# TraceLabs OSINT CTF
# Team BoxedOlive’s inaugural experience
# …

Jenn & hardBox

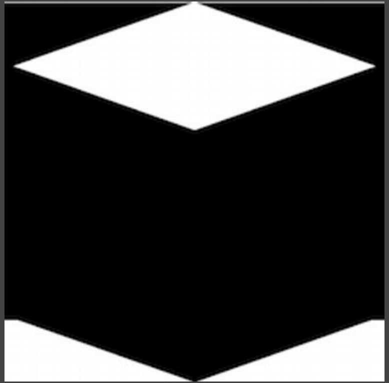
SLIDES

B|Sides Vancouver

# A bit about us

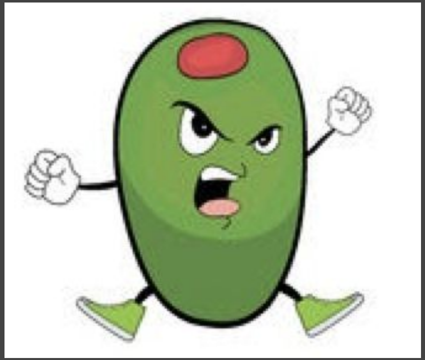
Darren aka hardBox

- Privacy, COM/OPSEC, moar
- OSINT, OSINT, OSINT!!!



Jenn aka Angry0live

- Appsec, privacy & compliance nerd
- OSINT enthusiast



# Intro

What is OSINT?

- Open Source Intelligence - aka OSINT - is intelligence “drawn from publicly available material”
  - Stuff your mom or grandma posts on Facebook

What is TraceLabs?

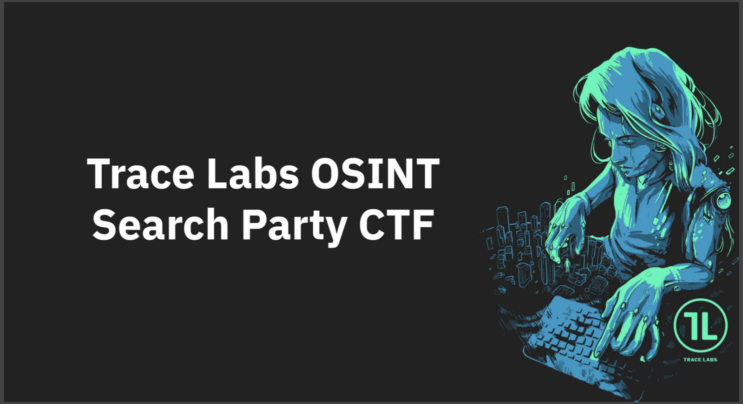
- Trace Labs is a nonprofit organization whose mission is to accelerate the family reunification of missing persons while training members in the tradecraft of open source intelligence (OSINT).

What is TraceLabs CTF?

- A regular CTF where new and seasoned OSINT enthusiasts alike get together for a friendly competition, where the outcome has real-world benefit

# How does TL-CTF work?

- Basics
  - Create an account on their platform
  - Give yourself a team name or join a team.
    - Teams of 1 are acceptable, max 4.
  - Join the intro call
    - Lots of good info
    - Rules of engagement (*these are important since these are real people in real life situations!*)
  - At kickoff, the subject info will be released
    - Subject names and some pertinent info to send you in the right direction
  - Discord channel for help & communicating with your judge



# How does TL-CTF work?

- Basics
  - After kickoff, you spend the next 4-6 hours scouring the internet looking for flags to score some **sweet points**
    - Most CTF's are designed for you to find flags that are deliberately placed in a system
    - Flags for this CTF are made up of real-world breadcrumbs that are related to the subject.
  - Submit the evidence like you're going to be audited - your submissions are judged
    - Screenshot, category, and *why* you think this is relevant to the subject
  - Evidence gets submitted to law enforcement to help with the case
- *Strict no-contact rule*
  - Passive OSINT/recon only
    - Collect & submit evidence
  - The subject does not want to be your Instagram friend, and this could seriously damage the hard work Law Enforcement has put in to date
  - No password resets allowed

# TL CTF Scoring System

## Friends/10 points

Relevant information on Friends. Including but not limited to:

- Name
- Aliases
- Birthdate
- IDs (driver’s license, passport, library card etc.)
- Work address
- Work phone number
- Email
- Home address
- Home phone number
- Social media handle
- any insightful info from friend’s comments

## Employment/15 points

Relevant information on Employment. Including but not limited to:

- Business Name
- Aliases
- Manager Name
- Start Date
- End Date
- IDs (badge, license, etc)
- Business Address
- Business Phone
- Email
- Social media handle
- any insightful info from employer’s comments

# TL CTF Scoring System

## Family/20 points

Relevant information on Family. Including but not limited to:

- Name
- Aliases
- Birth dates
- IDs (driver's license, passport, library card, etc.)
- Home address
- Home phone number
- Work address
- Work phone number
- Email
- Social media handle
- any insightful info from Family's comments

