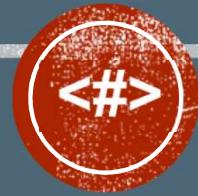




VENEMY

A Collection and Intelligence Tool for Venmo

Bsides Charleston | November 2019



```
root@ubuntu:~/bsides_charleston_2019# _
```

Michael - @mportatoes

- Red Team Operator at Millennium Corporation
 - Boss wrote RTFM
- Featured in the Raspberry Pi magazine suite (3x), has presented at CPV @ Defcon 27, Shmoocon XV, Cyphercon, and many other conferences
- OSCP, OSWP, CISSP, CEH, CRISC, Sec+, BS & MS from Auburn
- Enjoys CTFs, arcade games, maker culture, and dance parties w/ my toddler

Neal - @Shad0\\`Rec0n

- Senior Analyst
- CISSP, Sec+, Net+, CEH
- Husband, Father, Recon Marine
- TraceLabs Missing Person CTF Winner (2x incl. Defcon 27), DerbyCon VIII SECTF 3rd Place

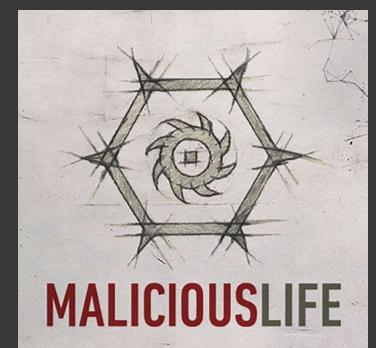
VENMO IN THE NEWS

- The EFF and Mozilla published an open letter to PayPal to fix Venmo's privacy holes (Aug. 2019)
- Mozilla launched a campaign to make transactions private by default (2018)
- publicbydefault.fyi – research on public transactions by Hang Do Thi Duc (2018)
- Vicemo (defunct, 2015) – Who is buying drugs, booze, and sex on Venmo
- “Security Research of a Social Payment App” (2014) – MIT grads

Data tells Stories



Shout out





Kari Smith paid Robert Brestan

Passport

Like · April 8



Leave a comment...

Travel?



Kari Smith paid Robert Brestan
Passport
Like · April 8



Leave a comment...

Travel?



Robert Brestan paid KayBee Photos
30% deposit for Robert & Kari Invoice ID: 158
Like · September 26

♥ KayBee Photos likes this.



Leave a comment...

Getting Married?



Kari Smith paid Robert Brestan
Passport
Like · April 8



Leave a comment...

Travel?

Getting Married?



Robert Brestan paid KayBee Photos
30% deposit for Robert & Kari Invoice ID: 158
Like · September 26

♥ KayBee Photos likes this.



Leave a comment...



Lenai Larkin paid Ted Frieden
Happy bday! We love u!
Like · 12 minutes ago

♥ Chris Dunnigan likes this.



Dolyn Hall: Happy birthday Ted!! Cool
Transaction!!
55 seconds ago

Birthday?

Roommates?

< Payment

Matt Johann paid Daniel Kolinski
Apr 20, 2017 at 3:08 PM Public

Be the first person to like this.

Hailey Davis paid Michael Geary
 Like · December 5, 2017

Leave a comment...

Hailey Davis paid Emily Baker
 Like · November 17, 2017

Leave a comment...

Hailey Davis paid Emily Baker
 Like · November 9, 2017

Leave a comment...

Hailey Davis paid Michael Geary
 Like · November 5, 2017

Leave a comment...

< Payment

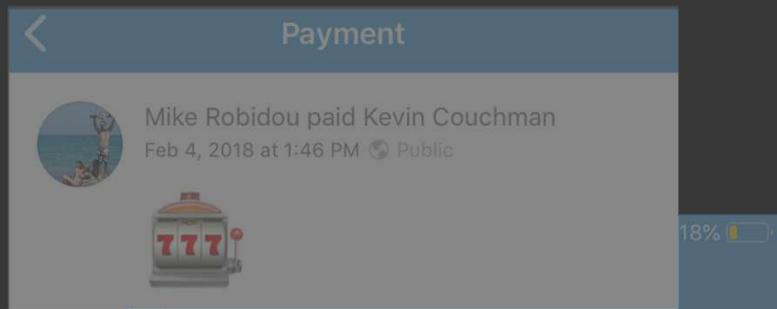
 Mike Robidou paid Kevin Couchman
Feb 4, 2018 at 1:46 PM Public

 18% 

 AS Andy Sukkar paid Mike Robidou
Feb 23, 2019 at 11:08 PM Public

Philly won in OT

Gambling

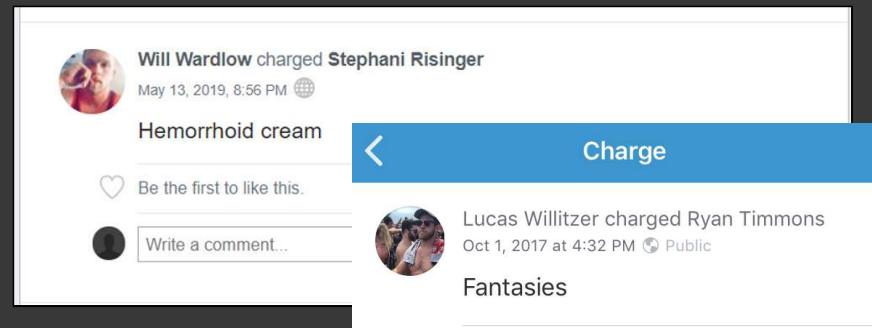
**Payment**

Mike Robidou paid Kevin Couchman
Feb 4, 2018 at 1:46 PM  Public



 Andy Sukkar paid Mike Robidou
Feb 23, 2019 at 11:08 PM  Public

Philly won in OT

**Will Wardlow charged Stephani Risinger**
May 13, 2019, 8:56 PM 

Hemorrhoid cream

 Be the first to like this.

 Write a comment...

**Charge**

Lucas Willitzer charged Ryan Timmons
Oct 1, 2017 at 4:32 PM  Public

Fantasies

**Gerrit Hagen paid Joey Cassaro**
Money laundering services.
Like · September 21

  Leave a comment...

Random?

Relationships

Payment

Mike Robidou paid Kevin Couchman
Feb 4, 2018 at 1:46 PM • Public

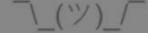


18% 

AS Andy Sukkar paid Mike Robidou
Feb 23, 2019 at 11:08 PM • Public

Philly won in OT

Tillie Simon paid Alec Kirazian
June 6, 2019, 9:02 PM • Public



Be the first to like this.

Write a comment...

Charge

Lucas Willitzer charged Ryan Timmons
Oct 1, 2017 at 4:32 PM • Public

Fantasies

Gerrit Hagen paid Joey Cassaro
Money laundering services.
Like · September 21

Payment

jamie chew paid Stephan Hiser
Jun 6, 2019 at 8:14 PM • Public

child support

Steven Edwards, Aaron Tabackman

Steven Edwards
34s 

Payment

Mike Robidou paid Kevin Couchman
Feb 4, 2018 at 1:46 PM ⚡ Public



18% 

Andy Sukkar paid Mike Robidou
Feb 23, 2019 at 11:08 PM ⚡ Public

Philly won in OT

Tillie Simon paid Alec Kirazian
June 6, 2019, 9:02 PM ⚡



Be the first to like this.

Write a comment...

Charge

Lucas Willitzer charged Ryan Timmons
Oct 1, 2017 at 4:32 PM ⚡ Public

Fantasies

Gerrit Hagen paid Joey Cassaro
Money laundering services.
Like · September 21

Payment

jamie chew paid Stephan Hiser
Jun 6, 2019 at 8:14 PM ⚡ Public



abigail cetner charged mackenzie hansen
uba
Like · April 29

 Leave a comment...



Lizzie Urda paid mackenzie hansen

May 13, 2019, 8:56 PM

Do u think our constant venmoing back and forth is obnoxious 🤪



Be the first to like this.



Write a comment...



Lizzie Urda paid mackenzie hansen

This is my third time venmoing you in 4 hours

Like · February 26

mackenzie hansen likes this.



Leave a comment...



Lizzie Urda paid mackenzie hansen

Beep beep

Like · February 26

mackenzie hansen likes this.



Leave a comment...



Lizzie Urda paid mackenzie hansen

Pee

Like · February 26

mackenzie hansen likes this.



Leave a comment...

YES

Lizzie Urda paid mackenzie hansen
This is my third time venmoing you in 4 hours
Like · February 26

Leave a comment...

Lizzie Urda paid mackenzie hansen
Been doing it since we started dating
mackenzie hansen likes this

Leave a comment...

Lizzie Urda paid mackenzie hansen
Do u think our constant venmoing back and forth is obnoxious 🥺
May 13, 2019, 8:56 PM

Be the first to like this.

Write a comment...



vs.

