Hybrid Software

When people hear hybrid, they usually think of a vehicle, specifically the Toyota Prius. The Prius first went on sale in Japan in 1997 and was available at all four of Japan's Toyota dealership chains, making it the first mass-produced hybrid vehicle. As of January 2017, the Prius Liftback was the world's top selling hybrid car with almost 4 million units sold.

A hybrid vehicle is one that uses two or more distinct types of power, such as submarines that use diesel when surfaced and batteries when submerged. Hybrid technology optimizes a vehicles' systems to use a combination of electric and gas power while you're driving. Therefore, depending on which mode you're in, you can use much less fuel and spend less money on gas overall.

In the world of Technology, Hybrid can have any number of meanings, but the intended outcome is the same as it is for vehicles; to save money and improve performance. Examples of hybrid technologies are:

Hybrid Storage Solutions provide a compromise where critical, pertinent data can be stored on high-performance flash media while other data resides on less expensive tiered storage.

Hybrid-core computing is the technique of extending a commodity instruction set architecture (e.g., x86) with application-specific instructions to accelerate application performance.

Hybrid Cloud Architecture is the combination of public and private clouds or on-premise by a wide area network or broadband connection, through which applications and data can be shared and which can be managed as a single IT architecture.

Cloud and on-premise computing environments come with their own strengths and limitations and it may not be clear which is the right approach for you. The ideal solution may lie somewhere in the middle: a hybrid IT solution. A Hybrid Cloud Architecture is the most fascinating and the key to using it, is a Hybrid Software.

Throughout this article, we will discuss the architecture of a Hybrid Cloud and how this unique structure will provide a company with increased flexibility without needing to compromise on the price tag.

Private clouds and on-premise environments offer companies greater control over their costs, computing resources, as well as security. The organization manages all of the infrastructure, and they can customize it to match specific needs. However, an entirely proprietary IT environment is costly to run and maintain, especially as a company grows and more server space is needed.

Public clouds, on the other hand, offer scalability and are easier to manage, because the cloud provider takes care of the maintenance of the infrastructure. Using a public cloud is cheaper, but it may provide less flexibility and control over critical factors such as bandwidth usage/requirements, speed to reviewing files, and storage security concerns (ownership).

Many organizations opt for hybrid clouds to balance the advantages and disadvantages of public clouds and private infrastructure. As needs and cost requirements change, companies can transfer tasks between their public and private IT architecture. This provides companies with the flexibility and security they need, while giving them a scalable and cost-effective solution.

Hybrid cloud benefits

1. Flexibility and scaling—hybrid clouds allow you to store sensitive and frequently used data on your on-premise server/storage, while storing other data, such as backup and archives, on a public cloud, or any digital media that will not be viewed very often. A hybrid solution also provides you with agility in case you need to increase or decrease your resources as needed on a short notice. If the sudden need for additional storage space for a few months due to increased seasonal demands occurs, you can purchase additional space on a public cloud with short notice and without needing to invest in temporary servers.

2. Cost saving—the cost of running and maintaining a private cloud or data center can increase quickly, especially as a business grows. A hybrid cloud solution takes advantage of the relatively cheap public cloud storage space, while still using private infrastructure for data that is frequently used or sensitive in nature.
3. Infrastructure—a hybrid infrastructure maintains their legacy on premise servers, while integrating with a public cloud in a way that is not disruptive to daily operations. This can be done by progressively integrating with a public cloud, while running the most critical operations from the on-premise environment.

Real world problem

Law Enforcement today not only deals with an exorbitant quantity of digital media files but also a large variety of file types. Adding another level of difficulty to the quantity and variety are the files sizes and complex file structures. Perfect examples of these complex file types are HDD and cell phone forensic snapshots, as well as 3D crime scene re-creation files. These are very large files made up of folders/files that need to be kept in a specific order.

Currently support of these types of digital media is incredibly complex, forcing Law Enforcement Agencies to use outdated methods, evidentiary bad practices, or create "junk drawers" of digital evidence to handle today's media content. Agencies' IT are also dealing with having to spend all of their time managing different individual files or secondary devices. Combine these issues with the cumbersome task of managing massive amounts of digital evidence over years and ensuring its availability for discovery, and it means that police agencies are facing a huge investment in traditional in-house IT just to manage the flood of content. Users either have to attempt to Zip up the files and then upload the massive package to the cloud, or just copy and paste it to a hard disk drive or thumb drive and manage it manually. Essentially, users are stuck using whatever they have and are instructed to "make the best of it."