## Home/25 points

Relevant information on subject's home. Including but not limited to:

- Address
- Landlord's name
- Landlord's phone number
- Recent accommodations
- Any meaningful interactions with the landlord
- Risks in the immediate area (e.g. sex offenders)
- Habits (e.g. couch surfing)

# TL CTF Scoring System

## Basic Subject Info/50 points

Basic relevant information regarding subject.
Including but not limited to:

- Name
- Aliases
- Birth date
- IDs (driver's license, passport, library card, etc.)
- Emails
- Social media handles
- Blogs or forum profile & relevant posts
- Personal websites
- Dating site profiles & relevant posts
- Craigslist or Kijiji profile & relevant posts
- Reddit accounts or sites of similar nature
- Online resume
- Physical description

## Advanced Subject Info/150 points

Advanced relevant information regarding the subject.
This can include but not limited to:

- Unique identifiers (e.g. tattoos, scars, piercings)
- Medical issues
- Habits (e.g. smoking, drinking, hitchiking, hangouts)
- Previous missing persons history
- Brand, model & carrier of cell phone(s)
- Vehicle year, colour, make/model, licence plate(s)
- Video game handles (e.g. xbox)
- IP address
- Any other information about where the subject might be headed

# TL CTF Scoring System

## Day Last Seen/500 points

Relevant information regarding the subject's last day seen. This can include but not limited to:

- Pictures of subject on day last seen (e.g. CCTV)
- Details of subject on day last seen (e.g. mood, altercations, conversations, etc)
- Person last seen with
- Intent to meet with someone
- Direction of travel
- Other details that relates to the day last seen

## Dark Web/1000 points

Relevant information on subject's home. Including but not limited to:

- Picture or details of subject sites such as backpage
- Discussion regarding subject on dark web sites
- The sales of goods by the subject on the dark web
- Any activity or post by the subject on the dark web
- Password breach data that includes the subject's username

## Location/5000 points

Relevant information pertaining to the current location of the subject.
This can include but not limited to:

- New information on location (not including Police update saying the person was found or an obituary
  - this is worth 150 points and under the category of Advanced Subject Info

# Prep

- Tickets
  - Eventbrite
  - EarlyBird tickets come with some free OSINT training
    - Darren was an earlybird
    - Jenn was sad

- team - BoxedOlive
  - Darren set up the team
  - Easy setup, one person sets up & sends the invite code
  - Team is necessary for participation - 1 - 4 members

