CTF Skills
Crypto & Hiding Information

presented by Mandy Galante, NJCCIC Education Outreach Services
New Jersey Cybersecurity and Communications Integration Cell

Welcome! During the workshop:

- Please use Q&A for questions
- Please use Chat for whole group chat topics
- If you will be following along, start up your VM + log into CyberStart Game & PicoCTF Gym

Workshop Info - Crypto + Hiding Info

Capture The Flag (CTF) competitions for CyberStart NCS and PicoCTF are coming up soon with opportunities for NJ students to shine and win prizes. Let's get ready! NJCCIC workshops will cover how to use key tools that the experts recommend for solving many CTF challenges.

The files needed to follow the workshop demonstrations / slides can be downloaded from this link http://bit.ly/CryptoFiles

- An active CyberStart Game license is necessary to access the CSGame challenges.

Cryptography challenges in CTFs

These challenges focus on ways of hiding information

Encryption - take plaintext → apply cipher with key → ciphertext

Encoding - take plaintext → apply an encoding system → encoded text

File Manipulation - make changes to the file so that it isn't useable.

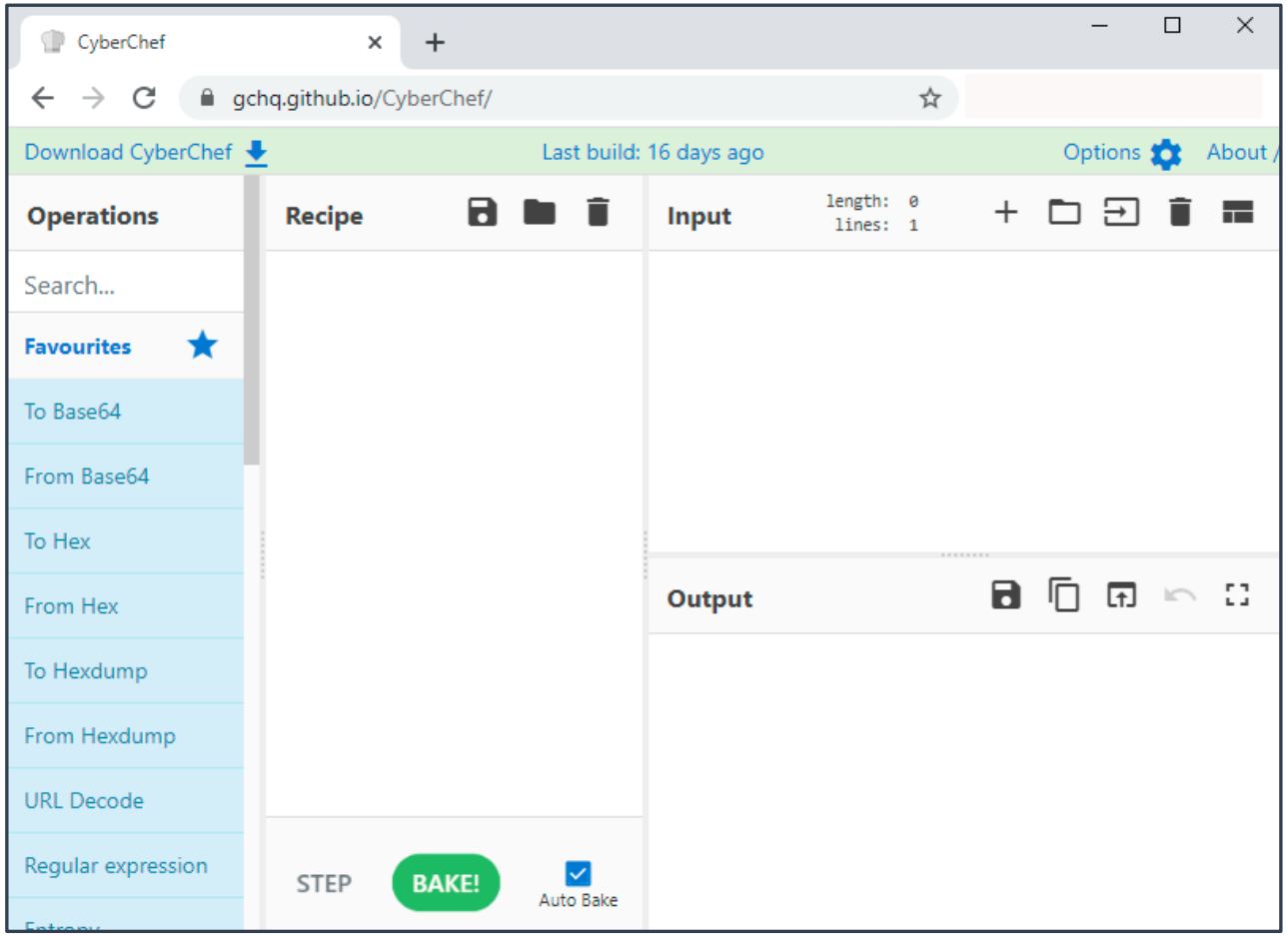
Steganography - hide text or a file "inside" another text or file.
LOTS of ways to do this !

