Ritu Gill, Unlocking OSINT

Mindy: [00:00:00] Welcome to Analysts Talk with Jason Elder. It's like coffee with an analyst, or it could be whiskey with an analyst reading a spreadsheet, linking crime events, identifying a series, and getting the latest scoop on association news and training. So please don't beat that analyst and join us as we define the law enforcement analysis profession.

One episode ahead time. Thank

Jason: you for joining me. I hope many aspects of your life are progressing. My name is Jason Elder and today our guest has 16 years of law enforcement and analysis experience, 12 of which with the Royal Canadian Mounted Police, she created the Open Source Intelligence Techniques website, which is resources for , open source intelligence, and social media investigation.

she's an instructor for . Sans coming to us from British Columbia, Canada. Please welcome Ritu Gill Ritu. How we doing?

Ritu: I'm doing great. Thank you so much.

Jason: Well, of course, Syd, we're gonna be talking about osen today and really looking forward to getting your perspective the different [00:01:00] techniques and what the dos and don'ts that you recommend to our listeners.

But first I wanted to go over how you got here. So how did you discover the law enforcement analysis profession?

Ritu: So, it starts way back. I did my bachelor's degree in criminology. At that time while I was finishing my degree, one of my instructors invited an analyst to come talk to us about what crime analysts do.

I was in my fourth year and I got really. Interested. And that's when my mind started kind of going towards the policing. Not only policing, but the role of analysts in policing. So after I finished my bachelor's I actually started a job with In a department with the muni police, the local police here in records.

From there I went and I learned a lot of the basics. So from the ground up, I learned the databases, the police databases, so those closed sources. I worked there until I ended up leaving about three years later. And I worked for the security unit. [00:02:00] 2010 Olympics. I assisted with the mobilization of police officers across Canada who were coming to work during the Olympic events in Vancouver.

From there, after the Olympics were over, I eventually moved federally. I still wasn't an analyst, but I had the opportunity. To move into a section. I worked actually for my then manager Baltej Dhillon, who's an incredible person. He was actually the first mounty from the RC m p who was permitted to wear a turbine because of his Sikh religion.

So I worked with Belte. He gave me a great opportunity to get into a researcher role. And then from there I moved into a more analytical role and kind of I moved to different sections throughout in the RC m p working as a researcher. Working as an analyst. And yeah, that brings me, I guess today where I work as a open source intelligence analyst for a law enforcement agency in British Columbia.

And I've been actively working as a ENT analyst for [00:03:00] a number of years now. Supporting investigations with open source research and trying to help files move forward. Provide recommendations and what investigators can do from the open source perspective. So that's kind of where I'm right now.

Jason: All right. Very good. So when you were in records, was it still your goal to become an analyst?

Ritu: When I was in records, it wasn't really a goal. That was the start of my career. So it was like the foundations of, you know, working in a police environment, learning the basics of everything. So that interest came later on when I was mm-hmm.

When I was in university. And when I had met another analyst who came in to speak, that's where I got really curious and interested in, in what a analysts for the police could do.

Jason: Yeah. Hmm. A and I've talked to several analysts now that began their career. In something other than an analyst position with the [00:04:00] police department, and it's, it is fascinating.

It, it seems like no matter what you do, you're getting something out of that. Records is a great example there because you're learning the data, you're getting, you're understanding how the police department collects records and what the computer system is. And, and so my always recommendation to anybody that's struggling to get into the profession is just find your way in somehow.

And I think that will help you in, in whatever form you're in with the police department.

A

Ritu: hundred percent. I, I agree, Jason. I think working when you work in a place like records, and I do have a lot of people ask, they're like, Hey, how did you, how do you get into what you do? I'm like, I started from the ground up.

I mean, I didn't just roll into the position I am in today. It was a series of, you know, steps I took, you know, finishing my degree, actively pursuing, looking for a [00:05:00] job in policing. And I was okay with starting from the bottom. And records was like that clerical kind of work, but it also gave me a lot of the foundations I needed.

And of course I mentioned earlier I talk about the learning the police databases. Well those are closed sources and if you look at what I do now, I'm a ENT person, which is the opposite. It's the open sources. But as a employee, as as a employee doing work for them it's important to know both.

It's important to understand how closed sources work and what we can get out of them. And it's also, of course, use using those in conjunction with open source at times. Hmm.

Jason: And then with the security position with the Olympics was that a full-time job or was that like part-time

Ritu: temporary? That was a full-time job.

I saw that being advertised. So at that time I was in records. I've been there for a few years. I felt I had learned as much as I could there. And I didn't. I wanted more opportunity. I know I wanted, I [00:06:00] knew I wanted to keep growing. And advancing my career. So I started looking and, and when I saw that job come up federally of course I was leaving a full-time job this to another full-time job.

Totally different. And I just took a kind of a leap of faith hoping for the best. I didn't know exactly what I was gonna land into. But it turned out it was probably one of the best decisions I made career-wise because it opened up so many more avenues after the Olympics were over.

Jason: So were you in a situation where you had.

Access to various agencies and could network. That's what I'm

Ritu: envisioning. Yes. At that time I mean there were so many different agencies and people and individuals that came together for, at the security unit. I mean, you know, I remember the military being there in the same venue and, and that kind of stuff.

So definitely a good opportunity to network. I was still, I feel when I look back, that was still really a younger time in my career, so I don't think networking was at the forefront of my mind at [00:07:00] that time. Yeah. However, I was working with people who were had many years ahead of me and so I feel like there was a lot of, you know, things I took away from working with them.

And it was still, I consider that still building those foundations of my career. Cuz I still wasn't in. The role I wanted to be in at the time. It just, it was the various steps and, you know, learning about mobilizing, mobilizing police officers right. From all across Canada and , what that entailed.