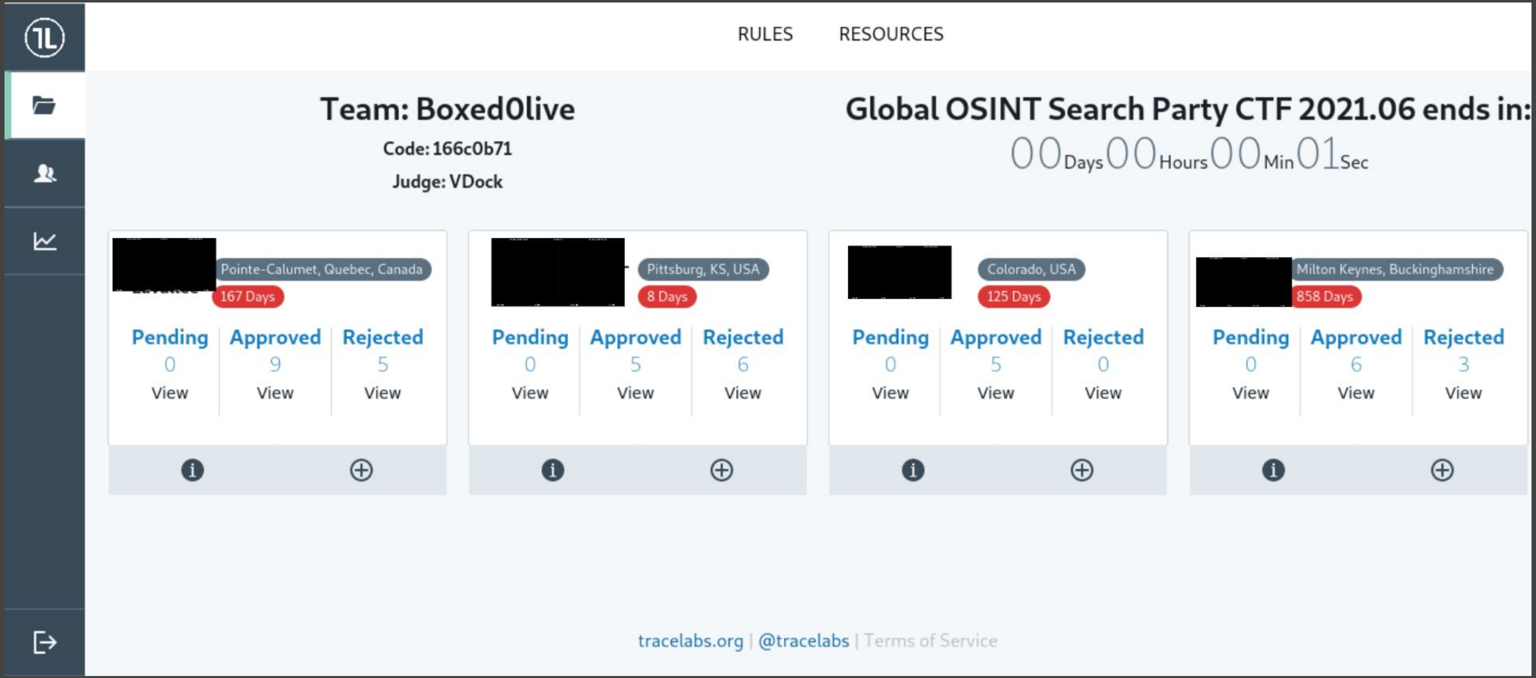
# Prep 2

- Tools
  - Jenn
    - Search engines, Michael Bazell books, Youtube, Darren, Sublime text
  - Darren
    - Basically pro level
    - ALL THE TOOLS - Start.me page
- Socks
  - Jenn
    - I was coming into this to learn, so I did a lot of searching on existing accounts (alphabet) but did create a new TikTok/Insta/Facebook account.
    - Might not do this again unless I was doing a lot of OSINT
  - Darren
    - Used existing passive research socks I have setup
    - Proper Socks setup takes time and your procedure depends on your OPSEC needs
- Comms - Private Discord Server
  - Shared Intel of the four subjects on Discord
    - Links to social media & news articles
  - MindMap

# D Day

- June 26th, 2021
- Kickoff at 8am PDT
- CTF starts 9am PDT
    - 6 hours play
- 4 subjects to look for (this time)
    - The subjects and number of subjects changes event to event
- Worldwide subjects, worldwide participation
- Coffee, coffee, coffee
- Searching and submitting flags
- 4pm Closing

# TL CTF Team Interface



Team: BoxedOlive

Code: 166c0b71

Judge: VDock

Global OSINT Search Party CTF 2021.06 ends in:

00 Days 00 Hours 00 Min 01 Sec

[redacted] Pointe-Calumet, Quebec, Canada

167 Days

| Pending | Approved | Rejected |
|---|---|---|
| 0 | 9 | 5 |
| View | View | View |

[redacted] Pittsburg, KS, USA

8 Days

| Pending | Approved | Rejected |
|---|---|---|
| 0 | 5 | 6 |
| View | View | View |

[redacted] Colorado, USA

125 Days

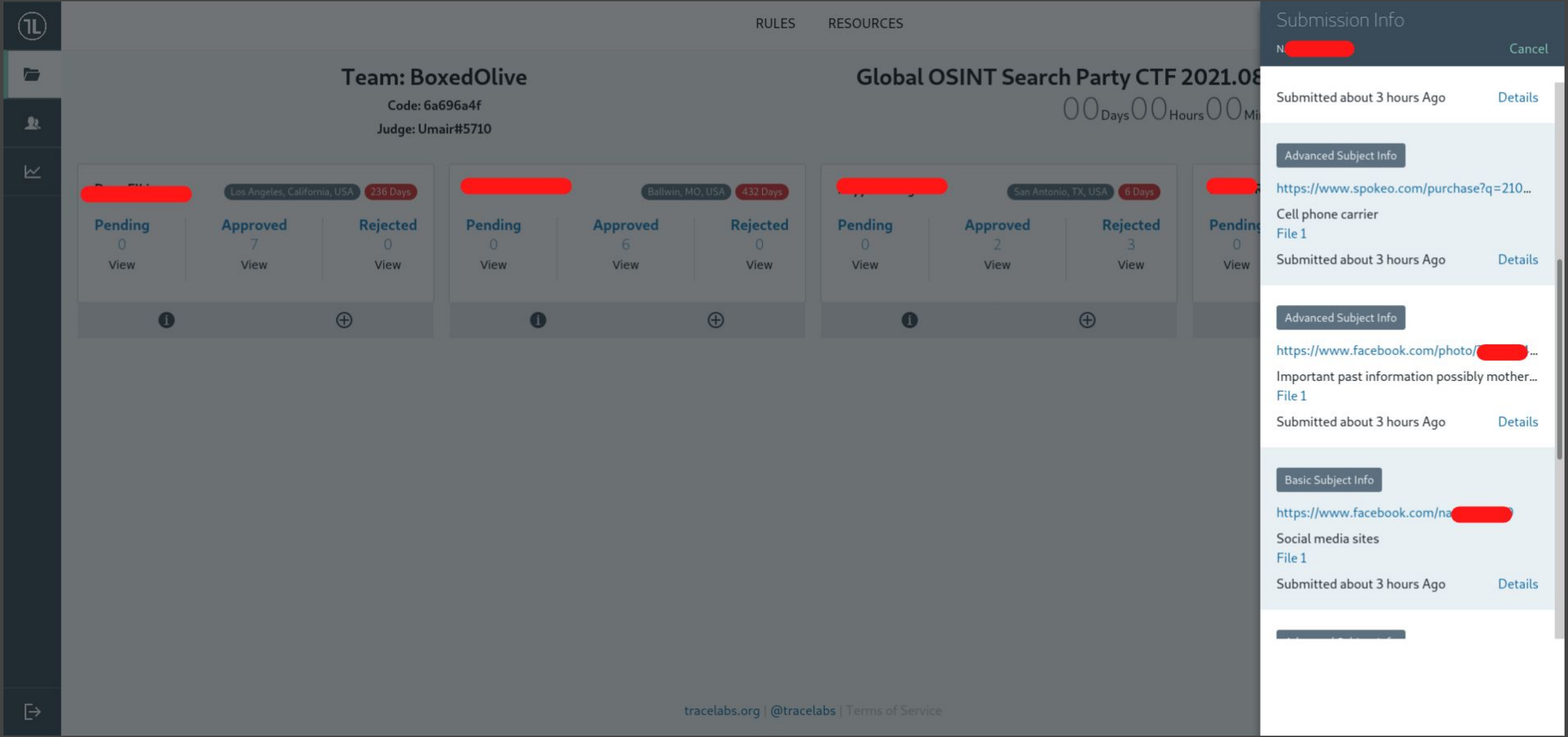
| Pending | Approved | Rejected |
|---|---|---|
| 0 | 5 | 0 |
| View | View | View |

