LEVEL UP

CASE STUDY

JASON JORDAAN SANS INSTRUCTOR

What made you get into digital forensics?

I had always loved computers and science, and loved solving problems. I was and still am a nerd and proud of it. I joined the police after I left school with dreams of becoming a detective, and I achieved that goal, becoming a detective dealing with fraud and white-collar crimes. I never stopped being interested in computers and technology and, as the resident geek, I began looking at computers as a potential source of evidence in the cases I worked.

This was really at the beginning when digital forensics was born, but I immediately fell in love with the possibilities. I could embrace my love for computers and technology, for solving problems, and it could help me catch bad guys and see justice done. So, I suppose you could say that I came to digital forensics right in the beginning stages of the discipline.

Now over 20 years later, digital forensics is my over-riding passion and is an integral part of who I am today. For me digital forensics is not a job, it is not something I do, it is now simply who I am.

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

I think there are a few things that help make a great digital forensicator. The first is a good problem-solving mind, coupled with logical and scientific aptitude. It's not about just being able to solve problems, you must actually love solving problems and get excited the more complex the problem is. The second is a real attention to detail, as it is often the small, seemingly insignificant things that can make or break a case. The third is a strong sense of ethics and having the courage to do the right thing...always. The fourth is a willingness to work hard and irregular hours. You need to be flexible and willing to work as long or hard as it takes to get the job done. Bad guys do not keep office hours, and neither do we.

> **"If you are not willing to adapt and change your plans at a moment's notice because of the actions of a bad guy, then forensics is not for you."**

If you are not willing to adapt and change your plans at a moment's notice because of the actions of a bad guy, then forensics is not for you. Lastly, and most importantly, you must be passionate about digital forensics and love learning, because this is one of the fields where you need to be self-directed and willing to constantly learn. These I feel are some of the core characteristics that allow someone to become a great digital forensicator.

What unexpected traits should a digital forensicator have?

There are a few that come to mind. A core trait is the ability to communicate clearly and easily, and the ability to educate others about what you do. I remember a really smart technical guy showing interest in digital forensics, but he stated that he didn't like working with people or talking in public. You need to be a people person in many respects (not an extravert, before anyone asks), because digital evidence and crime go hand in hand and you need to deal with perpetrators and victims; these are people, not machines. Technical skills are just simply not enough.

CONTINUE?

Another trait that is a huge advantage is good intuition. Now I am not talking about having a sixth sense or anything like that, but the ability to notice that something is irregular or out of place, or just doesn't quite seem right. You would be surprised how often these intuitive insights can resolve a case.

There is one trait however that many people in this field do not talk about, and that is being mentally strong and resilient. Dealing with crime and the evidence of crimes grind you down over time, and you are exposed to the darkest sides of human nature. If you are not mentally strong, digital forensics could break you.

How would you determine if someone's got what it takes to be a good forensicator in your team?
I get a lot of people who want to join my team. The first thing I ask is which digital forensic blogs they read, or who they follow on Twitter, or what videos they watch on YouTube. The simple fact of the matter is that if they don't do one or more of these things, then they are not really serious about digital forensics, as far as I am concerned, and they don't even get considered for my team.

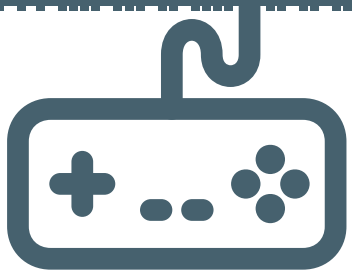
> **"The evidence that I find can help to convict criminals and allow justice to be done."**

The next step is to give them a created forensic image that we use, and I ask them to go away and conduct a forensic examination of the image, analyse it and then come back to me with their findings. All I tell them is the allegations in the case, then they are on their own. That weeds out the majority. If they can manage to work through the case on their own and show appropriate resourcefulness and an ability to identify core issues in the case through their own research, then they are the type of person I am looking for.

What brings you the most satisfaction out of a day's work?
There are two things that gives me the most satisfaction out of a day's work. The first is the intellectual satisfaction of solving a complex problem and finding answers that have people stumped. That eureka moment when you have solved the problem is one of the most amazing feelings for me. The second thing is the satisfaction that comes from making a difference. Generally, people use my skills when something has gone wrong, and the work that I do helps them find resolution, but when it comes to some of the crimes that I help to investigate, the evidence that I find can help to convict criminals and allow justice to be done. That is a sense of great satisfaction for me.

If you could wake up tomorrow with a new cyber security skill, what would it be and why?
That is a really difficult question to answer because technology is constantly changing. When I look at some of the new developments in the intersection between the physical and cyber world, I think an area in which we will be getting digital evidence in the future will be in autonomous systems, such as drones, vehicles and robotics. If I could wake up tomorrow with a new cyber security skill, I think for me it would be an in-depth understanding of these types of systems at an engineering and programming level. But I am positive that the day after I would need to learn or know something new again anyway.

What is the best advice you could give to an aspiring digital forensicator?
Stay hungry. Be hungry to learn. Be hungry to solve problems. Always want to know and do more. Don't give up, even when it becomes hard.



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