LEVEL UP

CASE STUDY

MATHIAS FUCHS SANS INSTRUCTOR

What made you get into digital forensics?

I started my InfoSec career as a penetration tester but that kind of work got less demanding over time. Even though you could break into companies in different ways every time, usually very basic attacks would be enough, so that was somewhat repetitive.

In DFIR (Digital Forensics and Incident Response) neither the investigator nor the customer sets the pace. In initial phases, the adversary is in control. It's the investigator's job to get and stay in control. I never learned so much in my life as in some of the investigations I was running.

Suddenly I was confronted with the best APT (Advanced Persistent Threat) groups known today and saw that what we teach in our classes is capable of detecting even those adversaries. That's just awesome.

According to you, what makes a great digital forensicator? What makes them tick?

A great digital forensicator never stops learning. One of the things I keep on repeating when I teach FOR508 is that whatever artefact you are looking at, the vendor of the OS didn't put it there to support forensics (aside from logs maybe). So, a really great forensicator needs to identify the artefacts that support his case, maybe even write a tool to extract them – that can be a very creative process at times.

To become and stay top-notch, a forensicator is very well connected with peers and loves to share new ideas, techniques and tactics.

> **"A digital forensicator needs a large dose of social competency to steer the breached organisation in the right direction."**

What unexpected traits should a digital forensicator have?

Management capabilities and social competency. Managing your team is only half the story; the most complex topic is managing the customer.

Typically, victims of big breaches are in headless chicken mode at first. A top-notch IR lead can help to apply a more structured approach to deal with the issue; that's mandatory to establish a workable environment. I've seen engagements turn from good to bad when the management of the victim decided to start the blaming game.

So, to summarise, as well as exceptional technical skills a digital forensicator needs a large dose of social competency to steer the breached organisation in the right direction.

CONTINUE?

LEVEL UP

How would you determine if someone's got what it takes to be a good forensicator in your team?
I throw them into the cold waters and see if they swim. I might not throw the biggest breach with the most demanding customer at them, but if I consider someone a potential future lead forensicator, nothing below an APT case will do.

That looks like a risky approach at first, but I make sure that I always stay in control of the case. That way I can steer the engagement lead out of deep waters when I have to. So far, that approach has never failed me.

What brings you the most satisfaction out of a day's work?
There are two things that can really make my day. Number one is when I find a trace of the attacker that allows us to crack the case. Number two is when I see one of my team members finding that golden artefact.

> **"We get new challenges every day and we even get paid to solve them. How could I not love that?"**

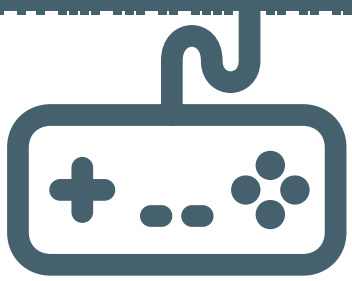
People are paying tons of money to solve riddles in escape rooms all over the world. We get new challenges every day and we even get paid to solve them. How could I not love that?

If you could wake up tomorrow with a new cyber security skill, what would it be and why?
I would love to wake up and have all the skills needed to be a cryptographer. As forensicators, we frequently work on malware. Currently, when the adversary encrypts the malware or malware configuration too well it just takes me an awful lot of time to understand what it can do and how it operates.

I admit that most of the time you don't need to decrypt everything but just leverage small mistakes the adversary has made. Still, understanding cryptography and mastering it are two different things. If you really mastered it, I believe the way you investigate malware would change.

What is the best advice you could give to an aspiring digital forensicator?
Learn how to hunt the attacker, hunt and then learn how to hunt better, go back to step 1. Always stay curious and accept that, in any investigation, at first you are only reacting.

Success in incident response for me is defined by how long it takes you as an investigator to switch from reaction only mode to active hunting mode that puts you ahead of the attacker. Only after you understand the full extent and mechanics of the breach will you be able to suggest a remediation plan.



Contact SANS
Email: emea@sans.org
Tel: +44 20 3384 3470
Address: SANS EMEA,
PO Box 124, Swansea, SA 9BB, UK
www.sans.org/level-up