```
[johndoe@bnc234 ~]$
```

Day 3: Cyber Security Workshop

STEM Workshop at ASA Now - HSD3

```
[johndoe@bnc234 ~]$ sudo su
[sudo] password for johndoe:
```

Agenda Overview:

1. Staying Safe Online + Netiquette recap
2. Intro to OSINT
3. Intro to Cryptography
4. Terminal Basics

Time-permitting Activities

- More picoCTF

Staying Safe Online

Who remembers some dangers related technology in today’s world?

From Monday:

- Sharing Personal Information on Social Media
- Malware
- Social Engineering
- Cyber Bullying

How can we protect against them?

Netiquette

Who remembers some Netiquette principles?

Why are they important?

From Monday:

- Avoid ALL-CAPS
- Think before you type
- Check your Grammar
- Avoid flaming
- Be kind

Intro to OSINT

Professional Googling

1. What is OSINT?
2. Why is it important?
3. OSINT Practice Problems

```
[johndoe@bnc234 ~]$ sudo su
[sudo] password for johndoe:
[root@bnc234 johndoe]# clear
```

What is OSINT?

OSINT: Open Source Intelligence

This is the ability to utilize publicly available resources on the internet to find and apply information.

With regards to OSINT against individuals and corporations, publicly available resources can include news articles, Google search results, and especially in the last decade, Social Media sites.

However, basic OSINT skills are extremely useful in many other areas of Cyber Security as well...

Why is it important?

Basic OSINT, simple and straightforward as it may seem, is the backbone of many areas of Cyber Security.

Applications:

- Quickly finding information related to a task
- Quickly researching information related to a vulnerability
- Researching a target during a Red-Team (Offensive Cyber Security) operation

OSINT Practice

Open a web browser on your computers and take a crack at these OSINT problems

(Raise your hand as soon as you have your answer!)

OSINT Practice: Question 1 - Presidents

Who was the president of the United States in 1940?

```
[root@bnc234 johndoe]# cd /etc/
[root@bnc234 etc]# cp passwd /home/johndoe/; clear
```

OSINT Practice: Question 2 - Shell Shock

What was the year that the security bug, now known as "Shell Shock", was discovered?

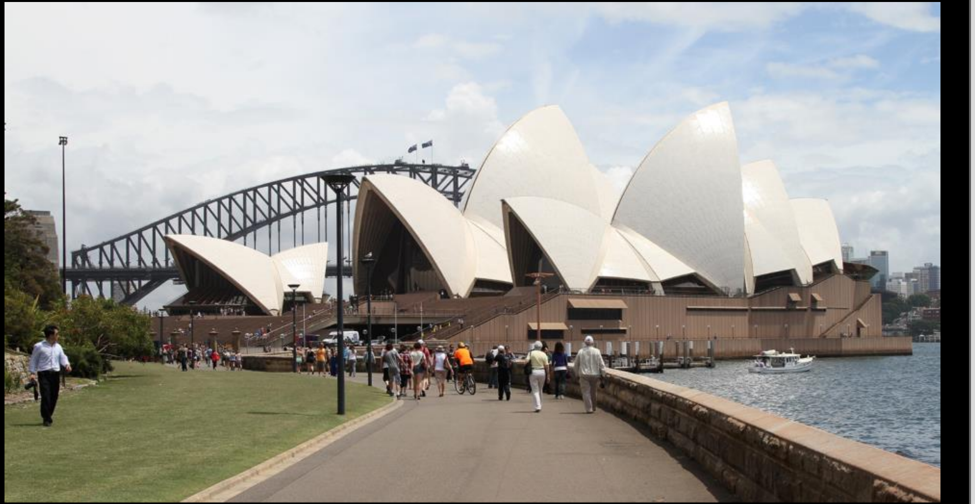
```
[root@bnc234 johndoe]#
```

OSINT Practice Question 3 - Location

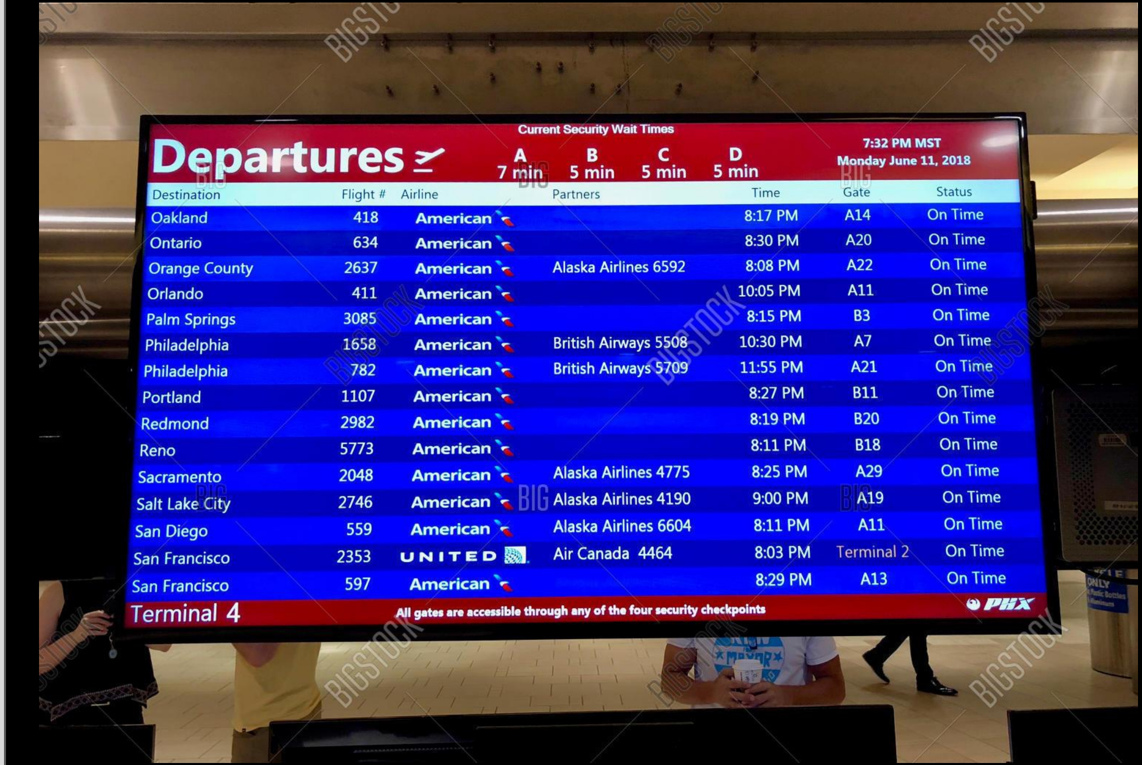
A suspect was seen entering the below building. What are the coordinates (in Latitude, Longitude) of their approximate location?