Consider the following scenario: A man is arrested in relation to a sexual assault investigation and his cell phone becomes a key part of the investigation. The LEA retrieves the cell phone and creates a 243 GB forensic snapshot. The LEA puts the copy of the snapshot onto a secondary device (e.g., HDD, thumb drive) and proceeds to place it in the physical evidence vault. After being indicted for the crime, he retains a lawyer. As part of the discovery process, the lawyer is informed that the suspect's cell phone was confiscated, and a forensic snapshot was taken of the phone's contents. The lawyer requests to see a copy of this cell phone.

The next day an officer is given the task of making copies of the secondary device to send to the prosecutor and the suspect's lawyer. The officer inserts the device into the computer to make the copy. He grabs a thumb drive and inserts it into the computer to begin the copying process. The new thumb drive isn't being displayed by Windows. The officer removes it and attempts to insert it and remove it several times only to find the USB port on that computer is bad. Without hesitation or giving it a second thought, he removes the original source device with the only copy of the cell phone snapshot. The officer doesn't hesitate to try it again on a new computer.

What the officer doesn't realize is that by removing the secondary device without properly ejecting it from windows, there is a chance of corrupting the device. When this happens, the LEA no longer has the cell phone nor the snapshot.

Based on this information and after meeting with his client, the defense attorney files a motion to dismiss the case, stating that the police do not have the evidence as requested. The suspect is released.

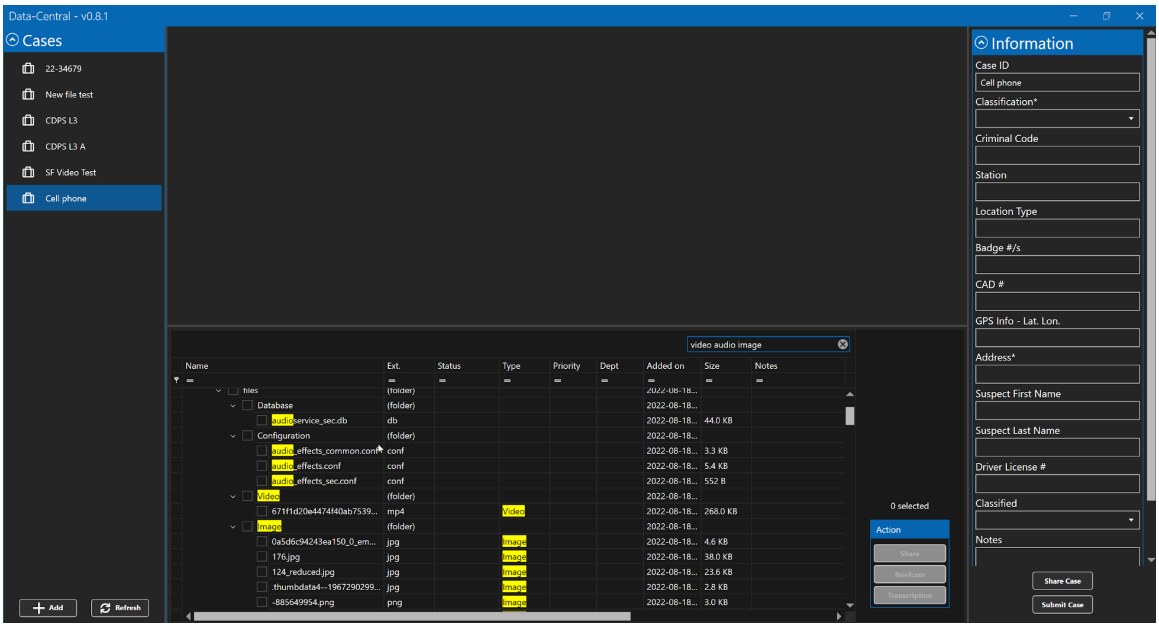
Why wasn't there a back-up of the evidence? Unfortunately, the cost of creating more copies on a secondary device is too high, and therefore, under-utilized. Since the snapshot was so large, the bandwidth limitation kept the LEA from uploading it to the cloud, and the evidence was lost forever. LEAs deal with multiple cell phone snapshots a day and this issue is happening more often.

