System forensics

Science

System forensics is the process of systematically examining computer media as well as network components, software, and memory for evidence. System forensics involves collecting, preserving, analyzing, and documenting evidence to reconstruct user actively. Appropriately collected evidence Is often presented In court to solve criminal cases and prosecute criminals. 2. How hastechnologyimproved the way criminal investigators perform their job?

Technology improved the way criminal investigators perform their jobs by making it easier to track things, there is different types of software out there today to help them with these issues, and make the Jobs easier, when you have different technology to help. 3. Why would a company report or not report a compromise case? The reason a company may or may not report a compromise because If It's not in their favor and they may report It If It's In their favor and vice versa. They wouldn't want to look Incompetent. 4. Who Is In charge of labeling and securing sensitive Information?

The one In charge of labeling and securing sensitive information is the forensic specialist. 5. What is the Daubers standard? The Daubers Standard provides a rule of evidence regarding the admissibility of expert witnesses' testimony during united States federal legal proceedings. 6. Why would someone use a hex editor in a forensic investigation? The reason someone would use a hex editor in a forensic Investigation is if the suspect has deleted files and has overwritten them on his or her hard disk, you can always use a hex editor to view any data stored In (or deleted from) both files and disk sectors.

A hex editor allows you to peek at the physical contents stored on a disk, regardless of he boundaries of files, directories, or partitions. 7. What is the largest known data loss incident to date? The largest known data loss incident to date Adobe systems, Inc - 10-3-2013, 8. What group runs tallboys? Open Security Foundation runs tallboys. 9. On the website Tallboys. Org, of the largest 20 incidents, how many of them were computer hacks as opposed to other Issues like stolen laptops and lost drives? 1% of the Incidents were computer hacks as opposed to the other Issues. 10. What built-Len Windows tool Is used to manage the Encrypted File System (FEES)? The certificates is was is used to manage the FEES.. . What is the presumption of innocence? All people accused off crime are legally presumed to be innocent until they are convicted, either in a trial or as a result of pleading guilty. This presumption means not only that the prosecutor must convince the Jury of the defendant's guilt, but also that the defendant need not say or do anything in his own defense.

If the prosecutor can't convince the Jury that the defendant is guilty, the defendant goes free. 2. The presumption of innocence, coupled with the fact that the prosecutor must prove the defendant's guilt beyond a reasonable doubt, makes it difficult for the overspent to put innocent people behind bars. 3. What is hearsay and provide an example when Computer evidence can be considered hearsay? " Hearsay' refers to statements made outside of court of law an example of Computer evidence that is considered hearsay is 4.

What is system integrity? System integrity is the state of a system where it is performing its intended functions without being degraded or impaired by

changes or disruptions in its internal or external environments 5. What skills are required by an expert witness? The skills required by an expert witness are: A background in law, law enforcement, or investigation. A membership in professional associations of computer forensic examiners, formal training, and certification. A thorough knowledge of the subject matter and tools.

Investigators must understand the kind of potential evidence they sought and analyzed and understand the tools they used to gather and preserve evidence. They should be accurate, truthful and impartial. 6. Locate and read the opinion Daubers v. Merrill DOD Pharmaceuticals. What was the case about? The Daubers v. Merrill DOD Pharmaceuticals was about two children ho had been born with birth defects and their parents sue Merrill DOD Pharmaceuticals Inc, claiming that the drug Benedictine caused the birth defects. 7. What was the outcome of the case?

The district court granted summary Judgment for Merrill DOD, and Daubers and Schuler appealed to the Ninth Circuit. 8. What previous Supreme Court ruling was superseded by the Federal Rules of Evidence as the standard for admitting expert scientific testimony? The previous Supreme Court ruling was superseded by the Federal Rules of Evidence as the standard for admitting expert scientific testimony was the Fryer's " general acceptance" Daubers puts theresponsibilityof the admissibility of evidence by placing the Judge in the role of " gatekeeper".