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

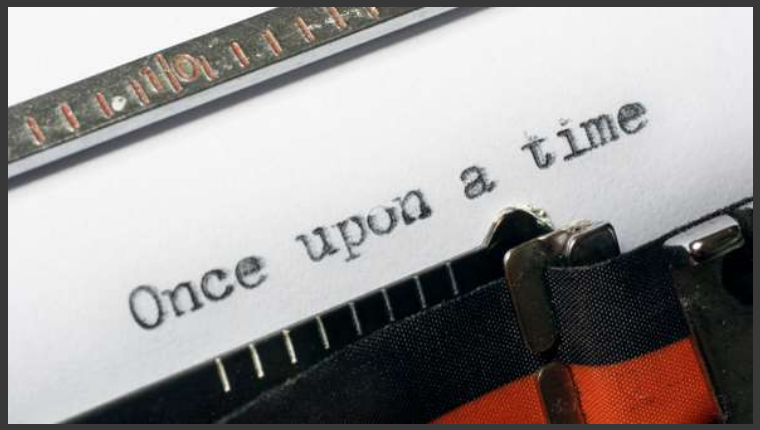
Neal - @Shad0\\\`Rec0n

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

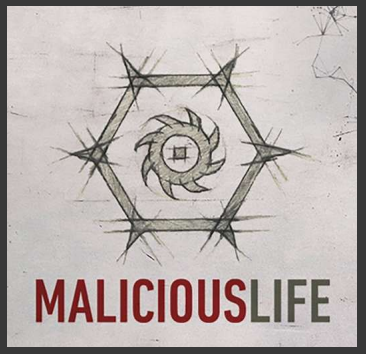
VENMO IN THE NEWS

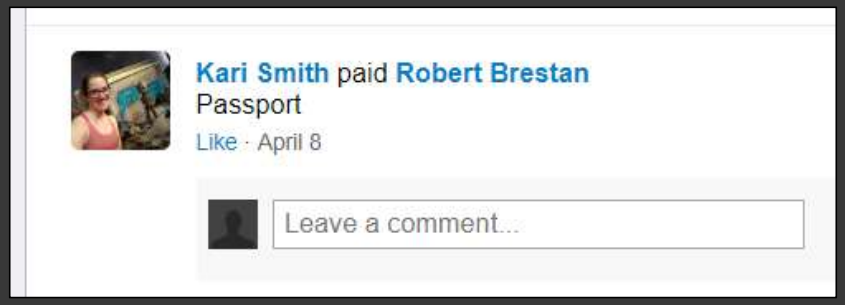
- The EFF and Mozilla published an open letter to PayPal to fix Venmo's privacy holes (Aug. 2019)
- Mozilla launched a campaign to make transactions private by default (2018)
- publicbydefault.fyi – research on public transactions by Hang Do Thi Duc (2018)
- Vicemo (defunct, 2015) – Who is buying drugs,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

Data tells Stories

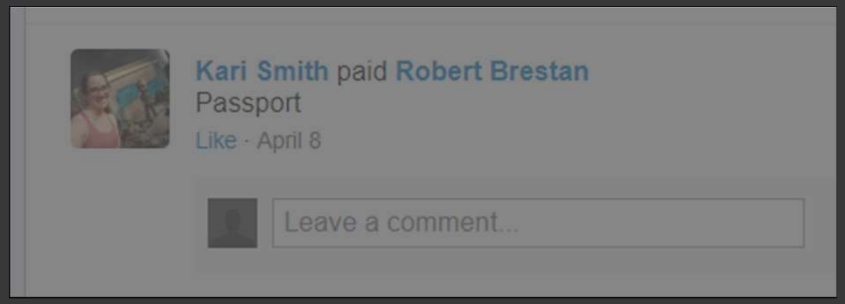


Shout out



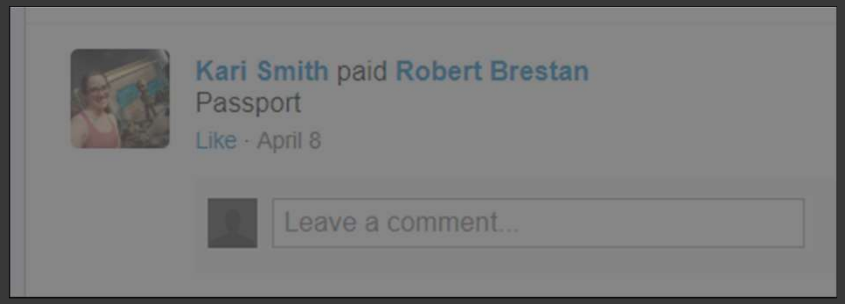

Kari Smith paid Robert Brestan
Passport
Like · April 8
Leave a comment...

Travel?



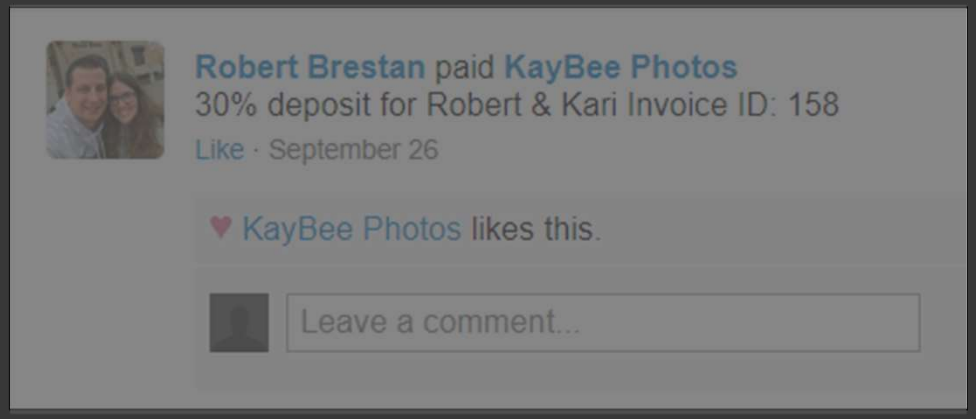
Travel?

Getting Married?

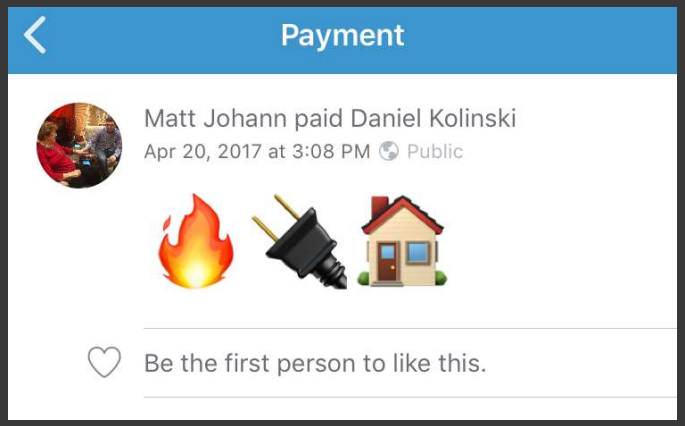


Travel?

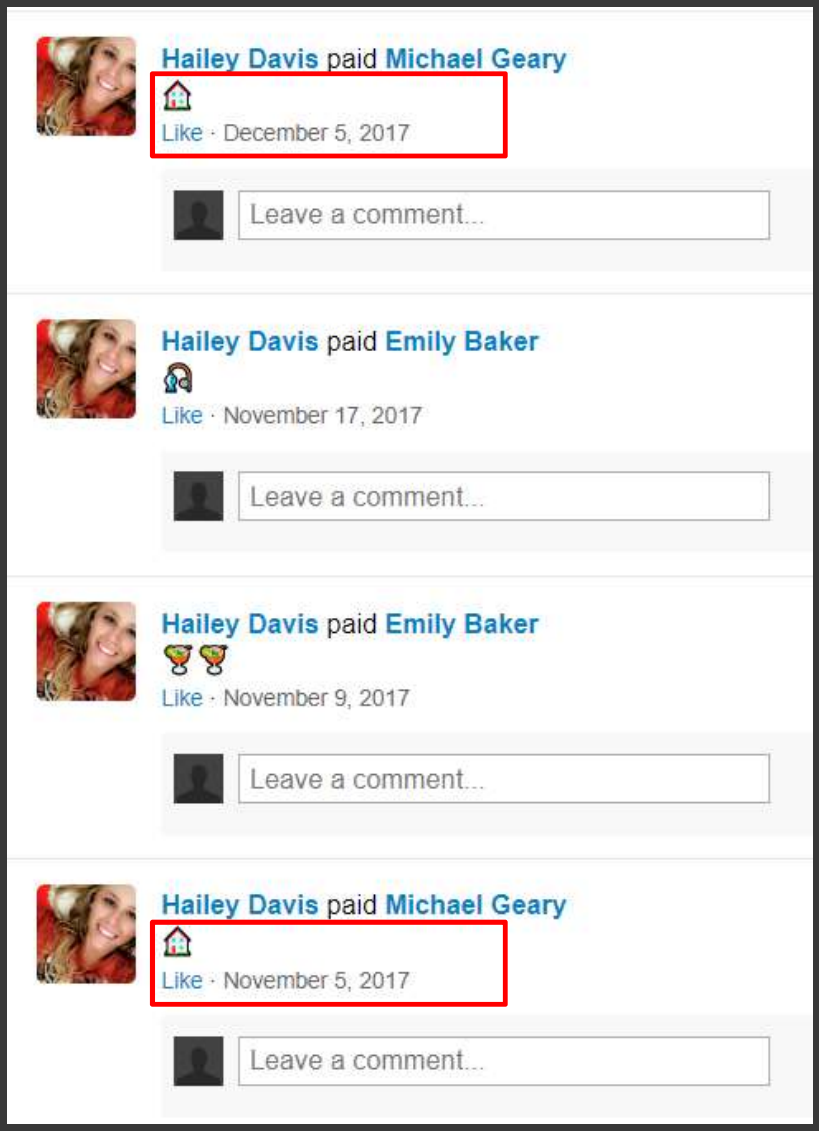
Getting Married?

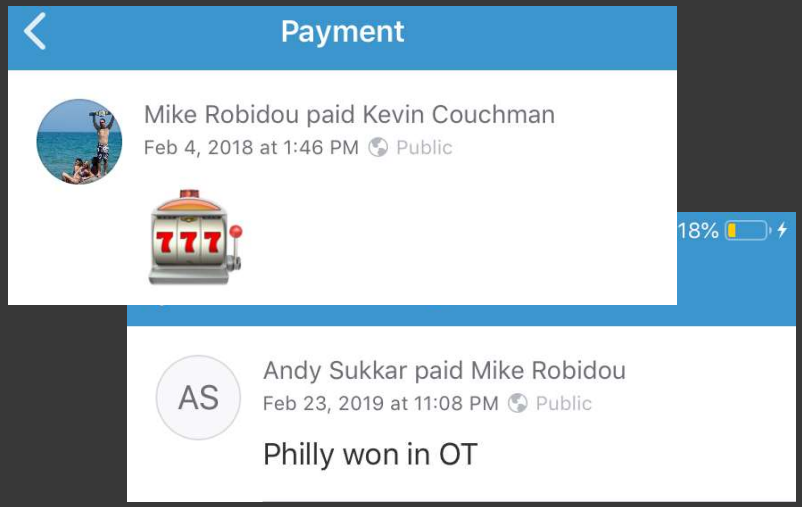


Birthday?

