Forensic OSINT Web Capture Software with Ritu Gill

[00:00:00] **Mindy:** Welcome to Analyst 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 be that analyst and join us as we define the law enforcement analysis profession one episode at a time.

[00:00:17] **Jason:** Thank you for joining me. I hope many aspects of your life are progressing. My name is Jason Elder, and today our guest is a returning guest. We welcome back Ritu Gill, who is the co founder of a new browser extension tool for screen captures called Forensic OSINT. , as you remember, she has a consulting business, OSINT Techniques.

[00:00:43] **Jason:** So please welcome Ritu Gill. Ritu, how we doing?

[00:00:48] **Ritu:** Hey Jason, thanks so much. I'm happy to be here and thanks for having me back on.

[00:00:54] **Jason:** Excellent. Yes, it's a returning guests. We have exciting tool to [00:01:00] talk about today and just give a general overview of this tool and we're going to go through the it.

[00:01:07] **Jason:** All the details of this tool and to let people know why they should have this tool as as analysts. So let's just start there of what this tool is. And then we'll get into all the details.

[00:01:20] **Ritu:** Excellent. So what is forensic OSINT? It is a Chrome extension that essentially will transform the way it.

[00:01:28] **Ritu:** OSINT investigators collect online evidence, so it not only allows someone to make screen captures, but it also will download all the source code and images of your screen captures, and at the same time it is hashing all the files. So it will include the metadata and this is really important because that includes things like your date and time stamps, which are really important if you have to take any of this information to court.

[00:01:56] **Ritu:** The tool was created. Because there was a gap in [00:02:00] the OSINT community for user friendly tools that work the way we need to when we're conducting our investigations.

[00:02:07] **Jason:** Alright, so you saw the need, , but, to put together a browser extension tool seems like A lot of work. I don't have any idea how to do this. How did this idea come to be?

[00:02:18] **Ritu:** So this is definitely a team effort. Rob Marriott is the other co founder of Forensic OSINT. It was his idea and he approached me and we both saw the value in building this tool up.

[00:02:30] **Ritu:** So we started with approach of, Full page web capture, one screen at a time. So, the reason why we did this is because it puts the user in charge of what they want to collect and when they want to collect it.

[00:02:44] **Jason:** Right, so, so then, I mean you said it was a, then this is just for Chrome, the browser Chrome.

[00:02:52] **Jason:** Just for the audience we'll have links in the show notes of all the information you need is. So there's a [00:03:00] video on how to download the extension and how to get the extension. And so there will be more information in the show notes for you to click on to get a visual of what we're talking about here.

[00:03:11] **Jason:** So, let's, get into a little bit more about what it does. So it captures the screen. That's always good. You said you talked about the, the timestamp and that's good for evidence and to make sure that you recorded exactly the time and what you saw on the screen.

[00:03:30] **Jason:** So what are, some of the other features?

[00:03:32] **Ritu:** So, Exactly like you said. So the bare bones it makes screen captures of online content. We talked about the hash values. We talked about metadata, but it also includes a built in knowledge base system for real time advice. Other data insights as you're conducting your online research.

[00:03:51] **Ritu:** So you could be on Facebook and you might be doing some research, but you can click on quick tips or general information about that website that will [00:04:00] help you. Maybe save certain things or look in certain places to gather more information it's it is designed to be intuitive and user friendly.

[00:04:10] **Ritu:** And that's the idea. It's not complicated. You don't need to take a week course trying to learn the tool. We wanted to make it as user friendly as possible. Other features that we have built into the app is a case management system. Because that helps investigators keep organized. So when they're making those captures, it will go into the case management system.

[00:04:33] **Ritu:** And from there, they can make their downloads and download their PDF reports. One of the recent features that we've included is something where you go on to, say, a YouTube video. And we've already had the feature of video downloads. We've had that from the start for certain sites like YouTube or TikTok.

[00:04:51] **Ritu:** But with this new feature it will expand all the comments and make the capture of those comments as well. So that's [00:05:00] quite helpful for users.