Link to image: https://bit.ly/osintLoc

(Tip: Reverse image search)



Flight Fiasco



Departures

Current Security Wait Times

A	B	C	D
7 min	5 min	5 min	5 min

7:32 PM MST
Monday June 11, 2018

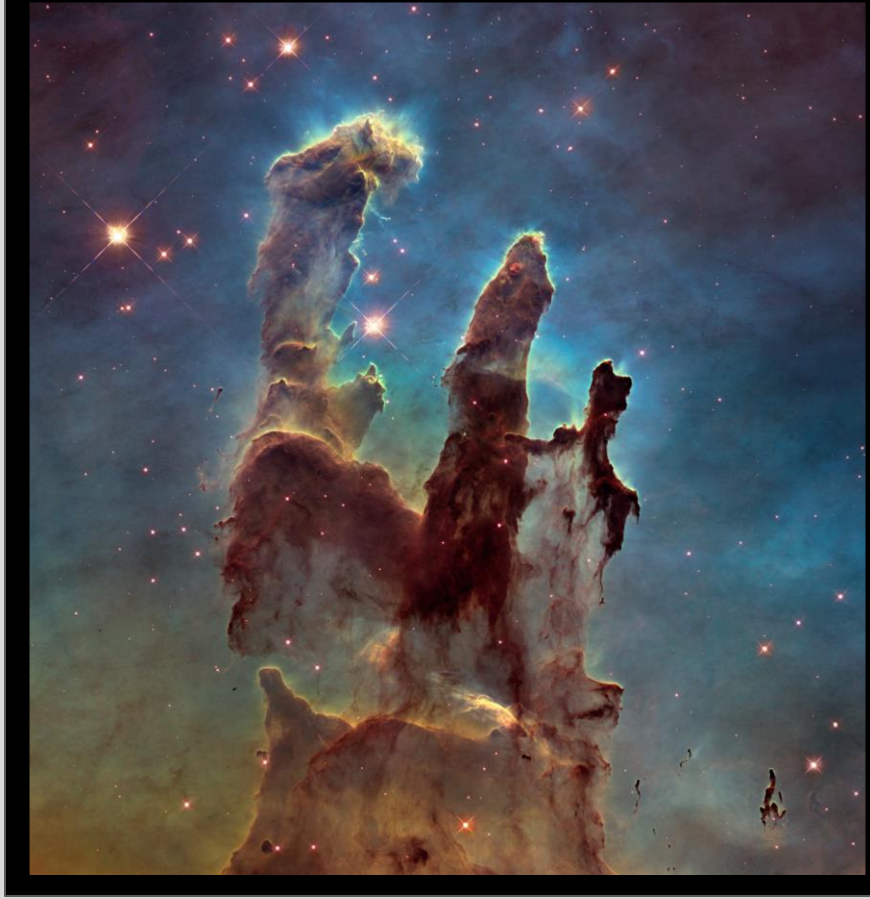
Destination	Flight #	Airline	Partners	Time	Gate	Status
Oakland	418	American		8:17 PM	A14	On Time
Ontario	634	American		8:30 PM	A20	On Time
Orange County	2637	American	Alaska Airlines 6592	8:08 PM	A22	On Time
Orlando	411	American		10:05 PM	A11	On Time
Palm Springs	3085	American		8:15 PM	B3	On Time
Philadelphia	1658	American	British Airways 5508	10:30 PM	A7	On Time
Philadelphia	782	American	British Airways 5709	11:55 PM	A21	On Time
Portland	1107	American		8:27 PM	B11	On Time
Redmond	2982	American		8:19 PM	B20	On Time
Reno	5773	American		8:11 PM	B18	On Time
Sacramento	2048	American	Alaska Airlines 4775	8:25 PM	A29	On Time
Salt Lake City	2746	American	Alaska Airlines 4190	9:00 PM	A19	On Time
San Diego	559	American	Alaska Airlines 6604	8:11 PM	A11	On Time
San Francisco	2353	UNITED	Air Canada 4464	8:03 PM	Terminal 2	On Time
San Francisco	597	American		8:29 PM	A13	On Time

Terminal 4 All gates are accessible through any of the four security checkpoints PHX

Our agent tracked a mysterious individual to an airport and deduced they are boarding flight #634. The agent managed to take a picture of the departure board. We need **you** to get the following information:

- What is the name of this airport?
- What's the date?
- Where is the individual's flight going, and from what gate?

