Unit 4: Continuity and Reliability

Welcome to Week 4.

This week's learning addresses the quality and reliability of evidence. You will read on different methods of evidence gathering; there appears to be inconsistency of application which might lead to complications when the crime is transnational. The focus, as it has been in the past two weeks, is on evidence gathering. However, attention will shift slightly to the human-aspect of evidence gathering. You will notice that lots is said about a variety of techniques, however, we do not know much about the extent of human-cognition (in the persona of the investigator) might in fact affect evidence gathering.

On completion of this unit you will be able to:

- Explore the implications and limitations concerning evidence gathering.
- Assess the quality of digital evidence.
- Apply evaluation skills to a case study.

Reflection:

Continuity of Evidence:
When we talk about digital continuity, we mean being able to use your data how and for as long as you want. This means keeping digital information through different stages of growth so that it stays complete, can be accessed, and can be used when needed. Management of digital continuity can be used to make sure that your company is managing information well enough to meet its requirements for forensic readiness. Controlled digital continuity makes this possible. (Continuity - Court Stage - Enforcement Guide (England & Wales), n.d.), (The National Archives, 2011).

Both keeping digital continuity and getting ready for a forensic examination are good ideas. Your business will need to know the details of your forensic preparedness policy if you are in the process of managing your digital continuity, and you will need to look at the forensic evidence as part of the process of identifying your information assets. If you go through this process, you are taking care of your digital continuity. If, on the other hand, you are in the process of making a forensic readiness plan, you need to be aware of the risks that come with the digital continuity of your evidence assets being interrupted and take steps to prevent such losses (The National Archives, 2011).

Reliability of Evidence:
Dependability refers to the degree to which a piece of evidence is regarded as trustworthy or believable (Study.com., 2022).

Evidence that May be Gathered Digitally:
Information like computer papers, emails, text messages, instant messages, transactions, photos, and internet history can be easily retrieved from electronic devices and used as proof. Other types of information that can be retrieved are: Since mobile devices use online backup systems, often called the "cloud," forensic investigators can access text

messages and photos made with a certain phone. On average, these systems keep 1,000 to 1,500 or more of the most recent text messages sent and received by the device (Forensics Science, 2020).

Also, many mobile devices can store information about where and when the device has been. Investigators can get this information by getting a list of the 200 most recent cell sites a mobile device visited. Both in-car satellite navigation systems and in-car satellite radios can give you the same information. Even photos posted on Facebook or other social networking sites may include location information. When a GPS-enabled smartphone takes a picture, the file information shows the exact time and place where the picture was taken. If investigators can get a subpoena for a certain mobile device account, they may be able to find out a lot about the device and the person who uses it (Forensics Science, 2020).

Evidence Handling Procedures (Boubez, 2021)

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

Methods those effects while collecting digital evidence (Jabeen, 2022)

1. **Information Risk on the Internet Being Stolen, Modified, or Attacked**
   Most of the time, gathering digital evidence is a simple process. The hard part is keeping it safe and making sure that it doesn't get messed with, have its data stolen, or become the target of cyberattacks. It is hard to stop these attacks and find tampering because the attacks are done in secret to make the tampering look like it didn't happen.
   To avoid this problem, law enforcement agencies should use high-quality enterprise-level digital evidence management systems that have a lot of security features to keep evidence safe and find tampering. It should help keep audit logs to keep track of the lifecycle of evidence, make sure there is a clear chain of custody, and keep digital evidence in its original form.
2. **Different digital devices, types of data, and amounts of data**
   Digital evidence is now available in many different ways, from devices like CCTV, body cams, drone cams, home security cameras, and many more. The problem for government agencies is that the amount of digital proof is growing at an exponential rate, which is a big problem.

Digital devices don't have enough space to store all kinds of digital evidence. Also, it is physically hard to sort through all the different devices and file types to find useful information.

3. **Controls on Administrative Access**

   The CJIS Security Policy makes it very clear that government agencies must keep digital evidence in a controlled environment or a safe physical place, and that only authorized people can access these data.

   This is one of the most common problems that law enforcement agencies have when they have to deal with a lot of digital evidence.

4. **Inaccuracies and Accidents**

   Humans aren't perfect, so mistakes are bound to happen due to things like biases that happen by accident, too much work, bad use of technology, random events, etc.

   It is important to hire people who have the right education, knowledge, and experience. The amount of work that needs to be done must be well managed so that the investigation doesn't get worse because of it. Any mistake, no matter how big or small, could make the evidence inadmissible in court.

5. **Getting information across**

   The most dangerous time for evidence is when it is being sent from one place to another, because this is when data are most likely to be lost, stolen, or changed. It is very hard to keep digital evidence from changing while it is in transit.

   You can't just store data on traditional devices like USB sticks or laptops and protect it with a password. These devices are easy to steal and break into. Even a simple Internet transfer done through email is fraught with danger.

6. **Putting on a show in court**

   Finally, if the court rules that the digital evidence can't be used because of problems with how it was handled. Also, government agencies should know that there are different ways to present evidence in court, considering the court's technology infrastructure and Internet connection. Based on this idea, the evidence must be moved and shown in a safe way.

   If the evidence can't be shown right away, you should download it and give it to the court. To go along with the digital presentation, it is strongly suggested that image stills from the video evidence be recorded and printed whenever possible, and that all other documents and photos be shown in printed form.

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

Continuity - Court Stage - Enforcement Guide (England & Wales). (n.d.). Www.hse.gov.uk. https://www.hse.gov.uk/enforce/enforcementguide/court/physical-continuity.htm

Forensics Science. (2020). Digital Evidence: How It's Done. Www.forensicsciencesimplified.org. https://www.forensicsciencesimplified.org/digital/how.html#:~:text=Evidence%20that%20May%20be%20Gathered

https://homework.study.com/explanation/the-reliability-of-evidence-refers-to-the-degree-to-which-evidence-is-considered-believable-or-trustworthy-there-are-six-factors-that-affect-the-reliability-of-audit-evidence-one-factor-is-the-indep.html#:~:text=The%20reliability%20of%20evidence%20refers,is%20considered%20believable%20or%20trustworthy.

Jabeen, S. T. & S. (2022, March 24). How to Overcome Major Problems in Handling Digital Evidence? Enterprise Video Streaming Solutions for Businesses, Enterprises, Government, Local, State Government, Healthcare, Education, Law Enforcement Agencies, Justice, Public Safety, Manufacturing, Financial & Banking Industry. https://blog.vidizmo.com/6-major-problems-in-handling-digital-evidence

The National Archives. (2011). Digital Continuity to Support Forensic Readiness. Cdn.nationalarchives.gov.uk. https://cdn.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf