Unit 3: What is ‘Evidence’ Anyway?

Welcome to Week 3.
This week’s learning continues exploring the topic of evidence gathering in the context of cybercrime. You will explore the difficulties of identifying evidence, and how this has been affected by legislation. Reading will include specific examination of the work of collecting evidence and the problems in connecting a suspect to the alleged crime.

On completion of this unit, you will be able to:

- Explore the implications and limitations concerning evidence.
- Set the study of cyber forensics within the bigger context of law enforcement.
- Identify and evaluate academic arguments.

Reflection:
What is Evidence?
Information that has been stored or transferred in binary format is the sort of data admissible as evidence in legal proceedings. It's not just on paper or in a file cabinet; it may also be located on the memory card of a computer or the internal storage of a mobile device. The term "e-crime," which refers to offenses committed via electronic means, is often used interchangeably with "digital evidence" (Webster, 2022).

As a result of the development of digital evidence forensics, law enforcement organizations are now able to exploit computers in criminal investigations and prosecutions.

Digital evidence refers to information that has been preserved or communicated in binary format and can be used as evidence in a legal action. In addition to other sites, it could be saved on a computer's hard drive or a mobile phone. The terms "e-crime" and "digital evidence" are frequently used interchangeably to refer to crimes committed online. Credit card fraud and child pornography are examples of electronic crime. In contrast, digital evidence is being used to prosecute all types of crimes, not just e-crime. Indicative of a suspect's purpose, presence at the time of a crime, and relationships with other suspects, for example, suspects' e-mails and mobile phone files may provide vital evidence. In 2005, a floppy disk was the crucial piece of evidence that led authorities to the BTK serial murderer, who had evaded capture since 1974 and was responsible for at least ten fatalities (*Digital Evidence and Forensics*, n.d.).

Computer forensics, the process of gathering and evaluating digital evidence, is fast becoming an integral part of the infrastructure of law enforcement agencies. This is being done to combat cybercrime and collect digital evidence pertinent to all crimes. The demand that law enforcement agencies train police to acquire digital evidence and keep up with rapidly evolving technologies, such as computer operating systems, is a challenge for these organizations (*Digital Evidence and Forensics*, n.d.). Let’s have a look at the case how the evidence work and how this case going with the evidence

"Gooda v. Burrows Case (Fraser, 2020) "

Whether or not the accused guy was the driver at the time in question was at issue in the 2020 case of Gooda v. Burrows.

Magistrate Theakston remarked that he knew beyond a reasonable doubt that the man in question was the one operating the vehicle. However, Chief Justice Murrell disagreed and listed the various factors that would have made positive identification extremely impossible.

Some of these factors were:

- There were three people in the car, and the police officer had not been able to tell who was behind the wheel.
- A man, a woman, and a child all left the car at once, with one leaving through the driver's side and two leaving through the back; it was dark outside; the police officer did not write down a description of the male suspect who, he believed, had left by the driver's side door. In any case, the police officer arrested the male suspect and a female suspect. The third person, a man who was also not there, was absent.
- The accused's prints matched those found in the trunk, the woman's prints matched those on the rear-view mirror, and her DNA matched those on the driver's seat controls.
- Footage from a closed-circuit television camera suggests the woman may have been driving for almost forty minutes before it was stopped.

There Are Several Things to Think About When Assessing Identification Evidence.
In his opening statement, the Chief Justice cited many sections of the Evidence Act that declare that identity evidence is "of a character that may be erroneous." Her Honor further mentioned that leading academic text writer on evidence Stephen Odgers, SC, has found a few factors that need to be met when examining identification evidence. The following are examples of such components:

- The witness's level of familiarity with the subject matter
- The witness's identification may not be as reliable if the subject is a member of a different racial group than the witness.
- The circumstances in which the perception was formed, which include the time spent on the task, the focus with which it was viewed, the observer's proximity to the topic, the ambient light, and the observer's emotional state
- The methods used for identification and whether they infer or imply that the person being identified is the perpetrator; and
- The prospect of having one's viewpoint "displaced," as when one is seen or told something that alters their prior frame of reference.

The Chief Justice's Findings
The Chief Justice determined that the police officer had no prior knowledge of the accused, that the accused was of Aboriginal descent and that the police officer was probably of Caucasian descent, that the "period of perception was an instant" and that the officer's focus would have been divided between the three people, and that the lighting was "not ideal."

Although it is unclear whether there was a possibility of relocation, the Chief Justice remarked that it may be relevant because the accused was the only male who was apprehended.

Her Honor concluded that "the combination of the above considerations, but particularly the brevity of the observation of a person of whom [the policeman] had no prior knowledge, and the obvious opportunity for there to be confusion between the two persons who exited the right side of the vehicle (one of whom was [the woman], a person who had very shortly beforehand been the driver of the vehicle) creates a reasonable doubt about the appellant's identification."

Instructions for Handling Digital Evidence (Evidence Handling Procedures) (Boubez, 2021)

1. Make a note of the gadget's current state.
2. Consult with Forensic Professionals
3. Be sure there is a clear line of custody.
4. There should be no changes to the Power Status at this time.
5. Be sure nothing bad happens to the Device.
6. Original data should never be altered in any way.
7. Always keep the device's digital isolation.
8. Prepare everything for long-term archiving.
9. Pay close attention to any deals that include the exchange of proof.
10. Perform regular audits of your evidence management program.

References:

Boubez, I. (2021, April 19). Preserving Digital Evidence, the Right Way: Your 10-Step Guide. Www.realtimenetworks.com. https://www.realtimenetworks.com/blog/preserving-digital-evidence-the-right-way-your-10-step-guide

Digital Evidence and Forensics. (n.d.). National Institute of Justice. Retrieved October 2, 2022, from https://nij.ojp.gov/digital-evidence-and-forensics

Fraser, A. (2020). The Problems with Identification Evidence. Armstrong Legal. https://www.armstronglegal.com.au/criminal-law/evidence/the-problems-with-identification-evidence/

Webster, M. (2022). Definition of EVIDENCE. Www.merriam-Webster.com. https://www.merriam-webster.com/dictionary/evidence#:~:text=1%20%3A%20a%20sign%20which%20shows