



Cybersecurity

21.3 The Final Report

Case Report National Gallery DC

Tracy's iPhone [2012-07-15-National-Gallery]

Table of Contents

[Case Report](#)

[National Gallery DC](#)

[Tracy's iPhone \[2012-07-15-National-Gallery\]](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Tracy's iPhone](#)

[Evidence to Establish Personas](#)

[Evidence relating to theft of valuable stamps](#)

[Evidence relating to defacement of museum art](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: WiFi and GPS Location Information](#)

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist the National Gallery, Washington D.C. (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museums are at the NGDC.

- Tracy is a suspect in the aforementioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

Based on all the evidence gathered and displayed below, it appears that Tracy and her brother Pat colluded together with an unknown third party named "King kthings" with the email: throne1966@hotmail.com , to steal the stamps. There is not enough evidence to establish that Tracy had any knowledge of the defacement of museum art, however there appears to be a connection between her and the alleged suspect.

Equipment and Tools

After obtaining the evidence, we used a tool called autopsy to view the contents and display and tag any information we thought was relevant to the investigation

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	iPhone 3G	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/logs

		/lockdownd.log.1
OS Version	IOS 4.2.1 (8C148)	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28 -0700	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log
User Email	tracysumtwelve@gmail.com	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/mobile/Library/AddressBook/AddressBook.sqlitedb
Phone Number	1 (703) 304-9661	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log
Serial Number	86004482Y7H	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log
ICCID	89014103255195342366	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log
IMEI	012021003735398	/img_tracy_phone-2012-07-15-final.E01/vol_vol5/root/Library/Lockdown/activation_records/wldcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	/img_tracy_phone-2012-07-15-final.E01
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	/img_tracy_phone-2012-07-15-final.E01

Evidence to Establish Personas

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy:

Phone Number: (703) 340-9961
Personal Email: tracysumtwelve@gmail.com
Work Email: tracy.sumtwelve@nationalgallerydc.org
Secret Email: coralbluetwo@hotmail.com
Relationship: Accused

Pat:

Phone Number: (571) 308-3236
Email: perrypatsum@yahoo.com
Secret Email: patsumtwelve@gmail.com
Relationship: Tracy's Brother

Terry:

Phone Number: (703) 829-6071
Email: unknown
Relationship: Tracy and Joe's daughter

Joe:

Phone Number: (206) 910-0932
Email: joe.sum.twelve@gmail.com
Relationship: Husband / ex-Husband

Carry:

Phone Number: (202) 725-2124
Email: carrysum2012@yahoo.com
Relationship: Acquaintance with Tracy

After discovering how everyone was connected to each other as well as their contact information, we then created a timeline based on the evidence to see who connects to the crime.

Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

Looking through the evidence of emails and sms communications, the conspirators are Tracy, her brother Pat, as well as a third man named "King kthings" <throne1966@hotmail.com>" (see in Appendix A)

There was one email sent to Pat from "King kthings", detailing what tools he needed to get the job done. As shown below.

```
-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)
```

Figure 1. Needs.txt

July 9th 2012 07:47:58 -0700

Tracy <tracysumtwelve@gmail.com> emailed Coral <coralbluetwo@hotmail.com> an attachment file named documents.zip with the Subject line of "things". Within the attachment, contained 3 pdf files: Stamp Insurance 1.pdf, Stamp Insurance 2.pdf, Stamp Insurance 3.pdf.

After further examination, it was discovered that there was an unzipped file with the title docs.zip, and within were the pdf's, viewable to everyone.