[00:05:02] **Jason:** Okay, so then with the case management, I can envision you're able to work on Multiple cases at once and save them off. So it's you can have different folders in there and be doing work for a little bit and then switch over maybe to another case or two and then dump those screenshots over over in the other folder

[00:05:27] **Ritu:** exactly.

[00:05:28] **Ritu:** So before you create any captures, you can create a case. You'll have a case name or a file number, and when you do that, all the captures will be put into that folder in the case management system, so it makes it really easy to organize your information, and you can jump to different investigations, different research projects because you'll have a name or a file number for each.

[00:05:51] **Jason:** Yeah, I also, you also mentioned there the different social media sites. I like that little tips one where if you're on X or [00:06:00] formerly known as Twitter or you're on Snapchat or you're on Facebook, there's like, oh, you might want to look here for this feature on this particular site because they're all just a little bit different and they house a slightly different information, right?

[00:06:14] **Ritu:** Exactly. And so another example of that might be if you're looking at an Instagram profile, if you click on quick tips, you'll see we have various different tips in there, but one of them is if you wanted to know the date this account was created, it will tell you the instructions of where to go on Instagram to find this account.

[00:06:34] **Ritu:** Find the month and the year, because that can be really helpful for certain files. Especially if sometimes, you know, if it seems like a fake account or something really recent, or it doesn't fit in the bigger picture of what you're investigating. Those are the types of tips you'll find.

[00:06:48] **Jason:** Okay. So you being a OSINT analyst, as a co founder, you built this as if.

[00:06:56] **Jason:** Like you're working your own case like you've struggled with . [00:07:00] I'm working a case. I need to capture everything. I can't find the tool out there that will do everything that I that I wanted to do. But now you've set this tool up with, with Rob to say, okay, from beginning to end, this is, this is how I easily can capture all this information as I'm doing my OSINT research.

[00:07:23] **Jason:** This flows nicely in terms of the techniques that you, teach and part of your consulting with OSINT.

[00:07:30] **Ritu:** That's right. It really. It has an intuitive interface, and the idea is to put the control in the, with the user, with the analyst the person working on the file, you decide what you need to save.

[00:07:44] **Ritu:** Because at the end of the day, you will speak to those screen captures, but if you're on a website and you're like, okay, I have these four tabs, I need to save each page, webpage. Well, you can go in and save each one of those webpages, [00:08:00] and the output is very easy to download, and it it is very straightforward in terms of how to do that.

[00:08:08] **Jason:** , There's a couple different versions here. There's the free version that anybody can download as long as they're using Chrome, and then there's a professional version that gives you a couple extras there. Let's go into the professional version now on how it differs from the free version and some of the extras you get for the cost.

[00:08:31] **Ritu:** Yeah, so the free version is, is available. Anyone can go to forensicocent. com and, and download the extension or just go straight to the Chrome web store and you can download it there. The free version is the non, it's a non forensic version, so it doesn't provide The hash values, but it gives you the idea of what the tool does.

[00:08:54] **Ritu:** So you can scroll and make a capture. You have a limited number of pages you [00:09:00] can do. You can download videos with a free version. There's other other things such as key value extractions. That's essentially like if you go to a Facebook page of an individual and you click on key value extractions, .

[00:09:13] **Ritu:** With a click of a button it will give you the Facebook user ID of that individual So that's also part of the free version So with a professional version though, you get the hashes of all the files you can capture full pages over 100 pages social media, for example, you also can download all the images from websites You can download pretty much up to I believe 50 video downloads It includes a lot of different features as well And you'll see if you go to the website and you click on pricing.

[00:09:49] **Ritu:** You're going to see on a really Clean table in terms of what you get for free on the free side, what you get on the professional side, and there's actually one other version. It's called professional elite, [00:10:00] and you're going to see what that how that differs as well. So it's outlined really clearly, and you'll see the value in.

[00:10:09] **Ritu:** What you get in the different payment structures.

