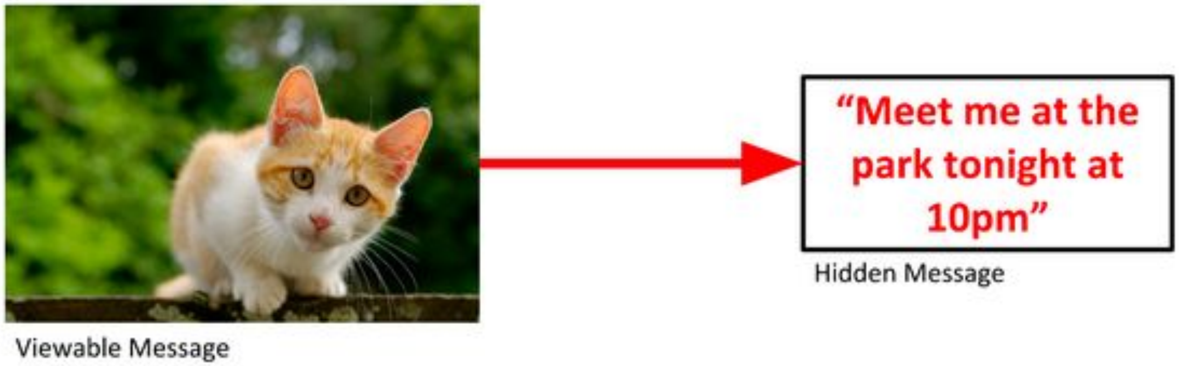
S.H.E.L.L.

SECURITY IS AN ILLUSION

Hiding Data in Files

Steganography

- Steganography is the practice of hiding data in plain sight. Steganography is often embedded in images or audio.
- You could send a picture of a cat to a friend and hide text inside. Looking at the image, there’s nothing to make anyone think there’s a message hidden inside it.



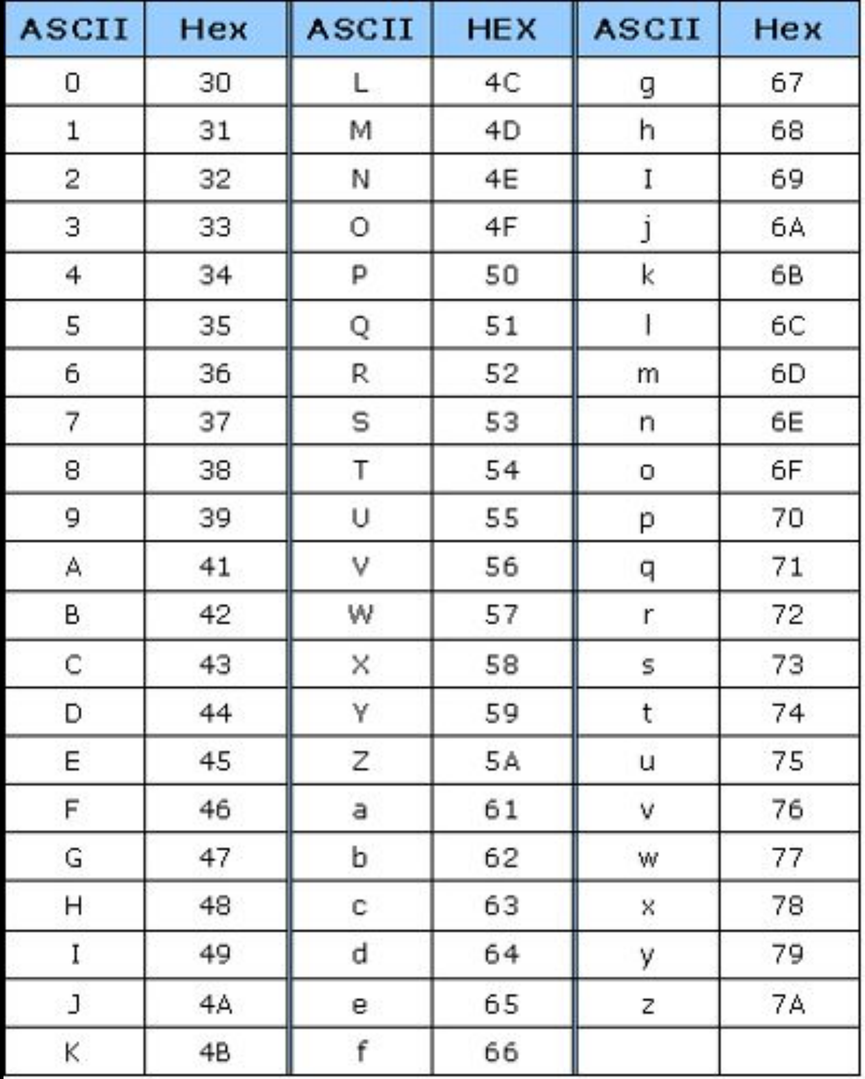
S.H.E.L.L.
SECURITY IS AN ILLUSION

HexDump

- File Extensions are not the sole way to identify the type of a file, files have certain leading bytes called file signatures which allow programs to parse the data in a consistent manner
- File signatures (also known as File Magic Numbers) are bytes within a file used to identify the format of the file. Generally they’re 2-4 bytes long, found at the beginning of a file.
- Example for PNG
- Magic Number -> 89 50 4E 47 0D 0A 1A 0A
- For zip
- Magic Number->50 4B 03 04
- Link to garykessler database https://www.garykessler.net/library/file_sigs.html

