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:**

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

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?

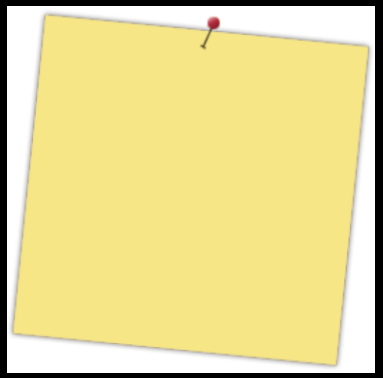
Looking into the trash, websites, mailboxes, etc. and putting pieces together.

EXAMPLES OF DOCUMENTS:

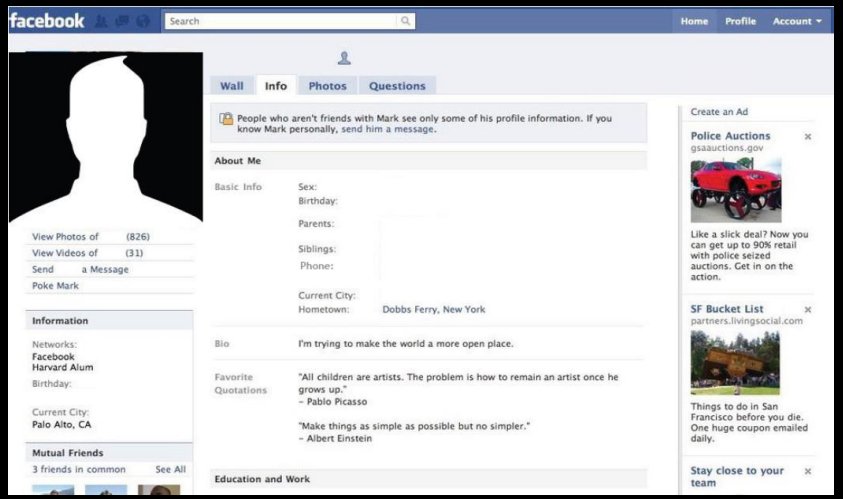
Credit Card, Electricity Bill, Facebook Profile, Paper Notes.

DUMPSTER DIVING

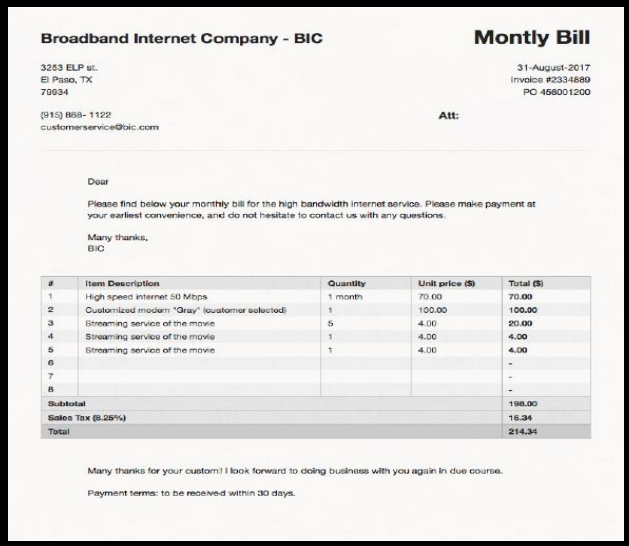
Credit Card



Sticky Note



Facebook Screenshot



Broadband Internet Company - BIC

Montly Bill

3253 ELP st.
El Paso, TX
79934

31-August-2017
Invoice #2334689
PO 456001200

(915) 888- 1122
customerservice@bic.com

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 @)