[redacted] Milton Keynes, Buckinghamshire

858 Days

| Pending | Approved | Rejected |
|---|---|---|
| 0 | 6 | 3 |
| View | View | View |

tracelabs.org | @tracelabs | Terms of Service



Team: BoxedOlive

Code: 6a696a4f

Judge: Umair#5710

Global OSINT Search Party CTF 2021.08

00 Days 00 Hours 00 Mi

[redacted] Los Angeles, California, USA 236 Days

| Pending | Approved | Rejected |
|---|---|---|
| 0 | 7 | 0 |
| View | View | View |

[redacted] Ballwin, MO, USA 432 Days

| Pending | Approved | Rejected |
|---|---|---|
| 0 | 6 | 0 |
| View | View | View |

[redacted] San Antonio, TX, USA 6 Days

| Pending | Approved | Rejected |
|---|---|---|
| 0 | 2 | 3 |
| View | View | View |

[redacted]

| Pending |
|---|
| 0 |
| View |

Submission Info

N[redacted] Cancel

Submitted about 3 hours Ago Details

Advanced Subject Info

https://www.spokeo.com/purchase?q=210...

Cell phone carrier

File 1

Submitted about 3 hours Ago Details

Advanced Subject Info

https://www.facebook.com/photo/[redacted]...

Important past information possibly mother...

File 1

Submitted about 3 hours Ago Details

Basic Subject Info

https://www.facebook.com/na[redacted]

Social media sites

File 1

Submitted about 3 hours Ago Details

tracelabs.org | @tracelabs | Terms of Service

# Lessons

- Jenn
  - Don’t spend too much time on one subject, burnout happens
  - Document *everything*
  - Might use a screen recorder next time + voiceover to walk through thoughts
  - Take breaks regularly
  - The emotional impact is real
  - Mindmapping makes sense in this kind of activity
- Darren
  - Review the point system details
  - Contact your judge after your first submission
  - Coordinate with your team members, have regular voice check-ins
  - Document your research and submitted flags in Discord/mind map

# Tools

- ★ Epieos Mail Checker https://tools.epieos.com/email.php
- ★ UserName Checker / Holohe https://whatsmyname.app
- ★ Spiderfoot https://github.com/smicallef/spiderfoot
- ★ OSINT Framework https://osintframework.com/
- ★ Multiple search engines - not just Google/Bing/DDG
- ★ Most of Darren's online and other tools are on the Start.me page
- ★ TweetBeaver - data on twitter accounts

