Cybersecurity

21.3 The Final Report

Case Report
National Gallery DC

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

Table of Contents

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.

- The evidence indicates that Tracy, utilising the alias Coral was plotting the stamp heist with her brother Pat, that was using the alias Perry
- Evidence of a multitude of emails between Tracy (Coral) and Pat (Perry) contained both images and letters of the National Gallery DC stamps in question.
- LookingHackwards found further evidence of a third associate named "King", who Pat under the alias "Perry" was trying to blackmail King into helping with the heist
- Tracy helped an individual called Carry smuggle the tablet into the gallery.
- The same individual Carry also received comms from Tracy on the National Gallery's security shift schedule.
- This was ultimately motivated by financial gain. .

Equipment and Tools

- Kali Linux
- Autopsy
- SQL
- Google Maps
- Epoch Converter

Details of Tracy's iPhone

Name	Findings	Location in iPhone image file
Model	Iphone 1,2	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/library/logs/AppleSupport/general.log
Host Name	Tracy Sumtwelves iPhone	vol5/mobile/preferences/SystemConfiguration
OS Version	iPhone OS 4.2.1 (8C148)	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/library/logs/AppleSupport/general.log
Install Time	6/6/2012 12:03:28	Vol5/AppleSupport/general.log
User Email	IMAP:tracysumtwelve@gmail.com POP: coralbluetwo@hotmail.com	vol5/mobile/Library/Mail/Envelope.Index
Phone Number	1(703) 340-9661	vol5/logs/lockdownd.log.1
Serial Number	86004482Y7H	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/library/logs/AppleSupport/general.log
ICCID	89014103255195342366	vol5/logs/lockdownd.log.1
IMEI	012021003735398	vol5/root/Library/Lockdown/activation_records/wildcard_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Provided to us
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	Provided to us

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
Relationship:	Accused

Pat:

Phone Number:	571 308 3236
Email:	patsumtwelve@gmail.com
Relationship:	Sister

Terry:

Phone Number:	703 829 6071
Email:	
Relationship:	Daughter

Joe:

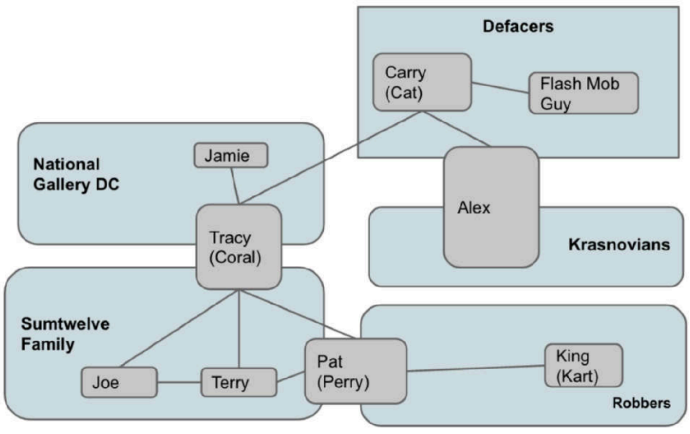
Phone Number:	Unknown
Email:	Unknown
Relationship:	Ex Husband

Carry:

Phone Number:	202 725 2124
Email:	carrysum2012@yahoo.com
Relationship:	Friend

King (Alias)

Phone Number:	Unknown
Email:	throne1966@hotmail.
Relationship:	Criminal contact of Pat



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.
Communications via email and sms collected between Tracy, Pat, and Carry with an attachment from King listing items needed for the robbery.
Needs.txt file found in coralbluetwo@hotmail.com/POP3.live.com/INBOX.mbox/9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx. Needed to be converted to PDF per SMS received on July 11.

-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)

Three insurance letters were found with the values of the stamps, in along with images of the stamps found in Stamp Images found in [/vol5/mobile/Media/DCIM/100APPLE/]

Stamp Insurance 1.pdf

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 25. Armed Forces Reserve	**$43,000.00**
Lot # 26. Stamp of Kazakstan2	**$29,000.00**
Lot# 27. BradyCo.	**$12,000.00**

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

For The Internal use of National Gallery and MyIStamp Collections Only.

IMG_0056

IMG_0067

IMG_0051

Stamp Insurance 2.