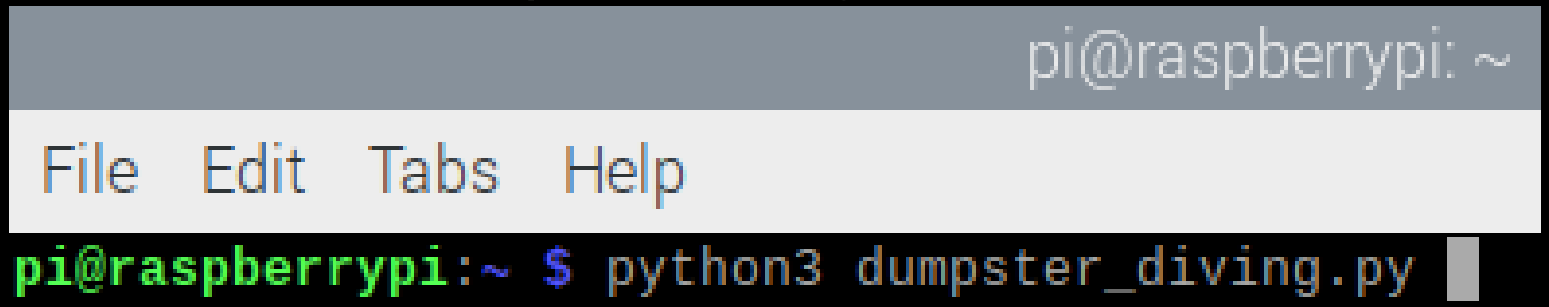
PIN: _____

Favorite Movie: _____

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

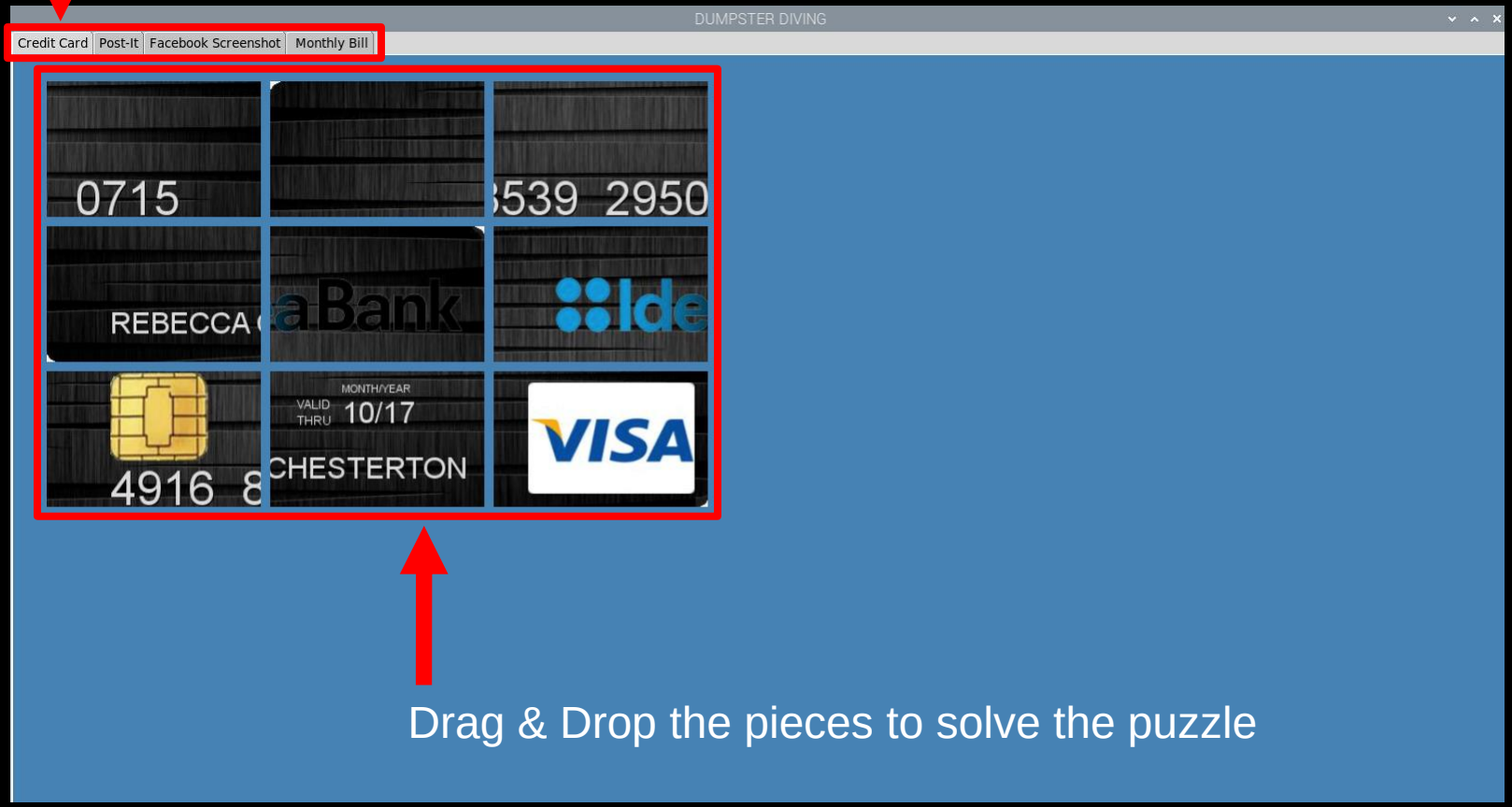
Year of Birth: _____

Dumpster Diving Command



DUMPSTER DIVING

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



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)

