Trace Labs OSINT Search Party

CTF CONTESTANT GUIDE

Date and Version Number	Contributors
June 18, 2020 Version 1.0	Adrian Korn (AK47Intel) Robert Sell (Creep) James Liolios (BlackBeard) Joe Gray (C_3PJoe) Rae Baker (wondersmith_rae) Gyle dela Cruz (Katniss-Melb) Alex Minster (Belouve) Alethe Dennis (Sud0F0x)
November 3, 2021 Version 1.1	Gyle dela Cruz (Katniss-Melb)

WHO WE ARE

Trace Labs is a Not-For-Profit organization with a mission to crowdsource the collection of Open Source Intelligence (OSINT) to generate new leads on missing persons cases. The missing persons issue is worsening which requires modern and scalable solutions at various levels to help mitigate risk to society.

We leverage our own custom CTF platform that enables the collection of OSINT to power crowdsourced Capture the Flag (CTF) events known as the “OSINT Search Party CTF”. OSINT refers to the collection, processing, and analysis of publicly available data such as social media, forums, government records, and even the dark web.

Trace Labs has taken the traditional CTF competition that we see in the information security community where participants hack into intentionally vulnerable servers to obtain “Flags” for points and evolved it into a real-life exercise where the participants’ contributions have real-world impact and the potential to enhance public safety.

Since its inception in 2018, Trace Labs has:

- Organized 30 CTFs globally
- Worked on 250+ missing persons cases
- Collected 30,000+ OSINT submissions from our crowdsourced community
- Brought together 2500+ contestants in our CTFs
- Brought together 500+ volunteer CTF Judges
- Worked with 10+ Law Enforcement Agencies

RESOURCES TO GET STARTED IN OSINT

// Trace Labs Discord

https://tracelabs.org/discord

// Trace Labs OSINT Search Party CTF Training Videos

Trace Labs has a 3 part training series that provides:

1. An introduction to Trace Labs
2. How to get started as a contestant on the OSINT Search Party CTF Platform
3. 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.

// Trace Labs OSINT Virtual Machine (VM)

The Trace Labs team has set out to create a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM by Michael Bazzell, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTFs a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

To get started, download the OVA file via our website below and run it in your choice of VM software (VMware Workstation, Virtualbox etc.).
https://www.tracelabs.org/initiatives/osint-vm

To log in use these default credentials: **Username:** osint **Password:** osint

The documentation for this VM is in: https://github.com/tracelabs/tlosint-live/wiki

We are continuing to build upon the Trace Labs OSINT VM and welcome any and all feedback. Our goal with this project is to create an OSINT focused VM that provides security, stealth, and the ability to easily save digital forensic evidence during an investigation all within an easy to use package.

// Trace Labs Past Blogs and Writeups

There is a list of writeups and blog posts about our past events at our GitHub link: https://github.com/tracelabs/searchparty-ctf-writeups

If you have writeups or blog posts, please let us know and we can get them added to that list.

// OSINT Training

Trace Labs endorses the following OSINT training providers and courses:

The OSINTion Introduction to People OSINT / Missing People OSINT

Regular 6-hour interactive virtual training courses on how to leverage OSINT in missing persons investigations run by Joe Gray:

This course is designed to hone specifically on the processes and tools used to perform "People OSINT" in situations where investigators are seeking to find missing people. This focuses on validating the information discovered and using it to pivot to valuable information, in both a OSINT Search Party CTF and a law enforcement setting.

https://www.theosintion.com/courses/introduction-to-people-osint-missing-people-osint/

Use promo code TraceLabs15 to receive 15% off!

OSINT Combine Academy On Demand Training

OSINT Combine has created a custom "Trace Labs OSINT Foundations Course" that is provided free of charge to the first 300 registrants of any Trace Labs Global OSINT Search Party event.

Additionally OSINT Combine offers **15% off any other OSINT Combine Academy course with the promo code TLSUPPORT** where they will donate 10% of proceeds on registrations from the code directly back to Trace Labs to support our mission of crowdsourcing OSINT to assist law enforcement in finding missing persons.

Check out the full on demand OSINT Course offerings from OSINT Combine at https://academy.osintcombine.com/courses

SANS SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis

This is 6-day foundational course in OSINT gathering led by Micah Hoffman moves quickly through many areas of the field. While the course is an entry point for people wanting to learn about OSINT, the concepts and tools taught are far from basic. The goal is to provide the OSINT groundwork knowledge for students to be successful in their fields, whether they are cyber defenders, threat intelligence analysts, private investigators, insurance claims investigators, intelligence analysts, law enforcement personnel, or just someone curious about OSINT.

https://webbreacher.com/sec487/

HOW DOES THE OSINT Search Party CTF WORK?

