

## The DFRWS Framework Classes

Peter Stephenson

The DFRWS Framework classes contain key elements that are under constant review by the digital forensics community. However, there is a continuity between the classes that is important. For example, we note that the Preservation class continues as an element of the Collection, Examination and Analysis classes. This indicates that *preservation* of evidence, as characterized by case management, imaging technologies, chain of custody and time synchronization, is an ongoing requirement throughout the digital investigative process. Thus *preservation* is "...a guarded principle across 'forensic' categories.". *Traceability*, likewise, is a guarded principle, but not across all forensic categories. The following topics discuss each of the DFRWS Framework classes in more detail. Elements marked with an asterisk (\*) are required.

### The Identification Class

The identification class describes the method by which the investigator is notified of a possible incident. Since about 50% of all reported incidents have benign explanations<sup>1</sup>, processing evidence in this class is critical to the rest of the investigation. Likewise, as it is the first step in the EEDI process, it is the only primary evidence not corroborated directly by other primary evidence. Therefore, a more significant amount of secondary evidence is needed to validate the existence of an actual event.

The DFRWS gives the following definition of the Identification Class:

*"Determining items, components and data possibly associated with the allegation or incident. Perhaps employing triage techniques."*

The descriptions that follow of the elements of the individual Framework classes are those

---

<sup>1</sup> Author's experience over 20 years of conducting incident response

that we have adopted as specific definitions for the purposes of EEDI. The DFRWS has, as of this writing, not developed such definitions. Elements marked with an asterisk (\*) are required elements within the DFRWS Class. The elements of the Identification class are:

- **\*Event/Crime Detection.** This element implies direct evidence of an event. An example of such direct evidence is discovery of a large number of credit card numbers having been downloaded from a server.
- **Resolve Signature.** This applies to the use of some automated event detection system such as an intrusion system or antivirus software program. The system in use must make its determination (of the presence of an event of interest) by means of signature analysis and mapping.
- **Profile Detection.** Like signature resolution, profile detection usually relies upon some automated event detection system. However, in this instance, the event will be characterized through matching with a particular profile as opposed to an explicit signature. Signatures generally apply to an individual event. Events, however, may come together in an *attack scenario*, or *attack profile*. Such a profile may consist of a number of events, a pattern of behavior, or pattern of specific results of an attack.
- **Anomalous Detection.** Again, like the preceding two elements, this usually relies upon a detection system. However, in the case of anomalous detection, the event is deduced from the detection of patterns of behavior

outside of the observed norm. This is the classic Sherlockian case of the dog that did not bark.

- **Complaints.** This element relies upon the direct reporting of a potential event by an observer. The observer may observe the event directly or simply the end result of the event.
- **System Monitoring.** System monitoring explicitly requires some sort of intrusion detection, anti-virus or similar system in place. It is less specific than other elements requiring a specific action (e.g., anomaly, profile of signature detection) and may be used together with another element of this class.
- **Audit Analysis.** This element refers particularly to the analysis of various audit logs produced by source, target and intermediate devices.

## **The Preservation Class**

The Preservation Class deals with those elements that relate to the management of items of evidence. The DFRWS describes this class as "...a guarded principle across 'forensic' categories.". The requirement for proper evidence handling is basic to the digital investigative process as it relates to legal actions.

The DFRWS defines this class as:

*"Ensuring evidence integrity or state"*

- **\*Case Management.** This element covers the

management of the investigative process by investigators and digital forensic examiners. Typical in this element are investigator notes, process controls, quality controls, and procedural issues.

- **Imaging Technologies.** This element is separate from the elements in the Collection Class in that it does not refer to specific hardware, software or techniques. The imaging technologies element refers to the *technology* used for imaging computer media. For example, physical imaging or bitstream backup may be considered an appropriate imaging technology whereas a logical backup would not be. The term “imaging” as used here is rather broad. It encompasses not only the technology used to create an image of computer media, but also the technology used to extract such items as logs from a device. In this case the log might be extracted from a bitstream image or it might be read out of the device to a peripheral as a result of a keystroke command issued by the investigator.
- **\*Chain of Custody.** This element refers to the process of limiting access to and subsequent alteration of evidence. In most jurisdictions chain of custody rules require that the evidence custodian be able to account for all accesses or possible accesses to items of evidence within his or her care from the time it is collected until the time it is used in a legal proceeding,
- **\*Time Synchronization.** This element refers to the

synchronizing of evidence items to a common time base. Since logs and other evidence are collected from a number of devices during the conduct of an investigation, it is clear that those devices can differ from each other in terms of time base. If all devices are in a single time-synchronized network, they will not, of course, differ. However, that rarely is the case and some effort must be made to obtain a common time base for all devices. There are two approaches one might take. The first is to adjust all times on evidence to a common device. The second is to use a common time zone (TZ) such as Universal Time (UT) or Greenwich Mean Time (GMT) as a baseline. No evidence is modified. The investigator simply notes the variance of a particular log or other piece of digital evidence from the pre-determined time standard. This also is referred to *normalizing* time stamps.