Jason: So what did you wanna be at this time? What was your goal

Ritu: at that time? I was still in the mindset of, okay, I want more. You know, and I wanted to continue and that was kind of always in my mind. When I did my bachelor's, I was like, I don't know exactly what I'm gonna do.

I'm gonna end up in policing. And then the whole analysis part came up and I was like, oh, being in a crime analyst, that's interesting. Mm-hmm. All I knew at that time was I wanted more. I didn't know what the path looked like at the time and I just, I looked for opportunities, you know I went to my managers and I'm like, Hey, is there room for [00:08:00] movement?

Would I be able to get a job as a researcher? So those things did come into my mind a little later on. When I did talk to managers, I put it out there that I was interested. I was like, I wanna learn to be, you know, what a researcher does, cuz that next step would be being an analyst. Right. So I kind of saw, had that foresight.

So that's what that looked like for me.

Jason: Okay. And then how long did you. The security job

Ritu: that job was. So it was about two years, I believe.

Jason: So when you look back at that then, , what comes to mind ?

Ritu: When I think of that time, I just think of, I guess the word opportunity really. Mm-hmm. I, I think that was a huge stepping stone for me to get into the next kind of segment of my career. I'm really glad I took the jump because, you know, a lot of people, other people could have applied and got the same job.

I had no idea at that time where I would end up after the Olympics were over because we were only given, Hey, you're gonna have this job until the [00:09:00] Olympics are done with. Mm-hmm. After that, there was a promise that you would get a job with the federal government, but, It did not specify where, so Oh, okay.

I, yeah. So I was kind of taking a big chance you know, I could have ended up working for any other department, really. Mm-hmm. Of course they wanted to know like, Hey, where would you wanna work? But that doesn't mean that you would get what you wanted always. I was kind of curious about gangs at that time.

I remember that. And yeah, that's kind of where, be Tej. Dylan came in and I got a phone call because at the end of the Olympics or near the end, it was like, you know, he's like, I have an opportunity. It was an admin position in his unit. And I said, well, Hey, yeah, I'm interested. That, that'd be interesting working in like a gang unit.

However, I don't wanna stay at the admin level. Is there something more that, that will be available? And at that time, he said, right now this is what we have, but you do have opportunity to grow. So he gave me enough information that made me say, I'll take the job. Yes, I'm [00:10:00] interested with the hope and, you know that I would get the opportunities to advance my career.

Right. Move from mm-hmm. Doing admin to more operational things like being a researcher or maybe being an analyst. So that was huge for my career. Okay.

Jason: So just so I'm understanding the terms, obviously admin to tactical, I certain types of work that you're doing there as an analyst, but then.

It sounds like is researcher the, the base level, and then you, it sounds like you then work your way up to an analyst, correct?

Ritu: Yeah. For, for at least for what I was doing at the time. Yeah. Like the, the, the path I took was of course the admin totally separate, but moving into a researcher role, again, I was already familiar with police databases, but as the role as a researcher were the steps towards being an.

It was like I was halfway there doing that

Jason: work. Okay. Okay. So, so what does a, what does a researcher do and what does an [00:11:00] analyst

Ritu: do? Well, I think, again, for my situation, I would say researcher was more, Hey, we have 10 databases, for example. And we would just extract information. It would be more, there would be some critical thinking of course, and, and perhaps some analysis.

But it was mostly pulling information that might be relevant to a file we were working on at that time. There's of course gonna be special parameters on what we're looking for, but I would say the biggest step when in going from, there's so many different types of analysts too. You have to keep that in mind, right?

Especially with policing. There's, you know, you could be a tactical analyst, you could be a crime analyst. They do different things. I would say the analyst part, the role can completely change. As a researcher say, I wasn't building up reports or writing reports, but a as an analyst, that's what I was, that's what I was doing.

I was writing profiles on say, a business or a person. So that involved critical thinking [00:12:00] analysis you know evaluating all the different things I'm finding and making sense of it. All right.

Jason: And then, so you start out as a researcher then, but on the admin side, and then where do you go from there?

Ritu: So in my SI situation, I gained a bunch of experience working as a researcher, so getting even more comfortable in, in supporting analysts, right? Mm-hmm. Because as a researcher able, able to work with the analysts, do not doing their work, but supporting their files, seeing what they do For me later on I ended up moving from a few sections, different sections.

And then I worked for a section called I would say this is where the open source kind of started. It was, mm-hmm. It's called fsoc, federal Serious Organized Crime Group. So I worked for them within, for the R C M P. And there was when I had the opportunity to start working full-time as an OSEN analyst.

Jason: Hmm. Now did it feel like this was home? And [00:13:00] what I mean by that is it seems like you were l on a journey to this point. You, you kind of didn't, you, you kind of had an idea what you wanted to do, but wasn't definite and you tried different aspects. To the, to law enforcement, different aspects to the department there.

Once you got to that open source area, did it feel like home?

Ritu: It did. Yeah, it definitely did. I would say that's where I felt I was like, I was waiting to kind of get to that spot, but also still really eager to learn everything I could about that role, about the ins and outs of doing that work. Because I was working alongside several kind of senior analysts, which was really helpful.

I would say sitting with them and taking in like their experience cause somewhere on the way to retirement. So they've been doing this job for a very long time. So I would say, yeah, like I definitely felt at home being there. Open source was, I mean, that wasn't what I thought back when I was [00:14:00] working Olympics at all.

I didn't know that that was a job at that time. You know, using publicly available information to support investigations. You know using social media, using other sources of other open sources and providing that to investigators to support their files. Okay.

Jason: So then, so I think obviously with smaller departments or where you're an analyst, you're the jack of many trades kind of thing, so there wouldn't be a department dedicated to open source there.