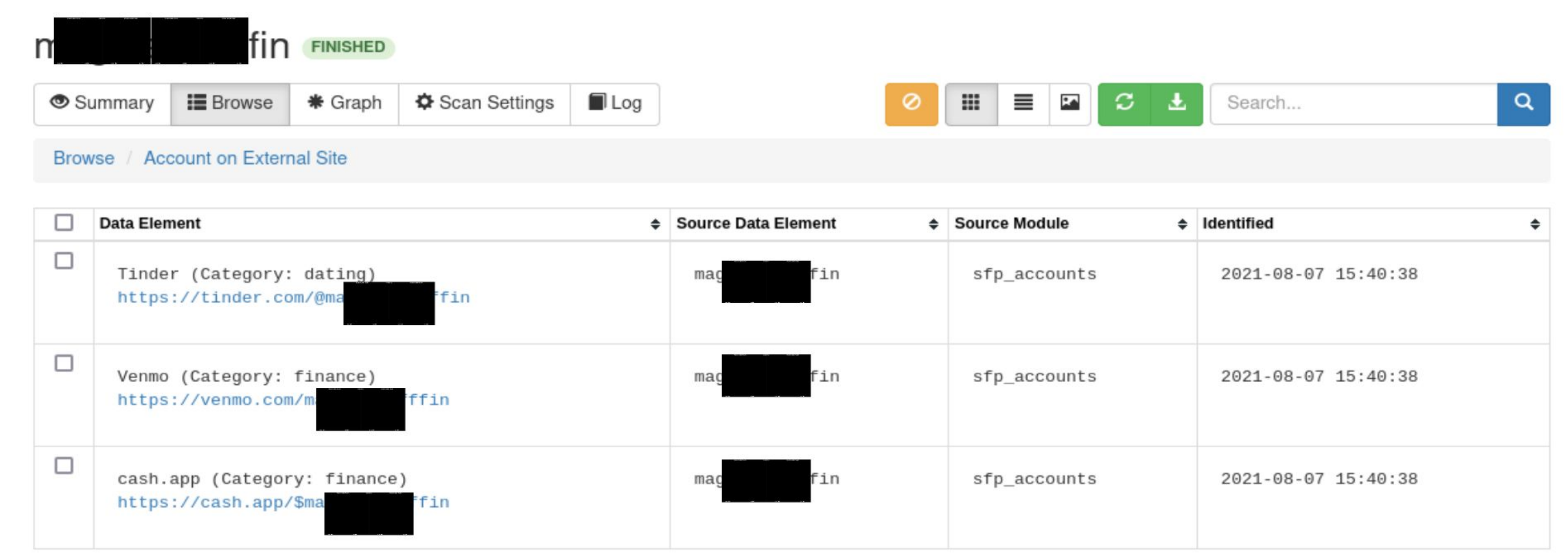
# Spiderfoot

SpiderFoot is an Open Source Intelligence tool written in Python that was developed by Steve Micallef in his free time.

The tool queries over 100 public information services and provides you with intelligence data about domain names, email addresses, names, IP addresses, DNS servers and much more. SpiderFoot has over 100 modules so anyone interested in security, from beginners to professionals can understand their security perimeter.