Tools we will cover tonight:

Cyberchef - file - strings - exiftool - hex editors - binwalk - steghide

CyberChef - “Cyber Swiss Army knife”

- A web app for encryption, encoding, compression and data analysis. https://gchq.github.io/CyberChef/
- Works in Chrome or Firefox - no need to install
- Can do layering
- Has auto-recognition of encoding
- Will give you a speed advantage
- Recipe * Input * Output



Encryption

take plaintext → apply cipher with key = ciphertext

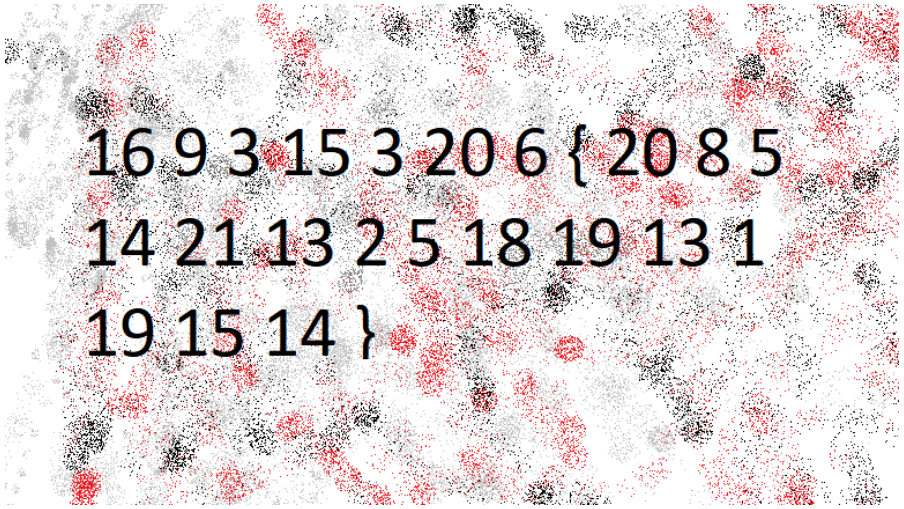
- Caesar / Rotation
- Substitution
- Atbash
- Affine
- Vigenere
- Rail Fence / Transposition
- Bacon
- AES
- . . . and more

Encoding

take plaintext → apply an encoding system = encoded text

- Morse Code
- Binary
- Decimal
- Hexadecimal
- Base 64 (or other bases)
- Pig Pen
- QR Code
- XOR
- . . . and more

Step 1 - identify the type/method



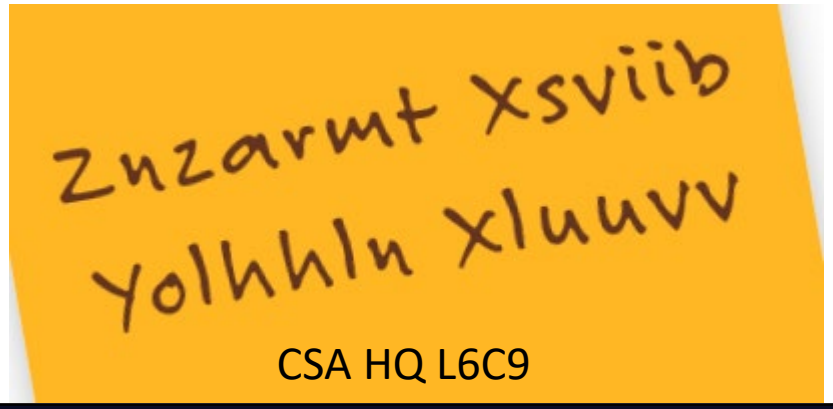
PicoGYM Numbers

CSA HQ L5C11

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

PicoGYM Easy1

PicoGYM Flag



CSA HQ L6C9

4163636f756e74204e756d6265723a203732343430393733353 1

CSA HQ L6C1

Step 2: use a Cyber Chef Recipe TRY IT

1. **Encoding:** Type the phrase *CTF{cryptography rocks}* in the INPUT section
2. Then try out the different encoding recipes in Cyber Chef
   Use Recipes in the Data Format category
3. Observe what the output looks like for each encoding type
4. Wait - what's the magic wand?!! Auto-recognition ☺

---

1. **Encryption:** now let's encrypt the same phrase *CTF{cryptography rocks}* with different encryption types
2. Observe what type of key each encryption type uses
3. What does the output look like?