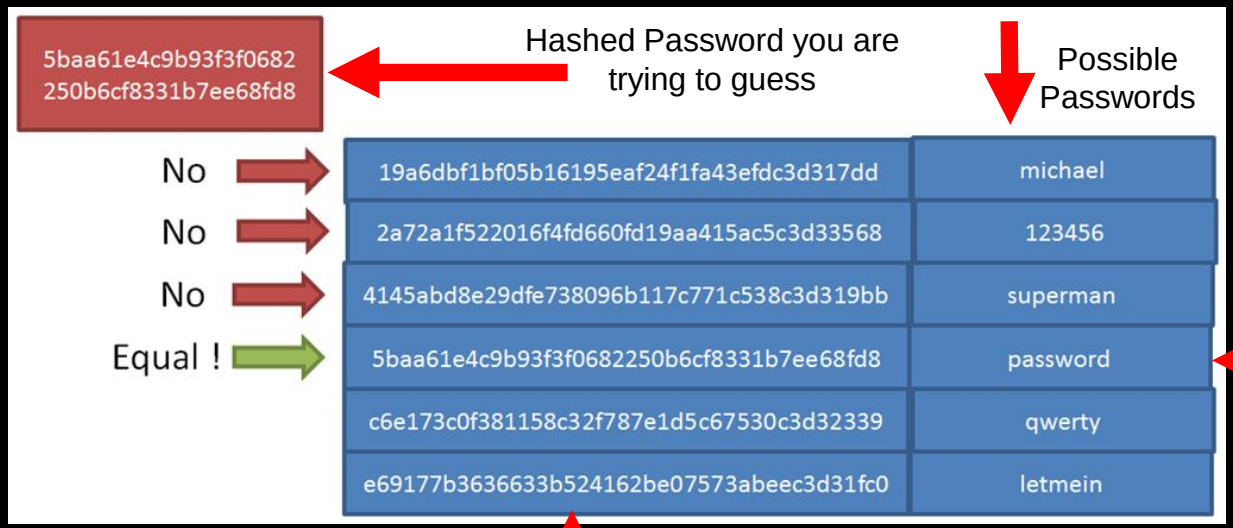
Command:

