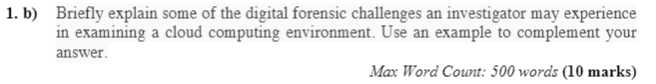


Locard’s principle refers to the event of exchanging evidence during a digital forensic investigation. According to Locard’s principle, it states that any contact between two items will result in an exchange.

This principle applies to any contact of evidence or items in a crime scene during an investigation, between for example, an offender and a victim can leave blood, a person and a weapon can leave fingerprints or between people and the crime scene itself could lead to witnesses and testimonies. Within the realms of digital forensics, examples of contact that exchange evidence could be that malicious attackers that intrude other computers will leave traces of their presence in the system logs, network logs and system registries.

Other examples include attackers that transfer elements from the crime scene such as a database file and stolen user passwords can be used as evidence which could link an individual to an intrusion.

Email harassment by sending threatening messages in for example Gmail or Outlook will lead to a number of traces. The browser used to send those messages will store the links and information of the sender’s hard drive along with date and time-related information, the original message contents and possibly IP addresses and access logs and the message sent in the mail folder of the offender’s email account.



When investigating in a cloud environment, the data is available through a client interface, In order to access these, the login credentials are needed. The local machine itself will not contain much data, as it is all possibly stored in the cloud and will contain very few local artifacts to examine.

Without the credentials needed to access the user’s cloud service, forensics investigators will need to get access to the actual cloud servers that are within the cloud provider’s possession. However it is to be noted that there are several clients that use the physical server provided by the cloud provider.

Cloud computing provides several advantages in the computing industry, as it provides faster integration of technology and the ability of resource and cost sharing. However in the realms of digital forensics, numerous factors such as information security, data jurisdiction, privacy and national law come into concern.

Data stored in the cloud is sectioned into separate single data structures which are then divided into a number of elements, making it quite difficult in order to identify and acquire the data needed.

Data lacks preservation and integrity, and will prove difficult for digital forensic investigators who need to ensure data is comprehensive, inclusive and verifiable for use in criminal or corporate investigations, assuming the investigators are able to acquire the data needed in the first place.

The benefits that have made cloud computing so popular are the reasons for concern for a digital forensics investigators

First 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.

The accessibility of data in terms of physical location and personnel access is something all organizations need to consider.

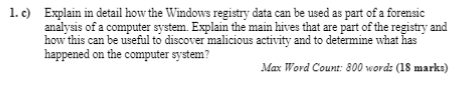
If the data is stored in a country that does not recognize data privacy or does not enforce existing laws, investigators could have a difficult time accessing the data to conduct their investigations.

Also, 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. Investigators have to ask if they are even allowed to acquire and investigate data that is stored in a different country.

Next, 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 Ireland or their country of origin



The windows registry can be described as a hierarchical database, that contains the values of a variety of variables in the Windows operating system and of the applications that run on Windows. It also contains a variety of other information such as profiles for all users, every application that was installed in Windows, ports being used, hardware available and types of document applications can create.

The registry contains hives, which can be described as a section in the registry which contains keys and values in the registry that has a set of supporting files that contain backuped data. In other words hives are a set of files set in the configuration manager.

The main hives or root keys of the windows registry are the following hives

HKEY\_CLASSSES\_ROOT

HKEY\_CURRENT\_USER

HKEY\_LOCAL\_MACHINE

HKEY\_USERS

HKEY\_CURRENT\_CONFIG

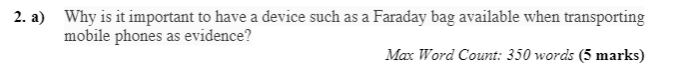
The first hive is the CLASSES\_ROOT. This is used to manage file type associations and data that associate file types with programs. It provides the information for Windows to know what to do when performing certain tasks such as viewing the contents of a drive or to open a certain type of file.

The next hive CURRENT\_USER contains configuration information for Windows and the software specific to the currently logged in user. The registry keys and values in this hive are used to control user-level settings such as wall appears, printers and shared drives, as well as other information such as settings changed in the Control panel are stored here.

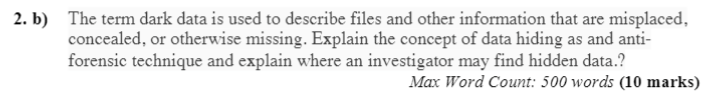
The hive LOCAL\_MACHINE stores configuration information for the software installed by the Windows operating system. As well as that, the hive keeps a record of any hardware used as well as the device drivers. It also stores information on boot configuration for Windows ⅞ and 10

The USERS hive stores user-specific configuration for all currently active users on the computer and machine. Each key represents a user on the system, and is lined with their security ID (SID). information on the user it stores includes when the user has logged on as well as mapped drives, printers and environment variables.