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery DC , Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 11. Woman's Profile	**$31,000.00**
Lot # 12. Stamp of Kazakstan	**$29,000.00**
Lot# 13. 1929 Napal	**$27,000.00**

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

For The Internal use of National Gallery and MyIStamp Collections Only.

IMG_0067

IMG_0055

IMG_0050

Stamp Insurance 3.pdf

NATIONAL GALLERY DC
WASHINGTON

Memorandum of Insurance Assurance:

TO: MyIStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MyIStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 1. Douglas MacArther	**$35,000.00**
Lot # 2. Nederland	**$30,000.00**
Lot# 3. Mongolia	**$24,000.00**

Terms do not cover period of transport from or to the National Gallery.

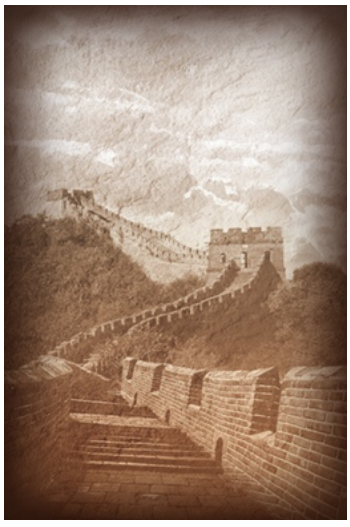
D'Mann

President National Gallery DC

For The Internal use of National Gallery and MyIStamp Collections Only.

IMG_0054

IMG_0065



IMG_0065

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.

-

Plot Timeline

We found evidence in Tracy's phone that confirms the correspondence between Tracy and Carry via SMS communications.

- 7/2/2012 - Pat informs Tracy about the stamp expedition
- Tue Jun 19 2012 02:38PM - Pat emails Tracy with an MP3 audio attachment that contains voice instructions on how to install VirtualBox Virtual Machine on her computer for "later use".
- 7/2/2012 - Tracy informs Pat about the stamp expedition
- Thu Jul 5 2012 06:18:23PM - Tracy & Carry organise a meetup at Bubba's Grill - "Sounds good let's shoot for one at Bubba's grill"
- Fri Jul 6 2012 11:49:31AM - Pat makes an arrangement via email with the email subject "can't pass up" with a proposition with someone that is known as "King", and Tracey.
- Fri Jul 6 2012 04:27:16PM - Tracy and Carry confirm the meeting at Bubba's Grill via SMS.
- Sat Jul 7 2012 07:36:35PM - Tracy receives an SMS from an unknown number that she has won a "FREE $1000 Target Giftcard". We found that the URL was faked to appear like it's actually from Target Corp, by the subdomain and the registration can't be found.
- Mon Jul 9 2012 10:44:11AM - Tracy sends an email to herself explaining which stamps to steal, and how much these stamps are insured for.
- Mon, Jul 9 2012 10:44:11 AM, Pat and King arrange a list of things that King will need to complete the job via email communication
- Tue, Jul 10 2012 11:24 AM, Pat forwards the list of things to Tracy
- Wed, Jul 11 2012 12:41:45 PM, Carry arranges for Tracy to deliver a tablet to Carry
- Thu, Jul 12 2012 05:06:45 PM, Tracy texts Carry to ask how the flashmob is going.

Artifact #	Timestamp	Header Information	Key Information	Evidence Location
#1	Tue, 19 Jun 2012 21:39:04 (UTC)	Pat comms with Tracy F: Perry Patsum perrypatsum@yahoo.com T: Coral Bluetwo coralbluetwo@hotmail.com Subject: Crazydave by the VMs	Hey Coral, Just got your email. That took longer than expected! Oh well! You've got to check out this new song by the VMs. I love the base. Tell me what you think! Attachment Crazydave.mp3	Mail 3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
#2	Fri, 6 Jul 2012 11:49:31	Pat talks to possible henchman From: Patsumtwelve@gmail.com To: throne1966@hotmail.com CC: coralbluetwo@hotmail.com	An Email exchange from Pat to a man called "King" with Alex CC'd in the email. The email reads, "King, Long time no see … I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole officer go years back. He is a strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, i feel he wouldn't be too happy. It's very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don't need a search warrant. Well hit me up, You know where to find me."	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
#3	Tue, 10 July 2012 11:24:57	Pat communication with Alex in regards to people carrying out job From: Patsumtwelve@gmail.com To: coralbluetwo@hotmail.com	An email from Pat to Alex in which pat states "Subject: Fwd: can't pass up" "This is what we need to get for the guy that is going to make our job happen". Attached is the forwarded email with the man in question King kthings, stating to Pat "You're too kind… I got you brotha. I need some tools in order to do this job for you. Here are some requirements that i will need:	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

