Nama : Fitrah Afriana

## NIM : 09021381520055

- 1. Analisa Forensik Image File
  - a. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

🛉 Add Data Source 📠 Images/Vide	os 🔣 Communications 🗧	Timeline 📗 Generate	Report 👩 Close Case 💈			A FID	• Keyword Lists	Q. K	eyword Search
	Show Rejected Results	Usting							( ) <b>v</b>
	Group by Data Source	/ing_mage/\$CarvedFiles Table Thumbnail							3 Resul
Data Sources		Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
SCarvedFiles (3)		/ f0000033.doc	img_mage/\$CarvedFiles/F0000033.doc	0000-00-00-00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00-00	20480	Unallocated
Views		/ f0000073.jpg	/img_image/\$CarvedFiles/f0000073.jpg	0000-00-80 00:00:80	0008-80-00 00:08-00	00:00-00-00 00:00:00	00:00:00 25-00-0000	8754	Unallocated
Results		/ f0000 104.zip	/mg_image/\$CarvedFiles/f0000104.zb	0000-00-00 00:00:00	0000-00-00 00:00:00	00:00:00:00:00:00:00	0000-00-00 00:00:00	2420	Unallocated
Encryption Detected (1)     Keyword Hits     Single Literal Keyword Search	÷ (0)								
Single Literal Keyword Searce     Single Regular Expression S									
	eardings								
Hashset Hits	earchigh	<		_					,
Hashset Hits Hashset Hits Hashse	ea or (a)		Indexed Text Message File Metadata	Lesuits   Other Occurrence					د
Hashset Hits	68 01 (0)			tesuits   Other Occurrenc of 1 Page	25		Text Source:	Vie Text	د ب
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>	68 01 (6)	Hex Strings Acolcate			28		Text Source: 1	Vie Text	د ~ ^
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>		Hex Strings Acolicate Matches on page: -	of - Match 🥧 🔶 Page: 1		28		Text Source: 1	Ne Text	د د
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>		Hex Strings Acolicate Matches on page: - Jianey Jungle	of - Match 🥧 🔶 Page: 1		25		Text Source: 1	%e Text	~
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>	ea un pu	Hex Strings Acolector Matches on page: - Jiamy Jungle 626 Jungle Are Ape 2 Jungle, 57 1111	of - Match 🥧 🔶 Page: 1		26		Text Source: 1	Ne Text	×
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>	ea 01 (97	Hex Strings Accidant Matches on page: - Jianey Jungle 626 Jungle Xre Apr 2 Jungle, SY 11111 Jianey:	of · Match <u>· </u> Page: 1	of 1 Page  🔶					3
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>	ea 01 (97	Hex Strings Accelerate Matches on page: - Jimmy Jungle 626 Jungle Are Apro 2 Jungle, MY 11111 Jimmy: Dude, pour pot mast	of - Match - Page: 1	of 1 Page ( )	anis for sending me t	the Cover Page. What			au plans the
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>		Hex Stings Accelerate Matches on page: - Jimmy Jungle 426 Jungle Are Apro 2 Jungle, SY 11111 Jimmy: Dude, your pot must matiguana seed? Ab	of - Match Pager 1	of 1 Page ( )	ants for sending set	are glad you told me	do you put in your +	oil when y	1 students.
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>		Hex Strings Acolomb Matches on page: - Jiamy Jungie 626 Jungie Ave App 3 Jungie, NY 11111 Jiamy; Dude, your pot mast matigiams seed? Ja These kids, they well	of - Match <u>e</u>	af 1 Page	ants for sending set	are glad you told me	do you put in your +	oil when y	1 students.
<ul> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>Interesting Items</li> <li>Accounts</li> <li>Tags</li> </ul>		Hex Strings Acclosus Matches on page: - Jumy Jungle 626 Jungle Are Aps 2 Jungle, NY 11111 Jungs, SY 11111 Jungs, Dude, your pet mark marijunan seeddr Ta	of - Match - Pager 1 In the base - is and/or the cross of Page Institution and the cross of Page Institutions and we determine how the guarantee and pagestance. Triv Inte guarantee and the guarantee and pagestance.	of 1 Page () h Times Magazine! Th rome guy in Columbia y don's trob buying heck. Their parents a year!	anks for sending so t from no. Ham, I'm so give then money for 1	are glad you told me lunch and they spend	do you put in your * about tangeting the it on my stuff. I'm	oil when y high schoo an entrepr	1 students. eneur. Am I