// Overview

This CTF is non-theoretical where contestants work in teams of up to 4 members to crowdsource the collection of OSINT to assist law enforcement in generating new leads on missing persons. In the information security community, a typical CTF will be of a technical nature where “flags” are hidden within pre-configured servers/virtual machines that contestants have to obtain using hacking techniques to gain points. Our CTF differs from this by having different flag categories based on pieces of information that law enforcement gathers in a case.

The contest runs as a Capture the Flag (CTF) format where contestants must collect various “flags” which equate to points. Since each flag submitted is treated as potential “net new intelligence”, Trace Labs has a team of volunteers known as “Judges” who validate each submission and award points if the flag meets the category requirements. At the end of each CTF, the team with the most points on the scoreboard wins.

// Scoring System

FRIENDS-10pts		
• Name • Aliases • Birthdate • IDs (driver’s license, passport, etc.)	• Work address • Work phone • Number • Email	• Home address • Home phone number • Social media handle (e.g. Facebook, twitter, etc.)

EMPLOYMENT-15pts		
• Business name • Aliases	• IDs (badge, license, etc.) • Business address	• Social media • Previous employers

- Manager name
- Start date
- End date
- Business phone
- Email
- Information from employer's comments

FAMILY-20pts

- Name
- Aliases
- Birth date
- IDs (e.g. driver's license, passport, library card)
- Work address
- Work phone number
- Email
- Social media handle
- Home Address
- Home phone number
- Information from family's comments

HOME-25pts

- Address
- Information from employer's comments Landlord's name
- Habits
- Any meaningful interactions with the landlord
- Risks in the immediate area
- Landlord's phone number
- Recent accommodations

BASIC SUBJECT INFO-50pts

- Name
- Aliases
- Birth date
- Pictures
- IDs (e.g. driver's license, passport)
- 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
- Emails

ADVANCED SUBJECT INFO-150pts

- Unique identifiers (e.g. tattoos, scars, piercings)
- Medical issues
- Habits (e.g. smoking, drinking, hitch hiking, hangouts)
- Brand/model/carrier of cell phones
- Make/year/color/license plate of vehicles
- Video game handles
- Any other information about where the subject might be headed
- Previous missing persons history

- IP Address

DAY LAST SEEN-500pts

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

DARK WEB-1000pts

- Must be sourced from a ".onion" URL
- Picture or details of subject on 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-5000pts

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

// Scope

As investigators, we do not get involved nor theorize or speculate, we only collect OSINT. We do not go after bad guys. We are not the police. Instead, we simply collect previous and public intelligence and provide this to the respective law enforcement so that they may pursue the appropriate course of action.

Part of this scope includes things a competitor should **NOT** do. These include (but are not limited to) attempting to log-in or reset passwords, attempting to send friend requests to the subject or their family/friends, and calling/texting/video messaging/FaceTiming the subject or their family/friends. We are aware that some

OSINT training courses advocate attempting password resets, but have made the decision to completely outlaw it in our competitions.

All of the actions in the preceding paragraph can lead to disruption of the **chain of custody.** A **chain of custody** is in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. Of particular importance in criminal cases, the concept is also applied in civil litigation (Wikipedia).

If the subject is missing to hide from law enforcement or has been abducted, errors in the chain of custody could influence the case wrongly (i.e. allowing a guilty person to receive acquittal or an innocent person to be provided a guilty verdict).

// Do's & Don'ts

DO Understand the Scope of The Trace Labs OSINT Search Party CTF

Make sure that you have read and understood the rules that apply to the CTF. You need to adhere to the rules or risk getting disqualified from the CTF and getting banned from the Discord. This is the URL: https://www.tracelabs.org/getinvolved/ctf/ctf-rules/

DO Provide Context in Your Submission

When you submit an entry to the CTF platform, always provide additional information to clarify the importance of your submission to the category. There is a field for relevance and supporting evidence. Use these fields to help your judge understand your submission. Remember that your judge may be judging two or more teams, and depending on the order of the submissions, your judge may not have seen a previous submission where you linked the clue you found to the missing person. Assume that the person opening your submission has no context about your findings.

