#JonSecOps

USB Evidence Recovery and Analysis Using FTK Imager and Hex Tools

Background

Agents at the Federal Bureau of Investigation (FBI) have been investigating the repeated theft of intellectual property. Several companies have claimed that a Chinese hosted website is posting and selling copied home building plans. A suspect was identified as Andrew Connor. His home was raided but no computers were present and neither was he. A 1GB USB thumb drive was recovered at the scene. Agents are hoping the thumb drive might have enough evidence to charge Connor with the theft of intellectual property. A note was found at the scene that vaguely indicated a meeting but no other information was recovered.

Request

Mr. McBride is to review the USB thumb drive for information related to the suspected crime and potential meeting with the suspect. Please report on the following information: • Where is the suspect meeting his contact? • Who is the contact at the meeting? • Provide the name of the item to be ordered. • What are the names of the plans being stolen? • What website are the plans stolen from? • What software does it appear the suspect has been using to duplicate the original plans?

Summary of Findings

During the investigation, pertinent information such as password encryption and hidden files were obtained and reported in the analysis section of this report.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Created	Working Copy	USB.001	13f2b3f7bdb9dd568d53e9b429ca0e1b
Supplemental	Text File	USB.001	N/A

Files			

Table 1: Case evidence items

Collection and Analysis

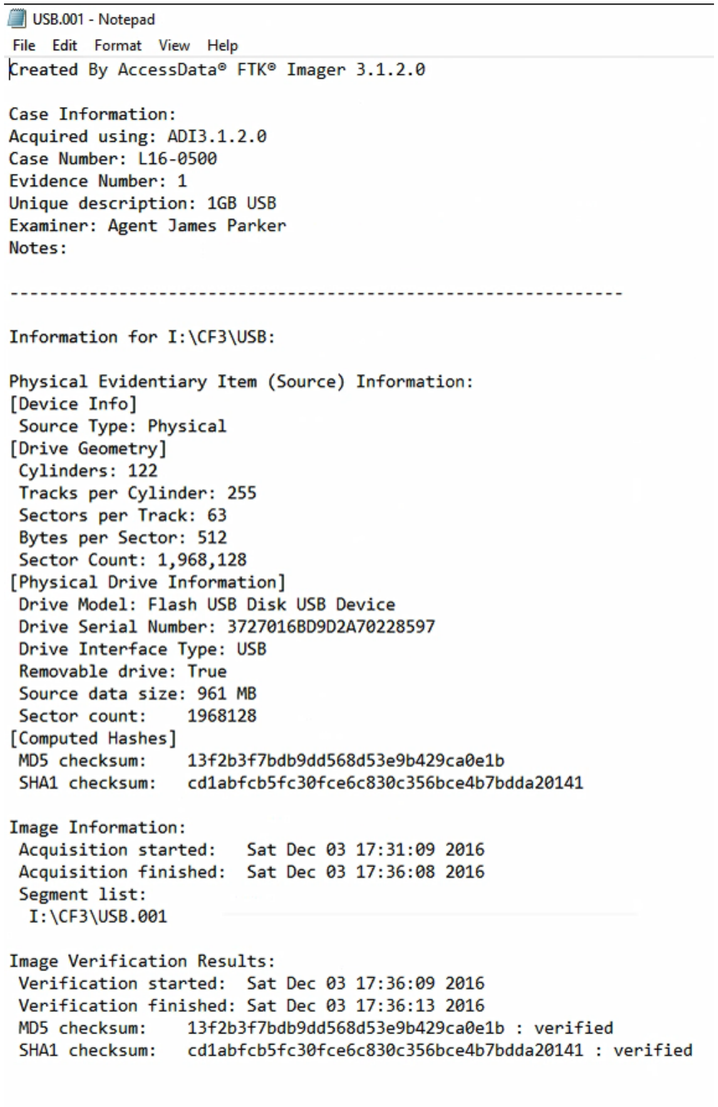
Collection

The USB drive that was captured during the raid was investigated and the findings are within the analysis section below.

Analysis

During the investigation, a text document named USB.001 was investigated. This file displayed information such as device info, physical drive information, computed hashes, image information and image verification results as displayed in Figure 1.

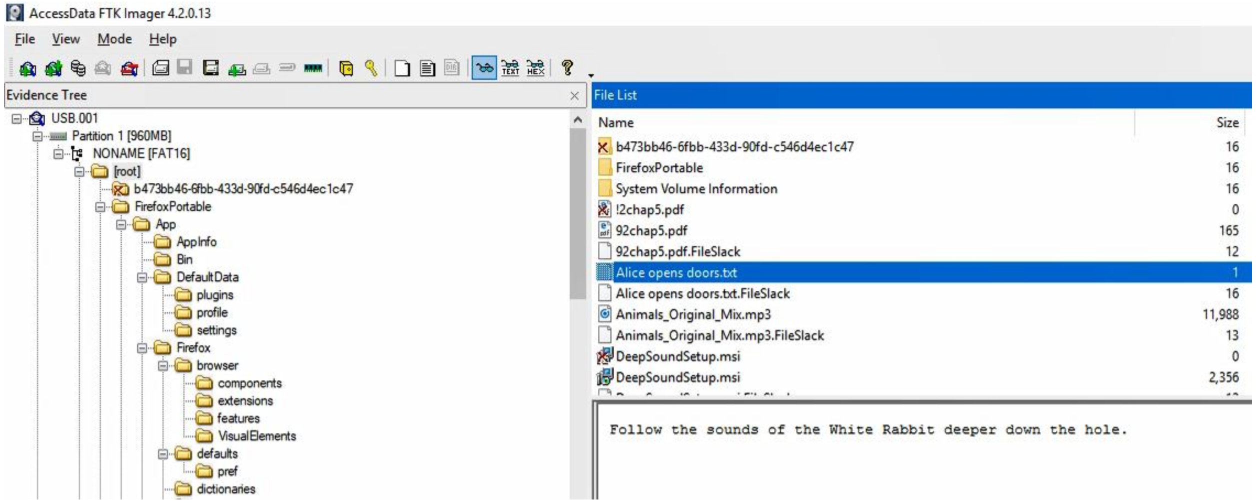
FIGURE 1: DEVICE INFORMATION



```
Created By AccessData® FTK® Imager 3.1.2.0

Case Information: 
Acquired using: ADI3.1.2.0
Case Number: L16-0500
Evidence Number: 1
Unique description: 1GB USB
Examiner: Agent James Parker
Notes: 

--------------------------------------------------------------

Information for I:\CF3\USB:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 122
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 1,968,128
[Physical Drive Information]
 Drive Model: Flash USB Disk USB Device
 Drive Serial Number: 3727016BD9D2A70228597
 Drive Interface Type: USB
 Removable drive: True
 Source data size: 961 MB
 Sector count:    1968128
[Computed Hashes]
 MD5 checksum:    13f2b3f7bdb9dd568d53e9b429ca0e1b
 SHA1 checksum:   cd1abfcb5fc30fce6c830c356bce4b7bdda20141

Image Information:
 Acquisition started:   Sat Dec 03 17:31:09 2016
 Acquisition finished:  Sat Dec 03 17:36:08 2016
 Segment list:
  I:\CF3\USB.001

Image Verification Results:
 Verification started:  Sat Dec 03 17:36:09 2016
 Verification finished: Sat Dec 03 17:36:13 2016
 MD5 checksum:    13f2b3f7bdb9dd568d53e9b429ca0e1b : verified
 SHA1 checksum:   cd1abfcb5fc30fce6c830c356bce4b7bdda20141 : verified
```

The AccessData FTK Imager software was used to open the USB.001 file that displayed system information. While using FTK Imager the root folder displayed a text file named Alice opens doors.txt with a message as displayed in Figure 2.