S.H.E.L.L.
SECURITY IS AN ILLUSION

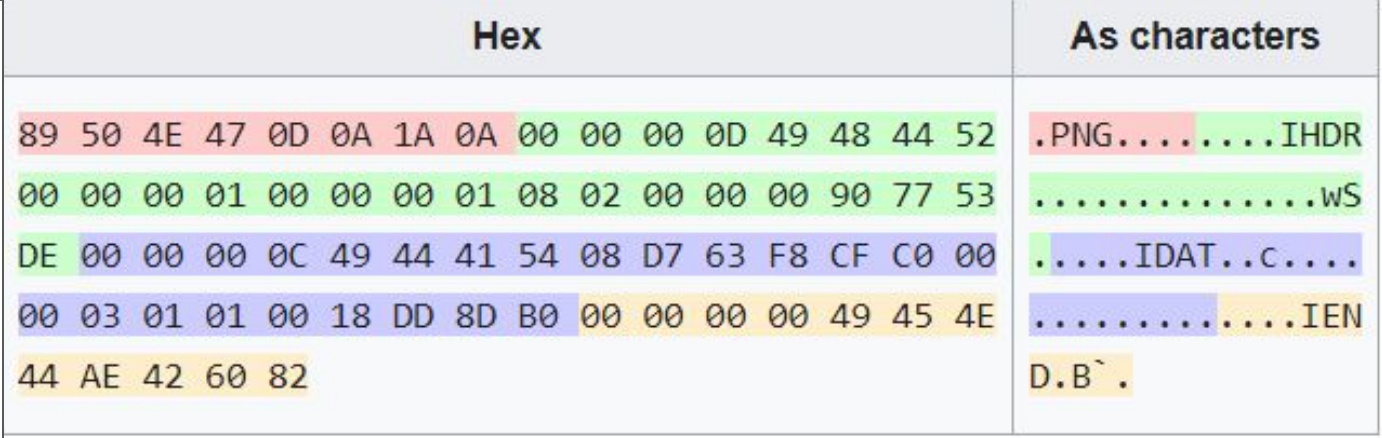
Hex to ASCII table



ASCII	Hex	ASCII	HEX	ASCII	Hex
0	30	L	4C	g	67
1	31	M	4D	h	68
2	32	N	4E	I	69
3	33	O	4F	j	6A
4	34	P	50	k	6B
5	35	Q	51	l	6C
6	36	R	52	m	6D
7	37	S	53	n	6E
8	38	T	54	o	6F
9	39	U	55	p	70
A	41	V	56	q	71
B	42	W	57	r	72
C	43	X	58	s	73
D	44	Y	59	t	74
E	45	Z	5A	u	75
F	46	a	61	v	76
G	47	b	62	w	77
H	48	c	63	x	78
I	49	d	64	y	79
J	4A	e	65	z	7A
K	4B	f	66		

S.H.E.L.L.
SECURITY IS AN ILLUSION

Structure of PNG Image



Hex	As characters
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	.PNG........IHDR
00 00 00 01 00 00 00 01 08 02 00 00 00 90 77 53	..............wS
DE 00 00 00 0C 49 44 41 54 08 D7 63 F8 CF C0 00	.....IDAT..c....
00 03 01 01 00 18 DD 8D B0 00 00 00 00 49 45 4E	.............IEN
44 AE 42 60 82	D.B`.

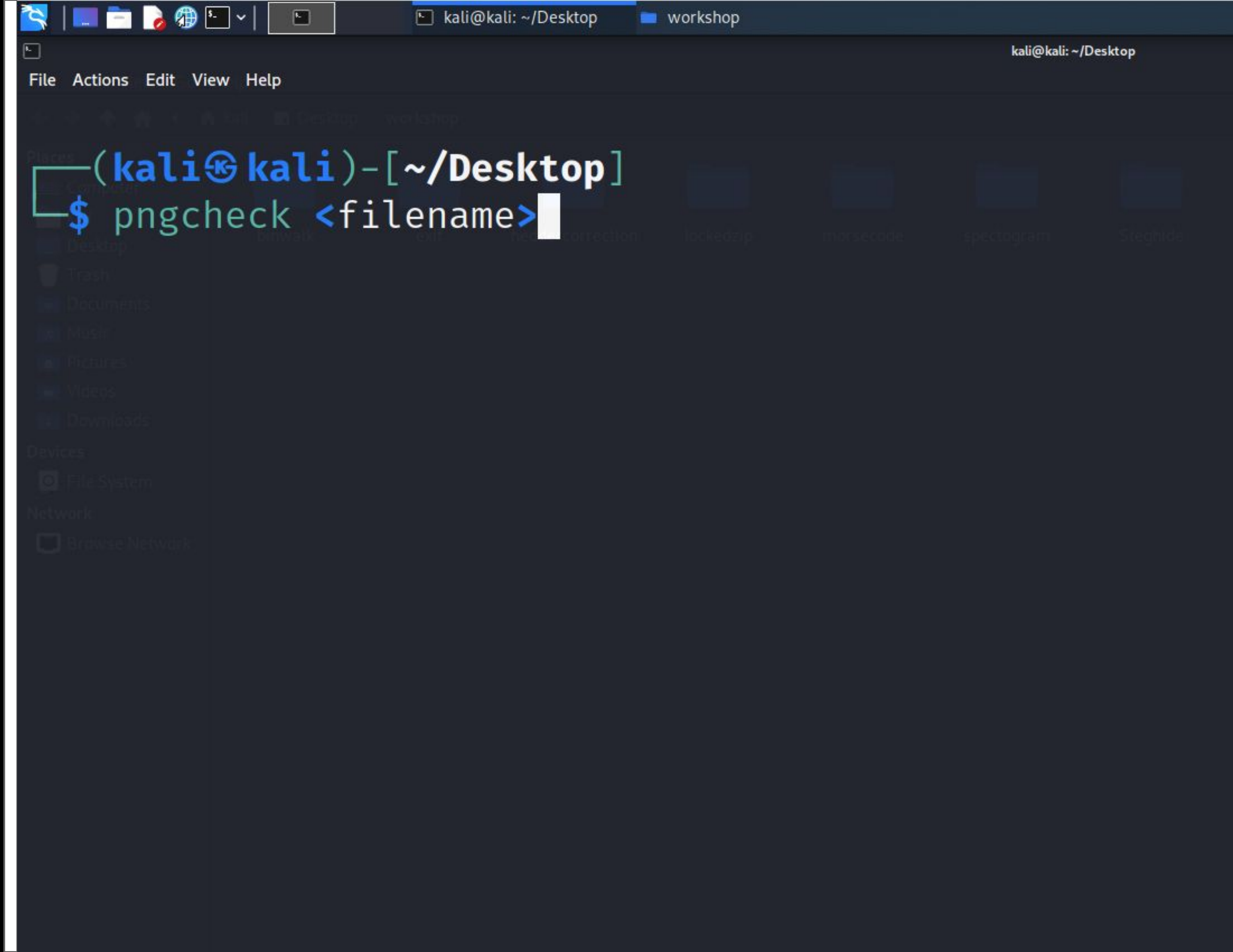
- **PNG image signature** 89 50 4E 47 0D 0A 1A 0A
- **IHDR Chunk:**It is the first chunk(in order) It contains information like width,height,bit depth,colour depth,compression method ect
- **IDAT chunk:**The IDAT chunk contains the actual image data, which is the output stream of the compression algorithm.
- IEND:marks the image end; the data field of the IEND chunk has 0 bytes/is empty.

Fun Fact

- Magic Numbers for zip are
  50 4B 03 04 which Stands for PK in ASCII
  These are the initials of Phil Katz co creator of zip format
- If you found these in a hex file there is a possibility that there might be an archive embedded in it

