**Digital Forensics Notes**

* **Digital forensics** is the branch of forensics that focuses specifically on reconstructing past events, that involved computers, communications, and related products, devices, accessories, and services.
* **Forensic** **science**, or forensics, is the application of any kind of science to legal problems and investigations, and the forensic sciences are the forms of scientific inquiry that have evolved for the purpose of developing legally significant evidence.
* **Digital** **evidence** is data that is stored or transmitted using a digital device and is relevant to a legal investigation.
* **Branches of Digital Forensics-** 
  + **Computer** **forensics** is concerned with preservation and analysis of digital evidence on computers (hard drives).
  + **Network forensics** is concerned with preservation and analysis of digital evidence of network events, such as traffic and logs and is found in network & firewalls.
  + **Mobile** **device** **forensics** is concerned with preservation and analysis of digital evidence on devices such as mobile phones, tablets, and GPS systems.
  + **Malware forensics** is concerned with finding and reverse-engineering malicious code.

**------------------------------------------------------------------------------------------------------------------------------------------**

* **Scientific Method-** To logically deduce what happened and prove your conclusions with appropriate confidence.
  + **Gather information on prior observations and background:** Background knowledge about the case, such as who is suspected of doing what, and the reason the investigation began.
  + **Form a hypothesis:** A candidate investigative hypothesis should be evaluated according to three criteria (Popper 2002)-
    - **Falsifiability:** It must be possible to show, by some feasible test, that the hypothesis is false. If a hypothesis is not falsifiable (a.k.a. refutable), then you cannot make rigorous scientific claims about its accuracy.
    - **Consistency:** The hypothesis must be consistent with all previous observations.
    - **Simplicity:** Other considerations being equal, a simpler hypothesis should be preferred.
  + **Develop predictions:** You predict specific things that you expect to be able to find if your hypothesis is true. For example, if your hypothesis is that “Alice sent Bob confidential information over e-mail,” you might predict that you will find e-mails from Alice that contain confidential information in Bob’s e-mail inbox.
  + **Conduct experiments:** You should conduct experiments and compare their results to your predictions to determine whether they confirm or refute your hypothesis with acceptable confidence.
  + **Draw conclusions and report findings:** You must draw conclusions for use in the wider investigation and generate a formal report.
* **Refutation-** Refutation refers to the process of disproving or challenging the validity or accuracy of evidence or claims presented during an investigation. It involves examining the evidence, methodologies, or arguments put forward by the opposing party and providing counterarguments or alternative explanations to refute their assertions.

**------------------------------------------------------------------------------------------------------------------------------------------**

* **Circumstantial vs. Direct Evidence-** Circumstantial evidence implies that an event occurred, while direct evidence demonstrates that an event occurred. For example, if an eyewitness testifies that he saw the defendant smash a glass case in a jewelry store, snatch up a diamond necklace, and run away, that would be direct evidence. On the other hand, if he testifies that he saw the defendant enter the jewelry store; he soon after heard an alarm ring; and he then he saw the defendant run out, that would be circumstantial evidence.
* **Circumstantial Digital Evidence-** Digital evidence is almost always circumstantial. For example, system logs, browser histories, and saved files can be direct evidence that a particular account on a computer was used to access a specific website but serve only as circumstantial evidence that the computer’s owner accessed the website. However, if an eyewitness testifies that she saw the owner using the computer at the time the website was accessed, that would directly link the owner to the action of viewing the website.
* **Forensic Soundness-** A method is forensically sound if it is rigorously performed according to the best practices of its discipline. Thus, you could consider forensically sound as roughly equivalent to “properly done” or “done according to best practices”.
  + Every interaction with the evidence and every step in the analysis should be rigorously documented.
  + Ensure that the evidence is not damaged or otherwise altered from its original state.
  + The analysis must be objective and unbiased.
* **Chain of Custody-** Chain of custody is the formal documentation of every individual who handled a piece of evidence along with where and when it was exchanged. Use of timelines.
* **Evidence Integrity-** Compromise, changes to files and data tampering. Can be implemented by preserving hash value, copies of original data, and using write blockers.

**------------------------------------------------------------------------------------------------------------------------------------------**

**A picture containing text, font, line

Description automatically generated**

* **Adversarial System-** In an adversarial system, the two sides to the dispute (the plaintiff and defendant in a civil case, or the prosecutor and defense in a criminal trial) a—namely, the injured party and those accused of being responsible for the injuries—present evidence to a third party—namely, a judge or jury— and ask that third party to make a decision about who is responsible for the injury and what kind of compensation is appropriate.
* **Inquisitorial System-** Judges decide what evidence to hear and direct the parties to produce the kinds of evidence that they think is most important. The judge dictates what evidence gets promoted and what experts he or she wants to hear.
* **Consequences of Adversarial System-**
* **The presentation of evidence can be really confusing**.
* **The ‘haves’ come out ahead:** Parties who have the most resources are most likely to win in court.

