Fundamentals of Digital Forensic Evidence

Dr. Frederick B. Cohen, Ph.D.
Fred Cohen & Associates and California Sciences Institute

Introduction and overview

Digital forensic evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter, to help jurors establish the facts of the case and support or refute legal theories of the case. The exhibits should be introduced and presented and/or challenged by properly qualified people using a properly applied methodology that addresses the legal theories at issue. The tie between technical issues associated with the digital forensic evidence and the legal theories is the job of expert witnesses.

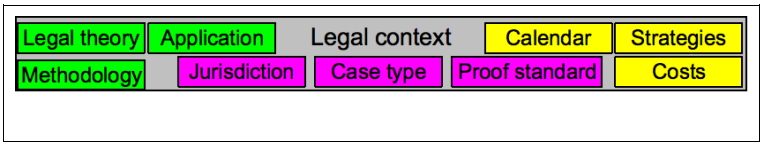
Exhibits are introduced as evidence by one side or another. In this introductory process, testimony is presented to establish the process used to identify, collect, preserve, transport, store, analyze, interpret, attribute, and/or reconstruct the information contained in the exhibits and to establish, to the standard of proof required by the matter at hand, that the evidence reflects a sequence of events that is asserted to have produced it. Evidence, to be admitted, must be shown by the party attempting to admit it, to be relevant, authentic, not the result of hearsay, original writing or the legal equivalent thereof, and more probative than prejudicial. Assuming that adequate facts can be established for the introduction of an exhibit, people involved in the chain of custody and processes used to create, handle, and introduce the evidence testify about how it came to be, how it came to court, and about the event sequences that may have produced it.

Digital forensic evidence is usually latent, in that it can only be seen by the trier of fact at the desired level of detail through the use of tools. In order for tools to be properly applied to a legal standard, it is normally required that the people who use these tools properly apply their scientific knowledge, skill, experience, training, and/or education to use a methodology that is reliable to within defined standards, to show the history, pedigree, and reliability of the tools, proper testing and calibration of those tools, and their application to functions they are reliable at performing within the limitations of their reliable application. Non-experts can introduce and make statement about evidence to the extent that they can clarify non-scientific issues by stating what they observed.

Digital forensic evidence is challenged by identifying that, by intent or accident, content, context, meaning, process, relationships, ordering, timing, location, corroboration, and/or consistency are made or missed by the other side, and that this produced false positives or false negatives in the results presented by the other side.

The trier of fact then must make determinations about how the evidence is applied to the matter at hand so as to weigh it against and in conjunction with all of the other evidence and to render judgements about the legal matters that the evidence applies to.

The legal context



Digital forensic evidence is and must be considered in light of the legal context of the matter at hand. This context includes, without limit:

- The legal matter determines the jurisdictions involved and thus the applicable laws and legal processes, the legal theories, methodologies, and applications of those methodologies that will be accepted, the requirements for admissibility of evidence, the requirements for acceptance of expert witnesses, the standards of proof, and many other similar things that impact the digital forensic evidence and its use.
- The nature of the case, whether it is civil or criminal, and sub-distinctions within these broad categories, affects the standards of proof and admissibly, the rules of evidence, the rules for trials, and many other aspects of what can and cannot be used in the legal matter and supported or refuted through digital forensic evidence.
- Limitations on elements of the case such as searches and seizures, which may be real-time or after the fact, compulsory or permission, and limited in various ways so as to prevent them from becoming "fishing expeditions" are informed by and help to form the context within which the digital forensic examiner must operate.
- Procedural requirements of legal cases may constrain certain arguments and evidence so that it can only be used at particular times or in particular types of hearings.
- The calendar is often daunting in legal matters, and in many cases there is very little time to do the things that have to be done with regard to digital forensic evidence. The calendar of the case may also impact the sequence in which evidence is dealt with, and this may result in additional complexities relating to the ordering of activities undertaken.
- Cost is an important factor because only finite available financial resource is available. While there may be an enormous range of analysis that could be undertaken, much of it may not be undertaken because of cost constraints.
- Strategies and tactics of the case may limit the approaches that may be taken to the digital forensic evidence. For example, even though some sorts of analysis may be feasible, they may be potentially harmful to the side of the case the forensic examiner is involved in, and therefore not undertaken by that side.
- Availability of witnesses and evidence is often limited. In some cases evidence may only be examined in a specific location and under specific supervision, while in most cases, witnesses are only available to the attorneys during limited time frames and under limited circumstances. For

the opposition to the party bringing the witness, these may be very limited and restricted to testimony under oath in depositions and elsewhere.

- Stipulations often limit the utility and applicability of digital forensic evidence. For example, if there is a stipulation as to a factual matter, even if the digital forensic evidence would seem to refute that stipulation, it can be given no weight because the stipulation is, legally speaking, a fact that is agreed to by all parties and therefore cannot be refuted.
- Prior statements of witnesses often create situations in which digital forensic evidence is applied to confirm or refute those statements. In these cases, the goal is to find evidence that would tend to refute the statements and thereby make the witness and their prior testimony incredible.
- Notes and other related materials are potentially subject to subpoena in legal matters, and therefore, conjectures on notes, FAXes, and drafts of expert reports as well as other similar material might be discoverable and used to refute the work of the experts. This tends to limit the manner in which the expert can work without endangering the case for their client.

