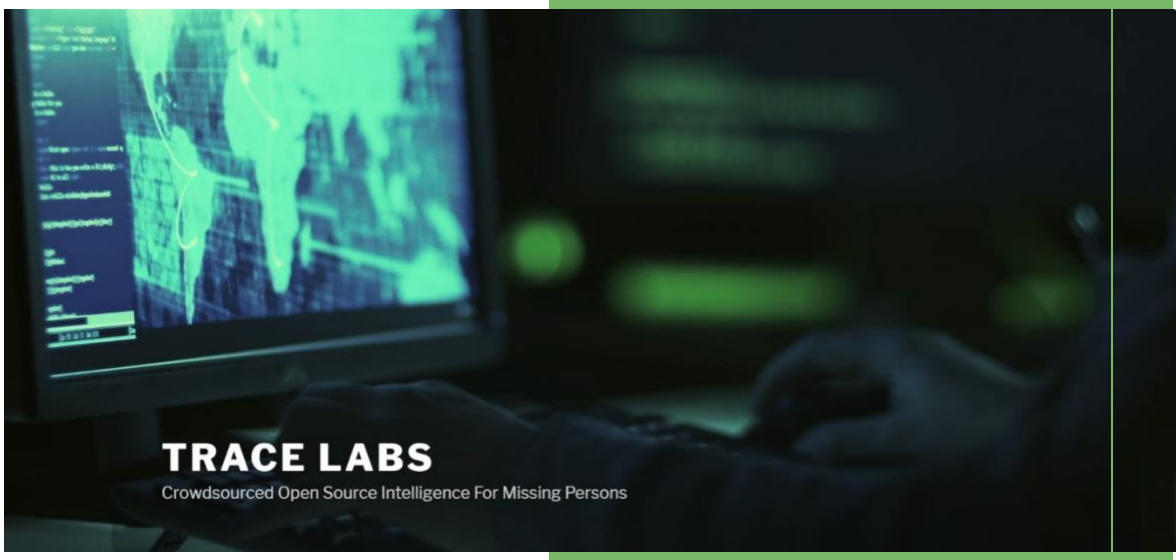
Trace Labs OSINT Search Party CTF Judge Guide v4



JULY 2021

Table of Contents

Revision History

Date	Change Author	Notes
23 Oct 2019	Katniss-Melb & Belouve	Version 1 - Initial Document
06 April 2020	Belouve, Adrian (AK47Intel), and James (Blackbeard)	Version 2 - Revisions for Global CTF IV
18 June 2020	Adrian Korn (AK47Intel)	Version 3 – Updated links and terminology
28 July 2021	Alex Minster (Belouve)	Version 4 – Updated links and guidance

Welcome and Thank You

Thank you all so much for volunteering to help in such a positive way, to demonstrate the effectiveness of #OSINTforGood, help sharpen the tradecraft of many other hackers, and above all else… to help many families through what may be a terrible reality by assisting law enforcement in the reunification process. Though this may be gamified, the ultimate goal is not for teams to put points on a board, but to help law enforcement gain traction in their missing persons investigations though solid and well-reported pieces of open source intelligence. You, as a judge, are a valued part of that process. Again, thank you!

Before the CTF

1. Set-up your Trace Lab Slack and OSINT Search Party **CTF platform** accounts. OSINT Search Party can be accessed at https://searchparty.tracelabs.org. Within a few days of the OSINT Search Party CTF, one of the Trace Labs organizers will set up a judge account for you.

2. Trace Labs has a 3 part training series that provides:

    a. An introduction to Trace Labs
    b. How to get started as a contestant on the OSINT Search Party CTF Platform
    c. How to be a volunteer judge in an OSINT Search Party CTF

    You can view this training series here to get some background on our organization and our CTF before reading onwards.

3. We also have a humorous 5 minute video put together for what to expect as a Trace Labs CTF Judge. This can be found on YouTube here: https://www.youtube.com/watch?v=I-cX-DJgxoE

4. Attend the Judge Briefing, which is held by our Judge Admins Belouve and HumanDecoded. This is usually a few days before the CTF and attendance allows for a great Q&A opportunity. If unable to attend, a recording will be made available that is recommended to watch before the CTF.