FIGURE 2: TEXT FILE MESSAGE



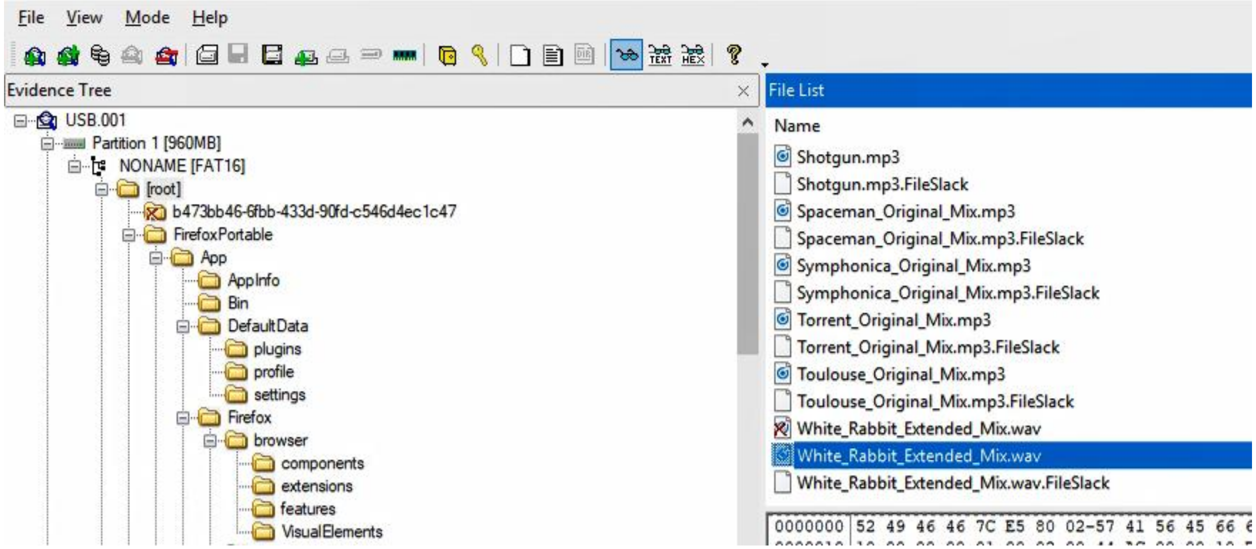
```
USB.001
  Partition 1 [960MB]
    NONAME [FAT16]
      [root]
        b473bb46-6fbb-433d-90fd-c546d4ec1c47
        FirefoxPortable
          App
            AppInfo
            Bin
            DefaultData
              plugins
              profile
              settings
            Firefox
              browser
                components
                extensions
                features
                VisualElements
              defaults
                pref
              dictionaries
```

Name	Size
b473bb46-6fbb-433d-90fd-c546d4ec1c47	16
FirefoxPortable	16
System Volume Information	16
!2chap5.pdf	0
92chap5.pdf	165
92chap5.pdf.FileSlack	12
Alice opens doors.txt	1
Alice opens doors.txt.FileSlack	16
Animals_Original_Mix.mp3	11,988
Animals_Original_Mix.mp3.FileSlack	13
DeepSoundSetup.msi	0
DeepSoundSetup.msi	2,356

```
Follow the sounds of the White Rabbit deeper down the hole.
```

Further investigation in the root file displayed a file named White_Rabbit_Extended.wav which is congruent to the text file message as displayed in Figure 3.

FIGURE 3: WAV FILE



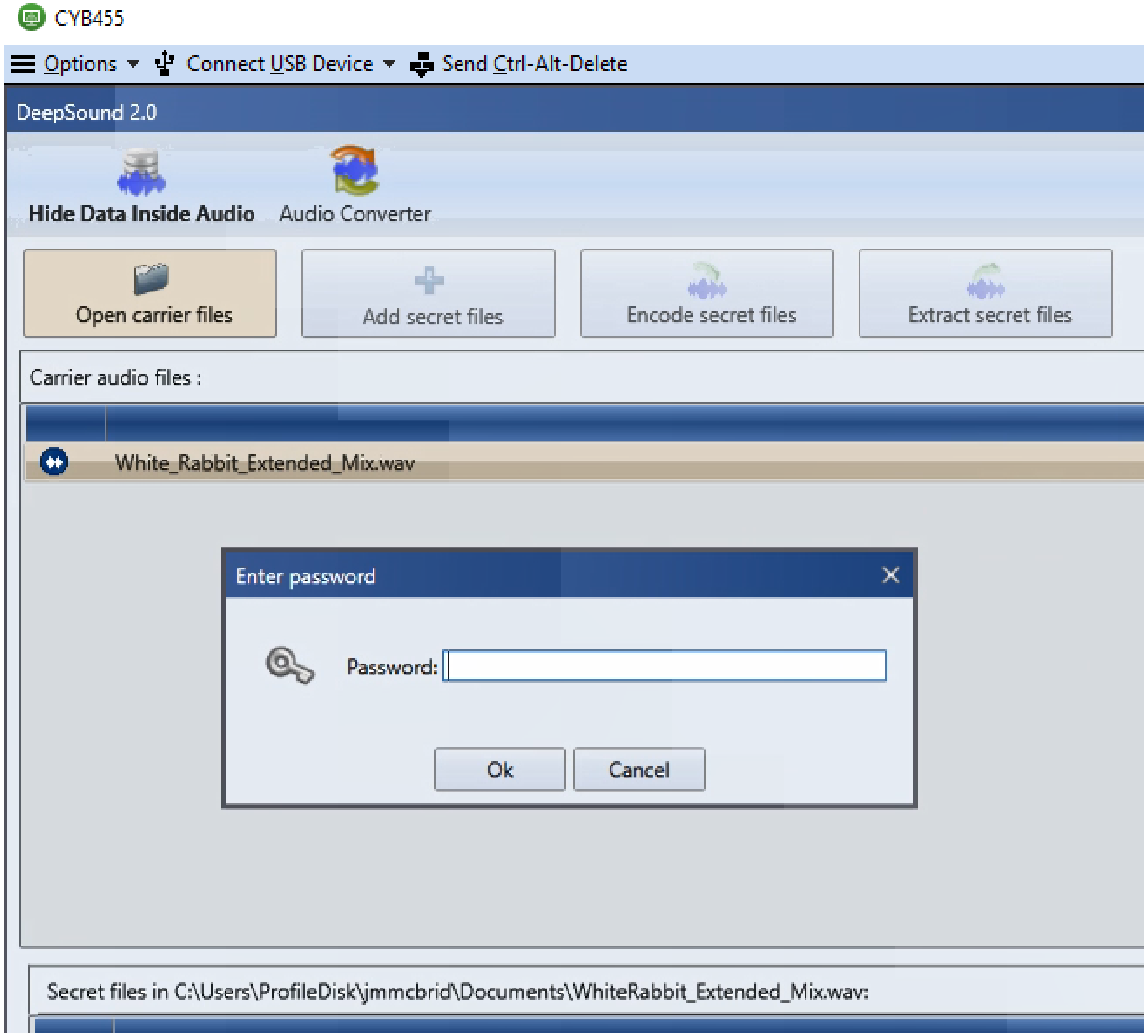
```
USB.001
  Partition 1 [960MB]
    NONAME [FAT16]
      [root]
        b473bb46-6fbb-433d-90fd-c546d4ec1c47
        FirefoxPortable
          App
            AppInfo
            Bin
            DefaultData
              plugins
              profile
              settings
            Firefox
              browser
                components
                extensions
                features
                VisualElements
```

```
Shotgun.mp3
Shotgun.mp3.FileSlack
Spaceman_Original_Mix.mp3
Spaceman_Original_Mix.mp3.FileSlack
Symphonica_Original_Mix.mp3
Symphonica_Original_Mix.mp3.FileSlack
Torrent_Original_Mix.mp3
Torrent_Original_Mix.mp3.FileSlack
Toulouse_Original_Mix.mp3
Toulouse_Original_Mix.mp3.FileSlack
White_Rabbit_Extended_Mix.wav
White_Rabbit_Extended_Mix.wav
White_Rabbit_Extended_Mix.wav.FileSlack
```

```
0000000 52 49 46 46 7C E5 80 02-57 41 56 45 66 6
```

The wav file was then exported from FTK Imager, saved within the Windows document folder and inputted into the DeepSound software to be investigated which displayed that a password was need displayed in Figure 4.

FIGURE 4: DEEPSOUND SOFTWARE WITH A PASSWORD NEEDED TO OPEN WAV FILE



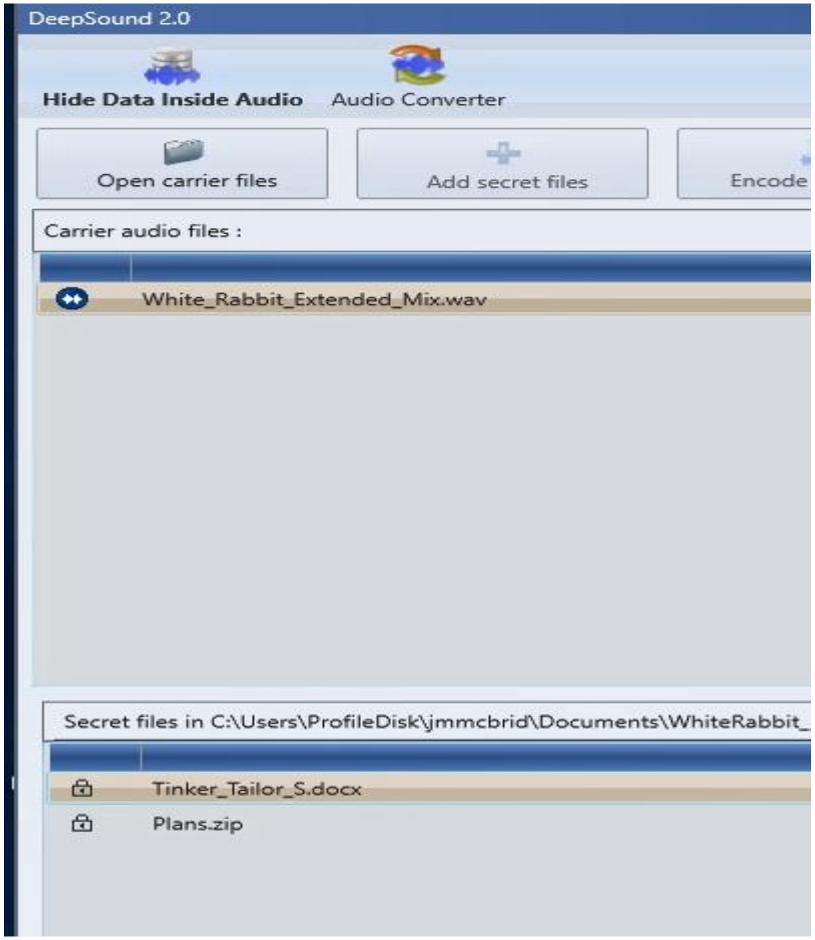
Carrier audio files :