There are many other similar legal contextual issues that drive the digital forensics process and the work of those who undertake those processes. And without this context, it is very difficult if not impossible to do the job properly. While it is the task of the lawyers to limit the efforts of the digital forensics evidence workers in these regards, it is the task of the workers to know what they are doing and how to do it properly within the legal context.

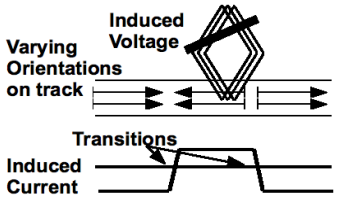


Figure 1 – The way floppy disks encode digital signals (from [2])

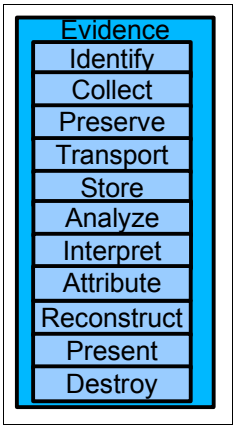
Digital forensic evidence consists of digital "bits", each of which is a '1' or a '0'; however, that evidence is realized in the physical world by physical mechanisms that, generally speaking, are not themselves digital. In some cases, the mechanisms by which the evidence was produced become part of the issue that must be addressed.

Those who engage in work related to digital forensic evidence must understand these issues at a rudimentary level in order to be useful to the legal process, and they must understand these issues and be willing to work within the context of the legal system and the specifics of the matter at hand in order to work in this area.

The processes involved with digital forensic evidence

While there are many other characterizations of the processes involved in dealing with digital forensic evidence (DFE), the perspective taken here will assume, without limit, the DFE must be identified, collected, preserved, transported, stored, analyzed, interpreted, attributed, perhaps reconstructed,

presented, and, depending on court orders, destroyed. [1] All of these must be done in a manner that meets the legal standards of the jurisdiction and the case.



Identification

In order to be processed and applied, evidence must first, somehow, be identified as evidence. It is common for there to be an enormous amount of potential evidence available for a legal matter, and for the vast majority of the potential evidence to never be identified. To get a sense of this, consider that every sequence of events within a single computer might cause interactions with files and the file systems in which they reside, other processes and the programs they are executing and the files they produce and manage, and log files and audit trails of various sorts. In a networked environment, this extends to all networked devices, potentially all over the world. Evidence of an activity that caused digital forensic evidence to come into being might be contained in a time stamp associated with a different program in a different computer on the other side of the world that was offset from its usual pattern of behavior by a few microseconds. If the evidence cannot be identified as relevant evidence, it may never be collected or processed at all, and it may not even continue to exist in digital form by the time it is discovered to have relevance.

Collection

In order to be considered for use in court, identified evidence must be collected in such a manner as to preserve its integrity throughout the process, including the preservation of information related to the chain of custody under which it was collected and preserved. Recent case law has established that there is a duty to preserve digital forensic evidence once the holder of that evidence is or reasonably should be aware that it has potential value in a legal matter. This duty is typically fulfilled by collecting and preserving a copy of the original evidence so that the actual original media need not be preserved, but rather, can continue to be used. Collection may involve many different technologies and techniques depending on the circumstance.

What is collected is driven by what is identified; however, a common practice in the digital forensics community has been to take forensically sound images of all bits contained within each media containing identified content. This provides the means to then identify further evidence contained within that media for subsequent analysis, assuming that the copy of the media was properly preserved along the way. The problem with this process today is that the volume of storage required has become very large in many cases, and this process tends to be highly disruptive of operating businesses that use these computers in a non-stop fashion. Consider the business impact on an Internet Service Provider if they have to cease operations of a computer that would otherwise be in use in order to preserve evidence.

Preservation of relevant log files and audit data is particularly important and should always be identified and preserved. This includes all logs associated with the servers used to send, receive, process, and store the evidence. Failure to do this becomes particularly problematic in cases when the purity of the evidence is at issue. For example, if an exhibit contains some corrupt content, the entire exhibit becomes suspect. If original records are not available to rehabilitate relevant portions of the exhibit, all of the evidence contained in the exhibit may be inadmissible. If there is suspicion of spoliation, the additional log files and related records will be necessary in order to show that redundant information exists that is consistent with the actual creation of the content at issue. Even information such as system crashes and reboots may be critical to a case because corrupt file content may be produced by those sorts of events and without the logs to show what happened when, that corruption may not be able to be reconciled with the need for preservation of the purity of the evidence.

> Many cases have hinged on log, audit, and other related data, if only to show that the other digital forensic evidence is real. And case after case today is being lost because of inadequate records retention and disposition policies and processes. Almost any case demands that evidence be properly identified and preserved, and that includes meta-data and log data, both locally and from independent third party sources who have no interest in the matter.