One of the biggest issues faced by law enforcement officials — and the reason an increasing number of agencies are concerned with not only the volume of digital media, but the complex structures related to them in their entirety — relates to evidence being lost, corrupted, or destroyed by a natural disaster.

Hybrid Software solution

The solution is **Data-Central** and our new **Case-Manager** feature. In the challenge described above, the solution is to take the 243GB cell phone snapshot (UFED file) and simply drag-and-drop the parent folder into the **DC** application. The exact file/folder structure of the cell phone dump will be displayed in a tree structure. It will be accessible within seconds (depending on final size) from **DC**. The reason it is so quick is because **DC** doesn't move or copy the files to a new location but rather it creates pointers/nodes to the files in their original location. The design being getting access to the files with velocity and not duplicating the files in several places.

The user, within the UI, does a wildcard search for video, audio, and images (image below), and is presented with 1,504 files as opposed to over 30,000 files. Using the keyboard to quickly arrow down through the tree, add priority flags and notes to each file (**Rapid Review** function) the user quickly reviews and prioritizes the files for all 1,504 files.



Once the user is satisfied with the critical evidence being found and tagged, they simply hit the submit case button. **Data-Central** is capable of several workflow options but we will focus on the hybrid software solution. The configured workflow then takes the entire first instance evidence (243GB snapshot) and creates an encrypted (AES-256) **Case-Pak,** while taking a copy of the prioritized files (videos, audio files, photos), and sending those to their DEMS in the cloud. The **Case-Pak** is stored locally on-premise and will be retrieved using the **Case-Manager** feature.

The **Case-Manager** feature within **Data-Central** is a Federated query being ran across a centralized Federated database as well as all local **DC** databases. The results from the query are for active cases within **DC** (within a customer's environment) and archived cases that have been sent to storage (on-prem or cloud). If the results are a match for a case the user that ran the query can request access to the case. The user simply right mouse clicks on the case and selects "Request Access." The admin and/or the case owner will be notified and can grant access to the requestor (LEA member).

If access is granted, the case will be displayed in the requester's own **Data-Central**. The user will have full access to his/her own files and database and be able to perform all functions and features of **Data-Central**.

As an administrator, you can change the members and their access level for any shared case in your organization. You can also change the sharing settings for a case, and the default sharing settings for all new cases. For example, if you're concerned about a specific user having access to a case, you can remove them or change their access level. As an administrator, you might need to add members to a case through the admin console if the case has no members or no managers. Or you might need to remove members from a case if they shouldn't have access to the contents.

As an administrator, you can change the access level for a member of a shared case, even if you're not a manager of the case. For example, if you're concerned about a specific user having Manager access to a case, you can reduce their access level.