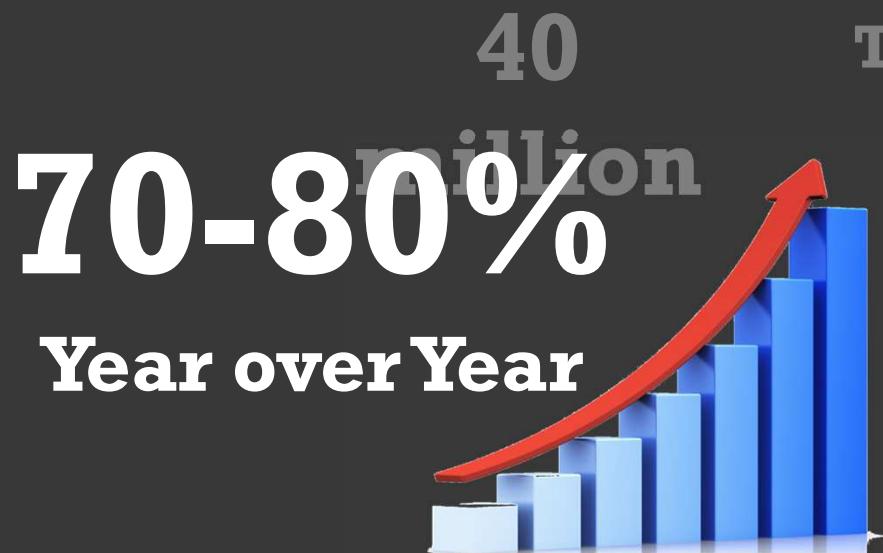


40
million

Total users **267 million**



vs.



Total users

267 million

70-80%
Year over Year



20-25%

Year over Year



vs.



267 million

20-25%
Year over Year





\$100,000,000,000



vs.



\$60

\$300

Per transaction



Information

?



Intelligence

BITE
ME

A large, stylized red logo with the words "BITE" and "ME" stacked vertically. A thick, curved red line starts from the top of the letter "B" in "BITE", loops around the bottom of the "T", then loops back up around the bottom of the "M" in "ME". The entire logo has a textured, grainy appearance.

SECURITY USE CASES

- Red Teams:
 - Reconnaissance
 - Spear-phishing scenarios
- Blue Teams:
 - Pro-active defense, personnel exposure
- Counter-Intelligence/Law Enforcement:
 - Building a social network of baddies
 - Identifying illicit transactions
- Personal
 - TraceLabs Missing Persons CTF
 - Identifying bots/baddies on other social media e.g. dating



DISCLAIMER



- Please use this for being an infosec hero
- Use at your own risk
- Not responsible for misuse
- Slides will be released; however, examples shown herein will be removed before public release

HOW 'BOUT THAT CODE?

- <https://github.com/mportatoes/venemy>
- Written in python3, native libraries
- Authenticated and Unauthenticated modules
- Installation and sample analysis can be found in the repo
- Neo4j used for graph analysis (see slide 33)

WHAT CAN WE GET?

- Authenticated:
 - Friends list, friend of a friend (FOAF)
 - Access to more API endpoints
 - All previous transactions
 - Timestamps, transaction ID, parties involved, item/description, profile pictures (w/possible link to Facebook), “Likes”/Comments
- Unauthenticated:
 - Last five transactions
 - Timestamps, transaction ID, parties involved, item/description, profile pictures (w/possible link to Facebook), “Likes”/Comments

PRIVATE VS PUBLIC

- Authenticated:

- API key is issued BEFORE an account is confirmed via email
- API key is valid for 30 minutes
- Can script this for temporary anonymous access

PRIVATE VS PUBLIC

Private Profile (Unauth)

A screenshot of a Venmo profile page for a user named Michael Portera. The profile picture is a placeholder image. The bio says "Only Michael Portera's Venmo friends can see Michael's payments." Below the bio is a "Join Michael on Venmo" button. At the bottom of the page, there is a JSON API response for the user's profile.

```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
data:
  username: "mporter"
  last_name: "Portera"
  friends_count: 43
  is_group: false
  is_active: true
  trust_request: null
  phone: null
  profile_picture_url: "https://s3.amazonaws.com/venmo/no-image.gif"
  is_blocked: false
  id: "████████████████████"
  identity: null
  date_joined: "2018-04-12T01:21:17"
  about: " "
  display_name: "Michael Portera"
  first_name: "Michael"
  friend_status: null
  email: null
```

API call will show the same basic info regardless

Public Profile (Unauth)

A screenshot of a Venmo profile page for a user named Peyton Sherwood. The profile picture is a placeholder image. The bio says "Peyton Sherwood paid Igram The Immigrant Groove for happy birthday!! venmo.com (web) still auto-fills "for"!!!!". Below the bio is a "Join Peyton on Venmo" button. At the bottom of the page, there is a JSON API response for the user's profile.

```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
data:
  username: "peyton"
  last_name: "Sherwood"
  friends_count: 345
  is_group: false
  is_active: true
  trust_request: null
  phone: null
  profile_picture_url: "https://venmopics.appspot.com/u/v2/s/4e0ea0cf-1425-4a9e-aea1-cb3f4981350f"
  is_blocked: false
  id: "████████████████████"
  identity: null
  date_joined: "2011-09-23T17:39:09"
  about: "Venmo rocks"
  display_name: "Peyton Sherwood"
  first_name: "Peyton"
  friend_status: null
  email: null
```

PRIVATE VS PUBLIC

Private Profile (Auth)

This screenshot shows a private Venmo profile for a user named Michael Portera. The profile includes a placeholder profile picture, a status message indicating membership since November 2017, and a note that the user is friends with the viewer. A sidebar on the right provides options to remove or block the user, and lists mutual friends. Below the profile, a feed section displays recent transactions from other users like Kinsey White, Ingrid Munoz, and Scott Piedmont. A message at the bottom encourages users to use the Venmo app for payment and charging.

API calls reveal all of these details in formatted JSON.

This is for visual purposes only.

Public Profile (Auth)

This screenshot shows a public Venmo profile for Peyton Manning. The profile features a real photo of him, a status message from July 2017, and a note that he has no mutual friends. A prominent "Add Friend" button is highlighted with a red border. Below the profile, a feed section shows transactions between Peyton Manning and Kylie Smith, including a currency exchange and a charge for flights and train tickets. A red arrow points down the page, indicating more content below the visible area.

FRIENDS LIST

- When setting up the mobile application, it will import your contacts and look up those users by their details
 - “*Venmo will use the names, phone numbers, and email addresses of your contacts to friend those that use Venmo, help you invite those that don't, improve your search results and as noted in our Privacy Policy.*”
- If the other party has no social media but uses Venmo, your public profile will show a connection to you
 - Example: Person A isn't friends with shady character, Person B, on any social media but Venmo found his number when importing contacts and now they are connected online

