#JonSecOps

Recovery and Analysis of Digital Images Using EXIF Metadata for Case Investigations

`

Background

Mr. McBride is the senior forensic examiner in the NYPD crime laboratory. A joint task force has been assembled to stop a suspected human trafficking ring. Officers have had little to go on to this point, but they were able to intercept a courier who was carrying an envelope. Inside the envelope was a 1GB Kexin USB thumb drive. An evidence technician imaged the device but could only locate a large block of data marked as “Unallocated”. Officers on the task force intercepted a JPG image from the suspected leader of the trafficking organization and have MD5 hashed the file (DAD6451BCDD7259156915746F147D644). If Mr. McBride is able to match this hash value with an item from the USB device the officers can then definitively link the device used to take the picture with other photos in the case. The case has been forwarded to Mr. McBride based on his experience as an examiner.

Request

Mr. McBride is requested to identify if the image of interest is found on the USB drive image. Carve for image files and recover any important metadata relevant to the investigation. Attempt to locate the suspect’s hideout (provide a physical address) and what camera was used to take the pictures.

Summary of Findings

During the investigation, files within the drive were carved using tools such as Scalpel and Foremost. With further investigation the JPG file with the MD5 Hash Value (DAD6451BCDD7259156915746F147D644) was discovered. Also, a hidden RTF file was discovered and opened in LibreOffice with the message: My hideout is in the brownstone in the city next to the pizza shop. Exchangeable Image File data was taken from all JPG and PNG image files. Information such as the JPG/PNG files date/time, latitude/longitude, make/model of the phone used and physical address of images taken were investigated.

`

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Carving and Metadata.zip	C18584e409cbe1c3e8d2cbbfa1c57cf
Evidence Created	Working Copy	CarvMetCOPY.zip	C18584e409cbe1c3e8d2cbbfa1c57cf
Evidence Examined	Working Copy	USB.001	945115187a6dd7c5c5e63d85bbae9af15d
Evidence Examined	Working Copy	USB.001.txt	01cad14a2914e7a54f1abfb9573c9c2f
Supplemental Material	Script Log 1	McBrideLAB3.txt	Cd0c8d77038d94407b39297b39297b02fd2e9b
Supplemental Material	Script Log 2	McBrideLAB3CONT.txt	DE04FC78031CDE32590F3FE5F125DAB3

Table 1: Case evidence items

Collection and Analysis

Collection

The 1GB Kexin USB thumb drive was given to the examiner from the NYPD task force for investigation. The USB file for investigation was named Carving and Metadata.zip. Immediately this file was hashed using the hashdeep command in Ubuntu by the examiner for evidence preservation purposes. This file was then copied using the cp command in Ubuntu and named CarvMetCopy.zip. The CarvMetCopy zip file was then hashed to ensure that it was a legitimate copy of the original file. The copied file was then unzipped and revealed 2 files called USB.001 and USB.001.txt.

`

Analysis

The USB.001 and USB.001.txt files were then carved by reconfiguring the scalpel tool to allow for jpg and png images to be investigated and sent to the Scapel_Results folder for results. Once this was done , the

Scalpel_Results folder was investigated and revealed a file called jpg-1-0. This folder revealed JPG images. No PNG files were found in the Scalpel_Results folder. JPG image 00000014 was the only image that was visible in the folder. All other images were non-visible. The JPG image files were then hashed using the hashdeep command revealing there MD5 Hash value displayed in FIGURE1.

FIGURE : 1
Scalpel Carved Files With MD5 Hash Values

Date / Time	Scalpel_Results/jpg-1-0 Folder	MD5 Hash Value
n/a	00000000.jpg	A4127fcc08eb3d3c4e36771e798d30c
n/a	00000001.jpg	Fbad09697c842d202f86be1e94f2a139
n/a	00000002.jpg	C4001bc08dce20c861ef6ddba74e66a
n/a	00000003.jpg	C689c1a7460ecbda2ffa2cdd9c76a7a7
n/a	00000004.jpg	561fb059b1cf479defd090b94bed6bb2
n/a	00000005.jpg	Eb14bc169b280e2edb06a7239fd7d9f5
n/a	00000006.jpg	38b7daef9cb0ddb5253b46229c2dc754
n/a	00000007.jpg	E439479ce545b66a076ad7b16ddbd30e
n/a	00000008.jpg	44b63c2efd4bd0c7a7e547274b565860
n/a	00000009.jpg	Dff493554a7148294f8f82d4aa2ccb15
n/a	00000010.jpg	Ccbeecaa82df536cbf06a89a970cee24
n/a	00000011.jpg	78ed5f13376382e16d179c2a385115f8