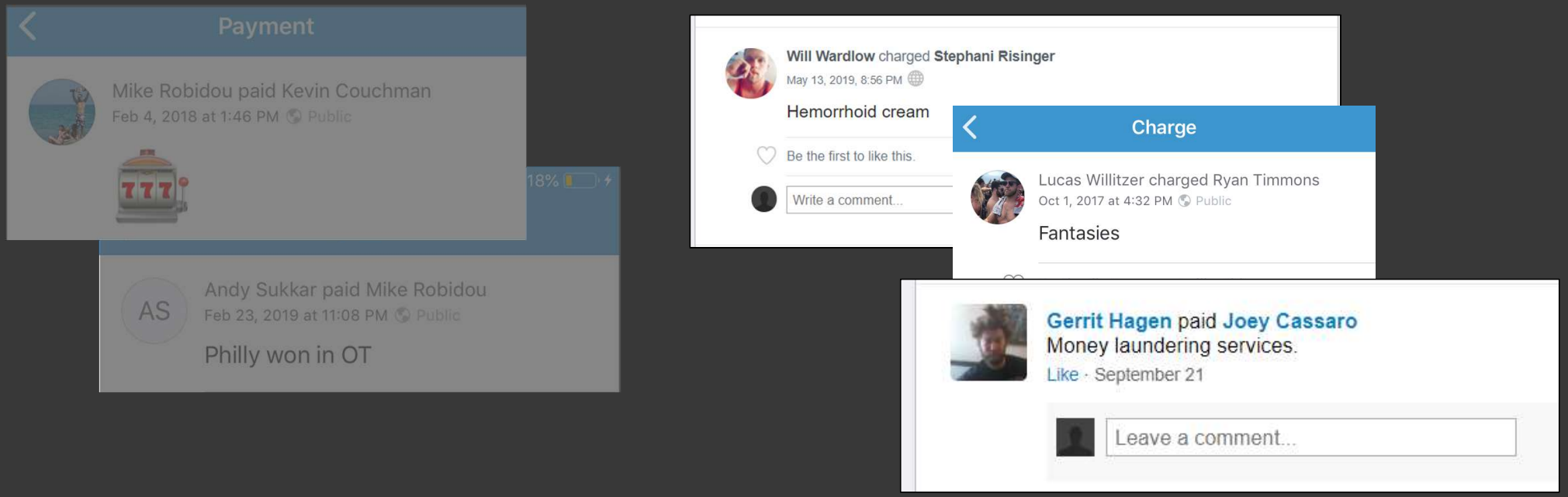

Payment
Matt Johann paid Daniel Kolinski
Apr 20, 2017 at 3:08 PM Public
Be the first person to like this.

Roommates?

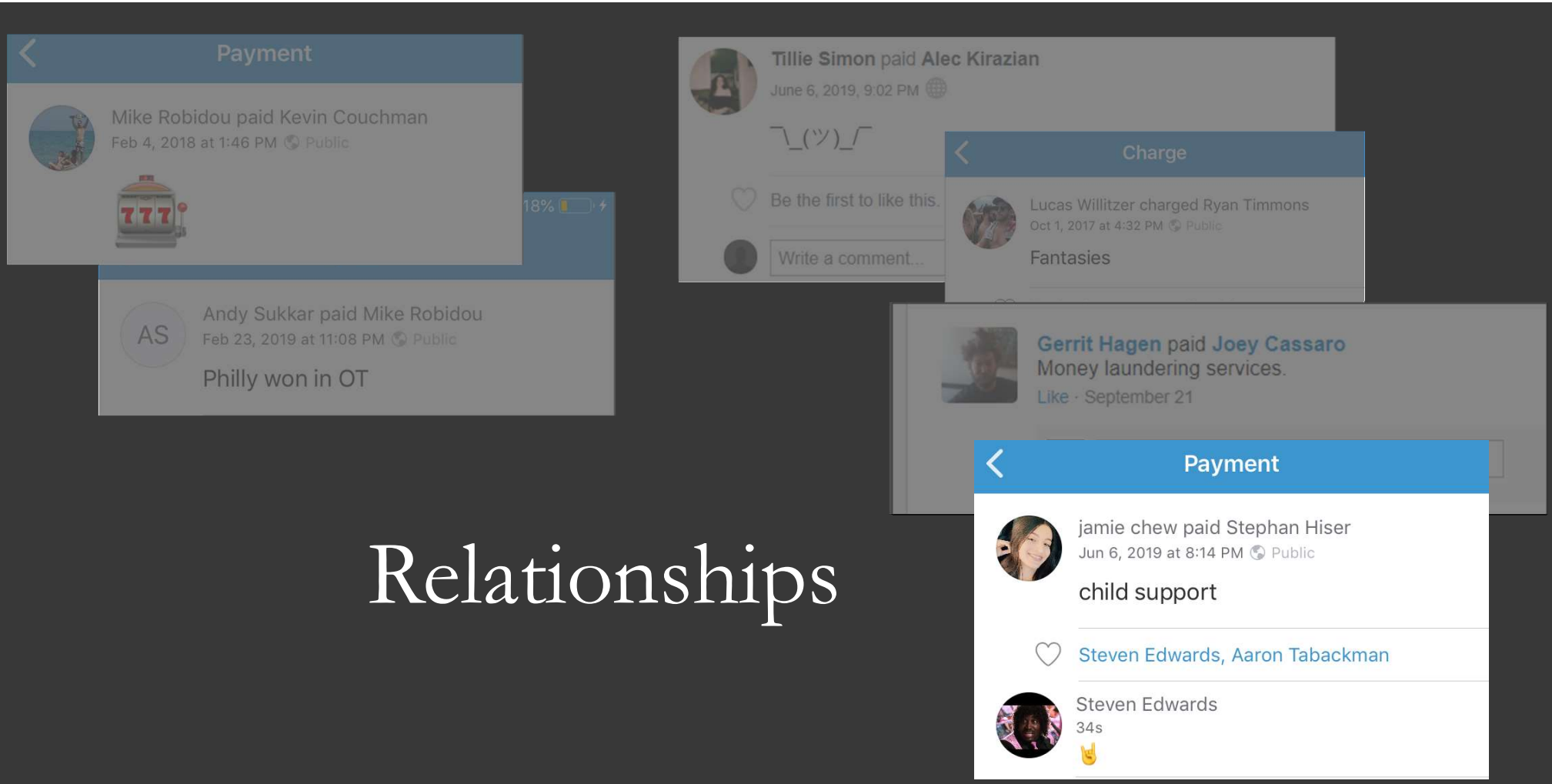

Hailey Davis paid Michael Geary
Like · December 5, 2017
Leave a comment...
Hailey Davis paid Emily Baker
Like · November 17, 2017
Leave a comment...
Hailey Davis paid Emily Baker
Like · November 9, 2017
Leave a comment...
Hailey Davis paid Michael Geary
Like · November 5, 2017
Leave a comment...


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
18%
AS
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

¯_(ツ)_/¯

Be the first to like this.

Write a comment...

Charge

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

Fantasies

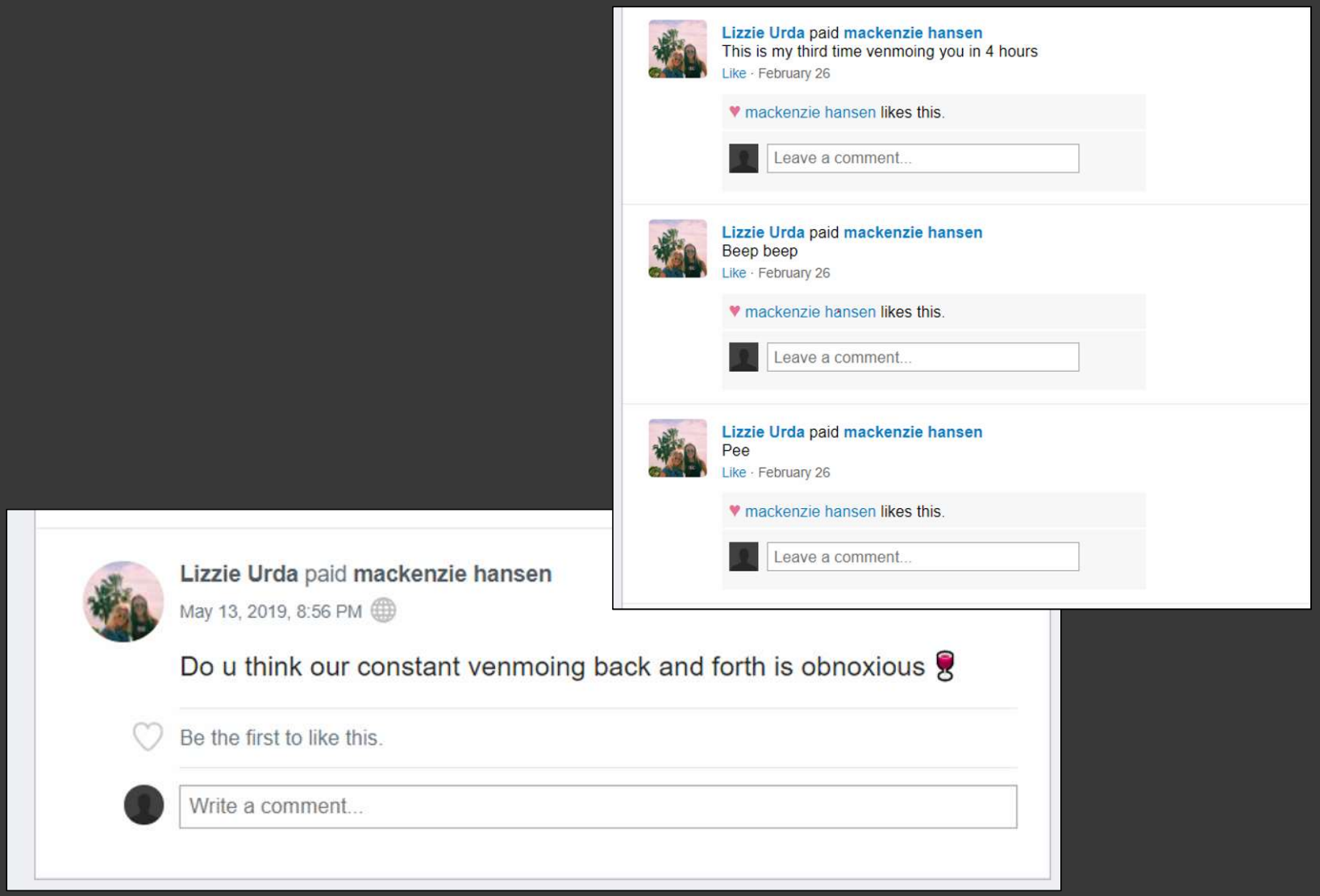
Gerrit Hagen paid **Joey Cassaro**
Money laundering services.
Like · September 21