So, and so I'm trying to get an understanding of how this works. So an investigator, you know, needs research that's more tactical based, so there's a group for that. If there's one, the need for more administrative information, they go there. And then now there's this open source unit. So if there's an open source need on, on the, based on the investigation that the detective would go there.

Is [00:15:00] that how it works? Yeah,

Ritu: I think like, I mean, the layout of how different police departments do it and, and or government agencies, it's all gonna vary from agency to agency for sure. You know, like you said, like there's certain police departments that kind of have it all right? They have a open source unit, they have a, like crime analysts in one section.

They have open source analysts in one section. That said, it's not always like that. Sometimes it's, hey, there's sometimes an analyst and you're doing everything. You're doing open source, you're doing. The analytical stuff as well. It, it really depends. But yeah, that is like essentially like my, my kind of the way I worked with other people was I would work with other analysts.

That was how it started out supporting that file. And, you know, they would do their other stuff. You know, sometimes some, some analysts did like phone dump analysis, but I might support the open source side of that to the file. So providing research, providing other things that I see online [00:16:00] that are maybe of interest to that file.

Okay.

Jason: So then when you're starting out in this ENT group, you mentioned that you're working with senior analysts. So this is already an established product that they have set up there. So what's the, what's the training like, or how are they teaching you how to do the job?

Ritu: So, I did a lot of I guess job shadowing in a way.

I mean mm-hmm. Just sitting next to them and learning, Hey, what, how are you doing profiles or how are you doing your, the report writing? Right. Cuz it, that varied from individual to in individual. Definitely. There was like a template maybe we followed but sitting with somebody, so it was almost like informal training.

Mm-hmm. That being said there are going into, depending on what section it was sometimes there was a more standardized process of like, Hey, you're gonna take these four courses, you're gonna take these four courses, and then you're gonna sit with this individual and learn, learn their job. Right.

Learn from them. For me, like I would say [00:17:00] anytime someone's asked like, Hey, how do you get into that? I'm like, there's so many different ways you can get into it. I would say definitely take the time and sit with the people that have been doing this for a while. Ask the questions, right? Because those were naturally come up when you're, you're looking at how somebody's process or you know, how, how they're finding information.

Yeah, there's a lot of like, tips, techniques, tricks learn, just learning from others. And that's why as the years kind of went by, I just picked up on some of these things as I went along. So definitely on both informal and formal training like a combination. But I would say being a self-starter is really, really important because I don't think a lot of this stuff like rolled into like onto my lap, like it was stuff I had to like seek out, you know, I had to put the interest out there.

At the end of the day, nobody's gonna, nobody's gonna just hand things to you. Like, I think you really. Be a go-getter when it comes to, I wanna learn that job, or I wanna, I wanna job shadow that person. Can I do that? Approaching managers, approaching the right [00:18:00] people that will be able to help you along the way.

Yeah, I

Jason: really like the tenacity and it I, I've been told that in my career too, that because I was asking the right questions led me down the path that I was getting , at a police department. So in terms of starting out with this unit and it's open source, I think a lot of people think open source, they automatically think social media.

what types of open sources are you using at this time?

Ritu: So everything I would say of course a lot of people think like, oh, social media, like, that's fun. And I'm like, yeah, like tons of fun. People put a lot of stuff out there that they shouldn't. Mm-hmm. However, open sources also encompass, encompass, like business records, right?

Because certain parts of the world that information isn't private, it's public information. Mm-hmm. So corporate records news media, of course that has a. Because of privacy laws, as I [00:19:00] mentioned, like some, some countries have a lot of information on their citizens and then there's some countries that really privatize the content and it's limited as to what you could find.

But definitely like all sorts of social media corporate records, like, so those public records, right? Like even down to things like arrest records, right? Places in the States that that is public information. Whereas in Canada, a lot of that is private information. Mm-hmm. And it varies from province to province as well you know, in terms of like what's available.

So knowing that is also helpful. I created a, a resource actually for Canadian investigators. It's a, it's a start me page. And I, I'll hopefully have the link for you for the show notes, but it, it will have all the open source resources that I could think of for each province across Canada. So it's just like one of those resources I never saw online and I just thought, why don't I create this thing just to help people out?

Because hey, if I'm doing an [00:20:00] investigation and, you know, I'm from the west coast, but if it's somewhere in Say it's in Ontario and I don't know what their, you know, open sources look like. Can, like, can we get company information on people? Well maybe that this is a resource somebody could look at and, and get a starting point at least.

Jason: I think most people just assumed it's all online, but through certainly. Opportunities where you can go to a particular government office and it's open source, but it's not something that may, may give out online.

Ritu: Yeah. I've, I typically, the, the open source I do it is mm-hmm.

A hundred percent online. Mm-hmm. You know, sitting behind a computer for, for 10 hours a day doing this. But yeah, that's said like, I mean, technically information at a library is open source. Right. There's things that you can get at a library, like, I mean, I haven't been to a library in a while, but there's certain databases that you can log onto Yeah.

And do searches. So those are open sources as well.

Jason: Also, would you [00:21:00] consider open source if it's something that you know, you might need to give your credentials for? For instance, you, you might be something where you have to let them know that you're in law enforcement.

Ritu: Yeah, I mean, it, it depends. So the way de open source is defined, I mean, it's publicly available information. Mm-hmm. That said, like it should be available to the public. If I'm giving my credentials, like there could be things like, there's database subscriptions mm-hmm. To things like pimple, right?

That's a people search engine. You gotta pay for it. And I have to enter some sort of login to get access. However, everything within that database is open source. So, I could say that, hey, there are paid open sources out there. Mm-hmm. You know? Mm-hmm. So are they publicly available? You could say Yes.

However, I gotta pay loads of money to get access, so those can still be considered open source.