AUTHENTICATED MODULE

```
Command Prompt
python venemy_auth.py -h
usage: venemy_auth.py [-h] [-u USER] [-f FRIENDS] [-t TRANS] [-a ALL]
                      [-c CRAWL] [-p]

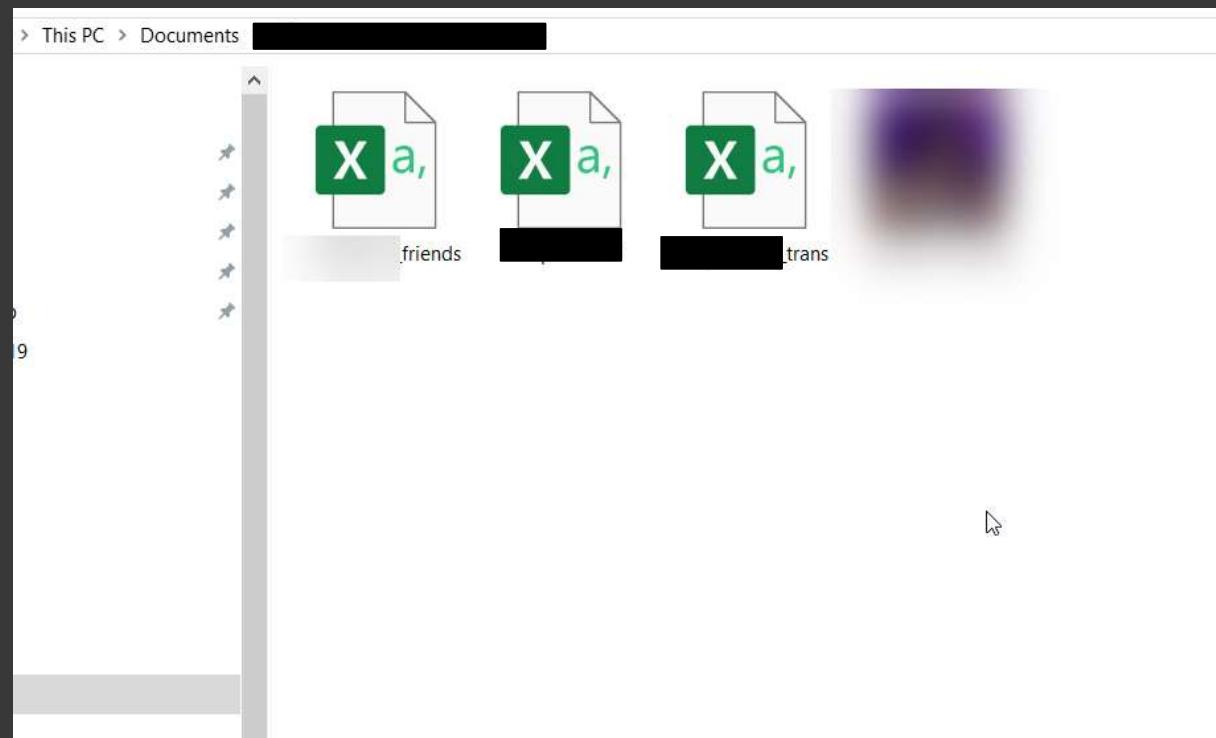
Venemy: An Intel Tool For Venmo - Use at your own risk

optional arguments:
  -h, --help            show this help message and exit
  -u USER, --user USER  Grabs basic info of user
  -f FRIENDS, --friends FRIENDS
                        Get friends
  -t TRANS, --trans TRANS
                        Get transactions of users
  -a ALL, --all ALL    Grab basic info, transactions, and friends of target
                       profile
  -c CRAWL, --crawl CRAWL
                        Crawl one level of friends (foaf) - this is incredibly
                        noisy!!! See README before running
  -p, --pics           Download user's public photos

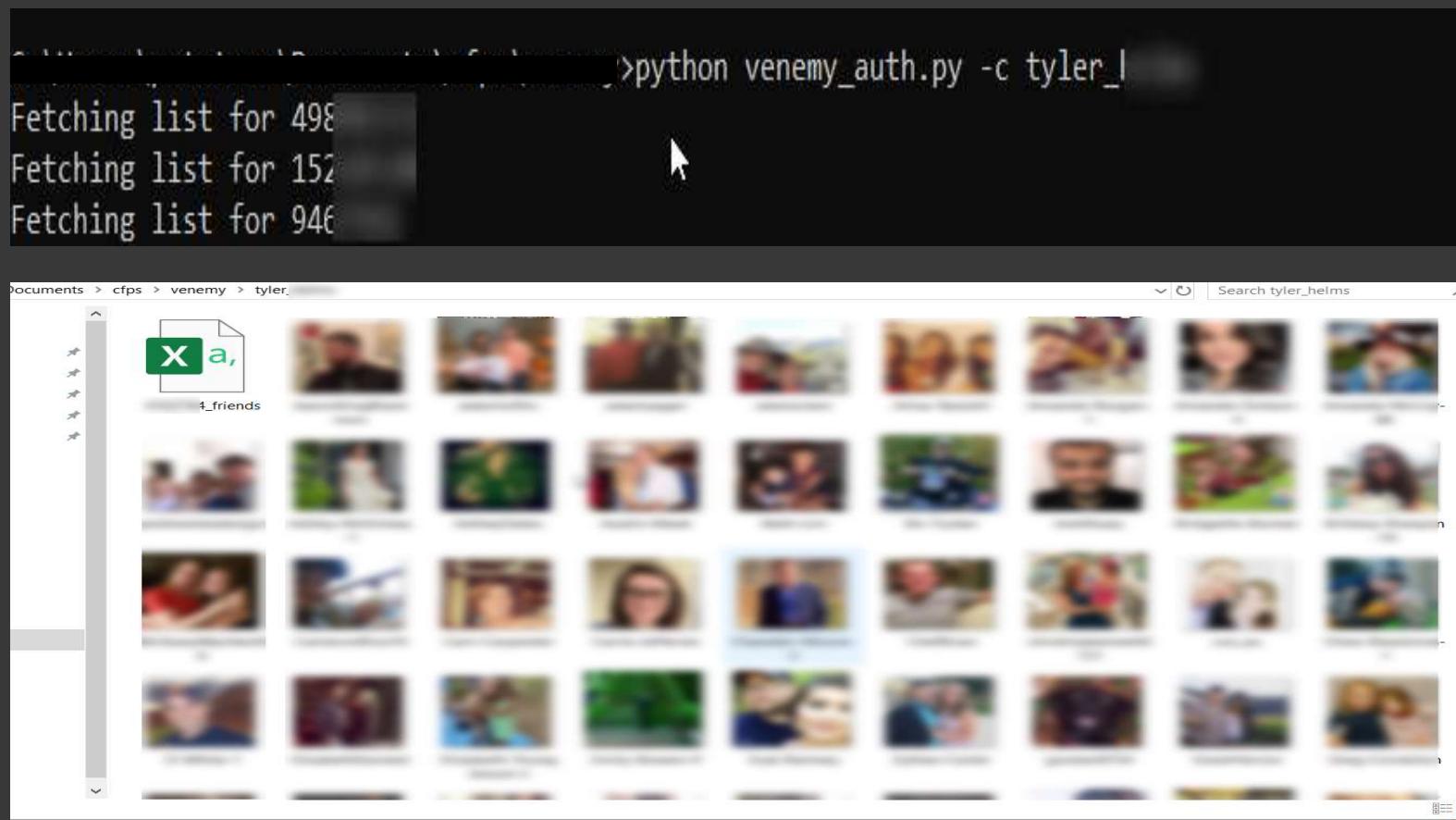
C:\Users\potatoes\Documents\cfps\venemy>
```

```
Command Prompt
python venemy_auth.py -a mpotatoes
[+] Data will be output to ./mpotatoes/
[+] Gathering user info...
[+] Gathering friend info...
[+] Gathering transaction info...
```

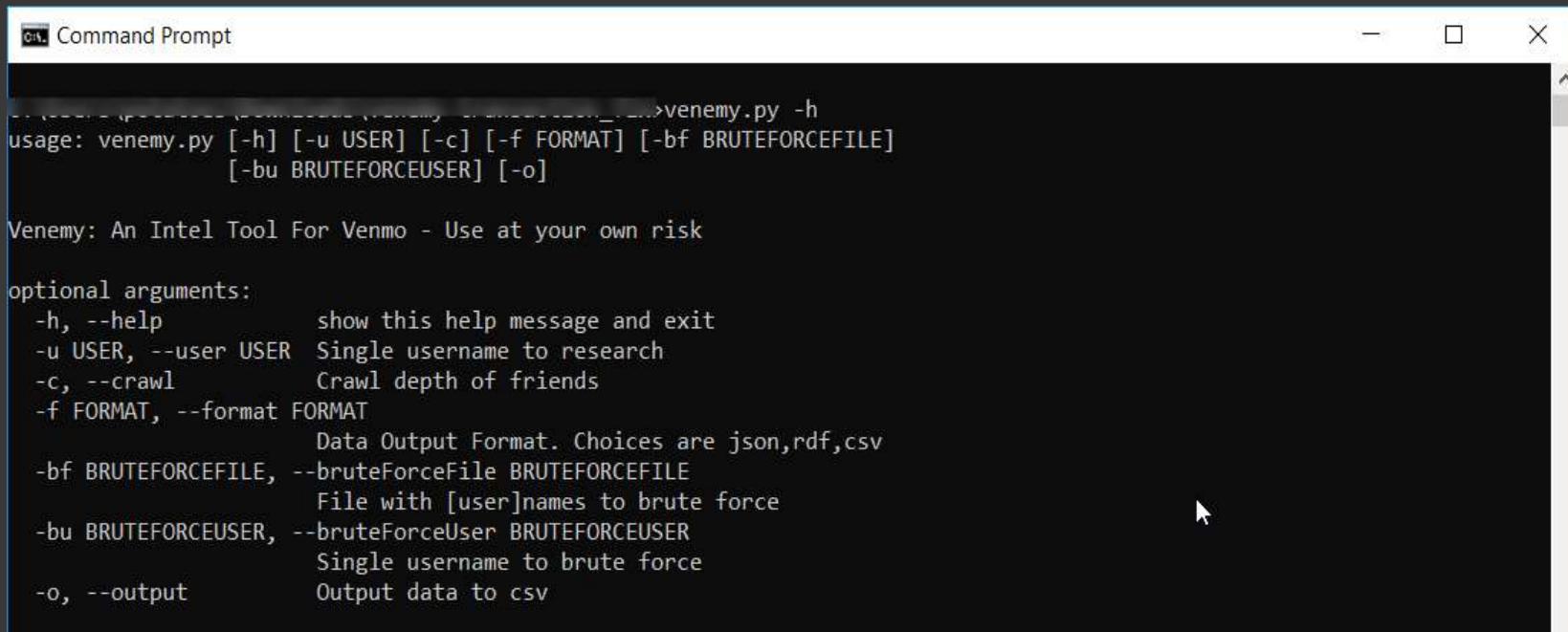
AUTHENTICATED MODULE



AUTHENTICATED MODULE



UNAUTHENTICATED MODULE



A screenshot of a Windows Command Prompt window titled "Command Prompt". The window contains the help output for the "venemy.py" tool. The text is as follows:

```
venemy.py -h
usage: venemy.py [-h] [-u USER] [-c] [-f FORMAT] [-bf BRUTEFORCEFILE]
                  [-bu BRUTEFORCEUSER] [-o]

Venemy: An Intel Tool For Venmo - Use at your own risk

optional arguments:
  -h, --help            show this help message and exit
  -u USER, --user USER  Single username to research
  -c, --crawl           Crawl depth of friends
  -f FORMAT, --format FORMAT
                        Data Output Format. Choices are json,rdf,csv
  -bf BRUTEFORCEFILE, --bruteForceFile BRUTEFORCEFILE
                        File with [user]names to brute force
  -bu BRUTEFORCEUSER, --bruteForceUser BRUTEFORCEUSER
                        Single username to brute force
  -o, --output          Output data to csv
```

