# Digital Evidence Acquisition and Unique Characteristics of Cloud Technology

Tri Dai Ho

School of Cyber Education, UMGC-Global

CCJS 321-7382: Digital Forensics in the Criminal Justice System

Professor Maurice Hicks

18th April 2023

1. **Digital devices may be collected in a broken state with deleted files. How can digital forensic practitioners extract or recover these lost files?**

   There could be multiple reasons why a device may be collected in a broken state or with evidence files that no longer exist in the system. It could be the frantic response of the suspect to cover his trace; or a lost, broken phone with no battery lying under an empty well waiting to be discovered. However, not all hope is lost since we can still recover these files.

   - If the OS and hardware are still operational. We can first check the Recycle Bin. According to rahi_garg, a contributor of geeksforgeeks.org (2022), there are two standard methods of deleting a file: Delete and Shif+Delete. In the first case, the files are still in the Recycle Bin.
   - If Recycle Bin does not yield any result, rashi_garg (2022) suggests using commercial file recovery software to retrieve these files. This can be accomplished because the system tags the deleted file with “delete” status and marks the stored cluster as “available” for new data. This means the deleted file can be retrieved successfully unless new data occupies this slot.
   - If we can still access the hard drive and the OS seems to sustain some damage that inhibits investigators from executing files, Sarah (2020) suggests we check for the most recent data backup or recovery file. Depending on the damage to the digital data on the hard drive, the investigator may need to boot in Safe Mode and run the recovery backup from there. Sarah (2022), running the most recent backup is the most cost-effective and fastest way to retrieve any lost file.
   - A more advanced technique in retrieving destroyed files is called data carving. This technique is a bit-precise and sequential different drive

examination (rashi_garg, 2022). Rashi_garg (2022) explains that data carving is not data recovery. It allows the forensic team to 1. Identify the signature and pattern of the file located on the disk, 2. Locate various artifacts that would not be available otherwise.

- Not only data entry and record can be helpful, but metadata can also offer valuable evidence, especially in $ LogFile of the New Technology File System (NTFS). According to Oh et al. (2022), this log file record data of file system transaction such as file creations, deletions, data changes, and name changes. These record units contain “redo” and “undo” data and can prove extremely important if the file system is broken or there is a sudden power outage.

2. **Locard’s exchange principle states, “A criminal action of an individual cannot occur without leaving a mark”. Explain what this principle means for digital evidence.**

Locard’s exchange principle visualizes the interaction between two systems that exist and interact with each other at a typical crime scene involving the victim and the criminal. In his classical view, Locard argues that there is no contact without a trace; both the victim and the criminal bring *something* to the scene and take *something* from the scene. Dr. Bay and Zatkyo (n.d.) propose that although Locard’s principle was born to solve physical crime, its underlying concept can still be applied in the digital world. The authors argue that even in the digital world, the relationship between victim and criminal still exists, and it concerns three aspects of this relationship: Are there two items? Is there contact? Is there an exchange of material? (Bay & Zatkyo, n.d.) Since criminals make virtual contact in the digital domain, they must leave a virtual trace. For example, the attacker naturally goes after ransom money in a ransomware attack. The

ransom will be transferred to the attacker's account, which is traceable evidence of the crime.

**a. Describe best practices that should be followed to ensure digital forensic practitioners don't leave their own "marks" on the evidence during collection and acquisition.**

According to GeeksforGeeks (2020), critical steps need to be followed to prevent data loss before bringing them to forensic experts. Time is highly important in preserving digital evidence.

1. **Do not change the device's current state:** If the device is OFF, it must be kept OFF; if it is ON, it must be kept ON. Call a forensics expert before doing anything.
2. **Do not plug any external storage media in the device:** Memory cards, USB thumb drives, or any other storage media you might have, should not be plugged into the device.
3. **Do not copy anything to or from the device:** Copying anything to or from the device will cause changes in the slack space of the memory.
4. **Do not open anything like pictures, applications, or files on the device:** Opening any application, file, or picture on the device may cause loss the data or memory being overwritten.
5. **Do not trust anyone without forensics training:** Only a certified Forensics expert should be allowed to investigate or view the files on the original device. Untrained Persons may cause the deletion of data or the corruption of important information.
6. **Make sure you do not Shut down the computer; if required, Hibernate it:** The digital evidence can be extracted from both the disk drives and the volatile

memory. Hibernation mode will preserve the contents of the volatile memory until the next system boot.

**b. Choose three items of digital evidence from the following list and describe what types of digital "marks" (artifacts) might be left by a user. (Laptop, Router, External Hard Drive, Thumb Drive, Smartphone, Gaming Console, IoT devices, Home Surveillance Systems, Vehicles)**

Digital artifacts are the traceable mark of a device when it interacts with a human user or another device on a network. In this essence, an artifact can be produced entirely unintended by the user; we can even treat it as the by-product of using the device. For this reason, digital artifacts are critical in digital forensics. If you were an intelligent criminal, you would remember to erase your physical presence. But would you remember to erase your digital presence? Even if you do, properly sterilizing a device from all traceable evidence requires very high technical expertise that few possess.