White_Rabbit_Extended_Mix.wav

Secret files in C:\Users\ProfileDisk\jmmcbrid\Documents\WhiteRabbit_Extended_Mix.wav:

With constructive thinking the password Alice was successful with opening the wav file and revealed a .docx file as well as a .zip file as displayed in Figure 5.

FIGURE 5: REVEALED FILES WITHIN WAV FILE



Carrier audio files :

White_Rabbit_Extended_Mix.wav

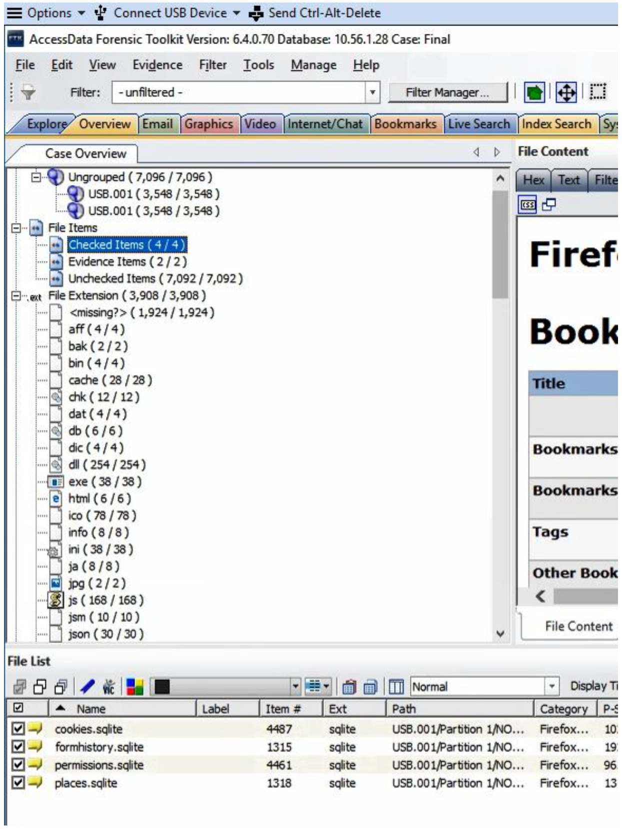
Secret files in C:\Users\ProfileDisk\jmmcbrid\Documents\WhiteRabbit_

Tinker_Tailor_S.docx

Plans.zip

The Tinker_TailorS.docx file was password encrypted. Further investigation in FTK revealed a folder named Checked Items and revealed a sqlite file named places as displayed in Figure 6.

FIGURE 6: PLACES SQLITE FILE



AccessData Forensic Toolkit Version: 6.4.0.70 Database: 10.56.1.28 Case: Final

Filter: - unfiltered -

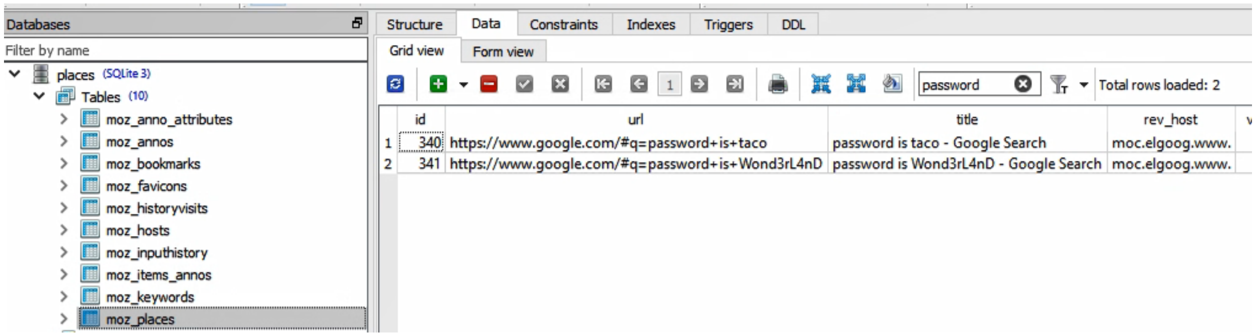
```
Ungrouped ( 7,096 / 7,096 )
    USB.001 ( 3,548 / 3,548 )
    USB.001 ( 3,548 / 3,548 )
File Items
    Checked Items ( 4 / 4 )
    Evidence Items ( 2 / 2 )
    Unchecked Items ( 7,092 / 7,092 )
File Extension ( 3,908 / 3,908 )
    <missing?> ( 1,924 / 1,924 )
    aff ( 4 / 4 )
    bak ( 2 / 2 )
    bin ( 4 / 4 )
    cache ( 28 / 28 )
    chk ( 12 / 12 )
    dat ( 4 / 4 )
    db ( 6 / 6 )
    dic ( 4 / 4 )
    dll ( 254 / 254 )
    exe ( 38 / 38 )
    html ( 6 / 6 )
    ico ( 78 / 78 )
    info ( 8 / 8 )
    ini ( 38 / 38 )
    ja ( 8 / 8 )
    jpg ( 2 / 2 )
    js ( 168 / 168 )
    jsm ( 10 / 10 )
    json ( 30 / 30 )
```

Normal

☑	Name	Label	Item #	Ext	Path	Category	P-S
☑	cookies.sqlite		4487	sqlite	USB.001/Partition 1/NO...	Firefox...	10
☑	formhistory.sqlite		1315	sqlite	USB.001/Partition 1/NO...	Firefox...	19
☑	permissions.sqlite		4461	sqlite	USB.001/Partition 1/NO...	Firefox...	96
☑	places.sqlite		1318	sqlite	USB.001/Partition 1/NO...	Firefox...	13

The places.sqlite file was investigated using SQLite Studio and displayed a folder named moz_places. By searching the term password in the search bar, revealed two passwords displayed in Figure 7.

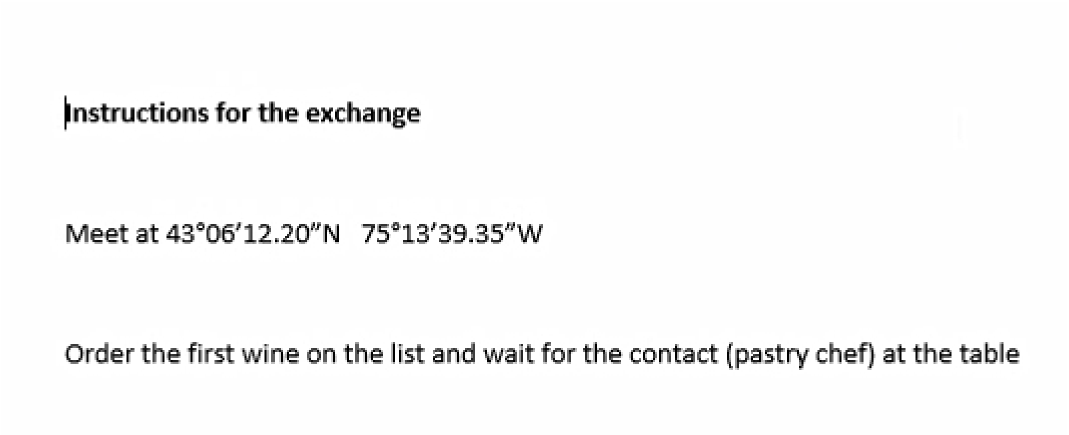
FIGURE 7: PASSWORD



	id	url	title	rev_host
1	340	https://www.google.com/#q=password+is+taco	password is taco - Google Search	moc.elgoog.www.
2	341	https://www.google.com/#q=password+is+Wond3rL4nD	password is Wond3rL4nD - Google Search	moc.elgoog.www.

The password Wond3rL4nd was used for the Tinker_TailorS.docx file and revealed the following message displayed in Figure 8.