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



PASSWORD AUDITING

Wordlist

cracking_wordlist - Notepad

File Edit Format View Help

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

Shadow File

shadow - Notepad

File Edit Format View Help

```
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$pY0nc1LbszWdYG70lQzmb/:18820:0:99999:7:::
swarren:$1$zlos79oe$Zt7v873HKWli9bHh1tAGV1:18820:0:99999:7:::
agibbs:$1$fbVCO5xq$yoeNTpwxr1EYXk3l9knCi0:18820:0:99999:7:::
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

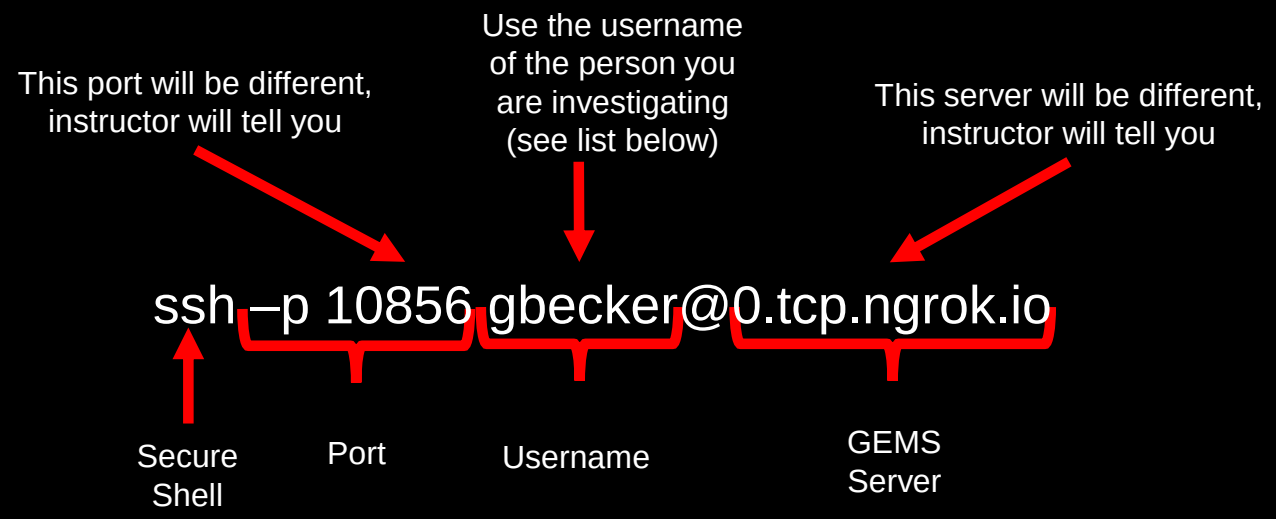
pi@raspberrypi: ~

File Edit Tabs Help

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

ACCESS CONTROL

– Establish a SSH connection to the GEMS server:



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

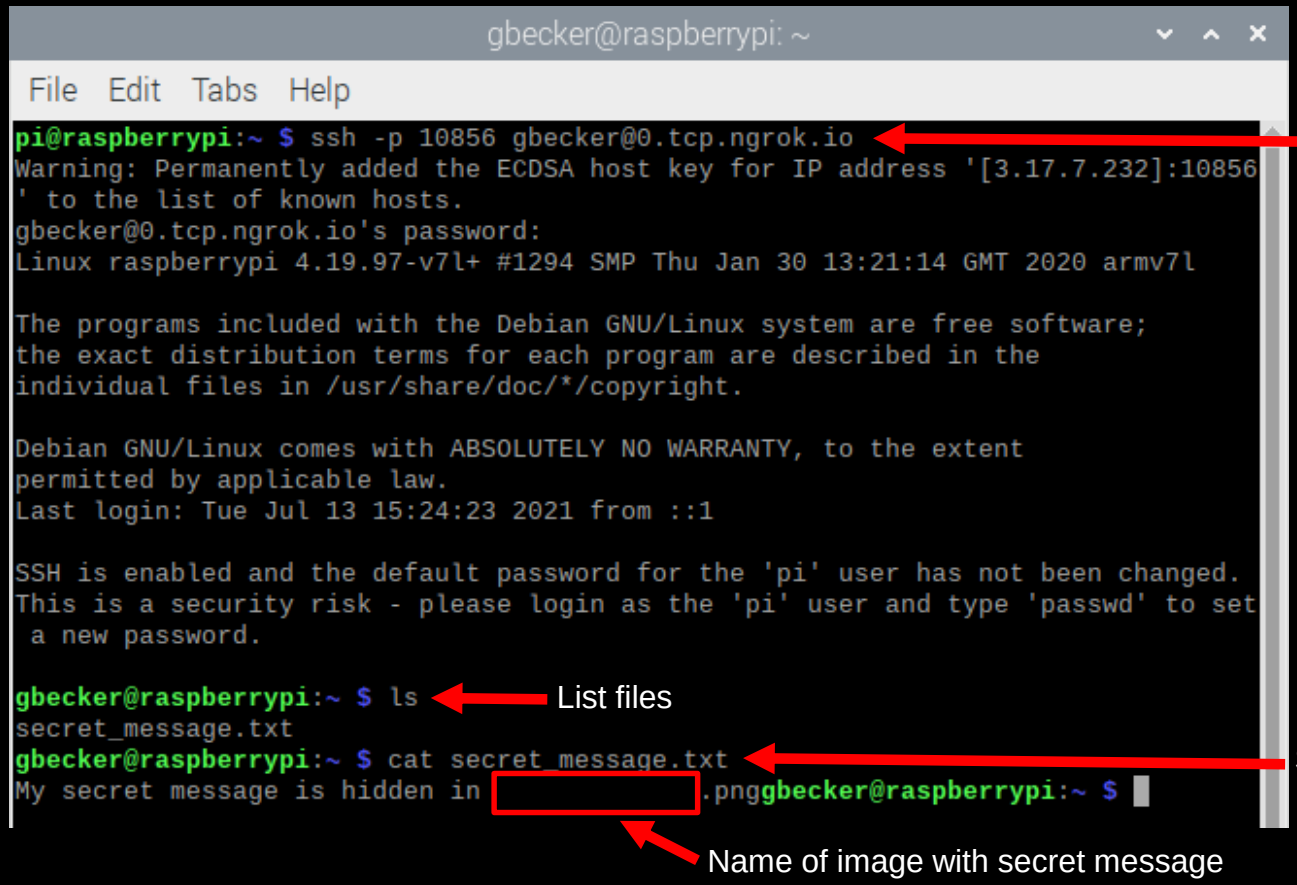
- gbecker
- apalmer
- spaterson
- rchesterton
- ikendal
- vthornton
- swarren
- agibbs
- jmathews
- lderrick
- dotis
- eowen

Example Command:

```
File  Edit  Tabs  Help
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



STEGANOGRAPHY

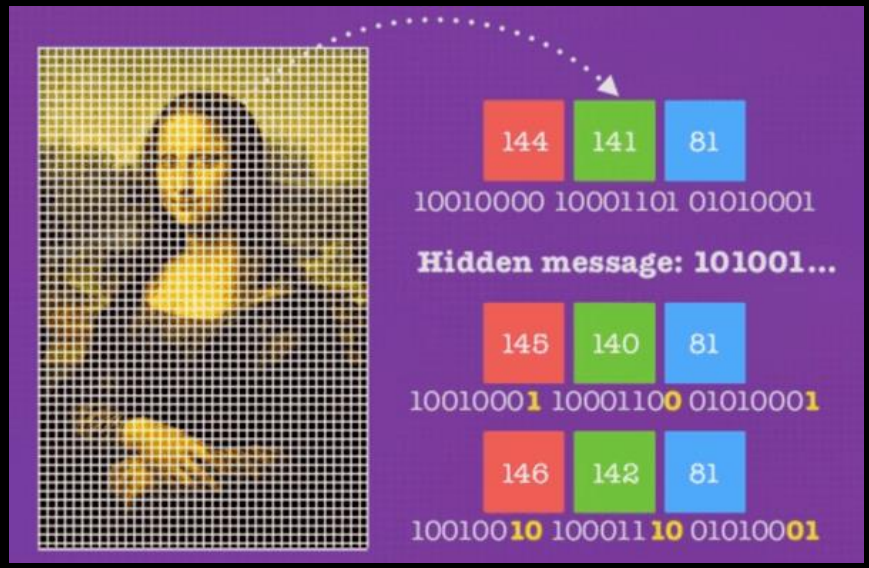
What?

- 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

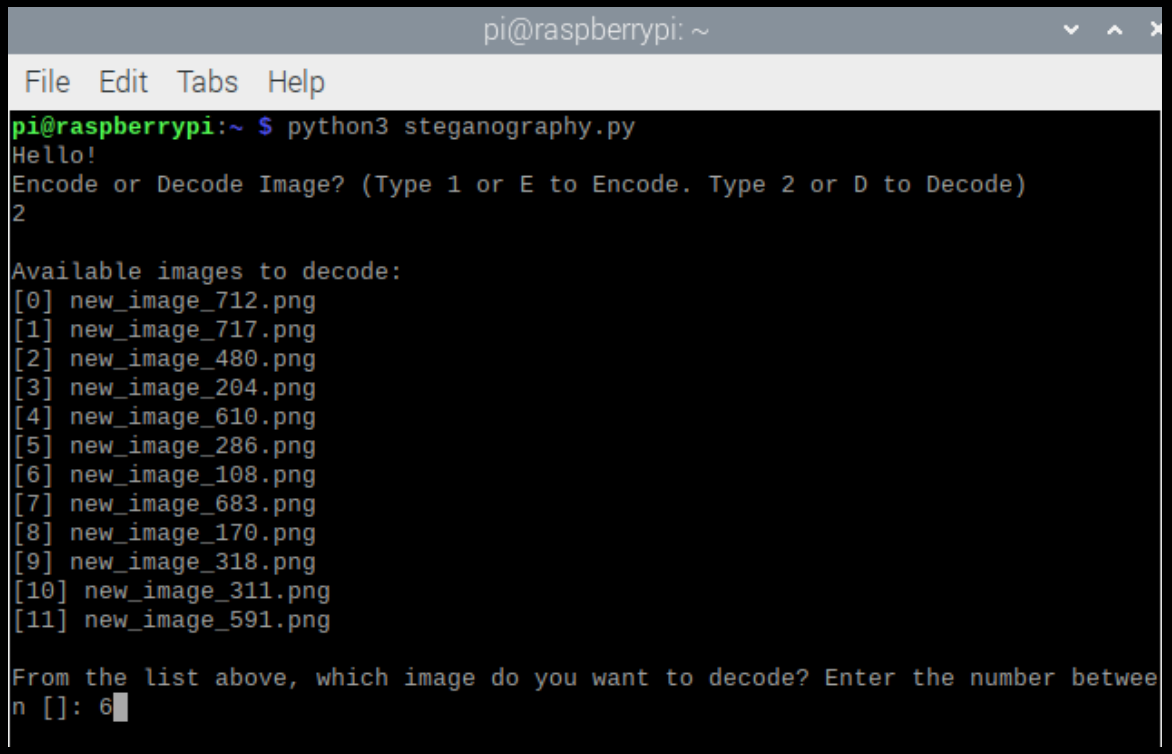
Steganography on Images.

