



# ENEMY

## A Collection and Intelligence Tool for Venmo

Layer 8 Conference | June 2019



```
root@ubuntu:~/venemy_L8_2019# _
```

## Michael - @mportatoes

- Red Team Operator at Millennium Corporation
- OSCP, OSWP, CISSP, CEH, CRISC, Sec+, BS & MS from Auburn
- Featured in the Raspberry Pi magazine, has presented at Shmoocon XV, CypherCon 4, National Cyber Summit

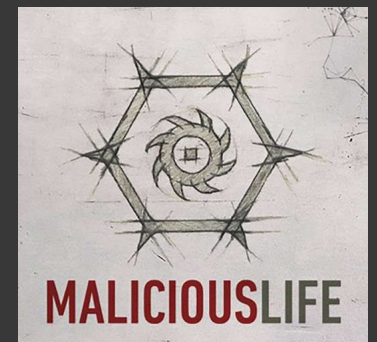
## Neal - @Shad0wRec0n

- Senior Analyst
- CISSP, Sec+, Net+, CEH
- Husband, Father, Recon Marine
- DerbyCon VIII SECTF 3<sup>rd</sup> Place

# Data tells Stories



*Shout out*





**Kari Smith** paid **Robert Brestan**  
Passport

[Like](#) · April 8



Travel?



**Kari Smith** paid **Robert Brestan**  
Passport

Like · April 8



Travel?

## Getting Married?



**Robert Brestan** paid **KayBee Photos**

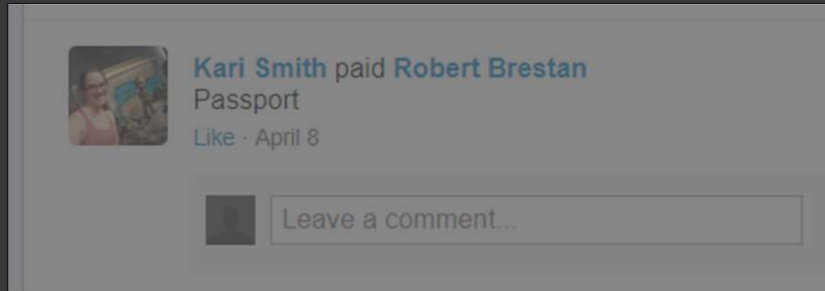
30% deposit for Robert & Kari Invoice ID: 158

Like · September 26

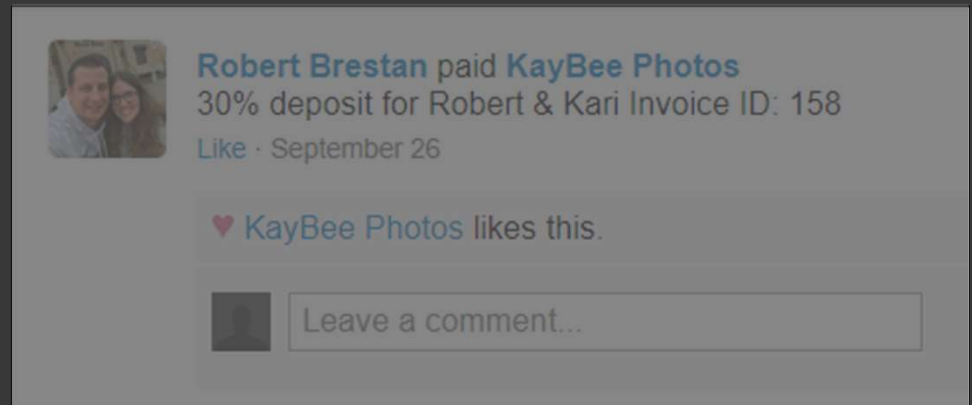
♥ **KayBee Photos** likes this.



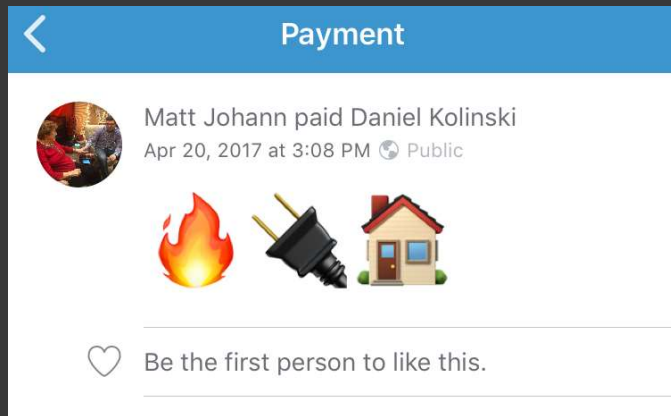
## Getting Married?