For example, if you submit a social media handle that has a different name from the missing person or uses an alias, provide some supporting information. Here's another example, when you submit a social media account for the mother of the missing person, be mindful of the fact that the mother may still continue to use her maiden name or may have remarried and taken a different last name.

Provide extra information to explain how you can be sure that this woman is the missing person's mother. You can grab a screenshot that shows the woman's relationship to the missing person.

If you are submitting clues that you got from watching a video, provide the timestamp when that relevant information was shown in the video and provide a short explanation of why you think it's relevant. This will greatly help your judge jump quickly to that segment of the video and it will speed up the judging process. If you can share the link to make the video start at the appropriate timestamp, indicate you have done so in your submission.

DO Establish a Line of Communication with Your Judge

This will help you and the judge stay on the same page and allow you to rapidly respond to feedback to/from the judge.

DO Check Your Bias at The Door

As you go through your OSINT investigations, you may encounter crude language, references to drug use, or another lifestyle that you are not accustomed to. Recognize that as human beings, we all have unconscious biases. However, we need to avoid making judgments based on photos or comments we've seen online. Our goal is to find clues to help law enforcement agencies find the missing person. Avoid speculation and only deal with facts.

DO Look at the Cultural, Ethnic, or Regional Background

By identifying the background of a subject, you can better understand family relationships and gather more relevant information. Consider using a VPN to use the location as your source IP address for your searches. Do some research to determine if people in a particular area use a particular search engine different than those you are accustomed to in your area.

If you can form teams with members from a different background, consider doing this. Most especially if the CTF has an international scope - meaning, missing persons from other countries outside of the USA or Canada. Having an understanding of other cultures will help you figure out whether the term brother

used by the missing person indicates kinship/familial relationship or it's just a cultural reference to indicate shared interests.

If you are submitting any information regarding outside family members, for instance, information on the new girlfriend of the missing person's father, provide relevant details on the importance of this piece of information. Check if there is any indication that there is a relationship between the other side of the family and the missing person.

DON'T Submit Every Follower in The Social Media List as a Friend

Don't submit all the people on the missing person's social media friend list. Look at whether there is meaningful interaction between the missing person and the friend (i.e. likes, comments, check-ins, tagged in events or pictures). Simply liking posts or photos is not indicative of actual friendship. Look at whether the friend had recent photos together with the missing person and whether they celebrated important milestones or public holidays together. Don't submit all the followers as friends, too. Look for any proof of actual engagement in each other's lives. We are providing this information to law enforcement agencies and we want to make sure that the leads we provide them don't lead them to wild goose chases.

DON'T Dispute Low Point Flags (>150 points) Unless You Believe it Provides Critical Intel to the Case

Provide as much context and relevant details in your submission to help your judge make a quick decision on this. If your submission has been rejected and you keep on re-submitting it, only to be rejected, look at the reasons. Initiate a quick discussion with your judge if you feel that it provides critical details. Avoid submitting duplicate information for different categories. The volume of submissions can be high and your judge may be overwhelmed with duplicate submissions. If you are found to be gaming the system, you risk being disqualified.

DON'T Get Outside Help, That's cheating!

Work with your team members. Don't ask your friends for help in finding information and neither should you post public social media announcements asking for information about the missing person.

Even after the event has ended, be mindful of what you post online. You're welcome to do a write-up or give a talk about your experiences while engaging in the CTF. We welcome it and feel free to share it in the Discord. However, we ask that you respect the privacy of the missing person and their family members. Don't post or mention specific case information publicly on social media, presentations, talks, webinars, blogs, etc. If you want to share screenshots of how you did your investigations/OSINT gathering, blur our names and other unique identifiers.

TIPS & TRICKS FOR CONTESTANTS

// How to Avoid Getting Trapped in a Rabbit Hole

Become familiar with the categories for the CTF!
https://www.tracelabs.org/getinvolved/ctf/

Give yourself a set time for collecting information for each category. For example, ten (10) minutes for finding publicly available information on the employment details of the missing person. Avoid getting stuck while reading conjectures or conspiracy theories in some missing persons forum/websites. Remember too that information from news articles or missing persons aggregate websites are not accepted since they are known to law enforcement.