FIGURE 8: TINKER TAILOR DOCUMENT



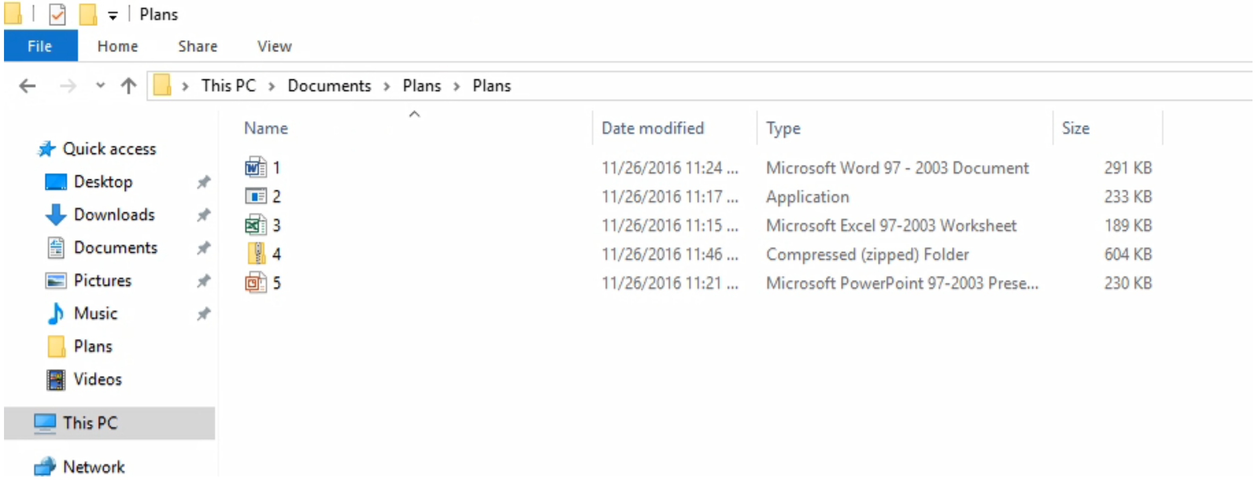
Instructions for the exchange

Meet at 43°06’12.20”N   75°13’39.35”W

Order the first wine on the list and wait for the contact (pastry chef) at the table

The plans zip file was also password encrypted and revealed 5 different file formats as displayed in Figure 9.

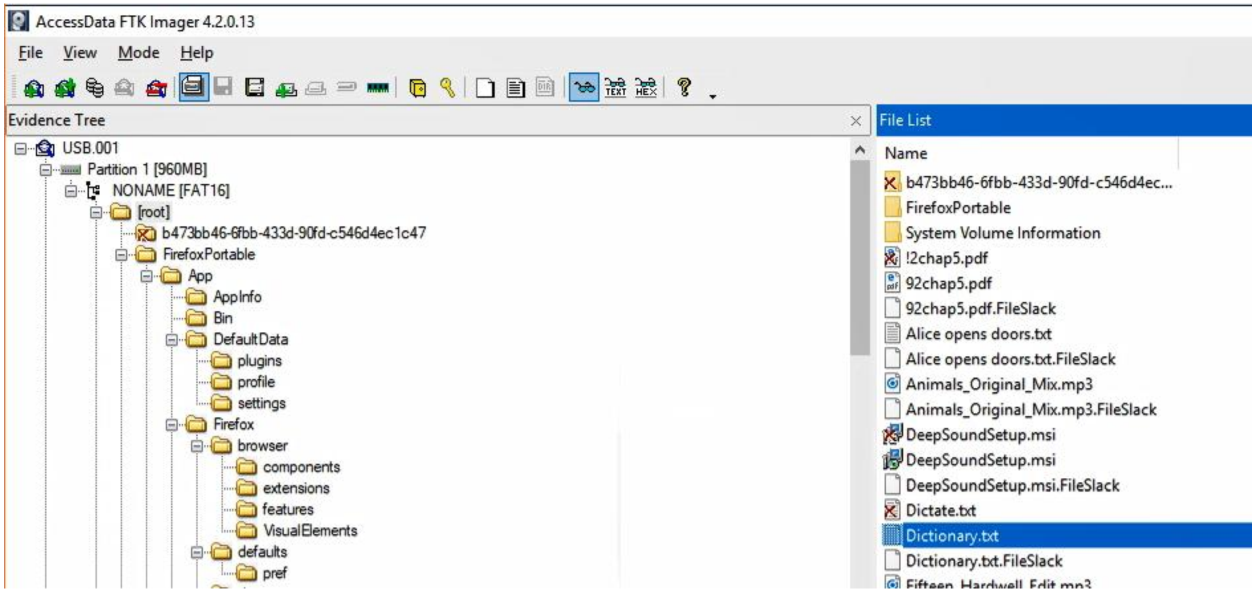
FIGURE 9: PLANS ZIP FOLDER



Name	Date modified	Type	Size
1	11/26/2016 11:24 ...	Microsoft Word 97 - 2003 Document	291 KB
2	11/26/2016 11:17 ...	Application	233 KB
3	11/26/2016 11:15 ...	Microsoft Excel 97-2003 Worksheet	189 KB
4	11/26/2016 11:46 ...	Compressed (zipped) Folder	604 KB
5	11/26/2016 11:21 ...	Microsoft PowerPoint 97-2003 Prese...	230 KB

Further investigation using FTK Imager revealed a Dictionary txt file within the root folder displayed in Figure 10.

FIGURE 10: DICTIONARY TEXT FILE

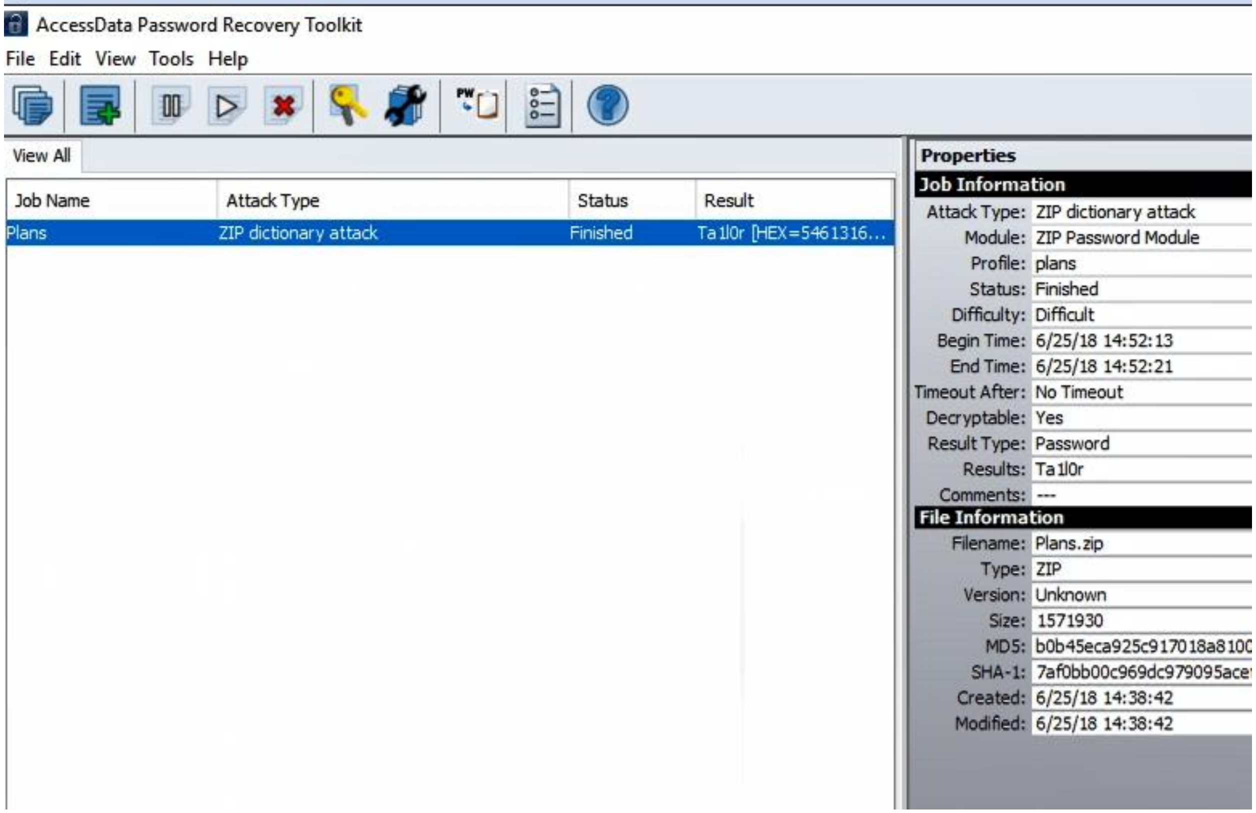


```
USB.001
  Partition 1 [960MB]
    NONAME [FAT16]
      [root]
        b473bb46-6fbb-433d-90fd-c546d4ec1c47
        FirefoxPortable
          App
            AppInfo
            Bin
            DefaultData
              plugins
              profile
              settings
            Firefox
              browser
                components
                extensions
                features
                VisualElements
              defaults
                pref
```

```
b473bb46-6fbb-433d-90fd-c546d4ec...
FirefoxPortable
System Volume Information
!2chap5.pdf
92chap5.pdf
92chap5.pdf.FileSlack
Alice opens doors.txt
Alice opens doors.txt.FileSlack
Animals_Original_Mix.mp3
Animals_Original_Mix.mp3.FileSlack
DeepSoundSetup.msi
DeepSoundSetup.msi
DeepSoundSetup.msi.FileSlack
Dictate.txt
Dictionary.txt
Dictionary.txt.FileSlack
Fifteen_Hardwell_Edit.mp3
```

The Dictionary text file will be used as a custom dictionary using PRTK to decrypt the plans.zip file. This process displayed the password Ta1l0r as displayed in Figure 11.

