Handling Evidence

Cybersecurity

Digital Forensics, Day 3

Class Objectives

By the end of class today, students will be able to:

- □ Use Autopsy to view and tag evidence from emails.
- □ Analyze SMS messages offline in Kali Linux.
- □ Decode hex data in the iPhone image
- □ Prepare a preliminary report using the *Group Evidence Worksheet*.

Warm Up Activity

In this activity, students will review the steps for exporting data from the iPhone image.

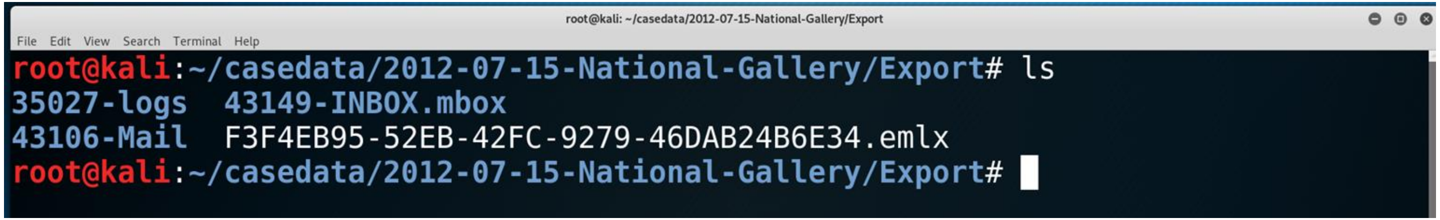
Activities/1-Stu_Warm_Up

Suggested Time:
10 minutes

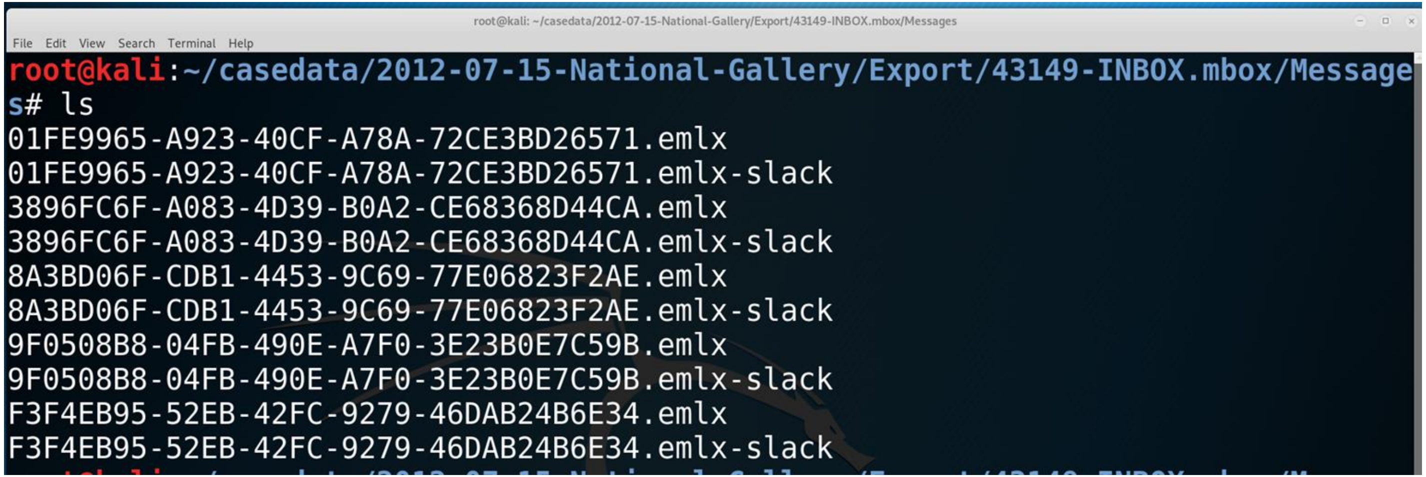
“What’s in Tracy’s Emails?”

Instructor Demo

Displaying the email messages in the INBOX.mbox/Messages folder.


root@kali: ~/casedata/2012-07-15-National-Gallery/Export
File Edit View Search Terminal Help

```
root@kali:~/casedata/2012-07-15-National-Gallery/Export# ls
35027-logs   43149-INBOX.mbox
43106-Mail   F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
root@kali:~/casedata/2012-07-15-National-Gallery/Export# 
```


root@kali: ~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Messages
File Edit View Search Terminal Help

```
root@kali:~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Message
s# ls
01FE9965-A923-40CF-A78A-72CE3BD26571.emlx
01FE9965-A923-40CF-A78A-72CE3BD26571.emlx-slack
3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx-slack
8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx-slack
9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx-slack
F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx-slack
```

Open a terminal window and cd to the directory that contains the INBOX.mbox directory.

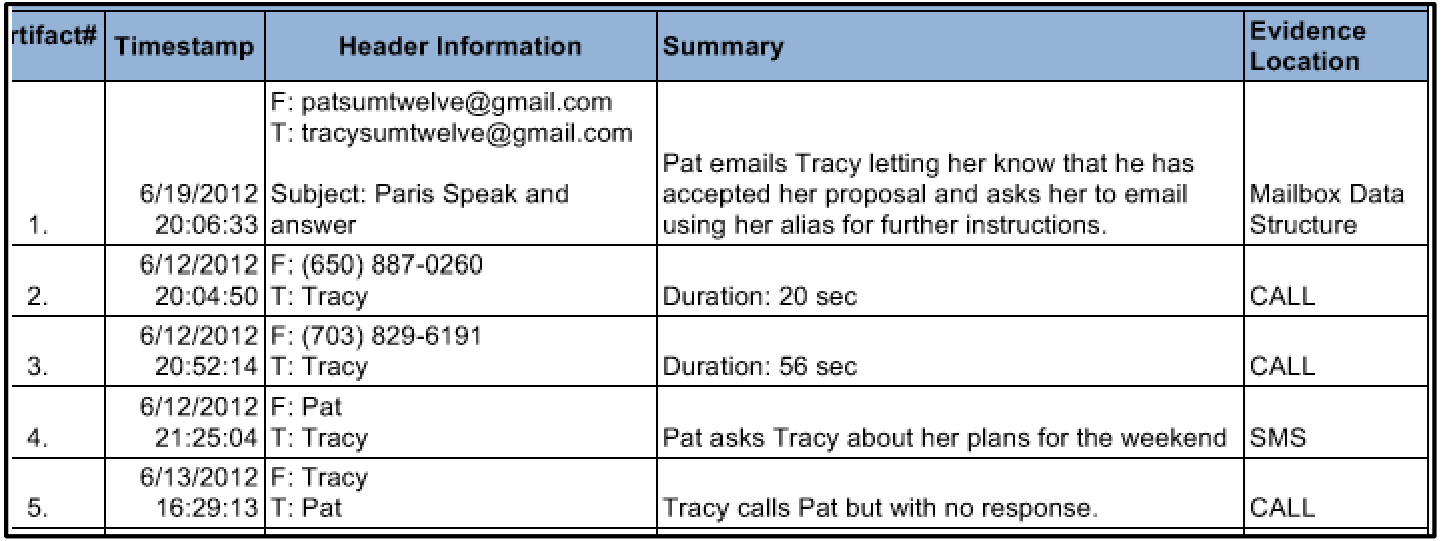
cd to the Messages folder and display the .emlx files.

Tracy’s Emails

Search for Contact Information

In the next activity, you will:

- Work in groups to examine Tracy's email messages to find any contacts from the scenario.
- Look at any email attachments.
- Tag any items of interest in Autopsy.



rtifact#	Timestamp	Header Information	Summary	Evidence Location
1.	6/19/2012 20:06:33	F: patsumtwelve@gmail.com T: tracysumtwelve@gmail.com Subject: Paris Speak and answer	Pat emails Tracy letting her know that he has accepted her proposal and asks her to email using her alias for further instructions.	Mailbox Data Structure
2.	6/12/2012 20:04:50	F: (650) 887-0260 T: Tracy	Duration: 20 sec	CALL
3.	6/12/2012 20:52:14	F: (703) 829-6191 T: Tracy	Duration: 56 sec	CALL
4.	6/12/2012 21:25:04	F: Pat T: Tracy	Pat asks Tracy about her plans for the weekend	SMS
5.	6/13/2012 16:29:13	F: Tracy T: Pat	Tracy calls Pat but with no response.	CALL

Activity: What’s in Tracy’s Emails?

In this activity, you will use Autopsy to examine Tracy’s email correspondence and generate a list of contacts and their email addresses.

Activities/2-Stu_Emails

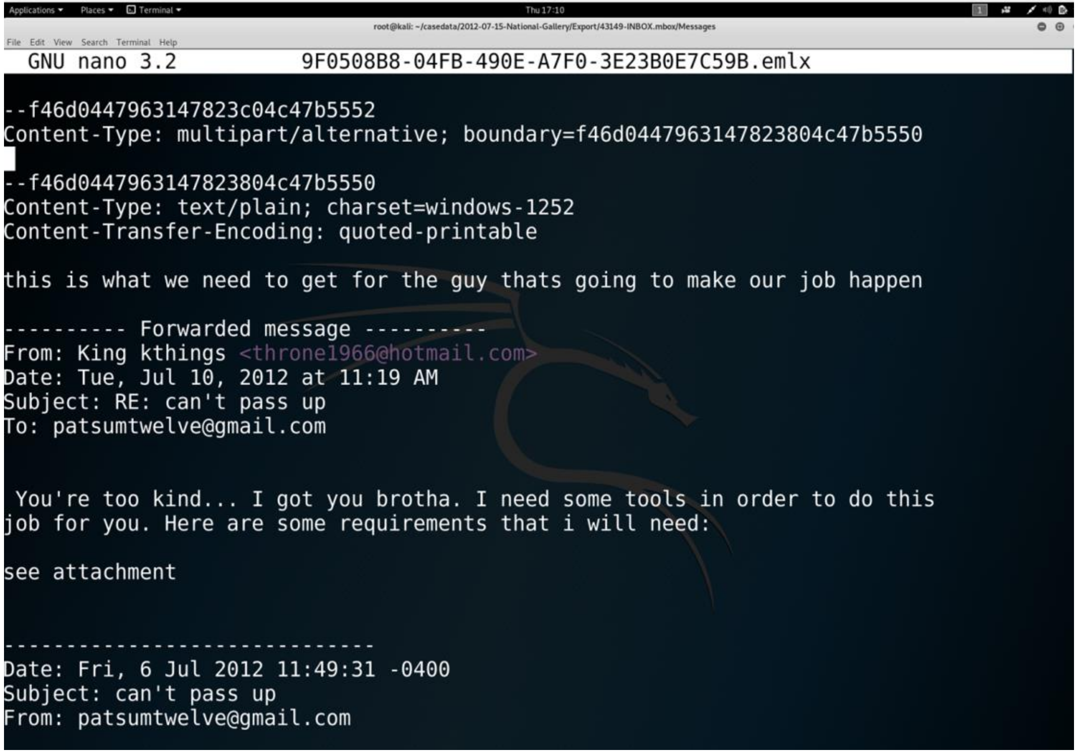
Suggested Time:
20 Minutes

Tracy’s Email Review

What evidence did you find?