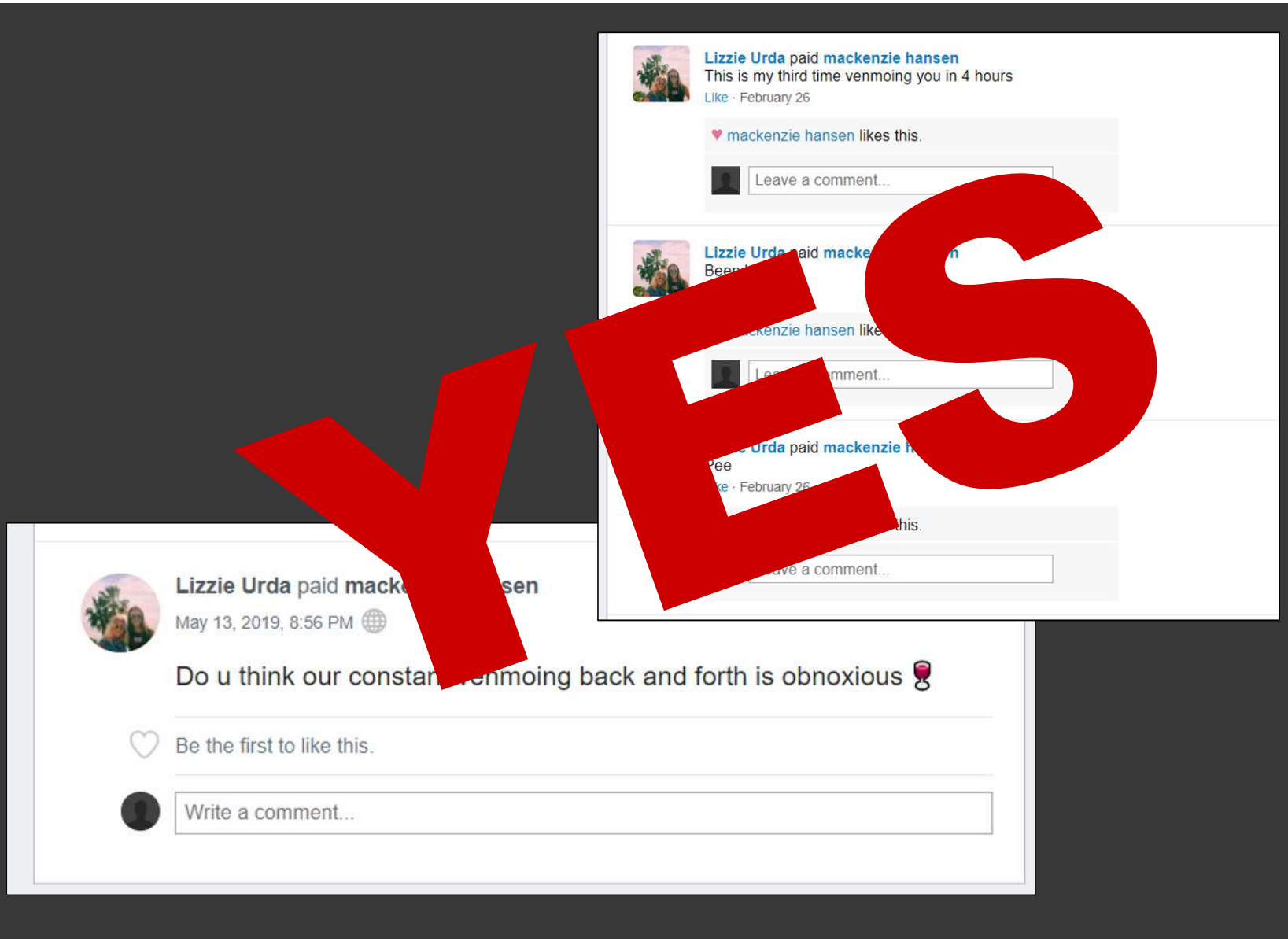
Payment

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
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...
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...
YES
Lizzie Urda paid mack sen
May 13, 2019, 8:56 PM
Do u think our constan venmoing back and forth is obnoxious
Be the first to like this.
Write a comment...

VS.

40 million

Total users

267 million

VS.

PayPal

40 million

Total users

267 million

70-80%

Year over Year

20-25%

Year over Year

~HALF are Public!

VS.

PayPal

40 million

Total users

267 million

70-80%

Year over Year

20-25%

Year over Year

$100,000,000,000

vs.

$60 $300

Per transaction

Information ? Intelligence

BITE ME

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?

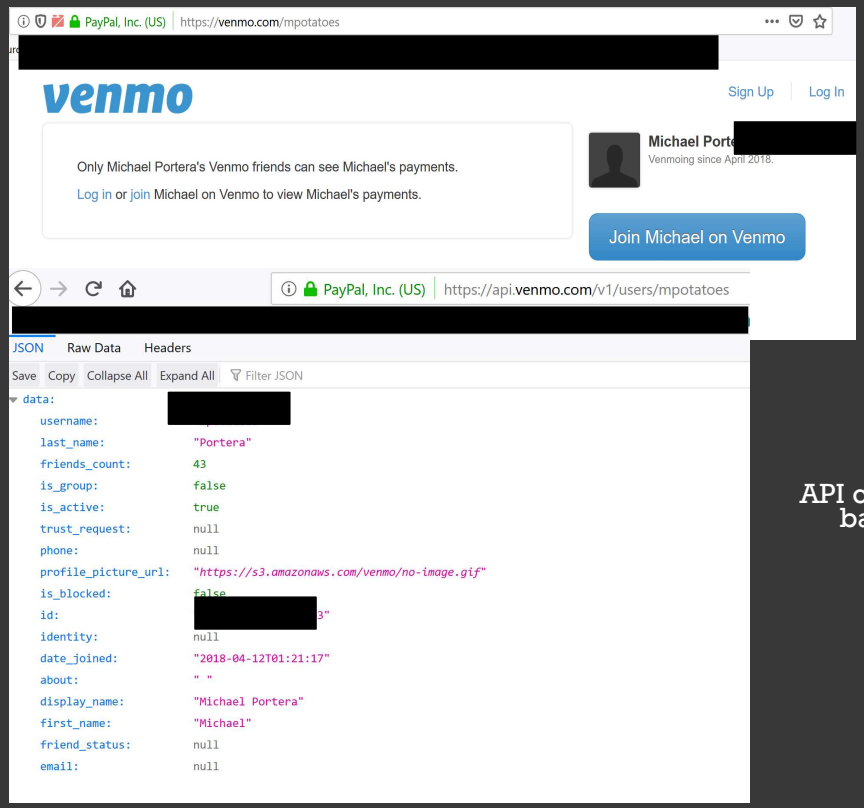
- Authenticated:
  - Friends list, friend of a friend (FOAF)
  - Access to more API endpoints
  - **All** previous transactions
    - Timestamps, transaction ID, parties involved, item/description, profile pictures (w/possible link to Facebook), "Likes"/Comments
- Unauthenticated:
  - Last five transactions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

PRIVATE VS PUBLIC

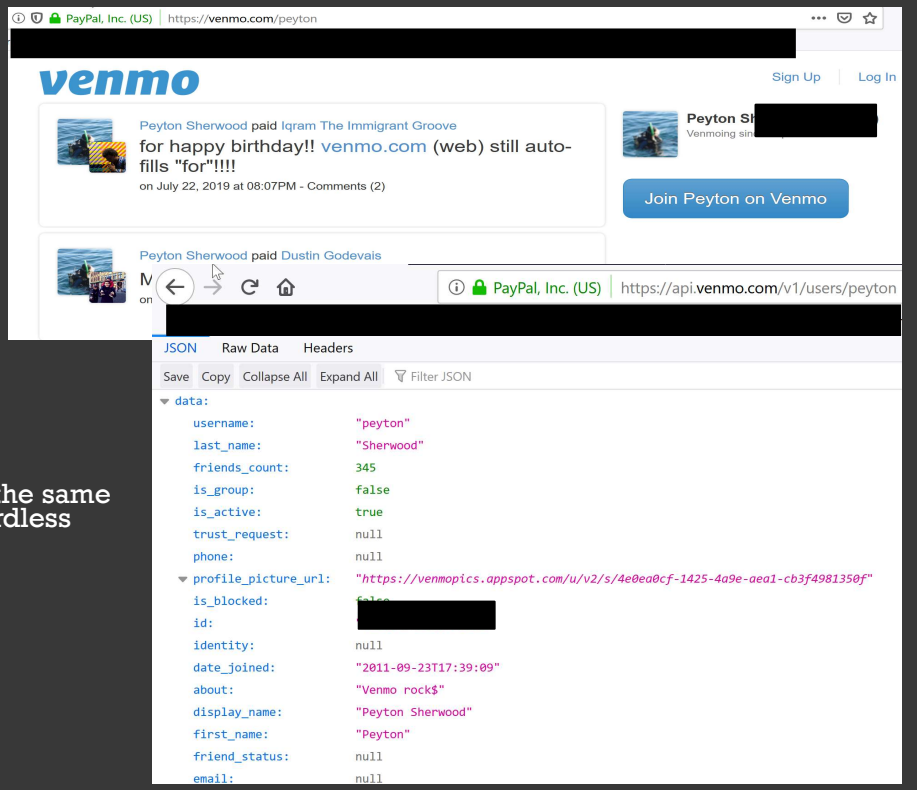
- Authenticated:
  - API key is issued BEFORE an account is confirmed via email
  - API key is valid for 30 minutes
  - Can script this for temporary anonymous access

PRIVATE VS PUBLIC

Private Profile (Unauth)



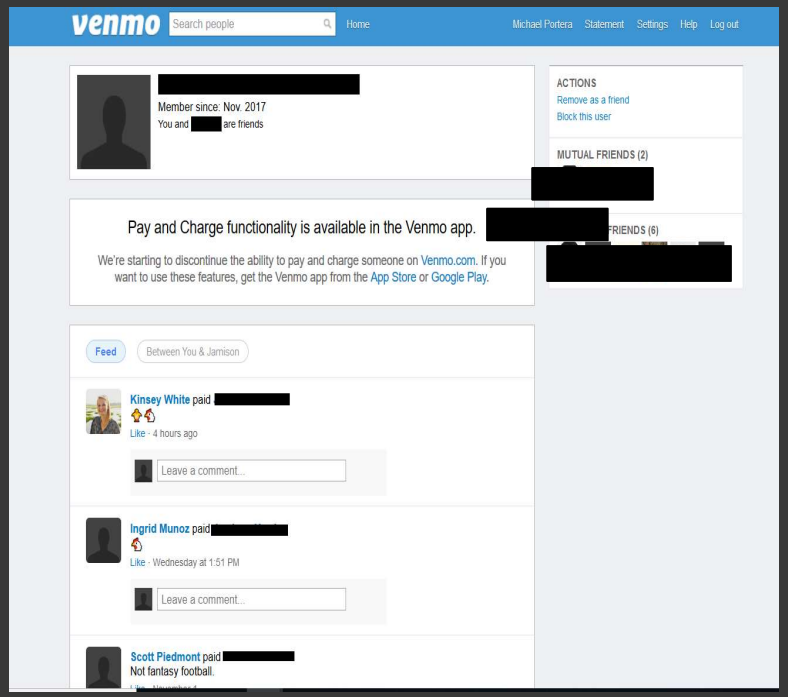
Public Profile (Unauth)



API call will show the same basic info regardless

PRIVATE VS PUBLIC

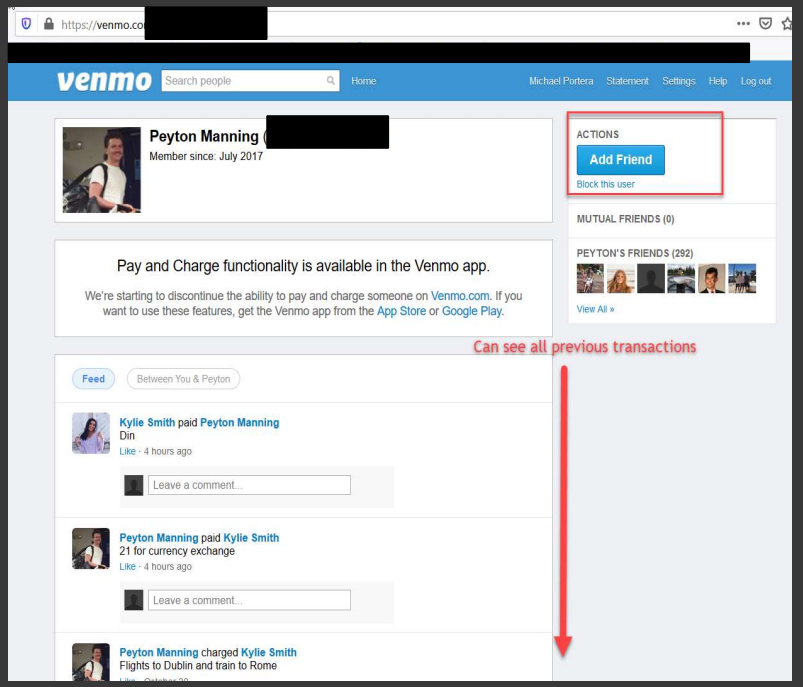
Private Profile (Auth)



API calls reveal all of these details in formatted JSON.

This is for visual purposes only.

