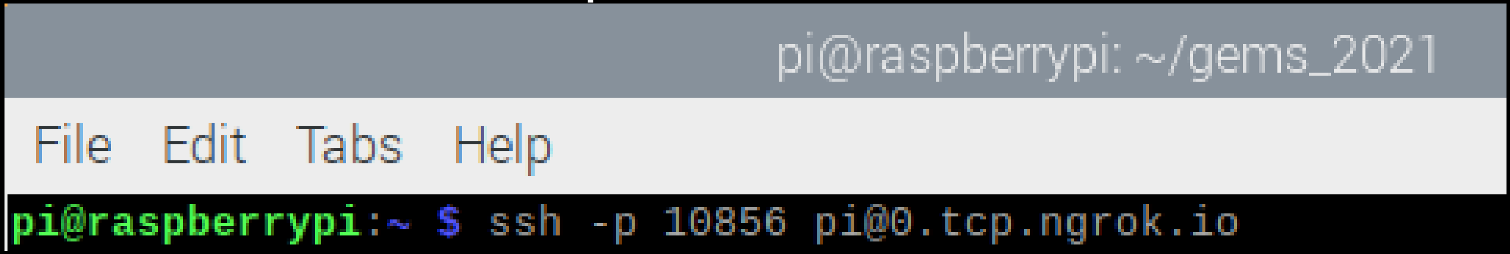
Secure Shell

Port

Username

GEMS Server

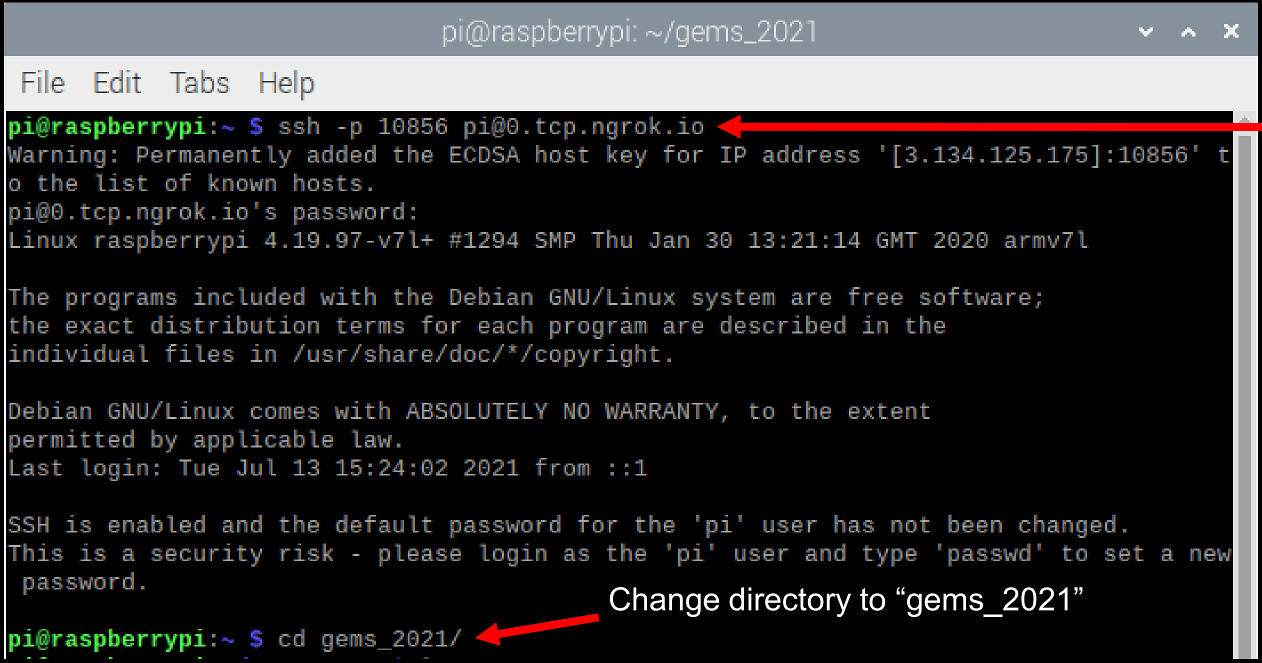
Example Command:



```
pi@raspberrypi:~ $ ssh -p 10856 pi@0.tcp.ngrok.io
```

ACCESS CONTROL

- After you establish the SSH connection, cd into the “gems_2021” folder.

