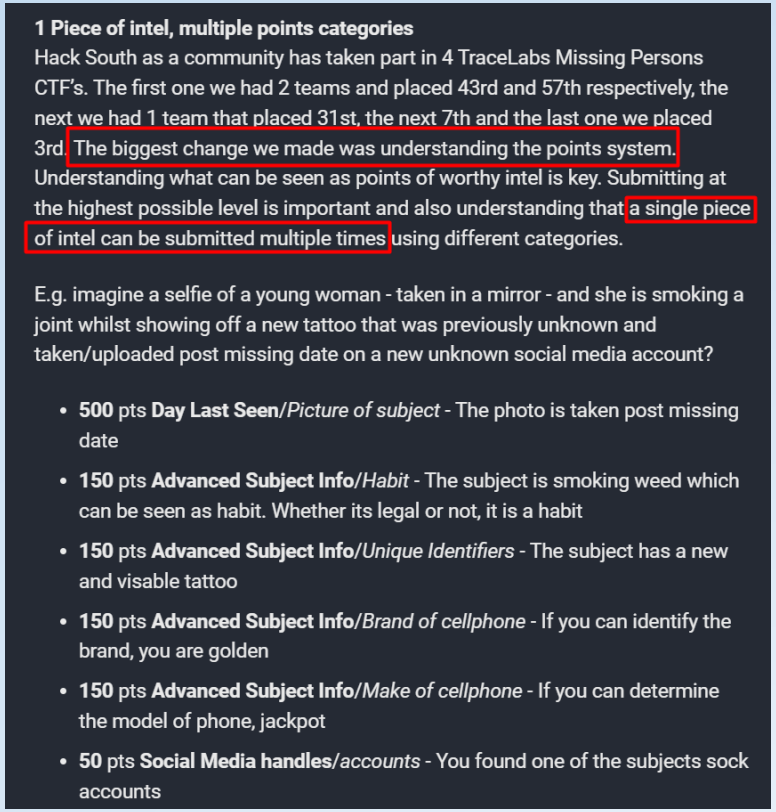
TraceLabs CTF Crash Course

Read - https://download.tracelabs.org/Trace-Labs-OSINT-Search-Party-CTF-Contestant-Guide_v1.1.pdf

VORTIMO

FORMAT

- Teams of 4 people
- 6 live cases
  - Every team gets the same cases
- 4 hours
- Submit the nuggets of info you get:
  - On TraceLab portal – one per team
  - A judge is assigned for your team
- Different things get different points
  - Eg 10 points for friend details, 200 points for email address etc etc
  - Read up on this!!!!
    - https://download.tracelabs.org/Trace-Labs-OSINT-Search-Party-CTF-Contestant-Guide_v1.1.pdf



1 Piece of intel, multiple points categories
Hack South as a community has taken part in 4 TraceLabs Missing Persons CTF's. The first one we had 2 teams and placed 43rd and 57th respectively, the next we had 1 team that placed 31st, the next 7th and the last one we placed 3rd. The biggest change we made was understanding the points system. Understanding what can be seen as points of worthy intel is key. Submitting at the highest possible level is important and also understanding that a single piece of intel can be submitted multiple times using different categories.

E.g. imagine a selfie of a young woman - taken in a mirror - and she is smoking a joint whilst showing off a new tattoo that was previously unknown and taken/uploaded post missing date on a new unknown social media account?

- **500** pts **Day Last Seen**/*Picture of subject* - The photo is taken post missing date
- **150** pts **Advanced Subject Info**/*Habit* - The subject is smoking weed which can be seen as habit. Whether its legal or not, it is a habit
- **150** pts **Advanced Subject Info**/*Unique Identifiers* - The subject has a new and visable tattoo
- **150** pts **Advanced Subject Info**/*Brand of cellphone* - If you can identify the brand, you are golden
- **150** pts **Advanced Subject Info**/*Make of cellphone* - If you can determine the model of phone, jackpot
- **50** pts **Social Media handles**/*accounts* - You found one of the subjects sock accounts

Rules - more

- All data collection is PASSIVE
  - No interaction with anyone except team members and judge
  - No friend requests
  - No password resets, no hacking
  - This might interfere with the case
- No data that is already known
  - From missing person report ;)
  - From law enforcement sites
  - From news articles

VORTIMO

Submitting data

- You are sending public info to the judge
  - Via the TL website / portal that will go live when competition starts
- It needs to verifiable!
  - URL + screenshot is the best
  - URL needs to be public / not behind paywall

You can request a new judge if the one you get doesn’t work out.

To do beforehand

- Create sock puppet accounts if you feel you need to
  - Facebook
  - Twitter
  - IG
  - Snapchat
  - eBay
  - LinkedIn
- Perhaps get some SIM cards to verify?

VORTIMO

To do beforehand 2

- Get Virtual Box / VMWare working and get the TraceLab VM working

- Install Vortimo and watch the tutorial (https://www.youtube.com/watch?v=Kvf59z7MI_w)
- Play along and make sure you know how to tag text, images and pages and how to export DBs.