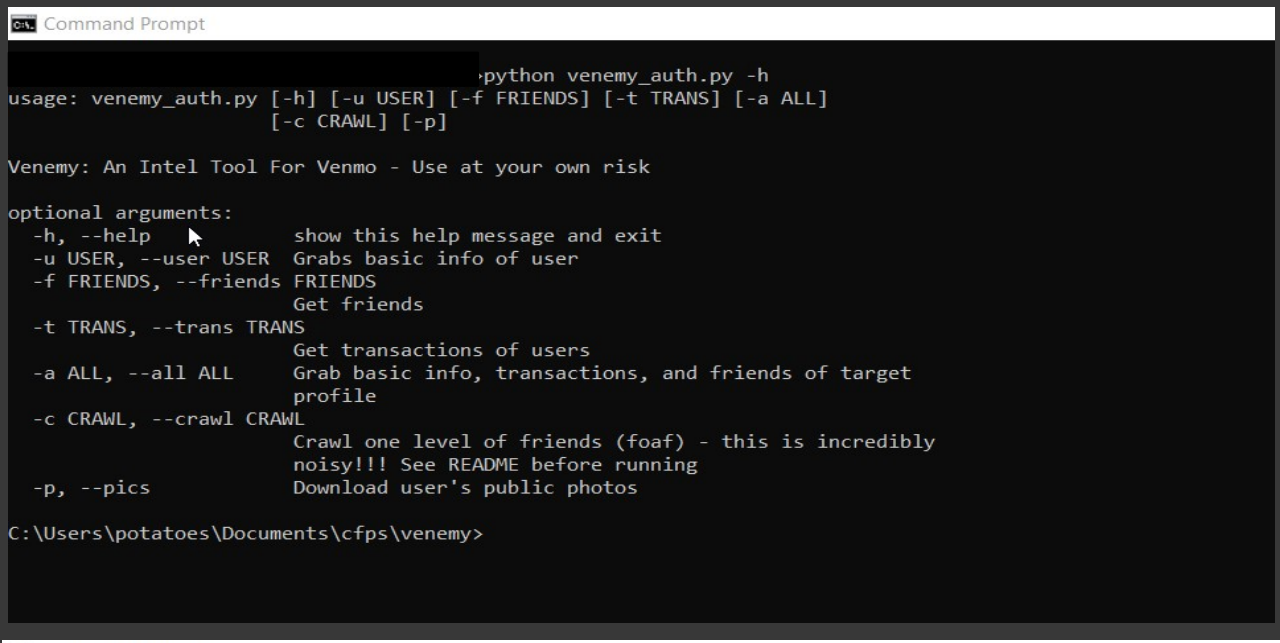
Public Profile (Auth)

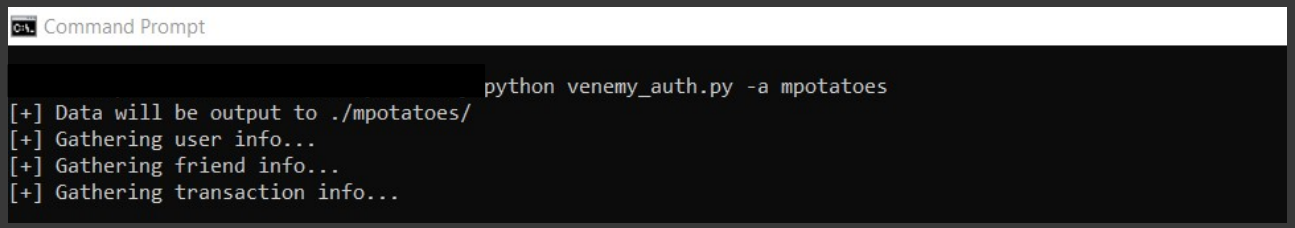


FRIENDS LIST

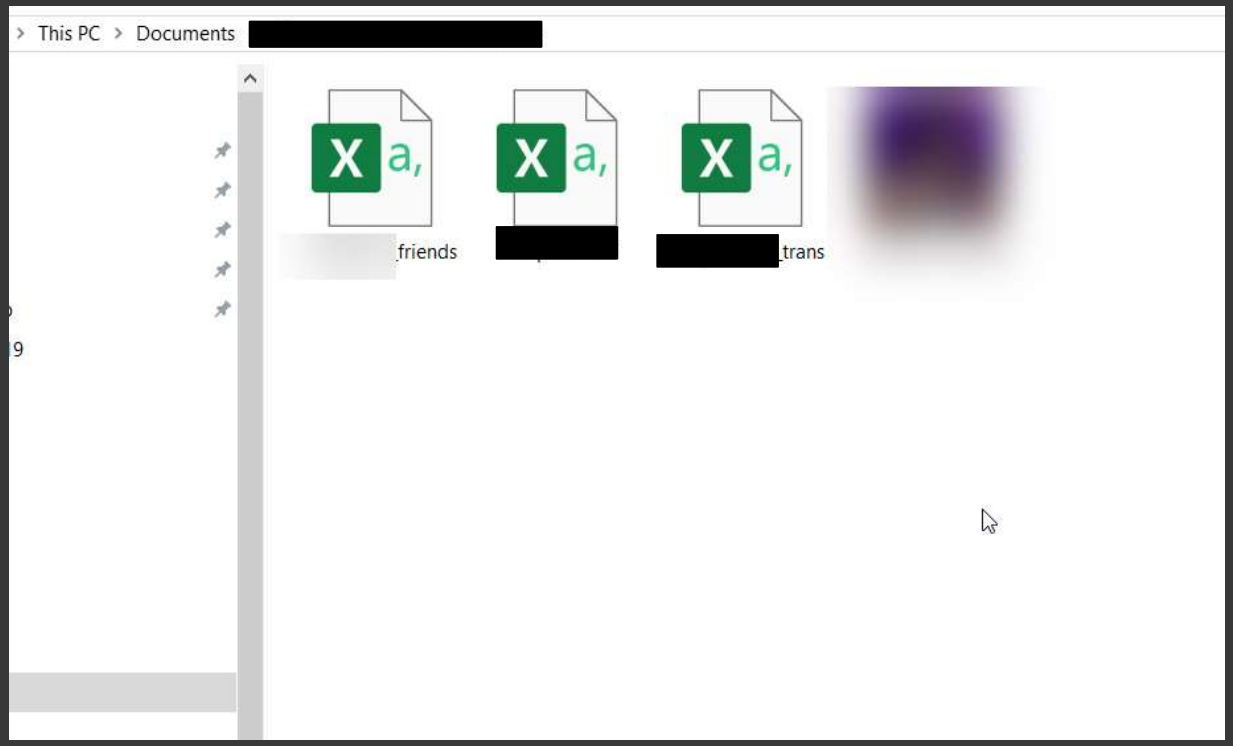
- When setting up the mobile application, it will import your contacts and look up those users by their details
  - *"Venmo will use the names, phone numbers, and email addresses of your contacts to friend those that use Venmo, help you invite those that don't, improve your search results and as noted 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