Tracy’s Email Review

Email 9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

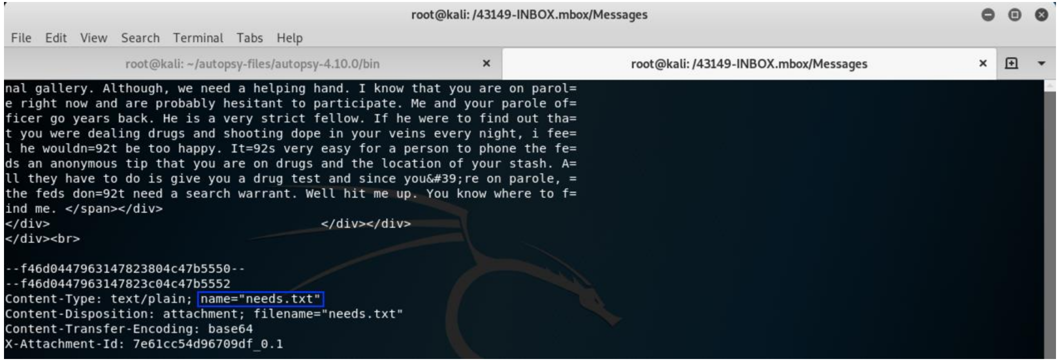


Applications ▾
Places ▾
Terminal ▾
Thu 17:10
root@kali: ~/casedata/2012-07-15-National-Gallery/Export/43149-INBOX.mbox/Messages
File Edit View Search Terminal Help

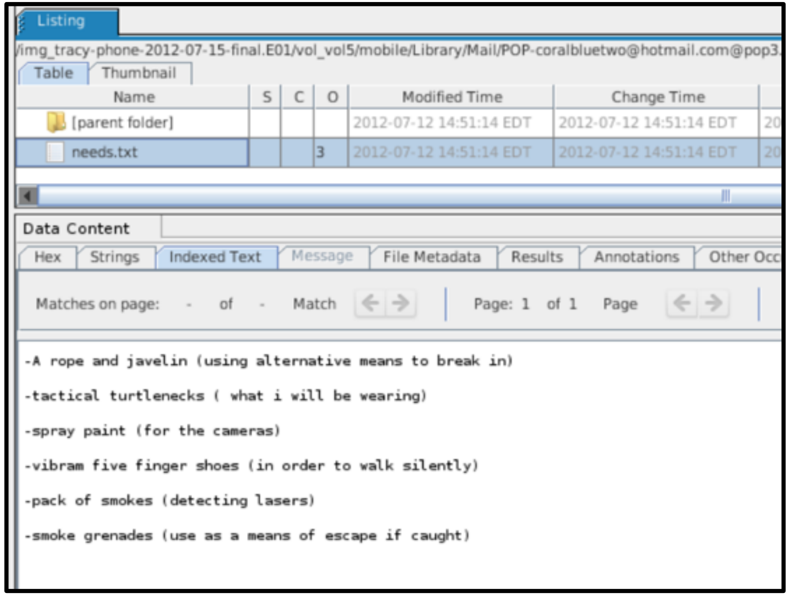
```
  GNU nano 3.2          9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

--f46d0447963147823c04c47b5552
Content-Type: multipart/alternative; boundary=f46d0447963147823804c47b5550

--f46d0447963147823804c47b5550
Content-Type: text/plain; charset=windows-1252
Content-Transfer-Encoding: quoted-printable

this is what we need to get for the guy thats going to make our job happen

---------- Forwarded message ----------
From: King kthings <throne1966@hotmail.com>
Date: Tue, Jul 10, 2012 at 11:19 AM
Subject: RE: can't pass up
To: patsumtwelve@gmail.com


 You're too kind... I got you brotha. I need some tools in order to do this
job for you. Here are some requirements that i will need:

see attachment



------------------------------
Date: Fri, 6 Jul 2012 11:49:31 -0400
Subject: can't pass up
From: patsumtwelve@gmail.com
```

Tracy’s Email Review

The email has an attachment.


root@kali: /43149-INBOX.mbox/Messages
File Edit View Search Terminal Tabs Help
root@kali: ~/autopsy-files/autopsy-4.10.0/bin
root@kali: /43149-INBOX.mbox/Messages

```
nal gallery. Although, we need a helping hand. I know that you are on parol=
e right now and are probably hesitant to participate. Me and your parole of=
ficer go years back. He is a very strict fellow. If he were to find out tha=
t you were dealing drugs and shooting dope in your veins every night, i fee=
l he wouldn=92t be too happy. It=92s very easy for a person to phone the fe=
ds an anonymous tip that you are on drugs and the location of your stash. A=
ll they have to do is give you a drug test and since you&#39;re on parole, =
the feds don=92t need a search warrant. Well hit me up. You know where to f=
ind me. </span></div>
</div>                                      </div></div>
</div><br>

--f46d0447963147823804c47b5550--
--f46d0447963147823c04c47b5552
Content-Type: text/plain; name="needs.txt"
Content-Disposition: attachment; filename="needs.txt"
Content-Transfer-Encoding: base64
X-Attachment-Id: 7e61cc54d96709df_0.1
```



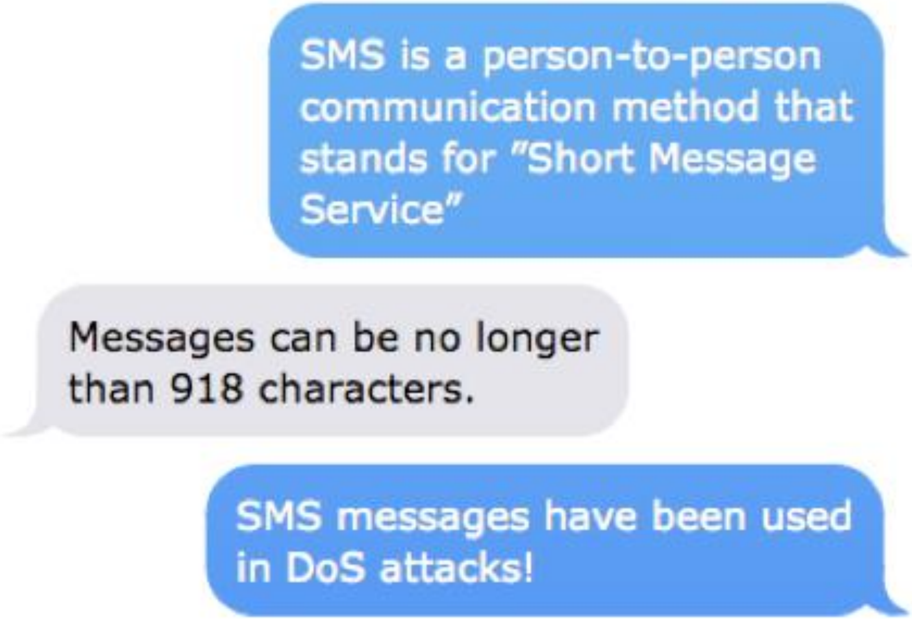
/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.