Alternatively, you can pick one person and then set a strategy for yourself to investigate that person, keeping the CTF flags in mind. If you try all the angles you can think of, then it's time to move on to the next type of information you seek and go to the next step in your strategy. Be ready to pivot into a more promising line of the investigation if something seems promising, but if it feels like nothing in your current vein of the investigation will yield any flags, it's time to cut bait and start over or move

on. Sometimes using tabs in your browser, a mind mapping application or notepad, or whatever tracking tools you prefer can help you stay on course and not get sucked down a rabbit hole that could prove to be just a dead-end and eat up a bunch of your time. A thumb-rule that successful teams implement is to spend no more than 1 hour on a subject if you are not finding anything.

// Avoid an Emotional Rollercoaster

So, you're all pumped up just before the CTF starts, then it starts and you see the details of the missing persons in the CTF platform. As you read through the case details, you suddenly realize that there's not much information but as you start searching for other leads, you feel more confident and you start to submit a lot of clues and relevant details. Then you wonder whether you will get any points at all. Sometimes you get a lot of your submissions quickly accepted, other times, it takes an hour or so. You cycle through a lot of emotions as the hours fly by.

It is normal to go through an emotional rollercoaster when you approach an event with a competitive mindset and there's that dopamine rush when you get the points on the scoreboard for the information you painstakingly researched and documented. For the sake of your sanity, approach the CTF as a process for finding information about the missing person and understand that this is a collective effort aimed at helping unify missing persons with their loved ones. Sometimes it can be frustrating to have your submissions not instantly accepted or at times rejected. Understand that there are more people participating compared to the number of judges volunteering. The judges have to verify the relevance of your submissions and often there is a lot of discussion amongst them that may add some delay in the awarding of points.

As you go through your OSINT research, you may encounter stories that are potentially heartbreaking or painful to process. Remember that your mental wellbeing is important. Do not force yourself to continue if it becomes detrimental to your mental health. If you do decide to continue with your research, make sure that after the CTF event is over, you take time to decompress. It could be as simple as making yourself a cup of tea, debriefing with your teammates or spending time with your loved ones.

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 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. For

Australian resources, visit:
https://www.health.gov.au/health-topics/mental-health-and-suicide-prevention/mental-health-and-suicide-prevention-contacts

If you are experiencing depression

Depression and Bipolar Support Alliance
Home | NAMI: National Alliance on Mental Illness

If you are experiencing anxiety

Anxiety and Depression Association of America, ADAA: Home
Anxiety Hotline Number | 24 Hour Anxiety Disorder Helpline

If you are experiencing stress

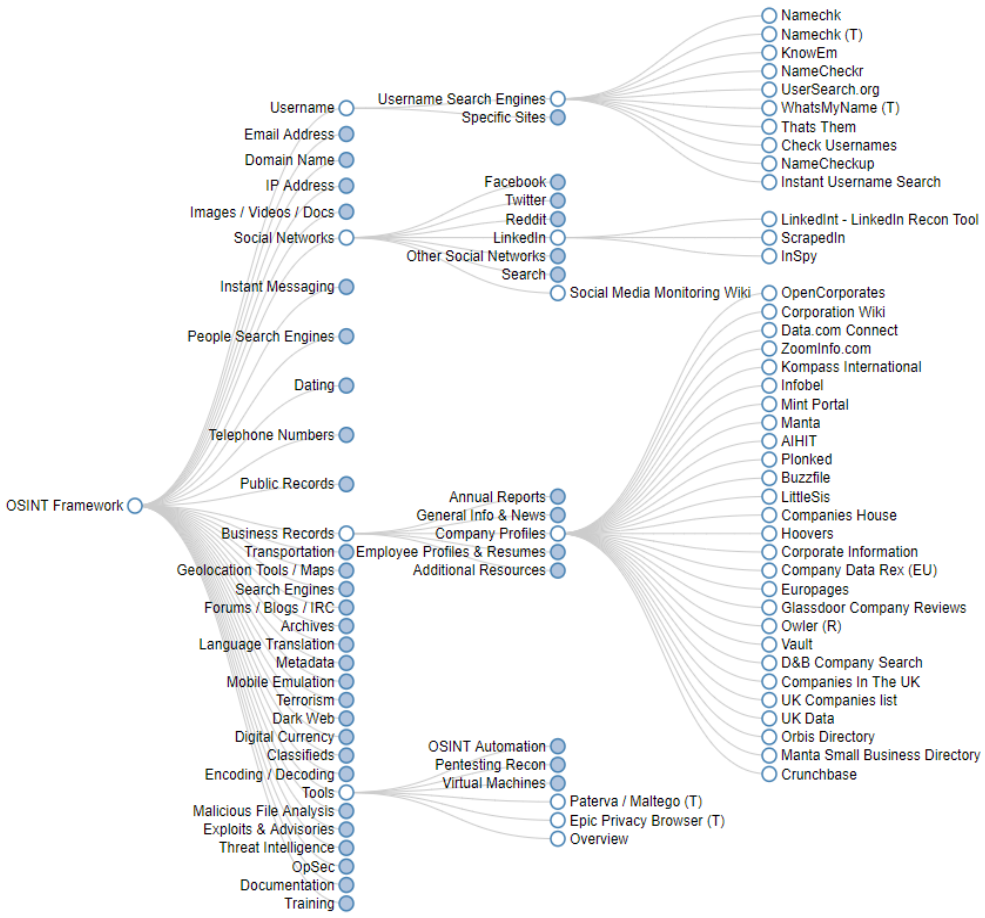
Tips for Coping with Stress|Publications|Violence Prevention|Injury Center
Stress management Resources

