BECOMING A DF PROFESSIONAL

So, You Want To Be A Digital Forensics Professional! Do You Have What It Takes?

by Rob Lee

/ ENTRY

Many who are just starting out routinely ask about how to start a successful career in digital forensics. These individuals range from completely inexperienced to individuals who have 15 years experience in the information security profession and are looking for a fresh job. Regardless of your background, starting out with new skills may seem intimidating. Here are some thoughts on how to prepare you to take the plunge into digital forensics.

/ WHY IS BECOMING A DIGITAL FORENSICS EXPERT CHALLENGING?

Science is usually based on that for each science that certain rules will exist that do not change over time. DNA can help match identity. Gravity will not change. Water molecules can be a liquid, solid, or a gas. None of these sciences change on a yearly or even daily basis.

However, with digital forensics, it does change. It radically changes month by month as new technology is released or introduced to the world. Just a simple service pack update to a machine could change everything that you used to know about it. The forensic artifacts could and have completely changed as a result. You can never assume that what works today to solve cases will still work a month from now. In addition, the amount of data being produced yearly is growing fast. It is growing faster than we can keep up with. How can we expect to be able to analyze it all?

For digital forensics, the science is constantly changing and the data potentially used in our analysis is growing exponentially. Digital Forensics is a very challenging field to remain an expert in. So where should you begin if you decide to become an expert in digital forensics.

/ DO YOU HAVE A PASSION FOR DIGITAL FORENSICS? DO YOU HAVE A CAPACITY TO LEARN?

There are two factors that I personally look for when I'm talking to an individual who is just starting out. The first is a passion for computer forensics and incident response. The second one is a very large capacity to learn. This individual realizes that everything is consistently changing and that they're always seeking opportunities to educate themselves. These individuals are never truly satisfied. They are always chomping at the bit to get that additional experience so they are moving forward.

Formal education is great and should be sought if possible. However, in the computer forensics world, there is more unknown than is known. As a result, regardless of background or education, the best in the digital forensics field are experts who jump right in when they encounter something that is new that they have not seen before.

> ***THE FIRST IS A PASSION FOR COMPUTER FORENSICS AND INCIDENT RESPONSE. THE SECOND ONE IS A VERY LARGE CAPACITY TO LEARN***

/ DO YOU HAVE A DESIRE TO BE AN EXPERT?

The individuals I have seen succeed in any career are those who crave to become an expert in their jobs. Not only do they show this in their professional life, I routinely witness that

they have this desire in their out-of-work lives as well. For example, if an individual decides that this summer they will finally learn how to play golf, they would dedicate the time required to not only learning it quickly, but also achieving a level of mastery. By the end of the summer they are not competing with the pros, but usually they are playing "bogey" golf and consistently shooting under a 100. This is a huge accomplishment in that little time frame.

This is not random luck. Usually this individual has these types of moments littered through their life. It isn't that they are talented. They are just tenacious and their desire to learn is so great it overcomes the usual point where most people might give up.

During interviews, I seek these individuals out through conversations not involving technology. I can usually get the individual to discuss the year where she learned to snowboard in a season. Or where the individual had to learn basic French because he liked a foreign exchange student. Typically these individuals will be successful at anything they choose to do.

The hard part here is that this is a personality trait, not a skill. This is a trait I happen to seek when I am looking to hire.

SINCE 90% OF THE SYSTEMS WE ARE INVESTIGATING ARE WINDOWS-BASED, EVERYONE IN THE FIELD KIND OF HAS TO HAVE THAT CORE

It just happens to be a good sign of future success.

/ DO YOU HAVE THE RIGHT BACKGROUND?

What skills and experience and skills do you need? I would definitely recommend that someone should become an expert at the Microsoft Windows operating system family. Windows operating systems are extremely complex and challenging to analyze despite their ease of use for the end user. Since 90% of the systems we are investigating are Windows-based, everyone in the field kind of has to have that core. Understanding completely where evidence exists on a windows operating system is crucial. You should also know how to find evidence if your automated tool fails as well. Knowledge of both the file system and operating system is crucial to your future success as a digital forensics professional. The core area is currently Windows, so I would start with the mastery there.

Once you have mastered the core areas in one operating system, I usually recommend that individuals develop a specialty niche area to become an expert in. There is a great need for experts in mobile device forensics. Mobile device forensics would therefore be a very good niche area for obvious future demand.