ANALYSIS WITH NEO4J

- Neo4j Graph Database
- Neo4j community edition is fully-featured and FREE
- FREE training materials and FREE certification
- Cypher Query Language
- InfoSec projects:
 - Bloodhound
 - ODIN
 - Vulnerability and Exploit Research (Analysing RPC w/ Ghidra and Neo4j)

ANALYSIS WITH NEO4J

- Cypher is derived from SQL and uses ASCII-Art to represent patterns

(**a**)**-[:friends_with]->(b)**

- Sample:

CREATE NODES:

1. CREATE (**a:Person** {Name: "Michael"})
2. CREATE (**a:Person** {Name: "Neal"})

CREATE RELATIONSHIP:

1. MATCH (**a:Person** {Name: "Michael"})
MATCH (**b:Person** {Name: "Neal"})
CREATE (**a**)**-[:friends_with]->(b)**

ANALYSIS WITH NEO4J

- Accepts CSVs and can even call a URL to load JSON

- CSV:

```
LOAD CSV WITH HEADERS FROM "file:///venmo_person.csv" as row
```

```
MERGE (person:Person {id:row.user})
```

```
ON CREATE SET
```

```
person.ext_id=row.external_id,person.username=row.username,person.name=row.name,person.date_created=row.date_created,person.biz=row.is_business,person.num_friends=person.num_friends,person.pic_url=row.picture_url
```

- Using a URL (json):

```
WITH https://api.shodan.io/shodan/host/search?key=APIKEY&query=net:1.2.3.4/24&page=1 as url
```

```
CALL apoc.load.json(url)
```

```
YIELD value
```

```
UNWIND value.matches as items
```

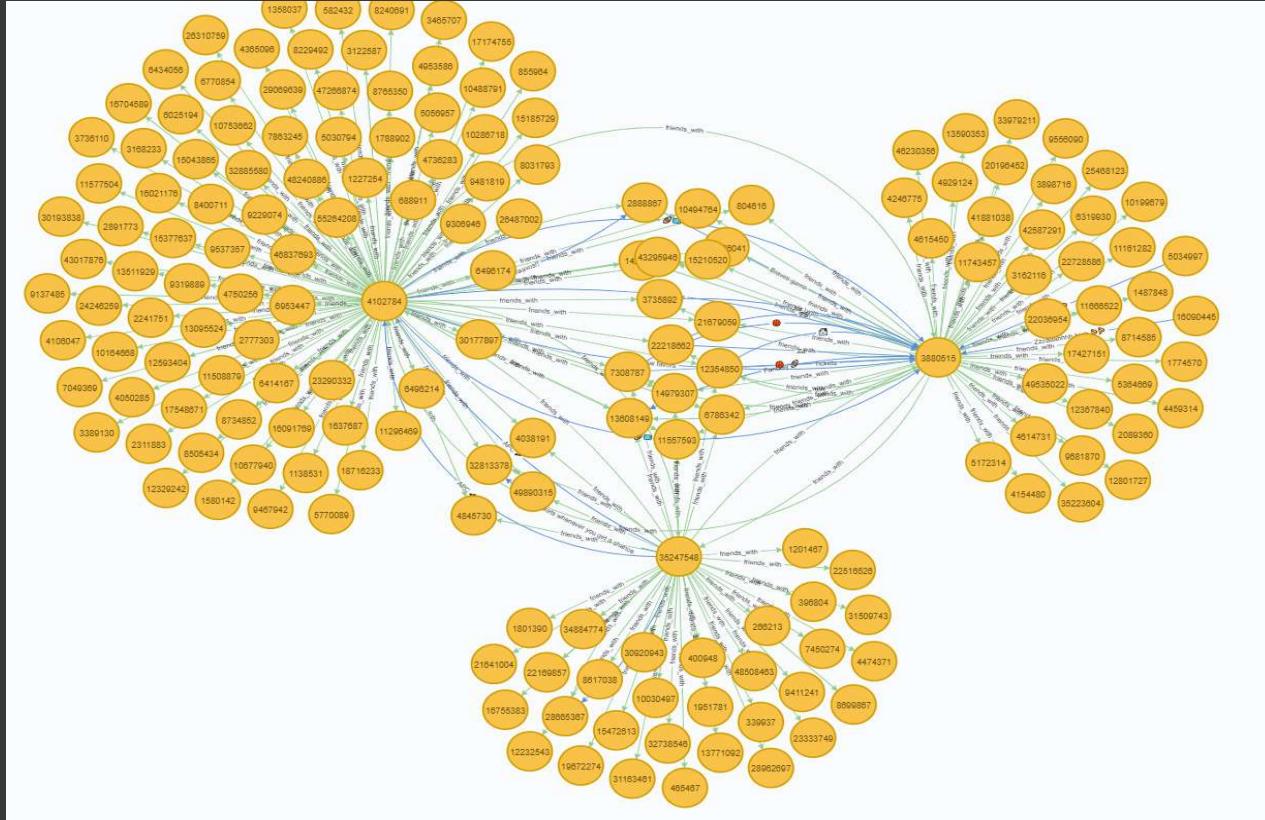
```
MERGE (ip:IP {name:items.ip_str})
```

```
ON CREATE SET ip.tags = items.tags,ip.org=items.org
```

```
MERGE (port:PORT {name:items.port})
```

```
MERGE (ip)-[:hasPort]->(port)
```

