ITMS 538 Forensics Analysis Investigation Midterm

My supervisor has personally selected me for a case in a big IT company. The case weapon is not found yet. The suspect seems to have hidden the weapon in a locker. During the search at the suspect's residence, a USB drive and an old coffee-stained scrap of paper was found.

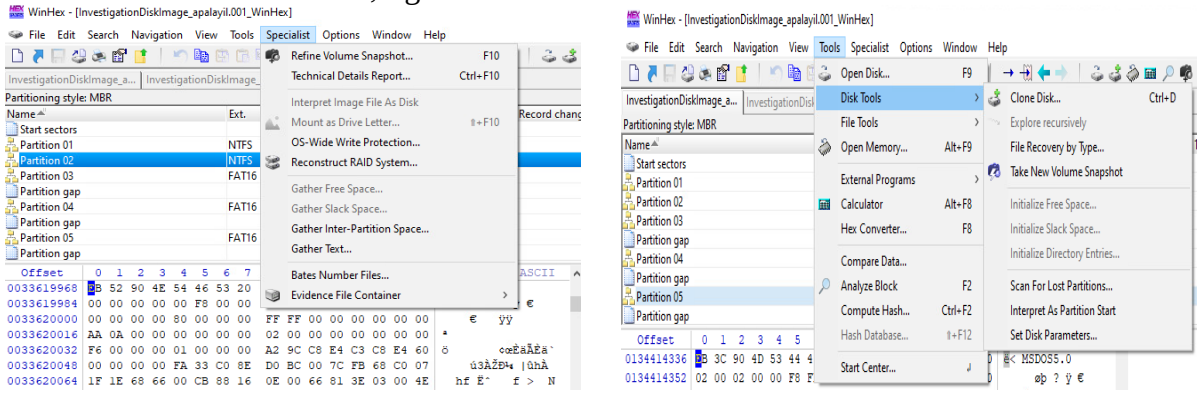
The items are given to me to investigate the case. I first look over the scrap paper and note down the information written over it. From left to right, the paper contained the following information:

- Start Here: P8 (Bootstrap Code) in red circle.
- Key:
  - Format: P <number>; S <number>
  - P -> partition number
  - S -> logical partition sector address
- What Forensics Tools???
  - Autopsy helps some, too
  - WinHex testdisk
- Idea… use FAT partition Boot Sector
  - https://www.ntfs.com/fat-partition-sector.html
- RGB color mapping stuff…
  - https://www.rapidtables.com/web/color/RGB_Color.html
  - https://colors.dopey.top/color-pedia/
- Partition #s can differ/use…
  - ~~testdisk~~
  - ~~Autopsy~~
  - WinHex
  - ~~mmls~~
  - ~~FTK Imager~~

After viewing the paper, I connected the USB drive and created a forensic copy of the drive to work on.

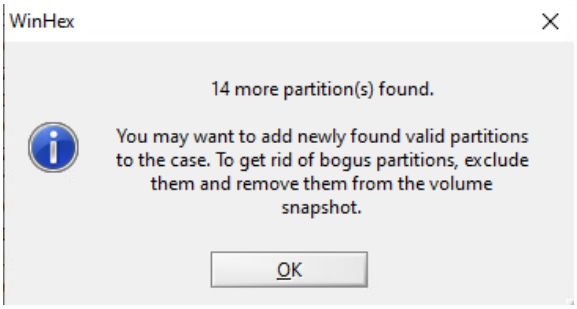
The forensic copy is created to my folder, and it contains the disk raw image. I start my investigation by opening the raw disk image in WinHex and click 'Interpret as a Disk' under the Specialist Menu.

WinHex shows the viewable partitions. While looking over the partitions, I see that the partition numbers are discontinuous. So, I go to the Tools Menu> Disk Tools> 'Scan for Lost Partitions'.



Menu Options.

Fourteen partitions were found in WinHex.



Partition(s) found

In the new partitions, Partition 8 is included. Since the scrap paper contained P8, I look over the ANSI ASCII of Partition 8.