FIGURE 11: PLANS.ZIP PASSWORD IN PRTK


AccessData Password Recovery Toolkit
File Edit View Tools Help
View All

Job Name	Attack Type	Status	Result
Plans	ZIP dictionary attack	Finished	Ta1l0r [HEX=5461316...

Properties

Job Information

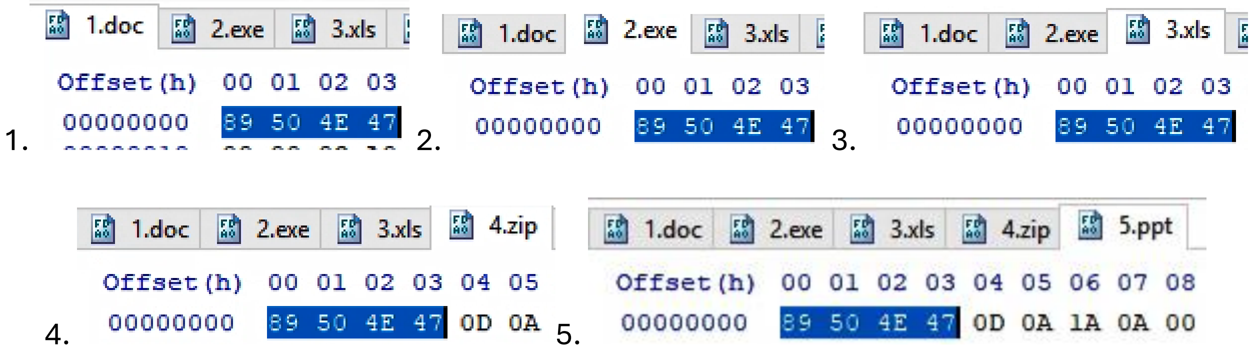
Attack Type: ZIP dictionary attack
Module: ZIP Password Module
Profile: plans
Status: Finished
Difficulty: Difficult
Begin Time: 6/25/18 14:52:13
End Time: 6/25/18 14:52:21
Timeout After: No Timeout
Decryptable: Yes
Result Type: Password
Results: Ta1l0r
Comments: ---

File Information

Filename: Plans.zip
Type: ZIP
Version: Unknown
Size: 1571930
MD5: b0b45eca925c917018a810c
SHA-1: 7af0bb00c969dc979095ace
Created: 6/25/18 14:38:42
Modified: 6/25/18 14:38:42

This password was used to decrypt the plans.zip file. When opening the files in the Plans folder, the files were unable to either open or read. Using HexEditor revealed that the files were PNG files because of the starting header of 89 50 4E 47 as displayed in Figure 12.

FIGURE 12: PLANS FOLDER DOCUMENT HEADERS USING HEXEDITOR



1.
```
1.doc  2.exe  3.xls
Offset(h)  00 01 02 03
00000000   89 50 4E 47
```

2.
```
1.doc  2.exe  3.xls
Offset(h)  00 01 02 03
00000000   89 50 4E 47
```

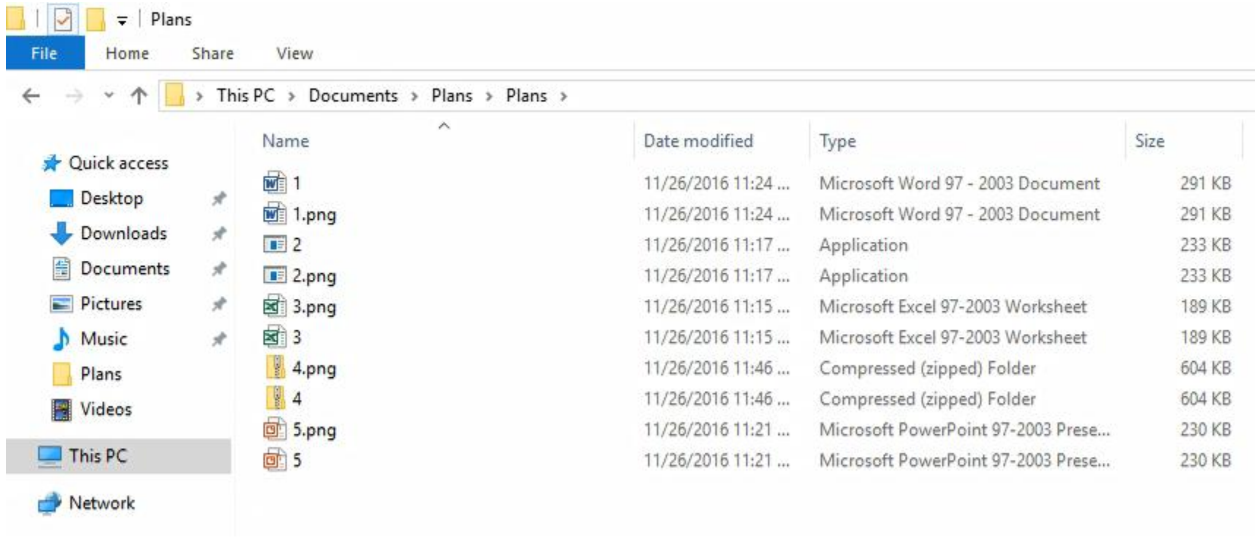
3.
```
1.doc  2.exe  3.xls
Offset(h)  00 01 02 03
00000000   89 50 4E 47
```

4.
```
1.doc  2.exe  3.xls  4.zip
Offset(h)  00 01 02 03 04 05
00000000   89 50 4E 47 0D 0A
```

5.
```
1.doc  2.exe  3.xls  4.zip  5.ppt
Offset(h)  00 01 02 03 04 05 06 07 08
00000000   89 50 4E 47 0D 0A 1A 0A 00
```

This validated that the files were not either a .doc, .exe, .xls, .zip or .ppt as previously displayed in Figure 9. Each file was then copied in the Plans folder and renamed with the file extension .png as displayed in Figure 13.

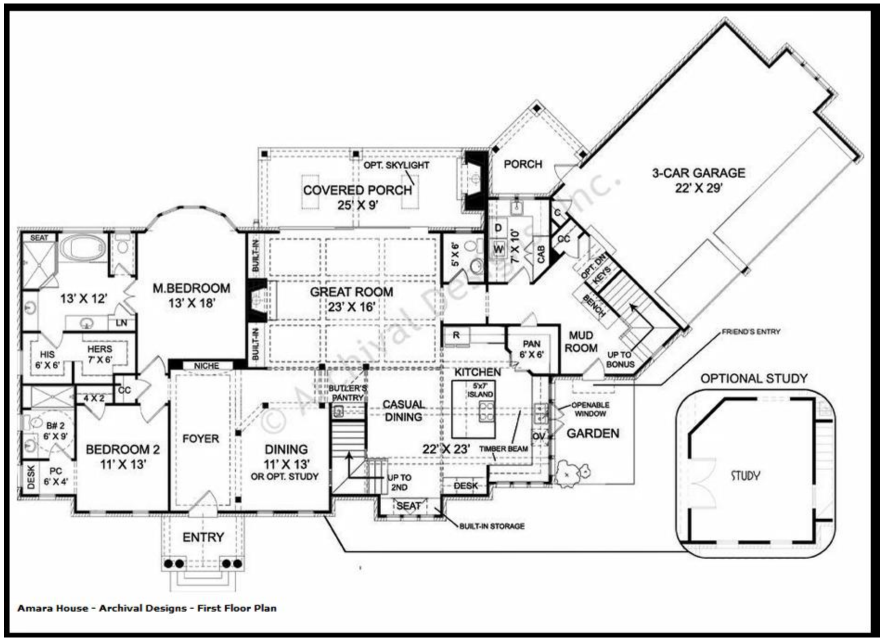
FIGURE 13: REFORMATTED FILES



Name	Date modified	Type	Size
1	11/26/2016 11:24 ...	Microsoft Word 97 - 2003 Document	291 KB
1.png	11/26/2016 11:24 ...	Microsoft Word 97 - 2003 Document	291 KB
2	11/26/2016 11:17 ...	Application	233 KB
2.png	11/26/2016 11:17 ...	Application	233 KB
3.png	11/26/2016 11:15 ...	Microsoft Excel 97-2003 Worksheet	189 KB
3	11/26/2016 11:15 ...	Microsoft Excel 97-2003 Worksheet	189 KB
4.png	11/26/2016 11:46 ...	Compressed (zipped) Folder	604 KB
4	11/26/2016 11:46 ...	Compressed (zipped) Folder	604 KB
5.png	11/26/2016 11:21 ...	Microsoft PowerPoint 97-2003 Prese...	230 KB
5	11/26/2016 11:21 ...	Microsoft PowerPoint 97-2003 Prese...	230 KB