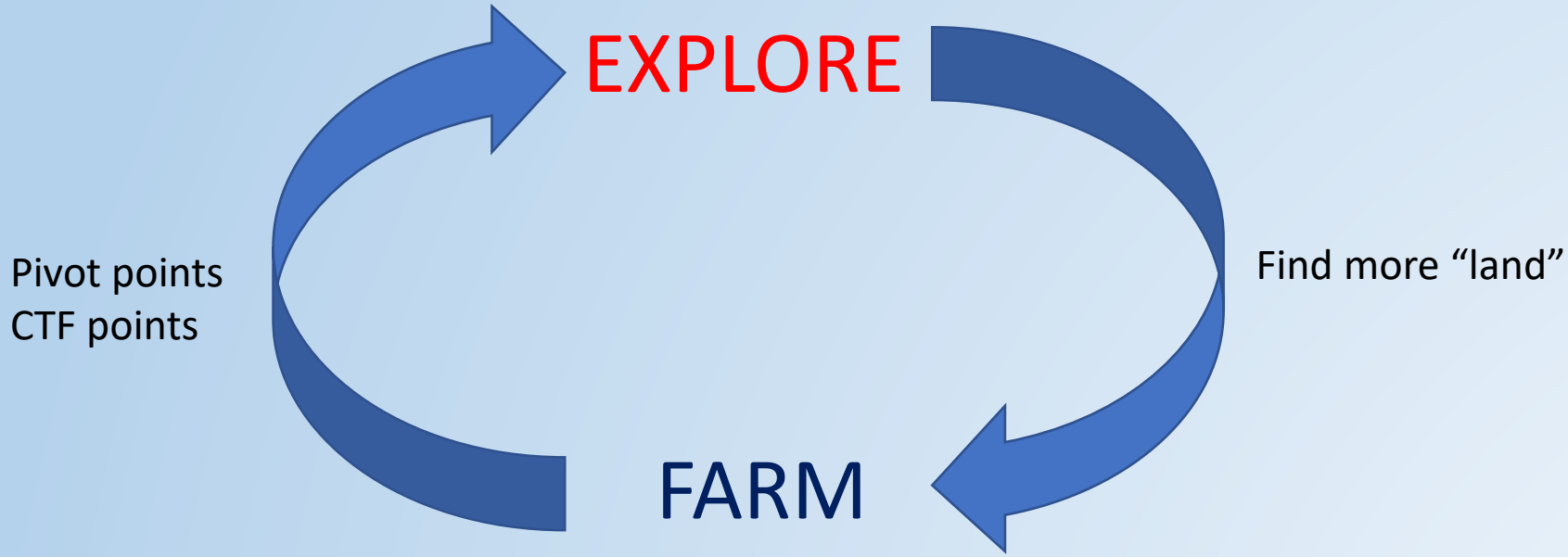
- Familiarize with OSINT-tool.com
- Get keys for services (RT will send prior to competition)

Methodology

- Explore and Farm
  - Cyclical process
- Explore – finding new land (to farm) by looking at pivot points.
  - Land => sites, social network profiles, blogs, forum profiles, domains
  - This is done by expanding pivot points (e.g. looking up a possible alias on all social networks)
- Farm – collecting all information that's on the land.
  - Combing (scrolling ,reading!) through social networks, reading many blog posts
  - Looking for pivot points to explore – which are also CTF points.

VORTIMO

OSINT lifecycle lol



Farming for Pivot/CTF points

- Things that you can identify that will lead to more “farmland”:
  - Email address
  - Alias
  - Phone number
  - Social network affiliation / profile
  - Photos
  - Names (of family or associates)

- These are also the things that the CTF gives points to
- Farmers needs to **take time to read**, scroll through, look for pivot points.
  - Vortimo can help by extracting phone/email etc. but eyeballing is best

VORTIMO

Pivot points - Name

- **Farm**: Will be given to you…☺
  - For relatives, use surname only + context (like country, city etc.)
    - For married females you might need to find maiden name
  - Spelling for some names can be different in different languages!
- **Explore**:
  - If name + surname unique, look up on Vortimo CSE (custom search engine) or other CSE
  - For wider results – just Google it..
    - With quotes
    - With “First letter of name [space] Surname” and other combos
  - Use other search engines too – country specific
    - Baidu, Yandex
  - Look the name up in leaks/dumps and DarkNet
    - Dehashed / Pipl / IntelX / HaveIBeenPwned
    - DarkWeb Search (OnionLand and on-TOR search engines)

VORTIMO

Pivot points – Email address

- **Farm -** in results of searches if email address is mentioned (duh)
  - Vortimo auto farms, but also eyeball for roelof [at] blah [dot] com
- Try likely personal email formats:
  - Name+surname@gmail.com / yahoo.com / outlook.com / mail.ru
  - (alias you've found)@gmail.com
- Manually try figure out a possible company email:
  - Get domain for email
  - Use Hunter to get email format (e.g. surname.name@company.com)

- **Explore** your attempts with
  - Dehashed / Epios / IntelX / Emailrep, Google / CSEs

Pivot points - Aliases

- **Farm**
  - Alias from social networks / forums / etc.
  - Can be in URL – like on Facebook
  - Try name+surname as alias too!
    - If desperate append 01/02 …
- **Explore** the alias on WhatIsMyName / Dehashed / UserSearch
  - Enumerate networks / places where it can be found.
- Search for the alias on CSE / Google (and other SEs)
- Look for the alias on social networks
  - (this is basically what above does)

VORTIMO

Pivot points – phone numbers

- **Farm** from dumps, posts, CSE.