Below are the contents of each pdf:

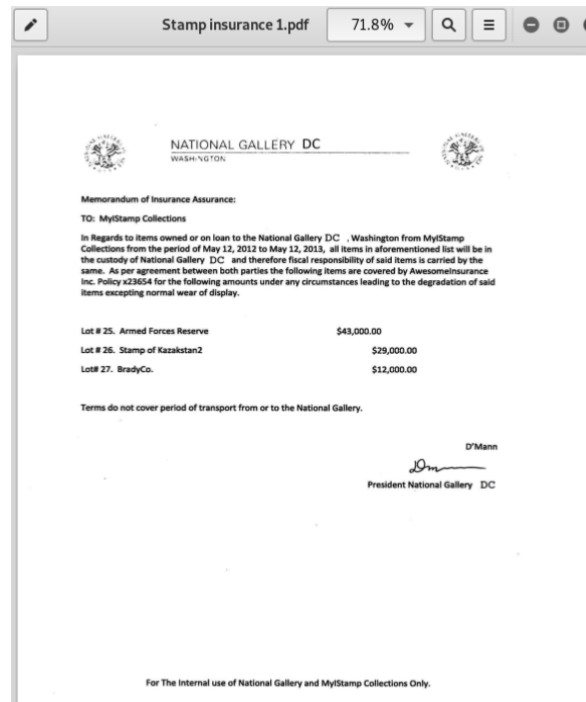


Figure 2. Stamp Insurance 1.pdf

Each Picture below found on her phone corresponds with each item listed in the Insurance

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0056.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0051.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0057.JPG



Figure 3. Stamps mentioned above

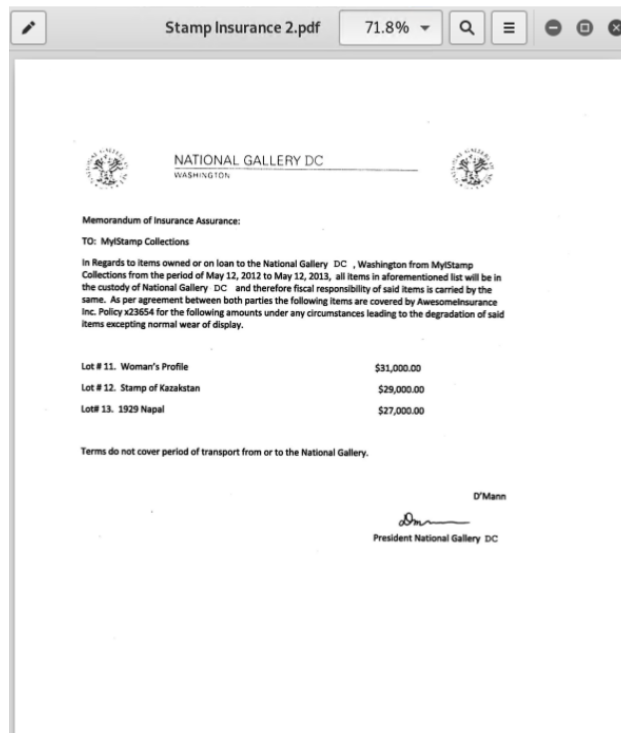


Figure 4. Stamp Insurance 2.pdf

Each Picture below found on her phone corresponds with each item listed in the Insurance

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0067.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0055.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0050.JPG



Figure 5. Stamps mentioned above

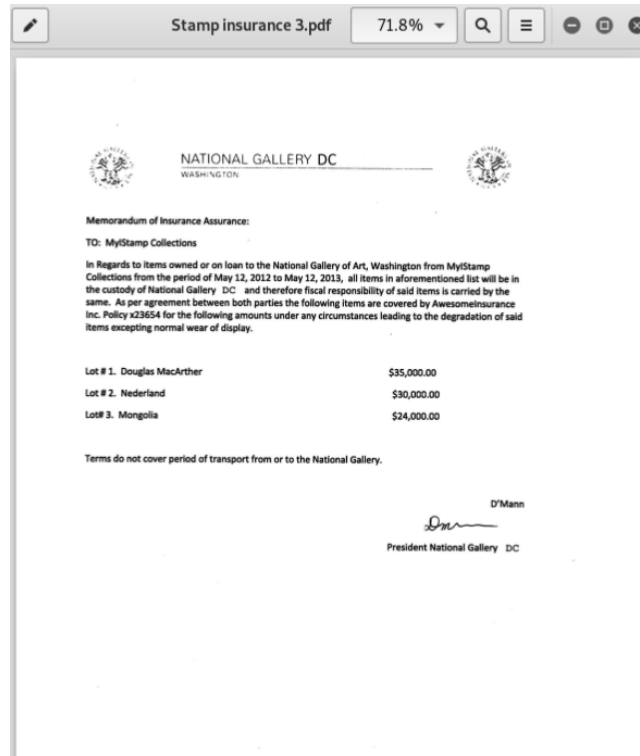


Figure 6. Stamp Insurance 3.pdf

Each Picture below found on her phone corresponds with each item listed in the Insurance

- /vol5/mobile/Media/DCIM/100APPLE/IMG_0054.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0065.JPG
- /vol5/mobile/Media/DCIM/100APPLE/IMG_0071.JPG



Figure 7. Stamps mentioned above

It is privileged information that is not meant to be redistributed outside.

Evidence relating to defacement of museum art

This sub-section provides details regarding the evidence found as it relates to the defacement of museum art.

There is not much evidence on Tracy's phone about the defacement of museum art, however it does show the connection between how Carry got intel on the museum and Tracy, our suspect, as well as the timeline of their communications below.

Email correspondence between Tracy and Carry, found in:

/img_tracy-phone-2012-07-15-final.E01/vol_vol5/\$CarvedFiles/f0408520.plist

As well as within Appendix A.

July 5 2012 11:51:00

Carry contacts Tracy via email.

July 6 2012 10:55:00

Carry and Tracy go out for lunch

July 9th 2012 14:18:00

Carry asks Tracy if she can sneak Carry's tablet into the gallery for her, so she can take pictures for the flash mob event.

July 10th 2012 06:29:00

Tracy emails back saying "I can definitely help get your tablet in. Our security guards can be pretty ridiculous sometimes! When would you want to get in and take a look around?"

July 10th 2012 06:48:40

Carry responds back saying "Awesome this will be a big help. Can I come in tomorrow, around 9?"

July 11 2012 12:41:45

Carry messages Tracy asking where she should meet her.

July 11 2012 12:49:08

Tracy messages Carry telling her to meet at the front and she will take the tablet in for her.

July 12 2012 17:06:45

Tracy messages Carry asking how the flash mob is going.

In conclusion, there is not enough evidence on the phone to tie it to the defacement of museum art, as most of the evidence and images found is mainly related to the theft of the stamps. There is not enough evidence to tie Tracy to the crime of defacement of museum art, she appears to not have any knowledge of the crime, however she did aid in sneaking in a tablet for her friend who is allegedly connected to the crime.

Plot Timeline

- On June 19 2012 at 2:38 pm, Pat <perrypatsum@yahoo.com> sends an email to Tracy <coralbluetwo@hotmail.com> that contains an attachment called Crazydave1.mp3
- On July 5 2012 at 6:16 pm, Carry messages Tracy about meeting at Bubba's Grill for lunch
- On July 7th 2012 at 7:36 pm, Tracy received an unknown spam message, with a link to "www.target.com.trdt.biz" as well as a code to enter "703". The link does not appear to lead anywhere and could have been removed.
- On July 9th 2012 at 7:47 am, Tracy <tracysumtwelve@gmail.com> emailed her secret account <coralbluetwo@hotmail.com> with 3 documents of stamp insurance pdf's.
- On July 10th 2012 at 8:24 am, Pat utilized his secret account <patsumtwelve@gmail.com> forwarded a message to Tracy's secret email <coralbluetwo@hotmail.com> with the email from "king kthings" <throne1966@hotmail.com> with the tools he needed to perform the job.
- On July 11 2012 at 12:49 pm, Tracy messages Carry to meet her out front so that she can bring in the tablet for her.

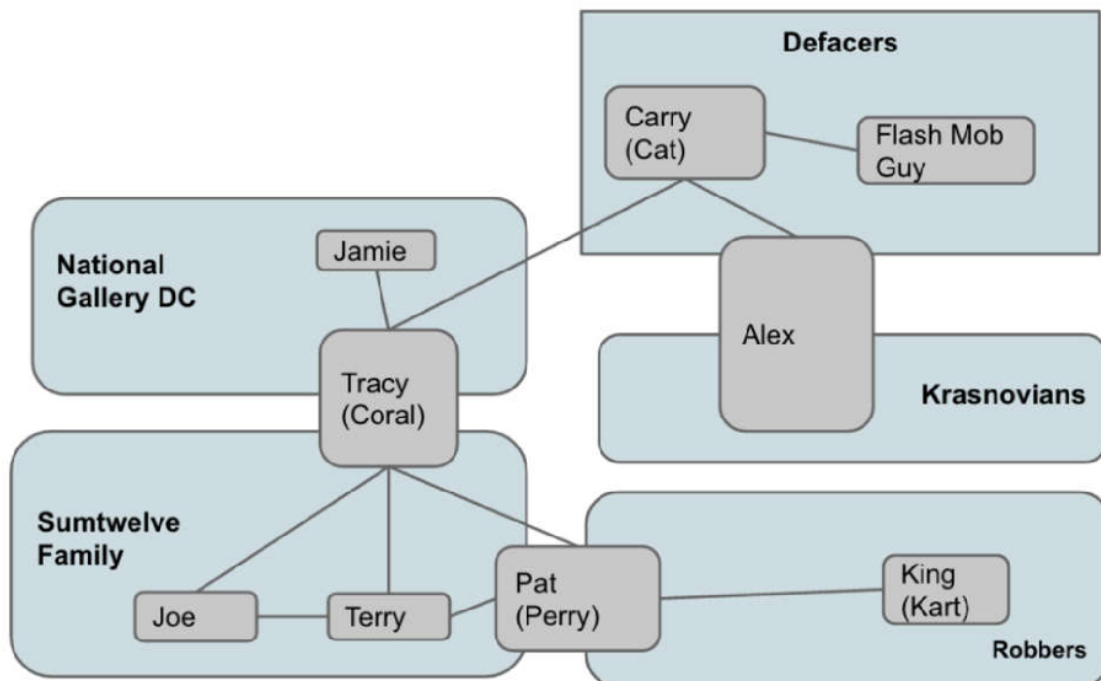


Figure 8. Taken from National Gallery Document - Relationships

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Tracy and Pat colluded with each other using email aliases. Pat utilized the alias <patsumtwelve@gmail.com> while Tracy utilized <coralbluetwo@hotmail.com>. Tracy's original email is <tracysumtwelve@gmail.com>, and Pat's original email is <perrypatsum@yahoo.com>.
- Pat instigated conversation with the unknown third party named "King kthings" with the email <throne1966@hotmail.com> to steal the stamps
- Carry asking Tracy to sneak in a tablet for her to take photos for her flash mob
- Tracy sends the stamp insurance pdf's to her secret email.
- Multiple WiFi and GPS locations, would need to look further to display who was near the museum as well as tie the suspects to each location.

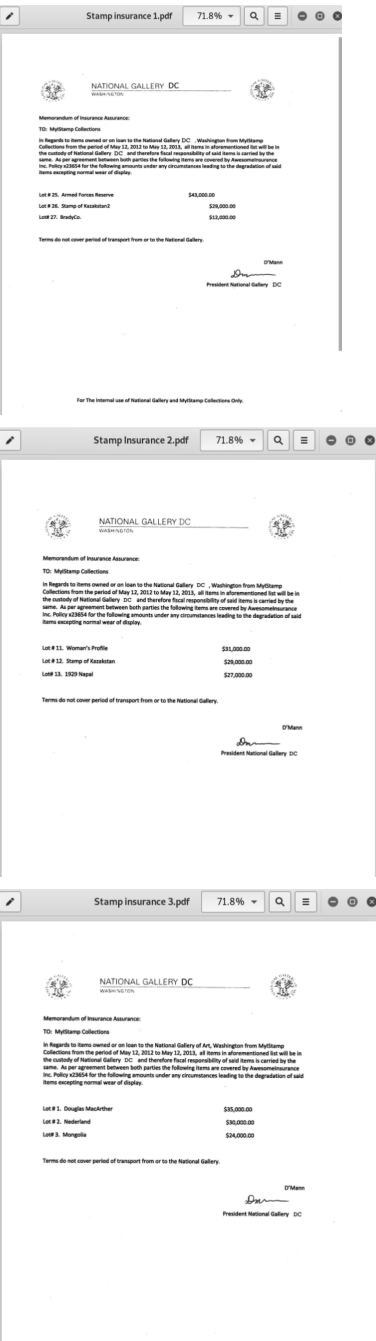
Appendix A: Correspondence Evidence

This subsection will provide an amalgamation of the email and SMS correspondence evidence.