Name	S	C	O	Modified Time	Change Time
[parent folder]				2012-07-12 14:51:14 EDT	2012-07-12 14:51:14 EDT
needs.txt			3	2012-07-12 14:51:14 EDT	2012-07-12 14:51:14 EDT

```
-A rope and javelin (using alternative means to break in)

-tactical turtlenecks ( what i will be wearing)

-spray paint (for the cameras)

-vibram five finger shoes (in order to walk silently)

-pack of smokes (detecting lasers)

-smoke grenades (use as a means of escape if caught)
```

“Who is Tracy Texting?”

What is an SMS?



SMS is a person-to-person communication method that stands for "Short Message Service"

Messages can be no longer than 918 characters.

SMS messages have been used in DoS attacks!

iPhone SMS

Steps to view SMS entries in an iPhone image

01 From the Tools menu, select File Search by Attribute.

02 Click the box next to Name and type `sms.db`.

03 Click the Search button.

04 Now select `sms.db` from the Listing pane.

05 Select the `Indexed Text` tab in the Data Content pane to see Tracy’s emails.

Activity: Who is Tracy Texting?

In this activity, you will view the SMS text messages on Tracy’s iPhone to gather more information about the case.

Activities/3-Stu_SMS

Suggested Time:
15 Minutes

Review: Who is Tracy Texting?

1. Use the file search to find the sms database.

2. View the messages in the Data Content pane.

3. Analyze the text messages and phone numbers to establish any connections to the case and answer the following questions:

- What is Terry’s phone number?
- What is Pat’s phone number?
- What was the fraudulent number that texted about a gift card? Is it relevant to the case? Why or why not?

4. Update your Evidence Worksheet with any additional evidence.

Review: Who is Tracy Texting?

What is Terry’s phone number?

703-829-6071. It is evident because she talks about her dad multiple times and Tracey informs her she cannot afford private school anymore.

What is Pat’s phone number?

571-308-3236. The text message refers toTracey as sis. A response message from Tracey identifies him as “pat”.

What was the fraudulent number that texted about a gift card? Is it relevant to the case?

206-910-0932. Looking at the website link that went with the message, it appears this text was spam. So, no it is not relevant.

Review: Who is Tracy Texting?

4. Update your Evidence Worksheet with any additional evidence.

Carry

- Email Cat2welve@gmail.com, Cat2welve@gmail.com Carrysum2012@yahoo.com,
- Phone: +1 (202) 725-2124

Alex J

- Email Alex.jfam11@gmail.com, Alexjfam11@gmail.com
- Phone: +1 (205) 208-5299

Drex Mustafar

- Email: bubbahotep2012@hotmail.com

Perhem Shien

- Email: Perhem.shien@gmail.com, supershien@live.com

Decoding Hex Data in Tracy’s iPhone

Sometimes
data we uncover will only
*be readable in a **hexadecimal***
numbering format.

Why is Hexadecimal Important?

The ability to read a hex dump will allow you to explore a whole new space of evidence that could not be read in the browsing data.

- Hex is used to display the location in memory at which data is stored.

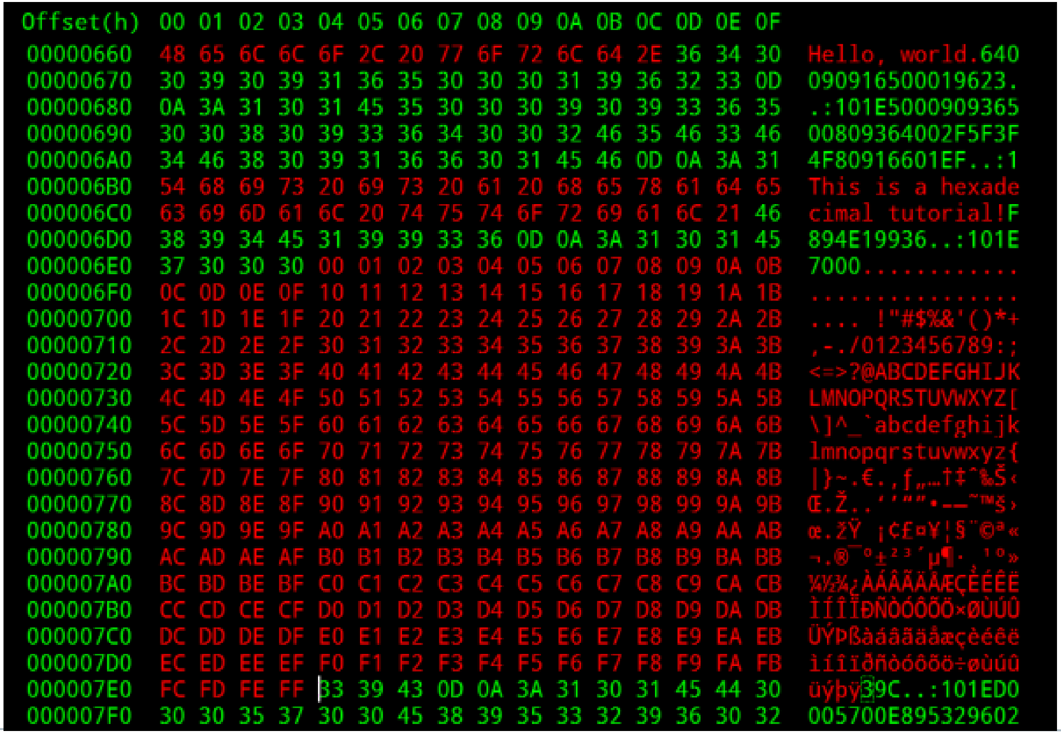
- Hex is used to decode data, such as executable code in a memory dump or a malicious document embedded in an image or network log.

Refresher: All information is stored in a computer as* binary 1*s and* 0*s.

- We need to encode this information into human-readable formats.
- Hexadecimal is the most common representation of binary encoding.