S.H.E.L.L.
SECURITY IS AN ILLUSION

pngcheck tool

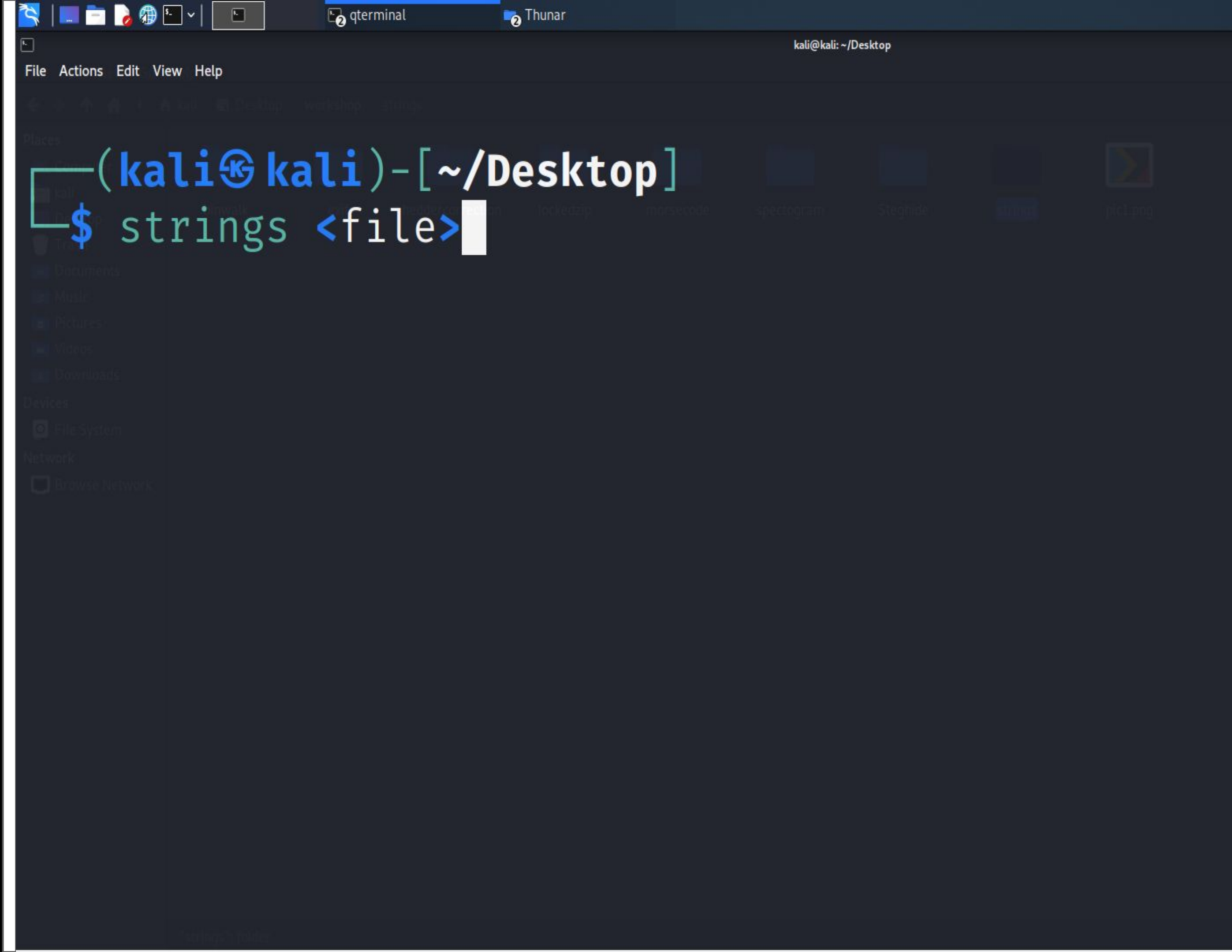


```
┌──(kali㉿kali)-[~/Desktop]
└─$ pngcheck <filename>
```

S.H.E.L.L.

SECURITY IS AN ILLUSION

Checking strings in a file

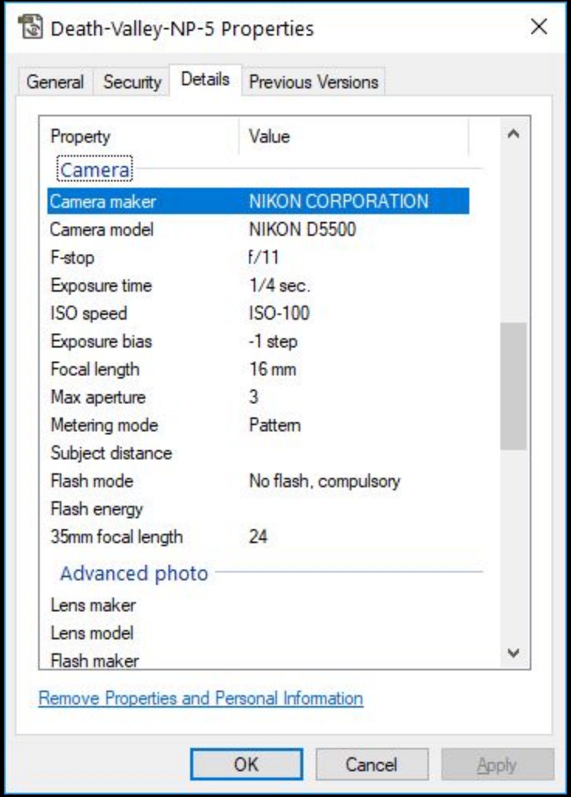


```
┌──(kali㉿kali)-[~/Desktop]
└─$ strings <file>
```

S.H.E.L.L.
SECURITY IS AN ILLUSION

Exif

Exchangeable image file format also known as exif is standard to add specific metadata tags.