5. Set-up burner accounts (otherwise known as ‘sock puppet’ accounts) in different social media platforms like Facebook, LinkedIn, Twitter, Instagram, Snapchat, etc. Consider using a photo from https://thispersondoesnotexist.com/ These accounts can be used for subsequent CTFs and do not need to be burned after each CTF, though this is up to each judge’s discretion. This can take about 30 to 45 minutes, depending on the depth you apply to your sock puppet accounts.

a. An introduction to setting up Sock Puppet accounts, from TraceLabs, is located here: https://www.youtube.com/watch?v=3KPO58wkw7M
b. TraceLabs held a webinar on Sock Puppets that is available here: https://www.youtube.com/watch?v=EEeJcZhxAf4 "An Evening With The Puppet Masters: A discussion on alternate social media accounts"
c. Jake Creps, a member of that panel, has a great guide to learn more about the process involved: https://jakecreps.com/sock-puppets/

6. Set up a VPN to use. We have several recommendations in the TraceLabs Slack. Realistically, it is up to you for which works best. Please take care to protect your own privacy and security. There may also be times where a VPN blocks access to a piece of intel that you need to validate. Please plan for this, and coordinate with another judge if you are having trouble accessing a submission from your team.

   You might also set up a VM (Virtual Machine) to operate in. This will further isolate your system and can be deleted or reverted at the conclusion of the CTF. Some use the TraceLabs OSINT VM or other VM systems, and this is up to you and your comfort with your system. Recommendations are available if you ask in the TraceLabs Slack.

   A brief tour of the TraceLabs VM is available here:
   https://www.youtube.com/watch?v=FlGdSZk1F6o

   The Introduction and installation of the TraceLabs VM is available here:
   https://www.youtube.com/watch?v=jjK0nvmOeUA

   TraceLabs additionally held a Live Demo with Q&A on the TraceLabs VM:
   https://www.youtube.com/watch?v=yZdOb-NSiAw

7. Prep some form of tracking for what your teams have submitted. You may be assigned multiple teams, and it gets hectic. Being able to have a document, tool, whatever works for you, to keep track of what a team has established, will help quite a bit. Some notes like "they established who the significant other is (light detail)" or "they found this social media account for the subject". It will help for you to be able to string together their process of established information. An example will be provided in the "*Team Tracking and Notes*" section, and will feature CherryTree. Feel free to use whatever tracking mechanism you want to use to cut through the confusion, so that you know where your teams are at, what they have established, etc. We trust you to be able to figure out what works best for your tracking.

   Please note: It is not recommended for thorough notes to be retained on the cases worked on. Please ensure that the notes are cleared away at the conclusion of the contest. This will be reiterated in the "*After the CTF*" section.

8. Become familiar with the different categories and points. I put details for the different categories and points at the end of this document for easy reference.

https://searchparty.tracelabs.org/categories

9. Review the canned responses in a later section. This should help in multiple ways, as you may use these to wordsmith a professional response to your teams, help build the tradecraft and reporting skills of your teams, and also inform you of what types of intel would be rejected.

   Please note: Trace Labs will sometimes encounter high-profile or high-publicity cases. Speculation and speculation forums are not accepted. News sites are also not accepted. Sites that are an aggregate or collection of news media articles or known information are not accepted. Encourage your teams to do good intel and good solid reporting.

10. Plan for how you will transition from the CTF to the rest of your day/night. As seen in videos above, judging can be tense. More details will be in the "*After the CTF*" section, but please prepare as needed to stay well.

During the CTF

1. Log into the CTF platform. You will see the names of the missing persons under cases. Click on the small I icon to view the details that Trace Labs has for the missing person.

2. Log in to the Trace Labs Slack group. This is how we will communicate with you and how you can ask questions. Please also note who the senior judges are that you can consult. We will try to announce senior judges that can be consulted for each event, but feel free to inquire in the channel for anything that you need additional guidance on. Beyond senior judges are the Judge Admins, which are currently Belouve and HumanDecoded, who can be consulted as needed.

3. On the right side, you will see the incoming submissions for the team(s) assigned to you. Click on the submission to expand it.

4. You'll need to validate their submissions by visiting the submitted URL. You may need to log into the social media platform using your burner account. If the URL is behind a paywall, this submission can be rejected. This is an open source CTF activity.