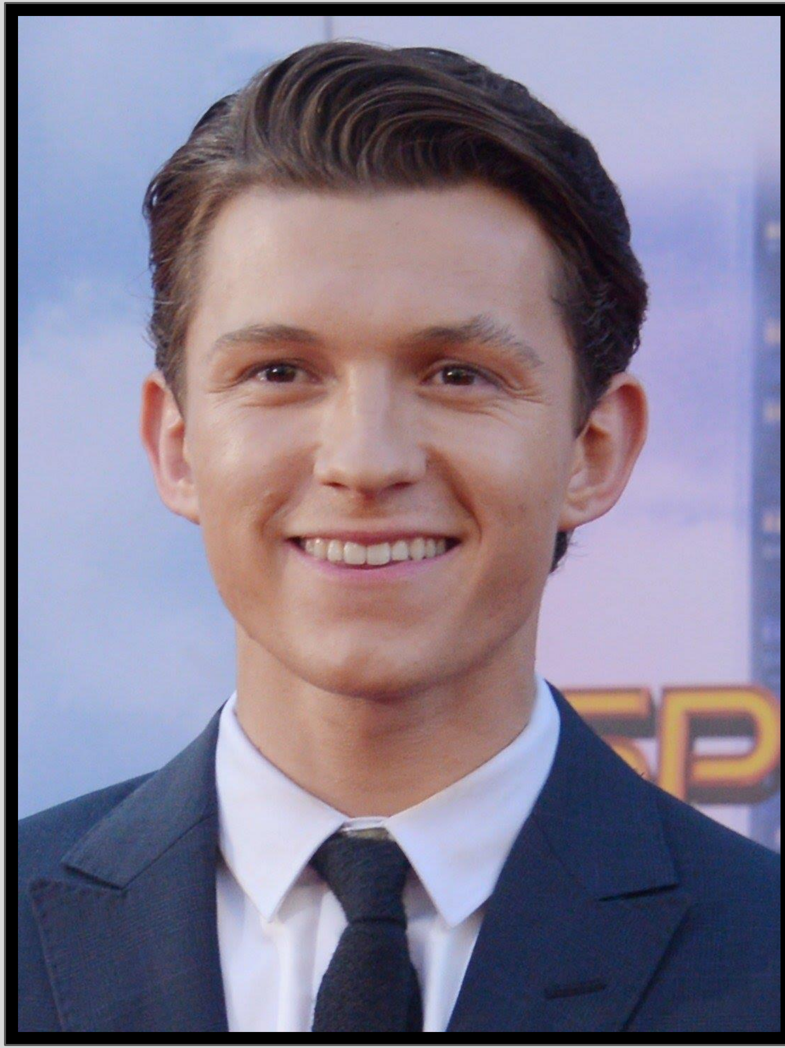
Link to image: Image



Telescopic Transmission

What space telescope took this image?

Link to image: Image



Famous Figure

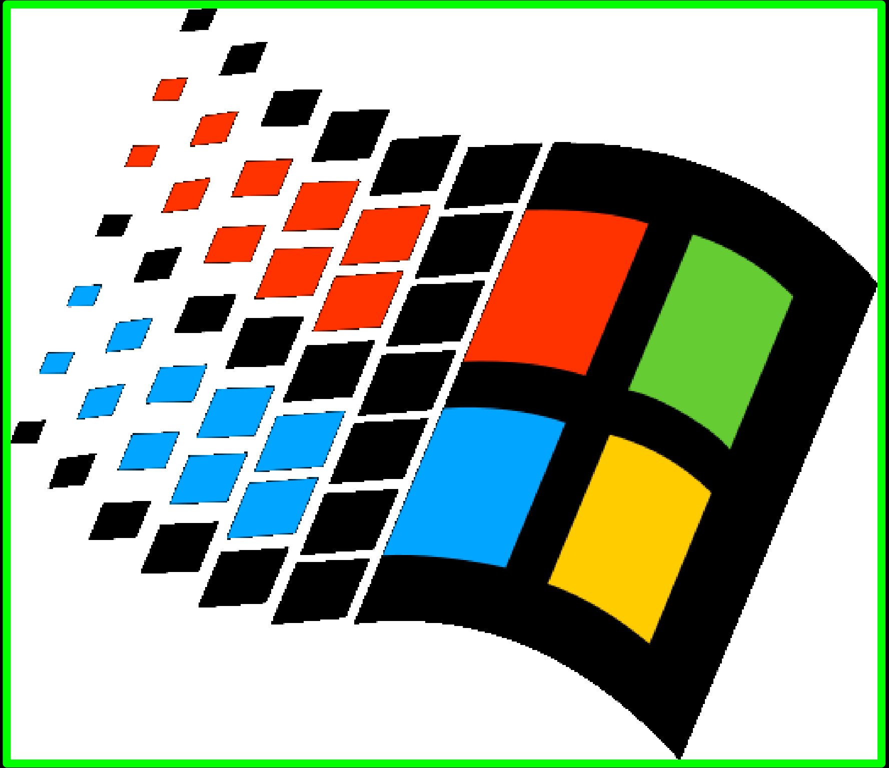
Who is this Actor?