			see attached” Attachment: Needs.txt	
#4	Thursday 5th July 2012 12:58:41	Email from: Woina.Honril@m57.biz email to: coralbluetwo@hotmail.com	Subject: busy body : I didn’t Attachment: 000001.doc & 000002.doc	F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
#5	1341586939 Saturday, July 7, 2012 1:02:19 AM GMT+10:00	Message to Pat (+15713083236)	Hey can you give me a call	sms.db
#6	1341689795 Sunday, July 8, 2012 5:36:35 AM GMT+10:00	+12069100932	Congratulations, your entry in the last months drawing won you a FREE $1,000 Target Giftcard! Enter “703” at www.target.com.trdt.bix to tell us where to ship it	sms.db
#7	1341933979 Wednesday, July 11, 2012 1:26:19 AM GMT+10:00	+15713083236	Hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know	sms.db
#8	1342010948 Wednesday, July 11, 2012 10:49:08 PM GMT+10:00	+12027252124 Message from Carry	Just meet out front I’ll take the tablet in	sms.db
#9	1342112805 Friday, July 13, 2012 3:06:45 AM GMT+10:00	+12027252124 Message from Carry	How’s the flashmob going	sms.db

Conclusion

Evidence found on Tracy's iPhone indicated the following:

- Artifact 1 & 2: Using different email accounts to hide their identities, Tracy and Pat plotted together. Tracy's alias was 'coralbluetwo@hotmail.com', while Pat's was 'patsumtwelve@gmail.com'. Their regular email addresses were 'tracysumtwelve@gmail.com' for Tracy and 'perrypatsum@yahoo.com' for Pat. Email attachment contained a list of things required for the commission of the theft.
- Artifact 6: A 'Gift Card' for $1000 was the message of an SMS sent to Tracy. It might be from Alex or from Carry through Alex. The website URL as its domain is set to be from Target, but it is actually in the trdt.biz domain. Nothing is known about that URL yet.
- Artifact 7: Tracy sent herself documents with insurance values of the stamps. Total value of $260,000.00.
- Artifact 1 & 2: Pat teamed up with a criminal 'King', who had the email address 'throne1966@hotmail.com', to snatch some rare stamps. Pat could manipulate King because he knew King's parole officer.
- Artifact 8 & 9: Carry plans to stage a flashmob at the museum. This way, he can divert the attention of the security guards while King steals the artifact. There is also mention of a Notepad
- Artifact 5: Evidence of communication between Pat & Tracy

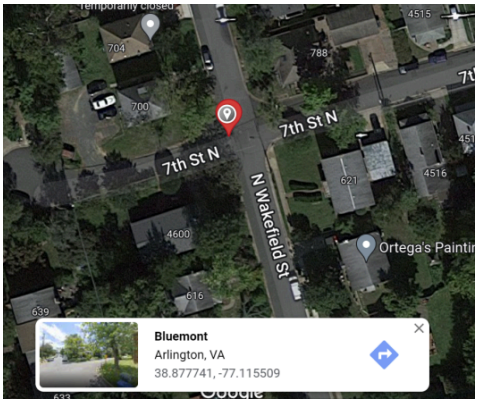
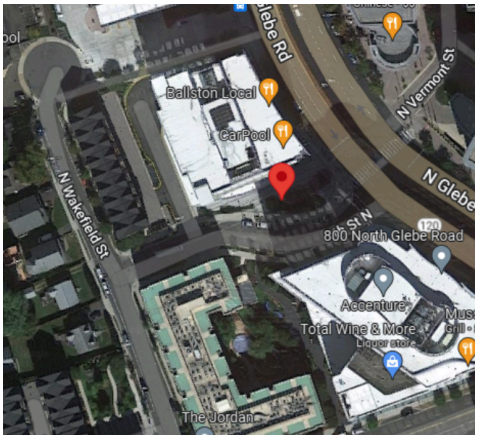
Appendix A: Correspondence Evidence

