**QUESTION 1**

**a) What is Locard’s principle and describe how this is relevant to a digital forensic  
investigation?**

**A criminal always leaves behind a trace when committing a crime**

Locard's Exchange Principle states that in the commission of a crime, the perpetrator leaves something at the crime scene, and takes away with him something from the crime scene. What it takes and leaves are consider evidences that can be used for investigation. This principle applies to digital forensics as the attackers will leave multiple traces of their presence throughout the environment, including in registry, sys- tem logs, network-level logs and Web server access logs or IP addresses and will take elements of the crime scene back with them, such as stolen user passwords or in a file or database.

<https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l30/lec.html#:~:text=Locard's%20Exchange%20Principle,something%20from%20the%20crime%20scene>.

**b) Briefly explain some of the digital forensic challenges an investigator may experience in examining a cloud computing environment. Use an example to complement your answer**

* When data is stored in a cloud computing environment, it is sectioned into single data structures, which in turn are divided into elements. This makes the process of identifying and acquiring data very difficult.
* Data that lacks preservation and integrity will prove difficult for digital forensic investigators who need to ensure data is comprehensive, inclusive and verifiable for use in criminal or corporate investigations
* The cloud is scalable, which means at one point or another, data from several businesses can occupy the same sectors within the storage media. This creates a dilemma during e-discovery, where the investigator could unknowingly acquire residual data from company X when company Y is being investigated.
* If the data is stored in a country that does not recognize data privacy and security laws, or does not enforce existing laws, investigators could have a difficult time accessing the data to conduct their investigations.
* not all data is stored in one location; a company could unknowingly be using cloud servers on several different continents. Even if the data is accessible, the jurisdiction of the data could be in question.
* The location of the data, coupled with a lack of logging or use of anonymous authentication, could make it very difficult to establish and maintain an accurate chain of custody. This lack of integrity in the data will result in a failed investigation.
* Therefore, organizations have to be mindful of the contracts they sign with cloud providers, or chances are the physical location of their data will not be in the Ireland or whatever the country of origin is

**c) Explain in detail how the Windows registry data can be used as part of a forensic  
analysis of a computer system. Explain the main hives that are part of the registry and  
how this can be useful to discover malicious activity and to determine what has  
happened on the computer system?**

The Registry contains information that Windows continually references during operation such as:

* User Profiles
* File extensions and installed applications
* Settings for folders etc
* System Hardware
* Port config for I/O comms

For a Forensic analyst, the Registry is a treasure box of information. It is the database that contains the default settings, user, and system defined settings in windows computer. Registry serves as repository, monitoring, observing and recording the activities performed by the user in the computer. The Data is stored in the main folders in a Tree like structure which is called Hive and its subfolders are called KEYS and SUBKEYS where each component’s configuration is stored called VALUES. Each Hive is a hierarchical structure and paths to hives are set in the Configuration Manager. The Configuration Manager creates the rook keys and links the hives together in the registry structure.

There are five main Hives:

* HKEY\_CLASSES\_ROOT (HKCR) Stores data that associates file types with programs
* HKEY\_USERS (HKU) Contains user-specific configuration information for all currently active users on the computer
* HKEY\_CURRENT\_USER (HKCU) contains configuration information for Windows and software specific to the currently logged in user
* HKEY\_LOCAL\_MACHINE (HKLM) stores configuration information for the software you have installed including the Windows operating system
* HKEY\_CURRENT\_CONFIG (HKCC) Info in the Hardware Profile currently being used

**QUESTION 2**

a) Why is it important to have a device such as a Faraday bag available when transporting  
mobile phones as evidence?



Faraday bags is a radio frequency isolation device, which can keep unwanted signals or interference and jam signals out of an enclosure. It contains 2 sealing strips which can ensure no communication can be made. By shielding the phone from radio waves, is to ensure that the contents of any phone kept as evidence are not tampered with as well as keeping the location being tracked by criminals.

**b) The term dark data is used to describe files and other information that are misplaced,  
concealed, or otherwise missing. Explain the concept of data hiding as an anti-  
forensic technique and explain where an investigator may find hidden data.?**

Data hiding is the process of making data difficult to find, it gives an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves.

Dark data is used to describe files and other information that are misplaced, concealed, or otherwise missing. Data can be hidden within the various components of the structure of the OS. Places to hide data are called the warrens where data hides from digital criminals. Information such as BIOS and device configuration are stored there. The HPA doesn’t show up in a file system or browsers such as Windows or Linux file browsers. Other areas that can hide data is the Device Configuration Overlay. This is a hidden area of the hard disk on a Windows Operating System where the metadata consists of several hidden and read-only files.

In addition, the slack space also exist between partitions on a hard disk it can be used as a whole separate file system and can be a place to hide files. Tools such as Slacker can be used to manage all the slack space into it’s own file system. So investigators need to be aware of slack space being a potential hiding place for files.

