Digital forensic science

Technology

USB flash drive

Science in itself is amazing. It has grown to greater aspects in a quick span of time. This is also the case with forensic science. In a company like Triton Corporation, many technological bits are accessible to employees. As the forensic manager, if I happen to learn of a case of wrong use of technology, I will handle the issue with necessary precautions as well as include vital confidentiality. Therefore, if at all the scenario was that of an employee allegedly found to be looking at inappropriate images of children engaged in sex acts using a USB drive, and in which case the International Affairs Director had confiscated the drive, I would approach the IAD professionally as well as emotionally based. I would understand that this is a worker who probably has been close to the IAD, maybe had coffee once or twice, and have been close to each other. Again, I would take into account that the employee in question has signed the waiver of rights. This in one way or another could mean the person is innocent. I would thus approach the director and kindly explain my course of action and why exactly it would be paramount to hand over the drive.

Case example taken as a flash drive, there are quite a number of ways of having a copy of the drive. The simplest would be copying the files to a computer just the usual way where one inserts the flash drive and views the content on the computer screen then he can either cut and paste or copy and paste. This, however, would work only if the drive is not bootable and does not contain multiple partitions. With this new and well diverse technology, the likelihood of the drive being a bootable one and containing multiple partitions is high. In cases like this one, one is expected to a have

software that can image and analyses the drive. Such software tools are accessible. They include FTK Imager, which images, and analyses content on drives such as flash drives, and other hard drives. ProDiscover Basic; this is another software that quite works like the previous one. However, this is more detailed as it also enables recording of the investigation process. DSi USB Write Blocker. This software is quite efficient in preventing write access to the USB. The write access reduces the legibility of the investigation and thus the software here is very important. These are some of the methods one would use so as to copy a USB drive.

Prodiscover Basic

I would use ProDiscover Basic as my software. It is an easy to use tool. It comes with beneficial qualities as highlighted above. It ensures that the evidence is not contaminated and also offers one a chance to document the findings if ever a court hearing is necessary. It would be particularly beneficial in that it can access last viewed images from the USB drive. It connects to the internet easily, if the supposed pictures were from an online source, I would definitely be able to know which source and at what time it was accessed. ProDiscover would be the key software in my investigation process.

Together with ProDiscovery, I would attach DSi USB Write Blocker. This would be vital to the investigation as it would aid in affirming the trust of the result. It would be fundamental to have concise evidence. Evidence should not be questionable when brought up in a case. Therefore, I would make sure any mistake is done away with. This software will be able to prevent access

to write, one of the most common mistakes during Digital forensic investigation.

With this use of the proper software and putting in enough of my time and concentration, I would be able to prove beyond doubt whether or not the USB drive contained the pictures, and if so, where were they obtained and when.