Why is Hexadecimal Important?

As it pertains to our forensics investigation, the ability to read a hex dump will allow us to explore a whole new space of evidence they could not read in the browsing data.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
 00000660 48 65 6C 6C 6F 2C 20 77 6F 72 6C 64 2E 36 34 30  Hello, world.640
 00000670 30 39 30 39 31 36 35 30 30 30 31 39 36 32 33 0D  090916500019623.
 00000680 0A 3A 31 30 31 45 35 30 30 30 39 30 39 33 36 35  .:101E5000909365
 00000690 30 30 38 30 39 33 36 34 30 30 32 46 35 46 33 46  00809364002F5F3F
 000006A0 34 46 38 30 39 31 36 36 30 31 45 46 0D 0A 3A 31  4F80916601EF..:1
 000006B0 54 68 69 73 20 69 73 20 61 20 68 65 78 61 64 65  This is a hexade
 000006C0 63 69 6D 61 6C 20 74 75 74 6F 72 69 61 6C 21 46  cimal tutorial!F
 000006D0 38 39 34 45 31 39 39 33 36 0D 0A 3A 31 30 31 45  894E19936..:101E
 000006E0 37 30 30 30 00 01 02 03 04 05 06 07 08 09 0A 0B  7000............
 000006F0 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B  ................
 00000700 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B  .... !"#$%&'()*+
 00000710 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B  ,-./0123456789:;
 00000720 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B  <=>?@ABCDEFGHIJK
 00000730 4C 4D 4E 4F 50 51 52 53 54 55 56 57 58 59 5A 5B  LMNOPQRSTUVWXYZ[
 00000740 5C 5D 5E 5F 60 61 62 63 64 65 66 67 68 69 6A 6B  \]^_`abcdefghijk
 00000750 6C 6D 6E 6F 70 71 72 73 74 75 76 77 78 79 7A 7B  lmnopqrstuvwxyz{
 00000760 7C 7D 7E 7F 80 81 82 83 84 85 86 87 88 89 8A 8B  |}~.€.‚ƒ„…†‡ˆ‰Š‹
 00000770 8C 8D 8E 8F 90 91 92 93 94 95 96 97 98 99 9A 9B  Œ.Ž..‘’“”•–—˜™š›
 00000780 9C 9D 9E 9F A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB  œ.žŸ ¡¢£¤¥¦§¨©ª«
 00000790 AC AD AE AF B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB  ¬.®¯°±²³´µ¶·¸¹º»
 000007A0 BC BD BE BF C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB  ¼½¾¿ÀÁÂÃÄÅÆÇÈÉÊË
 000007B0 CC CD CE CF D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB  ÌÍÎÏÐÑÒÓÔÕÖ×ØÙÚÛ
 000007C0 DC DD DE DF E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA EB  ÜÝÞßàáâãäåæçèéêë
 000007D0 EC ED EE EF F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB  ìíîïðñòóôõö÷øùúû
 000007E0 FC FD FE FF 33 39 43 0D 0A 3A 31 30 31 45 44 30  üýþÿ39C..:101ED0
 000007F0 30 30 35 37 30 30 45 38 39 35 33 32 39 36 30 32  005700E895329602
```

In order to better understand and decode hex, we'll need to take a closer look at ASCII and decimal characters.

Basic Character Encoding

In order to better understand and decode hex, we’ll need to take a closer look at ASCII and decimal characters.

- We can visualize the characters that represent a computer's data by using a **cipher**.
- These ciphers generally have a **lookup table** we use to interpret the meanings of encoded texts:

Example:

Plain alphabet : a b c d e f

Cipher alphabet: p h q g i u

Message: abc -> phq.

ASCII and The Decimal System

ASCII stands for the American Standard Code for Information Interchange.

- It is used to represent computer-stored characters in a *human-readable* format.
- Look down at you keyboards. Every character is part of ASCII: Upper and lowercase letters, special characters (!@#$ etc.), numericals (1,2,3,4…)

The Decimal system is a little more limited.

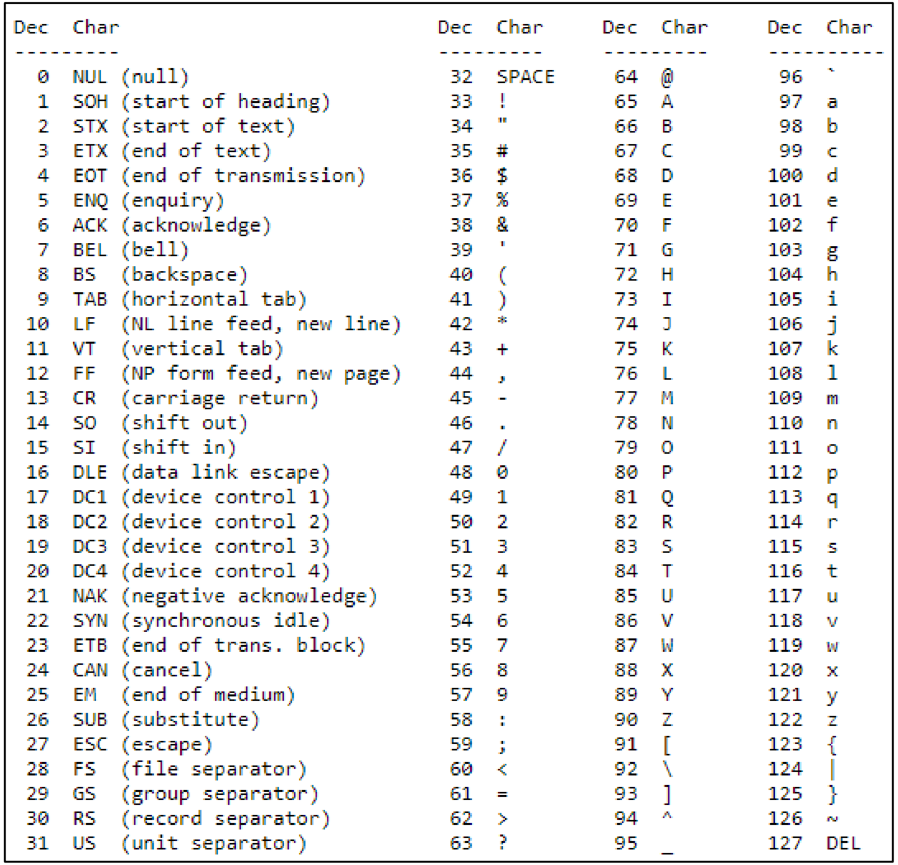
- Consists of the characters 12 3 4 5 6 7 8 9.
- The limited amount of characters doesn't mean we can't convey complex information. In fact, anything we write in ASCII can be converted in decimal format:

Example:

ASCII: *A, B, C. It's easy as 1, 2, 3!*

Decimal: 65 44 32 66 44 32 67 46 32 73 116 39 115 32 101 97 115 121 32 97 115 32 49 44 32 50 44 32 51 33

ASCII - Decimal Conversion



Dec	Char	Dec	Char	Dec	Char	Dec	Char
0	NUL (null)	32	SPACE	64	@	96	`
1	SOH (start of heading)	33	!	65	A	97	a
2	STX (start of text)	34	"	66	B	98	b
3	ETX (end of text)	35	#	67	C	99	c
4	EOT (end of transmission)	36	$	68	D	100	d
5	ENQ (enquiry)	37	%	69	E	101	e
6	ACK (acknowledge)	38	&	70	F	102	f
7	BEL (bell)	39	'	71	G	103	g
8	BS (backspace)	40	(	72	H	104	h
9	TAB (horizontal tab)	41	)	73	I	105	i
10	LF (NL line feed, new line)	42	*	74	J	106	j
11	VT (vertical tab)	43	+	75	K	107	k
12	FF (NP form feed, new page)	44	,	76	L	108	l
13	CR (carriage return)	45	-	77	M	109	m
14	SO (shift out)	46	.	78	N	110	n
15	SI (shift in)	47	/	79	O	111	o
16	DLE (data link escape)	48	0	80	P	112	p
17	DC1 (device control 1)	49	1	81	Q	113	q
18	DC2 (device control 2)	50	2	82	R	114	r
19	DC3 (device control 3)	51	3	83	S	115	s
20	DC4 (device control 4)	52	4	84	T	116	t
21	NAK (negative acknowledge)	53	5	85	U	117	u
22	SYN (synchronous idle)	54	6	86	V	118	v
23	ETB (end of trans. block)	55	7	87	W	119	w
24	CAN (cancel)	56	8	88	X	120	x
25	EM (end of medium)	57	9	89	Y	121	y
26	SUB (substitute)	58	:	90	Z	122	z
27	ESC (escape)	59	;	91	[	123	{
28	FS (file separator)	60	<	92	\	124	|
29	GS (group separator)	61	=	93	]	125	}
30	RS (record separator)	62	>	94	^	126	~
31	US (unit separator)	63	?	95	_	127	DEL

ASCII characters for numerical digits start at the decimal number 48 and end at 57.

48 (ASCII) = 0 (Decimal),

49 (ASCII) = 1 (Decimal),

57 (ASCII) = 9 (Decimal)

The ASCII upper letters start at the decimal number 65 and end at 90 in the ASCII table.

A (ASCII) = 65 (Decimal),

B (ASCII) = 67 (Decimal)

The ASCII lowercase letters start at decimal number 97 and end at 122.

a (ASCII) = 97 (Decimal)

b(ASCII) = 98 (Decimal)

Hexadecimal

- Data can more efficiently be stored and represented by encoding using the hexadecimal number system.

- The hex system uses **16 symbols** to represent the base values.

- It's a base 16 system: the base numbers range from 0-9 and then the letters A-F (which represent 12-15)