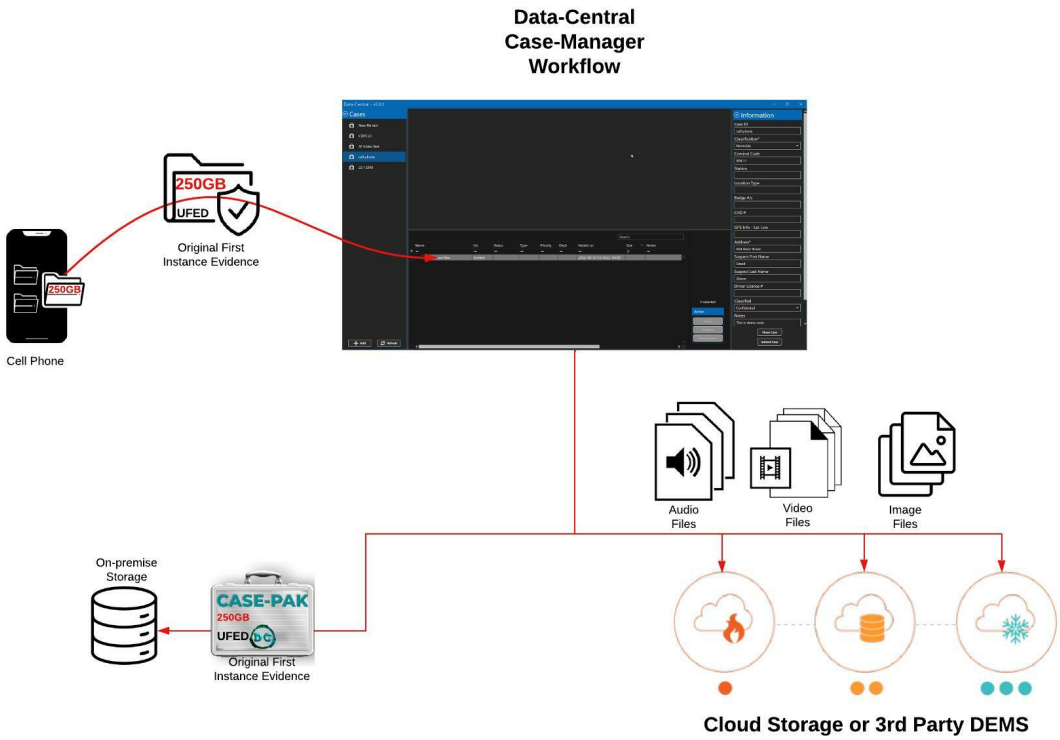
As an administrator, you can set the default sharing settings for cases by the organizational unit they're assigned to. You can also prevent members with Manager access from changing those settings. For example, if you have users in an organizational unit who you don't want sharing content outside of your organization, you can block external sharing and prevent managers from changing that setting.

Case-Manager Process

The process of digital evidence forensics consists of six elements:

1. **IDENTIFICATION**: Find the evidence, noting where it is stored.
2. **PRESERVATION**: Isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.
3. **ANALYSIS**: Reconstruct fragments of data and draw conclusions based on the evidence found.
4. **DOCUMENTATION**: Create a record of all the data to recreate the crime scene.
5. **PRESENTATION**: Summarize and draw a conclusion.
6. **DISSEMINATION**: Distribute evidence or property, to internal sources, external agencies, defense, prosecution, or the media

Case-Manager focuses on element 2, Preservation. For preservation, the challenge LEAs have is the sheer size of the files along with the complex structure. If the agency doesn't have the bandwidth or the budget to store several backup copies on several secondary devices and then keep them in multiple locations, preservation becomes a major issue. The answer is a hybrid software. Keep the large complex digital media snapshots (original first instance) on-premise, while uploading the specific, pertinent media content to the cloud (image below). The critical media content, consisting of videos, photos, audio files, text files and more, are the value and key to prosecuting the suspect. Once these files are uploaded, they can easily be shared, redacted, run through analytics, and used for a preliminary presentation to the defense counsel to keep it from ever going to trial.



The questions to ask are:

1. Does the prosecutor and legal counsel really need immediate access to the types of files that are only capable of being used by the devices' operating system?
    a. If there is no value in the system files, then why do those need to be sent to the DEMS?
2. Does the DEMS even handle these complex file structures?

The focus of these questions relates to elements 5 and 6, Presentation and Dissemination. Statistically, no more than about 5% of all criminal cases (misdemeanors and felonies) ever go to trial. The other 95% of cases are either dismissed, or a plea bargain is arranged between the defendant, their attorney, and the prosecutor for a final compromised disposition. The latter results in either the case being set for a Deferred Judgment and dismissed at a future date (if complied with the terms of the Deferred Judgment); or is reduced to a lesser charge than the one that the person was charged with.

The influence behind low trial percentage is due to the immediate presentation of critical, pertinent visual evidence confirming the suspect's likelihood of a loss in court, and the threat of maximum punishment if they were to proceed. Understanding this process is the driving force behind the creation of **Case-Manager** and **Data-Central**. The combined workflow of these two products addresses all six elements of digital evidence forensics.

DWS's Data-Central addresses proper and affordable solutions for managing evidence. **DWS's Data-Central** is middle-ware specifically written with digital evidence processing and security complications in mind. The **DWS** team not only has the software, but the experience to deal with these issues properly and efficiently. If you are challenged by current technology, budgets, and time-consuming manual processes and would like a demo or more information on **DWS's Data-Central** product, please **CLICK HERE**.

Dynamicworkflowsolutions.com