



Trace Labs Search Party CTF from a n00b's perspective

On Saturday 13th August 2022 I participated in the Trace Labs Search Party CTF for the first time. It was an awesome experience and I definitely want to do it again.

Trace Labs describes the Search Party CTF as a non-theoretical, gamified effort that allows for the crowdsourcing of contestants to perform a single task: Conduct open-source intelligence operations to help find missing persons. Whilst the goal is to find the person, it's done through finding individual flags that often build a picture of where the missing person may be.

There was no charge for this CTF (although there is usually a small charge) however before the event you need to register. Tickets are released by Eventbrite before the challenge begins and once you have your ticket, which includes your registration code, you can sign up on the CTF platform. Once registered you can either join a team or create a team, (it is possible to be a team of one). There are 4 members allowed per team. If you are joining a team the creator of the team will provide a code which is used when you click the option to join a team which then gives you access the team's dashboard.

While I was lucky enough to join a team with some Discord friends who have participated before if you're looking to join a team and don't know where to find one there is a dedicated channel in the Trace Labs Discord server to assist with helping people find teams to join. (Discord is a communications platform). I would definitely recommend joining a team, whether it's your first time or you've participated before. If you're new the guidance from someone more experienced is instrumental in getting off to a good start and understanding what's required. If you're an experienced player, then it's great to be able to bounce ideas off each other. Also the subject matter can be a little sombre and it's important to have fun so having teammates to chat with and help you to keep pushing forward is beneficial.

Before the event there is information provided by Trace Labs to guide you round the platform and explain how it works and what the rules are. Although I watched the videos provided by Trace Labs and read through the blogs they provide relating to the challenge I still wasn't sure what to expect. Fortunately, one of our team had competed in this challenge before so was able to provide support and guidance to me and our other team member, who was also new to the CTF. Their guidance was invaluable in getting started and making the CTF an enjoyable experience.

As explained above the challenge is to find relevant information on genuine missing person cases that could help law enforcement complete their investigations. This is done with passive OSINT (Open Source Intelligence) which is gathering information about a target without directly interacting with the target. You collect and analyse information from publicly available sources without interaction.


To begin with you are provided with information on a number of missing persons. You then use that information to find more intelligence. For example, you may use the information to find that person's social media account. However, you will need to ensure you have enough information to validate that the account is the correct one for the investigation.

Once you've found a relevant piece of information this is your flag and you submit it on the CTF portal. To do this you need to provide the piece of information, an explanation of why it is relevant and any supporting documentation (such as screenshots, URLs, etc). The submission is then reviewed by a judge. The judging panel comprises of volunteers who vet each submission to check it is valid and will then accept or reject it. If it is rejected there will be a comment to explain why and if the reason is that more evidence is needed, you can then search for more corroboration and resubmit with the extra details.

For each accepted flag you receive points. The number of points depends on the category of the information as they are based on the potential value to the investigation, so 'friends' may be 10 points, 'employment' 15 and so on right up to 5000.

Once you have an accepted flag you carry on finding more pieces of intelligence using what you have to find more links and following those leads to get more useful information. For each flag accepted the score for the flag is applied to your team and a scoreboard shows where each team is up to.

Although this time I did not find many flags myself I learned a lot and had fun. I'm very much looking forward to participating in future Trace Labs search party CTF's.



Contestant - Global OSINT Search Party CTF

Awarded to **Sarah Williams** (feet_of_clay@hotmail.co.uk)
Issued on **13 Aug 2022** at 8:00 am

Awarded for participation as a contestant in a Trace Labs Global OSINT Search Party CTF.


Share ...

Offered by **Trace Labs**

Badge Details

EARNING CRITERIA
Recipients must complete the earning criteria to earn this badge

Assist law enforcement in crowdsourcing new leads on missing persons cases using open source intelligence (OSINT) in a Trace Labs Global OSINT Search Party CTF.

[View External Criteria](#) 

TAGS

osint ctf osintsearchparty trace labs

NARRATIVE
What the recipient did to earn this Badge

Issued to contestants who successfully completed the Trace Labs Global OSINT Search Party CTF 2022 08 Defcon Vegas event.