Intelligence101 Interview with Robert Sell

INTERVIEW SERIES:
INTERVIEW WITH ROBERT SELL OF TRACE LABS
Providing Crowdsourced OSINT for Missing Persons
TRACE LABS

Question 1. The origin question – Can you tell me how Trace Labs got started, more specifically, where you guys came from (perhaps a bit of a back story) and what drove you to set up Trace Labs?

Trace Labs started with a frustration I had. I've been a volunteer in Search and Rescue for about ten years now and in that time I have seen some terrible things and also been lucky enough to help a few people. It has been a very rewarding experience and I feel very to be part of it. To see the tears on a parents face when you bring their child back from a mountain or river is beyond words. It really grounds you as a human being and makes you realize what is important. I always feel better as a father when I go home to my family after a Search and Rescue task (even if it was in the middle of the night and I have to work my day job in the morning).

However, I know how many missing persons we look for and its not that many in comparison to how many I see go missing. I often wondered who were looking for these people if we were not. I began to talk to police and the families of these missing persons and there seemed to be a gap there. Since most missing persons come home within a week and law enforcement will naturally prioritize criminal activity, missing persons may not always get a lot of police resources. Since most come home within a week (about 75%) this makes some sense. My concern was for those that do not. What would I do as a parent if my child was in the 25%? Would I know what the police were doing? Would there be transparency and would I get much police resources? Some of this depends on the location of the missing person but overall, as a parent I know I would want the world looking for my child. No amount of effort would be enough.

So I began to think about a way we could improve this situation. Since I work in IT as my day job, technology is often the solution I apply to most issues. Began to think about all the talented hackers and information security professionals I know and how they could help. I searched the Internet and very quickly found hackers who were fighting crime and helping families with missing members on their own. I reached out to them and asked them about my idea. I created a network of consultants whose identity I didn't know but their guidance was very helpful. They allowed me to understand the issue even more and provided me case after case of families that were destroyed by this.

Trace Labs was born soon after this. I took the idea to Vegas. Defcon is the worlds largest hacker convention and normally brings in about 20,000 of the world's talented information security professionals. Often zero day exploits and other discoveries are revealed there. Trace Labs was accepted as an official contest at Defcon 2018. At that time we were operating out of a Slack channel but we managed to make it work. We had dozens of contestants who found hundreds of data points. The next event was in Toronto, Canada and resulted in locating two of the missing persons. This was amazing as we never actually expected to find people. We just thought we could help law enforcement with more data.

Since then we have had events every month all around the world. This includes Australia, Canada, USA, Nepal and others. We have brought on 3 new Directors who are part of the senior leadership team and are really helping it to grow.

Readers would be particularly interested in the training and application of skills as an example of the type of work they can get in to.

Question 2. You teach OSINT skills and focus on finding missing persons. Do you have a case study, or example of a successful campaign you could share with the Intelligence101 audience?

Readers would be particularly interested in the method, tools and how they could learn the skills also.

So right now we don't actually teach OSINT however we have plans for this in the future. On our Slack channel we have constant questions and answers on various OSINT subjects. We also are beginning to hold crowd sourced OSINT events at universities where we partner with existing Information Security curriculum and provide a hands on real world experience.

As far as a case study of a successful campaign, I would likely say some of the biggest events we have had were in Toronto, Portland, Montreal and Australia. Those are some of the hot spots for OSINT operators right now. We see huge turn outs in those areas and they pack the room with high quality contestants. It is very normal for teams from those regions to get a location on a subject. While the smaller events are good as well, the bigger the group the better the results are.

Its hard to pick a particular team out from all the ones I have seen so I will generalize a bit. Here are some traits I have seen from successful teams:

1. Come prepared. You need social media accounts if you want to search within these platforms. This can be your existing account or a sock puppet but either way you need to be setup beforehand. We have seen platforms ban IPs where they see fresh accounts doing lots of searches. Also, you may not want to use your work laptop if your on the dark web. Finally, you want to have your VM (if your using one) and all your tools configured prior to the event. Setup can take a while with something like Maltego.

2. Team work: You don't have to have a team full of OSINT experts to do well. What does help a lot is a team that can coordinate and communicate. We have seen teams with beginners do well as they focused on lots of easy flags. Also seen teams with some beginners and some veterans do well when they divide and conquer. Also, some teams will have team members all look at different subjects. Helping each other seems to be the secret to success. I have even seen teams come together to get more OSINT which is rare in a CTF like this.

3. Work flow: Many beginners get stuck and this can lead to frustration. I often point them to the inteltechniques.com website as it has lots of tools on it. In particular, I like the new edition of

Michael Bazzell's book as it has some wonderful workflows at the back. This is key because it helps you visualize what you might find based on what you already have. As a SAR tracker, I am used to this mentality. I look for "sign," I don't look for the person. Sure it's great to find the person but I look for the footprints, broken branches and bruised leafs first. OSINT Operators have to think this way too. Start with the basics and then build off that.

4. Look on the peripheral: I often see teams do well when they focus less on the subject and more on the peripheral. Looking at friends, family and even employment can really help to get more details. For instance, Facebook comments can often tell you what ever the friends know. Instagram is great for timeline and detail in pictures. Criminal records can be very useful to find aliases. Club membership can also be useful. Be creative.