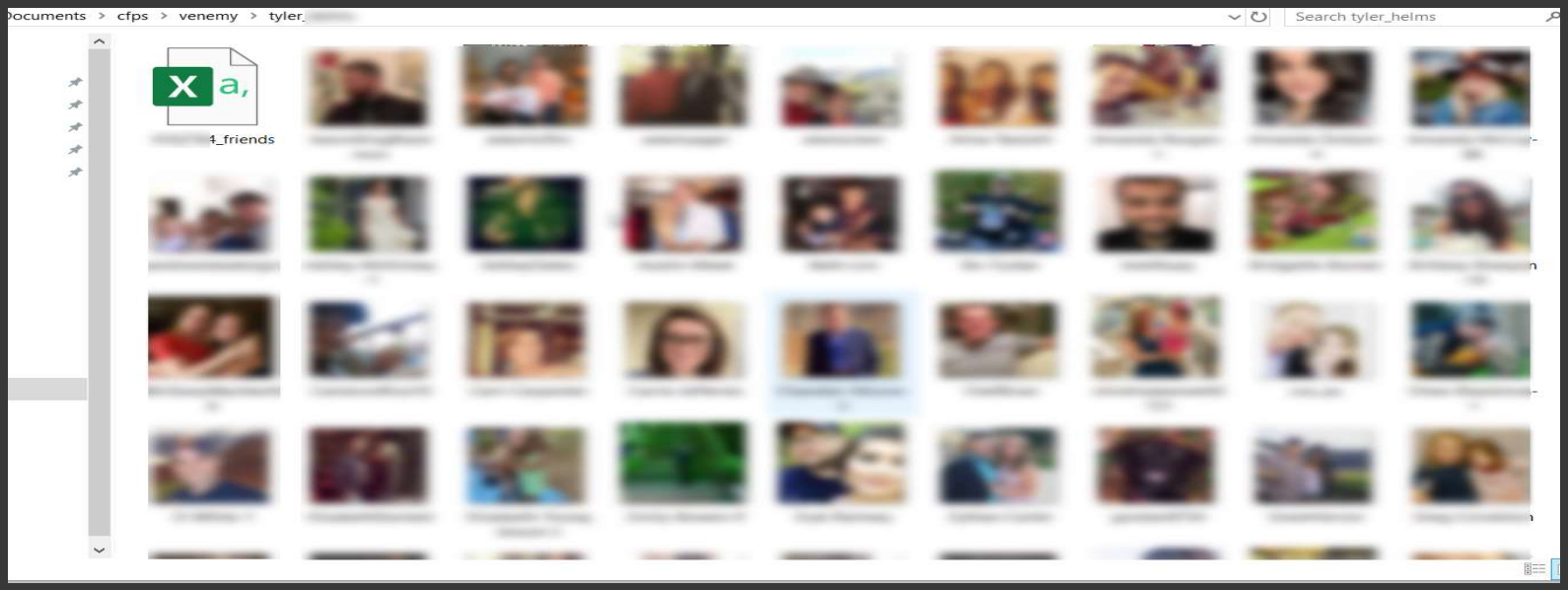




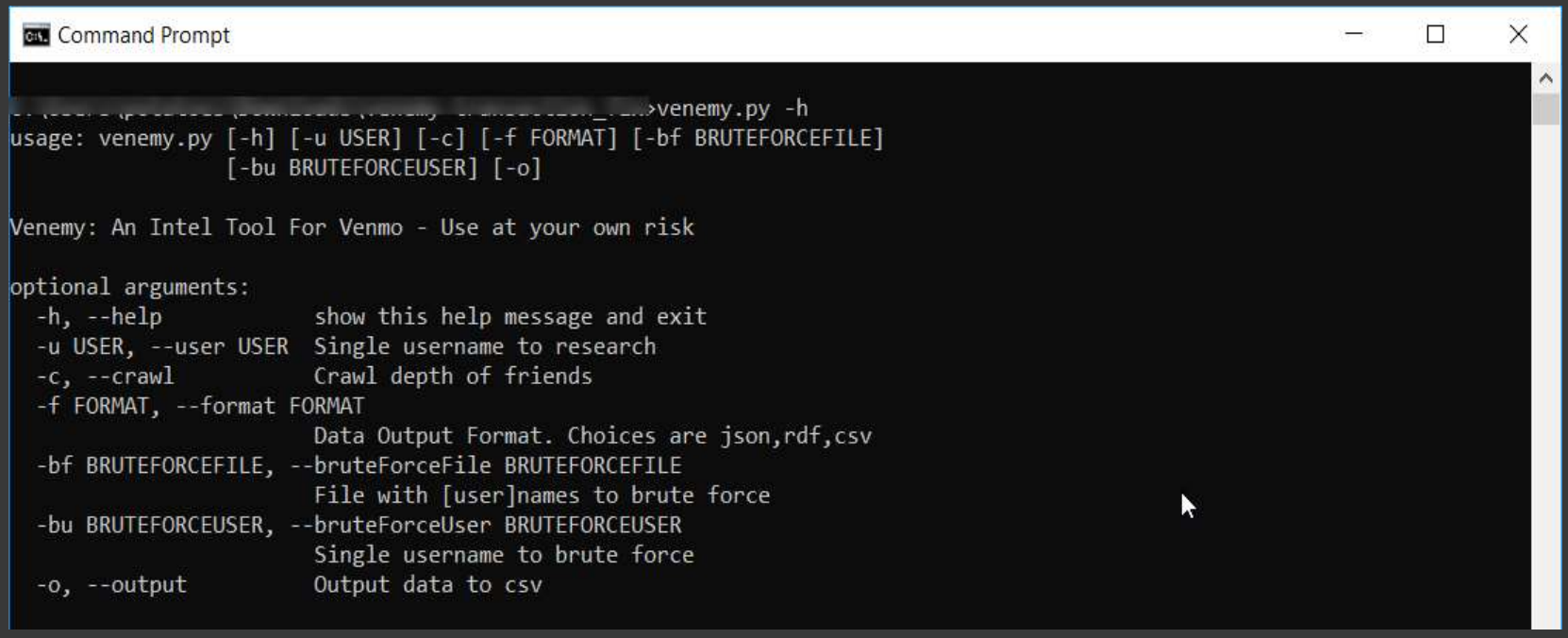
AUTHENTICATED MODULE



AUTHENTICATED MODULE



UNAUTHENTICATED MODULE



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

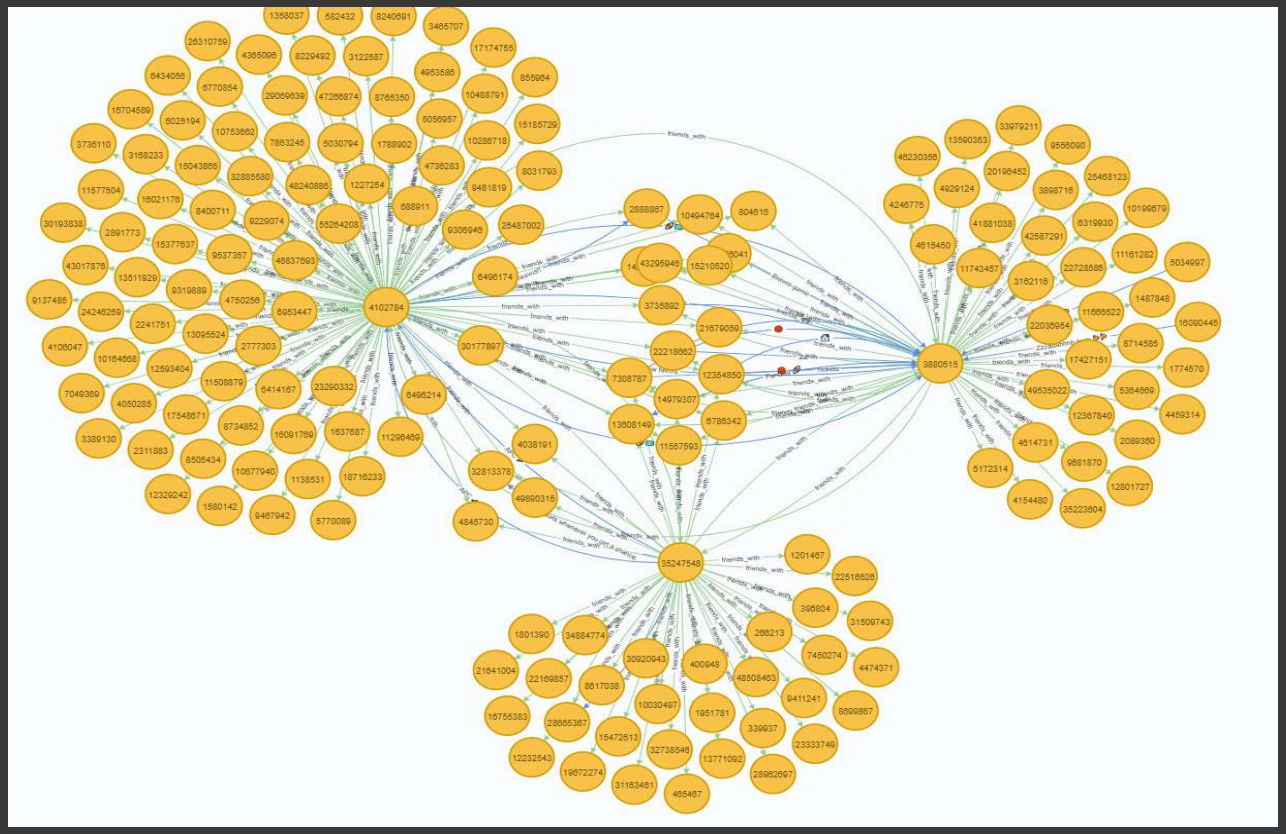
- Accepts CSVs and can even call a URL to load JSON
  - CSV:

```
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)
```

