NTS405 – Incident Response; Breaking Down Forensic Investigations

Jackson Nestler

University of Advancing Technology

NTS405 – Incident Response; Breaking Down Forensic Investigations

Objective

Given the forensic scenario "Case of the Stolen Exams," determine what (if any) problems there are with the investigation. These problems should lead to potential issues in getting a conviction.

Failure to Catalog, Document, and Securely Inspect Evidence

At 0:48, the investigator takes the USB out of its packaging and plugs it directly into his computer. There was no documentation as to where his "friend" got the USB (chain of custody compromised), no record that the USB existed other than the eBay listing, and no gloves to maintain any potential fingerprint analysis, despite it being unlikely.

Missing a Write Blocker

The investigator makes no note of having a software write blocker, and no hardware write blocker is present. Now the evidence can be heavily challenged in court and will likely lead to the suspect going free.

Documenting Evidence on a Personal Device

He uses his cell phone's camera to note down the serial number for the USB device. No process was written down for which program he's using to inspect the serial number and corresponding information. A serious lack of documentation overall. The photo being taken on a cell phone makes chain of custody even more difficult to maintain: the investigator won't turn in his cell phone when he's done taking the photo: who's to say he doesn't go home and manipulate it in Photoshop?

Improperly Inspecting a Suspect's Device

He walks up to Crispin's desktop and immediately begins his inspection. He even lured Crispin away by faking a conference: HR doesn't seem remotely involved, Crispin hasn't been notified that he's a suspect, and his computer was randomly selected to undergo this testing.

The actor opens the CD/DVD bay and inserts a CD that doesn't have any verification behind it: we have no way to know that the tools he's running are legitimate and haven't been modified since their distribution from source. By inserting the CD, he's modified the "natural state" of the computer by introducing his own content. Ideally, he'd acquire this system with the help of the legal department and HR, image it, then perform any forensics on the image.

Lying to Coworker

The investigator states that Crispin asked him to find files on the desktop: an outright lie and once again, the investigator is acting without any help from HR or the legal department.

Improperly Inspecting a Suspect's Browser

This is a recurring theme, but the investigator is taking very liberal steps to check whether Crispin was the one that had the USB drive plugged in. He's combed through the entire browser history without any probable cause: Crispin could sue the company for the inspector's actions.

Assigning Blame Without Proper Evidence

The investigator sees the exam answers in the "recent documents" menu, but previously stated that Crispin works on the content development team: Crispin has a totally legitimate reason to be viewing those answers and could get out of this situation easily. There's nothing shown that 100% indicates Crispin created the eBay account and was the one that listed it. It's a

shared device that Crispin obviously leaves unlocked, so Joe in accounting could have used Crispin's computer to post the listing.

"If I Had More Time"

The investigator claims that "if he had more time, {he} would image it and take it away." He already contaminated the evidence and found his "answer" through illegitimate means. He should have taken the machine for imaging after speaking to HR and the legal department first. His case has no legs to stand on.

Conclusion

This investigation is wildly inappropriate. There are so many problems with how the investigator handled the situation that leaves both him and the company wide open to lawsuits. Suggesting that any evidence collected could be used is completely out of left field and goes against the fundamentals of computer forensics.