Jason: All right. You mentioned the start me. [00:22:00] Was there any other products or anything else that you, when you look back of you're proud that you accomplished?

Ritu: I would say, well I definitely I've done a lot of, I would say a lot of little products or, you know, depending, cuz I have my government job and then I have my private consulting business as well, so it's different. So I'm not gonna, I won't be able to mention specific cases. Mm-hmm. But definitely like the most, I could say the most exciting files were the ones that had like, say, a national security angle.

Mm-hmm. Also another thing I'd mentioned when it comes to like just, it maybe interesting things, the cases that caught my eye the last couple of years just kind of kept things interesting were the, say the events at the US capital. January 6th. And then another one in Canada, across Canada was the Freedom Convoys.

Right? Kind of the anti-vaccine movement. So if you're wondering like, Hey, what was interesting, it wasn't just how much information was available in open sources during that time, mainly across social media [00:23:00] platforms, but the platforms that were being used that were like lesser known for Osen, that's what was really interesting and really relevant at that time.

So for instance, , there was an app being used during the Freedom Convoys called Zello. This was also used during the, the January 6th capital Riot. But Zelo is a two-way radio. So many of the people at the Freedom Convoy were communicating, using this app because they were driving and they were looking to connect with like-minded individuals who also wanted to protest.

Mm-hmm. So, I thought that was interesting. Just in general, like when I look at kind of like what, what took place contributions that you've met you were asking about. I was, there was a project that's no longer running, but it was called Osen, the Osen Cur Project. So re we recently kind of concluded creating more content for this nonprofit.

It essentially was a blog where a group of us osen people wanted to share osen techniques. Mm-hmm. The content is still up and it's [00:24:00] gonna stay up there. It's on a website called Osen curio.us. It's a great place for people to go and learn about open source, whether they're starting out, whether they wanna advance some of their scales.

So that's something. I was on the advisory board with o Stur for a few years. So that was a great thing that I thought we did as a group. Yeah, just cuz of time and whatnot. That's why we kinda had to conclude it just this actually month. We just thought, hey, there's a lot of content out there, but just cuz of everyone's limited time, it's hard to keep up with something like that.

John: Hi, I am John Ng I'm a prime analyst with the Las Police Service. The public service announcement that I have is for, especially for junior analysts, but also senior analysts, just be true to yourself and recognize that the police culture that you're in shouldn't necessarily shape who you are, but you have something to bring towards your service as a benefit as

well.

Kyle: Hi, my name is Kyle McFatridge [00:25:00] and I want to talk to you today about merging in construction zones. You've probably understood merging in construction zones to be getting over as fast as you can. This is not correct. Merging lanes are designed to be filled all the way to the point they end, and traffic then merges one vehicle at a time.

Ritu: Think about it logically where traffic flow better if people randomly stopped put on their turn signal and tried to get over. Or if both lanes were completely full, the lane is supposed to be full until the point you come to a traffic cone and can no longer fill it. So to the people that block that lane swerve at cars, honk, yell, or flip off people trying to use the merging lane correctly, you're not only rude, you are wrong.

You do not get angry at people who pass you in the left lane a couple miles from that construction site. So why would you then be angry at them for passing you at the construction site? So next time you come to emerge in a construction zone, remember to go all the way to the end and merge one car at a time.

You'll be doing it the right way

Jason: and help make traffic flow

Ritu: much better for everyone, even for those angry people. Thank

Jason: [00:26:00] you.

Now, , you mentioned some of those events where you're gathering the open source information, and did you know ahead of time what apps folks were going to be using? Or was that something you found out like as the event was happening?

Ritu: That's something I found out as the event was happening or the events were happening.

That was just through, I mean, looking on the online kind of angle of things, what was happen. During that time for the Freedom convoys, looking at things happening in Ottawa, you know, what people are saying online and then realizing, hey, they're using this app, what is this? Mm-hmm. And to my knowledge, I had no idea what Zello was.

I was like, what's Zello? So I started doing my research. I was like, oh, it's like a two-way radio. I'm like, makes sense, right? If you're driving, you're not gonna be texting. You can't, but you can hold down a button and leave a audio message. Right. Okay. So yeah, that's kind of like through my research and, you know, just curiosity [00:27:00] wanting to know like, Hey, what happened even after January 6th?

Like, okay. And then reading a lot of our articles and looking at, again, at that time, what are people saying online? What are some of the groups saying online? And then seeing this different apps that are being used at that time. I, I thought that stood out a

Jason: bit. Yeah. So it's, it's fascinating because to me it wouldn't take very much to stand up a forum or stand up an app, for instance, for just a particular purpose.

Right. If it was well organized, you just stand that up and that's the way you communicate in, in those forums. Right. And it's that it could be very temporary, it's not something that needs to be on forever. But if they have a particular need that we need to communicate during this particular time, and we want to obviously not be detected by the authorities, it seems to me that an an option would be to have one of these [00:28:00] temporary situations.

Ritu: Yeah, no, for sure. It was interesting because a lot of the, the channels, the Zello channels were posted publicly on like Facebook, and it wasn't like what I'm trying to say. It wasn't difficult to find them. Some of them were like, here's the QR code scan here to get to the, which would take you exactly to the right Zello channel.

Because I remember looking at the time, Zello was, you needed to know the exact name of the channel, otherwise you wouldn't be able to find it. Oh, okay. Yeah. So that, that was a little bit of a challenge, especially if you have like one word or one letter off, you're like, I can't find it. You know? Or they ha have it, they have other characters in it or something.