5. Once you have validated the submission, you click on the accept button and the team will get the points. You can also provide a comment to help motivate the team. If the category selected by the team was incorrect (maybe the team member didn't pay attention to the categories), you can change the category from the drop-down menu so that they get the correct points.

6. For exceptional submissions that may provide a lot of value for the law enforcement agency, you can use the "star" option. This will automatically accept the submission.

Important Note: For *any* Location submission (Highest value flag for 5000 points), in order for it to be approved, it must be brought up with multiple judges. Final approval can only be done by a member of the Core Team. Announce it in the judge channel and have other senior judges consult on it. If needed to get final approval of the submission, routing through the Judge Admins of @Belouve and @HumanDecoded will be the proper approach. We'll discuss with the core team and decide if we award points for such submissions. Additionally, any other high-value submission (1000 points or more) is recommended to have additional review, but not required.

7. Watch out for some teams who may keep on gaming the system by providing duplicate submissions. Check if they submitted the first entry under a lower point category and they realized that they should have submitted it under a higher point category. In this case, you can go back to the previous submission by clicking "History" in the CTF platform. Then choose the team name and change the first entry submission status to reject. Then accept the second entry and put in a comment that the previously accepted one has been rejected and that you're giving them the higher points instead.

   You may also consult the "*Team Tracking and Notes*" section for tricks on limiting this issue.

8. When you reject the submission, you can choose any of the "instant" rejection reasons. **Note:** When you use the canned "rejection" reasons, any text you put in the comment field will disappear.

9. To better help the team members improve their tradecraft, provide a short comment/explanation. But make sure that you don't use the "instant" rejection reasons because your text will disappear. Just use the normal reject button. I've provided some canned responses in a later section that have been used over several competitions.

After the CTF

Clean Up Your Data

Take steps to protect your identity and the security of your system. Some recommended steps are:

1. Revert or delete your VM environment
2. Clear out any notes taken in your private tools (CherryTree, Notepad, etc).
3. Log out of any of your sock puppet / burner accounts. If you intend for them to be burnt at the end of this contest, make plans to have them removed.
4. An antivirus / antimalware scan may be prudent on your machine as well.

These are recommendations, and you will know best how to clean up your machine and data. If you need guidance, reach out to others on the Slack channel.

Please note: It is not recommended for thorough notes to be retained on the cases worked on. Please ensure that the notes are cleared away at the conclusion of the contest.

Judge Feedback Form

You may be sent a feedback form to fill out, which should take less than 10 minutes. This helps Trace Labs be able to adjust and evolve for future events. This can be done immediately at the end, or within a day or two.

Judge Mental Health

The cases and intel, and the high rate of speed of the intel, can add a high degree of mental stress for a judge. In addition to this, the material may be disturbing, with examples being human trafficking, prostitution, pornography, suicide, and death of subject. There may be a number of heartbreaking tales that you just worked through in a short amount of time. This does not serve to be an all-encompassing mental health guide, but encouragement to keep aware.

Feel free to step away during if you need a moment to process something rough. I myself (Belouve) have done so in past cases, and you can hand off your work if needed.
A recommendation I have, from the "*Before the CTF*" section that is mirrored here, is to have some planned transition from the end of the CTF. Whether you plan to commit to watching a lighthearted movie at the end, hang out with your family, go for treats, or hang with friends. A planned positive activity after going through the CTF has always worked wonders personally. I say this at a time where there is a lot of global collective trauma with regards to the pandemic. For resources, we are working on additional avenues, including those on a more global level, but we wanted to leave the following resources here. If you need to reach out to a fellow judge or admin, please do so. Additional resources are listed at this site, from the National Alliance on Mental Health : https://nami.org/Find-Support

Additional Reference Sections and Guides

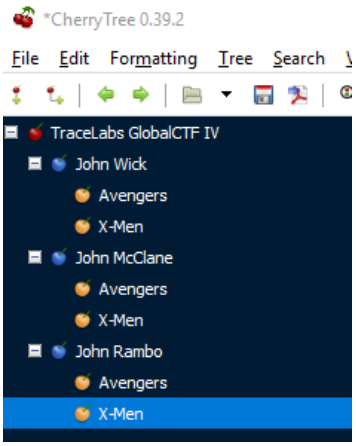
Team Tracking and Notes

I use CherryTree for this, and will insert a screenshot below. (https://www.giuspen.com/cherrytree/#downl) It also comes pre-loaded into Kali Linux, and is fairly cross-platform.