Finally the CURRENT\_CONFIG hive is a pointer to another location in the registry, and provides information of the hardware profile currently being used.



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



The concept of data hiding can be described as purposefully hiding data in order for it to become more difficult for investigators to find, but still making it accessible the the user who is hiding the data

Data can be hidden within the various components of the structure of the OS. These places where data is hidden are known as warrens, as they hide from predators. Places where data can be hidden is a hidden partition known as the Host Protected Area (HPA). 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.

Also a tool to use for hiding data is available, as there exists certain advanced utility tools that allow users to manage a separate slack space, as if it was their own separate file system.

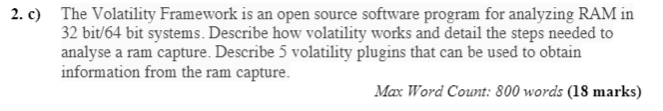
Investigators can search these warrens, in order to find data the has been hidden

For example , the HPA partitions can be searched by using data carving utilities such as Scalpel to find file formats. As well as that, using commands that search through files, results and specific messages such as GREP and linux and Strings in windows can be used to filter out specific messages and text passages in hidden partitions. The entire HPA can be copied as well by forensic duplication utilities , like DD utilities which can copy HPA partitions.

With regard to separate slack spaces that create partitions that cannot be detected by file browsing utilities called ghost partitions. In order to locate and access ghost partitions, a program such as Slacker can be used to manage ghost partitions as if it were a separate file system. Since the program executable would only be known by the user, investigators may be able to search the registry in order to find some executables that were recently run that seem suspicious

Another data hiding technique is editing the $BadClus metadata file. A hard disk drive will have certain corrupt or questionable sectors marked as bad, and moves the data to a new safe sector. When using disk editors such as WinHex, the contents of the $BadClus file can be edited to include the sector the files are hidden in as a bad sector. Investigators should examine the $BadClus files, as they always contain a file size of 0 bytes, and if the size is any greater, all clusters and sectors defined in the file should be extracted for examination.

Finally there are hiding spots within the registry, users can hide files in, such as string value hives, or certain contents can be stored in a bogus registry entry. Investigators have access to tools such as RegCheck which will examine the registry for any content that shouldn’t be expected within the registry.

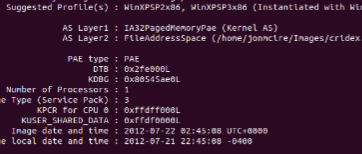


A ram capture is a snapshot of the RAM on a user’s computer. Examining a user’s RAM can provide a lot of information that would otherwise be lost when the user shuts down their machine. Volatility can examine there's captures using a variety of commands.

In order to examine a RAM capture, first access the capture itself and find the profile for the Capture in order to use all the other plugins to obtain information. To identify the image, use the command

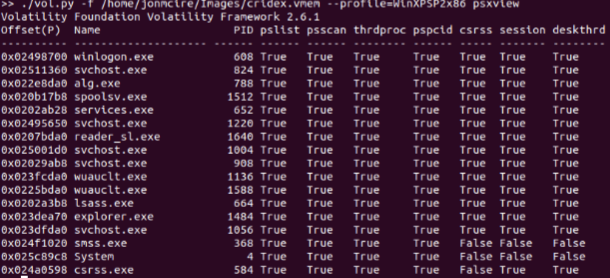


From this, we can understand basic information of the image such as the machine type and operating system used.



Once this information is gathered, a number of different plugins can be used to obtain information. One such plugin is 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.

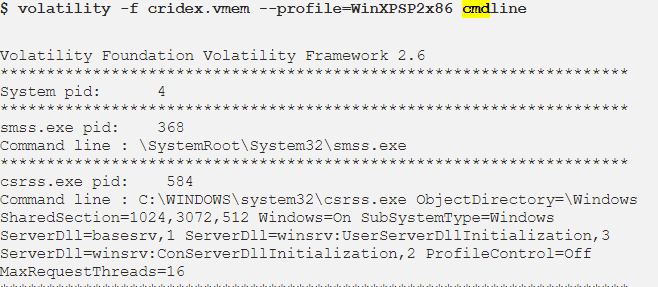
Another plugin is the psxview, which will show every single process that is hidden. A hidden process will give a False value in the pslist column , otherwise the process isn’t considered hidden.