```
base 16: 0 1 2 3 4 5 6 7 8 9 A B C D E F
```

Hex

Hex uses 16 characters to represent the base value. In other words, it is a base 16 system

The base numbers range from 0-9 and then letters A-F represent 11, 12, etc. (A = 11, B= 12, C =13 etc.)

Dec.	Hex.	Dec.	Hex.
0	0	8	8
1	1	9	9
2	2	10	A
3	3	11	B
4	4	12	C
5	5	13	D
6	6	14	E
7	7	15	F

Dec.	Hex.	Dec.	Hex.
16	10	24	18
17	11	25	19
18	12	26	?
19	13	27	?
20	14	28	?
21	15	29	?
22	16	30	?
23	17	31	?

What do you think comes next?

Hex

Hex uses 16 characters to represent the base value. In other words, it is a base 16 system

The base numbers range from 0-9 and then letters A-F.

Dec.	Hex.	Dec.	Hex.
0	0	8	8
1	1	9	9
2	2	10	A
3	3	11	B
4	4	12	C
5	5	13	D
6	6	14	E
7	7	15	F

Dec.	Hex.	Dec.	Hex.
16	10	24	18
17	11	25	19
18	12	26	1A
19	13	27	1B
20	14	28	1C
21	15	29	1D
22	16	30	1E
23	17	31	1F

And after 1F?

Hex

Hex uses 16 characters to represent the base value. In other words, it is a base 16 system

The base numbers range from 0-9 and then letters A-F.

Dec.	Hex.	Dec.	Hex.
0	0	8	8
1	1	9	9
2	2	10	A
3	3	11	B
4	4	12	C
5	5	13	D
6	6	14	E
7	7	15	F

Dec.	Hex.	Dec.	Hex.
16	10	24	18
17	11	25	19
18	12	26	1A
19	13	27	1B
20	14	28	1C
21	15	29	1D
22	16	30	1E
23	17	31	1F

Dec.	Hex.	Dec.	Hex.
32	20	40	28
33	21	41	29
34	22	42	2A
35	23	43	2B
36	24	44	2C
37	25	45	2D
38	26	46	2E
39	27	47	2F

Character Encoding

ASCII → Decimal → Hexadecimal

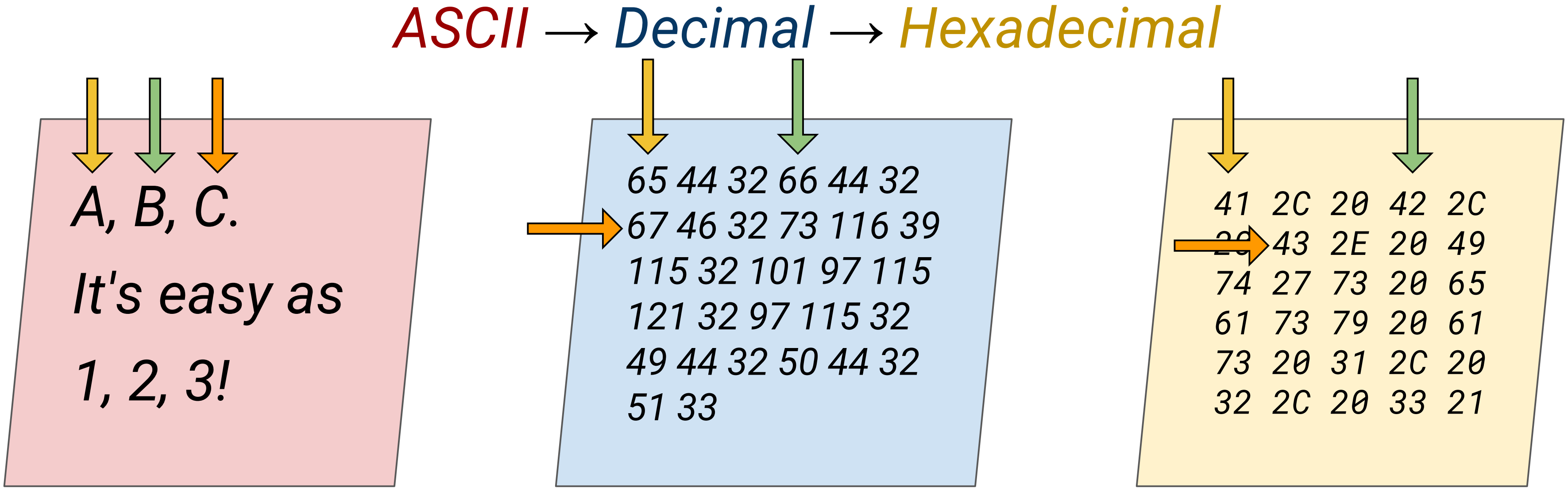
A, B, C.
It's easy as
1, 2, 3!

65 44 32 66 44 32
67 46 32 73 116 39
115 32 101 97 115
121 32 97 115 32
49 44 32 50 44 32
51 33