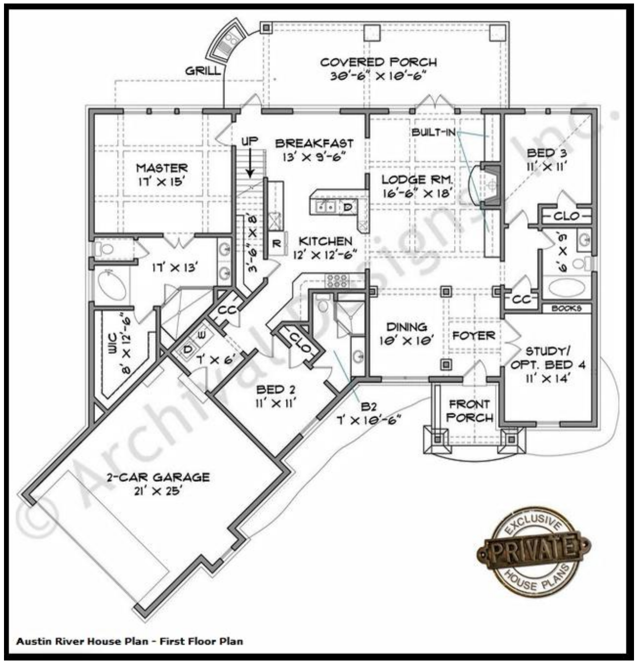
IranView was used to open the all five reformatted files and displayed five different home floor plans displayed in Figure 14.

FIGURE 14: FLOOR PLAN COMPILATION USING IRANVIEW



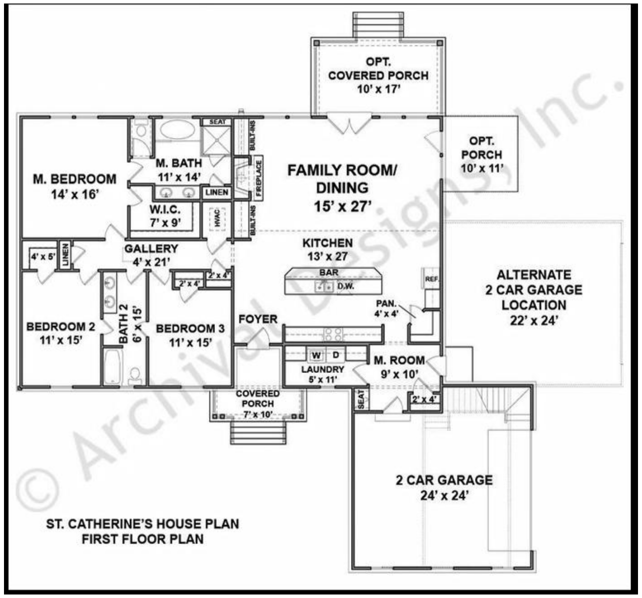
Amara House - Archival Designs - First Floor Plan

1.png

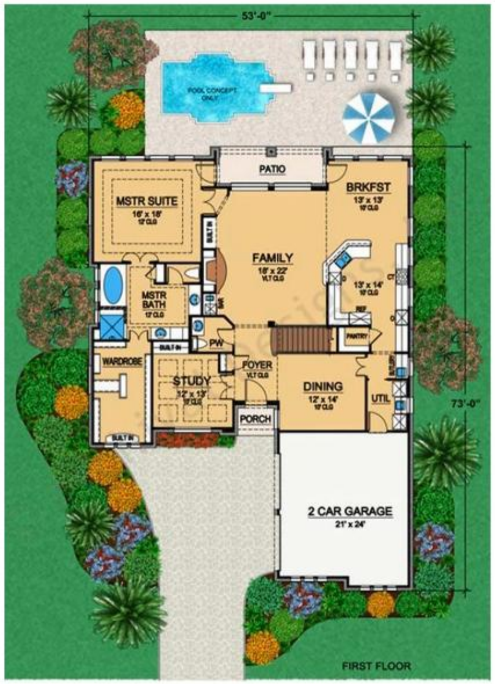


Austin River House Plan - First Floor Plan

2.png


OPT. COVERED PORCH 10' x 17'
OPT. PORCH 10' x 11'
FAMILY ROOM/ DINING 15' x 27'
M. BEDROOM 14' x 16'
M. BATH 11' x 14'
SEAT
BUILT-INS
FIREPLACE
LINEN
W.I.C. 7' x 9'
HVAC
BUILT-INS
KITCHEN 13' x 27
BAR
D.W.
REF.
PAN. 4' x 4'
ALTERNATE 2 CAR GARAGE LOCATION 22' x 24'
4' x 5'
LINEN
GALLERY 4' x 21'
2' x 4'
2' x 4'
BEDROOM 2 11' x 15'
BATH 2 6' x 15'
BEDROOM 3 11' x 15'
FOYER
W
D
LAUNDRY 5' x 11'
M. ROOM 9' x 10'
SEAT
2' x 4'
COVERED PORCH 7' x 10'
2 CAR GARAGE 24' x 24'
ST. CATHERINE'S HOUSE PLAN
FIRST FLOOR PLAN
© Archival Designs, Inc.