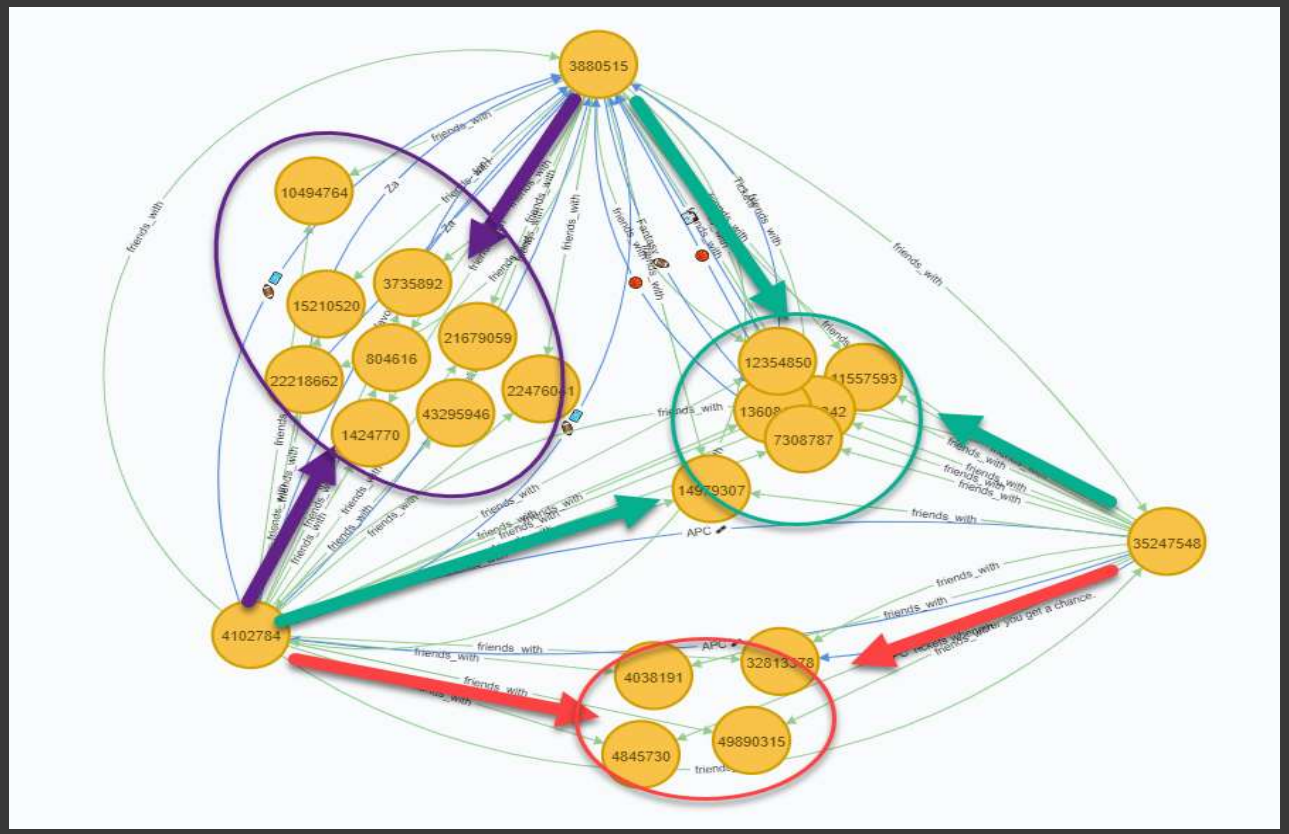
ANALYSIS WITH NEO4J



- Sample: Show me everything

Query: Match (N) return N

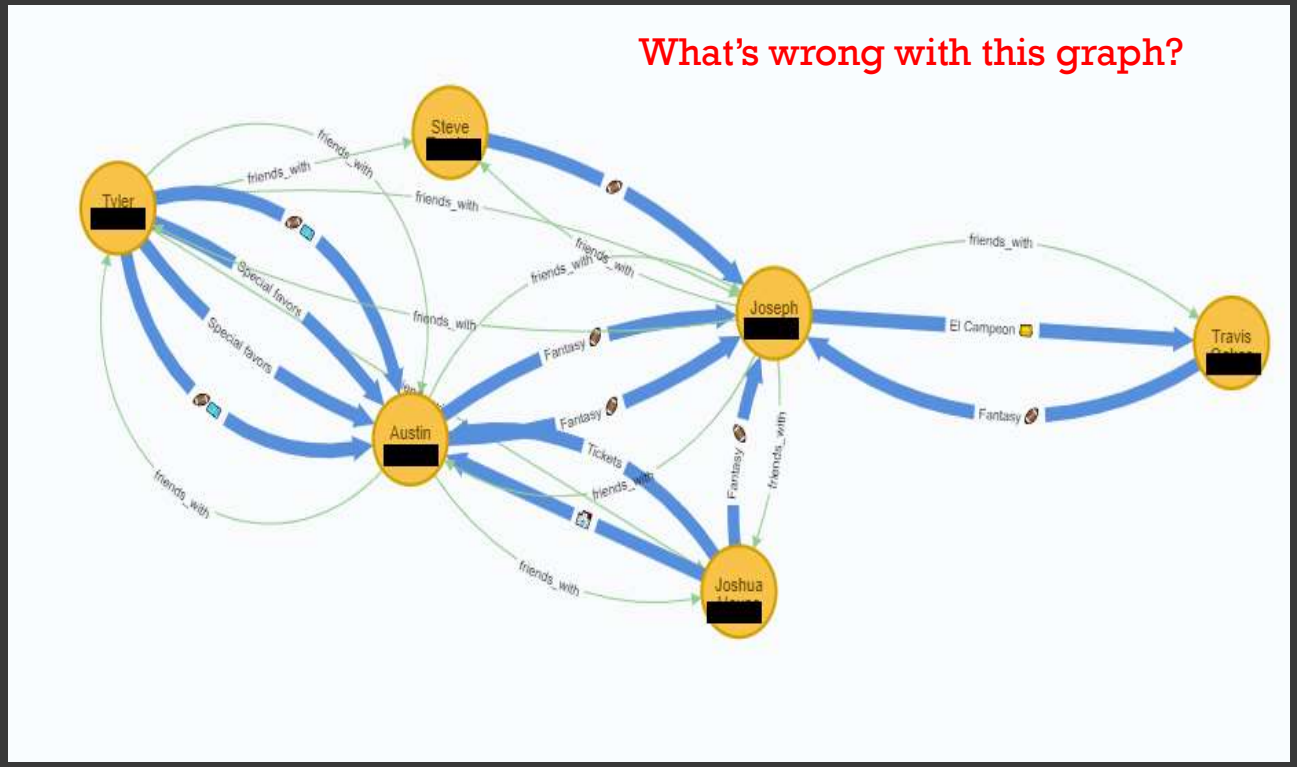
ANALYSIS WITH NEO4J



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

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

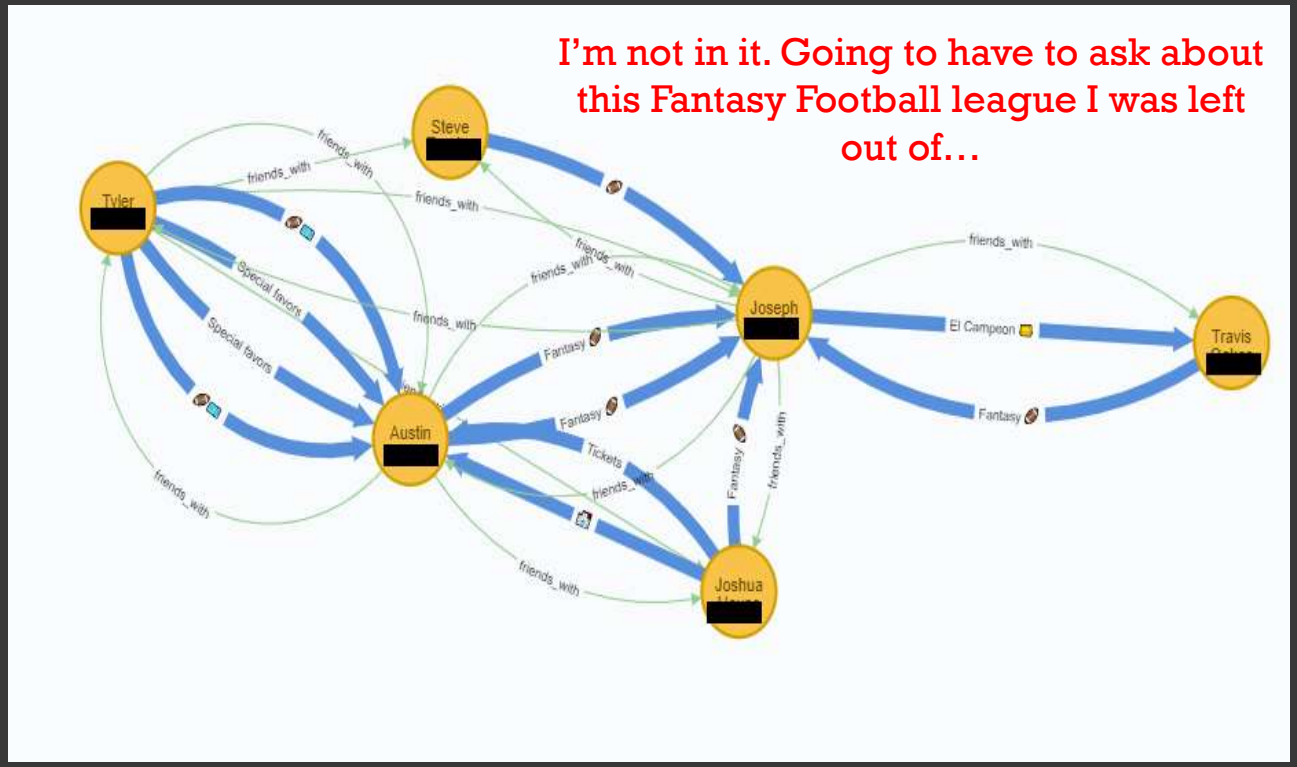
ANALYSIS WITH NEO4J



- Sample: Show transactions of my friends

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

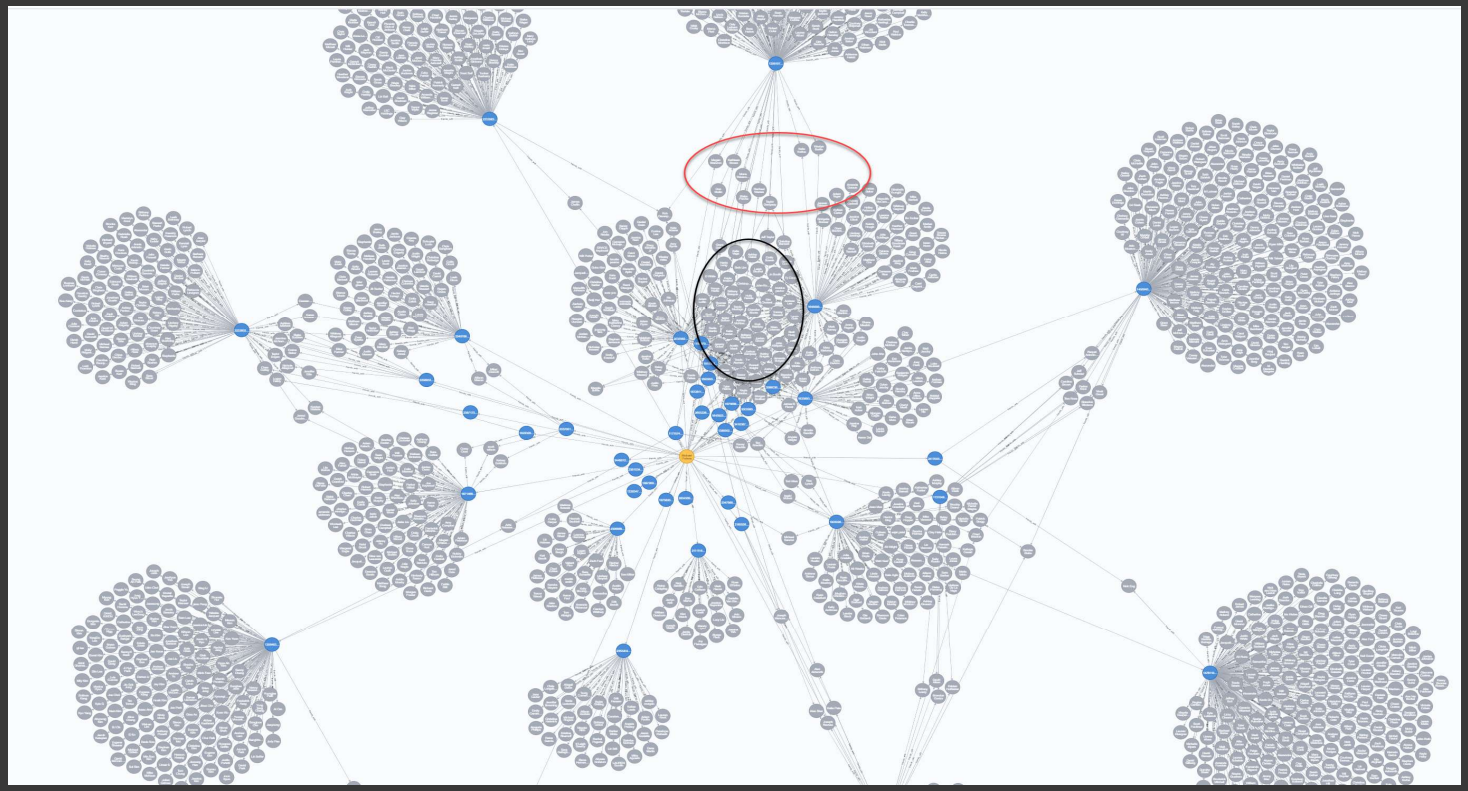
ANALYSIS WITH NEO4J



- Sample: Show transactions of my friends

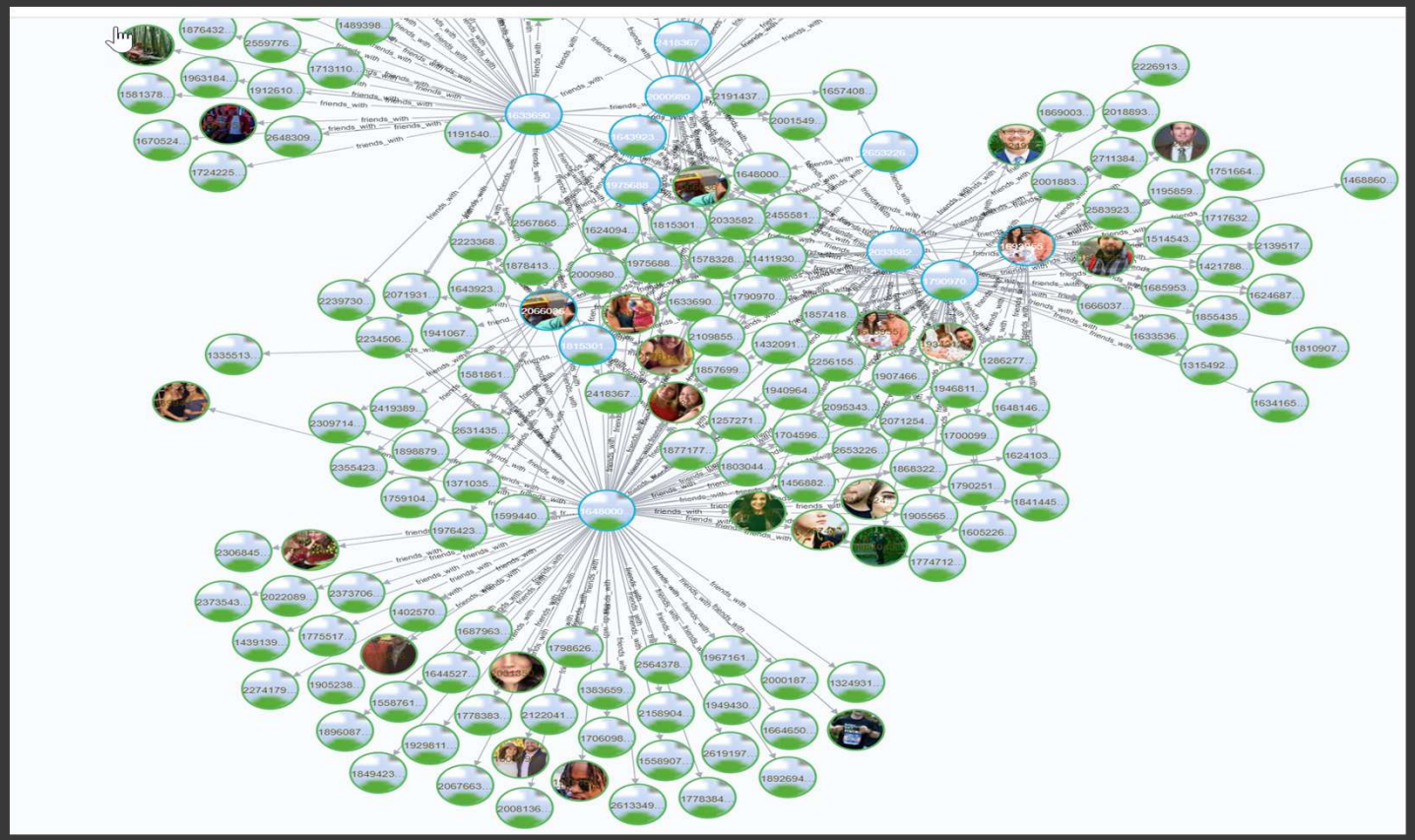
MATCH (p:Person)-[d:paid]->(q:Person) WHERE d.trans =~'.*🏈.*' RETURN p,q