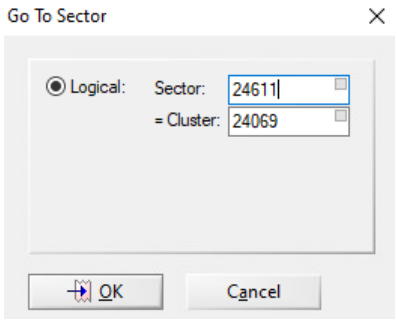
InvestigationDiskImage_a... | InvestigationDiskImage_a... | InvestigationDiskImage_a...

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	EB	3C	90	4D	53	44	4F	53	35	2E	30	00	02	01	04	00	ë< MSDOS5.0
00000016	02	00	02	00	00	F8	FE	00	3F	00	FF	00	80	00	00	00	øþ ? ÿ €
00000032	00	00	01	00	80	00	29	D1	2E	84	9E	50	38	3B	20	53	€)Ñ.„žP8; S
00000048	32	34	36	31	31	20	46	41	54	31	36	20	20	20	20	20	24611 FAT16
00000064	20	20	50	35	3B	20	53	35	35	39	33	35	20	20	20	20	P5; S55935
00000080	38	4E	24	7D	24	8B	C1	99	E8	3C	01	72	1C	83	EB	3A	8N$}$‹Á™è< r ƒë:
00000096	66	A1	1C	7C	26	66	3B	07	26	8A	57	FC	75	06	80	CA	f¡ |&f; &ŠWüu €Ê
00000112	02	88	56	02	80	C3	10	73	EB	33	C9	8A	46	10	98	F7	ˆV €Ã së3ÉŠF ˜÷
00000128	66	16	03	46	1C	13	56	1E	03	46	0E	13	D1	8B	76	11	f F V F Ñ‹v
00000144	60	89	46	FC	89	56	FE	B8	20	00	F7	E6	8B	5E	0B	03	`‰Fü‰Vþ¸ ÷æ‹^
00000160	C3	48	F7	F3	01	46	FC	11	4E	FE	61	BF	00	00	E8	E6	ÃH÷ó Fü Nþa¿ èæ
00000176	00	72	39	26	38	2D	74	17	60	B1	0B	BE	A1	7D	F3	A6	r9&8-t `± ¾¡}ó¦
00000192	61	74	32	4E	74	09	83	C7	20	3B	FB	72	E6	EB	DC	A0	at2Nt ƒÇ ;ûræëÜ
00000208	FB	7D	B4	7D	8B	F0	AC	98	40	74	0C	48	74	13	B4	0E	û}´}‹ð¬˜@t Ht ´
00000224	BB	07	00	CD	10	EB	EF	A0	FD	7D	EB	E6	A0	FC	7D	EB	» Í ëï ý}ëæ ü}ë
00000240	E1	CD	16	CD	19	26	8B	55	1A	52	B0	01	BB	00	00	E8	áÍ Í &‹U R° » è
00000256	3B	00	72	E8	5B	8A	56	24	BE	0B	7C	8B	FC	C7	46	F0	; rè[ŠV$¾ |‹üÇFð
00000272	3D	7D	C7	46	F4	29	7D	8C	D9	89	4E	F2	89	4E	F6	C6	=}ÇFô)}ŒÙ‰Nò‰NöÆ
00000288	06	96	7D	CB	EA	03	00	00	20	0F	B6	C8	66	8B	46	F8	–}Ëê ¶Èf‹Fø
00000304	66	03	46	1C	66	8B	D0	66	C1	EA	10	EB	5E	0F	B6	C8	f F f‹ÐfÁê ë^ ¶È
00000320	4A	4A	8A	46	0D	32	E4	F7	E2	03	46	FC	13	56	FE	EB	JJŠF 2ä÷â Fü Vþë
00000336	4A	52	50	06	53	6A	01	6A	10	91	8B	46	18	96	92	33	JRP Sj j ‘‹F –’3
00000352	D2	F7	F6	91	F7	F6	42	87	CA	F7	76	1A	8A	F2	8A	E8	Ò÷ö‘÷öB‡Ê÷v ŠòŠè
00000368	C0	CC	02	0A	CC	B8	01	02	80	7E	02	0E	75	04	B4	42	ÀÌ Ì¸ €~ u ´B
00000384	8B	F4	8A	56	24	CD	13	61	61	72	0B	40	75	01	42	03	‹ôŠV$Í aar @u B
00000400	5E	0B	49	75	06	F8	C3	41	BB	00	00	60	66	6A	00	EB	^ Iu øÃA» `fj ë
00000416	B0	42	4F	4F	54	4D	47	52	20	20	20	20	0D	0A	52	65	°BOOTMGR Re
00000432	6D	6F	76	65	20	64	69	73	6B	73	20	6F	72	20	6F	74	move disks or ot
00000448	68	65	72	20	6D	65	64	69	61	2E	FF	0D	0A	44	69	73	her media.ÿ Dis
00000464	6B	20	65	72	72	6F	72	FF	0D	0A	50	72	65	73	73	20	k errorÿ Press
00000480	61	6E	79	20	6B	65	79	20	74	6F	20	72	65	73	74	61	any key to resta
00000496	72	74	0D	0A	00	00	00	00	00	00	00	AC	CB	D8	55	AA	rt ¬ËØUª
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Partition 8 ANSI ASCII