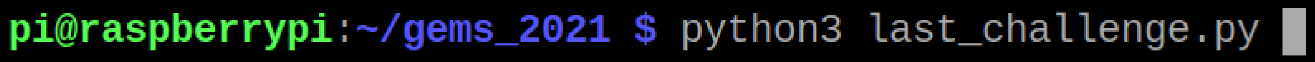


```
pi@raspberrypi:~ $ ssh -p 10856 pi@0.tcp.ngrok.io
Warning: Permanently added the ECDSA host key for IP address '[3.134.125.175]:10856' t
o the list of known hosts.
pi@0.tcp.ngrok.io's password:
Linux raspberrypi 4.19.97-v7l+ #1294 SMP Thu Jan 30 13:21:14 GMT 2020 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jul 13 15:24:02 2021 from ::1

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new
 password.

pi@raspberrypi:~ $ cd gems_2021/
```

ssh connection

Change directory to “gems_2021”

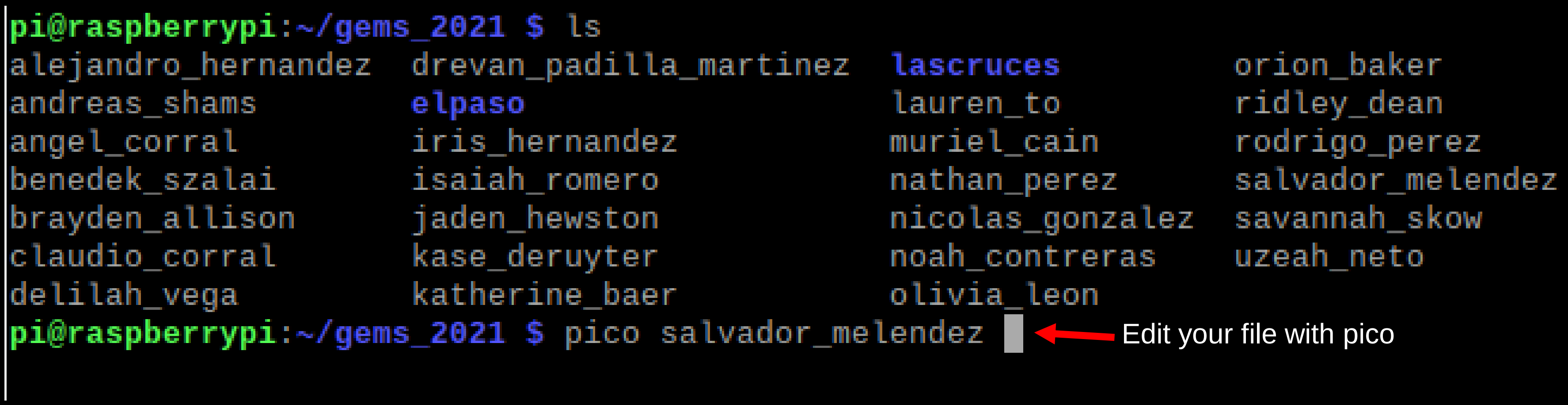
- Run the “last_challenge.py” script and answer the questions to unlock the survey.



```
pi@raspberrypi:~/gems_2021 $ python3 last_challenge.py
```

ACCESS CONTROL

- List files with “ls”, and look for your name.
- Use pico to edit the file with your name.