## **The Collection Class**

The Collection Class is concerned with the specific methods and products used by the investigator and forensic examiner to acquire evidence in a digital environment. As has been noted, the Preservation Class continues as an element of this Class. With the exception of the Legal Authority element, the elements of this class are largely technical.

The DFRWS defines this class as:

*“Extracting or harvesting individual items or groupings.”*

- **\*Approved Methods.** This element refers to the

techniques used by the forensic examiner or investigator to extract digital evidence. The concept of being *approved* is somewhat different than one might expect. *Approval* refers to the general acceptance in courts of the techniques and training or certifications of the individual performing the evidence collection. The most rigorous test of methods and technologies is the Daubert test. However, due largely to the immaturity of digital forensic science, most court tests have not had this level of rigor applied. For this reason, those elements in this class that relate to approval derive their authority from cases where the technique, technology or product has been challenged in a court of the same level as the case in question and has survived the test.

- **Approved Software.** This element addresses the specific software product used to collect evidence. The discussion of the approval process above applies. There is an issue specifically involving software used for digital forensic data collection. In order for a software program to be considered approved it must be identical in every way to the software that has survived either a Daubert hearing or a court challenge. That means that the software source code must be in every way identical in both instances of the program. Failing that, the program may need to undergo its own court testing. For the purposes of the Framework and subsequent EEDI procedures, however, a program that has any differences (i.e., version level, bug

fixes, source code changes, etc.) from the program tested originally is not considered to be *Approved Software*.

- **Approved Hardware.** This element describes the hardware, if any, used to collect evidence. Usually this is not an issue unless the hardware is designed specifically for use in a digital forensic evidence collection environment. To a lesser extent the caveats of sameness that apply to approved software apply to approved hardware. The hardware device used must in every way be identical to instances of the device that have survived court challenges. The Approved Hardware element does not apply to simple computers, disks or other media used by the examiner to collect evidence unless the device was developed explicitly for digital forensic evidence collection and contains special unique features for use in that environment only.
- **\*Legal Authority.** The Legal Authority element is the only element of this class that is non-technical. In most jurisdictions some legal authority is required prior to extracting information from computer media. This authority could be a policy, a subpoena or a search warrant as examples. Failure to comply with applicable laws may render the evidence collected useless in a court of law.
- **Lossless Compression.** This element refers to the compression techniques, if any, used by backup, encryption or digital signature software used to collect

and/or preserve evidence. If the software program uses compression, it must be proven to be lossless, that is, to have no impact whatever upon the evidence on which it is used.

- **Sampling.** If sampling techniques are used to collect evidence, it must be shown that the technique has no impact upon the evidence collected, or, if it has, that the impact can be demonstrated clearly and unambiguously. It must also be shown that the sampling method is valid (generally accepted by the mathematical community) and that the conclusions that may be drawn from the sample are defined clearly.
- **Data Reduction.** When techniques and/or programs (such as normalization) are used to reduce data that contains or may contain evidence, it must be shown that such techniques or programs produce valid, repeatable, provable results that do not affect, in any way whatever, the evidence being collected. For example, using data reduction directly on evidence would alter the evidence and would not be acceptable. However, using such methods or tools on a copy of the evidence would have no direct affect upon the evidence. Its affect upon the analysis of the evidence (the validity of conclusions, for example) is an issue for the Examination and/or Analysis Class(es).
- **Recovery Techniques.** This element refers to the recovery of data that may contain evidence from a digital

device. It specifically describes the methods used by the forensic examiner to extract evidence using approved hardware, software and methods. While the elements of approved hardware, software and methods refer to the naming (or brief description of) the element and the connection between the element and the appropriate court test by which it is approved, this element describes in detail the actual process used to recover the evidence. By extension, when non-forensic methods are used to collect information (traditional investigation methods such as interviewing), we consider these techniques to be Recovery Techniques and we apply the same rules to them (e.g., Approved Methods, Legal Authority, etc.) as we would in a digital environment. However, we apply the rules in the context of the technique used.