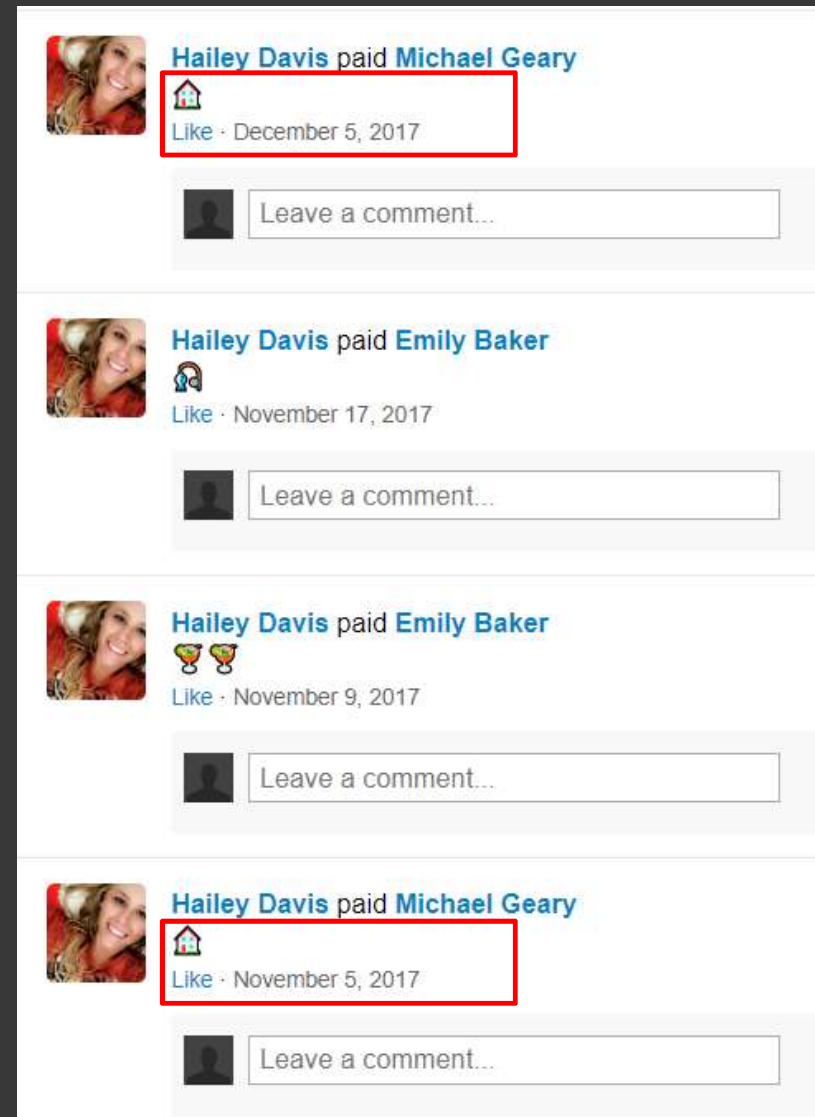
Travel?

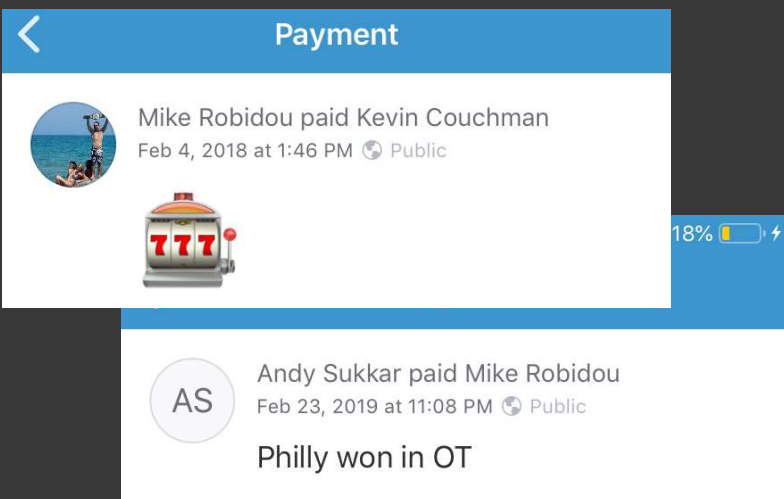


Birthday?



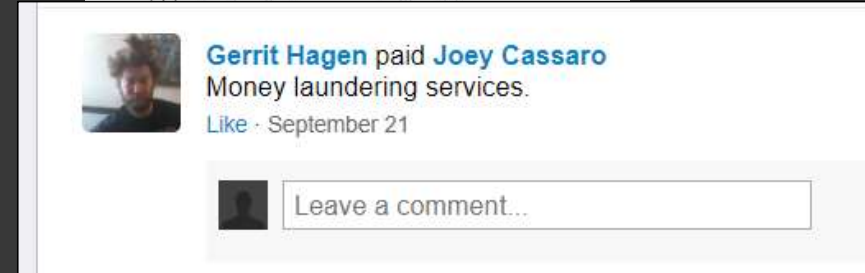
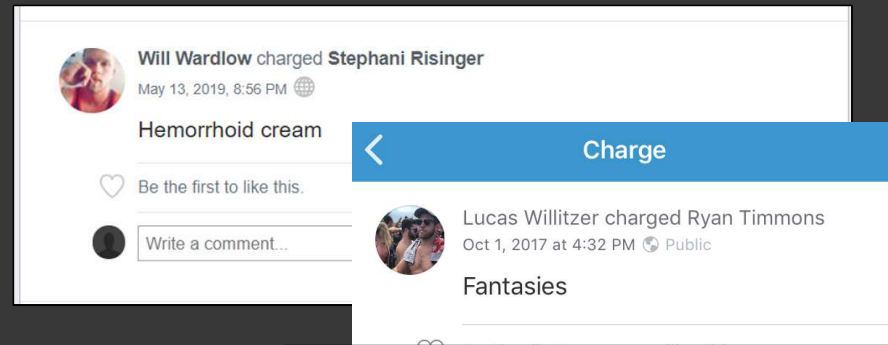
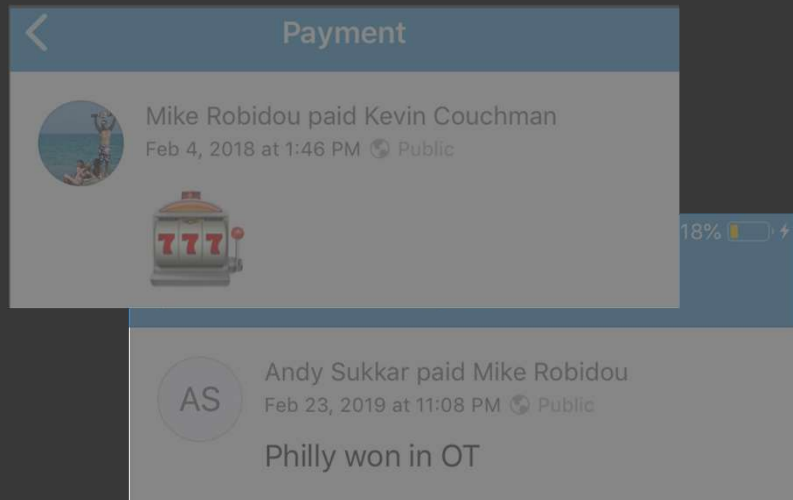
Roommates?