https://www.spiderfoot.net

# Spiderfoot



m[redacted]fin FINISHED

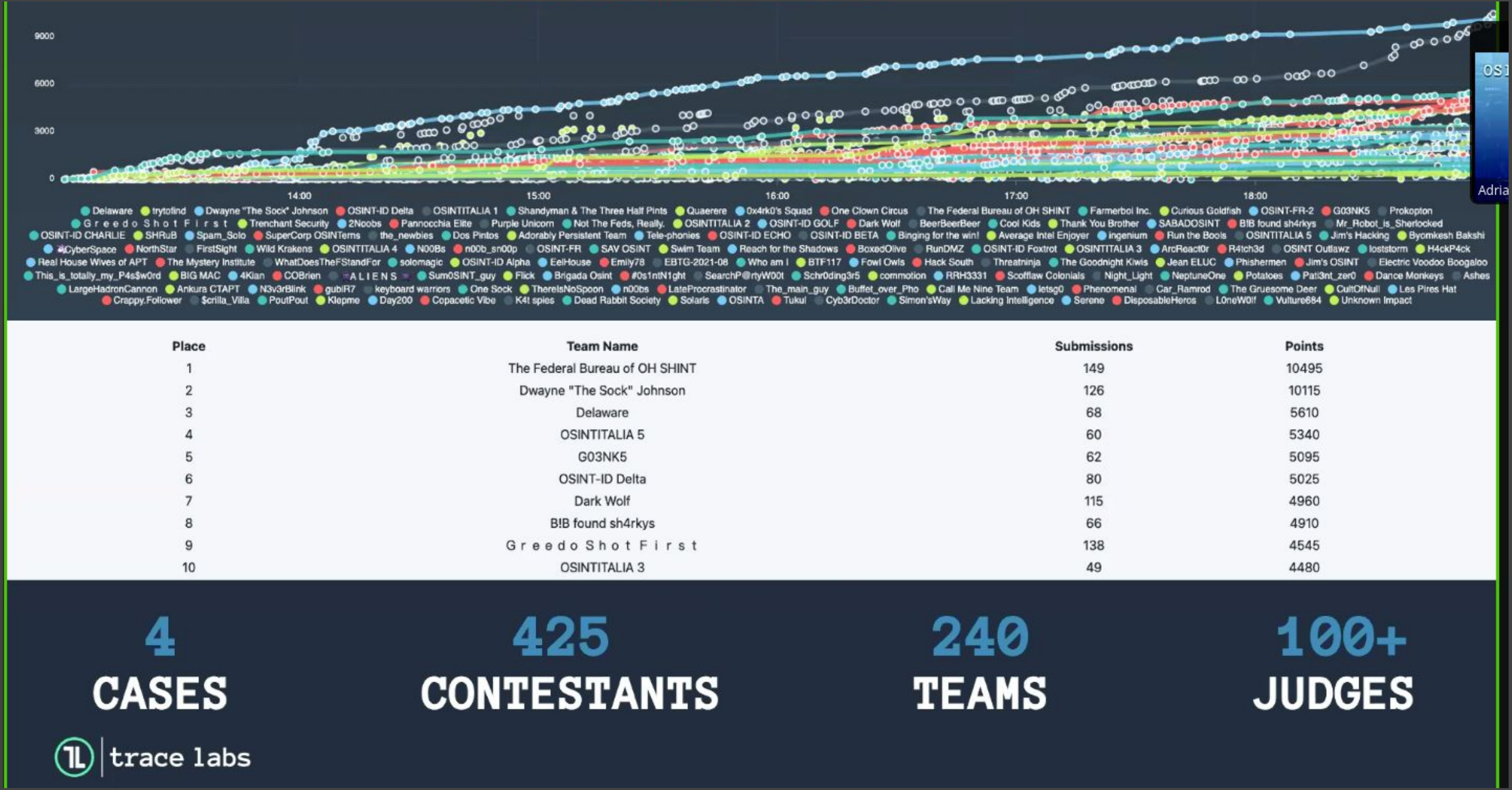
Browse / Account on External Site

| □ | Data Element | Source Data Element | Source Module | Identified |
|---|---|---|---|---|
| □ | Tinder (Category: dating)<br>https://tinder.com/@ma[redacted]ffin | mag[redacted]fin | sfp_accounts | 2021-08-07 15:40:38 |
| □ | Venmo (Category: finance)<br>https://venmo.com/m[redacted]ffin | mag[redacted]fin | sfp_accounts | 2021-08-07 15:40:38 |
| □ | cash.app (Category: finance)<br>https://cash.app/$ma[redacted]ffin | mag[redacted]fin | sfp_accounts | 2021-08-07 15:40:38 |

# Flags

- News stories (inadmissible) led to things like
  - Employment flags
  - Family & friends flags (name, photos, employment)
- Multiple flags from one username
- Higher points flags - cell phone type and carrier
- Review the type of flags and what they are worth before the CTF
- Expect to have some flags get rejected
- Talk to your judge!
- Be like Ross

# EndGame



| Place | Team Name | Submissions | Points |
|---|---|---|---|
| 1 | The Federal Bureau of OH SHINT | 149 | 10495 |
| 2 | Dwayne "The Sock" Johnson | 126 | 10115 |
| 3 | Delaware | 68 | 5610 |
| 4 | OSINTITALIA 5 | 60 | 5340 |
| 5 | G03NK5 | 62 | 5095 |
| 6 | OSINT-ID Delta | 80 | 5025 |
| 7 | Dark Wolf | 115 | 4960 |
| 8 | B!B found sh4rkys | 66 | 4910 |
| 9 | Greedo Shot First | 138 | 4545 |
| 10 | OSINTITALIA 3 | 49 | 4480 |