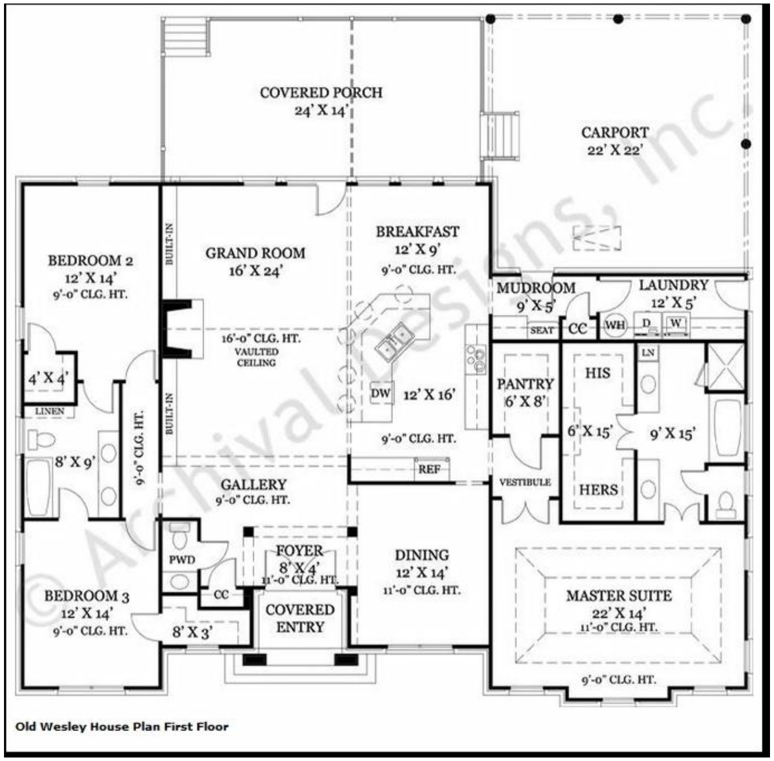
3.png



MEDINAH

Medinah House Plan First Floor

4.png

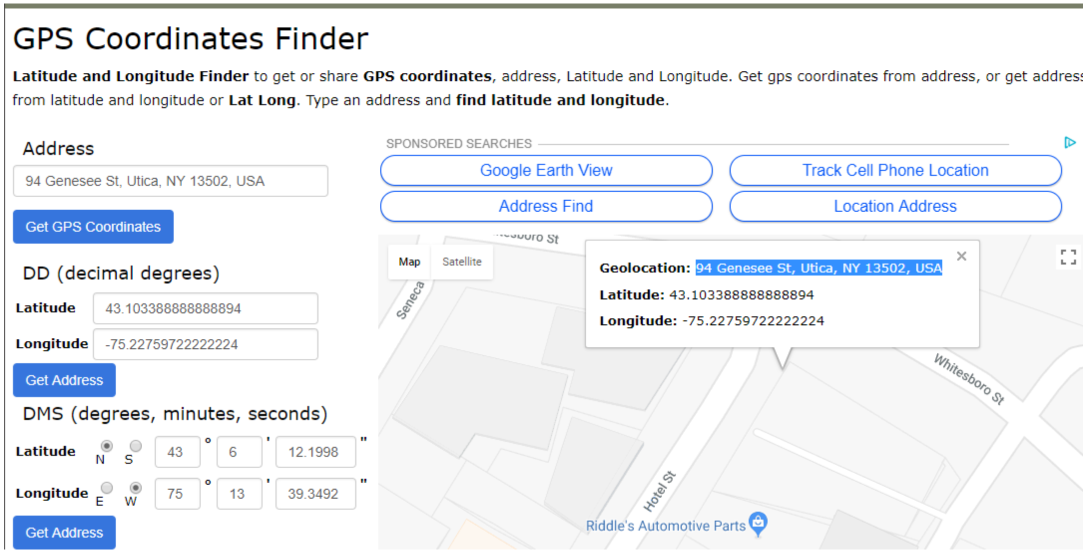


5.png

REQUEST ANSWERS

The obtained latitude and longitude information obtained from the Tinker_TailorS.docx file was used to find where the suspect is meeting his contact displayed in Figure 15.

FIGURE 15: MEETING LOCATION



GPS Coordinates Finder

Latitude and Longitude Finder to get or share **GPS coordinates**, address, Latitude and Longitude. Get gps coordinates from address, or get addres from latitude and longitude or **Lat Long**. Type an address and **find latitude and longitude**.

Address

94 Genesee St, Utica, NY 13502, USA

DD (decimal degrees)

Latitude 43.103388888888894

Longitude -75.22759722222224

DMS (degrees, minutes, seconds)

Latitude ● N ○ S 43 ° 6 ' 12.1998 "

Longitude ○ E ● W 75 ° 13 ' 39.3492 "

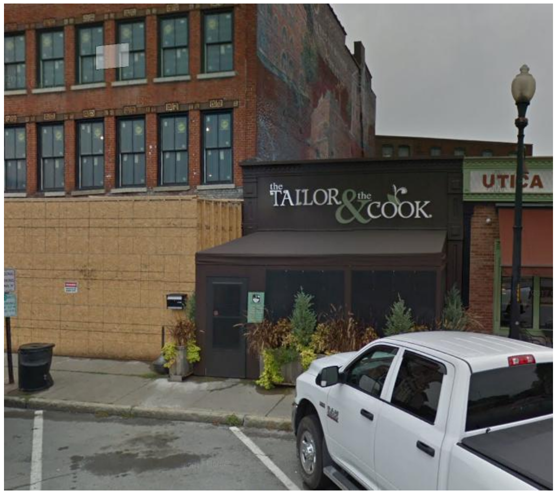
Geolocation: 94 Genesee St, Utica, NY 13502, USA

Latitude: 43.103388888888894

Longitude: -75.22759722222224

By inputting the address in Google Maps revealed the name of the meeting place which is The Tailor & The Cook displayed in Figure 16.

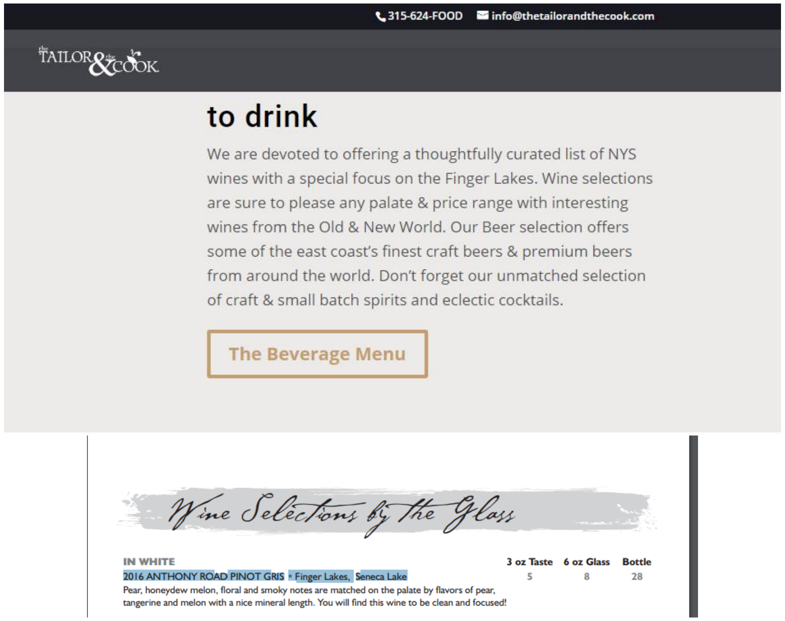
FIGURE 16: GOOGLE MAPS MEETING PLACE LOCATION



94 Genesse Street, Utica NY, 13502

The contact of the meeting was revealed in the Tinker_TailorS.docx file which is the pastry chef at The Tailor & The Cook as displayed in Figure 8. The item being ordered was revealed in the Tinker_TailorS.docx file in Figure 8 which was obtained by going to The Tailor & The Cook website found at URL http://thetailorandthecook.com/menu. This website revealed a beverage menu which was clicked and displayed multiple wine options and displayed the first wine item to be ordered named 2016 ANTHONY ROAD PINOT GRIS displayed in Figure 17.

FIGURE 17: WINE MENU OPTIONS



☎ 315-624-FOOD ✉ info@thetailorandthecook.com

the TAILOR & the COOK

to drink

We are devoted to offering a thoughtfully curated list of NYS wines with a special focus on the Finger Lakes. Wine selections are sure to please any palate & price range with interesting wines from the Old & New World. Our Beer selection offers some of the east coast's finest craft beers & premium beers from around the world. Don't forget our unmatched selection of craft & small batch spirits and eclectic cocktails.

The Beverage Menu

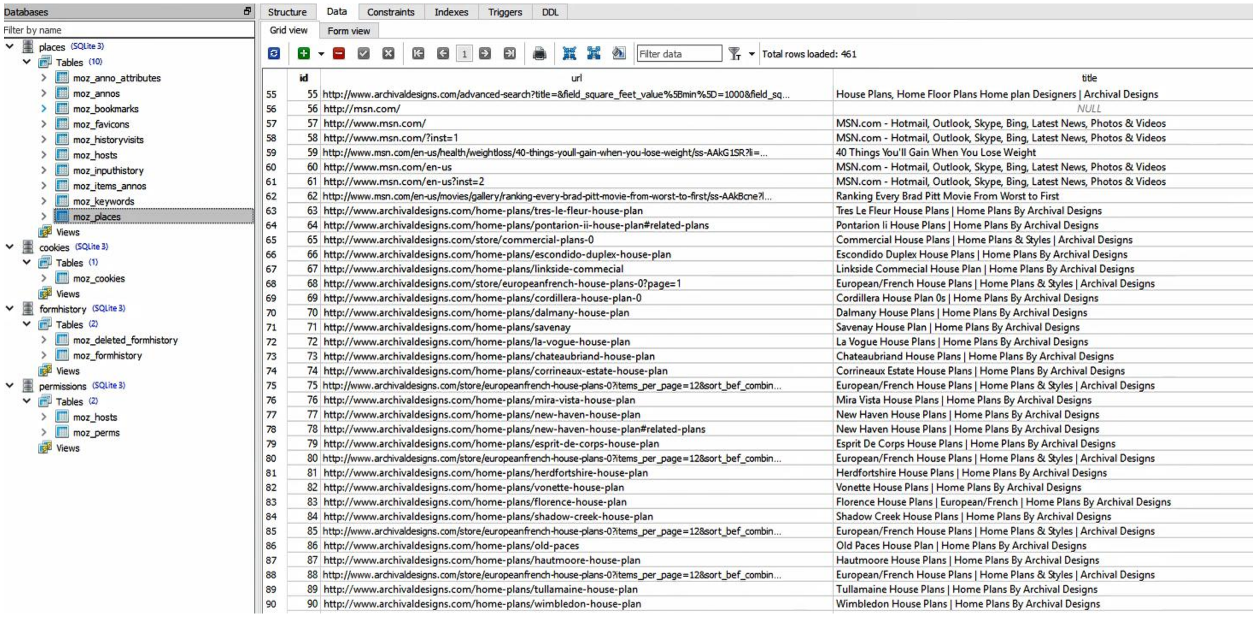
Wine Selections by the Glass

IN WHITE	3 oz Taste	6 oz Glass	Bottle
2016 ANTHONY ROAD PINOT GRIS • Finger Lakes, Seneca Lake Pear, honeydew melon, floral and smoky notes are matched on the palate by flavors of pear, tangerine and melon with a nice mineral length. You will find this wine to be clean and focused!	5	8	28

The names of the plans being stolen as displayed in Figure 14:
Amara House - Archival Design – First Floor Plan
Austin River House – First Floor Plan
St. Catherine's House Plan – First Floor
Medinah House Plan – First Floor
Old Wesley House Plan – First Floor

Possible other floor plans being stolen were found in the places database under the moz_places folder using SQLite Studio displayed in Figure 18.