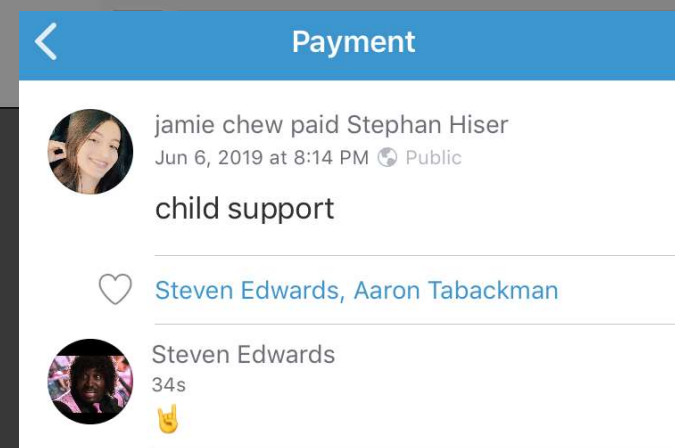
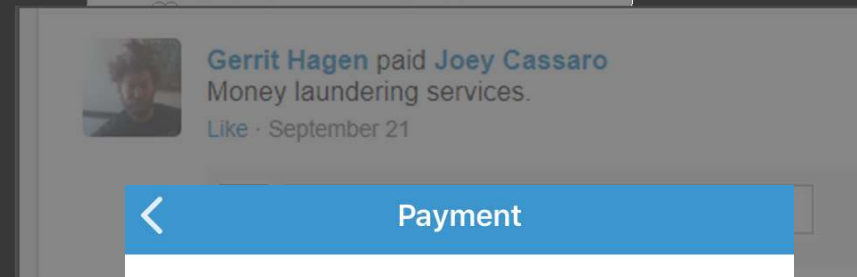
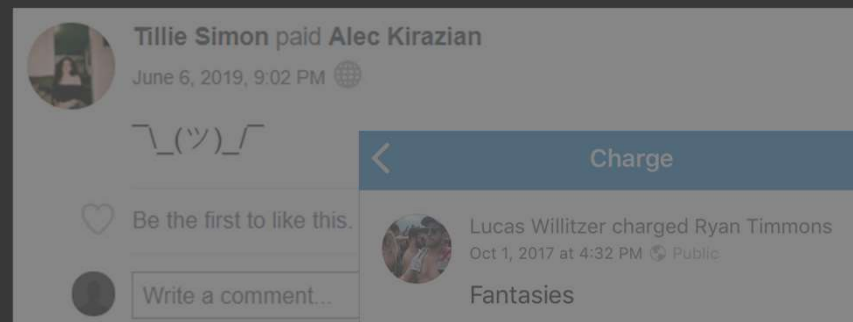
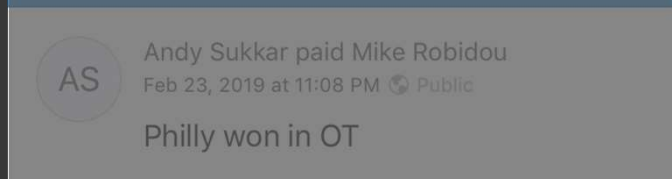
# Gambling





Random?


# Relationships





< Payment

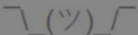
 Mike Robidou paid Kevin Couchman  
Feb 4, 2018 at 1:46 PM  Public





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 




 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


 David Ngo paid Lori Tran  
June 6, 2019, 8:30 PM 

Not happening

 Be the first to like this.

 Write a comment...

 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


♥ mackenzie hansen likes this.


 Leave a comment...

 **Lizzie Urda** paid **mackenzie hansen**  
Been 1  
mackenzie hansen likes this.

 Leave a comment...


 **Lizzie Urda** paid **mackenzie hansen**  
Pee  
Like · February 26

 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...



**40  
million**

**vs.**



**Total users 267 million**



vs.



40

Total users

267 million

70-80%

Year over Year



20-25%

Year over Year



**~HALF are  
Public!**



**70-80%**

**Year over Year**



**vs.**



**Total users**

**267 million**

**20-25%**

**Year over Year**







**\$100,000,000,000**



vs.



\$60

\$300

Per transaction



Information

?