While going over the ANSI ASCII, I see something which is like ‘the Key’ in the paper. P8; S24611 and P5; S55935.

I have got two LBA addresses, one in Partition 8 and the other in Partition 5. I start with Partition 8 and click on the left-hand bottom corner to go to specific sector (24611).



Go To Sector

I am then shown an RGB value in the ANSI window:

```
12600928 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12600944 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12600960 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12600976 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12600992 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12601008 | 00 00 52 47 42 3A 20 23  44 38 42 46 44 38 00 00    RGB: #D8BFD8
12601024 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12601040 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
12601056 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Partition 8 RGB value.

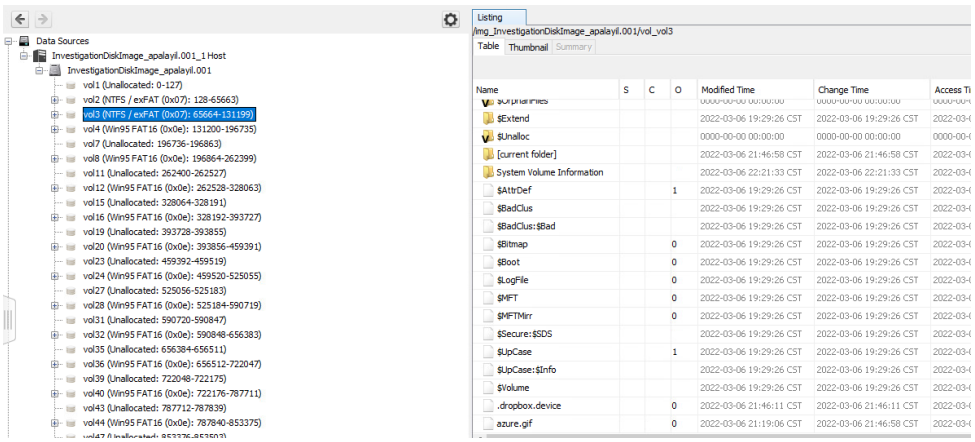
Using the URL from the scrap paper, I search the value I got the name ‘Thistle’ and after which I look over the sector in Partition 5. Going over the same steps above, I am shown another RGB value in the ANSI window:

```
28638816 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638832 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638848 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638864 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638880 | 00 52 47 42 3A 20 23 41  30 35 32 32 44 00 00 00   RGB: #A0522D
28638896 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638912 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638928 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638944 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
28638960 | 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Partition 5 RGB value.

