Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 19 of the official CISSP study guide. Here are the top things that you need to know from this chapter on investigations and ethics.

Know the definition of computer crime. Computer crime is a crime or violation of a law or regulation that is directed against or directly involves a computer. Be able to list and explain the seven categories of computer crime. Computer crimes are grouped into seven categories military and intelligence attack, business attack, financial attack, terrorist attack, grudge attack, thrill attack and hacktivist attack. Be able to explain the motive of each type of attack.

Know the importance of collecting evidence. As soon as you discover an incident, you must begin to collect evidence and as much information as possible about the incident. The evidence can be used in a subsequent legal action or in finding the identity of the attacker. Evidence can also assist you in determining the extent of the damage.

Understand the e-discovery process. Organizations that believe they will be the target of a lawsuit have a duty to preserve digital evidence in a process known as electronic discovery or e-discovery. The e-discovery process includes information governance, identification, preservation, collection, processing, review, analysis, production and presentation activities.

Know how to investigate intrusions and how to gather sufficient artifacts from the equipment, software and data. You must have possession of equipment, software or data to analyze it and use it as evidence. You must acquire the evidence without modifying it or allowing anyone else to modify it.

Know the basic alternatives for confiscating evidence and when each one is appropriate. First, the person who owns the evidence could voluntarily surrender it. Second, a subpoena can be used to compel the subject to surrender the evidence. Third, a law enforcement officer performing a legally permissible duty may seize visible evidence that the officer has probable cause to believe is associated with criminal activity. Fourth, a search warrant is most useful when you need to confiscate evidence without giving the subject an opportunity to alter it. Fifth, a law enforcement officer may collect evidence when exigent circumstances exist.

Know the importance of retaining investigatory data, because you will discover some incidents after they have occurred, you will lose valuable evidence unless you ensure that critical log files are retained for a reasonable period of time. You can retain log files and system status information either in place or in archives.

Know the basic requirements for evidence to be admissible in a court of law. To be admissible, evidence must be relevant to a fact at issue in the case. The fact must be material to the case and the evidence must be competent or legally collected.

Explain the various types of evidence that may be used in a criminal or civil trial. Real evidence consists of actual objects that can be brought into the courtroom. Documentary evidence consists of written documents that provide insight into the facts. Testimonial evidence consists of verbal or written statements made by witnesses.

Understand the importance of ethics to security personnel. Security practitioners are granted a very high level of authority and responsibility to execute their job functions. The potential for abuse exists and without a strict code of personal behavior, security practitioners could be regarded as having unchecked power. Adherence to a code of ethics helps ensure that such power is not abused. Security professionals must subscribe to both their own organization's code of ethics, as well as the ISC2 Code of Ethics.

Know the ISC2 Code of Ethics and RFC 1087 Ethics and the internet. All CISSP candidates should be familiar with the entire ISC2 Code of Ethics, because they must sign an agreement that they will adhere to it. In addition, be familiar with the basic statements of RFC 1087. Those are the study essentials that you'll need to know for chapter 19, investigations and ethics.