Intelligence

BITE  
ME

# HOW 'BOUT THAT CODE?

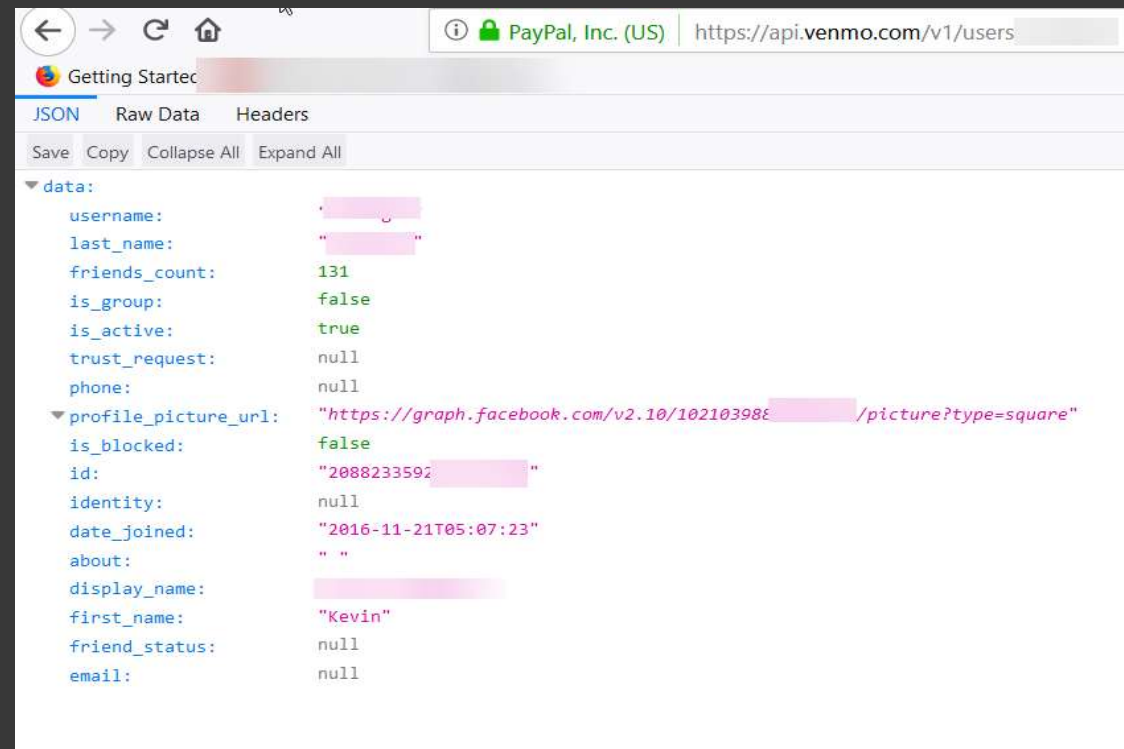
- <https://github.com/mportatoes/venemy>
- Written in python3
- Authenticated and Unauthenticated versions
- Neo4j used for graph analysis
  - Installation and sample queries can be found in the repo
- All samples herein have third party names redacted with partial IDs

# INFERENCES - CONTACTS

- 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 their connection to you

# INFERENCES - FACEBOOK

- You'll never find my Facebook account...
- Can find userID from the profile picture URL



# AUTHENTICATED MODULE

```

C:\Command Prompt

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

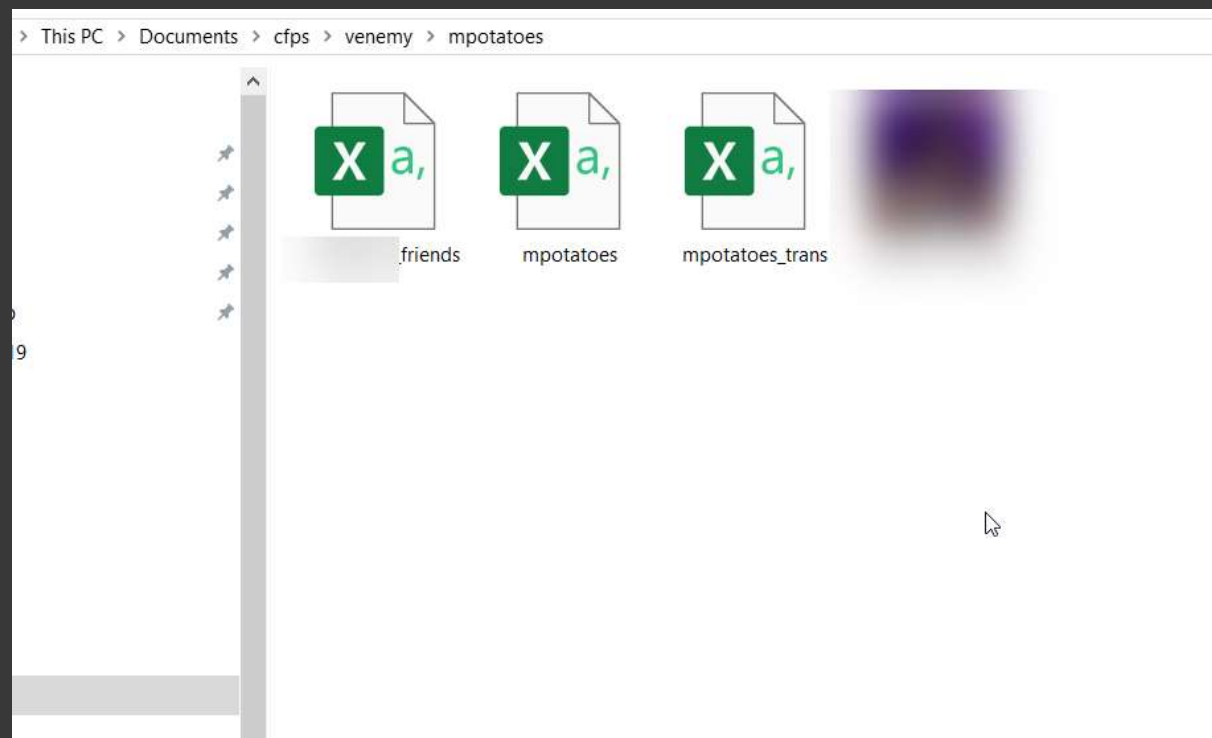
optional arguments:
  -h, --help            show this help message and exit
  -u USER, --user USER  Grabs basic info of user
  -f FRIENDS, --friends FRIENDS
                        Get friends
  -t TRANS, --trans TRANS
                        Get transactions of users
  -a ALL, --all ALL      Grab basic 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>

C:\Command Prompt

C:\Users\potatoes\Documents\cfps\venemy>python venemy_auth.py -a mpotatoes
[+] Data will be output to ./mpotatoes/
[+] Gathering user info...
[+] Gathering friend info...
[+] Gathering transaction info...
```