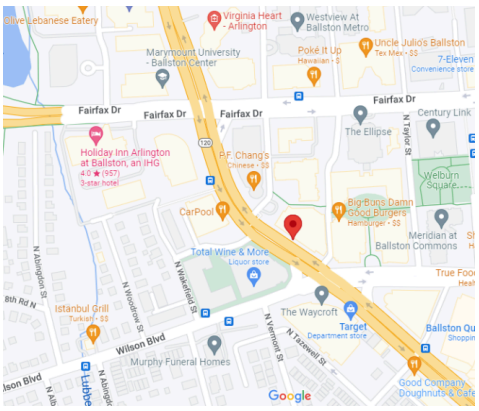
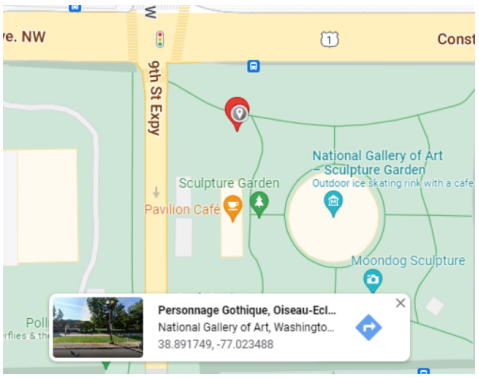
Artifact #	Timestamp	Header Information	Key Information	Evidence Location
#1	Fri, 6 Jul 2012 11:49:31	Pat talks to possible henchman From: Patsumtwelve@gmail.com To: throne1966@hotmail.com CC: coralbluetwo@hotmail.com	An Email exchange from Pat to a man called “King” with Alex CC’d in the email. The email reads, “King, Long time no see … I have a juicy proposition for you. Two weeks from now, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. Me and your parole officer go years back. He is a strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, i feel he wouldn’t be too happy. It’s very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you’re on parole, the feds don’t need a search warrant. Well hit me up, You know where to find me.”	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx
#2	Tue, 10 July 2012 11:24:57	Pat communication with Alex in regards to people carrying out job From: Patsumtwelve@gmail.com To: coralbluetwo@hotmail.com	An email from Pat to Alex in which pat states “Subject: Fwd: can’t pass up” “This is what we need to get for the guy that is going to make our job happen”. Attached is the forwarded email with the man in question King kthings, stating to Pat “You’re too kind… I got you brotha. I need some tools in order to do this job for you. Here are some requirements that i will need: see attached”	9F0508B8-04FB-490E-A7F0-3E23B0E7C59B.emlx

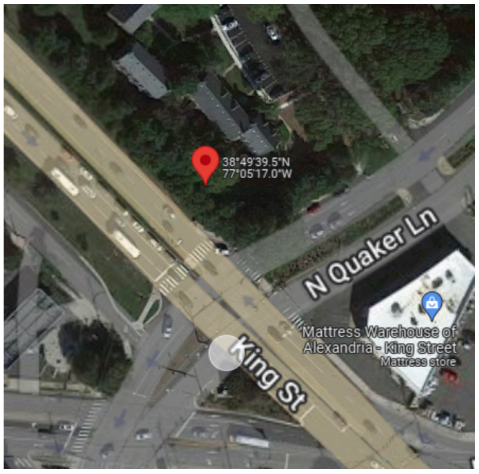
#3	Tue, 19 Jun 2012 21:39:04 (UTC)	Pat comms with Tracy F: Perry Patsum perrypatsum@yahoo.com T: Coral Bluetwo coralbluetwo@hotmail.com Subject: Crazydave by the VMs	Hey Coral, Just got your email. That took longer than expected! Oh well! You've got to check out thnonis new song by the VMs. I love the base. Tell me what you think! Attachment: Crazydave.mp3	Mail 3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
#4	Thursday 5th July 2012 12:58:41	Email from: Woina.Honril@m57.biz email to: coralbluetwo@hotmail.com	Subject: busy body : I didn't Attachment: 000001.doc & 000002.doc	F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx
#5	1341586939 Saturday, July 7, 2012 1:02:19 AM GMT+10:00	Message to Pat (+15713083236)	Hey can you give me a call	sms.db
#6	1341689795 Sunday, July 8, 2012 5:36:35 AM GMT+10:00	+12069100932	Congratulations, your entry in the last months drawing won you a FREE $1,000 Target Giftcard! Enter "703" at www.target.com.trdt.bix to tell us where to ship it	sms.db
#7	Monday July 9th: 10:44:11 UTC	F:tracysumtwelve@gmail.com T: coralbluetwo@hotmail.com Subject: things	Somethings. Attachments documents.zip	8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emailx
#8	1341933979 Wednesday, July 11, 2012 1:26:19 AM GMT+10:00	+15713083236	Hey sis yo friend coral got a email the attachment needs to be changed to pdf let her know	sms.db
#9	1342010948 Wednesday, July 11, 2012 10:49:08 PM GMT+10:00	+12027252124 Message from Carry	Just meet out front I'll take the tablet in	sms.db