I set up a hierarchy of:

Name of Trace Labs Event (Like Trace Labs Global 2021.08)

|--- Missing Subject Name (Like John Wick)
    |--- One of your assigned teams (like Avengers)
    |--- Another of your assigned teams (like X-Men)
|--- Another Missing Subject Name (like John McClane)
    |--- One of your assigned teams (like Avengers)
    |--- Another of your assigned teams (like X-Men)



← An example of the above setup

Validation Tips and Tricks

- Recognize that the submitted intel for many categories needs to focus on the missing person. With some high-profile cases, there may be a lot of intel submitted on individuals that are not the missing person, but a person of interest. This would not count in many of the categories such as Basic Subject Info or Advanced Subject Info, unless it can have a strong to the subject.

- Quickly discern the rejected sources. News sites, media sites (like a TV show about the missing person), speculation and speculation forums (like websleuths or Reddit), or aggregates of known data (such as Wikipedia or a fan site for the case) would also be rejected.

- All rejected items do have an exception, but it is extremely rare for it to do so. An example: News sites are not excepted, but there was a case where a news article referenced a funeral, and in that reference, was a very thorough family tree that included the subject. This was acceptable at the Family category for points. Again, very rare for exceptions, and there must be some very solid reporting and rationale for the intel.

Disputes

There will likely be disputes encountered on your rulings. Here are a few quick tips for them:

- First, make sure they saw or received the rejection notes. Sometimes they do get removed (glitch or an error on the judges' part), and to them, it seems like it was rejected with no reason given.
- Please always work to sharpen their tradecraft. A lot of times a dispute may arise because the intel is clear to them, but not clear to the judge or to any law enforcement that will then review it.
- Feel free to consult the canned judge notes for some guidance on common rejection reasons.
- Feel free to ask in the Judge Slack channel. Someone may be able to give you a response.
- Clarify to your team that you have consulted with other judges, and what the current ruling is.
- Also: accept that you, as a judge, might make mistakes. This will clear up a lot of tension in disputes, if you are willing to admit to your team that you made misjudged.
- Additionally, do not be afraid to consult one of the senior judges. They will be announced for each event. A couple of specific senior judges that are often around are Belouve and Katniss-Melb, both of whom helped author this document. The senior judges often spend a lot of their time helping out with disputes on rulings. We are here to help everyone.

Canned Judge Notes

Please read through the below canned responses in order to help shape your determinations of what good submissions we are looking for. These responses (and any notes about them) can help you to strengthen the value of your teams' submissions.

1. News media sites are not accepted for submissions, as information is likely already known to police. If established that the news site information is not known to police, then it can be evaluated and scored.

2. This is sort of a missing persons website/aggregate. Any leads such as these would have been shared with law enforcement, and may not be a new lead.
3. This podcast/YouTube video is sort of an aggregate of known missing persons information. Any leads such as these would have been shared with law enforcement, and may not be a new lead.

4. This video submission is not narrowed down enough to provide the reviewer with specific information. Please resubmit with notes calling out the specific timestamp and information enclosed. *(This is for submissions that may be a 20-minute video that does include valuable information, but not specified where. Judges may not have the time to watch a lengthy video in order to come across the piece if intel desired.)*

5. Speculation forums would not reach the level of validation needed. If more direct intel is provided, a resubmission will be retrieved.

6. Submission is information already included in police reports. *(This unfortunately happens more often than thought. The picture they submit as intel will be the same picture in the police report. Same for some other details, where your team may have just grabbed a name and started digging. The police report is on the tab within Search Party, and should be reviewed by judges and contestants. If an issue, please guide your teams to review the police report to not restate known information.)*

7. I am not seeing a clear connection established between this submission and the missing person.

8. Submission is behind a paywall or a paywall(ed) site.

We are not accepting the rationale of all followers are friends. The end goal is not getting points on a board, but providing actionable intel to law enforcement. Giving them pages of all followers will harm the Trace Labs relation with law enforcement and may delay the reunification process for the missing individual. We have had individuals script and strip every Facebook friend, and that has been rejected. If there is a case that the follower is an acquaintance of the subject, then that should be detailed in the submission, with a link that would make sense to law enforcement.