But yeah, that was, that was kind of interesting to me. Like I always say, like I did a presentation on lesser known platforms for ent. Mm-hmm. At a vent called the Calgary. Cyber Crime Summit in September, and I, I highlighted some of those lesser known platforms for ENT investigators and one of them was Zelo because I'm like, Hey, well here are a couple examples to show [00:29:00] you in the last couple of years where it came up, where it was being used, how it was being used, and then showing the audience what it looked like.

Right. You know, just giving, giving some visuals always helps to show people like, Hey, what I was seeing at that time, this is what I saw. This is what I saw on Facebook. This is what the app looked like. This is what maybe it sounded like. Right. It was a ten second clip of being like somebody being in a certain location or, or wanting to meet up with other people.

Yeah. That's,

Jason: man, that seems like so much, I'm just thinking in terms of trying to teach this, you talked about at the conference or through your instruction and, and even your consulting work. I mean, really it, it seems like it's never ending. It, it seems like it's so vast, and probably that's the reason now that I'm thinking about it out loud.

That's why you need a whole unit dedicated to this stuff because there's that many avenues to travel through to make sure that as you're supporting investigations that.[00:30:00] , you make sure to travel through all the different avenues.

Ritu: Yeah, definitely. I mean, having a team is definitely helpful cuz otherwise, I mean, it, it is, it was like data overload, right?

Mm-hmm. There's like too much information and that can be overwhelming. So definitely having like an idea of where you're gonna go before you go is always helpful, you know? Mm-hmm. Making sure you know what you're, what are you looking for, right? Because that will point you in some directions and not in others, right?

Yeah, having, definitely with open source, there's so many different ways you can go that you really need to ask yourself what's your intelligence? What's the intelligence question, right? What's the objective of the research? You always want to narrow your focus because otherwise you will go down rabbit holes and you.

You will get overwhelmed very

Jason: quickly. Yeah, because I, I've, I've said, I think you could spend all day on Facebook and Twitter if you wanted to, and it's Yep. It, it certainly is a lot. So you, you mentioned the [00:31:00] intelligence question. You mentioned the checklist that you have. Is there any advice that you normally give to folks asking about this stuff on how you narrow down your focus?

Ritu: I would say just generally starting with asking yourself what is the purpose of this investigation? Right? What's the purpose of my research? Is it, for example, you're trying to locate an individual, right? Because then I'm, I might not look at certain things that don't, you know, I'm not gonna look at old information.

I mean, that can give you some giveaways, but I might wanna look for if they have any activity on social media that's more current within the last few months. That might indicate where they are. You know, I might not, I might not include all open sources if it's just, Hey, we're just trying to locate the individual.

Is there anything I can see in their social media that points to a location a specific region maybe Are they even in the country? Are they traveling? Any of that? There's a lot of giveaways when it comes to a photo that somebody posts [00:32:00] and sometimes it looks innocent, but sometimes we can see things in the background that give away that they're in a certain country or they're traveling, or, hey, I think we know who they're traveling with.

Mm-hmm. Is

Jason: there a, a set of ENT data that, that you think is most likely overlooked that analysts aren't tapping into, but really should?

Ritu: I think it depends. It depends on somebody's experience. So, you know, of course I can talk about like, oh, these are my five top tools. A lot of people will know the general stuff, like they'll do search engines, but sometimes people limit themselves.

Sometimes somebody will be like, oh, I only Googled it. I just use Google. Well, we use multiple search engines because search engines index different parts of the internet. So that means if I do a search on Bing, I might find information that isn't available on Google. Yes, Google's pretty good. It captures a lot.

That said, does it capture the exact same stuff? No, not necessarily. And sometimes [00:33:00] the order of which it appears is different. Mm-hmm. So for me, like sometimes it's something simple as that where I'm like, Hey, make sure you do use at least two different search engines. And I do have examples of where I found information in Bing and that didn't catch in Google.

And so that's one of those reasons. And I, I do think it, it comes with experience knowing where to look, knowing what your options are. I always ask people like, Hey, what level of osen kind of do you conduct if, you know, are you like intro and everybody's definition of intro advanced, you know, and intermediate might be different too.

So I, I just keep asking questions until I understand it better.

Jason: Yeah, so I guess where, where do you define each one of those? Like how do you define intro intermediate advance?

Ritu: I think it depends on how much open source is part of your regular day-to-day job. Mm-hmm. Is it, you know, and then of course somebody's experience might be also like, I'm like, how much training do you have?

You know you know, are you already a trainer versus are you somebody [00:34:00] who is being trained or taking courses? So I think that matters too. I think the amount of time you put in with this stuff, you learn things that others just won't see. It is definitely a full-time job. I've had people ask like, Hey, can you do this on the side of your desk?

I'm like, yeah, you could, but you might not do the greatest job because open source tools change so quickly. Techniques that we use change so quickly that if you're like, if you're not in the know, if you're not in the kind of the, the quick turnaround, have to have some of these tools stop working or change, well then you're gonna miss things.

Of course, it's a mindset as well, like, I mean, being an analyst at the end of the day is, you know, making sure you're critically thinking about what you're looking at. Those things won't change, right? Those things stay as long as you continue doing that. You know, critically looking at what you're what you found online, what does it mean, mm-hmm.

But yeah, I definitely think depending on how much time somebody spends doing this work, I think that defines it how much just experience they have, because I think with experience [00:35:00] you end up learning so much over the years. Yeah.

Jason: Hmm. Well, how much do you feel when you're dealing with open source that is social media, I guess, versus non-social media?

I'll just, I'll just make it, you know, binary there. , what percentage of it is social media?

Ritu: I would say a very high percentage when it comes to, yeah, when it comes to open source.

Just cuz the amount of information people are sharing nowadays is, is it's expensive. It's not just on one social media. There's new social media coming out. I feel like every so often where we're like, oh, okay, there's a new trending app now and there's a new platform where people can share. I think that's a hu it's a huge percentage of open source.