What was the most recent movie he was featured in?

What character did he play in that move?

Link to image: Image

The **Ancient** OS

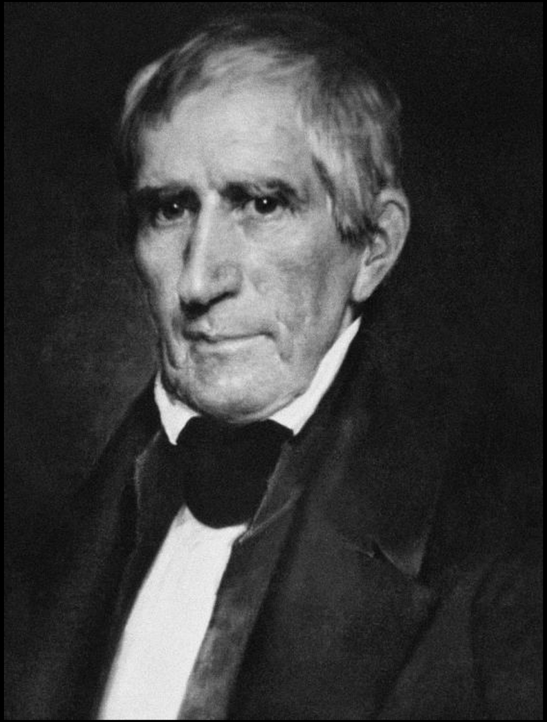


What version of Windows was released with this logo?

What year was this version of Windows discontinued

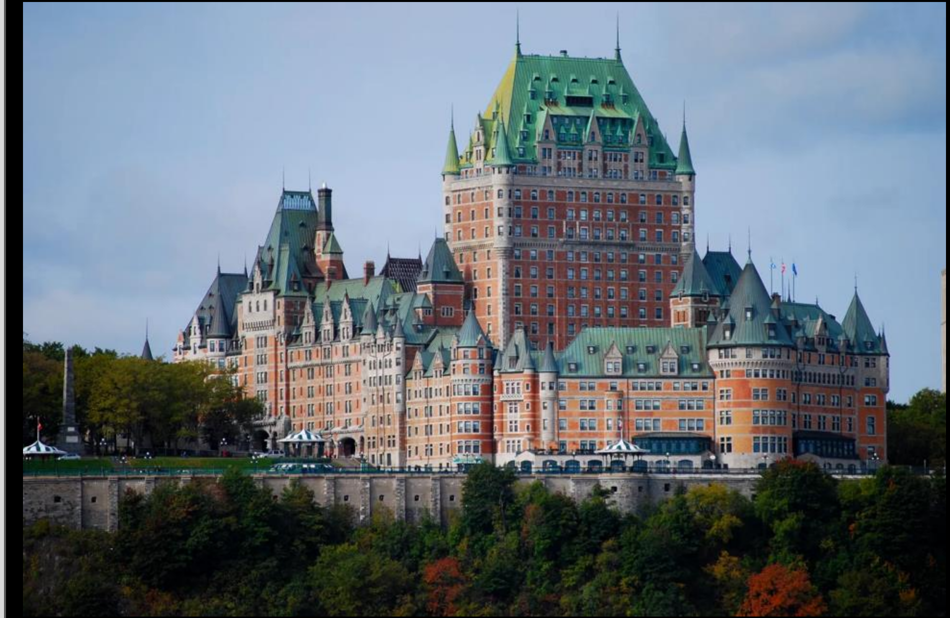
(No image link provided)

Famously Forgettable President



Who was the first U.S. President to die while in office?

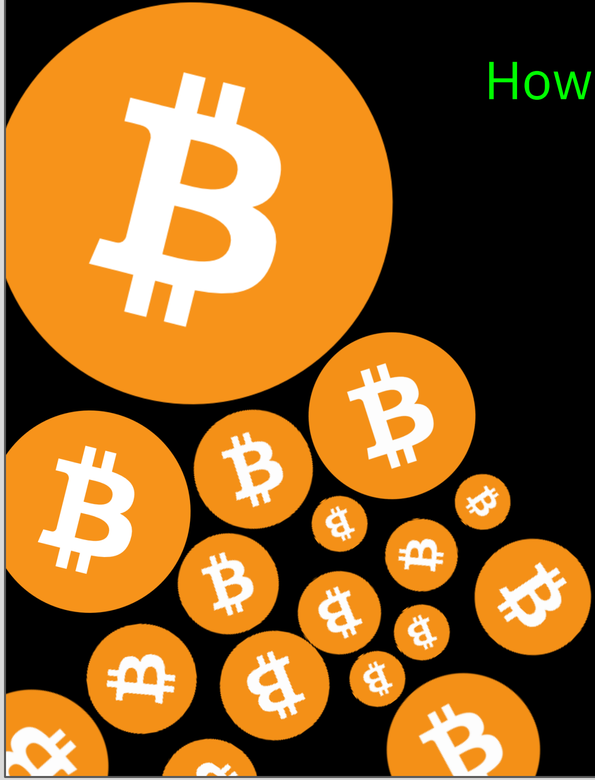
Bonus: Brilliant Buildings and More



- What is the name of this building?
- What city is this building located in?
- Who designed it?
- In what year did it’s construction begin?
- Who became Canada’s prime minister on December 5th of that year?