`

n/a	00000012.jpg	36c1007b6ab204d913179055335e532f
n/a	00000013.jpg	09d99792746f5cf680e762cf432b7cdb
10/30/2016 / 15:34:25	00000014.jpg	1e4f7a31e4146ba8e5eb3724e5c8c5c7
n/a	00000015.jpg	61ec6878f63e7f01351f269a4110970e
n/a	00000016.jpg	6a31688288b4a7a28dcb7fa9829dfabc
n/a	Audit.txt	
n/a	**Scalpel RTF File**	**MD5 Hash Value**
	00000000.rtf	3a553e6c466cb5083536b2b122383995

The foremost tool was also used for carving which revealed not only JPG image files but PNG image files. All JPG and PNG files were then hashed immediately using the hashdeep command for there MD5 hash value. The hash results of these files are displayed in FIGURE2. While using the hashdeep command against the JPG and PNG files, the hashdeep value of the intercepted suspect file was revealed in the 00170349.jpg file. This is displayed in bold red letters in FIGURE2.

FIGURE2:
Foremost Carved Files With MD5 Hash Values

Date / Time	**Foremost_Results2/jpg Folder**	**MD5 Hash Value**
9/4/2015 / 15:46:27	00136712.jpg	F256f4447a0e86c9dae2ec52de43eb54
9/9/2015 / 10:08:37	00144625.jpg	F212e085d463eca37682f4935890a87e
9/11/2015 / 20:21:00	00151376.jpg	440e46bdc49d1299b02e5637d5a942e8
9/11/2015 / 21:41:55	00161845.jpg	E88f20e39a4f68as5fe4d2cbc715ce92
10/04/2015 / 14:02:48	**00170349.jpg**	**Dad6451bcdd7259156915746f147d644**
12/18/2015 / 13:52:58	00180878.jpg	F74cd334296272aa3243d2a19079e466
12/18/2015 /	001090378.jpg	0170442ca20503cf835da88684e962c4

`

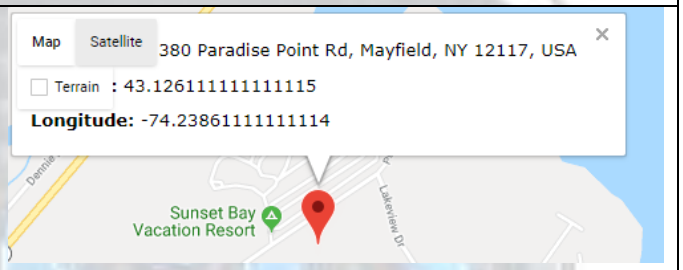
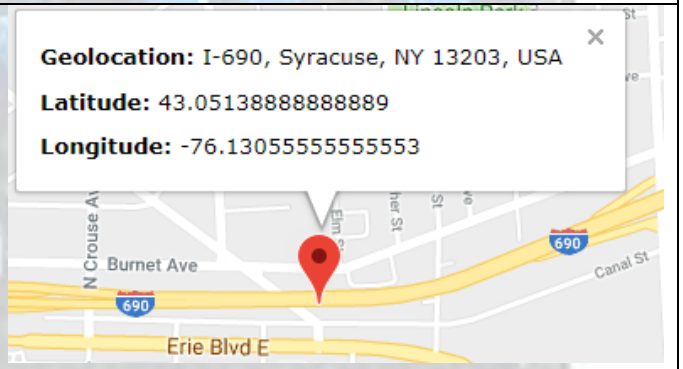
14:25:49		
12/18/15 / 17:00:24	00197902.jpg	A0c1833dbab60764e18d40347d54d319
12/18/15 / 18:29:12	00207218.jpg	9f60cccda6a441099c36bee25371f65e
12/18/15 / 19:52:08	00216857.jpg	B00cabc26047ce859291a774c92b573f
12/18/15 / 20:03:41	00229788.jpg	5d9dc734de5178466a13bffeb6041ddc
8/30/16 / 19:02:31	00235479.jpg	Dd883bd41e930ca504f533640256e10c
10/15/16 / 17:53:27	00243966.jpg	Dd5055faa8a6eca2d815d03cdd8f32ac
10:30:16 / 13:38:02	00252612.jpg	D97d89bobc7ef9fc18b0efd1694b53f0
10/30/16 / 15:34:25	00258705.jpg	1e4f7a31e4146ba8e5eb3724e5c8c5c7
10/30/16 / 15:50:30	00263177.jpg	761c9d2022372b3f5386c968a25c954c
11/19/16 / 16:26:56	00328938.jpg	93ee83d7b0e87fe327e7a88aab7ba540
	Foremost_Results2/png folder	**MD5 Hash Value**
n/a	00001064.png	7cc4ab82f1ec1b030d12da33f8240cec
n/a	00001210.png	1fe44e843bc97001659b5186bac907bf
n/a	00001316.png	7cc4ab82f1ec1b030d12da33f8240cec
n/a	00216812.png	772a1cb1f11b0c81a665c7d921e3af4
	Audit.txt	820752e3f130f44719f0a8401423575a6