ANALYSIS WITH NEO4J



- Sample: Show the friends of my friends

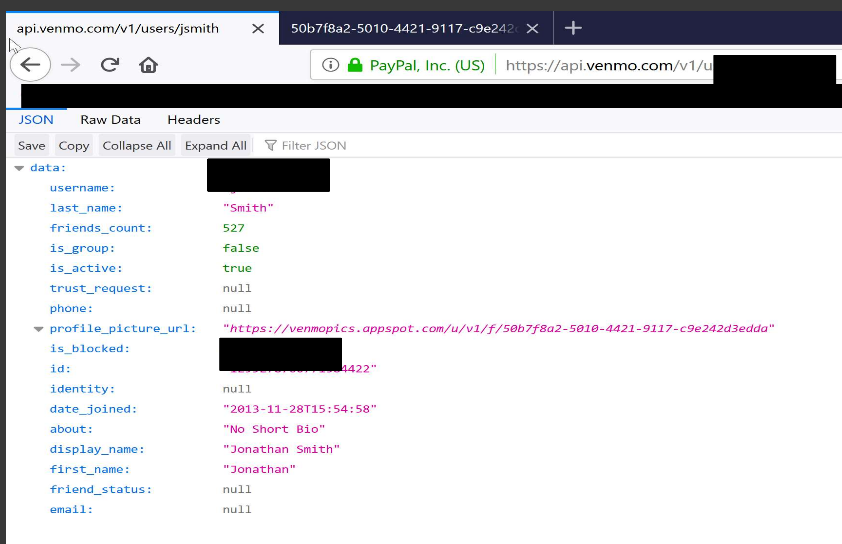
ANALYSIS WITH NEO4J

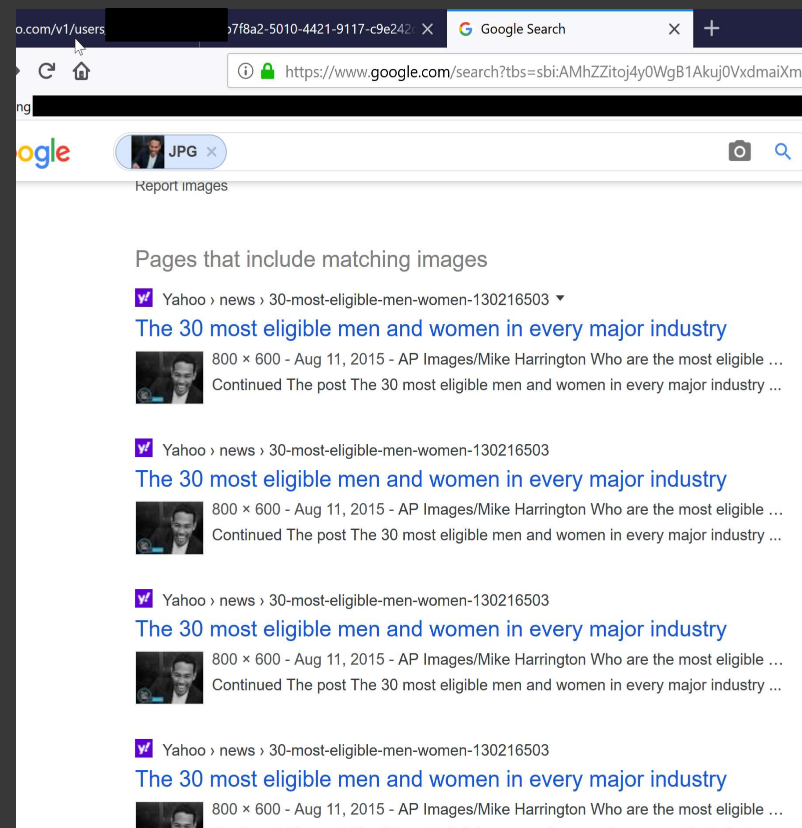


- Sample: Get fancy with some pictures

EXPANDING OUR OSINT

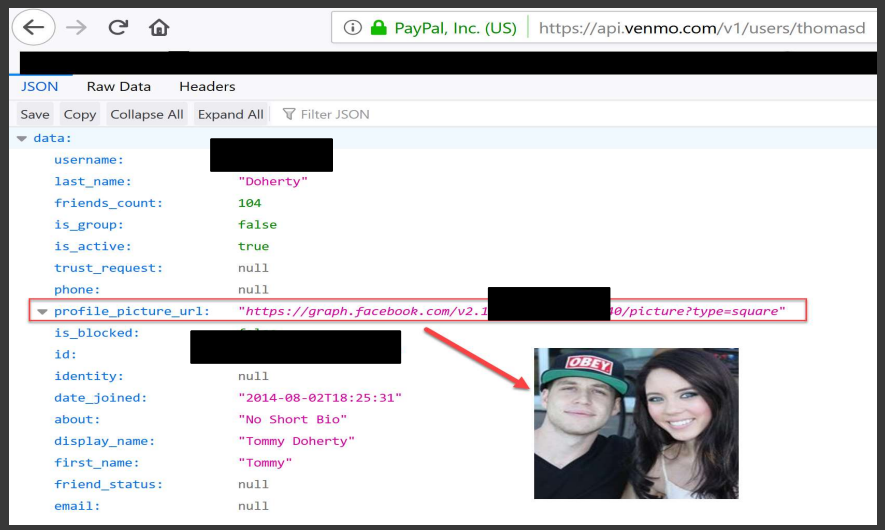
- Reverse image search for more profiles (Google, Tineye, etc)

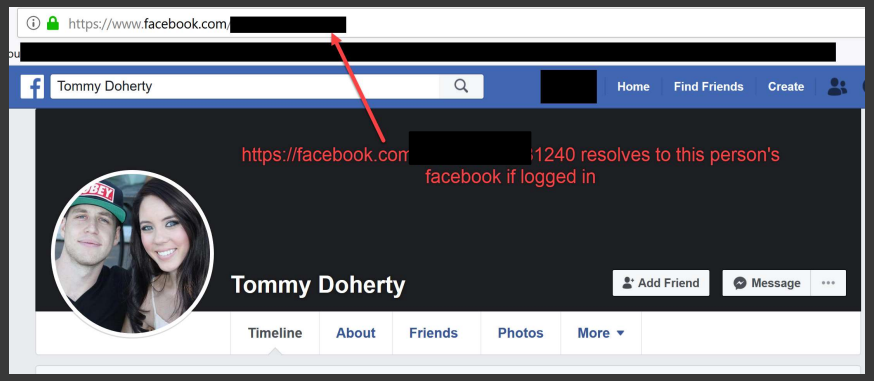


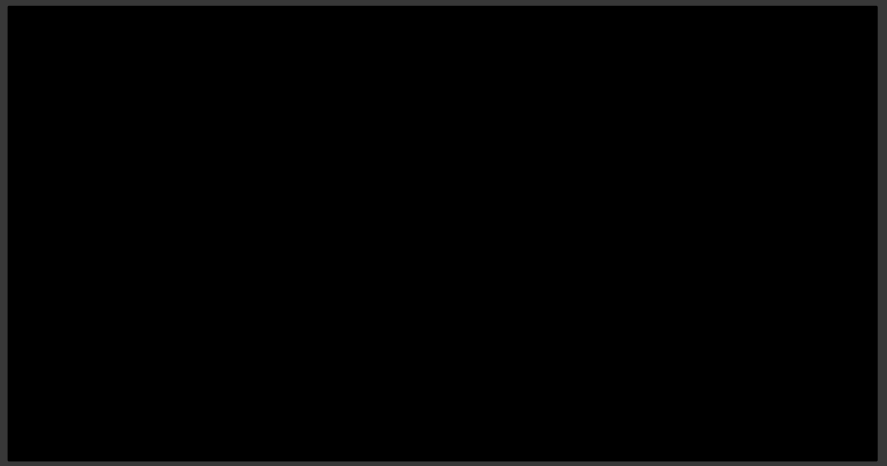


EXPANDING OUR OSINT

- Facebook UserID to Email
  - Can change picture size via ‘picture?type=[square,large,etc]’