[00:10:12] **Jason:** So you mentioned hash version and for those that are less than this and may not necessarily be Up to speed with all that's 0 cent. Can you just describe that a little bit?

[00:10:24] **Ritu:** . So, with hashing files, the best way to describe that is, if I have to go to court, and I have to provide these, these screen captures, they have a hash value, which means that I have not, edited anything.

[00:10:40] **Ritu:** It is true to what was captured at the time and including all the metadata and all that. So this is why hash values are so important. They're at that forensic level. And an example is here in Canada, there's been cases where it's said that you need to use forensic grade software to show that [00:11:00] investigators didn't alter.

[00:11:01] **Ritu:** Any of the content in between the time they captured it and when they came to court, and this is one way of doing it. That's what hash values provide.

[00:11:10] **Jason:** Okay, and then you also mentioned forensic versus non forensic. Can you just describe the differences between those two concepts?

[00:11:18] **Ritu:** Yeah,

[00:11:19] **Ritu:** so, with the two different versions, if you use the free version, you get non forensic. What that means is that it doesn't hash the files. And with the forensic version, you We'll hash all the files you'll get all that information included in your screen captures

[00:11:35] **Jason:** So it's talking a little bit about the pricing for the professional version.

[00:11:42] **Jason:** It's 55 a month or if you want to pay yearly. The yearly for the professional is 4 97 and the professional elite is 1097, and then there is the one time fee for [00:12:00] professional, which is 1,247, whereas the professional elite is 2,749. Just a point of clarification on the one time, so if you do the one time, does that mean you have the tool?

[00:12:15] **Jason:** Forever. Any updates that you come to the tool, you'll have access to. There's no additional costs after that one time.

[00:12:23] **Ritu:** Exactly. Yeah, that is the difference. So there are, and we have users who have purchased this because they saw the value and they use it at that level. And which is nice. I mean, that one time.

[00:12:35] **Ritu:** payment and you get to have all the updates for a lifetime.

[00:12:40] **Jason:** Yeah. And so you are from Canada. And so is is somebody from the States or maybe another country as they're purchasing, maybe it's an agency purchase. This will follow the guidelines that have been set forth for government agencies to purchase this.

[00:12:58] **Ritu:** Yeah, I think [00:13:00] really when it comes down to documentation, if someone has that need when it comes to online content this is a tool where you'll see professionals using it. We are a startup, so as we evolve, we're seeing more users, we're seeing really active OSINT people using this tool, which has been awesome.

[00:13:20] **Ritu:** It hasn't been established in case law yet, but we're hoping we'll get some Something good in that in the near future. So hopefully we'll, we'll see something like that.

[00:13:30] **Jason:** Yeah, I guess how unique is this tool? Is there, are you obviously created it because you were frustrated that there was nothing else out there?

[00:13:39] **Jason:** Is there anything that really compares to what this tool does?

[00:13:43] **Ritu:** Yeah, there are comparable tools out there specifically even for OSINT work. That said, they work a little different they will make captures in a different way. Sometimes the output can look a little different as well. There's several different [00:14:00] companies that do this.

[00:14:00] **Ritu:** If someone sees value in the way we're doing it and who's behind this tool, how we built it from our experience as well, then They might want to try it out. However, if you have different needs, and I think it's always worth exploring different things to see what works best for someone.

[00:14:16] **Jason:** Yeah, I mean, and I think that's the nice thing about your tool is that there is a free version so folks can try it out. And use it, and especially if they're doing this OSINT research, which seems everybody is in the law enforcement analysis world,, then this is definitely something that will make their lives easier to be able to document, because you can get yourself in a bind pretty quickly, , it's easy to click, and it's easy to jump all over to different websites, have a 20 tabs open on a browser and really then try to go back and like, okay, how do I document what I just [00:15:00] did?

[00:15:00] **Jason:** And this tool definitely seems like it helps analysts out by keeping all that together and organized and able to capture it fairly easily.

