General Discussion on Forensics in CISSP.

Terms and Concepts.

Session 1 9/26/2020 Classroom-1

NOTES

A little bit about me.

I joined Certification Station in July. Passed my CISSP at the end of August. I started discussing various topics and then decided to start doing these sessions every Saturday. Timings differ, sometimes I do it in the mornings and sometimes in the evenings. So please keep an eye on the Announcement Channel.

For Notes, you can go to the Classroom-1 Pinned Messages or you can also go to

www.icsbits.com/go/notes

Types of Rules and Types of Investigations.

Criminal Law	Criminal Investigation
Civil Law	Civil Investigation
Administrative Law	Agency Investigations
Private Regulations (Not a Law)	Private Investigators
Company Policies (Not a Law)	Administrative Investigation

Table 1

We are going to look at the different investigations and which will then require you to collect evidence. This will define what is called as Computer forensics, which is our topic for today. So before we define Computer Forensics, I think it important to define these different investigations.

So from Table 1 here, if an individual or a group or a company would violate, which is break or fail to comply with a rule of law such as Criminal Law, then there would be a Criminal Investigation. Similarly the rest of the corresponding investigations. Now there are a couple of things to note about this table. I created this, so this is not an official table. However, look at the third column and the fifth column.

Why is this distinction and difference between the types of law and the investigation types? Let us first define these laws really quickly. As I said, this is more of a Domain 1 discussion.

Criminal law is the body of law that relates to crime. Crime is an unlawful act punishable by a state or other authorities. Think of these as severe forms of acts. Murders, robbery, assaults etc.

Hence we will need Criminal Investigation to be conducted by State or Other Authorities such as FBI, Police etc.

Civil Law deals with rules and regulations between two parties, it is often personal and comes into picture when it is against a person or an organization or a business. You might be familiar with Judge Judy, Judge Rinder etc, they are arbitrators who oversee civil cases. You are hiring

a lawyer for a car accident who then assigns personal investigators to gather information. This is considered civil investigation.

Administrative Law deals with the body of law or rule of law that regulates government agencies. Administrative agencies are empowered by law to investigate various matters that fall under their legal jurisdiction.
Fair Labor and Standard Act, Department of Labor is authorized to investigate.
Computer Fraud and Abuse Act violations are investigated by the Department of Justice.

Private Regulations is when a group of companies or individuals or organizations come together and form rules to a certain aspect of the Industry. PCI DSS, Payment Card Industry Data Security Standards. To investigate a violation of a PCI DSS, there are PCI Forensic Investigators, PFI , another acronym but you do not need to remember for the exam. Is a third party investigator who has been accredited by the PCI.

Company Policies are those terms and agreements between employee and the employer, companies between companies, organizations between service providers and so on, violations of which will get you fired, and depending on the type of violation, it could lead into a civil or criminal lawsuit.
An employee uses his work computer to download some graphic images which are against the usage policy of the IT equipment. The HR department and IT Department investigates and presents the evidence to the management and the employee is fired.

Burden of Proof:
Beyond a reasonable doubt vs Weaker Evidence

Most civil cases do not follow the beyond reasonable doubt standard of proof.They use weaker evidence standards. This results in a not so rigorous investigation and evidence handling requirements.

For criminal cases, they have to meet the beyond a reasonable doubt standard of evidence. The prosecution must demonstrate that the defendant committed the crime by presenting facts from which there are no other logical conclusions. For this reason the criminal investigation must follow a very strict evidence collection and preservation process.

Computer Forensics:
is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

Computers can be considered a ‘scene of a crime’ – for example with hacking or denial of service attacks. They may hold evidence of crimes that happened elsewhere, in the form of emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud or drug trafficking.

There is another very important term

Electronic Discovery (E-Discovery) by EDRM - Electronic Discovery Reference Model.

It is simply a model that describes a standard process for conducting electronic evidence which could be in the form of paper records and electronic records.

- Facilitates the processing of electronic records for disclosure - Formatting, Redacting and Filtering.
- It is iterative process
- You start with terabytes of date but end up with a few kilobytes.

Quickly Define each of these terms.

Information Governance: Information is well organized for future eDiscovery Efforts
Identification: Quickly find the right type of information for litigation.
Preservation: Protect the information from alteration or deletion after identification
Collection: Gathering of ESI to perform more operation such as review, process etc,
Processing: Rough cut to reduce the irrelevant parts
Review: Redacted Copy, filter out information that is relevant but is protected by Attorney-client privilege.
Analysis: Data mining, where you have all these information from various sources and now you are making sense of them.
Production: Correct Format, filing, PDF copies, load them into database,
Presentation: Displaying the information to witnesses , the court and other parties,

Types:

- **Conclusive evidence:** Incontrovertible and irrefutable: you know, the smoking gun.
- **Best evidence:** Original, unaltered evidence, which is preferred by the court over secondary evidence. Read more about this in its upcoming section “Best evidence rule.
- **Direct evidence:** Oral testimony or a written statement based on information gathered through the witness’s five senses (an eyewitness account) that proves or disproves a specific fact or issue.
- **Hearsay evidence:** Hearsay evidence, in a legal forum, is testimony from a witness under oath who is reciting an out-of-court statement, content of which is being offered to prove the truth of the matter asserted. It is inadmissible in court.
- **Corroborative evidence:** Supports or substantiates other evidence presented in a case.

Other Types of evidence:

- **Direct evidence:** Oral testimony or a written statement based on information gathered through the witness’s five senses (an eyewitness account) that proves or disproves a specific fact or issue.
- **Real (or physical) evidence:** Tangible objects from the actual crime, such as the tools or weapons used and any stolen or damaged property. May also include visual or audio surveillance tapes generated during or after the event. Physical evidence from a computer crime is rarely available.
- **Demonstrative evidence:** Used to aid the court’s understanding of a case. Opinions are considered demonstrative evidence and may be either *expert* (based on personal expertise and facts) or *non-expert* (based on facts only). Other examples include models, simulations, charts, and illustrations.
- **Secondary evidence:** A duplicate or copy of evidence, such as a tape backup, screen capture, or photograph.
- **Circumstantial evidence:** Relevant facts that can’t be directly or conclusively connected to other events but about which a reasonable inference can be made.

Chain of Custody:

Chain of custody, in legal contexts, is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:		**Reason Obtained:**	
Case Number:			
Item Number:	**Evidence Type / Manufacturer:**	**Model Number:**	**Serial Number:**
Content Owner / Title:	**Content Description:**		
Content Owner Contact Information:			
Forensic Agent:	**Creation Method:**	**HASH Value:**	**Creation Date/Time:**
Forensic Agent Contact Information:			

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: _____

Page: 1 of _____

Proper chain of custody is able to answer the questions WHO, WHAT, WHEN, WHERE, and HOW?

- Who handled it?
- When did they handle it?
- What did they do with it?
- Where did they handle it?

Resources, Further Reading and Links:

Computer Forensics

https://searchsecurity.techtarget.com/definition/computer-forensics

https://www.forensiccontrol.com/what-is-computer-forensics

e-discovery

https://edrm.net/

Types of Evidence

https://i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/

Chain of Custody

https://www.studynotesandtheory.com/single-post/cissp-law-term-chain-of-custody