// Know When to Move On

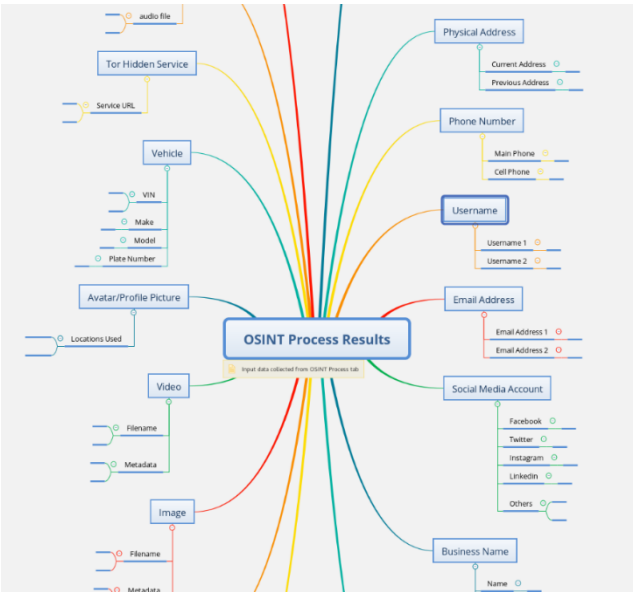
So, you have allocated time for each missing person's case but if you find that you can't get any other leads for any of the CTF categories, then consider it time to move on to another case. Sometimes you just keep on hitting roadblocks. Your time is better spent looking at other leads for another case. As stated before, A thumb-rule that successful teams implement is to spend no more than 1 hour on a subject if you are not finding anything.

// Develop a Pivot Chart

During the course of an investigation, there may come a point where you or your team hits a wall. First, understand that this is normal and happens to everyone. Second, there are measures you can take from the outset that will help when you hit the point of information exhaustion. Pivot Charts and Mind Maps are a great resource when it comes to discovering new areas to dive into. A great example of a Pivot Chart is the OSINT Framework created by **Justin Nordine** @jnordine https://osintframework.com/ The basic concept is that each piece of information found gets added to a chart and linked to the next piece of information until ultimately all avenues have been exhausted.



Additionally, the Mind Map featured on **Micah Hoffman's** @webbreacher blog and created by Steve Hall @shall_1 illustrates how a team can log and format the information acquired in order to see the missing pieces of the puzzle. In essence, the Pivot Chart and Mind Map are essentially the same, they just take different approaches.



// Coping with Success / Failure (It is OK to Fail)

In this contest, success equates to completing the goal and the goal is always: to find the missing persons. You can fully acknowledge this, and also accept that in this instance, hard work won't always equate to success. That said, there's no situation where anyone who competes in the CTF should ever consider their efforts as a failure.

We may not always find relevant or useful information to pass along to Law Enforcement (LE). But what we did accomplish was showing Law Enforcement that they truly have exhausted every lead and that they did their jobs well and to the best of their abilities. To them, that's extremely valuable and it puts their minds at ease.

Beyond what would be conventionally considered as the ultimate goal, locating a missing person alive and well, there is also the risk of locating details that could be disturbing about a missing person or what may have become of them. The most useful advice we can offer is to treat the investigation during the contest like the ride to the hospital in an ambulance. For the purposes of this analogy, you are the EMT in the ambulance and the missing person is the patient. You have limited time to do everything you can for them. But as soon as you reach the hospital you have to hand them over to the hospital staff (LE in this case) and move on to the next call, putting the patient and any concern for them out of your mind.

