CYBS-3743 Cyberforensics Fundamental: Differences in Criminal and Civil cases

---

*Computer forensics is a profession that deals specifically with evidence, and that means there is some type of court case involved. There are two categories of court cases in the US - **civil** and **criminal**.*

While this is not a course in government law, you still need to be aware of the differences in the two types of cases to give you some general idea about the judicial system. So, let's look at the differences and the impact that your evidence could have.

Let me reiterate - I am NOT a lawyer nor an expert in the judicial system. The concepts provided in this presentation are general and are delivered to provide some insight into the computer forensic profession.

1 - Digital evidence can be found in many common everyday electronic devices.

How a case is brought to court

It is fairly clear how a criminal case begins - **an entity breaks a *statute***, which per dictionary.com, is "an enactment made by a legislature and expressed in a formal document." In a criminal case, the governing legislature body **prosecutes** the law breaker, known as the **defendant**.

There are basically three categories where a computer can be related to a crime :

The computer is used as a target, or "subject", of the crime

- In this category, the computer is typically the property of the victim of the crime, and the forensic process is focused on identifying the ingress point of the intruder and the data that was exfiltrated or corrupted. Some of the most common cases in this genre are identity theft, corporate espionage, corporate sabotage, ransomware and other malware attacks.

The computer is used as an instrument of the crime

- The computer system itself is used to perpetrate a crime. So, the table turns, and now the defendant's computer commonly undergoes forensic analysis to identify and produce digital evidence such as hacking tools, the apps to make/manipulate/display child pornography (and the images as well), malware generators, illegal copyrighted media brokering (jukebox, movie server, digital library), and distribution of fake email (malmail, phishing, scams, etc.).

The computer is incidental to the crime

- In this case, the computer is not essential to the occurrence of the crime, but acts in support of the crime. Here again, most likely it would be a computer associated with the defendant. An example would be a customer list of a trafficker, or a spreadsheet of deals, or perhaps a calendar showing meeting times/places.

A civil case is also known as a lawsuit, and is precipitated by **some type of damage done to an entity that is not necessarily a crime**. Put into common vernacular, "You have done me wrong, and I am going to sue you!" The entity who feels wronged and initiates the lawsuit is called the **plaintiff**, and the alleged wrong-doer is, as also in a criminal case, the **defendant**. The plaintiff and the defendant are also referred to as "litigants," and are both private parties.

*Note : Typically the federal government cannot be sued. However, under certain circumstances (for instance, say you were injured in a car accident when hit by a US mail truck as a possible example) using the Federal Tort Claims Act, a civil case can be brought to court.

A case is generally cited as ***Prosecution / Plaintiff*** **v.** ***Defendant*** however the more specific citation includes more detail such as the court involved and the volume containing the record of the case, and, of course, the date. [For greater detail see How to Read a Legal Citation] The general case citation is the most common reference and is what is used in this class.

Examples of criminal cases involving digital evidence:

STATE of North Carolina v. Michelle Catherine THEER

- Defendant Michelle Catherine Theer was convicted of first-degree murder by aiding and abetting and of conspiracy to commit first-degree murder in the death of her husband, United States Air Force Captain Frank Martin Theer .
- Digital evidence : the State's evidence about computer documents related to body bags, specifically, concerning alleged searches on the website eBay for “body bag disaster pouches” stored in the memory of Defendant's home computer.

U.S. v. TYREE

- Scott Tyree pleaded guilty in 2003 to traveling in interstate commerce for the purpose of engaging in a sexual act with a minor, in violation of 18 U.S.C. § 2423(b), and transporting a minor in interstate commerce with the intent that such minor engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, in violation of 18 U.S.C. § 2251(a).
- Digital evidence: Using information from an online profile found on the victim's computer, digital investigators conducted further forensic examination of the computer and found substantial links to give them probable cause to get an IP address from Yahoo! relating to the suspected user. The IP address was assigned to Verizon and their customer records revealed the customer using this IP address at the time in question as Scott Tyree.

STATE of Kansas v. Dennis RADER

- Dennis Rader, a.k.a. the BTK serial killer convicted of first-degree murder
- Digital evidence : Rader wrote a "manifesto" using Microsoft Word and sent a digital copy on a floppy disk to the police. The metadata in the Word document provided the account name and owner of the software, which was the church where Rader was president of the church congregation.