Is it? Everything? It's definitely not everything. And of course things like asking yourself, so if you have a target group, you know, certain ages might be using certain apps, right? Mm-hmm. TikTok might be for a certain generation versus. [00:36:00] You know back in the day there was like MySpace, you know who used MySpace?

Is that still available? Who would use something like Flicker? Do people still use that today? Maybe it's for a certain group of people that, you know, like to take photos. Yeah. So different apps for different people.

Jason: Is second Life still around? That's showing my age? I'm probably asking that question.

Ritu: I don't, I actually second life. Is that what you just said? Yes. I don't think I even know about that, to be honest.

Jason: So I'm showing my age, age there that, you know, that's,

Ritu: I dunno that one to be honest. I'm like I'm gonna have to look it up. That's funny. Yeah, so definitely I, yeah, there's just so much social media, just people love sharing and oversharing.

I do a privacy talk where I always show people how they compromise themselves online, you know, by sharing too much. So I like to give examples of like, people doing that. Cause I'm like, Hey, this is how, this is what people are doing. This is why you shouldn't do it. Mm-hmm. You know kind of showing them that part of it.

[00:37:00] But yeah. Social media can be a lot of fun at the same time. Yeah.

Jason: I'm, I'm always surprised with people sharing information, especially when they're doing criminal activity. Right now, if it's a situation where they have a friend or a family member posting about them, and you, law enforcement finds it out that way, you know that that stuff certainly happens.

But yeah, I'm o I'm often surprised with just as you've mentioned with the events, like they're doing illegal activity and at the same time posting it for all to see, and it just seems to me that I would've thought that people would've smartened up by now. Yeah, I, you know what,

Ritu: I would think that too, but it is definitely not true because I, you know, people have the need to share, you know, just the way society's become, I think putting their life out there.

Yeah, you would think like a lot of times it might not be them. I mean, there are definitely individuals who will [00:38:00] literally be committ. A criminal act. Mm-hmm. Um, Doing something against the law and then posting it online. I don't know if it's just to get attention, not thinking they'll get caught. But I think a lot of times it's like you don't see, say exactly a criminal act, but you'll see like associations to people mm-hmm.

That you're like, Hey, okay. You know, you can find a lot on social media about a person, you know, their background, their lifestyle. What do they do? What, what motivates them? What influences them you know are they somebody that needs to be on social media every five seconds and you know, or do they need to post when they're working out?

I mean, it gives you a lot of lifestyle information about a person, you know, like they're at the gym every day. They have to take a photo of themselves every single day. Mm-hmm. You know yeah. Yeah. Well, but they're eating three times a day. And all the snacks too. But yeah, like it's definitely kind of interesting.

How people are. I mean, it varies. Some people are privacy conscious and then there's people that just aren't. Often I find you'll have our main [00:39:00] subject of interest who is privacy conscious, but then that person might have a girlfriend who has a open profile and sharing everything. Mm-hmm. Or we have the main subject and that person's privacy conscious, but his mother or parents or siblings are open.

Mm-hmm. So through these secondary targets, we can often find a lot about the main target.

Jason: I remember at, when I was at Cincinnati Police Department in Ohio, you were talking about 2009 timeframe. You know, social media, they were creating fake accounts, right? Yeah. To then, friend different targets to try to gather information from there.

And there was a bunch of rules there of what they could and couldn't, could not do. Right. Is, is that . Part of what you're doing too. Yeah,

Ritu: So, as well, one thing is, is there's a difference between passive and active osen.

So when I say that is like passive [00:40:00] osen gather collection is like, we're not engaging with people, we're not messaging them, friending them. Active goes into, I mean, it could be things that can be looked as, as a undercover operation. So that's different cuz if we're engaging people that that is no longer passive.

However, we do create research accounts for what we do. So regardless, I mean, I do passive osen and I have various fake accounts on social media. Because I don't want my name associated to the investigation, as in I don't want ritu Gill to be investigating all the targets, you know, because if somebody Googled my name, they'd be like, oh, they already know I'm an online investigator.

They already know I'm an ENT person.

All

Jason: right. So I. We have that call in segment of don't be that Alice. So I do wanna get into a little bit of that. So in terms of your advice on when it comes to assent, what, what you [00:41:00] advise things that analysts should not be

Ritu: doing?

Okay. So this one's big for open source and a lot of Osen analysts would understand this. Don't be the analyst who thinks a social media post will be there if they go back tomorrow. So what that means is if something's relevant and they see it, save it right away. Because so often I'll have analysts be like, oh, I didn't save it in time and that person deleted it.

So yeah, we don't be that analyst that doesn't sees something and doesn't savor it during that time and hopes tomorrow it'll be there. Cuz often it won't be there.

Jason: Yeah. Now is that just. The, the technique to do a screenshot, make sure you get the website, make sure you get the time. Is that, is that usually the course of action?

Ritu: Yeah, it depends. It depends again, like who you work for. Do you go, do you have to go ta testify in court? Making sure things are at a court standard, is it really important? And that would include things like within your [00:42:00] capture, there's different ways to capture online material, but making sure you have the date and time noted.

Do you have the URL captured? Do you have everything in that ca document, or sorry, that post including comments, expanded, you know, all, all that matters. If it's something that may not be going to court, the threshold will be definitely different. That said, yeah, it'll vary from case to case. Hmm.

Jason: Another one that we talked about a little bit yesterday and the prep call is stuff that I, I. I seem to hear, I'm not sure how much analysts are doing it, but it seems like when they're talking about open source, it seems like that's their entire focus.

Like they're only doing open source information and they're not combining what they're learning in open source with maybe human intelligence or maybe what they could get in closed systems. And their database is back at the department, whatever they have access to. It seems like [00:43:00] once they're in that mode of open source, they get a little bit of tunnel vision and that's where they'll stay and not bounce to the different sources that they have access to.