Smartphone: Smartphones yield some of the most personal information of their owner, whether a victim or a suspect. When all else equal, the criminal would enter the scene, complete the deed, and leave the scene while having their smartphone on them the entire time. The criminal may remember to destroy evidence, such as discarding clothing, or the weapon; however, not many would throw their smartphone away entirely after the fact. The same can be said for the victim. Many artifacts can be found on the smartphone, such as:

- Address book, note, or calendar.
- Social media accounts associated with smartphone owners.
- Tracking data from applications such as GPS, Health monitor

- Image and video deleted files.

Computer: Due to its higher processing and storage capabilities, computer artifacts vary in type and volume. In cybercrime, it is both the crime scene and the weapon. Artifacts that can be found on the computer such as:

- Email, and browsing history.
- Media, text files
- Data on volatile memory such as cache or RAM
- Hard drive

Router: In a home network, this device is the gateway for other devices to connect to the internet. Most routers these days have Wi-Fi antenna built-in, and artifacts from the router stem mainly from connectivity and network environment, such as:

- IP and MAC address
- Routing table and access list
- Service provider information
- Incoming and outgoing traffic

**c. How can examiners/investigators use this information to prove or disprove the allegations under investigation?**

As mentioned above, most criminals, except cybercrime, would attempt and sometimes succeed in erasing their physical presence on the scene but not their digital presence. The acting agent, location, and time form the three classical dimensions of any criminal activity. The digital artifacts introduce a fourth dimension in criminal investigation: virtual. As mentioned earlier, a smartphone would typically stay with the victim and the culprit throughout

the event. In other words, it virtually “witnesses” the crime happening. Since not all criminals are technologically adept, the artifact remains on the device. For instance, a 5G cell signal and wifi can tell if the device is in the vicinity of interest. My friend recently told me that his Android reminded him to rest and get good sleep since it recorded elevated heart rate and increasing movement detected by the censor. When combined, the two pieces of information are good enough to press the suspect with the question of why they were there and what they were doing. The same can apply to the victim, even if they cannot testify due to death or injury.

3. **What actions should a digital forensic professional take when encountering a running (live) laptop?**

According to the United States Secret Service (2015), there are several steps that the forensic team needs to perform to maintain evidence authenticity and the evidence needed.

- Live the laptop in the state of how we find it and take photos. The photos should include all parts and cables. If the laptop is running, take a photo of the screen.
- Obtain from users the necessary password, and PIN the need to unlock content or decrypt any encrypted file.
- Consider capturing the volatile data that still exist in RAM or cache when the laptop is on. If skillset and equipment permit, consider capturing networking data (IP address, network log, modern/router) data as the device still connects to the network.

- Properly document the devices in a Faraday bag and keep it away from the magnet or radio transmitter.

a. **What beneficial data may be found on the live system that would not be found on a powered-off (dead) system?**

A device such as a laptop can perform most tasks just as efficiently as a desktop, with one intrinsic characteristic: limited battery life. For this reason, when possible, a forensic investigator must consider a live capture attempt first. A live capture captures the evidence ideally in the state as if the device was used in the incident. As Amari (2009) addresses it, volatile data contains information on the device processes, open files, registry, network, password, encryption, or any hidden file. For instance, in a cybercrime, if the hacker uses fileless malware, we may not find any malware signatures by searching the hard drive. But such a feast can be accomplished by searching the volatile memory. Amari (2009) also points out that the user ID and password can temporarily be stored on the volatile in clear text. This can assist the forensic analyst tremendously if password or encryption cannot be obtained through an alternative means. The nature's short life of volatile memory means the data will be rewritten frequently and quickly. If we were to power down the machine, we would have a better disk image but potentially lose the volatile data. To put things in a better perspective, if we investigate an enterprise machine that runs on a hybrid or public cloud, it will be near impossible to turn off the "device."

4. **Describe cloud storage and explain its importance to investigators.**

   There are three main cloud deployments: public, hybrid, and private. Cloud storage typically refers to the public/hybrid cloud model in which the business data is stored off-site in a cloud vendor storage unit. The cloud can be considered a leasing model, in which the business will pay a monthly premium to rent out the storage unit to house their data. Due to this reason, forensics in a cloud environment has its unique requirements and challenges.