5. Expect to get stuck: As soon as you hit a wall, try something else. Sometimes that means switching subjects (we host 8 on each CTF) or perhaps try different techniques. Worst case, take a break and have a coffee.

Question 3. I get a lot of students and readers interested in Intelligence & investigation careers. What advice would you give to people interested in becoming a part of the work Trace Labs does?

We are always looking for people that are passionate about this industry. If they want to be part of Trace Labs, I can suggest a dozen projects they can help us with. Everything from training to community events. If they want some experience to put on a resume, I can assist with that.

One key differentiator that separates Trace Labs from other events or groups is that we focus on the non theoretical. Rather than doing OSINT on fake info we allow contestants to look for real people. I think this experience in itself is great experience. If a student or reader does not have time to support Trace Labs in one of our many committees then just register in our next virtual event and play the CTF. This is a lot of fun and is completed in a day. Check our Twitter for updates on these events.

Question 4. In terms of OSINT and your professional career, what are some of the challenges / pit falls you've had over the years? Could you share any lessons with how you overcome them?

My journey with OSINT has been one of continual challenges and pit falls. It seems the moment I think I have it figured out, I realize there is a bunch of stuff I don't know, a new tool I never knew about or a cool technique I didn't know. This is the state of OSINT these days. I listen to about 2 hours of podcasts and audio books per day which is mostly around this subject. I also do a lot of research on the industry in general. This makes me feel like I'm winning but the industry is moving so fast there are still lots of surprises.

Some lessons I have learnt the hard way are as follows:

1. Scale: This basically means get your platform and tools sorted out so you can begin an operation at a moments notice. You want to be able to operate without building a bunch of tools and then shut it down only to do it again the next day but perhaps on a different target. There are many things you can do to achieve this. I like to use a new VM for each operation (snapshots are your friend). I also think tools such as Hunchly greatly aid in operations. I document both my techniques and tool configurations so if I have to, I can build new.

2. Preferences: My preferences are meaningless to the subject. While I might be the boss at pulling stuff out of Facebook, if the subject prefers YouTube that doesn't matter. Find the social media that they prefer.

3. Friends: Don't be shy to ask for help. I am amazed at how helpful this can be. New perspectives can be amazingly helpful.

4. Time: We live in a world of 15 minute increments. My dentist got mad at me the other day when I told her I never just brush my teeth and instead always need to be doing something else while I'm doing that. Just brushing teeth feels like such a waste of time otherwise. She was not impressed. When you are doing OSINT it is best to turn the phone off (and the TV) and really focus. Make sure you have at least an hour to focus. I suggest at least a few hours but even one dedicated hour without distractions can be very productive. After four hours your mind will begin to have issues and you likely need a coffee, walk or some other stimulant. Avoid interruptions.

Question 5. What advice would you share with junior analysts (across any discipline) to increase their skills, so they can ultimately make a difference in their role and organisation?

I think two things can really make a difference:

1. Stop wasting time on theoretical practice: There are so many opportunities to do real OSINT. Our CTF is one example but there are so many. Do it for free and give it to customers as a gift. Sooner or later that customer will hire you. OSINT files are really starting to become more valuable and by showing potential employers what you can do is a great way to get interest.

2. Own your destiny: Fortune favors the bold. Stop waiting for people to give you a chance and instead go make it for yourself. I used to always wait for permission or wait for the right time. It never comes. Life is short. Instead, start doing OSINT on whatever you can. Do OSINT on your existing employer and then do a presentation on what you found. Not employed? Do it on the school you go to. Show them what private information they are revealing and the risk it presents. Do it in a professional way and don't try to scare them. Be factual.

As a hiring manager, I like nothing better than when an employee comes to me and says "Rob, I think this is an issue and I want to do this to fix it." I am immediately impressed. They identified and issue and then rather than complaining about it, they took ownership of it and figured out a solution. They are really just asking my permission to implement the solution. That's an all star employee. Not every boss will be keen to this but most will. Test the waters.

3. Be a professional: This makes all the difference in the world. This is not an OSINT specific recommendation but for anyone who in junior who wants to do well in an industry. Start with always showing your manners. Ensure you say "please" and "thank you." Understand the interview process and come ready to tell stories about your experience.

Bonus Question (if you feel like answering): Is there anything you think I should be asking you specifically? If so, maybe a quick answer?

One question we get a lot is, "what if the person does not want to be found?"

This is a fantastic question and our answer is that we only look for people the police are asking the public's help to locate. This is our invitation to assist. We get a lot of people asking us if we can go looking for their friend or family member and our answer is always a request to get the link to the page where the police are asking the public's help. This ensures we are always looking for valid missing persons as per the police. We must have faith in law enforcement to know when we should look for someone as no one else can make this call. So we basically act as an extension of this existing focus. Is it perfect? Likely no however we think we are providing a lot more good than bad. Plus, if we see a case where we think there is a risk we could be causing harm, we drop it. There are so many missing persons out there we are able to pick ones that have the greatest potential of benefiting from our efforts.

- End