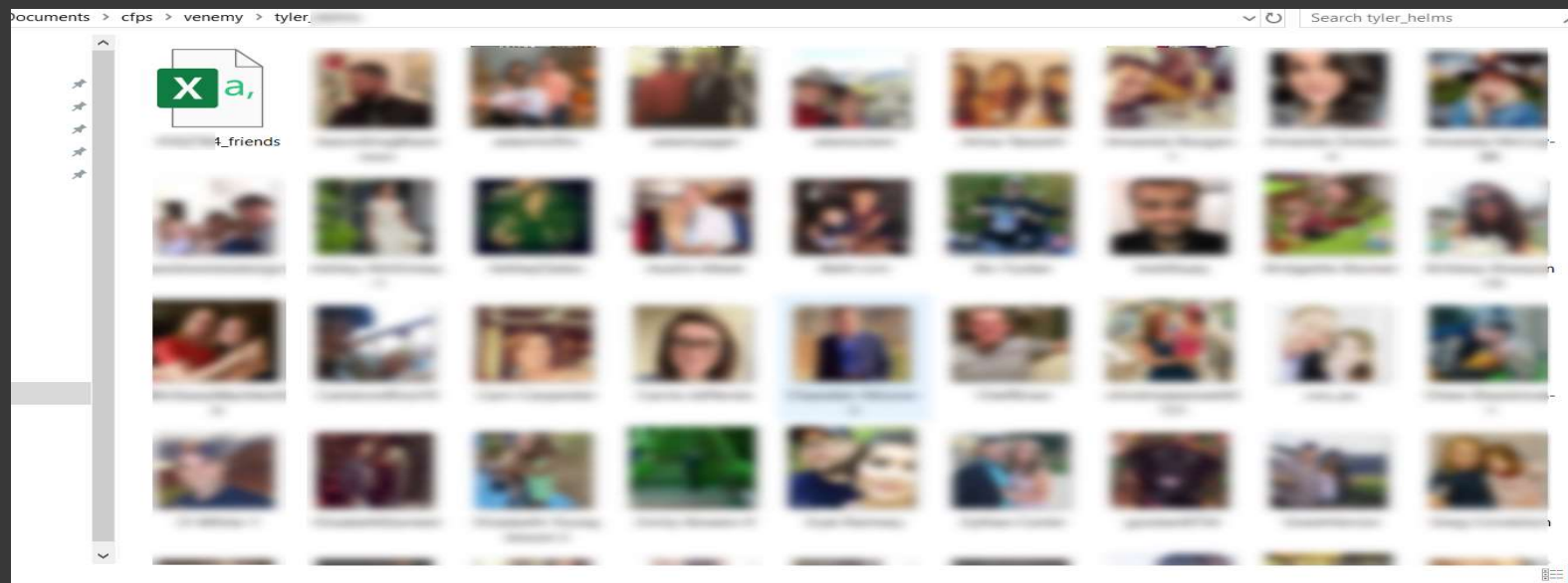
# AUTHENTICATED MODULE



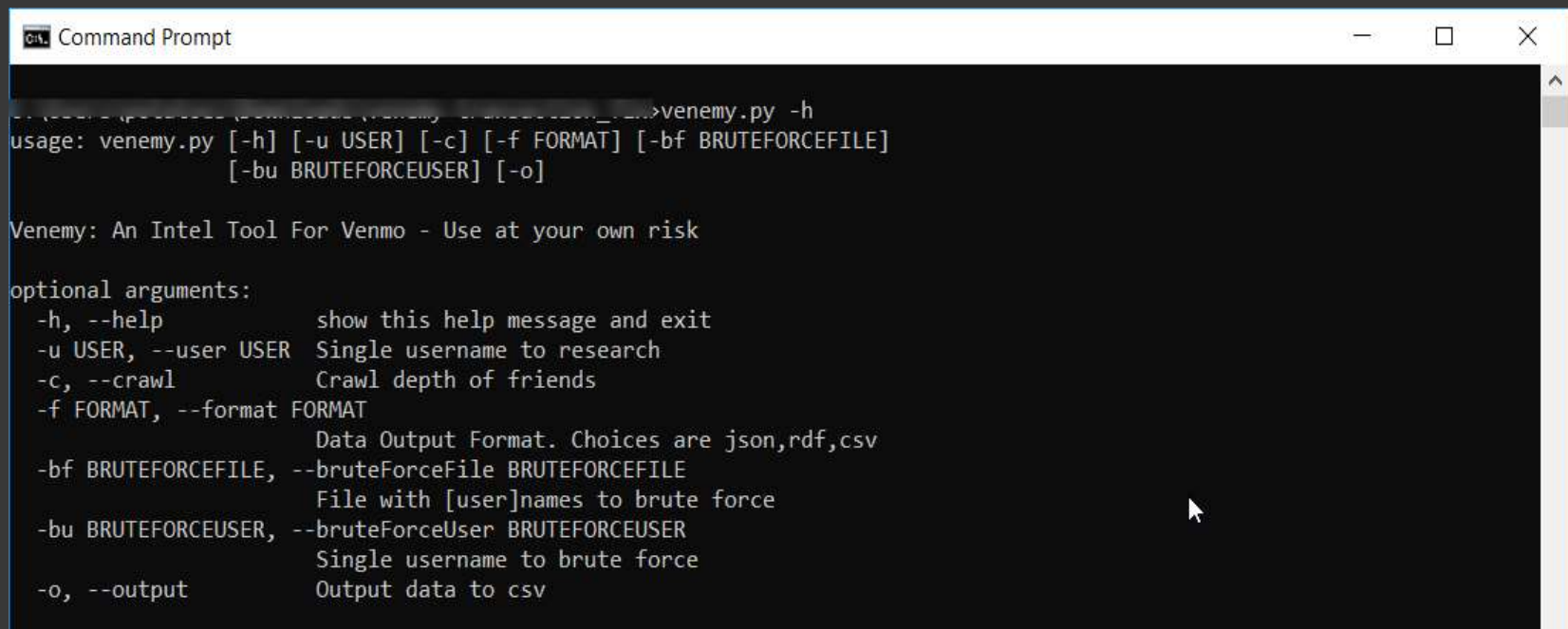


# AUTHENTICATED MODULE

```
C:\Users\potatoes\Documents\cfps\venemy>python venemy_auth.py -c tyler_l  
Fetching list for 498  
Fetching list for 152  
Fetching list for 946
```