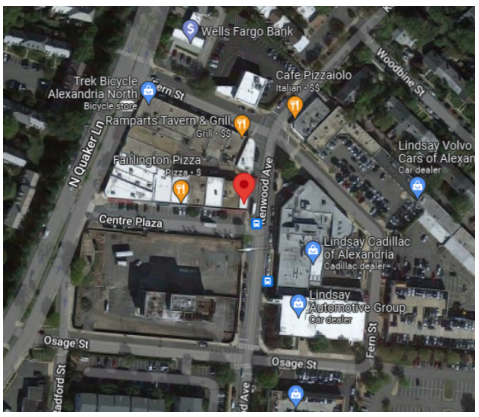
#10	1342112805 Friday, July 13, 2012 3:06:45 AM GMT+10:00	+12027252124 Message from Carry	How's the flashmob going	sms.db

Appendix B: WiFi and GPS Location Information

Location Information				
Artifact #	Time Stamp	Header Information	Body	Map Screenshot
1	Wednesday, June 13, 2012 3:01:21 PM GMT-4:00	Cell Location: 38°52'39.6"N 77°06'55.7"W	703 N Wakefield St, Arlington, VA 22203	
2	Wednesday, June 13, 2012, 7:01:21 PM GMT-04:00	Wifi Location: 38°52'50.0"N 77°06'55.9"W	703 N Wakefield St, Arlington, VA 22203	
3	Monday, July 2, 2012 12:19:23 PM GMT-04:00	Cell Location: 38°52'51.3"N 77°07'01.6"W	4600 Fairfax Dr, Arlington, VA 22203	

4	Thursday, July 5, 2012, 4:32:47 PM GMT-04:00	Wifi Location: 38°52'49.9"N 77°06'52.0"W	801 N Glebe Rd, Arlington, VA 22203	
5	Sunday, July 8, 2012, 12:33:36 PM GMT-04:00	Cell Location 38°53'30.0"N 77°01'24.6"W	Northwest Washington, Washington, DC 20408	
6	Tuesday, July 10, 2012, 4:31:10 PM GMT-04:00	Cell Location: 38°51'05.1"N 77°04'41.7"W	1700 Army Navy Dr, Arlington, VA 22202	

7	Tuesday, July 10, 2012, 4:31:12 PM GMT-04:00	Wifi Location; 38°50'54.0"N 77°04'55.9"W	2689 24th Rd S, Arlington, VA 22206	
8	Tuesday, July 10, 2012, 4:45:00 PM GMT-04:00	Cell Location: 38°49'37.4"N 77°05'10.0"W	1737 W Braddock Pl, Alexandria, VA 22302	
9	Tuesday, July 10, 2012, 4:45:01 PM GMT-04:00	Wifi Location: 38°49'39.5"N 77°05'17.0"W	4102 36th St S, Arlington, VA 22206	

10	Tuesday, July 10, 2012, 4:46:29 PM GMT-04:00	Wifi Location: 38°49'44.7"N 77°05'05.1"W	1701 Centre Plaza, Alexandria, VA 22302	

Cluster Map of Comms Locations