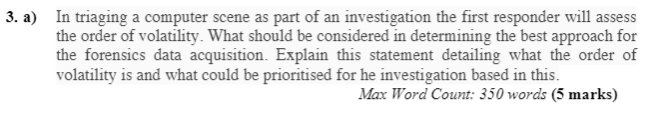


Filescan is a plugin that will show every single currently open file at the time, as well as the directory they are stored in. the use of GREP (or strings in Windows) can be used to search for specific files if needed, or file types.

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.

Finally the plugin of cmdline / cmdscan, allows to show which were the last commands were run





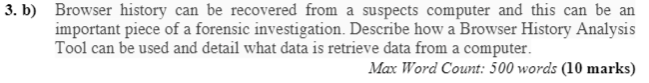
Data Acquisition refers to the procedure of gathering all evidence available from a source, which includes discovering and copying the contents of a file for example

The first responder will assess the order of volatility, which means the order in which all the digital evidence is collected based on the volatility of the evidence. Evidence that is the most volatile should be collected first, as it is more likely to be lost if for example the power gets shut down.

RAM is without a doubt one of the most volatile evidence of a digital source, as all data within RAM gets deleted as soon as power gets shut down. Cache memory is also volatile. A memory capture should be made asap before all the evidence is lost.

As well as that RAM contains very important information such as passwords, running processes, encrypted data, logged in user information, evidence of attached devices and open ports.

Other sources in order of volatility goes as Temporary files, local disks, external storage media, Network attached storage and finally Archival backups.



Browser history can provide a lot of insightful information that may prove useful in a forensic investigation, such as the suspect’s search history, cookies which store the suspect’s sessions, internet files downloaded and registry entries can all be useful evidence.

A browser history analysis tool such as Web Historian is able to discover which browser was used for history files by examining the directory structure of the suspect’s computer. This can prove useful if the investigator is unable to ensure which browser was used. As well as that, all finds can be outputted in a readable format such as Excel or HTML, allowing for each investigation, with abilities of filtering, sorting information with timestamps and URLs.

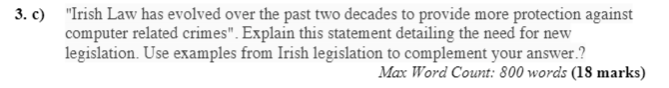
A Lot of information can be gained from browsers, such as images and pages that were viewed by the suspect, as well as Cookies which contain valuable information such as usernames or passwords.

There are history records which show the user’s activity, and internet files that can be recovered by file recovery utilities can be analyzed as well.

History files show the Url accessed, the file name that exists on the local system,the time that the file was accessed, modified and which directory it’s stored in, the HTTP headers received and finally the record type, whether it was browsed directly or it was redirected to.

Investigators may also search web servers, which contain a variety of log files such as IIS logs which contain the interaction between client and web servers.

Log files provide information on the HTTP traffic, in which the investigator can determine the order of requests and responses, and what content was obtained from requests.



During the early years of Irish Law, when it came to dealing with cyber crimes and law breaking involving technology, there were severe limitations in actually dealing with these types of crimes. At first there were 2 legislations

The Criminal Damage Act 1991 & the Criminal Justice (Theft & Fraud Offences) Act 2001

These acts weren’t designed against cyber crimes, in many different areas of crime such as dealing with unauthorised access. Unauthorized access under the Criminal Act 1991, is not considered to be a criminal damage act which is intended to cause damage, but it was merely considered to be a breach of confidentiality, as it was merely looking around.

The punishment of operating a computer in order to unlawfully access data with the intent of accessing data within or outside the state will be fined 500 pounds max or 3 months in prison, which is quite minimal.

Within the Criminal Justice (Theft & Fraud Offences) Act 2001 it states that a person who dishonestly, whether within or outside the State. A person who dishonestly, whether within or outside the State, operates or causes to operate a computer within the State with the intention of making a gain for himself, or herself or another , or of causing loss to another, is guilty of an offence.

However some misinterpretation can arise from some legislations , such as the Criminal Justice (Theft & Fraud Offences) Act 2001 to deal with information theft

It states Subject to section 5, a person is guilty of theft if he or she dishonestly appropriates property without the consent of its owner and with the intention of depriving its owner of it. It really isn’t clearly defined what is meant by property,