# UNAUTHENTICATED MODULE

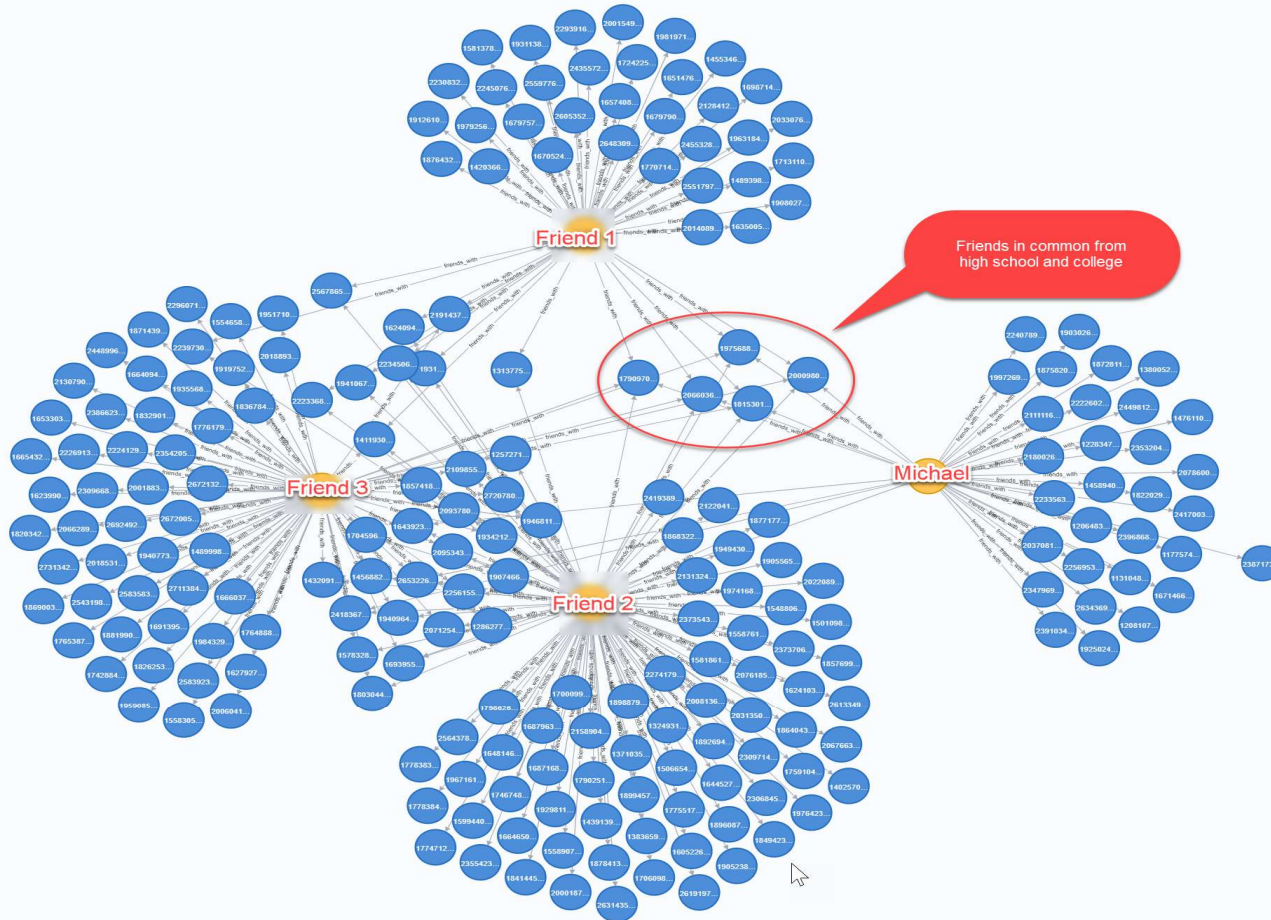


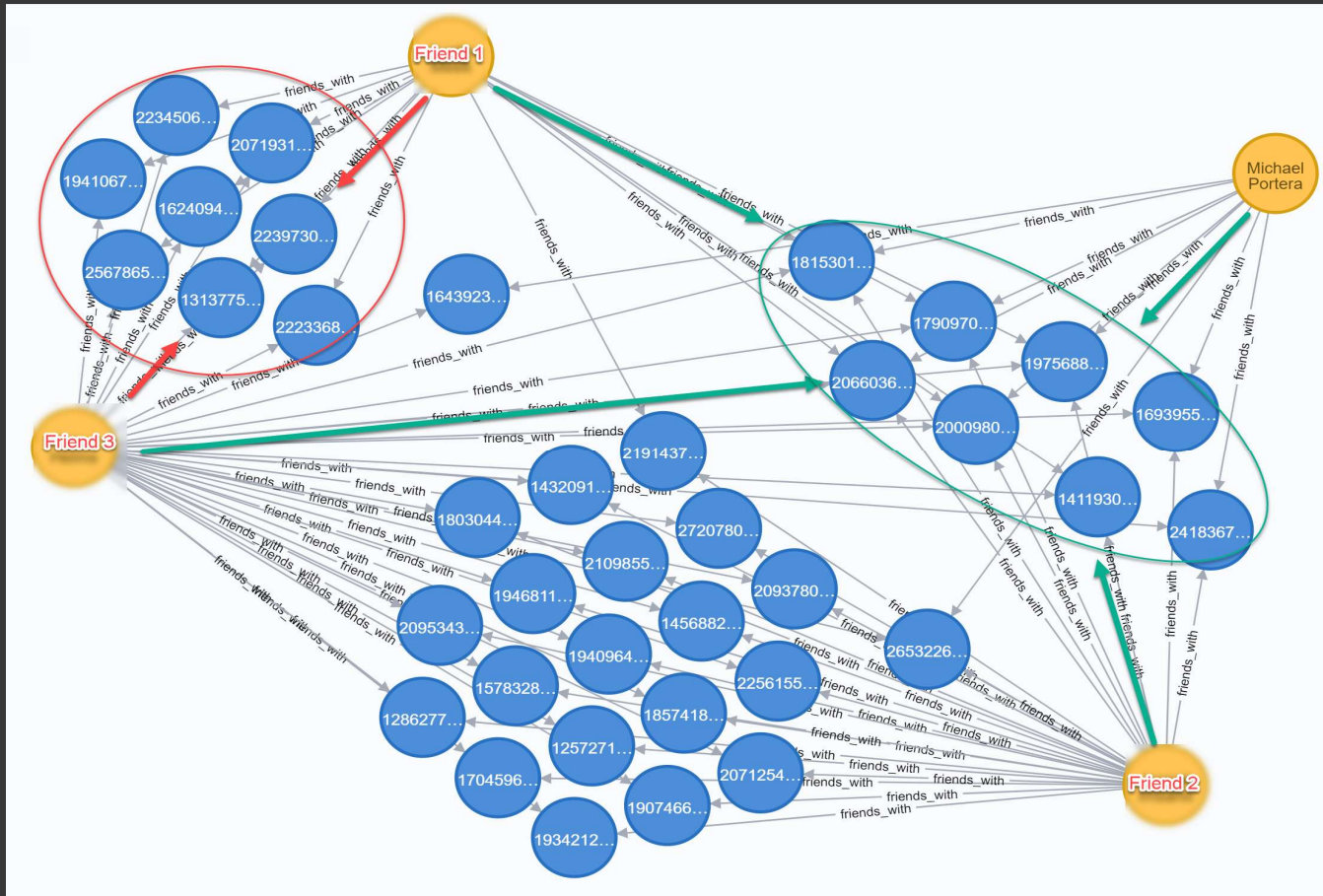
```
Command Prompt
C:\>venemy.py -h
usage: venemy.py [-h] [-u USER] [-c] [-f FORMAT] [-bf BRUTEFORCEFILE]
                [-bu BRUTEFORCEUSER] [-o]

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
```