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



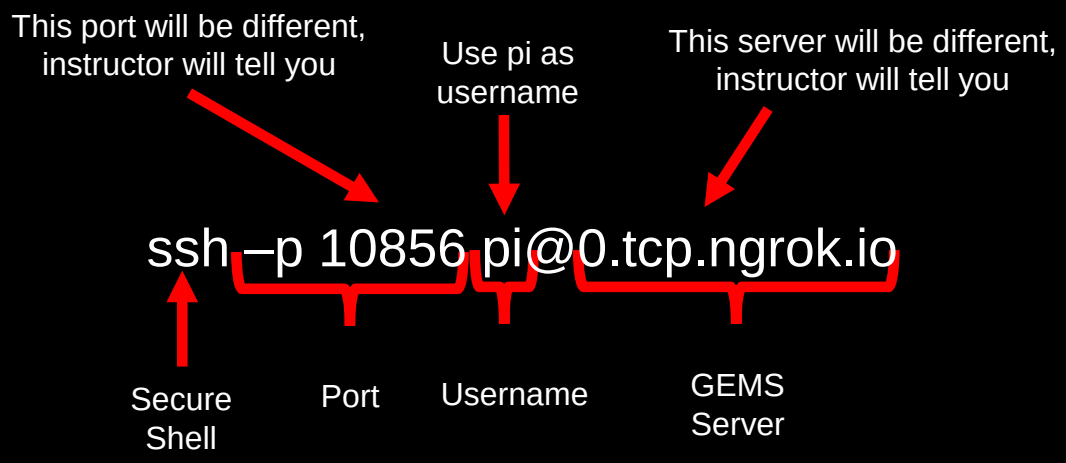
STEGANOGRAPHY

- 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.



ACCESS CONTROL

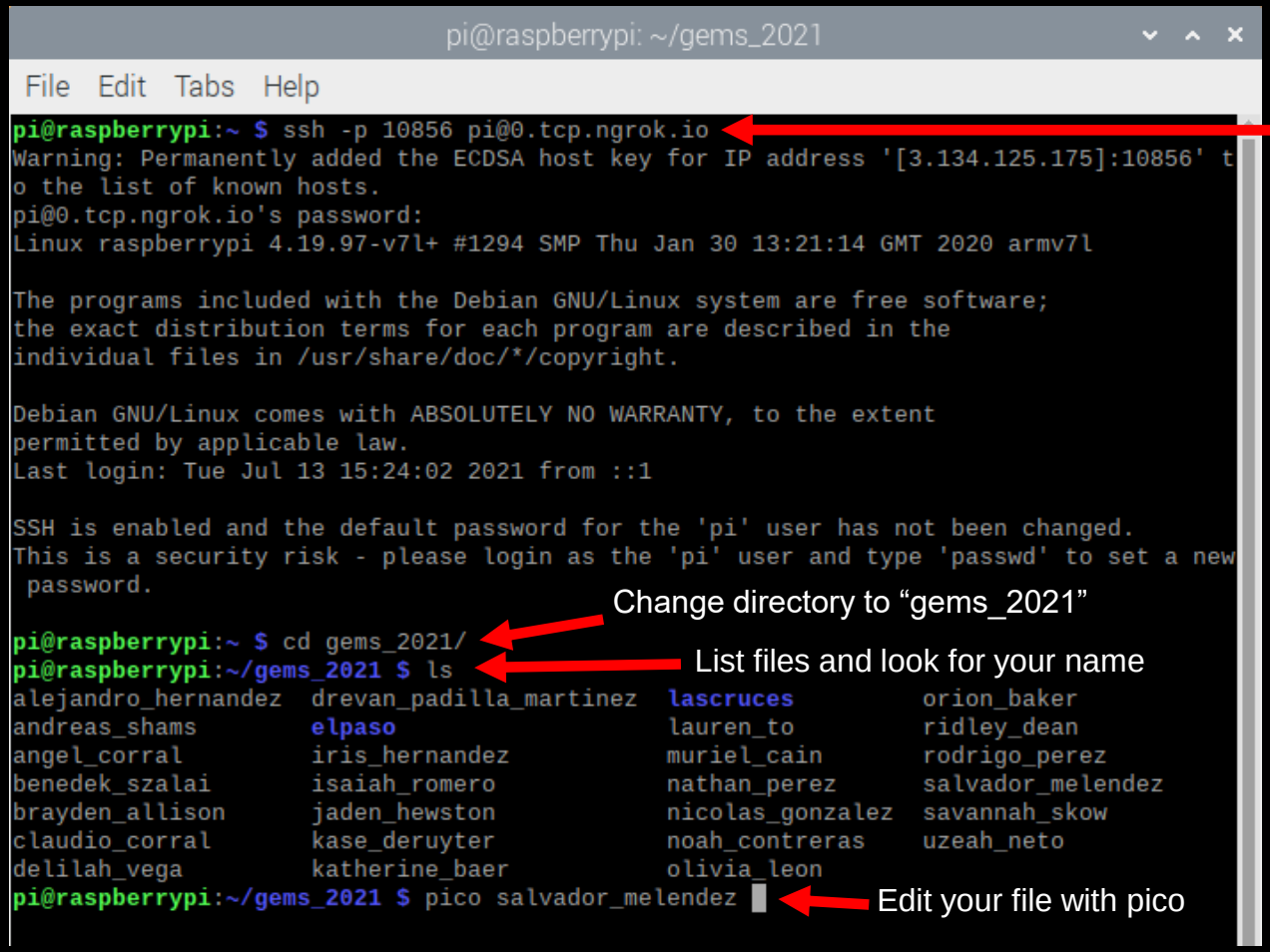
– Establish a SSH connection to the GEMS server