```
41 2C 20 42 2C
20 43 2E 20 49
74 27 73 20 65
61 73 79 20 61
73 20 31 2C 20
32 2C 20 33 21
```

Which decimal and hexadecimal characters represent “A” “B” and “C”?
Remember: every character, even commas and spaces, are encoded.

Character Encoding



ASCII → *Decimal* → *Hexadecimal*

A, B, C.
It's easy as
1, 2, 3!

65 44 32 66 44 32
67 46 32 73 116 39
115 32 101 97 115
121 32 97 115 32
49 44 32 50 44 32
51 33

```
41 2C 20 42 2C
20 43 2E 20 49
74 27 73 20 65
61 73 79 20 61
73 20 31 2C 20
32 2C 20 33 21
```

Note the sequential order of 65, 66, 67 and 41, 42, 43.
Each separate by the character for comma [,] and space [   ].

But *Why Hex?*

Hexadecimal is the most compact of all the Encoding systems we’ve looked at.

Remember, all disk data is ultimately represented as 1s and 0s.

You may recall from our Cryptography unit, conveying information with only 1’s and 0’s is *not efficient*.

For example:

“A, B, C. It's easy as 1, 2, 3!” =

01000001 00101100 00100000 01000010 00101100 00100000
01000011 00101110 00100000 00001010 01001001 01110100
00100111 01110011 00100000 01100101 01100001 01110011
01111001 00100000 01100001 01110011 00100000 00001010
00110001 00101100 00100000 00110010 00101100 00100000
00110011 00100001 00001010

But *Why Hex?*

Hexadecimal is the most compact of all the Encoding systems we've looked at.

Remember, all disk data is ultimately represented as 1s and 0s.

You may recall from our Cryptography unit, conveying information with only 1's and 0's is *not efficient*.

So, programs save space by converting binary to encoding formats.

Hex is the more compact than ASCII and Decimal.

Activity: Decoding Hex Data in Tracy's iPhone

In this activity, you will work through a few simple hex decodings. Then, you will work with a hex dump from Tracy's iPhone data in the Encase image file.

Activities/4-Stu_Hex_Autopsy

Suggested Time:
20 Minutes

Decoding Hex Review:

Decode the following:

```
48 65 6c 6c 6f 20 57 6f 72 6c 64

54 65 73 74 69 6e 67 20 31 32 33 21

41 6e 64 72 65 77

31 20 32 20 33 20 34 20 35 20 36
```

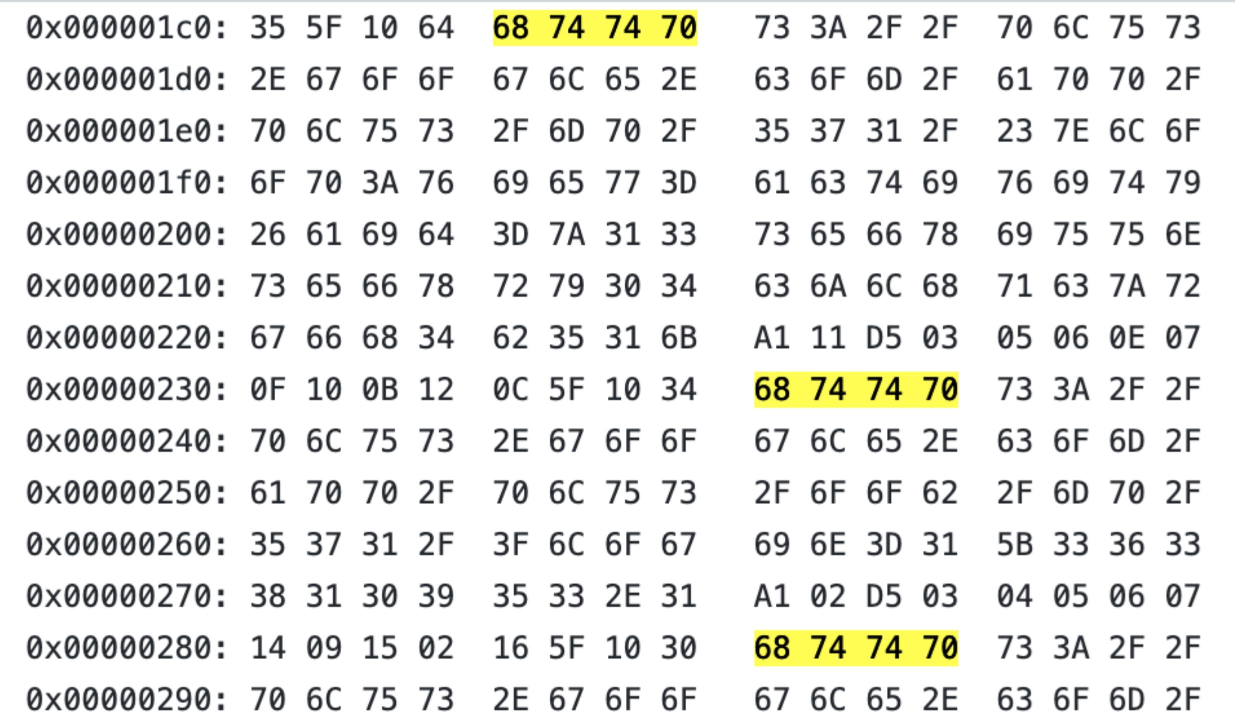
Decoding Hex Review:

Decode the following:

```
48 65 6c 6c 6f 20 57 6f 72 6c 64 = Hello World

54 65 73 74 69 6e 67 20 31 32 33 21 = Testing 123!

41 6e 64 72 65 77 = Andrew

31 20 32 20 33 20 34 20 35 20 36 = 1 2 3 4 5 6
```

Decoding Hex

Note: Knowing that `http` in hex is `68 74 74 70`, we can identify URLs in this hex sequence.



```
0x000001c0: 35 5F 10 64  68 74 74 70  73 3A 2F 2F  70 6C 75 73
0x000001d0: 2E 67 6F 6F  67 6C 65 2E  63 6F 6D 2F  61 70 70 2F
0x000001e0: 70 6C 75 73  2F 6D 70 2F  35 37 31 2F  23 7E 6C 6F
0x000001f0: 6F 70 3A 76  69 65 77 3D  61 63 74 69  76 69 74 79
0x00000200: 26 61 69 64  3D 7A 31 33  73 65 66 78  69 75 75 6E
0x00000210: 73 65 66 78  72 79 30 34  63 6A 6C 68  71 63 7A 72
0x00000220: 67 66 68 34  62 35 31 6B  A1 11 D5 03  05 06 0E 07
0x00000230: 0F 10 0B 12  0C 5F 10 34  68 74 74 70  73 3A 2F 2F
0x00000240: 70 6C 75 73  2E 67 6F 6F  67 6C 65 2E  63 6F 6D 2F
0x00000250: 61 70 70 2F  70 6C 75 73  2F 6F 6F 62  2F 6D 70 2F
0x00000260: 35 37 31 2F  3F 6C 6F 67  69 6E 3D 31  5B 33 36 33
0x00000270: 38 31 30 39  35 33 2E 31  A1 02 D5 03  04 05 06 07
0x00000280: 14 09 15 02  16 5F 10 30  68 74 74 70  73 3A 2F 2F
0x00000290: 70 6C 75 73  2E 67 6F 6F  67 6C 65 2E  63 6F 6D 2F
```

Decoding Hex

Which URLs did you find?

Decoding Hex

Which URLs did you find?

```
https://plus.google.com/app/plus/mp/571/#~loop:view=activity&aid=z13sefxiuunsefxry04cjlhqczrgfh4b51k

https://plus.google.com/app/plus/oob/mp/571/?login=1

https://plus.google.com/app/plus/mp/571/?login=1

https://plus.google.com/app/plus/oob/mp/571/?login=1

https://accounts.google.com/ServiceLoginAuth

https://plus.google.com/app/plus/mp/571/?login=1

http://www.google.com/search?q=gorgonzola&ie=UTF-8&oe=UTF-8&hl=en&client=safari
```

Decoding Hex

What do the URLs indicate?

- These URLs show that Tracy was browsing Google+.
- It's unclear from the browsing history alone, but the repeated visits to the `login` endpoint *may* suggest an attempt to break into an account (as opposed to a single successful login).
- And the final URL indicates that Tracy searched for "Gorgonzola" on Google, using her Safari web browser.

Decoding Hex

How Browsing Data can be used:

- Browsing history, along with timestamps, could provide an alibi for Tracy

- Visiting peoples' Google+ profiles proves Tracy is in contact with them.
  - This can be used as evidence that she knows someone she claims not to or to prove a link to another party in the investigation— a common objective when building conspiracy cases.

- Browsing history provides clues as to Tracy's interests.
  - Searches related to the crime under investigation can be used as evidence against her.
  - For instance: demonstrating that an individual accused of developing improvised explosives indeed downloaded improvised explosive handbooks is strong evidence against them.

Activity: What was Tracy’s Involvement?

In this activity, you will work in groups to finish documenting their finding and conclusions.

Activities/Stu_Final_Report

Suggested Time:
45 Minutes

Let’s Review: Case Scenario

01 What was Tracy’s Involvement in the case?

02 Who else is a person of interest?

03 What evidence did they gather?

Any Questions?

Class Objectives

By the end of class today, students will be able to:

🟩 Use Autopsy to view and tag evidence from emails.

🟩 Analyze SMS messages offline in Kali Linux.

🟩 Decode hex data in the iPhone image

🟩 Prepare a preliminary report using the *Group Evidence Worksheet*.