Ritu: Correct. You definitely wanna have an open mind when it comes to doing the research because at the end of the day, I think with open source it is a little bit sexy, so I think people tend to focus. On just the open source when there could be so much more. So you don't wanna get that to tunnel vision. You wanna have the open mind where you can not only do the open source, but keep your mind open to other sources of information, especially as an analyst.

If you have other databases, you know, you don't wanna misinformation that's literally sit in front of you, that could be utilized to gain more information or insight into the, the subject of interest. Okay,

Jason: so let's talk about your website. Now, as I've mentioned in your intro, you have open source intelligent techniques [00:44:00] and just to, what made you create a website for this?

Ritu: That's that's something I started when I decided, I was like, Hey, I wanna create, I wanna do something on the side in addition to my regular job. Still, I love open source. So I decided, I'm like, well, that's how I started out. I created a website, osen techniques.com. I called my business Osen Techniques and just registering the website was step one.

And then starting to add some op open source resources on there. That's what I use it for. It's mostly just to put, like, sometimes I'll do a talk and I'll add a link on my website of all the different resources I shared in that talk that type of thing. So I use it as that. It's also a way people can get ahold of me.

So if you, if somebody looks, they're like, oh, okay. They can email me at my proton mail. They can reach out to me, you know, they can connect with me on Twitter, that type of thing. I do have some, I have different sections. I change it up. It's not something I update on the regular I post mostly on Twitter, but my website is a [00:45:00] definitely a source of information.

I have some stuff that I've created over the years on my website. And an example of that is this is, I guess a small contribution, I'm gonna call it. I created a Google map called the Metro Vancouver shootings map. So it's just a link of, so in, in Metro Vancouver, we have an issue with gangs, and there's been a lot of shootings in the last few years.

So in 2021, I started tracking all these shootings that were related to the gang conflict. And I put it on a map, and that's one of the things that you'll see on my website just cause it, it's a really neat visual to see what, how it's progressed, how many shootings are related to the gang conflict, all this information.

Was gathered from open sources. So news media articles primarily where we know it's gang, it's linked to the gang. And how I sorted it was put it on a map and in red you'll see those are public places, like public shootings. So [00:46:00] again, a risk to public safety, which is a huge concern. And then the ones in black are residential related shootings.

So somebody was shot in a driveway or in their house. Just to, just to show the difference between how many we have public versus residential. That's, anyways, that's something that you'll find on my website. And I do have it's in a tiny url. It's tiny url.com/lmd gc.

Jason: Okay, good. Yeah, I did see that.

I didn't know, I didn't get the full story on that, but that I, I like that aspect. That's a good example of what you can learn just through o osen . And yeah, so you mentioned newspaper and it's funny, when I think back of the history of open source, your intelligence, The newspaper was used to be a pretty big resource.

And now certainly what's online is, is available, but I, I do know that a lot of newspapers and trying to [00:47:00] gather revenue streams will ha, you know, make you pay for certain content. There is. Do you, do you subscribe to newspapers or any kind of magazines?

Ritu: I would say generally, I mean, I don't subscribe to anything specifically mm-hmm.

But depends what I'm looking at. Like, I, like, you know, there's certain journalists that they specialize in, in, in the gang conflict in Metro Vancouver. So I might follow that person who will give me a lot of insights on what's happening. Mm-hmm. So that kind of thing. I, I will follow individuals over paper sometimes, but yeah, that, that's a huge source of information.

Even some of the, the, the briefings, right, that come out from the police directly, right? Mm-hmm. They're media releases. Those are important. I have, I'm signed up for some of those, which is always interesting cuz it keeps me in the know of what's happening. Things like our integrated homicide unit, well, they put out media releases every time.

You [00:48:00] know, somebody who's found dead and if it's gang related, I, I wanna, I wanna flag that. Right. So I keep, I keep close tabs on that, but a lot of it through Twitter, to be honest. Right. And it

Jason: seems to me, , just seems like with everything that we deal with as analysts, , it's free to a point, but then of course people are going with, with ENT being as popular was, you know, there's more and more vendors that are, have a product for law enforcement that will help them with their osint investigations.

What's your thought on those? I mean, certainly from your, from your side of things, it sounds like you've mostly gone the, the free. Route, but as since Osen has become more popular, you're certainly going to have more and more paid tools that are gonna be available to

Ritu: analysts. Yep. I mean, definitely like , I try to show people the free resources because I [00:49:00] know there's different people doing this work.

So, and not everybody, not every organization agency has the money or will pay for some of the tools out there. That said, I always say to people, there's certain software that as a osen analyst might not be relevant to what they do. Cuz you have to ask, like if it's like something to do with geolocation or social media monitoring and you're like, oh well we don't even do that, then why would you spend all that money getting that software?

Like, I've seen that where they're like, oh, we'll get this software. And I'm like, keep in mind you, do you understand what it's ex like pulling information from? It's only from open sources, so it's stuff you could find yourself. But you know, it will take you longer. But if you're not even doing that type of work, then what's the point of getting that software?

Like, think about why you would need it. There's some software that I would, you know, vouch for. I'd say like, Hey, that's a really good software for, say social network analysis. The, I would say for that one, I mean, it's not free, it's, you have to pay for it, but Shadow Dragon is a great ENT tool, I'm gonna say for ENT [00:50:00] or sorry for social network analysis.

And it can graph out a bunch of different connections. It uses mal, tego those things. But yeah, I definitely, like, I generally try to show people free methods, but if people specifically ask like, Hey, what software do you pay? Well then I say like, well what is it for? Are you looking for capturing software?