**c) The Volatility Framework is an open source software program for analysing RAM in  
32 bit/64 bit systems. Describe how volatility works and detail the steps needed to  
analyse a ram capture. Describe 5 volatility plugins that can be used to obtain  
information from the ram capture**.

A ram capture is a snapshot of the RAM on a user’s computer. Examining a user’s RAM can provide a lot of information that would otherwise be lost when the user shuts down their machine. Volatility can examine there's captures using a variety of commands.

In order to examine a RAM capture, first access the capture itself and find the profile for the Capture in order to use the plugins to obtain information.

Identify the image using the command ./vol -f imageinfo, this command will also provide information on the image such as the machine type and OS used.

Once this information is gathered, some of the different plugins that can be used are:

* pslist, which will show all the current running processes in the form of a list, along with its process ID, name and what time it was run.
* psxview, which will show every single process that is hidden. A hidden process will give a False value in the pslist column , otherwise the process isn’t considered hidden.
* Filescan is a plugin that will show every single currently open file at the time, as well as the directory they are stored in. the use of GREP (or strings in Windows) can be used to search for specific files if needed, or file types.
* Chromehistory is a plugin that needs to be downloaded externally as it doesn’t come within Volatility. It will provide all searches in chrome, and the response given. This can be used to determine which websites were visited in the chrome browser, as well as the date it was visited in.
* cmdline / cmdscan, allows to show which were the last commands were run

**Case management and report writing**

|  |  |
| --- | --- |
| **TRIAGE** | * Assess any risks (to people, systems, or data) Mitigate as many risks as possible * Determine priorities * Is saving the data more important than nabbing the culprit? * Is identifying the culprit worth a financial loss? |
| **FIRST RESPONSE** | * Use the crime scene first-response protocols whenever possible * Determine the best method for collecting evidence * Perform live-response if necessary * Collect evidentiary materials in a forensically sound manner |
| **SCENE MANAGEMENT** | * Preserve the scene for other investigators Survey the scene * Document the scene (with photos and videos) Search the scene * Try to virtually reconstruct the crime |
| **LAB PREPARATION** | * Prepare a repository for digital evidence * Sufficient storage and security * Ensure proper tools are ready * Ensure personnel are ready to receive evidentiary materials |
| **EVIDENCE HANDING** | * Prevent environmental contamination * Block electromagnetic transmissions (faraday) * Maintain excellent chain of custody logs * Have a way to keep devices powered during transport * Don’t damage anything! |
| **EVIDENCE EXAMINATION** | * Use the right tool for the job * Document everything you do * Never touch the originals |

**Triage (sort of select)**

Forensic triage is the process by which digital evidences from a crime or investigation are collected, assembled, analysed and prioritized.

**Write blocking**

A Write blocker is a tool designed to prevent any write access to the disk permitting read-only access to the data storage devices without compromising the integrity of the data. A write blocking if used correctly can guarantee the protection of the chain of custody. There are two types of write blockers, Hardware write blocker and Software write blocker.

Hardware write blockers are used to intercept and block any modifying command from ever reaching the storage device. Hardware writes blockers such as Tableau for example, performs identical operation to a software write blocker, which is to permit read-only access in a device, preserving it’s data integrity.

Software write blockers are installed of a forensic workstation. Software write blocker tool operates by monitoring and filtering drive I/O commands sent from an application or OS through a given access interface. An example of a write blocker that is software based would be the Windows Registry, this involves editing one of the hives stored changing the variables in the Windows registry. However, one of the main issues with using this method is that messing with the registry tool could end up making the entire system unstable and would require a back-up registry to resolve.

The Tableau Forensic USB 3.0 Bridge

**Data carving**

Data carving, also known as file carving, is the forensic technique of reassembling files from raw data fragments when no filesystem metadata is available. It is a common procedure when performing data recovery.

First step in the file carving process is to identify the header and footer, which is where the file signature begins an end. Using a hex editor such as HxD, it can bring up the hex code of the file. Inspect if, usually either the header or footer, has been altered, an investigator can check if the hex code is in place. Changing the signature back to how it’s supposed to be (so FF D8 FF) can create a new file with the original contents of the missing JPG file.

As well as that, this technique can simply extract any hidden files without it being corrupted but are simply in unallocated space by using the hex editor to extract all the bits from the header to the footer of a specific file type and using that to recreate the file.

**Legal - ireland 2017**

*A person who, without lawful authority or reasonable excuse, intentionally accesses an information system by infringing a security measure shall be guilty of an offence.*

**international Convention**

In 2001, 26 member countries convened in Budapest and signed the Council of Europe Convention on Cybercrime to create “a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation”. The COE Convention on Cybercrime represents an aspirational policy document, a country that ratifies the Convention commits to putting in place a legislative framework that deals with cybercrime according to Convention requirements. Within this commitment, each country is given discretion in relation to the full scope, say, of a criminal offence, by defining its particular elements of dishonest intent or requiring that serious harm be done before an offence is deemed to have been committed.