The images in both the Scalpel_Results folder and Foremost_Results2 folder where further investigated using the ImageMagick tool. This tool is used using the identify command which reveals exif type information for all image files. Exif information such as date/time, latitude/longitude, and the make/model of camera was obtained. The GPS latitude/longitude information was used to get physical address locations as well as display these locations in chronological date order of when the suspect took the pictures when using their phone. The date/time, latitude/longitude file information is displayed in FIGURE 3. The phones make and model information is displayed in both FIGURE 4 and FIGURE 5.

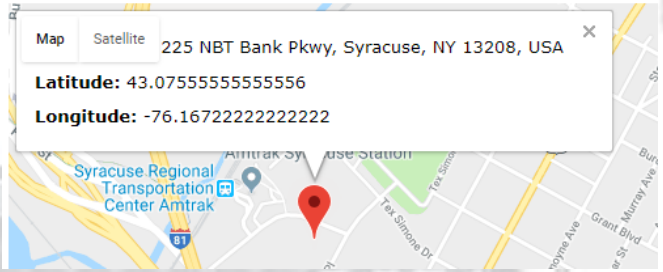
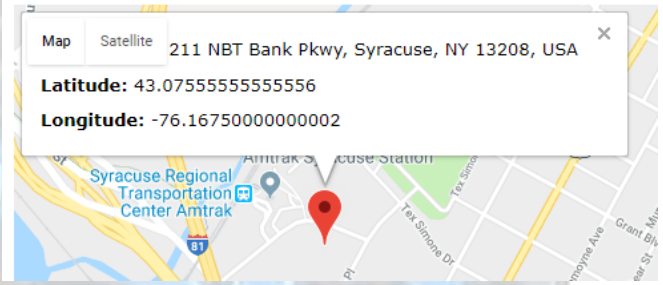
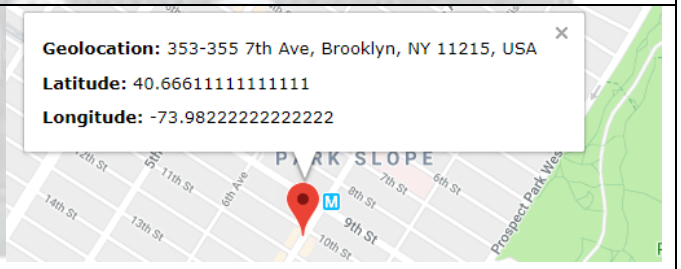
FIGURE3:

Suspects Physical Location In Chronological Order Using Latitude & Longitude Coordinates from Images Captured