A picture containing text, screenshot, font, line

Description automatically generated

* **Members of the Courtroom-**
  + **Judge:** Officer responsible for ensuring the fair and impartial administration of justice. The judge interprets and applies the law, makes rulings on procedural matters, and decides the outcome of the case.
  + **Jury:** A group of individuals selected from the community who are responsible for impartially evaluating the evidence and determining the verdict based on the facts presented in court.
  + **Prosecutor:** District attorneys or state attorneys, prosecutors represent the government and are responsible for presenting the case against the defendant. They gather evidence, question witnesses, and argue for the conviction of the accused.
  + **Defense:** Lawyers who represent the defendant and advocate for their rights and interests. Defense attorneys examine the evidence, cross-examine prosecution witnesses, present a defense strategy, and seek to undermine the prosecution's case.
  + **Victim:** Testify in the court and plaintiff for a civil case.
* **Lawyers are in charge of the courtroom, and they run the show.**
* **Plea Bargain-** When defendants accept plea bargains, they basically give up all of their rights to force the prosecutor to prove the case beyond a reasonable doubt. In exchange they get a more lenient sentence and/or less serious charges.

**------------------------------------------------------------------------------------------------------------------------------------------**

* **Judges in Oregon are chosen by non-partisan ballot elections and secondly by appointment.**
* **Jury Selection-**
  + Jury Pools
  + **Voir Dire:** Attorneys for both sides ask them questions, trying to discover whether or not they have some bias that would prevent them from listening to the evidence and evaluating it in a fair and impartial way. (Voir dire is French for “to see, to speak.”)

**------------------------------------------------------------------------------------------------------------------------------------------**

* **4th Amendment-** Components protection against unlawful seizure, probable cause, warrants and unreasonable search and seizure. No warrants shall be issued unless they’re supported by “probable cause.” You have to specify the places where the seizure will take place, and the people or things that you plan to seize.
* **Exceptions for a Warrant-**
  + Consent
  + Exigent Circumstances: It means there’s some good reason why investigators need to proceed right now, quickly, without getting a warrant.
  + Plain View
  + Third Party Doctrine
* A warrant, as we have discussed, requires “probable cause.”
* A subpoena requires “reasonable relevance.” Subpoenas are very common in civil cases as well as criminal cases.
* A 2703(d) order requires “specific and articulable facts showing that there are reasonable grounds to believe that... the records... sought, are relevant and material to an ongoing criminal investigation.”
* Subpoenas are easier to get than warrants. Even lawyers can give a subpoena.
* Subpoenas are applied whenever and on anything as long as there is a case standing.

**------------------------------------------------------------------------------------------------------------------------------------------**

* **Burden of Proof-** Responsibility of a party to present evidence and convince the factfinder of the truth or validity of their claims.
  + Civil Case: General impression and preponderance-
    - Plaintiffs establish that their claims are more likely than not to be true.
  + Criminal Case: Beyond Reasonable doubt-
    - Prosecution makes sure that there is no reasonable doubt in the minds of the factfinder that the defendant committed the alleged crime.
* **Computer Fraud and Abuse Act-** Unauthorized access of protected (government and private parties) computer systems.
  + Unauthorized access as long as they are trying to enforce terms of service.

**------------------------------------------------------------------------------------------------------------------------------------------**

* **Concept of Privacy-** 
  + Right is implied under the 4th Amendment.
  + Reasonable expectation of Privacy.
* **Stored Communication Act-**
  + Protection of Stored Communications
  + Government Access to Stored Communications
  + Search Warrants and Court Orders
  + User Consent and Service Provider Exceptions
* **Stored Communication relates to emails.**
* **One should know what is involved and what is not.**
* **Electronic Communications Privacy Act-**

**A diagram of information flow

Description automatically generated with low confidence**

* **Wiretap vs Pen Register-**
  + Wiretap involves the interception and monitoring of the actual content of electronic communications, while pen register captures metadata associated with the communications.
  + Wiretapping requires a court order or warrant based on probable cause, while pen register surveillance typically requires a lower standard, such as a court order based on relevance or specific statutory authorization.

**------------------------------------------------------------------------------------------------------------------------------------------**

* **Technical Information-**
  + Shellbags are found in NTUser.dat and Usrclass.dat
  + Autopsy is used to find out information about an image disk/ drive.
  + FTK manager is used to carve images and extract information from an image.
  + Shellbag explorer is used to extract information about all operations performed on that system.
  + Registry explorer is used to find information about network logs in a system.