[00:15:10] **Ritu:** Yeah, that's, that's exactly it, Jason. And it is easy to go down that rabbit hole and have all these different tabs open. Documentation is so important, and so that's what Forensic OSINT offers among other things.

[00:15:24] **Ritu:** I tell people, regardless of the tool you're using, you have to be able to explain what you did, you know, how you did it, when you did it, and Our tool does help with that because it does capture those dates and times with, within the captures. We have a free version, try it out, see if it works for you, see if you see value in it.

[00:15:44] **Ritu:** And you can easily just go download the tool from the link to the Chrome store is on forensicocin. com.

[00:15:51] **Jason:** I should have asked this earlier. , because this is on Chrome and it's an extension, that must lend an advantage for the tool being a Chrome [00:16:00] extension.

[00:16:00] **Ritu:** Yeah, it's a, right now it's a Chrome extension only.

[00:16:04] **Ritu:** That said, it, it's, Will evolve over time. We've had the questions where people are saying, Hey, will you be on Firefox? Will you go to other browsers? We don't know exactly what that will look like, but that is something where you're keeping in mind. And right now our focus is on the Chrome browser Chrome extension.

[00:16:24] **Ritu:** There's a lot of different Chrome extensions, actually that are quite helpful for OSINT that are specifically to the Chrome browser.

[00:16:31] **Jason:** OK, so you did mention what's next.

[00:16:34] **Jason:** So let's let's go there. So what do you envision is next for the tool? Because I when I hear someone that created a software created a tool that I always think of what Sean Bair told me when he created his first tool is like if you like Your tool in development, you waited too long to release it because you should always hate the version that you have because there's [00:17:00] always stuff to do.

[00:17:01] **Jason:** There's always the what's next. There's always ways to make it better before the launch. So now that we're past this, you got it launched. What are some things that you're working on to improve the tool?

[00:17:12] **Ritu:** Yeah, as I mentioned, we are continuing to evolve the tool and. Adding more features, and we're using feedback from the OSINT community to see what's next.

[00:17:23] **Ritu:** We do have our own ideas in terms of what is next, but we also are very open to hearing what the community has to say. So this is something that we are constantly looking at. We get lots of different messages every day in LinkedIn or on LinkedIn. Or on our other social media profiles but again, if people have great ideas, send us an email or , reach out to us on socials.

[00:17:50] **Jason:** Yeah. So it looks like as, again, I took your advice and jumped on , the page where it goes through the different [00:18:00] versions. It's going into with the ability of capturing comments on YouTube, for instance. And being able to take notes , on some of this stuff.

[00:18:10] **Jason:** So not only do you have the case management side of it where you can capture the different screenshots, keep them organized with all your different cases, but you can also take some notes in there as well as to, make sure that you fully understand them. Why you captured it cuz i could just think i didn't don't get into osin research all that much but i just know how my brain works i'll get in there i might capture it perfectly and then and then days weeks months go by and i'm being like why did i capture that or what was i gonna use that for so i can imagine that that note writing.

[00:18:51] **Jason:** Feature is going to be very useful.

[00:18:53] **Ritu:** Yeah, it's really helpful being able to just, reference why exactly what you're saying reference why you made that capture [00:19:00] or how it's related back to the objective. So Intel question. Again, these. Little features built within to the app are meant to just help the analysts as they go, and we will continue to look for other ways that we can support investigators and researchers and analysts as they do their online research.

[00:19:20] **Jason:** All right, and then right now you have an exclusive limited time offer for those that purchase the Professional Elite. So what does someone get with this special offer?

[00:19:32] **Ritu:** So with this exclusive offer, you'll get a 30 minute call directly with me. So we can talk about pretty much anything OSINT related.

[00:19:44] **Ritu:** You'll also get and this could be an online training. Session with me or a course directly from me as well to do with different OSINT courses, such as introduction to open source intelligence or Instagram for [00:20:00] investigators, or learning about the Wayback Machine and how OSINT people use that.