Joe Jacob's supplier of marijuana is **Jimmy Jugle**. And then the address listed for the supplier in **626 Jungle Ave Apt 2 Jungle**, **NY 11111**. The information is obtained in the file **f0000033.doc** 

b. What crucial data is available within the coverpage.jpg file and why is this data crucial?

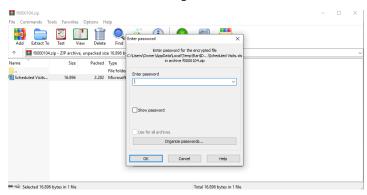
🕂 Add Data Source 📠 Images/Vid	eos 🔣 Communications 🧮	Timeline 💧 Generate Report	🐞 Close Case 🗧			<u> </u>	Keyword Lists	Qr Keyn	ord Search
	Show Rejected Results	Listing							+ + = =
€ →	Group by Data Source	/mg_mage Table Thumbnail							2 Result
Data Sources		Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
I Vess		y Unalloc_1_0_1474559	Amg_mage/Unalloc_1_0_1474559	0000-06-00.00:00:00	0000-00-00 00-00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1474560	Unelocated
Results     Extracted Content		CarvedFiles	/img_kvage/@CarvedFiles	0000-00-00-00:00:00	0000-00-00-00:00:00	00:00:00-00-00:00:00	0000-00-00-00:00:00	0	Allocated
Hashset Hits     E-Mail Messages     Interesting Items     Accounts		¢ Hex Strings Application Indi	exed Text Mossings - Nie Metadata - No	ulta   Other Occurrences					
Tags Reports		Matches on page: - of	and the second second second	1 Page 🗧 🔿			Text Source: File	Text	~
		702200 2192 2192 2194 2194 2194 2194 2194 2194							Î
		.*b8 \05**F07							

Crucial data is available within the **coverpage.jpg** file is password "**pw=goodtimes**", which was inserted by the suspect. This data crucial, because open could the locked **f0000104**.zip

c. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?



## extract the file **f0000104.zip**



From the file Scheduled visits.xls which is extracted from the f0000104.zip.

File How	e Insert Pay	pe Layout Formulas Data Revie	w View Add-Ins	Team										۵ 🕜	
Cut	Arial	- 10 - A A = = =		Gene		٠		]	-	<b>*</b>	Σ Auto	2	<b>7</b> A		
ste J Form	t Painter B Z	Ū· ⊞· ≜·Δ· ≡≡≡	谭 律 🔚 Merge & Cen	ler • 📑 •	% , 3	1.23	Conditional For Formatting * as Ta	nat Cell hie • Styles •	insert	Delete Forma	t Q Clea	·	ter * Select *		
Clipboard	6	Font G	Alignment	6	Number	ra i	Styles			Cells		Editio			
850	+ (n	fx Monday (1)													
A	В	C	D	E	F	G	н	1	J	K	L	М	N	0	
Month	DAY	HIGH SCHOOLS													
2003															
April	Monday (1)	Smith Hill High School (A)													
	Tuesday (2)	Key High School (B)													
	Wednesday (3)	Leetch High School (C)													
	Thursday (4)	Birard High School (D)													
	Friday (5)	Richter High School (E)													
	Monday (1)	Hull High School (F)													
	Tuesday (2)	Smith Hill High School (A)													
	Wednesday (3)	Key High School (B)													
	Thursday (4)	Leetch High School (C)													
	Friday (5)	Birard High School (D)													
	Monday (1)	Richter High School (E)													
	Tuesday (2)	Hull High School (F)													
	Wednesday (3)	Smith Hill High School (A)													
	Thursday (4)	Key High School (B)													
	Friday (5)	Leetch High School (C)													
	Monday (1)	Birard High School (D)													
	Tuesday (2)	Richter High School (E)													
	Wednesday (3)	Hull High School (F)													
	Thursday (4)	Smith Hill High School (A)													
	Friday (5)	Key High School (B)													
	Monday (1)	Leetch High School (C)													
	Tuesday (2)	Birard High School (D)													
May															
	Wednesday (3)	Richter High School (E)													
	Thursday (4)	Hull High School (F)													
	Friday (5)	Smith Hill High School (A)													
	Monday (1)	Key High School (B)													
	Tuesday (2)	Leetch High School (C)					0.4								