Examples of civil cases involving digital evidence :

ANZALDUA v. NORTHEAST AMBULANCE FIRE DISTRICT

- Stevon Anzaldua was a paramedic and firefighter with the Northeast Ambulance and Fire Protection District and was terminated for sending emails expressing concerns about the Fire Department and its Chief of "rule-bending" to a newspaper reporter.

LVRC HOLDINGS, LLC v. CHRISTOPHER BREKKA

- LVRC Holdings sued Christopher Brekka, a former employee, for emailing himself sensitive company information and inappropriately accessing the corporate system after he had left the company. The emails containing business data were found, but the access was not apparent.

How evidence is obtained

As with all cases, there can be many interpretations and nuances on how evidence is obtained. But for this class, we are going to stick to the basics (again, this is not a government law course).

In a civil case, evidence can be produced in the Discovery phase of the case via the Request for Production of Things or, more commonly, a **court order**, such as a **subpoena**, can be issued. Typically in the case of digital evidence, a *Cease and Desist* court order is issued as soon as the judge reviews and acknowledges the probable cause as to why the party should immediately stop working with the device. This is to preserve the data as much as possible. (But, in practice, this can be hit or miss, largely depending on how much "heads up" the opposing party had prior to the issuance of the order.)

*Note - As a consultant, I always have the client sign a *Letter of Authorization* as a step in securing the evidence for collection.

Yet obtaining evidence for a criminal case almost always requires a **warrant**, due to the U.S. Constitution **4th Amendment which protects private citizens from unreasonable search and seizure**. The *exclusionary rule* is a principal which essentially says that "evidence collected or analyzed in violation of the U.S. Constitution is inadmissible for criminal prosecution in a court of law."

That being said, however, there are circumstances where a warrant is not needed to obtain evidence for a criminal trial. While there are several obscure tactics/conditions that are tucked away for more gregarious lawyers to utilize [I highly recommend The Law: Illegally Obtained Evidence for an interesting short read], for this class, we shall just look at the typical reasons that would apply (keep in mind, these were primarily constructed to protect an arresting law officer from criminal weapons or contraband):

1. **Exigent Circumstances** : Exigent equates to emergency - this means that there is a possibility of the destruction or harm to a person or evidence in a time-sensitive situation where a warrant could not be attained speedily. From our digital evidence perspective, protecting electronic devices from harm could be something that we might consider in this case.

2. **Search Incident to Lawful Arrest** : This is primarily associated with contraband, and making sure there is no weapon close at hand to the arrested party, as it only applies to searching the person or the radius of the "wingspan" of the person. However, as far as we are concerned, this may involve a small personal electronic such as a PDA or phone.

3. **Consent** : While it may seem like this is simple, this can be difficult if the searched party says they were coerced or if they actually did not have the authority to provide consent to search. A lawful search without a warrant for this exception can only occur if they have consent from a person who has the authority to give it. Probable cause is not required if the consent is knowingly and intelligently given.

4. **Plain View** : Again, this would appear to be obvious, but this can be tricky as it applies to digital evidence. There is significant controversy [Plain View Doctrine in Digital Evidence Cases—A Common Sense Approach] mainly surrounding the fact that digital evidence is binary, and it is the interpretation of the binary code that presents a view, not the data itself. The interpretive display of a picture can certainly be taken into consideration as probable cause to secure a warrant, however.