- Sample: Show all 1<sup>st</sup> contacts for me and three friends

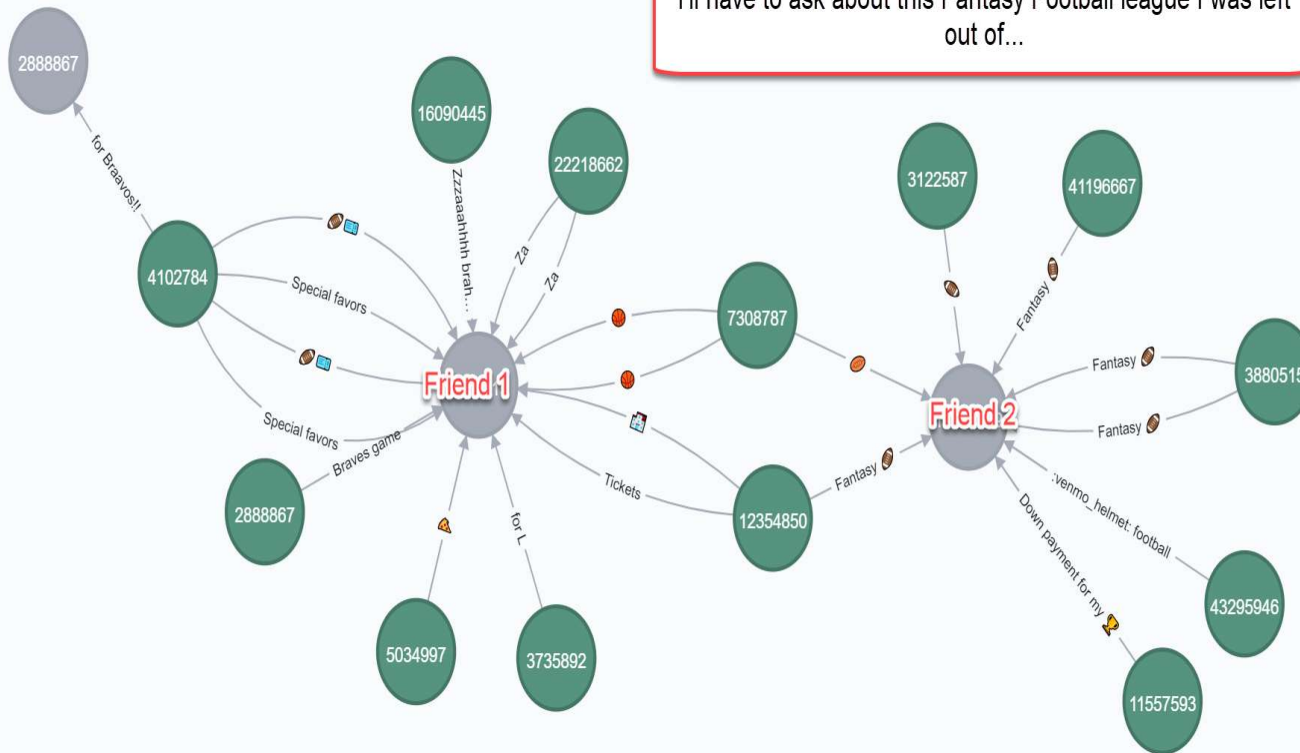




- Sample: Show only common friends between me and/or three of my friends

*match (person)-[:friends\_with]-(friend) with friend, count(\*) as friend\_count where friend\_count > 1 return friend, friend\_count*