File Hor			eview View Add-Ins Tear									Σ AutoSum	- A	۵ 🕜	n @ 1
Cop	Arial	- 10 - A' A' = =	🕳 🐎 🔤 Wrap Text	Gene	al	٧			🔏 i 🗄	i 👬 🖷		Fill *	77 🖓		
Paste J Form		፱ •   ⊞ •   🎰 • 🚣 • 🔳 🗃	🗃 🗊 🗊 📷 Merge & Center -	<b>9</b> -	%, 3	: -3	Conditional Formatting * a	Format C	iell Ir les -	isert Delete P	ormat	2 Clear *	Sort & Find & Filter * Select *		
Clipboard		Font G	Alignment		Number		St	yles		Cells		E.	siting		
B50	- (*	fx Monday (1)													
	В	С	D	E	F	0	B H	1	J	K	1	. M	N	0	PC
25 May															-
36	Wednesday (3)	Richter High School (E)													
27	Thursday (4)	Hull High School (F)													
28 29 30	Friday (5)	Smith Hill High School (A)													
29	Monday (1)	Key High School (B)													
30	Tuesday (2)	Leetch High School (C)													
31	Wednesday (3)	Birard High School (D)													
12 13 14 15 16 17 18 19 10	Thursday (4)	Richter High School (E)													
33	Friday (5)	Hull High School (F)													
34	Monday (1)	Smith Hill High School (A)													
85	Tuesday (2)	Key High School (B)													
36	Wednesday (3)	Leetch High School (C)													
37	Thursday (4)	Birard High School (D)													
38	Friday (5)	Richter High School (E)													
9	Monday (1)	Hull High School (F)													
10	Tuesday (2)	Smith Hill High School (A)													
11	Wednesday (3)	Key High School (B)													
12 13 14	Thursday (4)	Leetch High School (C)													
13	Fridary (5)	Birard High School (D)													
14	Monday (1)	Richter High School (E)													
15	Tuesday (2)	Hull High School (F)													
46	Wednesday (3)	Smith Hill High School (A)													
17	Thursday (4)	Key High School (B)													
18	Friday (5)	Leetch High School (C)													
June 9															
50	Monday (1)	Birard High School (D)													
51	Tuesday (2)	Richter High School (E)													
2	Wednesday (3)	Hull High School (F)													
52 53	Thursday (4)	Smith Hill High School (A)													
54	Friday (5)	Key High School (B)													