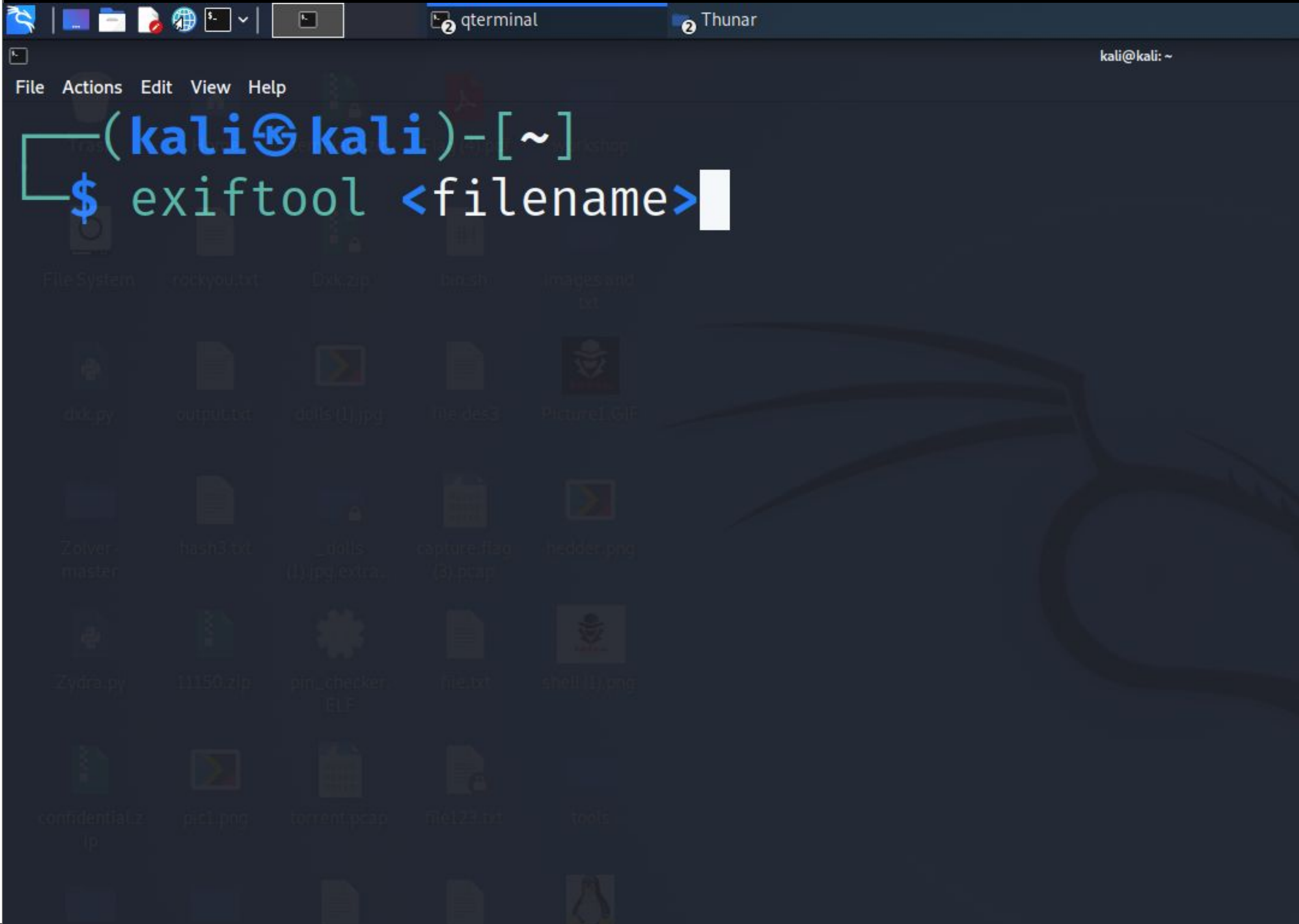


Death-Valley-NP-5 Properties

Property	Value
Camera	
Camera maker	NIKON CORPORATION
Camera model	NIKON D5500
F-stop	f/11
Exposure time	1/4 sec.
ISO speed	ISO-100
Exposure bias	-1 step
Focal length	16 mm
Max aperture	3
Metering mode	Pattern
Subject distance	
Flash mode	No flash, compulsory
Flash energy	
35mm focal length	24
Advanced photo	
Lens maker	
Lens model	
Flash maker	

Exiftool

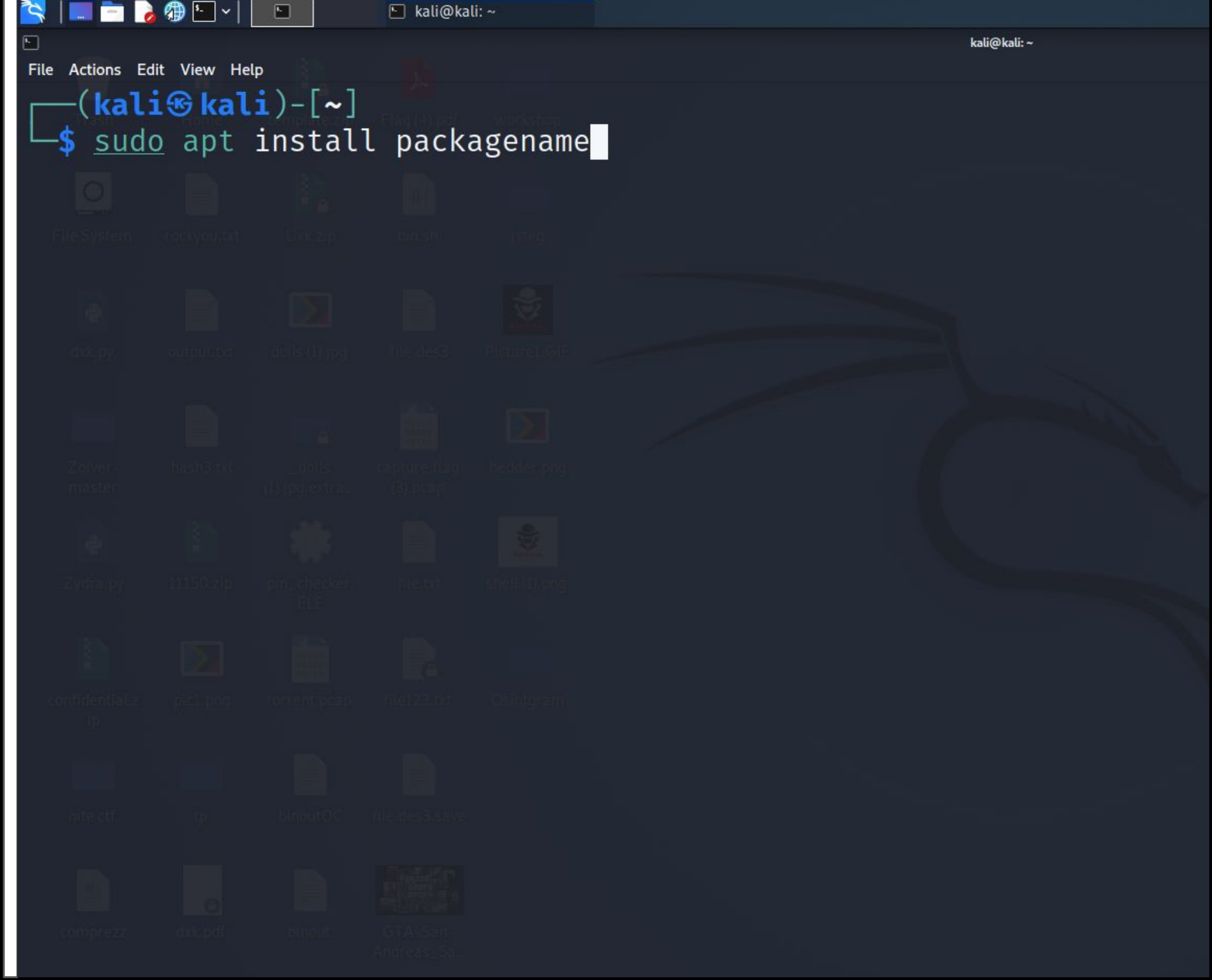
- In linux you can use Exiftool



```
┌──(kali㉿kali)-[~]
└─$ exiftool <filename>
```