## **The Examination Class**

The Examination Class deals with the tools and techniques used to examine evidence. It is concerned with evidence discovery and extraction rather than the conclusions to be drawn from the evidence (Analysis Class). While the Collection Class deals with gross procedures to collect data that may contain evidence (such as imaging of computer media), the Examination Class is concerned with the examination of that data and the identification and extraction of possible evidence from it. Note that the Preservation Class continues to be pervasive in this class.

The DFRWS gives the following description of this class:

*“Closer scrutiny of items and their attributes (characteristics)”*

- **\*Traceability.** This element is, arguably, the most important element in the EEDI process. It is the traceability and continuity of a chain of evidence throughout an investigation that leads to the credibility and correctness of the conclusions. According to the DFRWS “Traceability (cross referencing and linking) is key as evidence unfolds.”.
- **Validation Techniques.** This element refers to techniques used to corroborate evidence. Evidence may be corroborated in a variety of ways. Traditionally, evidence is corroborated by other, relevant evidence. However, digital evidence may stand on its own merit if its technical validity can be established. For example, a fragment of text extracted from an image of a computer disk may be shown to be a valid piece of evidence through various technical validation techniques. Its applicability or usefulness as an element of proof in an investigation may be open to interpretation, but that it is *valid* data would not be in dispute. A log, however, if extracted from a device that had been penetrated by a criminal hacker would require additional corroboration (validation) to show that the hacker had not altered its contents.
- **Filtering Techniques.** When dealing with evidence acquired from certain types of digital systems (such as intrusion detection systems) it is not uncommon to find that the gross data has been filtered for expediency by the system. While many intrusion detection experts would

agree that filtering at the source (the incoming data flow from sensors) is not as appropriate as filtering the display while preserving the original data, such source filtering does occur. This element requires that the investigator and/or forensic examiner determine and describe the filtering techniques used, if any, and apply the results of that description to the determination of the validity of the data as evidence. Another application of filtering is the extraction of potential evidence from a gross data collection<sup>2</sup> such as a bit-stream image of digital media. Some digital forensic tools use filters to extract data of a particular type such as graphical images. This element requires that the filtering technique be defined clearly and understood by the investigator or forensic examiner. These tools may also use the filtering technique of matching a known hash value to digital items on a gross data collection. Items that match the known hash are presumed to be the same as the item for which the hash value was originally generated. Again, the techniques and tools applied must be clearly understood by the investigator or the forensic examiner.

- **Pattern Matching.** This element addresses methods used to identify potential events by some pre-determined signature or pattern. Examples are pattern-based

---

<sup>2</sup> A gross data collection is a file or files containing data collected from a digital source that may contain individual evidentiary data.

intrusion detection systems and signature-based virus checkers. When the pattern or signature is unclear, ambiguous or demonstrates a large number false positives or negatives, the evidence and conclusion following from it are open to challenge.

- **Hidden Data Discovery.** This element refers to the discovery of evidence that is hidden in some manner on computer media. The data may be hidden using encryption, steganography or any other data hiding technique. It may also include data that has been deleted but is forensically recoverable.
- **Hidden Data Extraction.** This element addresses the extraction of hidden evidence from a gross data collection.

## **The Analysis Class**

The Analysis Class refers to those elements that are involved in the analysis of evidence collected, identified and extracted from a gross data collection. The validity of techniques used in analysis of potential evidence impact directly the validity of the conclusions drawn from the evidence and the credibility of the evidence chain constructed therefrom. The Analysis Class contains, and is dependent upon, the Preservation Class and the Traceability element of the Examination Class.

The various elements of the Analysis Class refer to the means by which a forensic examiner or investigator might develop a set of conclusions regarding evidence presented from the other five classes. As with all elements of the Framework a clear understanding of the applicable process is required. Wherever possible, adherence to standard tools, technologies and techniques is critical. Finally, when mapping this class to the DIPL or when performing model checking, we are concerned solely with the process, not the results of the analysis or the detailing of the contents of evidentiary items.

The Link element is the key element used to form a chain of evidence. It is related to traceability and, as such, is a required element.

This class is described by the DFRWS as:

*“Fusion, correlation and assimilation of material to for reasoned conclusions.”*

### **The Presentation Class**

This class refers to the tools and techniques used to present the conclusions of the investigator and the digital forensic examiner to a court of enquiry or other finder of fact. Each of these techniques has its own elements and a discussion of expert witnessing is beyond the scope of this thesis. However, for our purposes we will stipulate that the EEDI process emphasizes the use of timelines as an embodiment of the Clarification element of this class.

This class has the following DFRWS description:

*“Reporting facts in an organized, clear, concise and objective manner.”*