It's okay to be affected by this experience. It's a crazy blend of contradictions to win points and celebrate those points while finding that the person was in a bad way or in terrible danger. It's very important to make peace with the fact that finding nothing and

scoring no points on a case may be the best possible outcome for that missing person. Your participation alone is a success in and of itself, not only for LE and the missing person but for you. You're going to push yourself and learn new things. You'll get better each time you come back to try again and you'll have the opportunity to impact lives in a positive way, even if that's simply helping a teammate see something from a new perspective and learn how to do a missing person OSINT investigation in a more efficient way.

If you're reading this, you've already made the choice to be successful in this contest.

// Focus on Valuable Information that Law Enforcement Needs

Some information is undoubtedly more important to Law Enforcement after a person has been missing for some time. We have provided a few of the most commonly requested pieces of new information from LE:

1. License Plates
2. Cell Phone Numbers
3. Alias Social Media Profiles
4. New Social Media Posts After Missing Date
5. New locations of the missing person

// Don't Forget the Mission

The primary goal as an investigator in these CTF Events is to find new and publicly available information on missing people. The secondary goal is to enhance your OSINT skills and learn new techniques through other participants on your team.

// Take Into Account Geographic Region and Use Appropriate Search Engines with Geo Settings

Use a variety of search engines. Google is great, but do not discount Bing, DuckDuckGo, Baidu, and Yandex. This is in addition to any regional search engines. Do not put all your proverbial eggs in a single basket, get multiple outputs. Also, take

into account spellings from different areas. For example, ‘organize’ is the way to spell it in the USA, whereas other parts of the world spell it ‘organize.’

TIPS FOR TEAMS

// Different Perspectives Make a Solid Team

It is important throughout the competition to look at each case from multiple perspectives in order to gather the full picture. While your personal perspective is valuable and matters, it is limited by your own experiences and biases. Sometimes our egos get in the way and we believe we have the best solution to a problem. However, we must consider the overall mission which ultimately is greater than each of us as individuals. A 2018 study by Yugo Hayashi found that when groups are made up of members with differing perspectives their problem-solving performance was greater than groups with similar perspectives (Hayashi, Y., 2018). One key advantage of investigating with a team is the opportunity to learn from each other. Differing backgrounds, experience levels, and approaches are all extremely valuable to help build a well-rounded skill set.

// A Diverse Team is an Asset

Taking part in Trace Labs events often means trying to discover information on subjects located across various countries, with varied backgrounds. Having a diverse team is an asset when tracking subjects who speak a different language, or with assorted cultural norms. While we certainly do not suggest picking members based solely on their ethnicity or gender, we do suggest being open and welcoming to everyone with the understanding that different experiences may sometimes be useful.

// Initiate a Private Dialogue with Your Teammates

Prior to the competition, we suggest meeting up with your chosen team members to discuss and plan logistics. This should be done in a private area such as a DM in the Trace Labs Discord, Zoom meeting, Google Meet, etc. where **only** your team

members have access. Ideally, the team should determine how to divide up the investigation, who will be submitting flags and how, where to share your findings with the team as to not duplicate efforts.

Example:

Person 1: Submits flags and communicates with judge
Person 2: Investigates missing people 1 & 2
Person 3: Investigates missing people 3 & 4
Person 4: Investigates missing people 5 & 6
All people rotate every hour to the next job

// Get Second Opinions

If at any point you or your team are unsure about the legitimacy of a submission or the tactic used to obtain the information please reach out to your judge first. There is no shame in asking for a second opinion and in the end, it will most likely save everyone time to have items clarified. Please also note that judges work on clearing info for several teams at once so be patient and work with them knowing that all points will be counted/cleared by the end of the day. Do not hesitate to hop on a team call using Slack, Zoom, GoToMeeting, Discord, or other platforms to verbally discuss, sometimes text doesn't translate well and it could take more time to explain in writing. You can also share your screen on some platforms.

// Work with Your Judge

Each team in the CTF gets assigned a volunteer judge at the start of the event. Because your judge will be reviewing all of your submissions, we suggest reaching out via Slack DM to introduce yourself to begin building a relationship. If you have any questions about whether your submission is appropriate or within the correct topic be sure to ask your judge first.

// Cleanup Post-CTF

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 Discord.

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.