   - The hardware is the property of the cloud vendor; even if there is a warrant, the forensic investigator still needs to be mindful of their legal boundaries. Seizing business data from an employee may allow the investigator to seize the entire unit or the computer. However, cloud computing units are the property of the cloud vendor, and a warrant issued on the business data may not cover seizing a third-party property.
   - Cloud environment is of high availability. Shutting down an entire unit to obtain a static image can affect multiple businesses renting out the same racks. Therefore, most of the time, the investigator must perform live acquisition techniques.
   - Cloud has built-in security and interlace of redundancy. This means any access to the data inside the interested unit requires a password and encryption key from both the business and the cloud vendor.
   - Since the cloud is built with redundancy, the same data can be duplicated in multiple locations, just like a RAID configuration. A disk image can contain data from other operations and other entities.

Volatile memory, for this reason, can be unreliable or diluted with unrelated data from other businesses.

a. How can investigators preserve and gain access to cloud data?

The following are five ways to gain access to cloud data and preserve the evidence.

1. Give the cloud vendor a heads-up. This method is not technical in nature but can be extremely useful because it allows the Cloud IT team to have time to sort out the service requirement and other compliance issues in advance. Secondly, it allows adequate time for three ways of communication between the business, the cloud vendor, and the investigators.
2. Most cloud providers offer monitoring tools packaging in their cloud solutions. The investigators can leverage this built-in tool to obtain an accurate snapshot of the virtual disk image and RAM into remote storage.
3. For PaaS cloud deployment, it is best to have specialized in evidence acquisition in cloud environments. The better option is to contact the Cloud Security team and request directly from them. Since Cloud Security is more familiar with the setup and requirements, they can procure the evidence.
4. Cloud computers use virtual machine technology, which is a virtual environment for users to load and run their processes. Even virtual machines require a physical disk to load the OS at the very minimum.

This can serve the investigator's advantage since they can take an image of the virtual machine's hard disk.

5. Cloud data is backed up periodically using various data backup methods. The investigator can request assistance from Cloud IT to extract these archived backups. This can be tremendously helpful since the Cloud may have the backup around the time the incident happens, allowing a more pertinent acquisition and analysis.

**b. Do investigators need legal authorization to access the data? Why or why not?**

Legal authorization is a must to access cloud data for multiple reasons.

1. Cloud data is stored and located off-site in a third-party location. The same rack that runs the interest data also runs and stores data from other entities not mainly involved in the incident. This means that the best practice of taking photos of the device must be exercised outside the server room.
2. Due to multiple legal constraints, the investigators often need the Cloud IT team to fetch the data. This means the evidence acquisition is made by the Cloud vendor personally and not the investigator. Rafael and Granja (2017) highlighted the importance of the evidence-handling process in the chain of custody, where each person involved may need to testify about the integrity of the evidence in Court. Since the cloud vendor houses the data, and potentially the party that acquires the evidence, they are a part of the chain of custody.

3. Wilson (2013) brings forth the disparity in legal processes due to differences in the geo-location of the business that owns the data, and where the data is stored and processed. The current legal system has no clear guidance to tell which jurisdictions to follow, whether by the location of the business headquarters or the data server. Redundancy and resiliency are characteristics of most cloud ecosystems. This means the data of interest may be on a server, not even on the US continent.

## References

Amari, K. (2009). *Techniques and tools for recovering and analyzing data from volatile memory* [White paper]. SANS Institute. https://sansorg.egnyte.com/dl/S2wfxDfQS3

Bay, J., & Zatkyo, K. (n.d.). The digital forensics cyber exchange principle. *DFI News*. Retrieved April 16, 2023, from http://www.csc.villanova.edu/~dprice/fall2014/extra_handouts/The_Digital_Forensics_Cyber_Exchange_Principle_-_2013-04-22.pdf

Oh, J., Lee, S., & Hwang, H. (2022). Forensic recovery of file system metadata for digital forensic investigation. *IEEE Access*, *10*, 111591–111606. https://doi.org/10.1109/access.2022.3213030

Rafael, G. D. R., & Granja, F. S. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1. https://doi.org/10.1504/ijesdf.2017.10002624

Sarah. (2020). The Best Way To Recover Files From Broken Computer | Quick & Easy. *MiniTool*. https://www.minitool.com/data-recovery/recover-files-from-broken-computer.html

GeeksforGeeks. (2020). Digital evidence preservation digital forensics. *GeeksforGeeks*. https://www.geeksforgeeks.org/digital-evidence-preservation-digital-forensics/

GeeksforGeeks. (2022). Recovering deleted digital evidence. *GeeksforGeeks*. https://www.geeksforgeeks.org/recovering-deleted-digital-evidence/

United States Secret Service. (2015). *Best practices for seizing electronic evidence* (4.2). U.S. Department of Homeland Security. https://www.cwagweb.org/wp-content/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf

Wilson, D. (2013). Legal issues of cloud forensics [White paper]. Global Knowledge. https://d12vzecr6ihe4p.cloudfront.net/media/965983/wp-legal-issues-of-cloud-forensics.pdf