Link to image: Image

Imagine owning Bitcoin *lol*



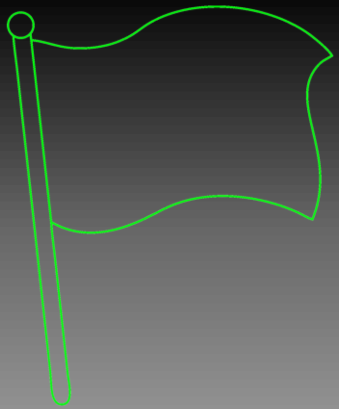
How much money (in USD), did Mt Gox lose in their 2014 hack?

Intro to CTFs

*coolCTF{
these_are_addictively_fun_
I_cant_stop_
please_help_meeeeeeeeeeeeeeeeee}*

1. What are CTFs?
2. picoCTF
3. What is a terminal?
4. picoCTF webshell
5. Basic Shell Commands

What are CTFs?



Cyber Security CTFs (aka. Capture the Flag), are gamified practice exercises that let you learn and practice a wide variety of Cyber Security Topics in a fun and rewarding manner.

The goal of CTF challenges are almost always to find a “flag”, often in the format of nameOfCTF{xxxxx}.

picoCTF

picoCTF: A very beginner friendly CTF website built by students at Carnegie Mellon University designed specifically for Middle and High School students new to Cyber Security.

Navigate to https://picoctf.org/, make an account, and log in.

Click on the “Practice” tab in the Navigation Header, and then click on the “Practice picoGym” Button to be taken to a list of practice CTF problems.

picoCTF: Obedient Cat

Navigate to https://play.picoctf.org/practice/challenge/147

Take 5 minutes to try this problem on your own.

Note: There is NO penalty to using hints on this website. Sometimes, it is even impossible to solve a problem without them!

Solution Demo for Obedient Cat

Intro to Cryptography

Secret Messages

Secret Messages

K290aGVyIHN0dWZm

1. What is Cryptography?
2. Common Ciphers
3. Practice Problems

What is Cryptography?

Cryptography: The art of writing or solving codes.

- Oxford Languages Dictionary

Cryptography is an extremely broad, rapidly evolving, and at times, complex topic with many subfields and applications, especially in those related to security and privacy.

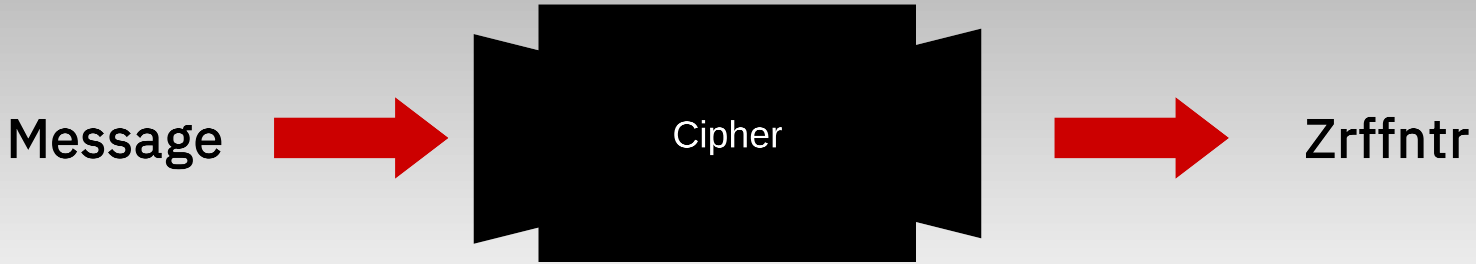
However, we will be focusing on some of the more fun and beginner-friendly areas today.

What are Ciphers?

Ciphers are one of the oldest Cryptography techniques, with some even dating back all the way to Ancient Greece in 400 BCE!

Ciphers apply a direct, predetermined transformation to the message text.

Common Ciphers: Substitution, Caesar, ROT13,



Message

Cipher

Zrffntr

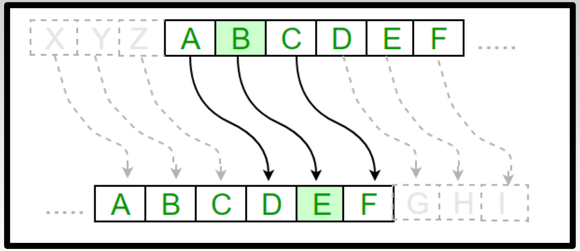
Caesar Cipher

The Caesar Cipher is a type of Substitution Cipher that relies on shifting the letters in a message based on a given offset.

Example: “Hello abcdz” shifted with an offset of 3 becomes “Khoor defgc”
(Notice how the ‘z’ wrapped around the alphabet to end up at ‘c’)

Weakness: Because there are only 26 letters in the alphabet, it is relatively simple and straightforward for a human to look at all 26 transformations and determine which one is likely the decoded message.