- **Explore**
  - Look in leaks and dumps (Dehashed, IntelX, Pipl, Facebook dump etc)
    - Remember that number could be captured in different formats – try others too
  - For US based – there are many high quality paid for services
    - Other country specific services – look for specific service.
  - TrueCaller / SyncMe
  - EveryoneAPI / Nuestar (if you lucky to have it)
  - HLR – shows if number is roaming
  - Search on CSE/Google, other SEs
    - Remember to try different formats (+YY ABC DEFG, ABC DEFG, ABCDEFG with quotes, without etc)

VORTIMO

Pivot points - photos

- **Farm**
  - In profiles / pages, specifically profile pictures but also vanity icons
  - Input name (or alias etc) -> Do an image search on Google / Yandex / Bing
    - Look for context (age, gender etc)

- **Explore**
  - Reverse image search!
    - Yandex / Google / Bing / TinEye
      - OSINT-tool, right click on image
    - No results? - Also crop image to specific features and redo it
  - Geolocation
    - An art on its own!
  - Changes are slim but look for interesting Exif info
    - Dates / Camera model / serial number / phone make / exotic software used
    - Vortimo auto extracts Exif from all images

VORTIMO

Search engine (SE) specific things

- Most SE use same operators. Some that's useful to know:
  - Quotes
    - (duh)
  - +word
    - Has to contain this word
  - Site: TLD – e.g. site:za
    - Only results from sites in this TLD
- Most punctuation is omitted in searches
  - Searching for "roelof vortimo com" is the same as search for "roelof@vortimo.com"
- Swapping terms around in quotes gives different results!
  - "roelof temmingh" =/= "temmingh roelof"
  - For name searching this is NB as some places might have name, surname in Excel spreadsheet and it's indexed the other way around (as example)

VORTIMO

Going back in time – don’t forget!

- For certain sites, its VERY useful to go back in time.
  - Should be obvious why
    - (deleted data, site changed, old contact details)
  - This is mostly only useful for “static” sites – like blogs, own sites, company sites. There are more than these than you might think!
  - Does not work well for social networks
    - Eg Facebook/Twitter/IG pages aren’t indexed by archive.

- Use WayBack machine at archive.org

VORTIMO

Social networks

All the usual stuff. But remember these:

- Always reverse image search profile picture!
- Look for friends / followers with same surname (family)
  - If female, find the maiden name, look for family members
- Focus on photos with
  - Other people
  - Geo-locatable features (houses, city features, restaurants, road signs etc.)
  - Cars (plates!), boats, planes – any transport device
  - Anything with text (documents, banners, graffiti)
  - Body piercings, tattoos, birthmarks, anything that's likely permanent.
- Facebook/Vkontakte/Twitter/IG etc
  - Scroll to first posts. This is where best info is.
- Twitter
  - Look at first friends/followers. This is the first people friended and almost always a good indication of who they personally know.

- ^ where possible of course.

Dumps / Leaks

- Some of the best leads are here
  - Pivot immediate (name <-> email <-> alias <-> profile)
- See where the dump came from
  - Register on this service if it makes sense
  - Try to search/find the person on this service
  - Farm the info on the profile ☺
- If password is clear-text, try to think of the context
  - Is it a DOB? Anniversary date? Person's name they know?

Other things

- Getting stuck – farming vs exploring
  - Farming – scrolling one profile/social network forever. Especially when it's overwhelming amount of data).
    - There's more out there and you're wasting time.
  - Exploring – not taking the time to read (& farm) what you've already discovered.
    - You've missed important things, you're pushing buttons and clicking links and not reading.
- Tools vs manual
  - Use tools where it's useful to use tools.
    - Looking up data in dumps / leaks
    - Enumerating networks / profiles – e.g. repeating the same thing over/over
    - Things people just can't do – e.g. reverse image search, Exif extraction
    - Kitchen sink / Run All lookups, links – e.g. shotgun when you're stuck.
  - Use eyeballs for context
    - Things computers can't do – understanding what you're reading/exploring, giving context to it.
    - Finding pivot points, understanding what info has value
- Getting stuck on exploring (and there's nothing to farm)
  - Know when it's time to move on to the next case
    - If you're on page 20 of Google results there's likely no more info there…
    - If input values are too common and you're getting only false positives.
    - If you've farmed everywhere and there's no more pivot points.