S.H.E.L.L.
SECURITY IS AN ILLUSION

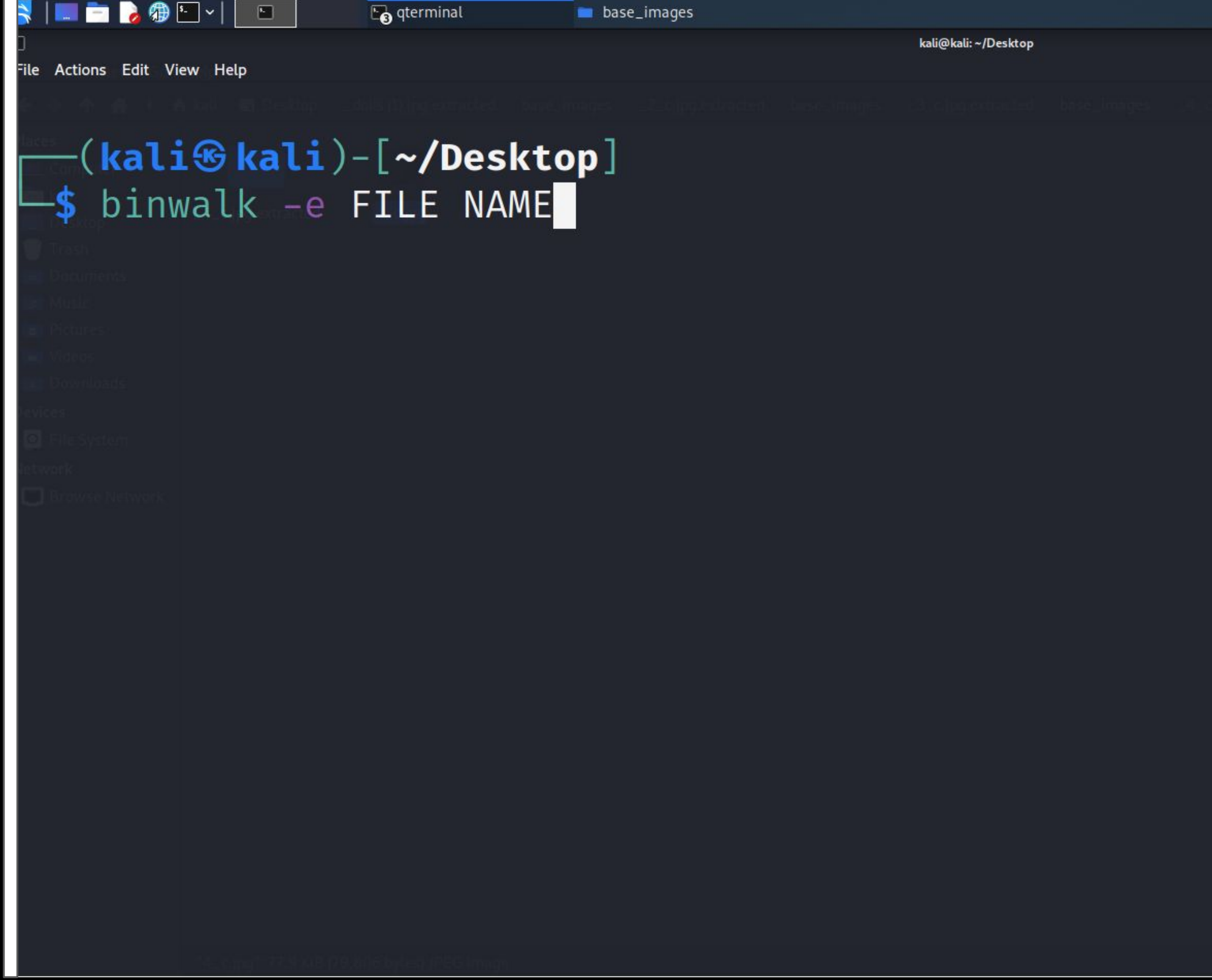
How to install packages using apt



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install packagename
```

S.H.E.L.L.
SECURITY IS AN ILLUSION

binwalk



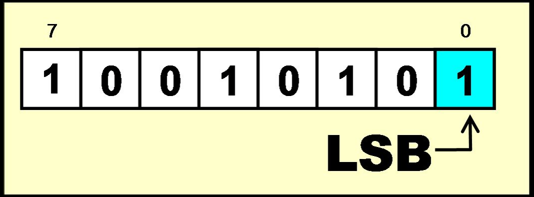
```
┌──(kali㉿kali)-[~/Desktop]
└─$ binwalk -e FILE NAME
```

S.H.E.L.L.

SECURITY IS AN ILLUSION

Least Significant Bit Encoding

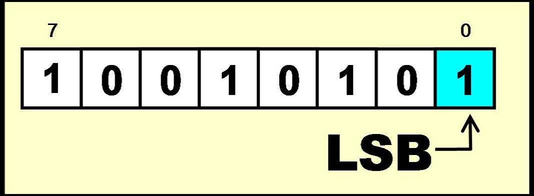
LSB, the least significant bit is the lowest bit in a series of numbers in binary; which is located at the far right of a string. For example, in the binary number: 10111001, the least significant bit is the far right 1.