FIGURE 18: MORE POSSIBLE FLOOR PLANS BEING STOLEN

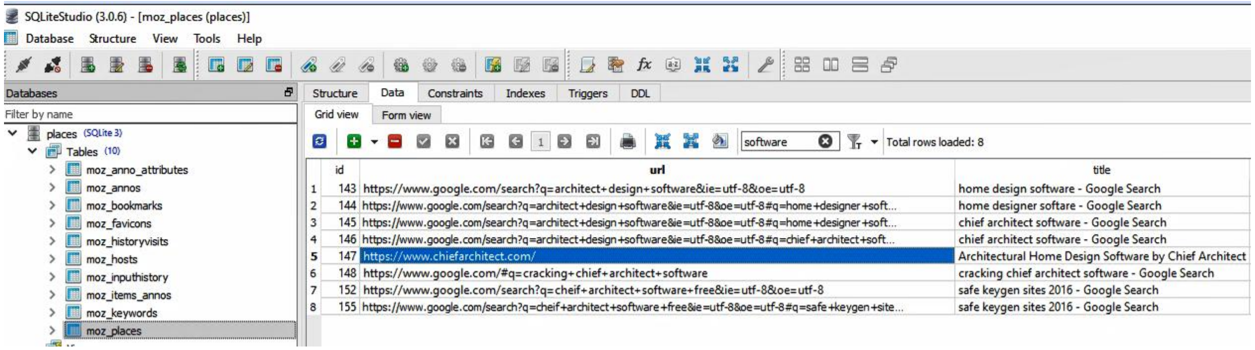


	id	url	title
55	55	http://www.archivaldesigns.com/advanced-search?title=&field_square_feet_value%5Bmin%5D=1000&field_sq...	House Plans, Home Floor Plans Home plan Designers | Archival Designs
56	56	http://msn.com/	NULL
57	57	http://www.msn.com/	MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos
58	58	http://www.msn.com/?inst=1	MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos
59	59	http://www.msn.com/en-us/health/weightloss/40-things-youll-gain-when-you-lose-weight/ss-AAkG1SR?li=...	40 Things You'll Gain When You Lose Weight
60	60	http://www.msn.com/en-us	MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos
61	61	http://www.msn.com/en-us?inst=2	MSN.com - Hotmail, Outlook, Skype, Bing, Latest News, Photos & Videos
62	62	http://www.msn.com/en-us/movies/gallery/ranking-every-brad-pitt-movie-from-worst-to-first/ss-AAkBcne?l...	Ranking Every Brad Pitt Movie From Worst to First
63	63	http://www.archivaldesigns.com/home-plans/tres-le-fleur-house-plan	Tres Le Fleur House Plans | Home Plans By Archival Designs
64	64	http://www.archivaldesigns.com/home-plans/pontarion-ii-house-plan#related-plans	Pontarion Ii House Plans | Home Plans By Archival Designs
65	65	http://www.archivaldesigns.com/store/commercial-plans-0	Commercial House Plans | Home Plans & Styles | Archival Designs
66	66	http://www.archivaldesigns.com/home-plans/escondido-duplex-house-plan	Escondido Duplex House Plans | Home Plans By Archival Designs
67	67	http://www.archivaldesigns.com/home-plans/linkside-commecial	Linkside Commecial House Plan | Home Plans By Archival Designs
68	68	http://www.archivaldesigns.com/store/europeanfrench-house-plans-0?page=1	European/French House Plans | Home Plans & Styles | Archival Designs
69	69	http://www.archivaldesigns.com/home-plans/cordillera-house-plan-0	Cordillera House Plan 0s | Home Plans By Archival Designs
70	70	http://www.archivaldesigns.com/home-plans/dalmany-house-plan	Dalmany House Plans | Home Plans By Archival Designs
71	71	http://www.archivaldesigns.com/home-plans/savenay	Savenay House Plan | Home Plans By Archival Designs
72	72	http://www.archivaldesigns.com/home-plans/la-vogue-house-plan	La Vogue House Plans | Home Plans By Archival Designs
73	73	http://www.archivaldesigns.com/home-plans/chateaubriand-house-plan	Chateaubriand House Plans | Home Plans By Archival Designs
74	74	http://www.archivaldesigns.com/home-plans/corrineaux-estate-house-plan	Corrineaux Estate House Plans | Home Plans By Archival Designs
75	75	http://www.archivaldesigns.com/store/europeanfrench-house-plans-0?items_per_page=12&sort_bef_combin...	European/French House Plans | Home Plans & Styles | Archival Designs
76	76	http://www.archivaldesigns.com/home-plans/mira-vista-house-plan	Mira Vista House Plans | Home Plans By Archival Designs
77	77	http://www.archivaldesigns.com/home-plans/new-haven-house-plan	New Haven House Plans | Home Plans By Archival Designs
78	78	http://www.archivaldesigns.com/home-plans/new-haven-house-plan#related-plans	New Haven House Plans | Home Plans By Archival Designs
79	79	http://www.archivaldesigns.com/home-plans/esprit-de-corps-house-plan	Esprit De Corps House Plans | Home Plans By Archival Designs
80	80	http://www.archivaldesigns.com/store/europeanfrench-house-plans-0?items_per_page=12&sort_bef_combin...	European/French House Plans | Home Plans & Styles | Archival Designs
81	81	http://www.archivaldesigns.com/home-plans/herdfortshire-house-plan	Herdfortshire House Plans | Home Plans By Archival Designs
82	82	http://www.archivaldesigns.com/home-plans/vonette-house-plan	Vonette House Plans | Home Plans By Archival Designs
83	83	http://www.archivaldesigns.com/home-plans/florence-house-plan	Florence House Plans | European/French | Home Plans By Archival Designs
84	84	http://www.archivaldesigns.com/home-plans/shadow-creek-house-plan	Shadow Creek House Plans | Home Plans By Archival Designs
85	85	http://www.archivaldesigns.com/store/europeanfrench-house-plans-0?items_per_page=12&sort_bef_combin...	European/French House Plans | Home Plans & Styles | Archival Designs
86	86	http://www.archivaldesigns.com/home-plans/old-paces	Old Paces House Plan | Home Plans By Archival Designs
87	87	http://www.archivaldesigns.com/home-plans/hautmoore-house-plan	Hautmoore House Plans | Home Plans By Archival Designs
88	88	http://www.archivaldesigns.com/store/europeanfrench-house-plans-0?items_per_page=12&sort_bef_combin...	European/French House Plans | Home Plans & Styles | Archival Designs
89	89	http://www.archivaldesigns.com/home-plans/tullamaine-house-plan	Tullamaine House Plans | Home Plans By Archival Designs
90	90	http://www.archivaldesigns.com/home-plans/wimbledon-house-plan	Wimbledon House Plans | Home Plans By Archival Designs

The website that the floor plans are being stolen from is www.archivaldesigns.com.

The software that suspect appears to be using to duplicate the floor plans is called Chief Architect Software. This was found using SQLite in the places database under the moz_places folder by searching software as displayed in Figure 19.

FIGURE 19: SUSPECTS SOFTWARE USED FOR DUPLICATION OF FLOOR PLANS



	id	url	title
1	143	https://www.google.com/search?q=architect+design+software&ie=utf-8&oe=utf-8	home design software - Google Search
2	144	https://www.google.com/search?q=architect+design+software&ie=utf-8&oe=utf-8#q=home+designer+soft...	home designer softare - Google Search
3	145	https://www.google.com/search?q=architect+design+software&ie=utf-8&oe=utf-8#q=home+designer+soft...	chief architect software - Google Search
4	146	https://www.google.com/search?q=architect+design+software&ie=utf-8&oe=utf-8#q=chief+architect+soft...	chief architect software - Google Search
5	147	https://www.chiefarchitect.com/	Architectural Home Design Software by Chief Architect
6	148	https://www.google.com/#q=cracking+chief+architect+software	cracking chief architect software - Google Search
7	152	https://www.google.com/search?q=cheif+architect+software+free&ie=utf-8&oe=utf-8	safe keygen sites 2016 - Google Search
8	155	https://www.google.com/search?q=cheif+architect+software+free&ie=utf-8&oe=utf-8#q=safe+keygen+site...	safe keygen sites 2016 - Google Search

Conclusion

The requested information was obtained and documented in this report by the examiner. Using tools such as FTK Imager, FTK, IranView, SQLite and HexEditor contributed to successful findings which should lead to a successful criminal conviction of the suspect being considered.