Unit 2: Principles of Evidence and Proof

Welcome to Week 2.
This week's learning introduces you to issues concerning proof. The burden of proof in the English legal system usually is usually borne by the prosecution. However, in some cases, the burden of proof might lie on the defendant. The standard of proof also varies depending on the law under which the alleged offence is committed. If the act is criminal, the standard of proof will need to be proved 'beyond reasonable doubt'. If the act comes under civil law, the standard of proof will be 'on the balance of probabilities', that is, 'more likely than not'. There is a whole doctrine of the admissibility of evidence but, in the case of cybercrime, the applicability of the normal rules is more problematic. This is because the evidence might not exist in a physical form. You will have the opportunity to explore further the nature of evidence in the forthcoming weeks. However, during this week, you will concentrate on issues concerning the standard and burden of proof.

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

- Explore the implications and limitations concerning evidence.
- Set the study of cyber forensic within the bigger context of law enforcement.
- Identify and evaluate information to build up a case analysis.

Reflection:
Basically, there are two types of laws which are substantive and adjective law. The evidence is fall under the adjective law (Diffen, 2020).

Evidence: The type of data admissible as evidence in judicial proceedings is information that has been saved or transmitted in binary format. It can also be found on the hard drive of a computer or a mobile phone, among other places. Digital evidence is commonly used interchangeably with the phrase "e-crime," which refers to crimes committed utilizing computers and the internet. **Proof in cyber security** is termed as some type of 100% authentic information, data or POC collected by the concerned committee about an illegal or malicious incident to show it to higher authority (Cohen, & Winters., 2021).

Principles of Evidence:
Here below we are concluding the some of the major principles of evidence which are (Smibert, J., 2014):

- The scope of the evidence should be limited to the question(s) at hand.
- With a few exceptions, hearsay testimony is inadmissible under all circumstances.
- In every case, the best evidence must be provided.
- No evidence is regarded decisive unless it has been cross-examined.

In the private sector, the reaction to cybersecurity incidents (such as a distributed denial of service attack, illegal access to systems, or data breach) involves processes that must be followed to contain the incident, investigate it, and/or remedy it. It is feasible to respond to a cybersecurity incident in one of two ways: quickly recover or collect proof (Cyber Security Coalition, 2015). In the first technique, referred to as "recover swiftly," the

emphasis is not on the storage and/or collection of data, but rather on containing the incident in order to minimize the amount of damage it does. Since its primary focus is on speedy response and recovery, it is possible that crucial data will be disregarded. The second technique entails keeping a watch on the cybersecurity event while focusing on the usage of digital forensic apps to collect evidence and information on the incident's occurrence. The primary objective of the inquiry into the cybersecurity incident has been the collection of evidence, which has hindered the recovery process. Not only can the commercial sector employ these tactics, but so can other sectors. The strategy pursued by organizations in the private sector is dependent on the organizations' priorities.

There are protocols to adhere to when collecting potentially explosive evidence. Volatile evidence should be gathered in the order of its volatility, i.e., the most volatile evidence should be gathered first, followed by the least volatile evidence. According to the Request for Comments (RFC) 3227 document, the following is an example of the order of volatile data (Brezinski and Killalea, 2002). It begins with the most volatile data and progresses to the least volatile data.

- ARP, also known as address resolution protocol,
- Registers, cache routing table,
- Cache
- Process table,
- Kernel statistics,
- RAM temporary file systems
- Disk remote logging and monitoring
- Data pertinent to the system's physical configuration and network topology
- Storage media

The integrity of digital evidence is easily damaged, therefore any carelessness in its handling can jeopardize its veracity. Due to its sensitivity and fragility, data must be treated according to certain protocols to prevent it from becoming corrupted during processing. These guidelines define the steps that must be followed out in a specific order when handling digital evidence. The initial processing of digital evidence consists of the following four phases: identification, collection, acquisition, and preservation (katharina.kiener-manu).

1. **Identification:** During the identification phase of the investigation, preliminary information about the cybercrime case is acquired prior to the collection of digital evidence. This preliminary information is analogous to that gathered during a standard criminal investigation. The investigator searches for answers to the following questions:
    - Who is accountable for it?
    - What took place?
    - When did the unauthorized use of the computer occur?
    - Where did the internet criminal behavior occur?