Rot 13: A Caesar Cipher with an Offset of 13



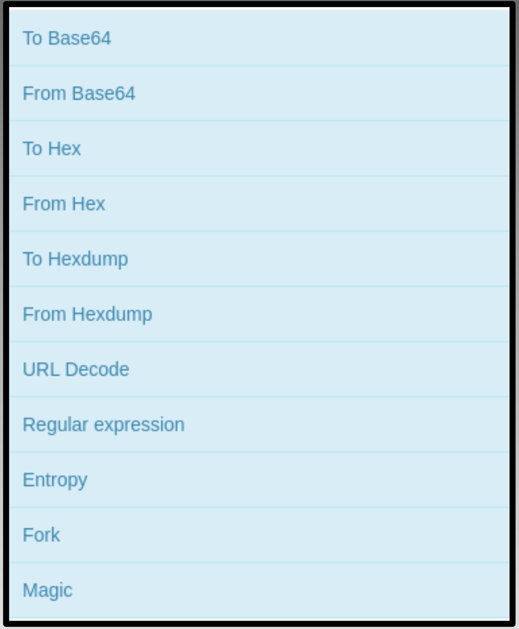
(Go back to previous slide)

Cyber Chef

https://bit.ly/CyberChefLink

Powerful online set of web tools.

Includes many resources for Cryptography challenges.



To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Caesar Cipher Practice

Try to reverse the following Caesar Ciphers!

Rot 13: SnfgEnoovg

Shifted +10: Wyexdksx

Shifted +21: Hvmodvi

Shifted +??: Akzrogdlx

Shifted +??: Bdynawxej

Finish Early? Try these picoCTF problems!

- 13 | Rot 13
- Mod 26 | Rot 13
- caesar | Caesar Cipher

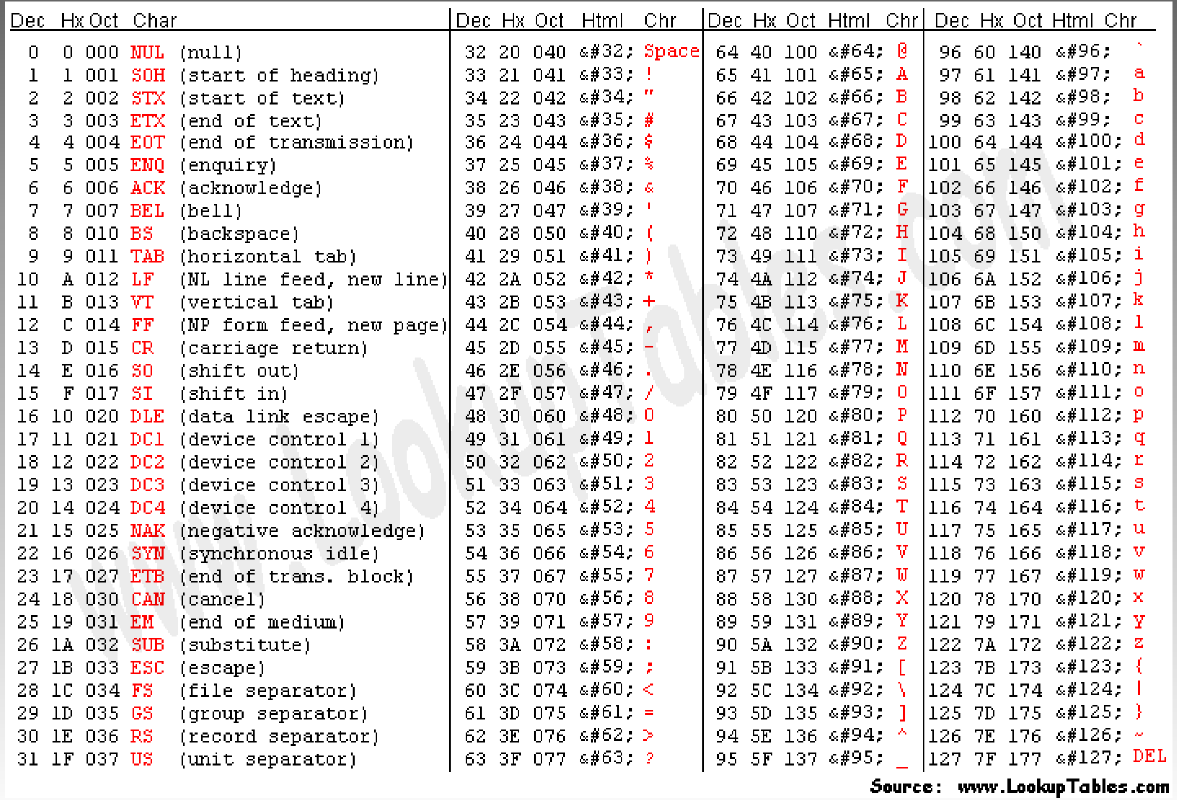
(7 minutes)

Text Encoding

There are many ways to represent the same text.

To the right is an ASCII table, various different ways to represent the numbers that correspond to different computer characters.

Note: Cyber Chef has options to convert from these other formats to text. Try typing the “From” keyword into the search box to get started.



Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040	&#32;	Space	64	40	100	&#64;	@	96	60	140	&#96;	`
1	1	001	SOH (start of heading)	33	21	041	&#33;	!	65	41	101	&#65;	A	97	61	141	&#97;	a
2	2	002	STX (start of text)	34	22	042	&#34;	"	66	42	102	&#66;	B	98	62	142	&#98;	b
3	3	003	ETX (end of text)	35	23	043	&#35;	#	67	43	103	&#67;	C	99	63	143	&#99;	c
4	4	004	EOT (end of transmission)	36	24	044	&#36;	$	68	44	104	&#68;	D	100	64	144	&#100;	d
5	5	005	ENQ (enquiry)	37	25	045	&#37;	%	69	45	105	&#69;	E	101	65	145	&#101;	e
6	6	006	ACK (acknowledge)	38	26	046	&#38;	&	70	46	106	&#70;	F	102	66	146	&#102;	f
7	7	007	BEL (bell)	39	27	047	&#39;	'	71	47	107	&#71;	G	103	67	147	&#103;	g
8	8	010	BS (backspace)	40	28	050	&#40;	(	72	48	110	&#72;	H	104	68	150	&#104;	h
9	9	011	TAB (horizontal tab)	41	29	051	&#41;	)	73	49	111	&#73;	I	105	69	151	&#105;	i
10	A	012	LF (NL line feed, new line)	42	2A	052	&#42;	*	74	4A	112	&#74;	J	106	6A	152	&#106;	j
11	B	013	VT (vertical tab)	43	2B	053	&#43;	+	75	4B	113	&#75;	K	107	6B	153	&#107;	k
12	C	014	FF (NP form feed, new page)	44	2C	054	&#44;	,	76	4C	114	&#76;	L	108	6C	154	&#108;	l
13	D	015	CR (carriage return)	45	2D	055	&#45;	-	77	4D	115	&#77;	M	109	6D	155	&#109;	m
14	E	016	SO (shift out)	46	2E	056	&#46;	.	78	4E	116	&#78;	N	110	6E	156	&#110;	n
15	F	017	SI (shift in)	47	2F	057	&#47;	/	79	4F	117	&#79;	O	111	6F	157	&#111;	o
16	10	020	DLE (data link escape)	48	30	060	&#48;	0	80	50	120	&#80;	P	112	70	160	&#112;	p
17	11	021	DC1 (device control 1)	49	31	061	&#49;	1	81	51	121	&#81;	Q	113	71	161	&#113;	q
18	12	022	DC2 (device control 2)	50	32	062	&#50;	2	82	52	122	&#82;	R	114	72	162	&#114;	r
19	13	023	DC3 (device control 3)	51	33	063	&#51;	3	83	53	123	&#83;	S	115	73	163	&#115;	s
20	14	024	DC4 (device control 4)	52	34	064	&#52;	4	84	54	124	&#84;	T	116	74	164	&#116;	t
21	15	025	NAK (negative acknowledge)	53	35	065	&#53;	5	85	55	125	&#85;	U	117	75	165	&#117;	u
22	16	026	SYN (synchronous idle)	54	36	066	&#54;	6	86	56	126	&#86;	V	118	76	166	&#118;	v
23	17	027	ETB (end of trans. block)	55	37	067	&#55;	7	87	57	127	&#87;	W	119	77	167	&#119;	w
24	18	030	CAN (cancel)	56	38	070	&#56;	8	88	58	130	&#88;	X	120	78	170	&#120;	x
25	19	031	EM (end of medium)	57	39	071	&#57;	9	89	59	131	&#89;	Y	121	79	171	&#121;	y
26	1A	032	SUB (substitute)	58	3A	072	&#58;	:	90	5A	132	&#90;	Z	122	7A	172	&#122;	z
27	1B	033	ESC (escape)	59	3B	073	&#59;	;	91	5B	133	&#91;	[	123	7B	173	&#123;	{
28	1C	034	FS (file separator)	60	3C	074	&#60;	<	92	5C	134	&#92;	\	124	7C	174	&#124;	|
29	1D	035	GS (group separator)	61	3D	075	&#61;	=	93	5D	135	&#93;	]	125	7D	175	&#125;	}
30	1E	036	RS (record separator)	62	3E	076	&#62;	>	94	5E	136	&#94;	^	126	7E	176	&#126;	~
31	1F	037	US (unit separator)	63	3F	077	&#63;	?	95	5F	137	&#95;	_	127	7F	177	&#127;	DEL

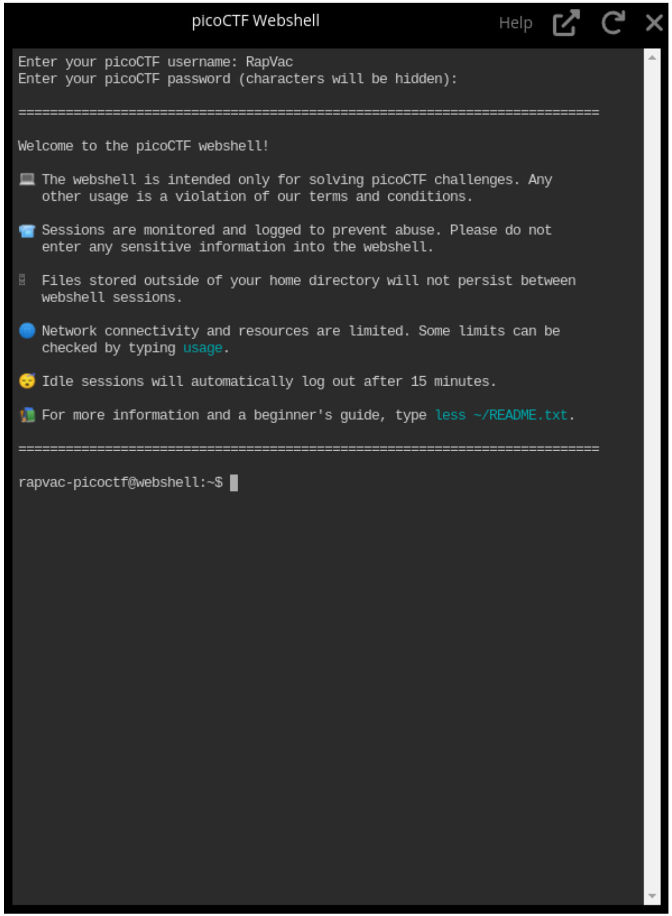
Source: www.LookupTables.com

What is a terminal?