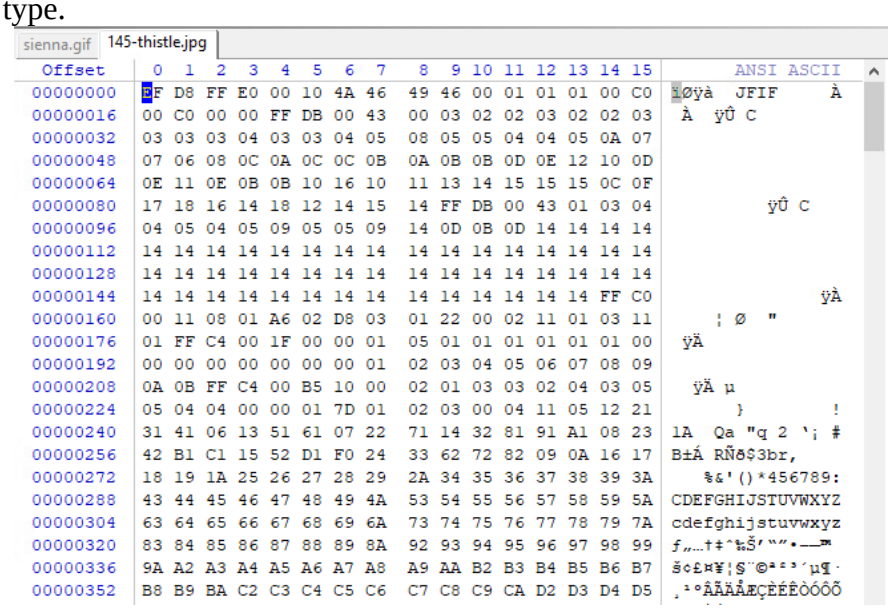
I searched the value in the color mapping URL and get the name ‘Sienna’.

After noting the following data, I open the raw disk image in Autopsy, create a forensic copy with Autopsy. The software sorts the different partitions, file views, and even deleted files. I parsed through the File views and found files named thistle.jpg and sienna.gif, which I extract in my folder. By going over each partition I landed with vol3 (NTFS/ exFAT (0x07): 65664-131199) partition was the location where the files were placed.