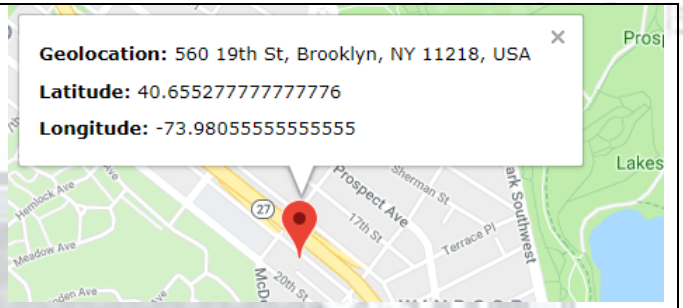
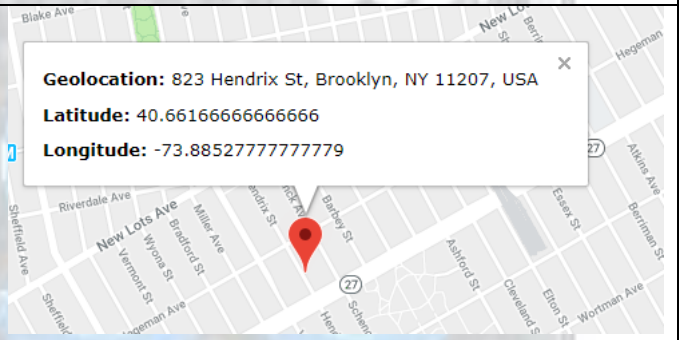
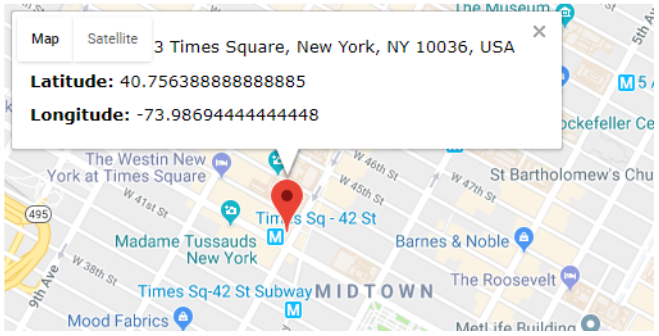
`

Scalpel_Results/ jpg-1-0 Folder	Foremost_Results2/jpg Folder	Date / Time	Map Image and Physical Address Of Longitude and Latitude Coordinates
	00136712.jpg 	9/4/2015 / 15:46:27	 **LAT**- 43/1, 7/1, 34/1 N, **LONG**- 75/1, 14/1, 19/1 W
	00144625.jpg 	9/9/2015 / 10:08:37	 **LAT** – 43/1, 3/1, 5/1 N **LONG**- 76/1, 7/1, 50/1 W

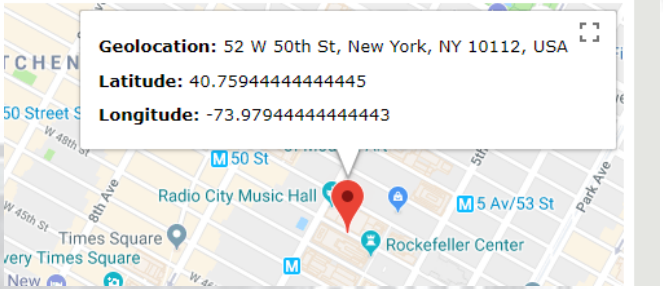
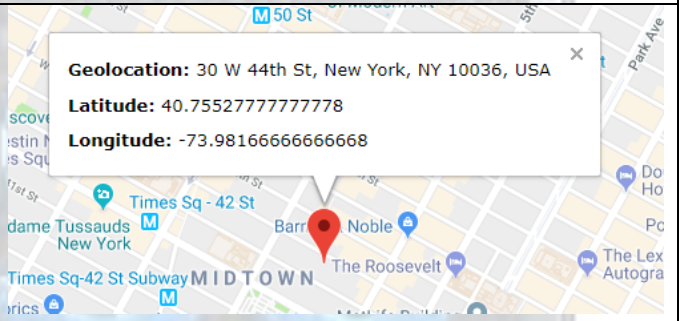
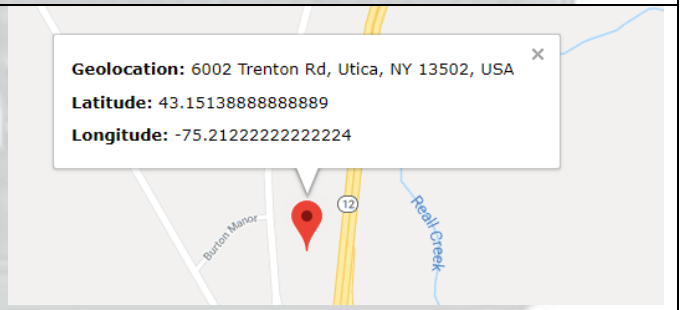
`

	00151376.jpg 	9/11/2015 / 20:21:00	 **LAT** 43/1, 4/1, 32/1 N **LONG**- 76/1, 10/1, 2/1 W
	00161845.jpg 	9/11/2015 / 21:41:55	 **LAT** 43/1, 4/1, 32/1 N **LONG** 76/1, 10/1, 3/1, W
	00170349.jpg 	**10/04/2015 / 14:02:48**	**N/A**
	00180878.jpg 	12/18/2015 / 13:52:58	 **LAT** 40/1, 39/1, 58/1 N **LONG** 73/1, 58/1, 56/1 W