Example Command:

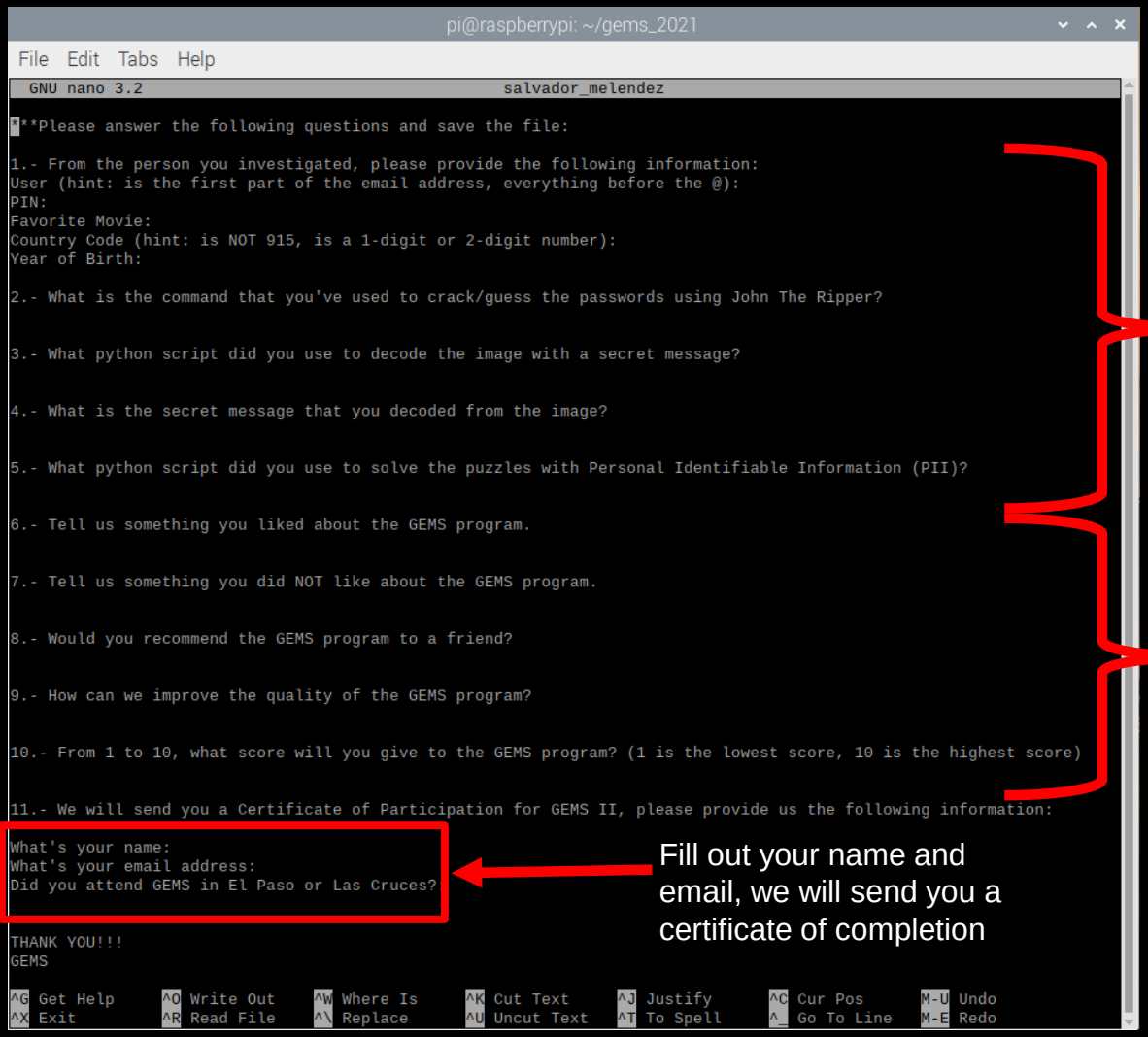
ACCESS CONTROL

- After you establish the SSH connection, cd into “gems_2021” folder, list files with ls, and look for your name.
- Use pico to edit the file with your name.