	nac Painter	$-10 - A^* A^* \equiv =$ $\underline{u} + \underline{u} + \underline{b} + \underline{A} + \underline{c} \equiv \equiv \equiv$ Fort	参・ III Wrap Text 連律 III Menge & Center・				Conditional Form Formatting * as Tabl	at Cell le • Styles •	Insert	Delete Format	Σ AutoSum = 2 Fill = 2 Clear =	Sort & Find & Filter * Select *		
Clipboard B50	• G	fort 5	Alignment 6		Number	- 6	Styles			Cells	Ee	eng		_
	B	C C	D			0	н				L M	N	0	P
A 6	Tuesday (2)	Smith Hill High School (A)	D	E	P	0	s M		J	K	L M	N	0	P
1	Wednesday (2)	Key High School (B)												
2	Thursday (3)	Leetch High School (C)												
3	Friday (5)	Birard High School (D)												
4	Monday (1)	Richter High School (E)												
5	Tuesday (2)	Hull High School (F)												
6	Wednesday (2)	Smith Hill High School (A)												
7	Thursday (4)	Key High School (B)												
8	Friday (6)	Leetch High School (C)												
9 June	r noay (o)	Leeton riigh School (C)												
Julie	Monday (1)	Birard High School (D)												
1	Tuesday (2)	Richter High School (E)												
2	Wednesday (3)	Hull High School (F)												
3	Thursday (4)	Smith Hill High School (A)												
4	Friday (5)	Key High School (B)												
4	Monday (1)	Leetch High School (C)												
6	Tuesday (2)	Birard High School (D)												
6	Wednesday (3)	Richter High School (E)												
8	Thursday (4)	Hull High School (F)												
9	Friday (5)	Smith Hill High School (A)												
9	Monday (1)	Key High School (B)												
1	Tuesday (2)	Leetch High School (C)												
2	Wednesday (3)	Birard High School (D)												
3	Thursday (4)	Richter High School (E)												
1	Friday (5)	Hull High School (F)												
5	Monday (1)	Smith Hill High School (A)												
5	Tuesday (2)	Key High School (B)												
7	Wednesday (3)	Leetch High School (C)												
8	Thursday (4)	Birard High School (D)												
0	Friday (5)	Richter High School (E)												

There are other 5 High Schools that Jacobs visits frequently, aside from Smith Hill High School, they are:

- Briard High School
- Richter High School
- Hull High School
- Key High School
- Leetch High School
- d. For each file, what processes were taken by the suspect to mask them from others?
  - Cover Page.jpg : The suspect simply change the file extension from .jpg to .jpgc
  - F0000033.doc : The suspect have deleted this file
  - Scheduled Visits.exe : The suspect simply change the file extension from .zip to .exe. The file is protected with a password
- e. What processes did you (the investigator) use to successfully examine the entire contents of each file?
  - Mount the image file to Autopsy 4.8.0. for the examination.
  - Add to Disk Image / VM File category.
  - There are 3 files: cover page.jpgc, Jimmy Jugle.doc, Scheduled Visits.exe.
  - checked the files for find instructions and find instructions [The supplier's] name for question number 1.
  - Looking for clues **Crucial data** for answering question number 2, immediately check the f0000073.jpg which is the Coverpage.jpg, but I am not another find anything.

- Then looking **Another High School** for question number 3. I used file called **f0000104.zip** which a **Scheduled Visit File**. But, because autopsy can't see through the zip file, export file .zip to my Desktop for further inspection.
- After exported it, the zip file requested a password. I used a **password : goodtimes** that I got earlier to unlock the zip file.
- I can access the hidden file is **ScheduledVisits.xls**, and then see what's inside it.
- Evidently, it the location of the sale of marijuana.

**img\_3.jpg** was real image. Taken with Apple iPhone 8 Plues camera at date 2018:10:11 and time 21:50:08.

· • • • •	🔁 Timeline 👔 Generate Report 🍙 🤅	Dose Case is			<u>▲</u> <sup>63</sup> ⊙ •	Keyword Lists	Qr Keyword	Search
Deta Sources     J.PG		Location	Modified Time	Change Time 0000-00-00 00:00:00	Access Time 0000-00-00 00:00:00	Created Time	Size	1 Read
	K Hex Stangs Application It Matches on page: - of	ndexed Text Pressor File Metadata - Match 🔄 🏓 Page: 1	Results: Other Occurrent of 1 Page 🗲 🔶			Text Source: File Te	ext	~
ing Top ≟ Repris	Head Mode Preventing CC 2013 Mode 1 Hardwar, SR Hardwar, SR Hardwar, Hardwar, Hardwa	(Mindowa)2010:10:12 10:08:04						^

**img\_4.jpg** was fake image. Because the image was edited with Adobe Photoshop CC 2018 (Windows) at date 2018:10:12 and time 18:28:36.

## 2. Analisa Forensik Gambar / Foto