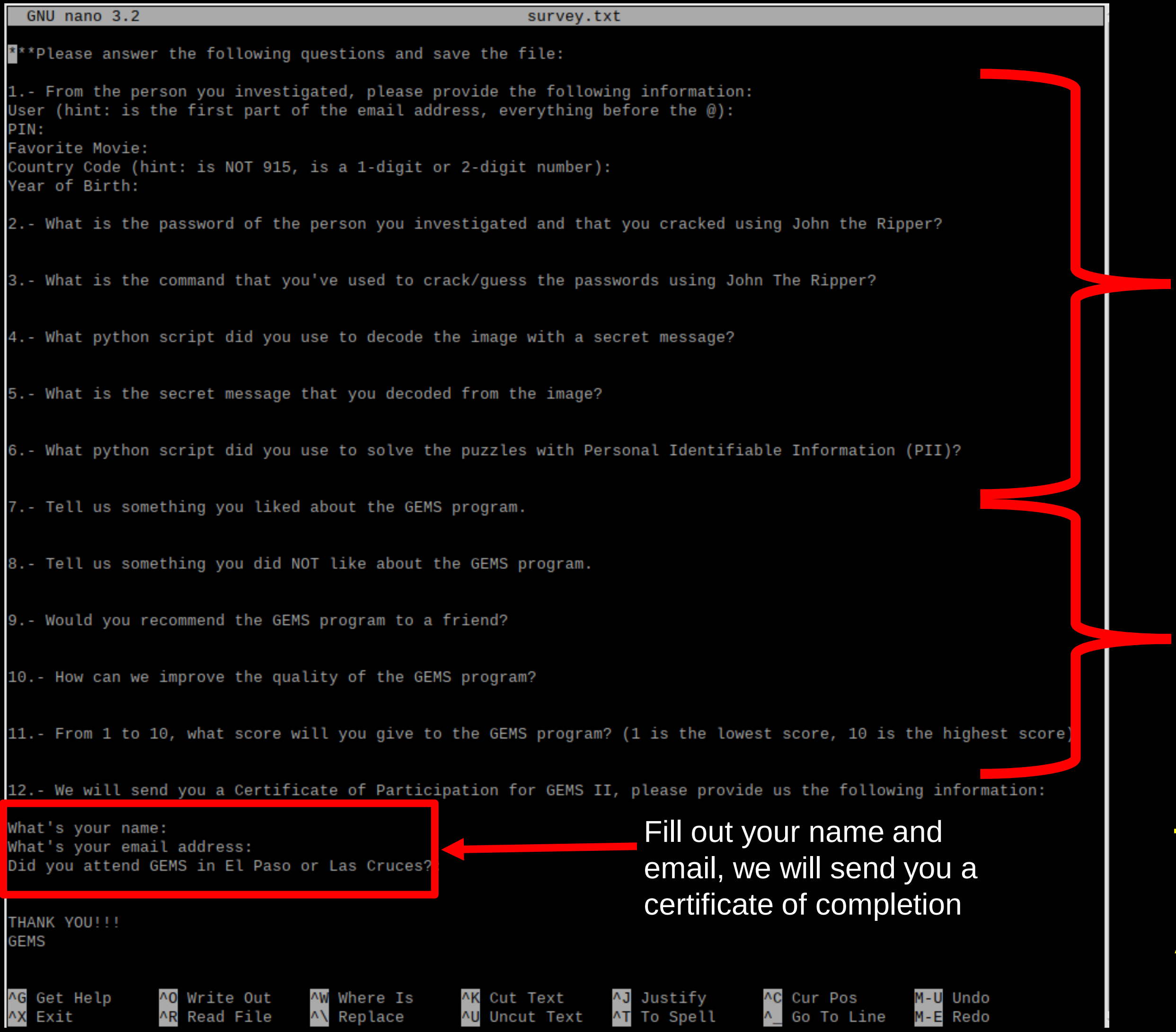


```
pi@raspberrypi:~/gems_2021 $ ls
alejandro_hernandez  drevan_padilla_martinez  lascruces          orion_baker
andreas_shams        elpaso                   lauren_to          ridley_dean
angel_corral         iris_hernandez           muriel_cain        rodrigo_perez
benedek_szalai       isaiah_romero            nathan_perez       salvador_melendez
brayden_allison      jaden_hewston            nicolas_gonzalez   savannah_skow
claudio_corral       kase_deruyter            noah_contreras     uzeah_neto
delilah_vega         katherine_baer           olivia_leon
pi@raspberrypi:~/gems_2021 $ pico salvador_melendez
```

Edit your file with pico

SURVEY

– Answer the Quiz & Survey.



```
 GNU nano 3.2                                        survey.txt

***Please answer the following questions and save the file:

1.- From the person you investigated, please provide the following information:
User (hint: is the first part of the email address, everything before the @):
PIN:
Favorite Movie:
Country Code (hint: is NOT 915, is a 1-digit or 2-digit number):
Year of Birth:

2.- What is the password of the person you investigated and that you cracked using John the Ripper?


3.- What is the command that you've used to crack/guess the passwords using John The Ripper?


4.- What python script did you use to decode the image with a secret message?


5.- What is the secret message that you decoded from the image?


6.- What python script did you use to solve the puzzles with Personal Identifiable Information (PII)?


7.- Tell us something you liked about the GEMS program.


8.- Tell us something you did NOT like about the GEMS program.


9.- Would you recommend the GEMS program to a friend?


10.- How can we improve the quality of the GEMS program?


11.- From 1 to 10, what score will you give to the GEMS program? (1 is the lowest score, 10 is the highest score)


12.- We will send you a Certificate of Participation for GEMS II, please provide us the following information:

What's your name:
What's your email address:
Did you attend GEMS in El Paso or Las Cruces?


THANK YOU!!!
GEMS


^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line   M-E Redo
```