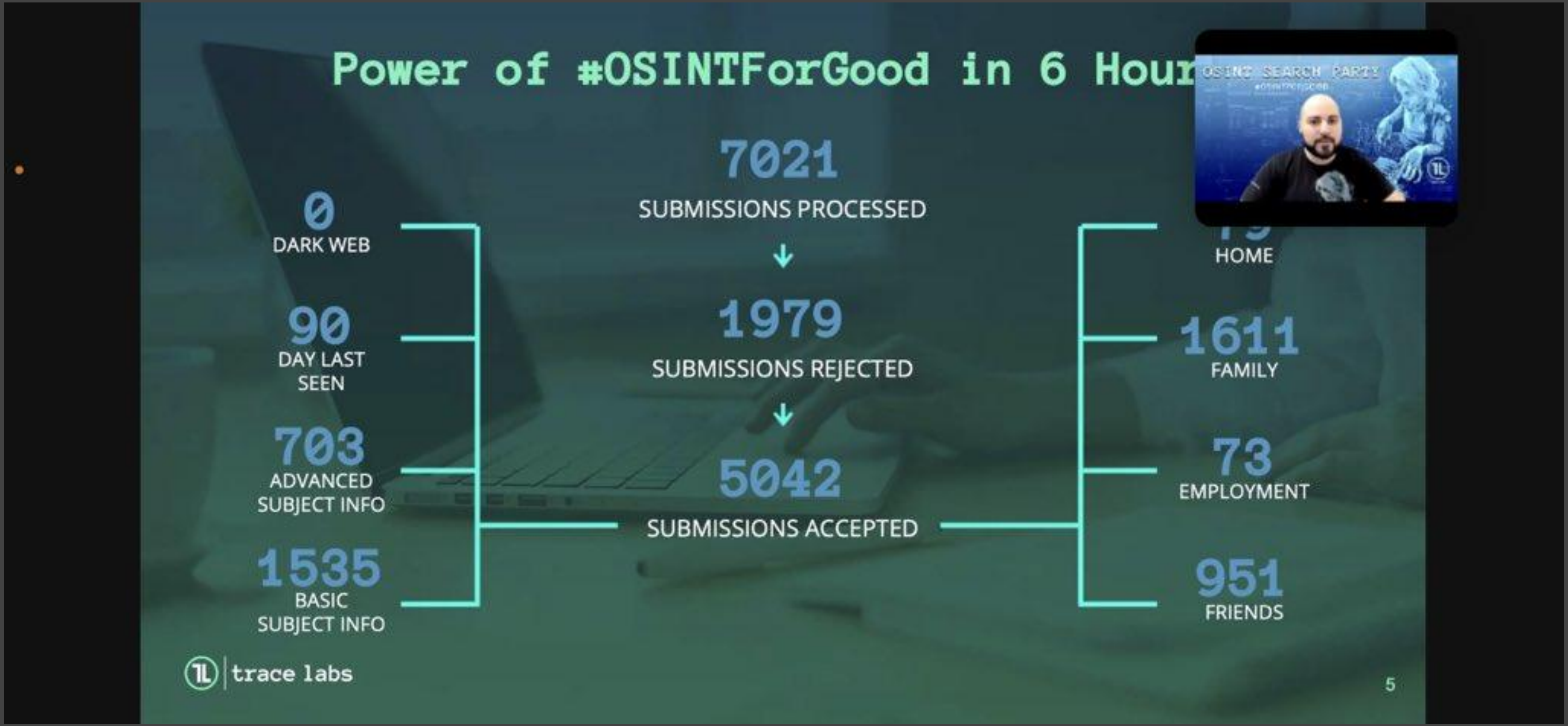
**4** CASES

**425** CONTESTANTS

**240** TEAMS

**100+** JUDGES

# EndGame



## Power of #OSINTForGood in 6 Hour

7021
SUBMISSIONS PROCESSED

↓

1979
SUBMISSIONS REJECTED

↓

5042
SUBMISSIONS ACCEPTED

0
DARK WEB

90
DAY LAST SEEN

703
ADVANCED SUBJECT INFO

1535
BASIC SUBJECT INFO

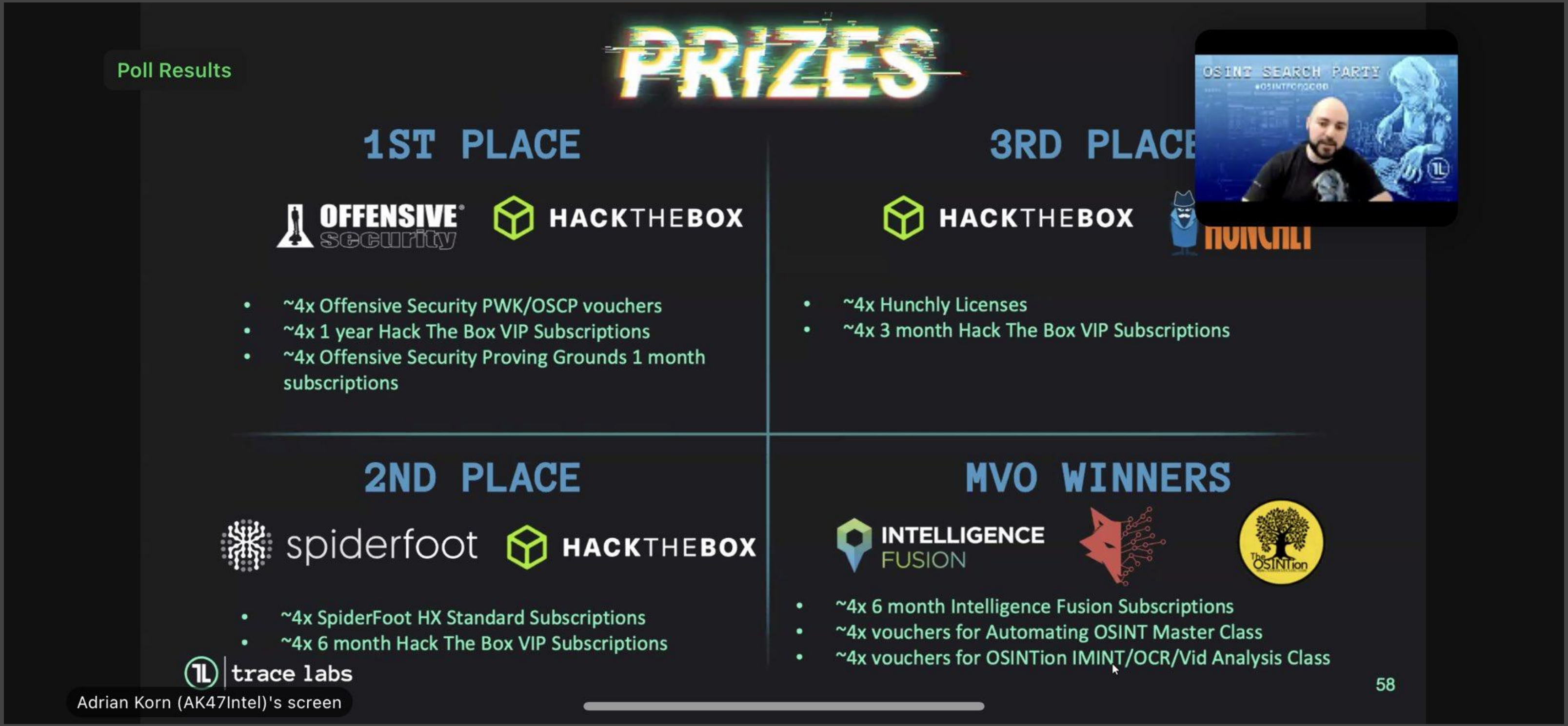
[illegible]
HOME

1611
FAMILY

73
EMPLOYMENT

951
FRIENDS

# EndGame



## PRIZES

### 1ST PLACE

- ~4x Offensive Security PWK/OSCP vouchers
- ~4x 1 year Hack The Box VIP Subscriptions
- ~4x Offensive Security Proving Grounds 1 month subscriptions

### 3RD PLACE

- ~4x Hunchly Licenses
- ~4x 3 month Hack The Box VIP Subscriptions

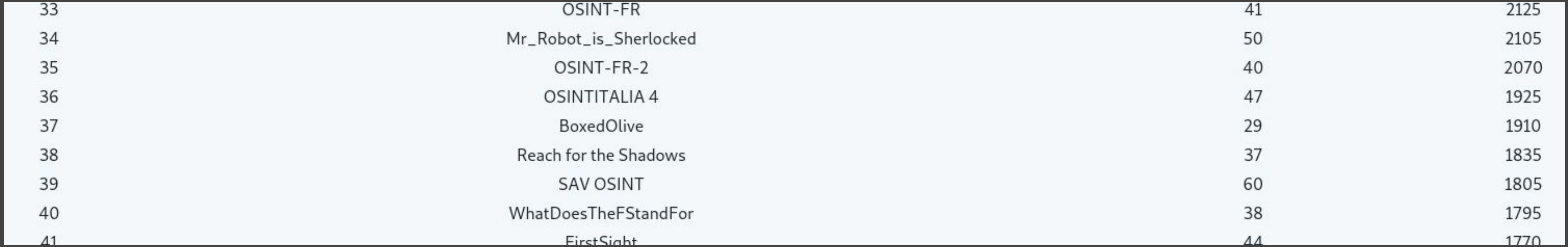
### 2ND PLACE

- ~4x SpiderFoot HX Standard Subscriptions
- ~4x 6 month Hack The Box VIP Subscriptions

### MVO WINNERS

- ~4x 6 month Intelligence Fusion Subscriptions
- ~4x vouchers for Automating OSINT Master Class
- ~4x vouchers for OSINTion IMINT/OCR/Vid Analysis Class