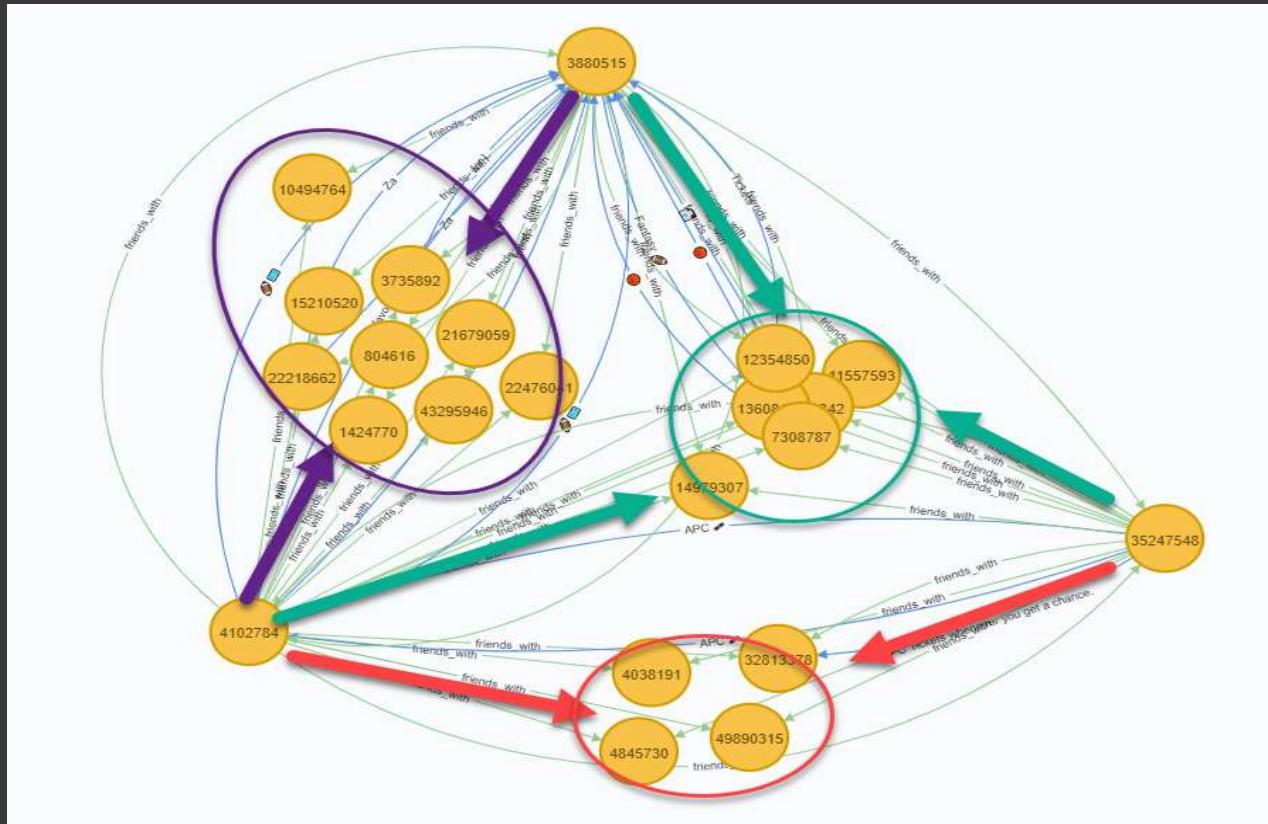
ANALYSIS WITH NEO4J



Query: Match (N) return N

- Sample: Show me everything

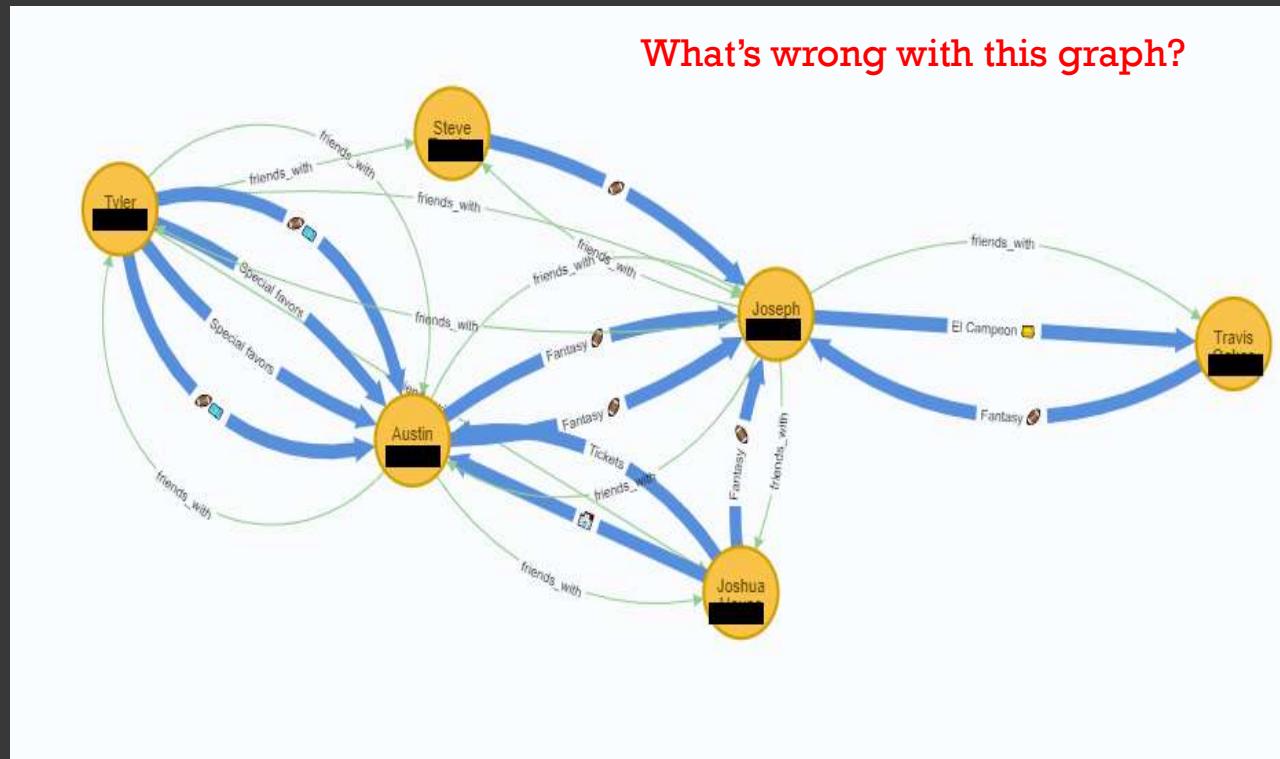
ANALYSIS WITH NEO4J



Query: match (p:Person)-[:friends_with]->(q)<-[friends_with]-(f:Person) RETURN p,q,f

- Sample: Show only common friends between me and/or two of my friends

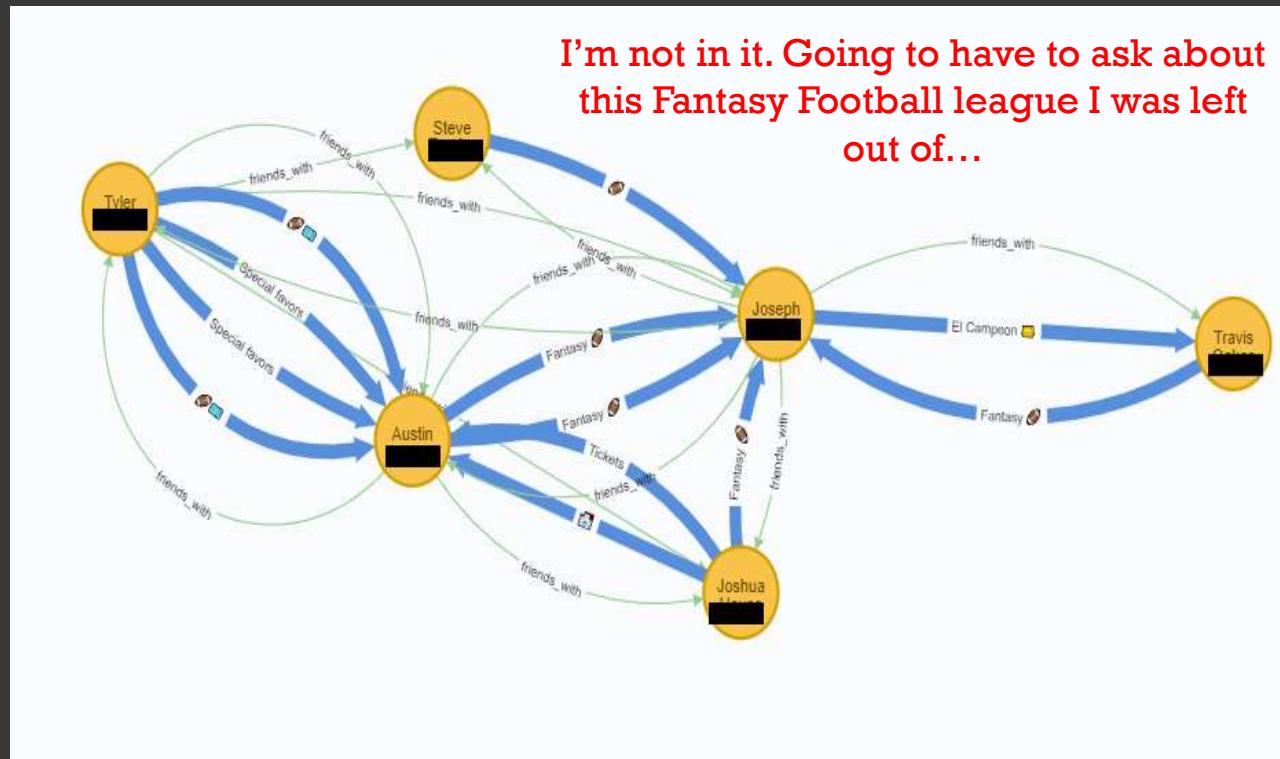
ANALYSIS WITH NEO4J



- Sample:
Show
transactions
of my friends

```
MATCH (p:Person)-[d:paid]->(q:Person) WHERE d.trans =~'.*\u26bd.*' RETURN p,q
```