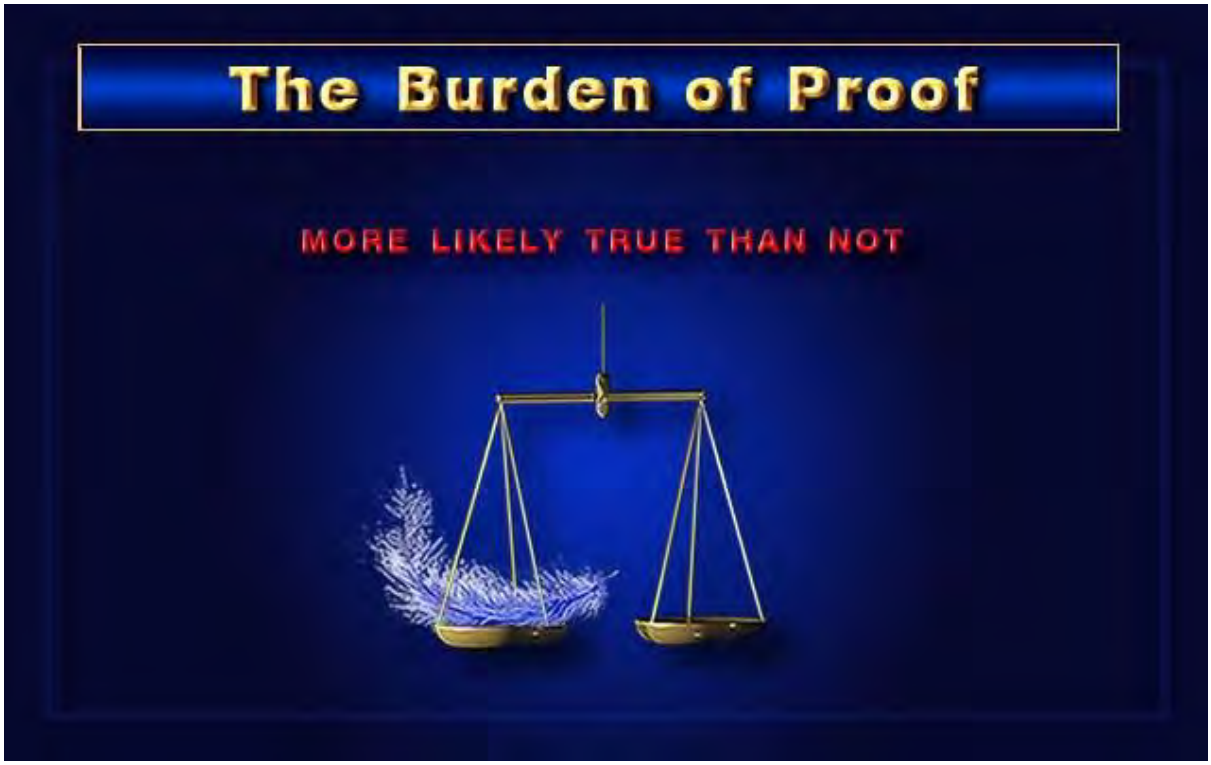
5. **Caretaker Function** : I consider this a "common sense" exception as it applies to lost or abandoned articles. When items are turned into the police, such as a cell phone or wallet, naturally the officer can search the item to try to find the owner. This also applies to abandoned items, such as back packs, briefcases, etc.

6. **Impounded Vehicle** : Very similar to the *Caretaker Function*, a vehicle that has been properly impounded for legitimate reasons, such as a parking violation, can be searched. This makes sense to search it for anything harmful, again similar to *Search Incident to Lawful Arrest*.

7. **Motor Vehicle Exception** : This applies if a vehicle has been detained for a *legitimate* reason (and this is KEY), and the officer has some probable cause to suspect there is criminal evidence in the vehicle (such as contraband, weapons, cell phone, etc.).

If the evidence has not been obtained through a warrant or one of the exceptions, it is not admissible, and any digital evidence derived from the evidence is deemed as "fruit of the poisonous tree," and therefore also not admissible.

Burden of Proof



The burden of proof has many degrees ranging from *Reasonable Indications* (very low) to the most intense, *Beyond Reasonable Doubt*. We have all heard that the defendant is innocent until proven guilty, so it is incumbent on the prosecution/plaintiff to produce evidence to prove their case for judgement.

The burden of proof in a **civil case** for a plaintiff to provide to the court is a **Preponderance of the Evidence**. Simply put, it means that the evidence is more likely to be true than not true - that the evidence is *compelling* in nature. So, presenting your evidence in the most convincing way is paramount to your case.

Now, with **criminal cases**, the standard is raised to the highest degree of scrutiny : **Beyond Reasonable Doubt**. Per the definition from the free dictionary :

"*The standard that must be met by the prosecution's evidence in a criminal prosecution: that no other logical explanation can be derived from the facts except that the defendant committed the crime, thereby overcoming the presumption that a person is innocent until proven guilty.*

If the jurors or judge have no doubt as to the defendant's guilt, or if their only doubts are unreasonable doubts, then the prosecutor has proven the defendant's guilt beyond a reasonable doubt and the defendant should be pronounced guilty.