- The **shell** is an interface that takes text commands and gives them to an operating system to execute.
- Used to be the only way to control Unix-like operating systems.
- Now we have nice graphics to make the user experience better.
- The **terminal** lets you feed commands to the **shell.**

picoCTF webshell

- picoCTF handily provides users with a **terminal** in the web browser.
- Allows you to do many of the linux-specific CTFs on any operating system.
- Same commands as you would find on the Linux OS.



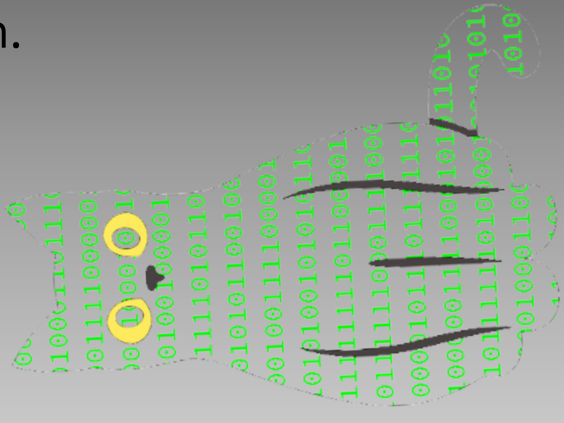
```
Enter your picoCTF username: RapVac
Enter your picoCTF password (characters will be hidden):

=========================================================================

Welcome to the picoCTF webshell!

💻 The webshell is intended only for solving picoCTF challenges. Any
   other usage is a violation of our terms and conditions.

📼 Sessions are monitored and logged to prevent abuse. Please do not
   enter any sensitive information into the webshell.

   Files stored outside of your home directory will not persist between
   webshell sessions.

🌐 Network connectivity and resources are limited. Some limits can be
   checked by typing usage.

😴 Idle sessions will automatically log out after 15 minutes.

📚 For more information and a beginner's guide, type less ~/README.txt.

=========================================================================

rapvac-picoctf@webshell:~$ █
```

Netcat

Allows you to connect to and communicate with a specific port on a foreign computer from your terminal in a 2-way connection.

Example:

```
$ nc test.server.com 1234
```



Let's break it down and explain each part:

- `nc`: Invoke the Netcat command.
- `test.server.com`: The foreign computer you want to connect to.
- `1234`: The port on that computer you want to connect to.

Text Encoding Practice

Try to convert the following encoded messages into regular English text.

Decimal: 82 111 98 111 116
78 101 98 117
108 97

Hex: 4e 69 6f 62 69 75 6d
43 6c 6f 75 64

Base 64: Um9ja2V0ZHluZQ==

TWF0aGVtYXRpY3M=

Finish Early? Try these picoCTF problems!

- The Numbers
- Bases
- what's a net cat?
- Lets Warm Up
- 2Warm
- Nice netcat...
- Based (Hard)

Basic Shell Commands

ls

List all files in a directory (aka folder).

Format: *ls*

cd

Change your directory. File paths in linux are written starting at root (the first ‘/’). Ex: /home/username/somedir

Format: *cd <path>*

mkdir

Create a directory branching from your current one. Ex: if you are in /home/username/ and do *mkdir test*, *ls* will reveal **test**

Format: *mkdir <name>*

file

Get information about a file, such as it’s type.

Format: *file <filename>*

cat

Display the contents of a file.

Format: *cat <filename>*

wget

Download a file from a link

Format: *wget <link>*

*Note: *<filename>* can optionally be substituted for the absolute path of a file.

Your turn now! Navigation:

We found a file in your ` /usr/share/evil_files/ ` directory. Use your terminal to tell us the name of that file. *(Hint: use the cd and ls commands)*

- ➢ What is the flag inside the file? *(Hint: use the cat command)*

We noticed a hidden file in your ` /dev/secret/ ` directory. What is the name of the file? *(Hint: use the ` ls -a ` command to show hidden files)*

- ➢ What type of file is this? *(Hint: use the ` file ` command to reveal the file type)*

We used a Caesar cipher to hide the flag inside the file.

- ➢ What is the unciphered flag? *(Hint: use a tool like Cyberchef to decode the flag)*

picoCTF: Shell Command Practice

- First Grep | Hint: grep command or Ctrl+F
- strings it | Hint: strings command
- extensions | Hint: file command
- Information | Hint: View image metadata, the flag is hidden in Base-64

Note:

These questions are very hard relative to the ones you have seen earlier today.

If you get stuck, try to use our hints with your OSINT skills to move forward!

(10 minutes)

More picoCTF Practice:

- First Grep (Done)
- Lookey Here
- Tab, Tab, Attack
- Wave a flag
- information (Done)
- Nice netcat… (Done)
- crackme.py
- Extensions (Done)
- The Numbers (Done)
- Let’s Warm Up (Done)
- 2Warm (Done)

Credits

Thank you to Benjamin Arbit for helping with the content, graphics, and formatting of this slide show.

He also made The Cat.