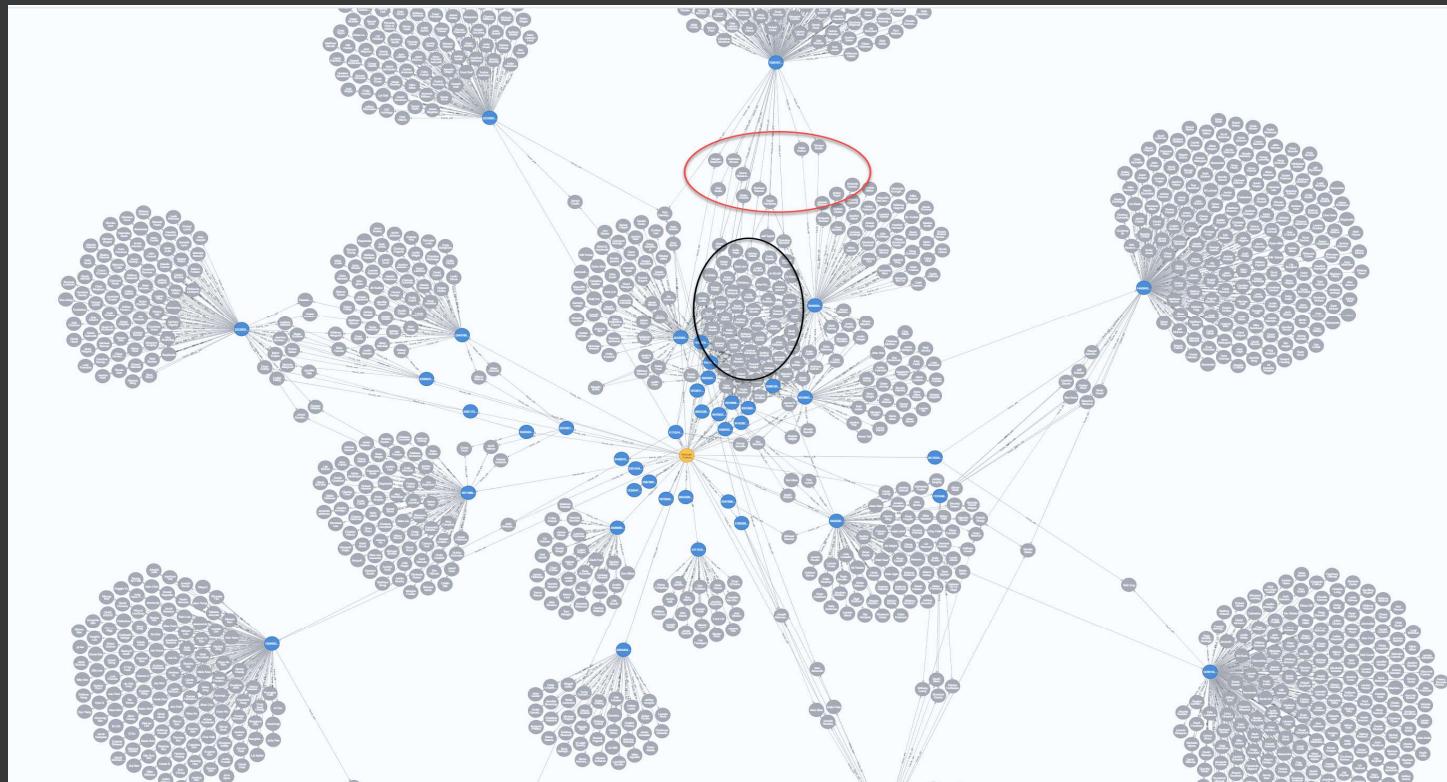
ANALYSIS WITH NEO4J



- Sample:
Show transactions
of my friends

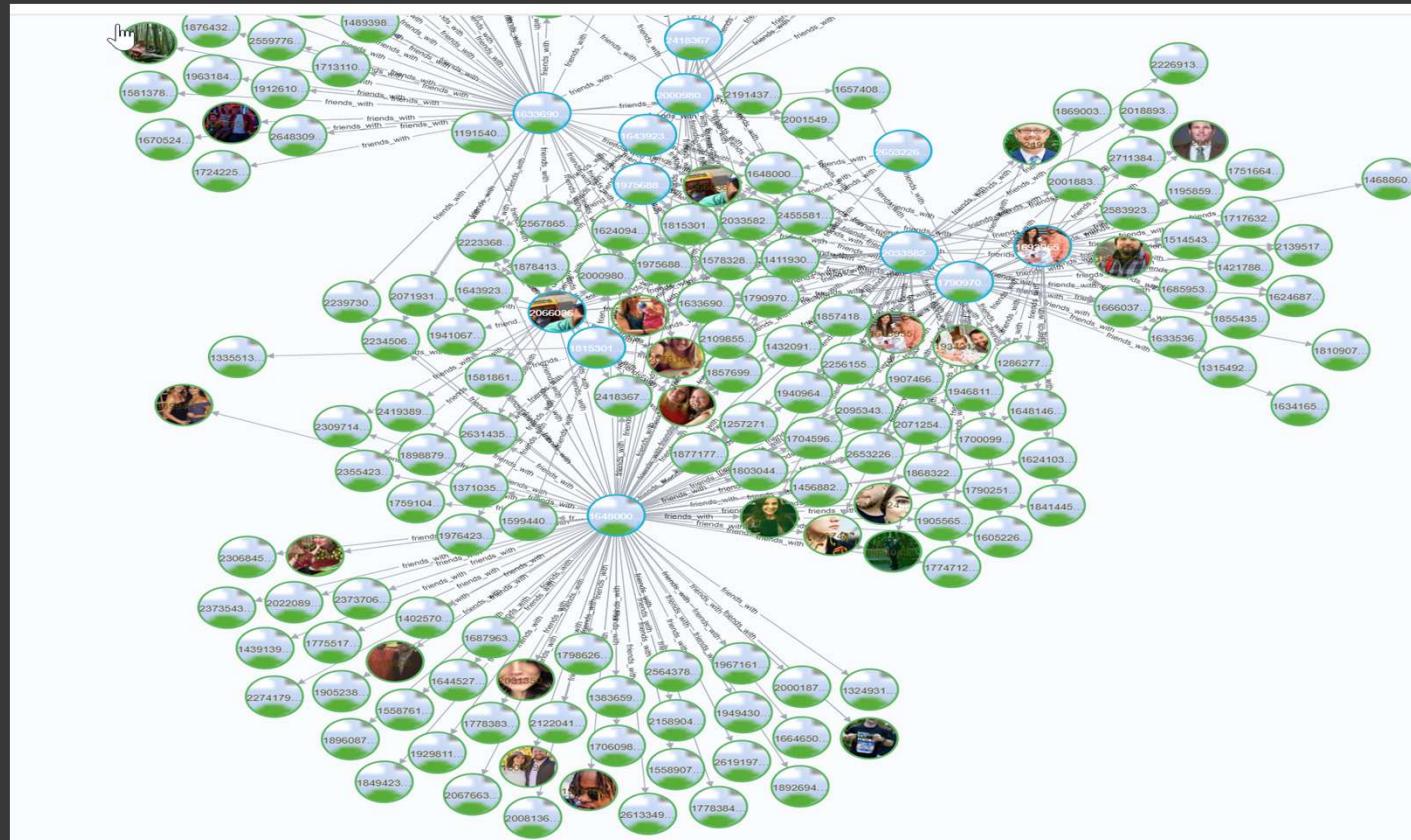
```
MATCH (p:Person)-[d:paid]->(q:Person) WHERE d.trans =~'.*\u26bd.*' RETURN p,q
```

ANALYSIS WITH NEO4J



- Sample: Show the friends of my friends

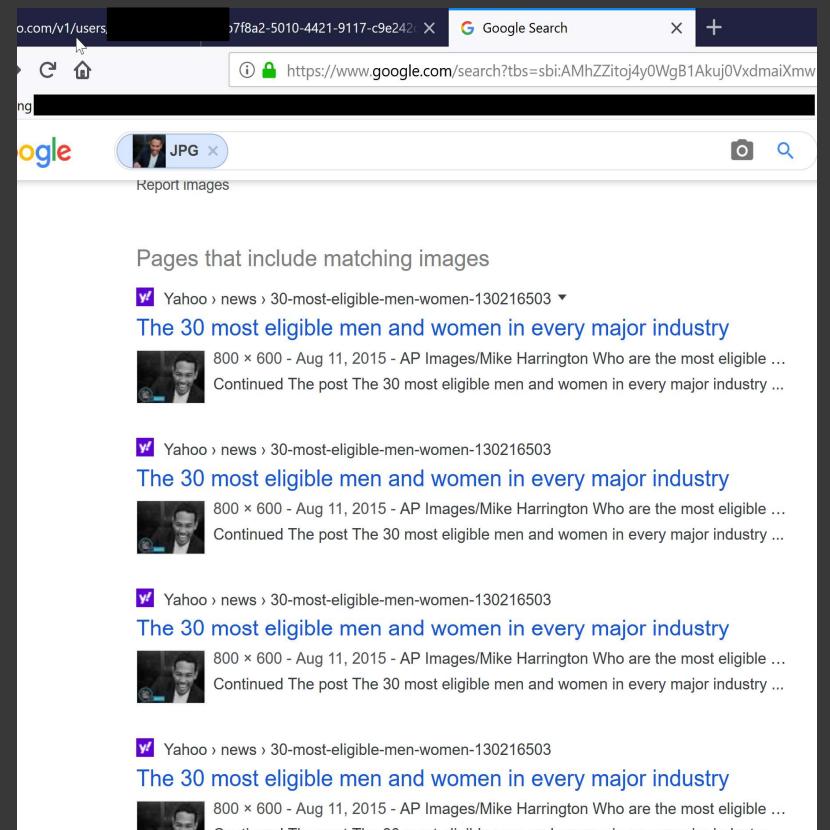
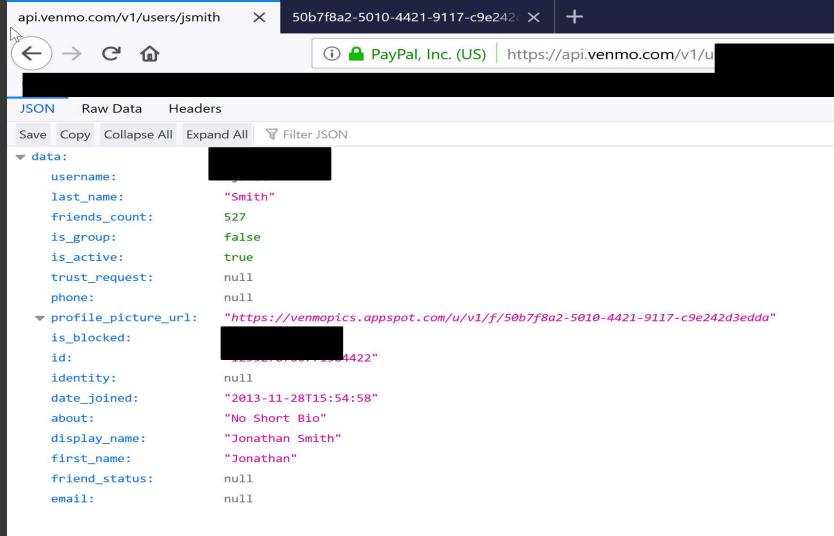
ANALYSIS WITH NEO4J