`

	001090378.jpg 	12/18/2015 / 14:25:49	 **LAT** 40/1, 39/1, 19/1 N **LONG** 73/1, 55/1, 50 W
	00197902.jpg 	12/18/15 / 17:00:24	 **LAT** 40/1, 39/1, 42/1 N **LONG** 73/1, 53/1, 7/1 W
	00207218.jpg 	12/18/15 / 18:29:12	 **LAT** 40/1, 45/1, 23/1 N **LONG** 73/1, 59/1, 13/1W

`

	00216857.jpg 	12/18/15 / 19:52:08	 **LAT** 40/1, 45/1, 34/1 N **LONG** 73/1, 58/1, 46/1
	00229788.jpg 	12/18/15 / 20:03:41	 **LAT** 40/1, 45/1, 19/1 N **LONG** 73/1, 58/1, 54/1 W
	00235479.jpg 	8/30/16 / 19:02:31	 **LAT** 43/1, 9/1, 5/1 N **LONG** 75/1, 12/1, 44/1 W
	00243966.jpg 	10/15/16 / 17:53:27	N/A

`

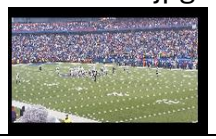
	00252612.jpg 	10:30:16 / 13:38:02	N/A
	00258705.jpg 	10/30/16 / 15:34:25	N/A
00000014.jpg 		10/30/2016 / 15:34:25	N/A
	00263177.jpg 	10/30/16 / 15:50:30	N/A
	00328938.jpg 	11/19/16 / 16:26:56	N/A

FIGURE4

EXIF Information Obtained Of The Make And Model Of Phone Used

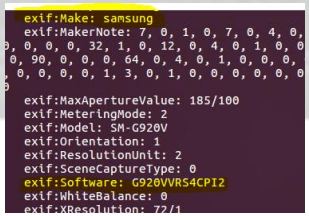
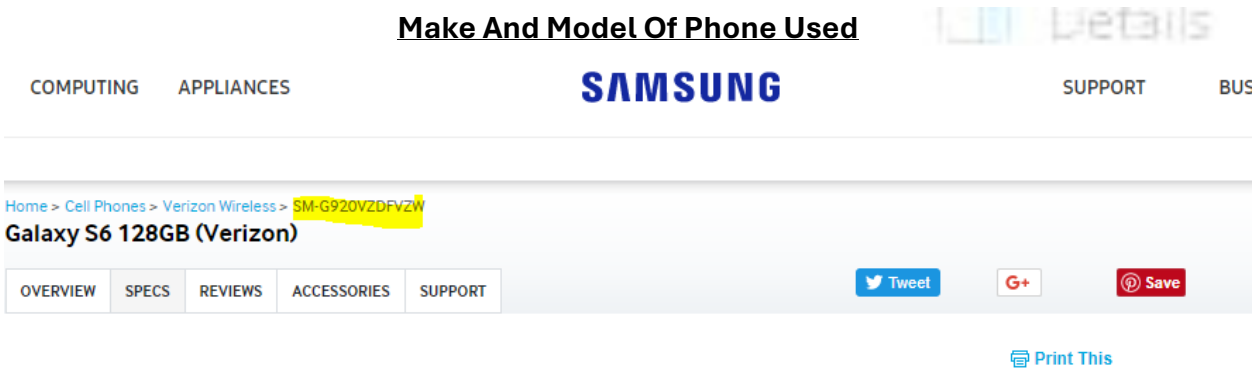


FIGURE5

`

Make And Model Of Phone Used



Upon further investigation file 00216812.png found in the Foremost_Results2 folder revealed an secret message displayed in FIGURE 6.

FIGURE6
Secret Message

The scalpel tool was used against the USB.001 and USB.001.txt files but reconfigured and customized to reveal RTF files which was sent to the ScalpelResults3 folder. This was done by inputting the file code: RTF y 2500000 \x7b\x5c\x72\x74\x66 into the scalpel configuration file. The ScalpelResults3 folder displayed folder rtf-0-0 and file 00000000.rtf. This file was then opened and displayed the message: My hideout is in the brownstone in the city next to the pizza shop. All images obtained were investigated and file 00180878.jpg was the file that coincided with the rtf message. This is displayed in FIGURE 7.