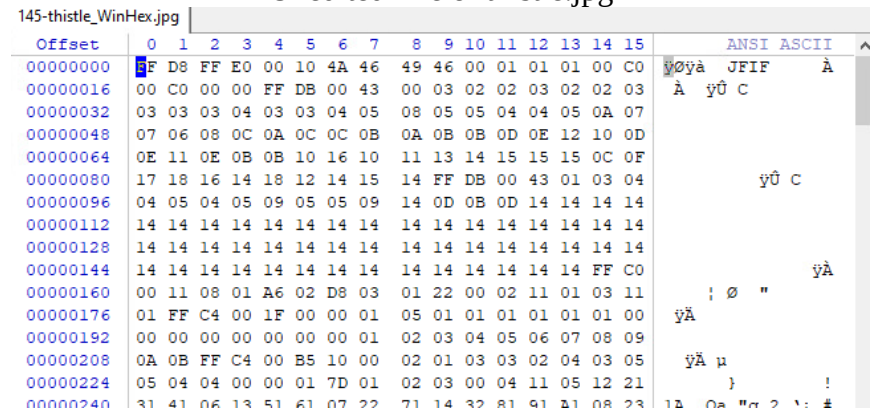


Autopsy disk sortation view with file location

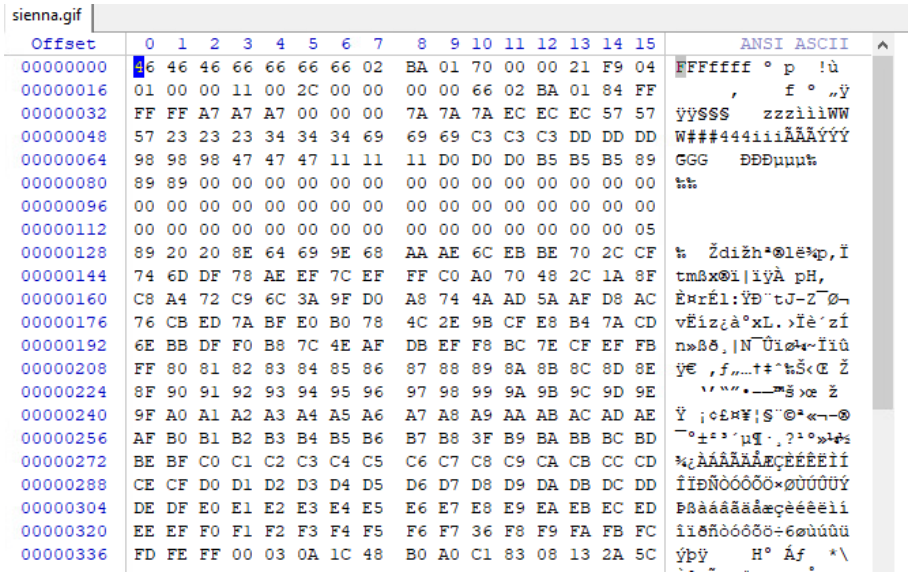
The files are corrupted, so I open them in WinHex and edit the Hex values to match the correct file signature type.



Unedited File of thistle.jpg



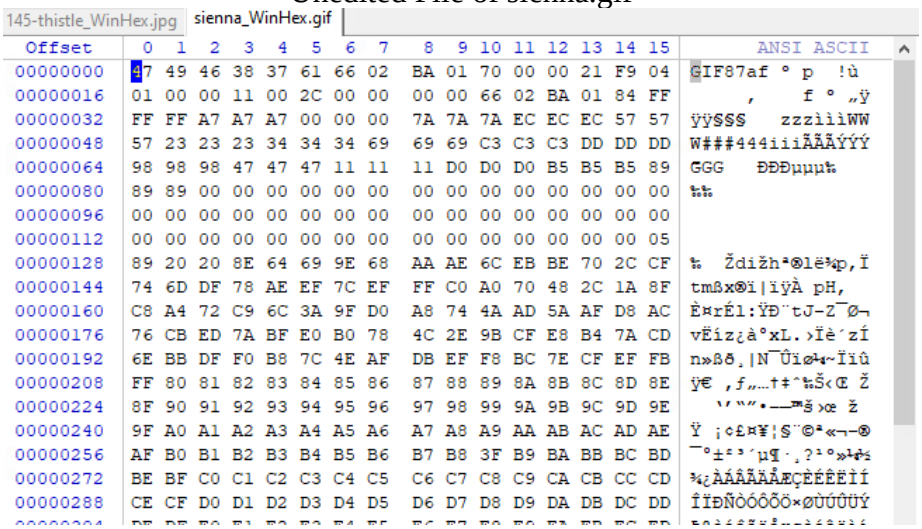
Edited File of thistle.jgp



sienna.gif

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	46	46	46	66	66	66	66	02	BA	01	70	00	00	21	F9	04	FFFffff ° p !ù
00000016	01	00	00	11	00	2C	00	00	00	00	66	02	BA	01	84	FF	, f ° „ÿ
00000032	FF	FF	A7	A7	A7	00	00	00	7A	7A	7A	EC	EC	EC	57	57	ÿÿ§§§ zzzìì WW
00000048	57	23	23	23	34	34	34	69	69	69	C3	C3	C3	DD	DD	DD	W###444iiiÃÃÃÝÝÝ
00000064	98	98	98	47	47	47	11	11	11	D0	D0	D0	B5	B5	B5	89	GGG ÐÐÐµµµ‰
00000080	89	89	00	00	00	00	00	00	00	00	00	00	00	00	00	00	‰‰
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	05	
00000128	89	20	20	8E	64	69	9E	68	AA	AE	6C	EB	BE	70	2C	CF	‰ Ždižh ª®lë¾p,Ï
00000144	74	6D	DF	78	AE	EF	7C	EF	FF	C0	A0	70	48	2C	1A	8F	tmßx®i|ïÿÀ pH,
00000160	C8	A4	72	C9	6C	3A	9F	D0	A8	74	4A	AD	5A	AF	D8	AC	È¤rÉl:ŸÐ¨tJ-Z¯Ø¬
00000176	76	CB	ED	7A	BF	E0	B0	78	4C	2E	9B	CF	E8	B4	7A	CD	vËíz¿à°xL.›Ïè´zÍ
00000192	6E	BB	DF	F0	B8	7C	4E	AF	DB	EF	F8	BC	7E	CF	EF	FB	n»ßð¸|N¯Ûïø¼~Ïïû
00000208	FF	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	ÿ€ ‚ƒ„…†‡ˆ‰Š‹Œ Ž
00000224	8F	90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	‘’“”•–—™š›œ ž
00000240	9F	A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	Ÿ ¡¢£¤¥¦§¨©ª«¬-®
00000256	AF	B0	B1	B2	B3	B4	B5	B6	B7	B8	3F	B9	BA	BB	BC	BD	¯°±²³´µ¶·¸?¹º»¼½
00000272	BE	BF	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍ
00000288	CE	CF	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	ÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝ
00000304	DE	DF	E0	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	EB	EC	ED	Þßàáâãäåæçèéêëìí
00000320	EE	EF	F0	F1	F2	F3	F4	F5	F6	F7	36	F8	F9	FA	FB	FC	îïðñòóôõö÷6øùúûü
00000336	FD	FE	FF	00	03	0A	1C	48	B0	A0	C1	83	08	13	2A	5C	ýþÿ H° Áƒ *\