- Sample: Get fancy with some pictures

EXPANDING OUR OSINT

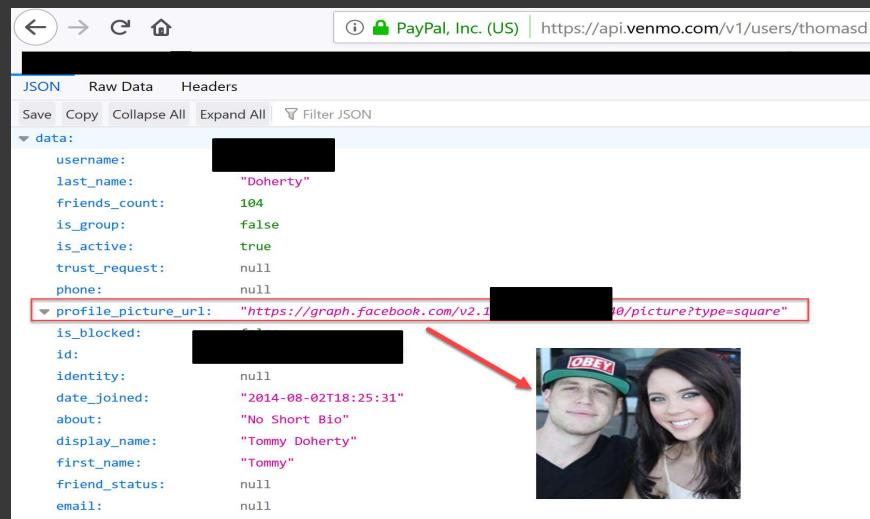
- Reverse image search for more profiles (Google, Tineye, etc)



EXPANDING OUR OSINT

■ Facebook UserID to Email

- Can change picture size via
'picture?type=[square,large,etc]'



```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
data:
  username: [REDACTED]
  last_name: "Doherty"
  friends_count: 104
  is_group: false
  is_active: true
  trust_request: null
  phone: null
  profile_picture_url: "https://graph.facebook.com/v2.1/[REDACTED]/[REDACTED]/picture?type=square"
  is_blocked: false
  id: [REDACTED]
  identity: null
  date_joined: "2014-08-02T18:25:31"
  about: "No Short Bio"
  display_name: "Tommy Doherty"
  first_name: "Tommy"
  friend_status: null
  email: null
```



EXPANDING OUR OSINT

- Username/Name to other profiles

Matthew Gardner charged Stuart Dameron
iPad
on May 5, 2019 at 10:45PM - Comments (0)

Matthew Gardner paid Brian Cantley
Suit
on April 5, 2019 at 04:26PM - Comments (0)

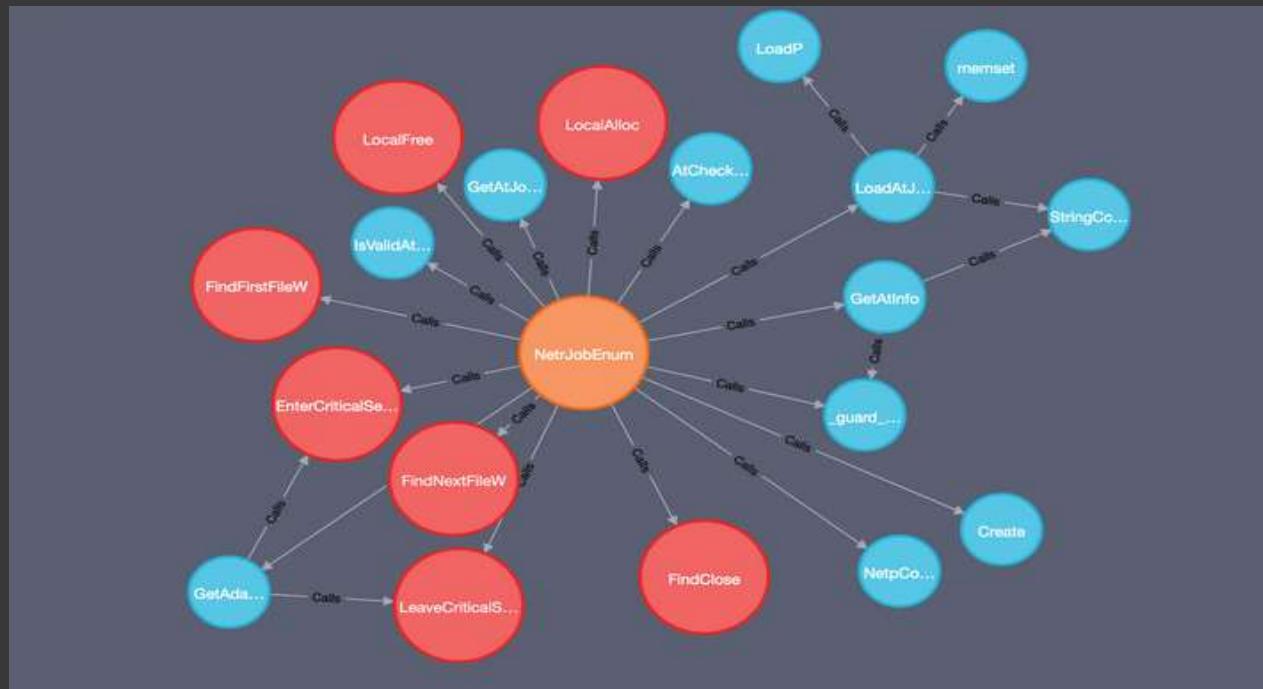
Matthew Gardner Retweeted
The Rose Hoez @Rose_Hoez · Feb 18
Hannah B realizing that she is yet again the runner up to Caelynn #Bachelor #BachelorNation

Matthew G.
563 TOTAL 390 UNIQUE

Matthew G. is drinking a Tiki Talk by Yellowhammer BREWING, INC.

EXPANDING OUR NEO4J

- Red Teams: New TTPs

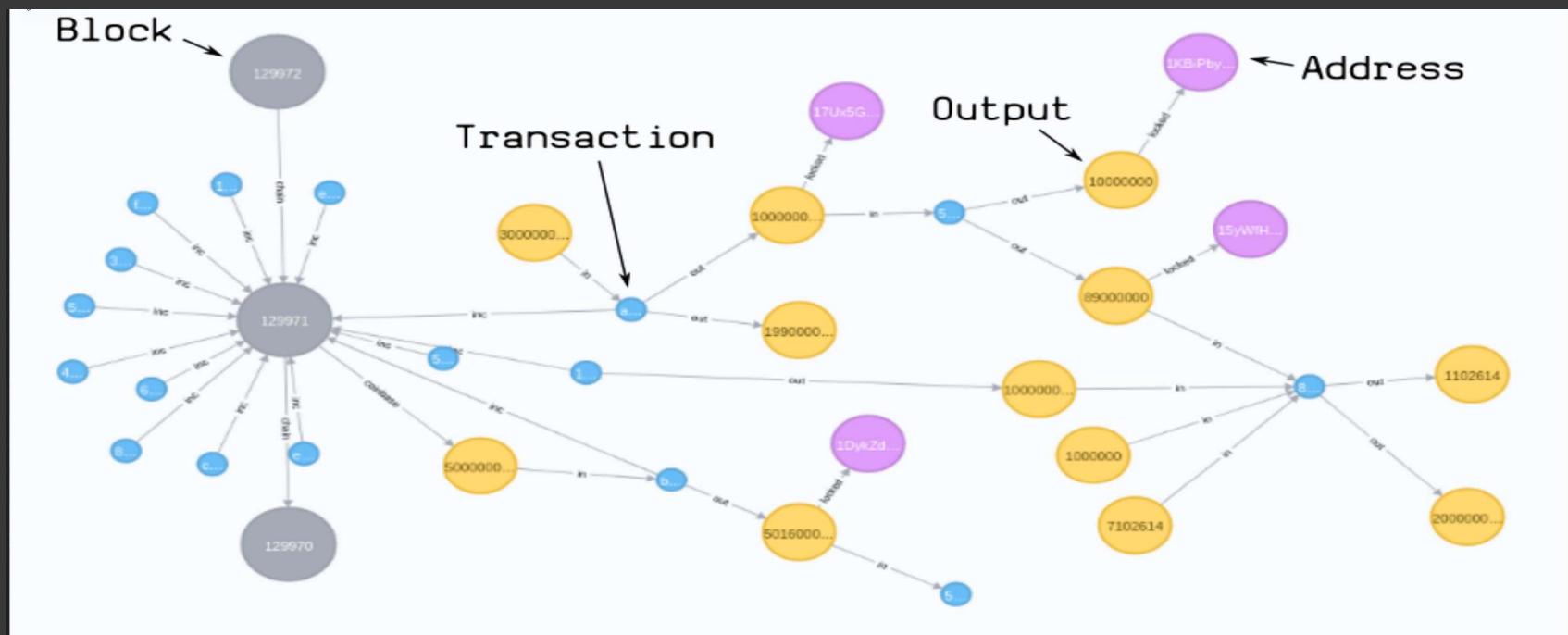


- “Analyzing RPC with Ghidra and Neo4j”
- Analyzing binary functions and calls
- What else?!

