Digital Evidence Security

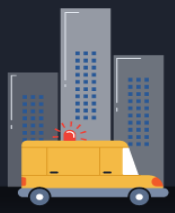
Is your evidence secure enough to email?

Defense attorneys stand in the frontlines to protect the rights of individuals accused of crimes either as private practice, or public defense counsel for those who cannot afford to hire an attorney. Defense attorneys investigate their clients' cases, negotiate plea agreements, and represent their clients vigorously in trial and appellate courts. Vigorously is the key word, and every year defense attorneys get smarter and more savvy about digital evidence presented against their client, fighting to keep digital evidence from being accepted as an exhibit by the court. As the defense attorneys learns and understands the digital evidence workflow (image below), they are seeking any mistake or gap in the process that may have been overlooked. They will ask questions regarding digital evidence processing in an attempt to exclude the evidence, get a prejudicial position with the judge, or create reasonable doubt with the jury. Questions specific to the security of the evidence and proper processing are:

- Are the files original or have they been compressed or altered from the “first instance” state?
- How were they copied, ingested , imported etc.?
- Did the original file receive a proper hash value for authenticity?
- Are the files encrypted at rest?
- How were they sent, i.e., DVD, thumb drive, Dropbox, emailed?
- How are the files stored?
- Who has access to the storage?
- Is there an audit trail showing who accessed the files?
- Does this audit trail include IT/Storage admins who might access the files outside of the DEMS?

THE NINE PHASES OF DIGITAL FORENSICS

1 First Response



As soon as a security incident occurs and is reported, a digital forensic team jumps into action.

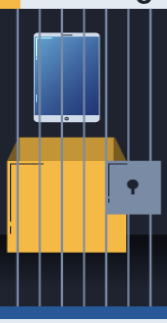
2 Search and Seizure

The team searches devices involved in the crime for evidence and data. Investigators seize the devices to make sure the perpetrators can't continue to act.

3 Evidence Collection

After seizing the devices, professionals collect the data using forensic methods to handle the evidence.

4 Securing of the Evidence



Investigators store evidence in a safe environment. In the secure space, the data can be authenticated and proved to be accurate and accessible.

5 Data Acquisition

The forensic team retrieves electronically stored information (ESI) from the devices. Professionals must use proper procedure and care to avoid altering the data and sacrificing the integrity of the evidence.

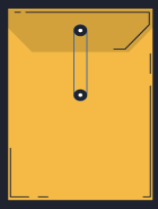
6 Data Analysis

Team members sort and examine the authenticated ESI to identify and convert data that is useful in court.

7 Evidence Assessment

Once ESI is identified as evidence, investigators assess it in relation to the security incident. This phase is about relating the data gathered directly to the case.

8 Documentation and Reporting



This phase happens once the initial criminal investigation is done. Team members report and document data and evidence in accordance with the court of law.

9 Expert Witness Testimony

An expert witness is a professional who works in a field related to the case. The expert witness affirms that the data is useful as evidence and presents it in court.

Law enforcement, prosecutors and the courts are questioning, in the current legal climate, if the evidence was processed properly and secure enough to withstand scrutiny. Is the evidence secure enough to be emailed and safe enough from unscrupulous IT/storage administrators? We are not advocating emailing evidence, just questioning if the process is safe enough to distribute via CD's DVDs, thumb drives, DropBox technology or other methods. Law enforcement agencies have their DEMS and storage managed by City IT or third-party companies. As employees come and go there are challenges in managing digital evidence access, distribution, and archiving. If personnel have direct access to digital evidence outside of the DEMS SW, then it is easy to take a look outside of the controlled environment via email, physical media, or third-party servers and storage.

Another risk in the workflow is when evidence has to be shared from the LEA, to prosecutors, to the defense counsel and to the courts. Each time this happens, the risk of it being viewed, copied, or altered by an unintended person increases. The need to protect the evidence at rest and in transit is more important than ever.

There are many reasons why digital media evidence must be distributed and all of them come at a risk if not properly processed, authenticated and secured from start to finish! Many agencies lack simple methods for distribution to be successfully achieved due to old technology, antiquated rules, budgets, and lack of personnel. As the volume increases, the need grows exponentially and **DWS's Data-Central** addresses properly and affordably solutions for evidence handling. **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