Online Resources for Decoding

CyberChef - does almost everything BUT just in case you need a bit more:

Vigenere Solver - https://www.guballa.de/vigenere-solver

QuipQiup - substitution cipher solver - https://www.quipqiup.com/

AES Solver - https://www.devglan.com/online-tools/aes-encryption-decryption

Rumkin - lots of classic ciphers - http://rumkin.com/tools/cipher/

Cryptii.com or practicalcryptography.com

Boxentriq.com - cipher identifier
https://www.boxentriq.com/code-breaking/cipher-identifier

dcode.fr or dCode.xyz

CyberStart - HQ:L4C11 File Manipulation-wrong extension

Briefing: We've recovered a bunch of .gif files from an old hard drive one of the gang members threw out. We thought they were innocent enough until we started wondering whether they were all actually gif files.

Files: nine cat-gif-0*.gif - I renamed to L4C11cat-gif-01, 05 and 06

Hint: Can we be sure they're all really .gif files? In previous cases the CPA have solved we've seen gang members change the extension on files so it looks like something different. Perhaps try opening the files in a text editor to see if they are actually all .gifs.

Plan:

bring into CyberChef to see what is auto-detected

OR use '**file**' command to determine the file type. Add the necessary extension and open.

Steganography - “hide in plain sight”

1. Text hidden in the actual picture - small type, in the border, color is the same.
2. Info in the Metadata of a picture - exiftool
3. Text hidden in the Hex of the picture - hex editor OR strings
4. File within a file - binwalk tool
5. Steganography software - steghide tool

Text hidden in the actual picture

Zoom in very, very close to the top of the picture to find the message.

Steg-LightsPic.jpg
CSAW 2014

PicoGym: So Meta

File Metadata

Briefing: Find the flag in this picture.

Files: pico_img.png - I renamed to SoMeta_img.png

Hint: What does meta mean in the context of files?
Answer: “metadata” is information about the file - date created, date modified, GPS on where it was taken, flash, author . . . lots more.

Plan:

- in Terminal, use ‘exiftool’ command
- OR online Exif viewer like http://exif.regex.info/exif.cgi - includes a map feature
- OR bring into CyberChef and use Extract Exif Recipe BUT this only works on JPG image files - not PNG or GIF

CyberStart - ForL2C2 Info in Hex of file

Briefing: When our team gained access to the photographer's photos we found a folder with some photos in it, but the photos seem to be pretty uninteresting from a quick look. Have a look at them yourself and see if you can find anything interesting. **Tip:** The flag is in the image.

Files: paris-05.jpg - I renamed to L2C2_paris-05.jpg

Hint: Some tools in Linux can show if a string of data has been added to a file.

Plan:

- use ‘strings’ command on each file
- OR open the file in a hex editor like the GHex app in the VM

CyberStart - HQ:L9C9 Info in Hex of file

Briefing: One of the Spetzners lives in Tayga, a heavily forested area with a lot of bears! Taking photographs of them and posting them to a nature site. We thought it was fairly innocent until one of the agents spotted something weird about one of the images.

Tip: There's a hidden file, open it to get the flag.

Files: 8 files challenge-bearwatch-pic-0*.jpg

- I renamed to L9C9-bearwatch-pic.0*.jpg

Hint: Take a close look at each of the images, try opening them in a hex editor such as bless. Do you see anything unusual about them?

NOT A GOOD HINT!

CyberStart - HQ:L9C9 Info in Hex of file

Plan:

1. Open each image in Ghex or another hex editor, scroll to bottom and you notice the ‘msgPK’ at the end
2. Try ‘strings’ to see if there is any useful text in each file
3. Try ‘exiftool’ to see if there is anything useful in the metadata of each file
4. Use Binwalk to see if there are any other files embedded into this picture file
   In Terminal, binwalk -e <filename>
   The -e option tells binwalk to extract any files it finds embedded
   binwalk -e L9C9* (this will run binwalk on all the bear files)
5. Finds a zip file in file 06 - cd into the director created by binwalk
6. Use the ‘unzip’ command to extract the zip file and run the included program to get the flag.

CyberStart - Forensics:L4C4 Steghide

Briefing: Downloaded images from suspect's camera. We've received word that they've already been taken off the camera, a secret inserted into them, and put back, ready to be passed on to another gang member at the end of the tour.

Tip: The flag is in the image.

File: masai-mara-01.jpg - I renamed to ForL4C4_masai-mara-01.jpg

Hint: Did you know steghide has an extract feature?

Plan:

- use **steghide info <name of file>** to find out if there is hidden data
- To extract the data, use **steghide extract -sf <name of file>**

Connect With Us

NJCCIC@CYBER.NJ.GOV

1-833-4-NJCCIC
(1-833-465-2242)

@NJCYBERSECURITY

CYBER.NJ.GOV