# End Game - Our Score



| Standings | Teams | Submissions | Score |
|---|---|---|---|
| 33 | OSINT-FR | 41 | 2125 |
| 34 | Mr_Robot_is_Sherlocked | 50 | 2105 |
| 35 | OSINT-FR-2 | 40 | 2070 |
| 36 | OSINTITALIA 4 | 47 | 1925 |
| 37 | BoxedOlive | 29 | 1910 |
| 38 | Reach for the Shadows | 37 | 1835 |
| 39 | SAV OSINT | 60 | 1805 |
| 40 | WhatDoesTheFStandFor | 38 | 1795 |
| 41 | FirstSight | 44 | 1770 |

# Resources

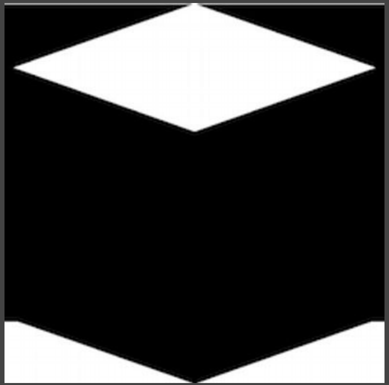
- https://www.tracelabs.org/initiatives/search-party
    - Contestant & Judge guides plus YouTube training playlist
- https://inteltechniques.com/
- https://start.me/p/b5gQBm/osint-sauve
- https://osintframework.com/
- https://www.sans.org/blog/-must-have-free-resources-for-open-source-intelligence-osint-/
- https://github.com/tracelabs/searchparty-ctf-writeups
- https://webbreacher.com/2018/07/12/osint-map/

SLIDES

# Contact

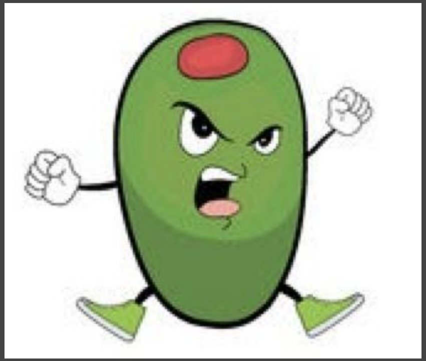
Darren aka hardBox

- Twitter: @hard_Box



Jenn aka Angry0live

- Twitter: @heyitsjlemmen



# Questions?

pmitf.com