Unedited File of sienna.gif



145-thistle_WinHex.jpg | sienna_WinHex.gif

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	47	49	46	38	37	61	66	02	BA	01	70	00	00	21	F9	04	GIF87af ° p !ù
00000016	01	00	00	11	00	2C	00	00	00	00	66	02	BA	01	84	FF	, f ° „ÿ
00000032	FF	FF	A7	A7	A7	00	00	00	7A	7A	7A	EC	EC	EC	57	57	ÿÿ§§§ zzzìì WW
00000048	57	23	23	23	34	34	34	69	69	69	C3	C3	C3	DD	DD	DD	W###444iiiÃÃÃÝÝÝ
00000064	98	98	98	47	47	47	11	11	11	D0	D0	D0	B5	B5	B5	89	GGG ÐÐÐµµµ‰
00000080	89	89	00	00	00	00	00	00	00	00	00	00	00	00	00	00	‰‰
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	05	
00000128	89	20	20	8E	64	69	9E	68	AA	AE	6C	EB	BE	70	2C	CF	‰ Ždižh ª®lë¾p,Ï
00000144	74	6D	DF	78	AE	EF	7C	EF	FF	C0	A0	70	48	2C	1A	8F	tmßx®i|ïÿÀ pH,
00000160	C8	A4	72	C9	6C	3A	9F	D0	A8	74	4A	AD	5A	AF	D8	AC	È¤rÉl:ŸÐ¨tJ-Z¯Ø¬
00000176	76	CB	ED	7A	BF	E0	B0	78	4C	2E	9B	CF	E8	B4	7A	CD	vËíz¿à°xL.›Ïè´zÍ
00000192	6E	BB	DF	F0	B8	7C	4E	AF	DB	EF	F8	BC	7E	CF	EF	FB	n»ßð¸|N¯Ûïø¼~Ïïû
00000208	FF	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	ÿ€ ‚ƒ„…†‡ˆ‰Š‹Œ Ž
00000224	8F	90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	‘’“”•–—™š›œ ž
00000240	9F	A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	Ÿ ¡¢£¤¥¦§¨©ª«¬-®
00000256	AF	B0	B1	B2	B3	B4	B5	B6	B7	B8	3F	B9	BA	BB	BC	BD	¯°±²³´µ¶·¸?¹º»¼½
00000272	BE	BF	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	¾¿ÀÁÂÃÄÅÆÇÈÉÊËÌÍ
00000288	CE	CF	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	ÎÏÐÑÒÓÔÕÖ×ØÙÚÛÜÝ

Edited File of sienna.gif

I create a new copy of the following files and view them. The jpg file contains a set of coordinates which I believe is a false lead and dismiss that evidence. The gif file however, contained a combination of 4 numbers which could possibly be the combinations to the locker.