- How did the internet illegal behavior occur?

2. **Collection:** The term "crime scene" refers to more than simply the physical location of digital devices that were either used in the commission of a cybercrime or were the target of a cybercrime. In the context of cybercrime, "crime scene" has a far wider meaning. The phrase "cybercrime crime scene" refers to the physical location of digital devices, computer systems, and servers, in addition to the digital devices themselves, which may or may not include digital evidence. When a cybercrime is suspected, reported, or seen, the crime scene is instantly safeguarded. The first responder is responsible for identifying the crime scene, safeguarding it from contamination, and conserving volatile evidence. To avoid the destruction of evidence, this is performed by isolating the users of any digital devices located at the crime scene (for example, by detaining them in a different room or location) (Nelson, Phillips, and Steuart, 2015)

3. **Acquisition:** There are several methods to complete the buying procedure. The approach used is governed on the kind of digital device being utilized. For instance, the method for obtaining digital evidence from mobile devices such as smartphones differs from the procedure for obtaining digital evidence from a computer's hard drive. Smartphones and other mobile devices are more difficult to access than PC hard drives.
   Unless live acquisition is performed, the evidence is recovered from the seized digital devices at the forensic laboratory (i.e., static acquisition). In the forensics lab, digital evidence must be collected in a way that safeguards the integrity of the evidence (by ensuring that the data has not been altered), or in other words, in a forensically sound manner. To achieve this, the procedures and instruments used to gather digital evidence must be able to either prevent modifications to the data or, if this is not possible, at least restrict the implications of any changes that do occur (SWGDE Best Practices for Computer Forensic Acquisitions, 2018).

4. **Preservation:** Digital evidence preservation prevents tampering. ISO/IEC 27037 requires that digital evidence's integrity be preserved throughout its processing. First responders, investigators, crime scene technicians, and/or digital forensics experts must demonstrate that digital evidence was not altered during identification, collection, and acquisition. The ability to do so depends on the digital device (such as computers and mobile phones) and the conditions encountered by them (e.g., need to quickly preserve data). A chain of custody proves this. In order: "The way investigators keep the crime scene and any evidence there throughout an investigation. It includes who gathered the evidence, where and how, and who claimed ownership and when. It shows who had proof " (Maras, 2014, 377). The chain of custody should contain the names, titles, and contact information of those who identified, gathered, and acquired the evidence, as well as facts regarding the transferred evidence, the date and time of the transfer, and

the purpose for the transfer. The chain of custody should also include the transfer's justification.

References:

Diffen. (2020). Procedural Law vs Substantive Law - Difference and Comparison | Diffen. Www.diffen.com. https://www.diffen.com/difference/Procedural_Law_vs_Substantive_Law

Cyber Security Coalition. (2015). CYBER SECURITY INCIDENT MANAGEMENT GUIDE CENTRE FOR CYBER SECURITY BELGIUM. https://www.agoria.be/upload/agoriav3/Cyber-Security-Incident-Management-Guide-2015.pdf

Smibert, J. (2014). Principles of Evidence. Brrln.org. http://www.brrln.org/uploads/documents/218/eng.pdf

Brezinski, D., & Killalea, T. (2002). Network Working Group. https://www.rfc-editor.org/pdfrfc/rfc3227.txt.pdf

katharina.kiener-manu. (n.d.). Cybercrime Module 4 Key Issues. Www.unodc.org. Retrieved September 30, 2022, from https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/intro.html

Nelson, B., Phillip, A., & Steuart, C. (2015). LM Guide to Computer Forensics & Investigations - Lab Manual (5th Edition). Amazon. https://www.amazon.com/LM-Guide-Computer-Forensics-Investigations/dp/1285079086

SWGDE Best Practices for Computer Forensic Acquisitions. (2016). SWGDE - Forensics. Www.swgde.org. https://www.swgde.org/documents/published-by-committee/forensics

Marie-Helen Maras. (2015). Computer forensics : cybercriminals, laws, and evidence. Jones & Bartlett Learning.

Cohen, & Winter. (2021, August 31). What's The Difference Between Evidence and Proof in NH Law? Cohen & Winters. https://www.cohenwinters.com/whats-the-difference-between-evidence-and-proof/