Answer the Quiz

Answer the Survey

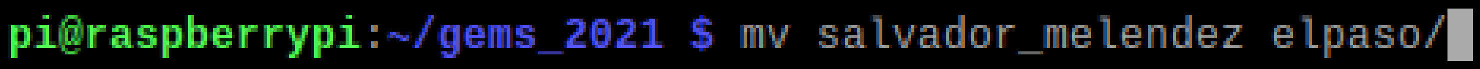
Fill out your name and email, we will send you a certificate of completion

DON'T FORGET TO SAVE THE FILE WITH YOUR ANSWERS!!!

SURVEY

- Move your file to “elpaso” or “lascruces” (depending on where you are at).

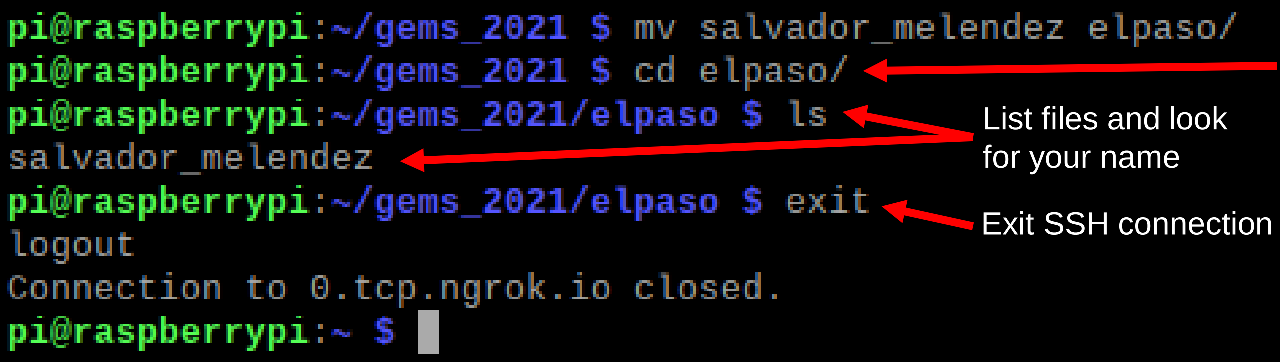
Example Command:



```
pi@raspberrypi:~/gems_2021 $ mv salvador_melendez elpaso/
```

- Verify if your file was moved by using cd and ls (as shown below), then exit the SSH connection by typing “exit”.

Example Command:



```
pi@raspberrypi:~/gems_2021 $ mv salvador_melendez elpaso/
pi@raspberrypi:~/gems_2021 $ cd elpaso/
pi@raspberrypi:~/gems_2021/elpaso $ ls
salvador_melendez
pi@raspberrypi:~/gems_2021/elpaso $ exit
logout
Connection to 0.tcp.ngrok.io closed.
pi@raspberrypi:~ $
```

Change directory to “elpaso” or “lascruces”

List files and look for your name

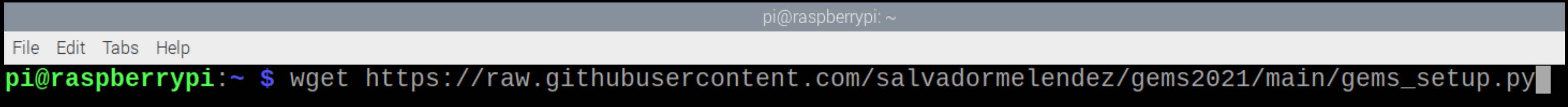
Exit SSH connection

DOWNLOAD FILES

- Ready for the challenge?
- Open a terminal and download all the needed scripts from the internet by using the following command:

wget https://raw.githubusercontent.com/salvadormelendez/gems2021/main/gems_setup.py

Example Command:



```
pi@raspberrypi:~ $ wget https://raw.githubusercontent.com/salvadormelendez/gems2021/main/gems_setup.py
```

- Run the python script by typing:

    python3 gems_setup.py

- Wait until you see a message saying: “You are all set!”

- Start the challenge with Dumpster Diving (slide 7). Follow slides 7 through 18.

    These slides are in your Raspberry Pi (/home/pi/challenge.pdf)

    To open the slides, open a terminal and type the following command:

    xdg-open challenge.pdf

CONTACT INFORMATION

Salvador Melendez, Ph.D.

UNCLASSIFIED email: salvador.melendez3.civ@mail.mil