[00:20:05] **Ritu:** So that is something that we offer right now.

[00:20:08] **Jason:** Yeah. And what, just to remind folks what the Wayback Machine is.

[00:20:11] **Ritu:** So the Wayback Machine is essentially if you. are researching a website, and maybe you want to see how it's evolved over time or maybe if something's been deleted off of a website, you can plug it into the Wayback Machine to see what it looked like previously if it's been captured there.

[00:20:29] **Ritu:** So it's kind of Also known as the Internet Archive. But it's a great tool for researchers. It's I've used it for so many years now, and it's always been part of my top five tools for OSINT.

[00:20:42] **Jason:** Okay. Now does that, does your extension feed into that archive?

[00:20:47] **Ritu:** So when you say feed in, I would say it can be used on the Internet Archive.

[00:20:51] **Ritu:** It can be used on various different sites, pretty much if it's on the Internet. You're, you can go to the Forensic OSINT [00:21:00] extension and you can make a screen capture right from there. You can even capture a full page in situations if you need to do that.

[00:21:07] **Jason:** And then, I guess from there, how would it be part of the archive for the

[00:21:13] **Ritu:** So that's okay.

[00:21:14] **Ritu:** So that's kind of a different question. So I would say if you to answer your question, you can go to the Internet Archive or Wayback Machine and you can ask it to archive things for you. The option is called save, save page. So you request it to save something. You can do that from just the OSINT research level.

[00:21:33] **Jason:** Okay. All right. No, okay. That makes sense. I just wanted to make sure I, you know, some people might, might want to participate in that way back and some people might not. So that's why I was answering the question of making sure that what your tool did and how it interacted if it, if it did. .

[00:21:49] **Jason:** Okay. So I guess as you've gotten feedback, you talked about different users getting feedback. , is there anyone in particular that sticks out? They're like, Oh, that's not what this [00:22:00] tool does. Or maybe that's what they're asking for is the moon type of thing. So just to any interesting feedback that you've gotten so far.

[00:22:09] **Ritu:** We're always open to everyone's feedback and we have had All sorts of feedback over the last number of months But really, like, I don't take things personally that way We're trying to create something that's going to be excellent for the community, And being open to some of that criticism is, I think, really important as well, because If we can take it and it we see the value in that if it's constructive feedback, then let's See what we can do with it, you know, see how we can evolve our our product And make it better for everyone using it.

[00:22:44] **Ritu:** And when I say that like i'm also a user So for me, I need to make sure it's the best tool for me as well. So there's incentive there from OSINT investigators mindset.

[00:22:57] **Jason:** Very good. And so, as, as [00:23:00] mentioned, there's this tool and Ritu does a lot of consulting. She's got articles up on the website. She's got OSINT definitions.

[00:23:09] **Jason:** She's got other utilities. She, she writes a newsletter. Basically, she eats, sleeps, and breathes this, this OSINT stuff. So again check out the tool. And help out a fellow analyst with a startup company, which is fantastic. Ritu, as we finish up here, , I'll give you the last word, like I normally do with my guests, is there anything else that you want to add?

[00:23:34] **Ritu:** I would just say, remember, I mean, this is definitely aligned with the topic today, but remembering to document your findings. Because it's often that one time you don't do it and then you go back and a post is removed or a website's down. This is why documentation and OSINT is so important.

[00:23:51] **Ritu:** This is why screen captures matter. And as always, I tell people, stay curious when you're doing your online research. [00:24:00] And, you know, continue to be open to learning and connecting with the larger OSINT community online.

[00:24:08] **Jason:** All right. Very good. Well, it was awesome to hear back from you. Thank you for your time today.

[00:24:14] **Jason:** Good luck with the startup and you be safe.

[00:24:17] **Ritu:** Thank you so much, Jason. It's been my pleasure being on your show again.

[00:24:21] **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 and other episodes found on our website at www.

[00:24:29] **Mindy:** leapodcasts. 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 leapodcasts at gmail. com. Till next time, analysts, keep talking.