/ MORE INFO

http://blogs.sans.org/computer-forensics/

http://computer-forensics.sans.org

Handbook of Digital Forensics and Investigation by Eoghan Casey

Windows Forensic Analysis DVD Toolkit, Second Edition by Harlan A. Carvey

/ GET CERTIFIED IN A REPUTABLE DIGITAL FORENSIC CERTIFICATION

The debate over whether to get certified is over. Most career fields have a gateway test that will enable you to practice your chosen profession. Regardless of the color of certification, I personally feel that in order for the profession to be recognized on equal footing with other fields, we need a gateway test. The certifications serve as a way for individuals to independently show their skills meet the minimum standards through testing. Simply taking and passing a test does not make you an expert, but it helps establish you are credentialed with the basic foundations of the profession. For our peer professions to take us seriously, certification and testing of personnel should take place. As a result, become certified in one of the popular certifications.

/ WHERE WOULD SOMEONE WITH FORENSIC SKILLS FIND THE BEST OPPORTUNITIES TODAY?

It comes down to location. Look where your large government centers are found, for example, Washington D.C., London, Singapore, or Canberra. These locations should probably be the first on your list of locations that have the highest concentration of digital forensic specialists. For large corporate forensic jobs, look to business capitols and trading centers such as Hong Kong, Dubai, Chicago and New York City. Smaller cities would also be possibilities if the individual concentrates on working for local law firms, local law enforcement, or remote fortune 500 corporate locations. To get your career starting faster though, I would consider moving to one of the larger cities or government centers.

/ WANT TO KNOW WHERE THE GROWTH OPPORTUNITIES ARE FOR DIGITAL FORENSICS?

From my perspective, there are two growth areas for professionals in digital forensics. First, commercial firms are realizing that they need internal digital forensic and incident response experts to help with ongoing and eventual incidents. Everyone is at risk these days. These companies are seeing that they need incident responders and a dedicated computer forensic capability for eDiscovery and operational forensics associated with security operations. They agree they need to grow their own teams.

The second area where I see the largest future growth in digital forensics is in e-discovery. E-discovery has traditionally focused on email and documents retrieval and production with a sprinkle of digital forensics. I see that sprinkle growing to a flood for digital forensics. We are starting to see e-discovery litigation requesting records of chat sessions, social networks, and twitter. E-Discovery lawyers have been handicapped with the thought that many case-changing digital forensic artifacts are deemed too difficult or costly to produce. However, it is theoretically possible with digital forensics today to ask specific questions that could alter the outcome of important cases. For example, a USB device was discovered outside the main door that contained stolen data on it. You could scan the enterprise network easily to identify which workstations that specific USB device had been plugged into and possibly show specifically who placed the stolen files on the device. With e-discovery and digital forensics moving closer together, more cases will be won by those utilizing a technical digital forensics team than those who use the simple document retrieval e-discovery methods currently being used.

In the end, I always tell individuals that in order to succeed in digital forensics you must have.

- Passion for digital forensics
- Capacity to learn
- Desire to become an expert

Even if an individual does not have the complete background yet, I would usually take the risk at giving an individual a chance to prove themselves if they can clearly show that they have the first three traits. For more specific advice for your situation, please feel free to contact me (see our 360 page). /

FOR LARGE CORPORATE FORENSIC JOBS, LOOK TO BUSINESS CAPITOLS AND TRADING CENTERS SUCH AS HONG KONG, DUBAI, CHICAGO AND NEW YORK CITY

/ AUTHOR BIO

Rob Lee is a Director for MANDIANT (http://www.mandiant.com/), a leading provider of information security consulting services and software to Fortune 500 organizations and the U.S. Government. Rob is also the Curriculum Lead for Digital Forensic Training at the SANS Institute (http://forensics.sans.org/). Rob has more than 13 years experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served in the U.S. Air Force as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on Information Operations. Later, he was a member of the Air Force Office of Special Investigations where he conducted computer crime investigations, incident response, and computer forensics. Prior to joining MANDIANT, he directly worked with a variety of government agencies in the law enforcement, Dept. of Defense, and intelligence communities where he was the technical lead for a vulnerability discovery and exploit development team, lead for a cyber forensics branch, and led a computer forensic and security software development team. Rob also coauthored the bestselling book, Know Your Enemy, 2nd Edition. Rob earned his MBA from Georgetown University in Washington D.C. Finally, Rob was awarded the "Digital Forensic Examiner of the Year" from the Forensic 4Cast 2009 Awards.