1. In Module 7, we introduced n-version software development and an example in the context of malware analysis.

Betty uses a URL blocker tool to block malicious websites. Whenever she visits a website, the URL blocker tool checks the website against a blacklist and if found, blocks the webpage. Discuss how Betty can use the N-version approach and the cloud to improve the accuracy of this tool. What would be the components of such a cloud-based n-version URL blocker (**explain with a diagram**)?  (2.5+2.5=5)

**DIAGRAM:**

A diagram of a website

Description automatically generated

Drawn at: lucid.app

**EXPLANATION:**

The host agent, a lightweight agent that runs on the host, will receive the request first and be responsible for forwarding it to the cloud and receiving a response. The request will be routed to the cloud-based analysis engine by the host agent. Several (N-versions) of the analysis engine's tools are operating continuously. Each tool will receive an HTTP request or a domain name and use its databases to determine whether or not the domain has been marked as harmful. Other tools can determine the website's state if the first one is unable to determine the domain's status. The host agent received the status from the analysis engine and acted accordingly: if the status were malicious, it would block the request; otherwise, it would enable the request to be opened by the browser.

The analysis engine on the cloud side will additionally forward the requests' analysis activities to the Forensics activity of the server. In order to assist us with forensics in the future, this will maintain an archive of the queries made by the host agent and the responses we receive from the analysis engine. Using the N-versions strategy has the advantage of providing us with a large database to search for the necessary information; if one tool is unable to determine the website's state, another one may be able to. Assume that three tools are operating simultaneously. The analysis engine receives a new website request, which is recorded online the same day. The databases of the first two tools are current and do not include the website's information, but the third tool does. Regarding the malicious website, the third tool will reply to the host agent. Therefore, we are not reliant on a single tool database here.

2. Bob, the builder, is corrupt and uses a cloud-based accounting tool to manage the transactions of his illegal business. Fred, the forensics investigator, is assigned to investigate Bob. Fred raids Bob's office and seizes Bob's laptop. However, since Bob uses a cloud-based accounting tool, there is nothing on Bob's laptop. All the evidence is stored in the cloud. Fred's next task is to run a forensic investigation against Bob. What are the challenges that Fred would face in conducting a digital forensics investigation against Bob? (Please review the **various stages of the digital forensics process workflow** as discussed in **module 8** and answer this question only in terms of different stages of the workflow). (5)

Workflow:

Identification 🡪 Collection 🡪 Organization 🡪 Presentation

**IDENTIFICATION:**

Now that we have the laptop, we must determine what and where the data is stored. which cloud Bob was storing his data on. Bob is utilizing a cloud-based tool, but what if the data that is stored there is encrypted? The investigator must get the paperwork ready in order to get in touch with the cloud service providers if the tool isn't logged in. Bob might have uploaded additional data to the cloud, but we require the information related to the accounting tool. Other features of the program might also be available, but the investigator must actively search for the transaction records. It's also possible that Bob erased the transaction data. It is important that the investigator explain whether the cloud suppliers are able to provide the erased data. Depending on the data, some cloud services retain data for up to 30 days after it has been deleted. The Slack space can assist in data recovery if the data has been deleted and not written on or if the data was written on. To obtain the real data, we must cite the source.

**COLLECTION:**

He follows the chain of seizing and documenting the evidence when the crime scene is searched for evidence. Thus, the inquiry must be thorough. The disk can be shared with the co-tenants when the cloud has been located. Data from the disk may reveal information about another person who is using the same drive as the criminal. It would be difficult to extract the evidence from a large amount of data if the cloud provider provided the data. If the data was deleted but nothing was written on it, or if there was writing on it, the Slack space can help with data recovery. The investigator must ensure what data should be extracted in to do this process.

**ORGANIZATION:**

After the data is gathered, a timeline should be created for the events drawn from it. Locating the illegal data. Identifying the parties involved in transactions. What was done, by whom, and how much money was transferred? We might be able to identify any more people or organizations involved in illegal activities thanks to the information. The author's step must be included with the organization and documentation of each step. The evidence needs to be presented such that it is true to the case and reliable.

**PRESENTATION:**

This is the time to present the evidence in a way that will convince a jury. As an expert witness, the investigator is required to testify. A strong report and presentation are necessary to convey the data to the court. In order for the court to acknowledge the information as accurate, acceptable, and trustworthy, it must be provided.