



**Robert Fried**  
Forensic Associate

“ I am constantly reminded of the infamous words of Sgt. Joe Friday of Dragnet: “Just the facts, ma’am”.

## A Day in the Life of a Forensic Examiner

by Robert Fried, Forensic Associate, DOAR Litigation Consulting

Digital forensics is a truly fascinating field that is constantly evolving. Essentially, digital forensics involves the identification, collection, documentation, acquisition and analysis of electronic data, in such a way that the integrity of the source media is preserved, as to allow for its admissibility in court. Using specialized hardware and software tools, “a true, exact copy” of a source media can be captured during the creation of a bitstream image. It is this ability to obtain an exact copy of the original evidence that makes digital forensics unique. When one thinks about forensics in the traditional sense, it is not uncommon to envision the collection and processing of evidence, at a crime scene, whereas for example, a small sampling of a powdered substance may be tested to see if it is a narcotic. However, with respect to digital forensics, the integrity of the original evidence is in no way compromised.

Digital evidence can be found in many different devices and can exist in various formats. It is no longer just the hard drive that is of interest. Other devices that may be of interest include: external hard drives, thumb drives, personal digital assistants, Blackberrys and even flash media commonly found in digital cameras, camcorders, and Global Positioning System (GPS) devices. In actuality, the list continues to grow with the passing of each day. It is the job of the DOAR Data Forensics team to properly identify and subsequently acquire the data stored on such devices. To help capture such data, the Data Forensics team is equipped with specialized software and hardware, which has been validated for its ability to preserve the integrity of the media contained within these devices.

In addition to having specialized tools in their toolkit, the Data Forensics team also utilizes specific protocols to document the devices and media which it acquires. One of the most essential aspects of documentation involves maintaining the chain of custody for each device/media to be acquired. DOAR’s Chain of Custody form is a document which keeps track of the movement of each piece of evidence from the time of its collection for preservation through the time it has been returned after being forensically acquired.

“ Digital evidence can be found in many different devices and can exist in various formats.”

Another aspect of documentation involves photographing the device and its associated media. Photographs are taken of the device’s make, model and serial number, and other labels that may be affixed to the device. Within each photograph will be a unique evidence number that has been assigned to the device. Similarly, the media associated with the device is photographed in the same manner. Most media has a physical label which specifies its technical details (e.g., make, model, serial number, capacity, etc.). These details, as well as any others, are captured by way of photographs, which can be referred to at any time.

The process of documentation continues with the DOAR Forensic Acquisition form. This form contains many different fields. The form helps to document specific details about the source device/associated media, the methodology/software utilized to create the bitstream image of the source media, as well as specific details about the target media. One of the most important of all the fields is that which contains the Acquisition and Verification MD5 hash values. A MD5 hash is a value based on a mathematical algorithm applied to a set of data. In a sense, a MD5 hash value can be thought of as a “digital fingerprint” to help identify specific data. The Acquisition MD5 hash value is calculated by the forensic acquisition software as the source device is being read. The Verification MD5 hash value is calculated by the forensic acquisition software based on the data contained within the bitstream images which reside on the target media. In order for a forensic acquisition process to be deemed successful, the Acquisition and Verification MD5 hash values must match; if they do not, something has changed on the source media during the process. If such a situation occurs, it needs to be properly documented and possible sources of error need to be articulated.

Once the integrity of the bitstream image obtained is verified, the evidence is transported to DOAR’s secure, Evidence Storage Facility. The evidence will remain in storage until a request for analysis is received from the client. When a request is made, a “working copy” of the evidence is created. A “working copy” is a copy of the bitstream image files from the original target media that are then saved onto a new target media. The “working copy” allows the examiner to maintain the original target media in secure storage where it can be retrieved, if needed.

“The work of a forensic examiner goes beyond acquiring and analyzing data.”

Requests for analysis can vary based on the nature of a litigation. Often, the scope of an analysis may be specified within a court order. Requests for analysis, for example, may include the extraction and inventory all user-created files (e.g., Microsoft Office type documents, Adobe PDFs, etc.) modified by a particular custodian during a specific time period. Another request may be to determine if a custodian utilized a thumb drive on their computer system or accessed a specific folder or file on their former employer’s network. Each request is specific, which helps to keep the analysis portion of the job both interesting and as rewarding. It is important to note that the smoking gun may not exist in every case; but when you help the client uncover details they would have otherwise been unaware of, it’s truly a great feeling.

The work of a forensic examiner goes beyond acquiring and analyzing data. It is also important for the forensic examiner to be able to articulate their findings by in a written formal report. The report provides details as to the methodologies and techniques employed throughout the course of the forensic acquisition and analysis process. The format of the report is easy to follow and the findings are discussed in such a way that an average reader with limited technical knowledge can understand what was done and what was discovered. The report is objective, with some subjectivity relating to conclusions that are drawn and recommendations based on the findings. Therefore, when writing a forensic report, I am constantly reminded of the infamous words of Sgt. Joe Friday of Dragnet: “Just the facts, ma’am”.

Once the client reviews the report, the forensic examiner may be requested to prepare an affidavit or to offer expert-witness testimony as to their findings, with. Therefore, it is essential for a forensic examiner to possess a strong technical understanding of how data is stored, where it can reside, and what methodologies are necessary to properly preserve its integrity.

At the end of the day, it is the forensic examiner’s ability to convey their knowledge and findings to a panel of jurors that is key!

#### About the Author:

Robert Fried is a Forensic Associate for DOAR's Discovery Consulting Group. In this position, Robert performs forensic acquisitions and subsequent analyses for the firm's clients. Prior to joining DOAR, Robert was a Computer Crime Specialist with the National White Collar Crime Center (NW3C) in Fairmont, WV. In this position, he was extensively involved in the instruction and development of basic and advanced computer forensics courses for local, state, and federal law enforcement agencies.

Robert Fried holds a B.S. and a M.S. in Forensic Science with a concentration in Advanced Investigation. In addition, he holds Certificates in Law Enforcement Science, Forensic Computer Investigation and Information Protection and Security from the University of New Haven and SEARCH (The National Consortium for Justice Information and Statistics). Robert is a member of the International Association for Identification (IAI), an Associate Member with the American Academy of Forensic Sciences (AAFS), and a member of the International Association of Computer Investigative Specialists (IACIS), from which he obtained certification as a Forensic Computer Examiner and for which he serves as a certification coach. In addition, Robert has attained the EnCase Certified Examiner certification, which recognizes mastery of computer investigation methodology as well as Guidance Software's EnCase computer forensic software during complex computer examinations.

Robert has been published in the area of digital forensics by organizations such as the SANS Institute and the High Technology Crime Investigation Association (HTCIA), and he has instructed at annual international conferences and organized events for the HTCIA and the IAI.