`

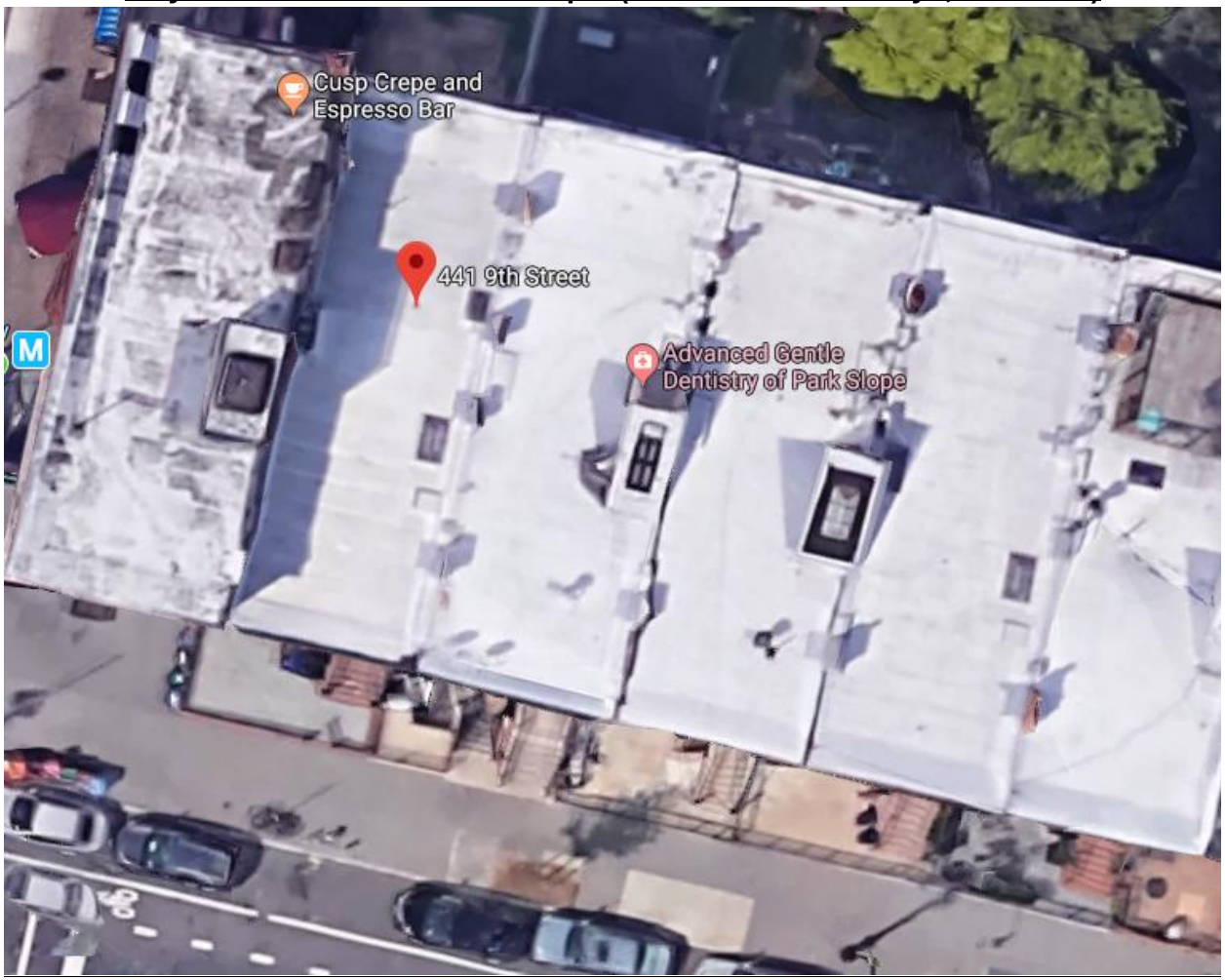
FIGURE7
Hide Out Spot

Further investigation was needed, and Google Maps revealed the physical address of the suspects hide out spot displayed in Figure 8.

Figure 8

Google Map Image

Physical Address of Hide Out Spot (441 9th Street Brooklyn, NY 11215)



`

`

Conclusion

The examiner successfully found the required MD5 hash value file that coincided with the hashdeep value of the intercepted suspect file which was revealed in the 00170349.jpg file. With further investigation the examiner found a secret message in file 00216812.png. With the usage of scalpel, the hidden rtf file was obtained and revealed the suspects hideout. The usage and information obtained from tools such as scalpel, foremost and ImageMagick successfully incriminated the potential suspect.