The term connotes that evidence establishes a particular point to a moral certainty and that it is beyond dispute that any reasonable alternative is possible. It does not mean that no doubt exists as to the accused's guilt, but only that no Reasonable Doubt is possible from the evidence presented."

Consequences

In a **civil litigation**, if the plaintiff wins the case decision, the result is the defendant renders **compensation for the damages**. The compensation can take many various forms, such as money, custody, or a retraction. Financial reparation is the most common.

In a **criminal trial**, **the outcome can be life-altering** for the defendant if found guilty. First, the conviction is on the record of the defendant which can affect future job opportunities, whether the crime was an infraction, misdemeanor, or a felony. In addition, **penalties can include a simple citation, a fine, parole, jail time, or even a death sentence**.

So you can now see why the burden of proof is more strict in a criminal case than in civil litigation.

Summary

In summary, we have this type of structure for digital evidence in a court of law:

How is the case brought to court:

- Civil : plaintiff sues a defendant for reparation of damages
- Criminal : a defendant violates a statute

Who are the parties involved in the case :

- Civil : Plaintiff v. Defendant, where plaintiff and defendant are private parties

- Criminal : Prosecution v. Defendant, where prosecution is the governing body upholding the statute, defendant is a private party

How is evidence attained :

- Civil : court order, subpoena, Letter of Authorization
- Criminal : warrant (due to the 4th Amendment)

What is the burden of proof :

- Civil : a preponderance of the evidence
- Criminal : beyond a reasonable doubt

What are the consequences to the defendant if the case is lost :

- Civil : financial reparation for damages
- Criminal : life-altering outcome including arrest record, parole, fine, jail, death

So, the impact of digital evidence can be significant! The profession of computer/digital forensics can greatly affect the outcome of a case, as can be seen in the examples of case citings in section 1

References and Articles

- **Definition of statute** : http://www.dictionary.com/browse/statute
- **How The Computer Criminals Control Information – Types of Computer Crime** : http://www.datatriage.com/how-the-computer-criminals-control-information-types-of-computer-crime/
- **How to Read a Legal Citation** : http://lawlibguides.byu.edu/c.php?g=315332&p=2106921
- **Civil Cases vs. Criminal Cases - Key Differences** : https://litigation.findlaw.com/filing-a-lawsuit/civil-cases-vs-criminal-cases-key-differences.html
- **The Role of Computer Forensics in Civil Investigations** : https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/computer-forensics-investigations/civil-investigations/
- **Computer-Based Discovery in Federal Civil Litigation** : Kenneth J. Withers, Federal Judicial Center, Washington, DC : http://www.uscourts.gov/sites/default/files/elecdi01_1.pdf
- **How to Sue the Federal Government** : https://www.wikihow.com/Sue-the-Federal-Government
- **Evidence (law) - Wikipedia** : https://en.wikipedia.org/wiki/Evidence_(law)
- **The Law: Illegally Obtained Evidence**: https://www.universalclass.com/articles/law/illegally-obtained-evidence.htm
- **Getting Evidence for Court** : http://www.courts.ca.gov/documents/getting-evidence.pdf
- **Exceptions to the Warrant Requirement** : https://lawshelf.com/courseware/entry/exceptions-to-the-warrant-requirement

- **Investigations: Seven Exceptions to the Search Warrant Rule** : http://lawofficer.com/archive/investigations-seven-exceptions-to-the-search-warrant-rule/
- **The Free Dictionary - Beyond a Reasonable Doubt** : https://legal-dictionary.thefreedictionary.com/beyond+a+reasonable+doubt
- **Burden of proof (law)** : https://en.wikipedia.org/wiki/Burden_of_proof_(law)
- **Civil Court Cases- FindLaw** : https://litigation.findlaw.com/filing-a-lawsuit/civil-court-cases.html
- **Classification of Crimes - FindLaw** : https://criminal.findlaw.com/criminal-law-basics/classifications-of-crimes.html

Glossary items in this lesson :

- **Civil case**
- **Criminal case**
- **Plaintiff**
- **Prosecution**
- **Defendant**
- **Case citation**
- **Court order**
- **Subpoena**
- **Warrant**
- **4th Amendment**
- **Burden of Proof**
- **Preponderance of the Evidence**
- **Beyond a Reasonable Doubt**
- **Compensation**
- **Life-altering penalties**