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
SMS Row ID 6	12 Jun 2012 21:25:04	From: (571) 308-3236 (Pat)	What are you up to this weekend?	sms.db
SMS Row ID 7	13 Jun 2012 17:30:28	From: (703) 829-6071 (Terry)	I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. -T	sms.db
SMS Row ID 8	13 Jun 2012 18:30:38	To: (571) 308-3236 (Pat)	I don't have any big plans. How about you?	sms.db
2: 3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx	19 Jun 2012 14:38:59 -0700	Sender IP: 98.138.89.197 From: perrypatsum@yahoo.com To: coralbluetwo@hotmail.com Subject: Crazydave by the VMs	Attachment: Crazydave1.mp3	img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/IMAP-tracysumtwelve@gmail.com@imap.gmail.com/INBOX.imapmb/Messages
SMS Row ID 12	3 Jul 2012 13:41:51	To: (703) 829-6071 (Terry)	Hey honey. I'm not sure if we can afford Prufrock anymore... What do you think about maybe switching to someplace else?	sms.db
SMS Row ID 13	3 Jul 2012	From: (703) 829-6071 (Terry)	moving schools at this point would be the worst! i would	sms.db

	14:04:32		rather live with dad and stay at prufrock then change schools :(
5: F3F4EB95 -52EB-42F C-9279-46 DAB24B6 E34.emlx	5 Jul 2012 12:58:42 -0700	Sender IP: 208.97.132.83 From: Woina.Honril@m57.biz To: coralbluetwo@hotmail.com Subject: Busy	Content: I didn't. Attachment: filename="000001.doc"	img_tracy-phone-2012-07-15-final.E01 /vol_vol5/mobile/Library/Mail/IMAP-tracysumtwelve@gmail.com@imap.gmail.com/INBOX.imapmb/Messages
SMS Row ID 14	5 Jul 2012 18:18:23	From: (202) 725-2124 (Carry)	Sounds good let's shoot for one at Bubba's grill	sms.db
SMS Row ID 15	5 Jul 2012 18:20:26	To: (202) 725-2124 (Carry)	Okay that sounds great. See you there	sms.db
SMS Row ID 16	6 Jul 2012 15:02:19	To: (571) 308-3236 (Pat)	Hey can you give me a call	sms.db
SMS Row ID 17	6 Jul 2012 15:08:37	From: (571) 308-3236 (Pat)	Sis I'm really busy can we can do this later	sms.db
SMS Row ID 18	6 Jul 2012 15:11:54	To: (571) 308-3236 (Pat)	No pat this is important I need you to call me soon	sms.db
SMS Row ID 19	6 Jul 2012 15:13:31	From: (571) 308-3236 (Pat)	Ok ok I'll call in 5	sms.db
SMS Row ID 20	6 Jul 2012 16:27:16	From: (202) 725-2124 (Carry)	I have a table inside	sms.db
SMS Row ID 21	6 Jul 2012 16:27:50	To: (202) 725-2124 (Carry)	Okay brt	sms.db

SMS Row ID 22	7 Jul 2012 19:36:35	From: (206) 910-0932 (unknown)	Congratulations, your entry in last months drawing won you a FREE \$1,000 Target Giftcard! Enter "703" at www.target.com.trdt.biz to tell us where to ship it	sms.db
------------------	---------------------------	-----------------------------------	---	--------

<p>3: 8A3BD06F -CDB1-44 53-9C69-7 7E06823F 2AE.emlx</p>	<p>9 Jul 2012 07:47:58 -0700</p>	<p>Sender IP: 209.85.216.171 From: tracysumtwelve@gmail.com To: coralbluetwo@hotmail.com Subject: things</p>	<p>Attachment: documents.zip</p> <p>Documents.zip:</p> <ul style="list-style-type: none"> - Stamp Insurance 1.pdf - Stamp Insurance 2.pdf - Stamp Insurance 3.pdf 	<p>img_tracy-ph one-2012-07 -15-final.E01 /vol_vol5/mo bile/Library/ Mail/IMAP-tr acysumtwelv e@gmail.co m@imap.gm ail.com/INBO X.imapmb/M essages</p>
---	--	--	--	--