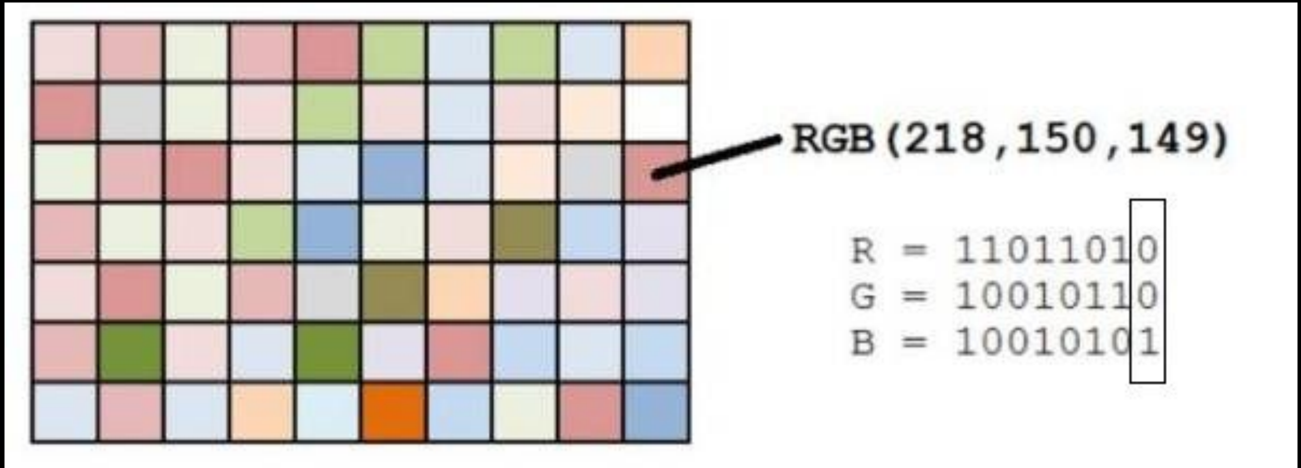


S.H.E.L.L.
SECURITY IS AN ILLUSION

RGB Colour Model

RGB Colour model:
RGB(8bits,8bits,8bits)
8bits=2^8=256 Colours
Total colours=(256x256x256)
=16777216 colours



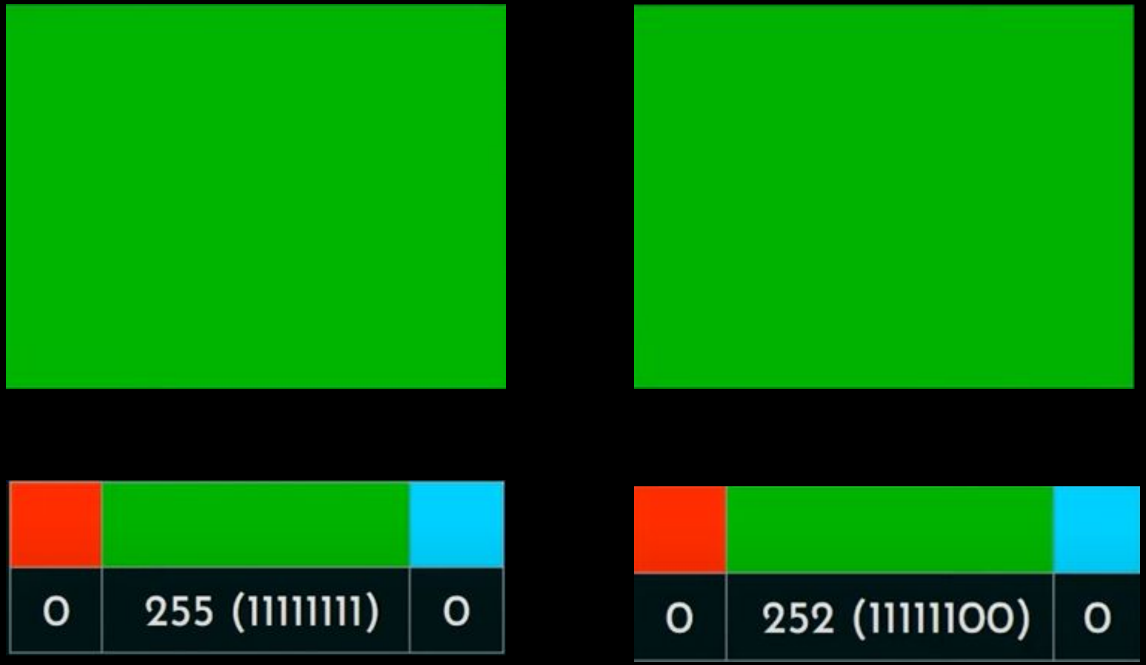

RGB(218,150,149)

R = 11011010
G = 10010110
B = 10010101

Fact!!!

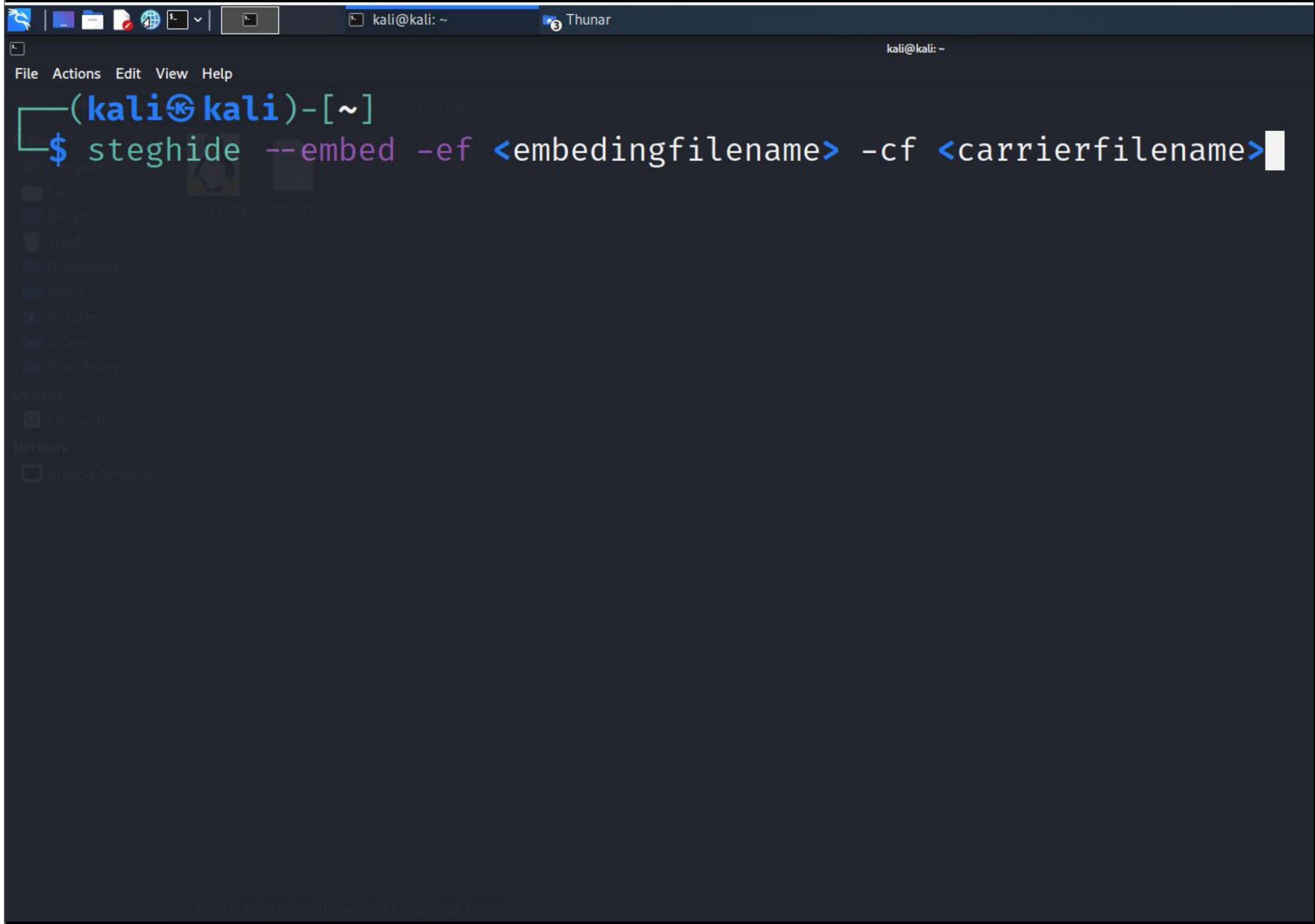
Out of those 16777216 colours
Human eye can distinguish about 10 million different colours
The human eye can’t distinguish between remaining 6 million colours

Can you Differentiate between these two colours?



S.H.E.L.L.
SECURITY IS AN ILLUSION

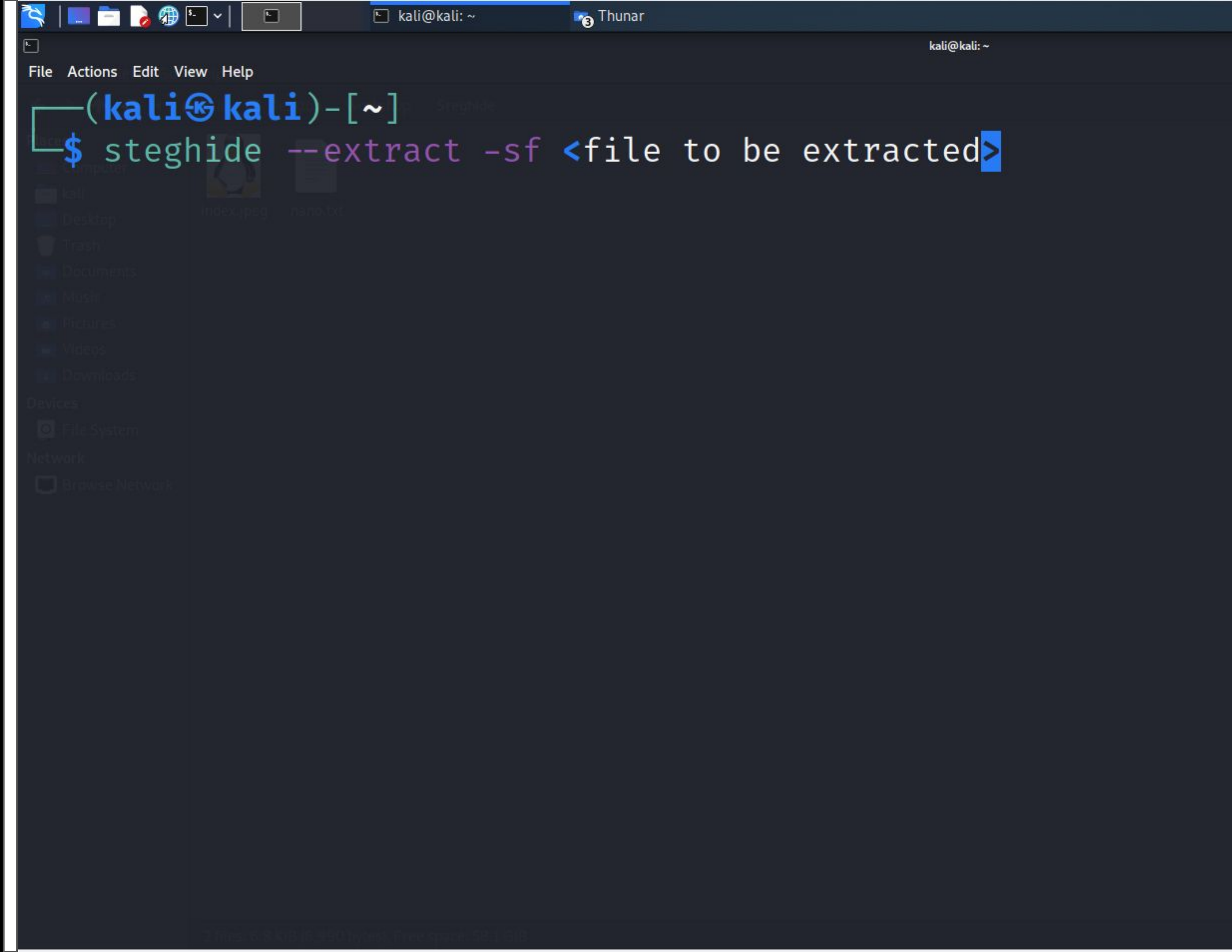
Hiding data using steghide