You know, is it something like Hunch Lee? Hunch Lee is a software specifically for online investigations. It was created by individual named Justin Seitz, who's a Canadian. And this, this tool, I have to give that plug, but yeah, Justin is a, is a great guy and. Yeah, it's not an expensive software, but it's something a lot of law enforcement agencies in the US and in Canada use.

But yeah, and, and I would tell people, you know, it's not, it's, it doesn't cost a lot, so it's worth it for what it does. .

Jason: . So for those that are looking to get into either a unit or a position that is the full-time [00:51:00] Osen analysts, what advice do you have for

Ritu: them? So, number one, I would say get involved.

I mentioned this earlier, but you have to be a self-starter. So you have to start with researching about osen. I would say get, get behind the keyboard and start learning how other people are using open source intelligence. There's a lot of information out there just on the, on the internet. Get on twen Twitter and search for the keywords osen and see the amount of posts that you'll see out there.

There's an individual on Twitter named Sector 0 3 5, who every Monday releases a blog. Post called week a week in ent. So what he has here is some amazing tips and resources mentioned every week. So new information, things that you might not known of. You can go back into the archive and, and dig up the, you know, the first one that came out.

I'm not sure what number we're on, but he's he's published a bunch. I think that, that is a great resource to learn more about osen. Okay,

Jason: good. And then do [00:52:00] you have any speaking engagements coming up or training coming up on osen?

Ritu: I have, I do, I do a lot of public talks. I am doing one for, I believe it's Mac Dev Yvr in Vancouver. In person. It's gonna be about online privacy and that's gonna be in May. Otherwise there is a new ENT course offered by sans, which is, the course is called SEC 4 97 and it's brand new, and there's a new, new author named Matt Edmondson, who's a great guy and great author who teaches the course.

I'd mentioned that right now because that, that course has a lot to offer. There's a lot of information, a lot of good

Jason: takeaways from it. Alright, good. And to the listeners, we've obviously talked about various topics here, dealing with osen today, and Retu has mentioned different websites. We'll make sure that we get all those links to those [00:53:00] websites in the show notes including.

Three twos so they can catch her there. And she's a great follow as well. And so I highly recommend that you reach out and follow her on the various sites. Alright, three, two. Then before we get to personal interest one question I'd like to ask my guest is return on investment and stuff that may be not important today, but will be five years ago.

So folks, analysts can study it today and it'll have a pretty good return on investments, say five years from now.

Ritu: I would say I would say definitely things like staying up to date with new technology and trends things like networking, right? Definitely those are things that, you know, these are gonna continue to be important.

Staying engaged with people that's so important for the field. Even things like, you know, getting, getting some courses on critical thinking and analysis. That will only help you be a better analyst as the time goes on. [00:54:00] All right, good.

Jason: And let's move on to personal interest then. And you have taken the time to hone your skills in lock picking.

Ritu: Yes. So I definitely wanna do some. Non ENT work. So one of the things I got into was lock picking that was introduced at a security conference called BSides. So besides Seattle and besides San Fran were the ones I went to last year, lock picking is a lot of fun. Just a little hobby, but they had little lock picking villages, which I attended.

It keeps people off screens for a while and you just work with your hands. And it is fun when you actually open a lock and you're like, oh, okay. Like, learning the different ways learning. Some people are so good at it, but that was a lot of fun. So that's some one little hobby that I have. Just to stay off the screens cuz I spend so much time on computers.

Jason: Yeah. You dealt with combination locks too, right?

Ritu: Yep. Combination locks as well. Yeah. Like they had a fun little Lock picking village at [00:55:00] besides San Fran last June. You know, if you open the combo lock, you get a little tree inside. But again, like it was just, you know, trial and error and then learning for other people.

Like, I'm like, how are you doing this? Like, how is, how are, how do we do this? It's not like I have any background in lock picking. Yeah. Just doing it for fun. But that was always like, those little wins are pretty exciting. Cause I'm like, wow, I just opened a combo lock and I'm like, I have zero, like, you know, experience from the.

But yeah, they make it fun. You know, you get a little treat if you actually are able to break into it.

Jason: Yeah. So, yeah, my wife had a combination lock that she forgot the combination to. And she, just to wrap this up nicely, she Googled it. You found a couple YouTube videos, found a couple other open source websites gives little tips and tricks on how, what to listen for and what to feel for in terms of the combination lock.

And she was able to figure out how to, what the code was and how to open it. So I was, I was pretty impressed

Ritu: [00:56:00] by that. Y it's amazing how much information is online on the videos, you know, starting for beginners, it's like telling you what to do, what to look for, and then just, you know, if you have spare.

Around the house. Start with those, right. Start with the basics and move from there. I mean, you can always go to some of these BSides security conferences are all around the world, so attend a local one, and usually they have a lock picking village, but the ones I have at least have and that's, that's where you, you go, you take it for a spin.

Jason: Yeah. Sounds fun. All right. Re two. Our last segment to the show is Words to the World. And this is where I give the guests the last word. You can promote any idea that you wish. What are your

Ritu: words to the world? I don't know if I have one for this Words to the World. I don't really, I don't even know what to say for that one, so I'm not really sure I'm gonna go with that, if that's okay.

Okay.

Jason: Well, I leave every guest with, you've given me just enough to talk bad about you later. Okay. But I do appreciate you being on the show too. [00:57:00] Thank you. Okay. Thanks so much. And you be safe.

Ritu: Thank you. Thanks so much for having me.

Mindy: Thank you for making it To the end of another episode of Analysts Talk with Jason Elder. You can show your support by sharing this in other episodes found on our website@www.elliotpodcasts.com. If you have a topic you would like us to cover or have a suggestion for our next guest, please send us an email at elliot eight podcast gmail.com.

Till next time, analysts, keep talking.