Thus, I presume 58-97-36-17 is the combination to the locker.

I hereby submit my findings and add the attachment of the progress which is logged in the evidence log and the following is the screenshot of my log.
https://docs.google.com/spreadsheets/d/1UR4lTEDEyMyfvpt0Rx9WJ3h_9fN_6LdPthi6dF10GJI/edit?usp=sharing

#	Forensic Evidence	Evidence Description	Evidence Format	Mechanism by Which Forensic Evidence was Discovered	Forenic Tool(s) Used to Discover Evidence	Relationship to Other Evidence	Location of Evidence
Forensic Investigator:		Alan Palayil					
Example	SFF20_PPG.pdf	Sundance 2020 Film Festival Guide	PDF	Found file by browsing using the tree viewer on the left panel under Data Sources	Autopsy, v 4.17.0	No link to evidence from the case as this is an example. Normally, you would explain the link of this evidence to clues or other evidence from the case.	**Path to file:** volume 4/Documents/SomeStuff/Cinema/SFF20_PPG.pdf
1	InvestigationDiskImage_apalayil.001	The raw disk image of the USB Drive	raw disk image	Recovered the disk image through the USB drvie in evidence.	File Explorer	Main evidence to find the 4 number combination to the locker	Path to file: E:\Labs\Midterm Forensic exam\InvestigationDiskImage_apalayil.001
2	InvestigationDiskImage_apalayil_WinHex.001	Created a copy of disk image to work on without damaging the original data.	raw disk image	Forensic copy to go through the contents without damaging the evidence	WinHex	Main evidence to find the 4 number combination to the locker	Path to file: E:\Labs\Midterm Forensic exam\InvestigationDiskImage_apalayil_WinHex.001
3	InvestigationDiskImage_apalayil_Autopsy.001	Created a copy of disk image to work on without damaging the original data.	raw disk image	Forensic copy to go through the contents without damaging the evidence	Autopsy, v 4.17.0	Main evidence to find the 4 number combination to the locker	Path to file: E:\Labs\Midterm Forensic exam\InvestigationDiskImage_apalayilAutopsy.001
4	thistle.jpg	Recovered from Autopsy, and the file is extracted our forensics folder. The file itself is corrupted so we open Winhex to check how the file is corrupted	JPG	Found through the clues in the scrap paper and browsing through the tree viewer on the left panel under Data Sources	Autopsy, v 4.17.0	While cross-checking the RGB value found in Partition 8 of the disk with the color mapping url, the name thistle is recovered and the .jpg file including the same name is found in vol3 of the disk image.	Path to file: /img_InvestigationDiskImage_apalayil_Autopsy.001/vol_vol3/thistle.jpg
5	sienna.gif	Recovered from Autopsy, and the file is extracted our forensics folder. The file itself is corrupted so we open Winhex to check how the file is corrupted	GIF	Found through the clues in the scrap paper and browsing through the tree viewer on the left panel under Data Sources	Autopsy, v 4.17.0	While cross-checking the RGB value found in Partition 5 of the disk with the color mapping url, the name sienna is recovered and the .gif file including the same name is found in vol3 of the disk image.	Path to file: /img_InvestigationDiskImage_apalayil_Autopsy.001/vol_vol3/sienna.gif
6	thistle_WinHex.jpg	Created a copy of disk image to work on without damaging the original data. We correct the file signature using the correct dataset and the file is viewable.	JPG	Forensic copy to edit the file contents without damaging the evidence	WinHex	While browsing through the file in WinHex, I corrected the file signature to make the file viewable	Path to file: E:\Labs\Midterm Forensic exam\Extracted File\thistle_WinHex.jpg
7	sienna_WinHex.gif	Created a copy of disk image to work on without damaging the original data. We correct the file signature using the correct dataset and the file is viewable.	GIF	Forensic copy to edit the file contents without damaging the evidence	WinHex	While browsing through the file in WinHex, I corrected the file signature to make the file viewable	Path to file: E:\Labs\Midterm Forensic exam\Extracted File\sienna_WinHex.gif