```
┌──(kali㉿kali)-[~]
└─$ steghide --embed -ef <embedingfilename> -cf <carrierfilename>
```

S.H.E.L.L.
SECURITY IS AN ILLUSION

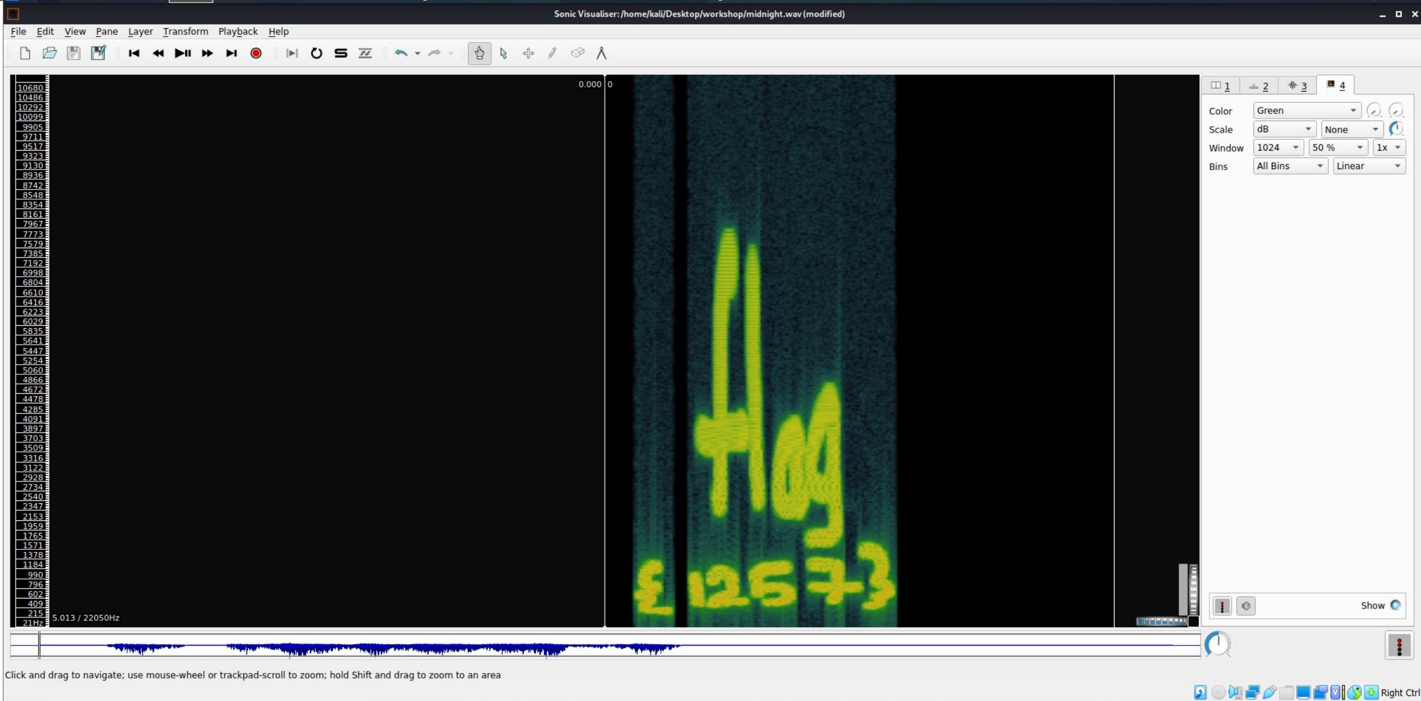
Hiding data using steghide