SURVEY

– Answer the Quiz & Survey.



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).

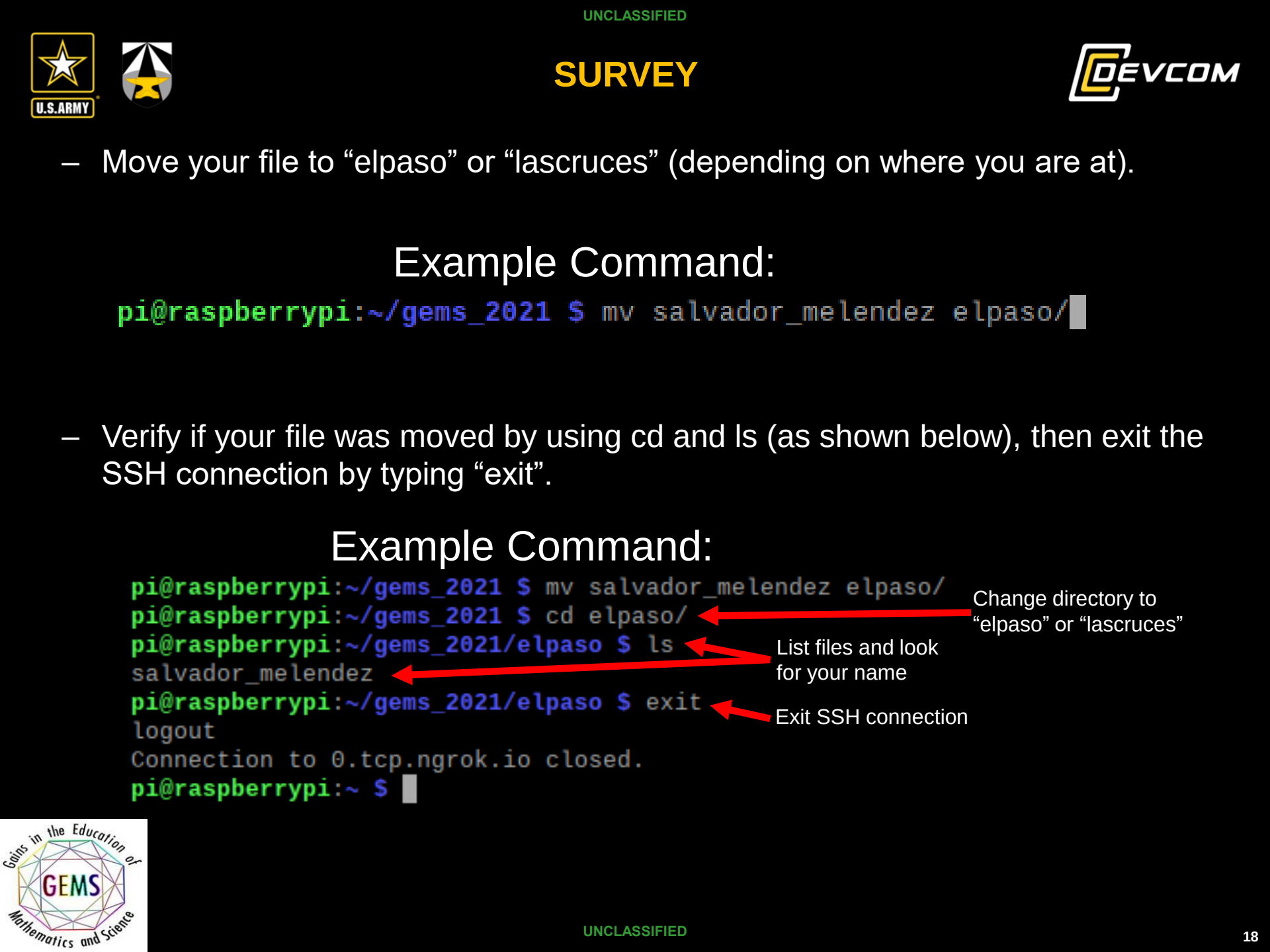
Example Command:

```
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:~ $
```



DOWNLOAD FILES

- Ready for the challenge?
- 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:

- 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)

CONTACT INFORMATION

Salvador Melendez, Ph.D.
UNCLASSIFIED email: salvador.melendez3.civ@mail.mil