ID 29	2012 18:58:24		dad isn't busy	
1: 01FE9965 -A923-40C F-A78A-72 CE3BD26 571.emlx	11 Jul 2012 04:18:03 -0700	Sender IP: 216.54.194.119 From: microsoft@reply.digitalriver.com To: coralbluetwo@hotmail.com Subject: Free Office training Spam email for training course for office.com	Content: Free Office training course	sms.db
SMS Row ID 30	11 Jul 2012 12:41:45	From: (202) 725-2124 (Carry)	I'm almost there where should I meet you?	sms.db
SMS Row ID 31	11 Jul 2012 12:49:08	To: (202) 725-2124 (Carry)	Just meet me out front, I'll take the tablet in.	sms.db
SMS Row ID 32	12 Jul 2012 17:06:45	To: (202) 725-2124 (Carry)	How's the flashmob going	sms.db
SMS Row ID 33	13 Jul 2012 01:02:10	From: (703) 829-6071 (Terry)	I really want to go to Dad's this weekend. He said he'll take me shopping for school	sms.db

Appendix B: WiFi and GPS Location Information

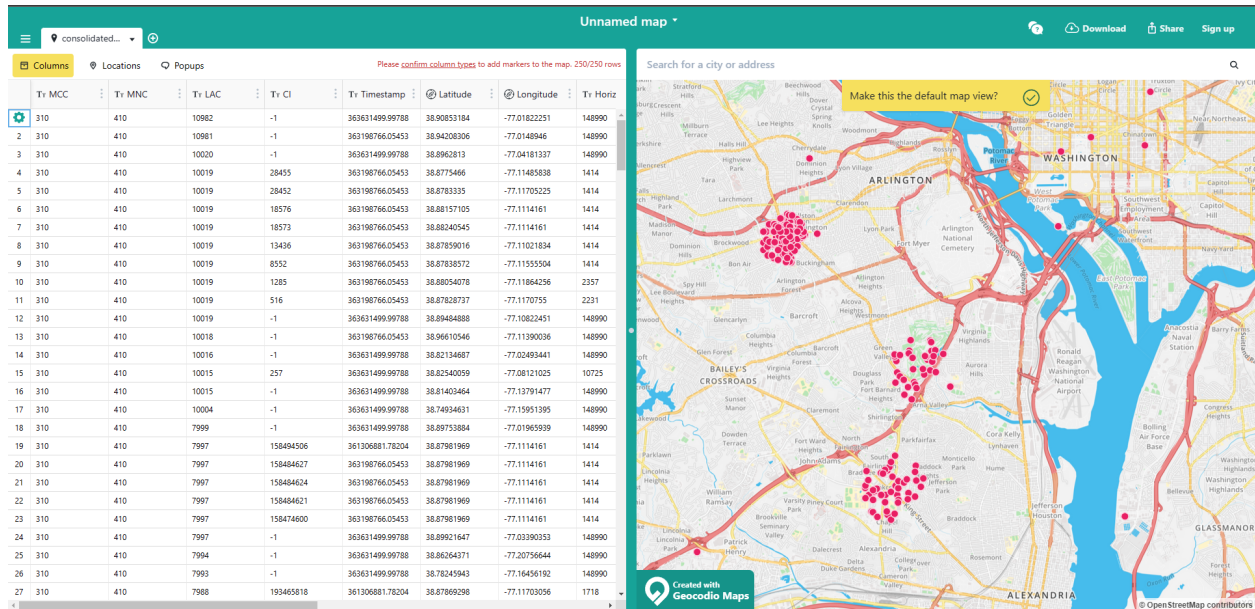


Figure 9. Geo-location data

After checking and inputting the coordinates, we discovered that there were 3 huge clusters, not sure if any have to do with the date or planning of the theft. To find that out we need to delve deeper into those clusters.