```
┌──(kali㉿kali)-[~]
└─$ steghide --extract -sf <file to be extracted>
```

S.H.E.L.L.
SECURITY IS AN ILLUSION

Data Hidden In Spectrogram



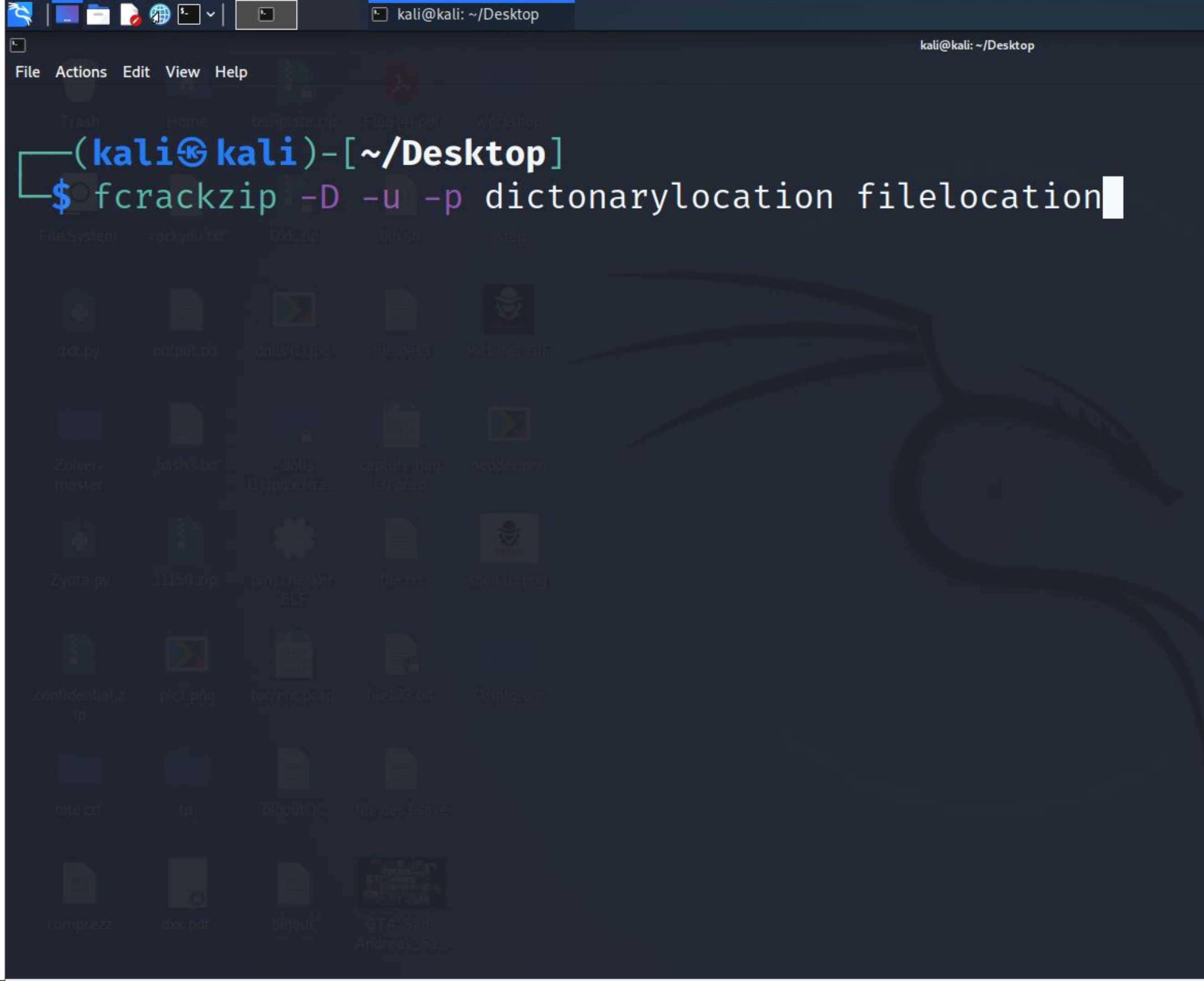
Sonic Visualiser: /home/kali/Desktop/workshop/midnight.wav (modified)

Color: Green
Scale: dB, None
Window: 1024, 50 %, 1x
Bins: All Bins, Linear

Click and drag to navigate; use mouse-wheel or trackpad-scroll to zoom; hold Shift and drag to zoom to an area

Link to sonic visualiser : https://www.sonicvisualiser.org/

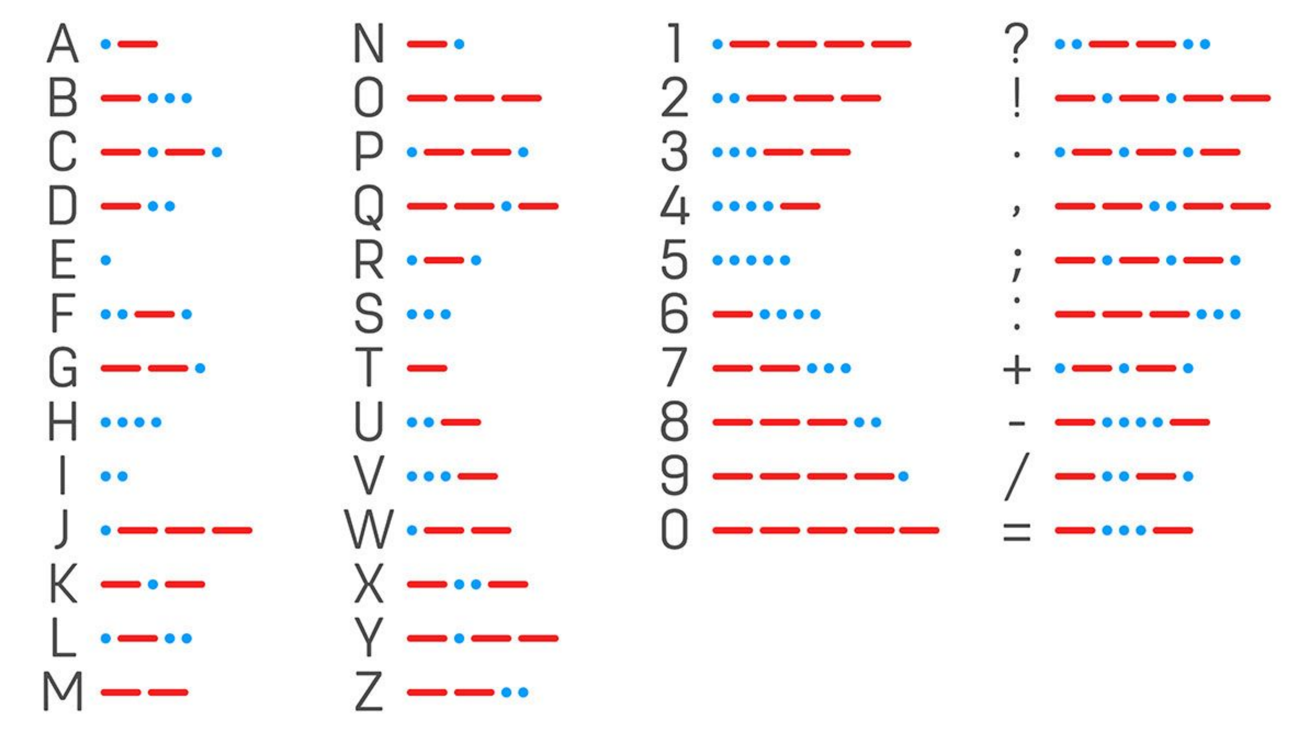
Password Cracking of zip using fcrackzip



```
┌──(kali㉿kali)-[~/Desktop]
└─$ fcrackzip -D -u -p dictonarylocation filelocation
```

S.H.E.L.L.
SECURITY IS AN ILLUSION

Morse Code



A	•—	N	—•	1	•————	?	••——••
B	—•••	O	———	2	••———	!	—•—•——
C	—•—•	P	•——•	3	•••——	.	•—•—•—
D	—••	Q	——•—	4	••••—	,	——••——
E	•	R	•—•	5	•••••	;	—•—•—•
F	••—•	S	•••	6	—••••	:	———•••
G	——•	T	—	7	——•••	+	•—•—•
H	••••	U	••—	8	———••	-	—••••—
I	••	V	•••—	9	————•	/	—••—•
J	•———	W	•——	0	—————	=	—•••—
K	—•—	X	—••—				
L	•—••	Y	—•——				
M	——	Z	——••				

Link to decoding website
https://morsecode.world/international/decoder/audio-decoder-adaptive.html

S.H.E.L.L.

SECURITY IS AN ILLUSION

Thank You