Categories

NOTE: Any information that can be used to help locate the subject has value. While many items are listed below, there will be many items that are not and will be valued as the CTF progresses. More is better and you will likely get points for items not listed here if it is deemed to help the investigation.
These are drawn from the site accessible at: http://searchparty.tracelabs.org/categories This may be accessible outside of a current CTF as well. In case of conflict between this guide and what is on CTF platform, the CTF platform takes priority.

FRIENDS / 10 points

Relevant information on FRIENDS. This can include but not limited to:

- Name
- Aliases
- Birthdate
- IDs (driver's license, passport, library card etc.)
- Friend's work address
- Friend's work phone
- Email
- Friend's home address
- Home phone number
- Social media handle (e.g. Facebook, twitter, etc.)
- Any insightful information from friends' comments

EMPLOYMENT / 15 points

Relevant information on EMPLOYMENT. This can include but not limited to:

- Business name
- Aliases
- Manager name
- Start date
- End date
- IDs (badge, license, etc.)
- Business address
- Business phone
- Email
- Social media
- Previous employers
- Any insightful information from employer's comments

FAMILY / 20 points

Relevant information on FAMILY. This can include but not limited to:

- Name(s)
- Alias(es)
- Birth date
- IDs (e.g. driver's license, passport, library card)
- Work address
- Work phone number
- Email(s)
- Social media handle(s) (Facebook, Twitter, etc)
- Family's home address
- Home phone number
- Last time they saw the subject
- Information from family's comments

HOME / 25 points

Information that is relevant regarding the SUBJECT'S HOME. This can include but is not limited to:

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

BASIC SUBJECT INFO / 50 points

BASIC relevant information regarding the SUBJECT. This can include but is not limited to:

- Name
- Aliases
- Birth date
- Pictures
- IDs (e.g. driver's license, passport, library card)
- Blogs or forum profile and relevant posts
- Dating site profiles/posts
- Craigslist, Kijiji, Reddit or sites of similar nature profiles/posts
- Social Media Handles/Accounts
- Personal websites
- Online resume
- Physical description
- Emails

ADVANCED SUBJECT INFO / 150 points

ADVANCED relevant information regarding the SUBJECT. This can include but is not limited to:

- Unique identifiers (e.g. tattoos, scars, piercings)
- Medical issues
- Habits (e.g. smoking, drinking, hitch hiking, hangouts)
- IP Address
- Any other information about where the subject might be headed
- Brand/model/carrier of cell phones
- Make/year/color/license plate of vehicles
- Video game handles (e.g. XBOX, Steam)
- Breached Passwords: Must show hashed or cleartext password
- Any other information about where the subject might be headed
- Previous missing persons history
- Police update saying the person was found or an obituary

DAY LAST SEEN / 500 points

Net new intelligence surrounding subject's day last seen OR Intelligence that proves activity/engagement after day last seen

- Details about subject's physical appearance on day last seen (clothing, hair, etc)
- Details of subject's state of mind on day last seen (mood, altercations, conversations, etc)
- Activity from a social media account exclusively controlled by the subject, after they went missing
- Location information since subject went missing, up to the current date
- Account creation after day last seen
- Person last seen with
- Intent to meet with someone
- Direction of travel
- Other details that relate to the day last seen
- Non-speculative sightings of subject after they went missing, with valid routes to follow up with reporting
- Pictures posted of subject from after day last seen
- Pictures of subject on or after day last seen (e.g. CCTV)

DARK WEB / 1000 points

Relevant information found on the DARK WEB about the subject
Your submission must originate from a .onion URL to be considered Dark Web - Eg. https://dsfjldsjflj.onion and must only exist on the Tor network – Eg. http://facebookcorewwwi.onion would not count as Dark Web

- **Must be sourced from a ".onion" URL**
- **pictures or details of subject on human trafficking related 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**

LOCATION / 5000 points

- Relevant information pertaining to the current location of the subject. Current location being defined as: Exact location/address the subject has been in past 24 hours, or will imminently be present at. Broad geographical descriptions will not count for this category.
- As this is the highest point flag, it will require the highest level of accuracy and thoroughness in reporting and context. Speculation has no place in this intel.
- This does not include a police update saying the person was found or an obituary - this will get you 150 points and can be under the category Advanced Subject Info.