Source: <https://blog.xpnsec.com/analysing-rpc-with-ghidra-neo4j/>

EXPANDING OUR NEO4J

- CI/LE: Analyzing bitcoin transactions #followthemoney



Source: <https://neo4j.com/blog/import-bitcoin-blockchain-neo4j/>

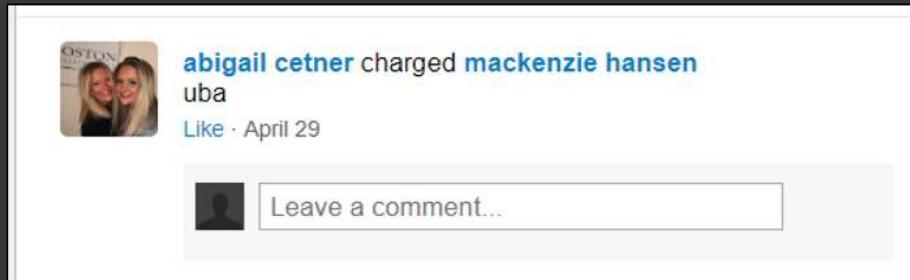
EXPANDING OUR OSINT

- Personal/LE: Trace Labs
 - Find a target's profile on a platform, find their friends
 - Find those friends on other social media and see if they uncover any new profiles pointing back to the target
 - Use input file function from Venemy to brute-force names or collect on known profiles



SAMPLE USE CASE

- Offense: Social Engineering



To: cetner@email.com

From: noreply@ubersupport.tech

"There was an issue with your transaction on April 29...please see the attached or visit <>"

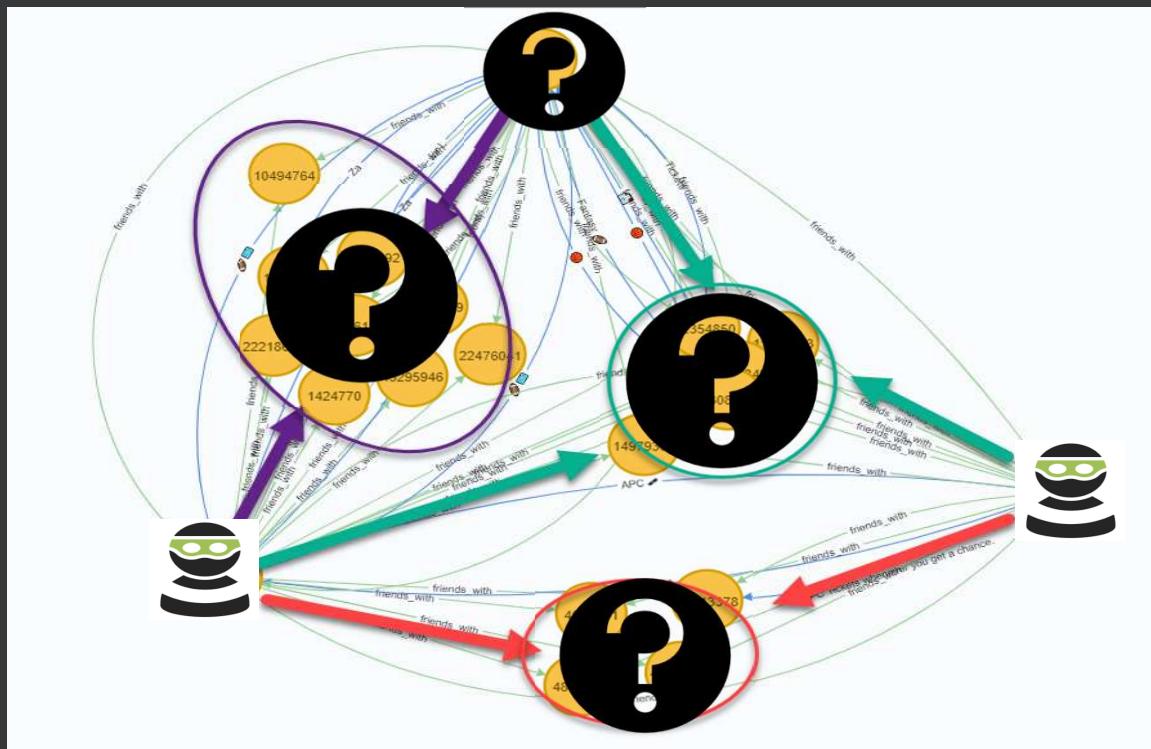
To: hanzen@email.com

From: noreply@venmosupport.net

"There was an issue with your transaction, 1a2b3c4d, on April 29 with Abigail Cetner. Please <>"

SAMPLE USE CASE

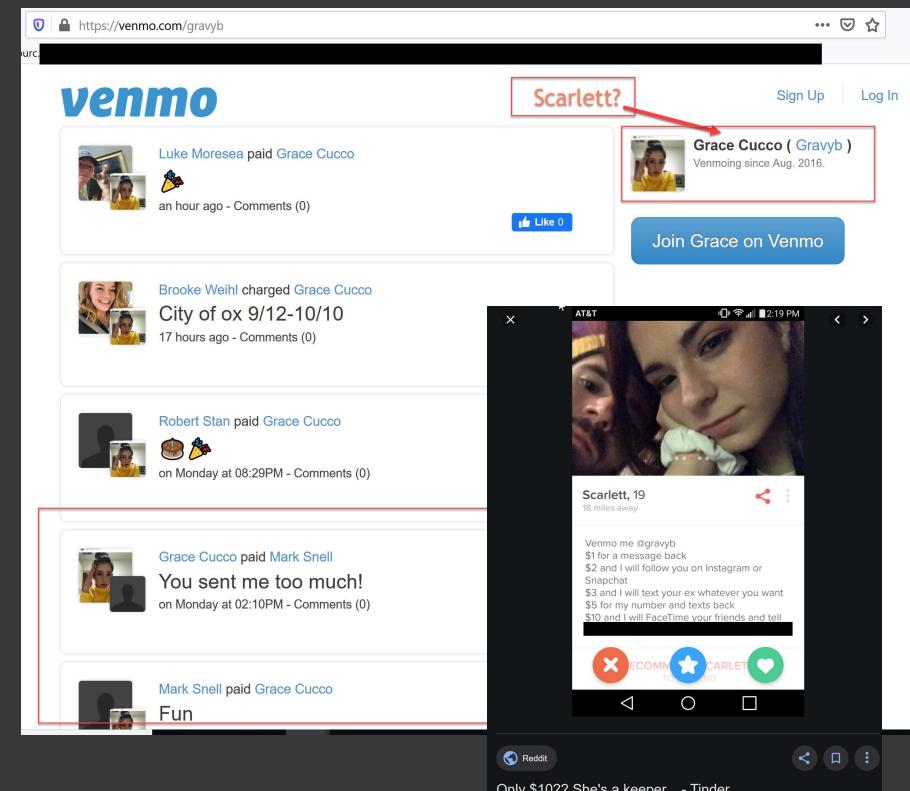
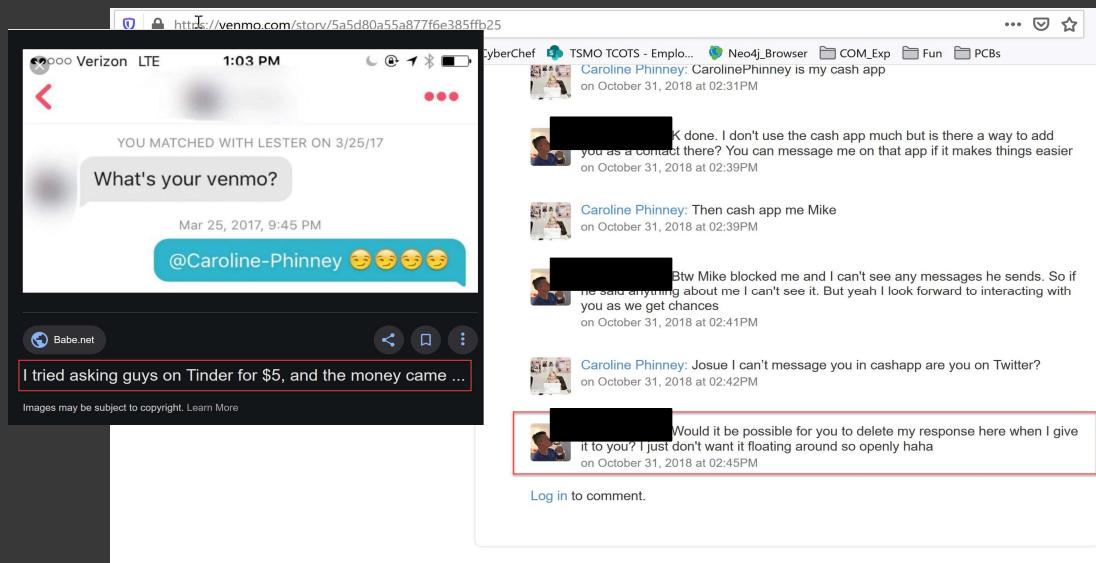
- CI/LE: Persons of Interest



- Whose are the common contacts amongst the persons of interest?
- Are there different contacts from other social media outlets?

SAMPLE USE CASE

■ Personal Security: Bot and fraud detection



TIPS

- Set Profile and Transactions to Private
- Set PAST transactions to private