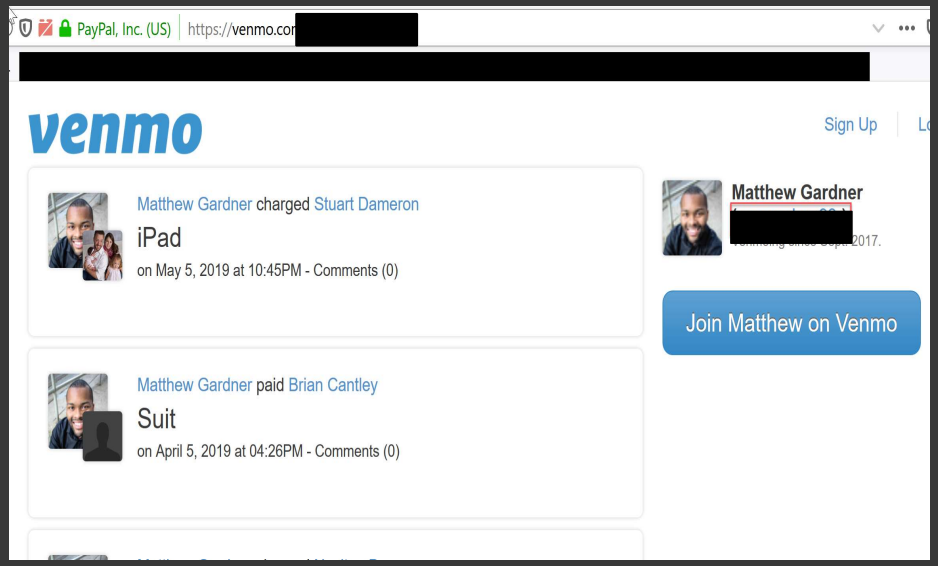


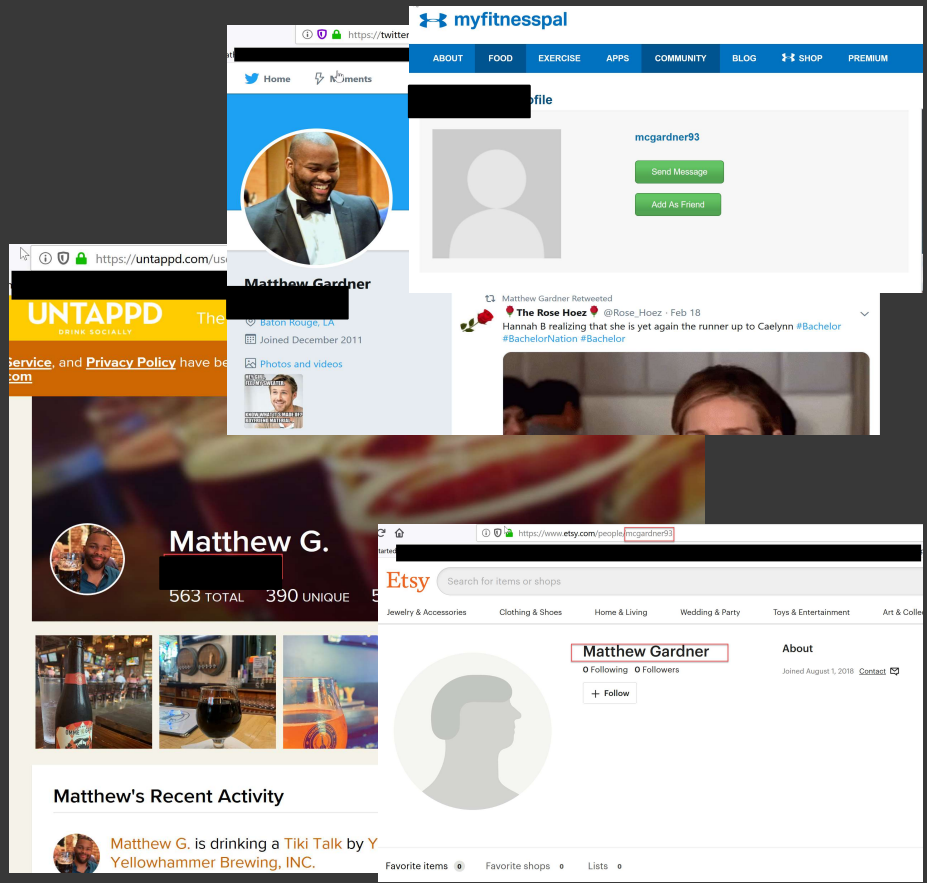




EXPANDING OUR OSINT

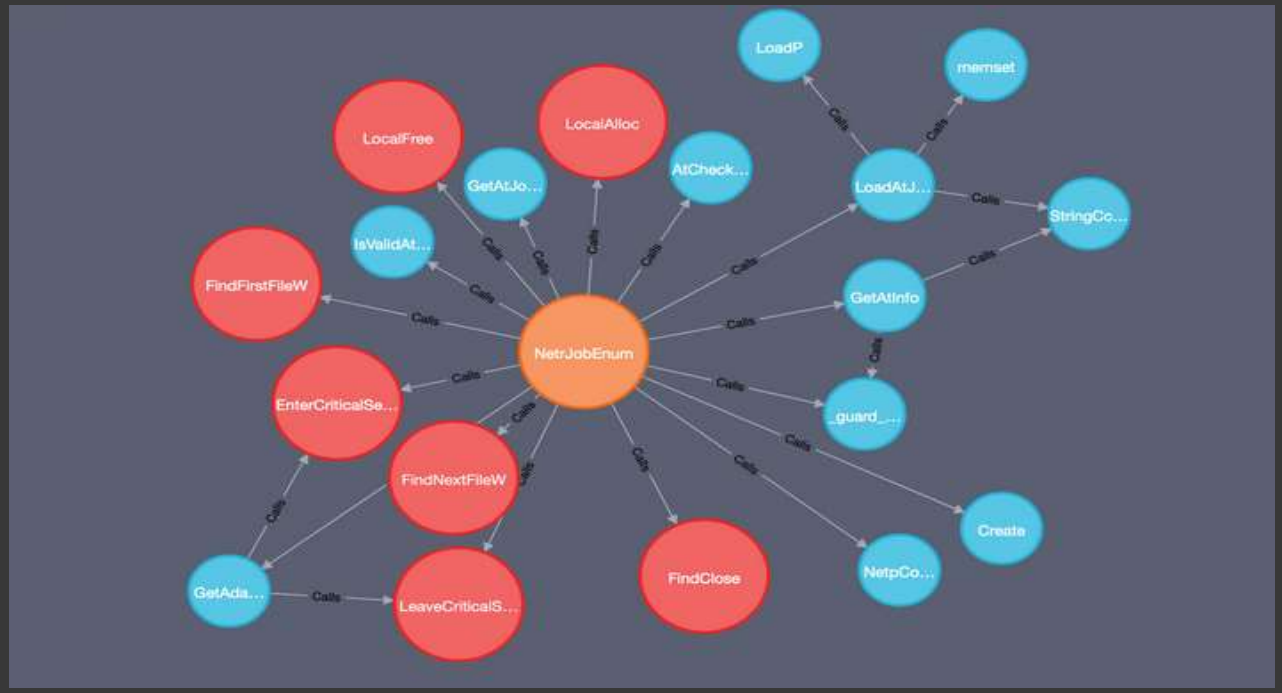
- Username/Name to other profiles





EXPANDING OUR NEO4J

- Red Teams: New TTPs

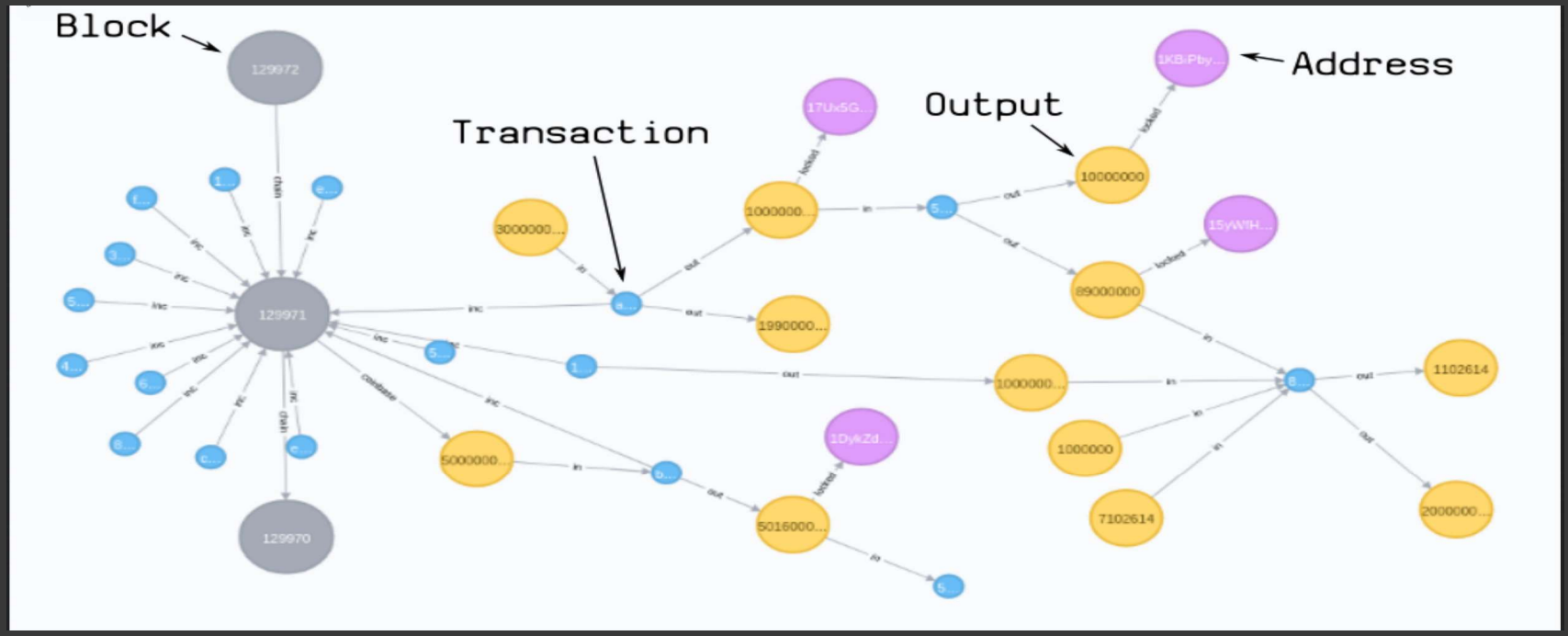


- "Analyzing RPC with Ghidra and Neo4j"
- Analyzing binary functions and calls
- What else?!

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

EXPANDING OUR NEO4J

- CI/LE: Analyzing bitcoin transactions #followthemoney



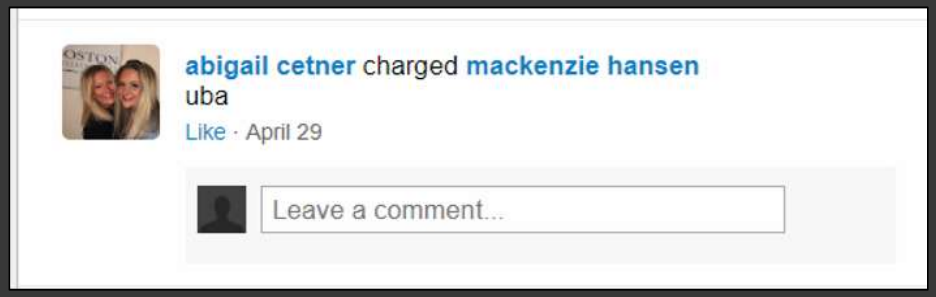
Source: https://neo4j.com/blog/import-bitcoin-blockchain-neo4j/

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

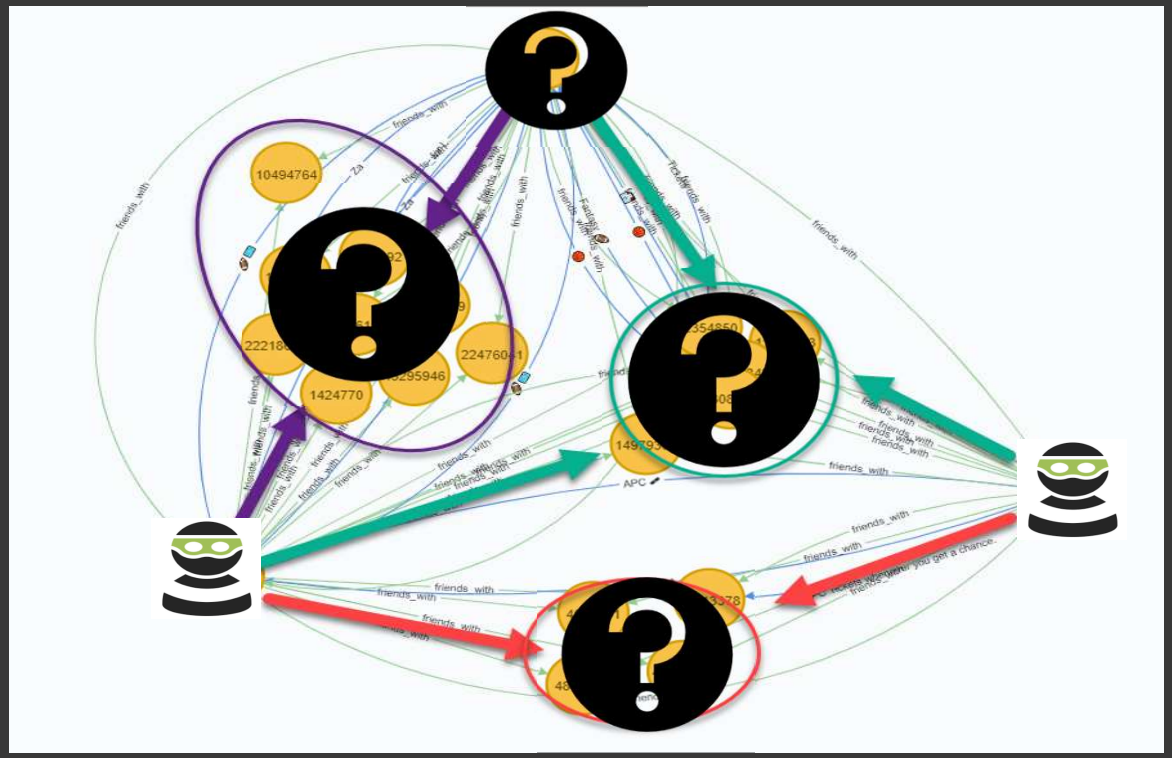


To: cetner@email.com
From: noreply@ubersupport.tech
"There was an issue with your transaction on April 29…please see the attached or visit <>"

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

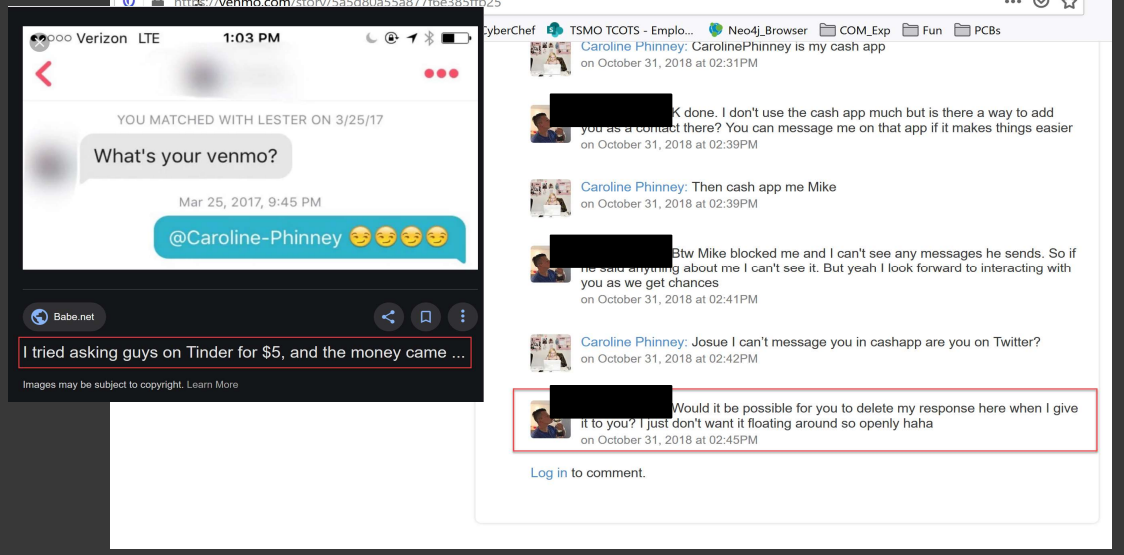
- CI/LE: Persons of Interest

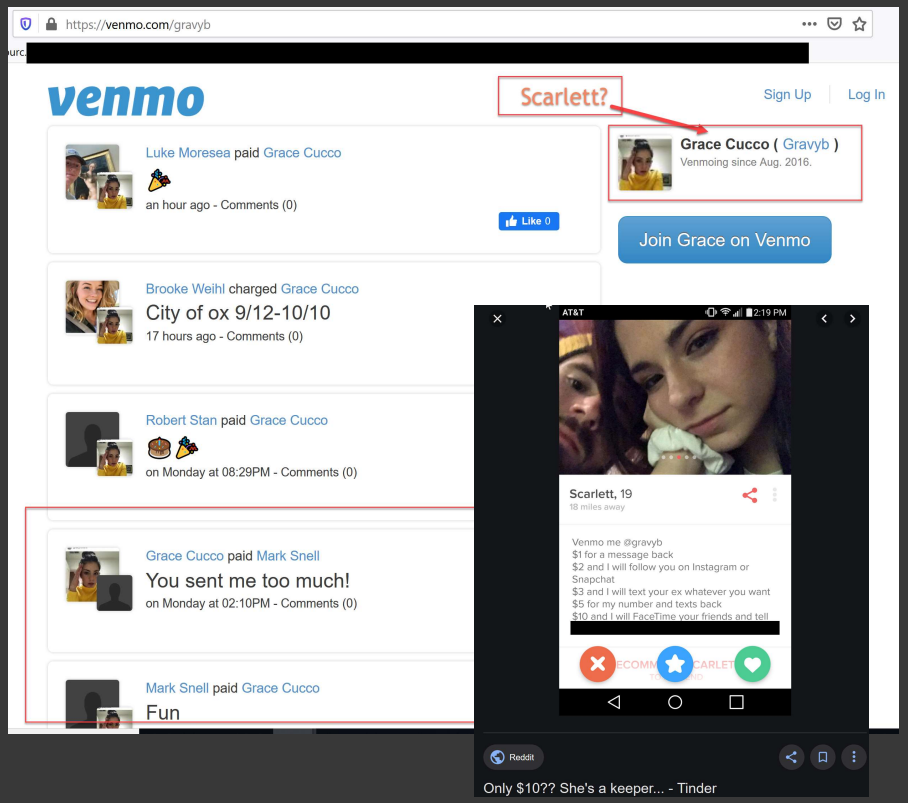


- Whose are the common contacts amongst the persons of interest?
- Are there different contacts from other social media outlets?

SAMPLE USE CASE

- Personal Security: Bot and fraud detection





TIPS

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