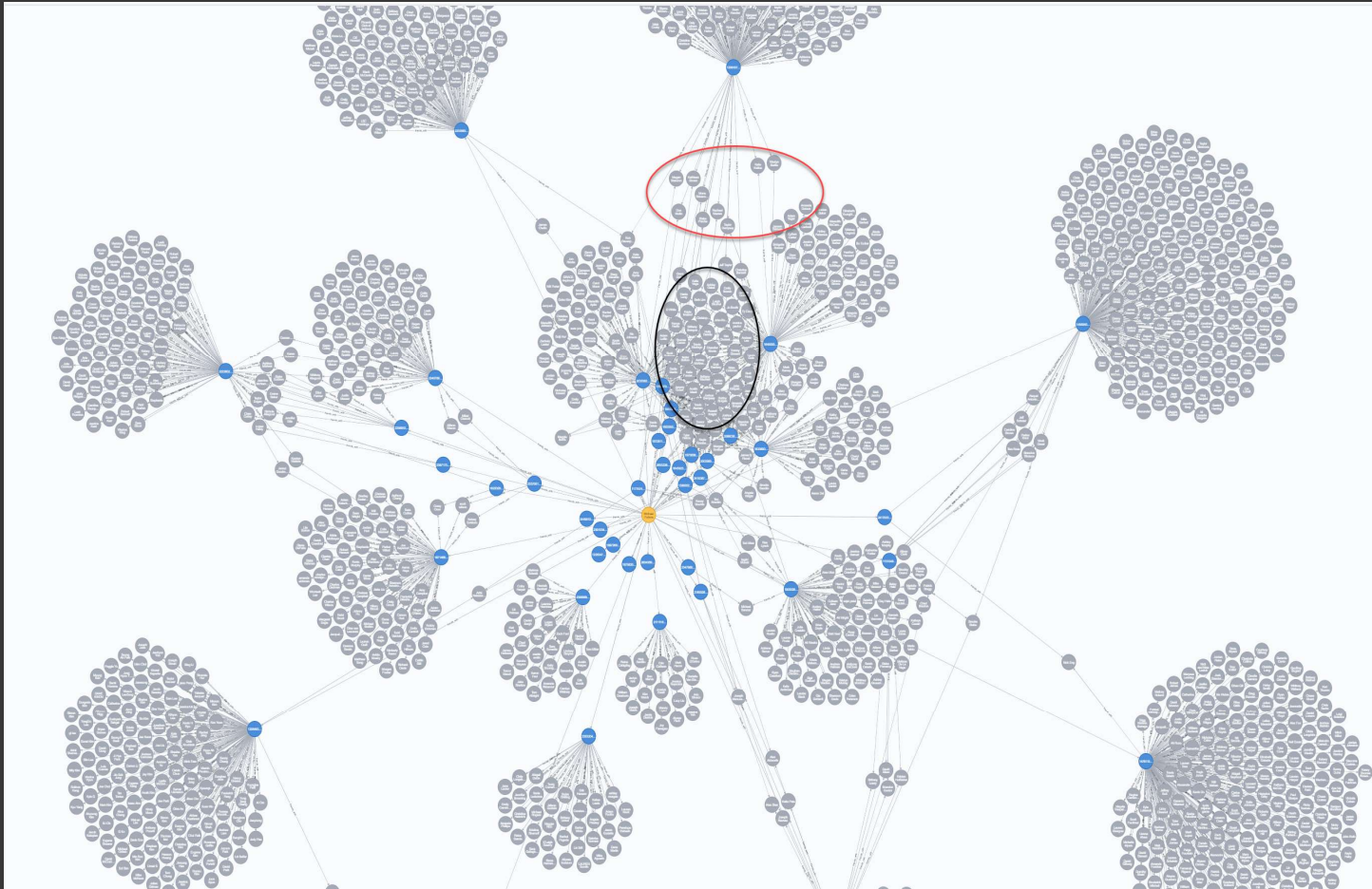
I'll have to ask about this Fantasy Football league I was left out of...



■ Sample:  
Show  
transactions  
of my friends

*MATCH (actor)-[d:deals]->(target) RETURN \**





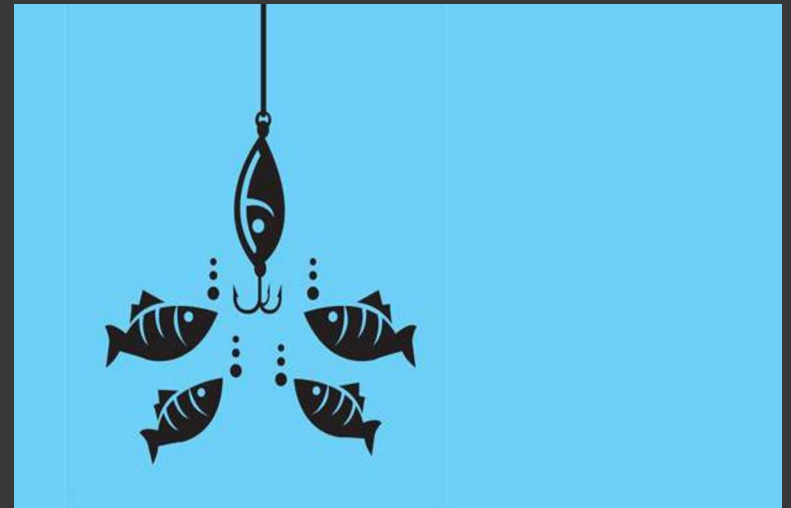
■ Sample: Show the friends of my friends



Bad Guys / Hunting



Phishing / Pen-Testing





---

You can use all the quantitative data you can get,  
but you still have to distrust it and use your own intelligence and judgment.  
~**Alvin Toffler**



# ENEMY

## A Collection and Intelligence Tool for Venmo

Layer 8 Conference | June 2019



```
root@ubuntu:~/venemy_L8_2019# _
```