Transportation

Evidence must sometimes be transported from place to place. For example, when collected from a crime scene, the evidence must somehow be moved to a secure location or it may not be properly preserved through to a trial. Digital forensic evidence can generally be transported by making exact duplicates, at the level of bits, of the original content. This includes, without limit, the movement of the content over networks, assuming adequate precautions are taken to assure its purity during that transportation. Evidence is often copied and sent electronically, on compact disks, or in other media, from place to place. Original copies are normally kept in a secure location in order to act as the original evidence that is introduced into the legal proceedings. If there is any question about the bits contained in the evidence, it can be settled by returning to the original. Facsimile evidence, printouts, and other similar depictions of digital forensic evidence may also be transported, but they are not a good substitute for the original digital forensic evidence in most cases, among other reasons, because they make it far harder, if not impossible, to properly analyze what the original bits were. For example, many different bit sequences may produce the output depictions, and identical bit sequences may produce different output depictions. Care must be taken in transportation to prevent spoliation as well. For example, in a hot car, digital media tends to lose bits.

Increasingly evidence is transported electronically from place to place, and even the simplest errors can cause the data arriving to be incorrect or improperly authenticated for legal purposes. Care must be taken to preserve chain of

custody and assure that a witness can testify accurately about what took place, using and retaining contemporary notes, and taking proper precautions to assure that evidence is not spoliated and is properly treated along the way. [1]

Storage

In storage, digital media must be properly maintained for the period of time required for the purposes of trial. Depending on the particular media, this may involve any number of requirements ranging from temperature and humidity controls to the need to supply additional power, or to reread media. Storage must be adequately secure to assure proper chain of custody, and typically, for evidence areas containing large volumes of evidence, paperwork associated with all actions related to the evidence must be kept to assure that evidence doesn't go anywhere without being properly traced. Many different sorts of things can go wrong in storage, including, without limit, decay over time, environmental changes resulting in the presence or absence of a necessary condition for preservation, direct environmental assault on the media, fires, floods, and other external events reaching the evidence, loss of power to batteries and other media-preserving mechanisms, and decay over time from other natural and artificial sources.

Analysis, interpretation, and attribution

Analysis, interpretation, and attribution of evidence are the most difficult aspects encountered by most forensic analysts. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence; however, the actual number of possible sequences may be almost unfathomably large. In essence, almost any execution of an instruction by the computing environment containing or generating the evidence may have an impact on the evidence.

Since it is infeasible to reconstruct every possible sequence to find all of the sequences that may have produced the actual evidence in a any particular case, analysts focus in on large sets of sequences of events and tend to characterize things in those terms. For example, if the evidence includes a log file that appears to be associated with a file transfer, the name of the file transfer program included in the log file will typically be associated with common behavior of that program and used as a basis for the analysis. The user identity indicated in the log file may be associated with a human or group, and this creates an initial attribution that can then be used as a basis for further efforts to attribute to the standard of proof required.

Of course the presence of this record in an audit trail doesn't mean that the program was ever run at all or that the thing the record indicates ever took place or that the user identified caused the events of interest. There are many possible sequences of events that could result in the presence of such a record. For example, and without limiting the totality of possible event sequences, the record could have been placed there maliciously, it could be a record produced by another program that looks similar to the program being considered, it could

have been a record produced by the program even though the file transfer failed, the record could have been produced by a Trojan horse acting for the user, or the record could be there because of a failure in a disk write that produced a cross-link between disk blocks associated with different sorts of records.

The analyst seeking to interpret the evidence should seek to take into account the alternative explanations for evidence in trying to understand what actually took place and how certain they are of the assertions they make. It is fairly common for supposed experts to make leaps and draw conclusions that are not justified. For example, an analyst might write a report stating something like "X did Y producing Z" where X is an individual or program and Y is an action that produced some element of the evidence Z. But this is excessive in almost all cases. A more appropriate conclusion might be "Based on the evidence available to me at this time, it appears that X did Y producing Z". And of course it helps if some or many of the alternative explanations have been explored and shown to be inconsistent with the evidence. That's one of the reasons that seemingly irrelevant evidence might be very useful in a legal matter. For example, evidence from system logs might indicate that there were no detected disk errors, system crashes or reboots, or other anomalies reflected in the log files for the period in question, and that therefore, the explanations associated with these sorts of anomalies are inconsistent with the evidence. But without those log files or some other evidence, this conclusion cannot be reasonably drawn.

In networked environments, there are potentially far more sequences of bits that may be relevant to the issues in the matter at hand. As a result, there is potentially far more evidence available, and the analysis and interpretation of that larger body of evidence leads to many more potential analytical and interpretive processes and products. It could be argued that this increases the complexity of analysis exponentially, but in reality, the additional evidence tends to further restrict the number of histories that are feasible in order to retain consistency of interoperation across the evidence. As an example, the file transfer record identified above might be greatly bolstered or flatly refuted by corresponding records on remote systems from which the file was asserted to be downloaded and through which the transfer may have come.

Analysis, interpretation, and attribution of digital forensic evidence are also reconcilable with non-digital evidence and externally stipulated or demonstrated facts. As an example, if the digital forensic evidence appears to show that person X was present at the local console of a computer in Los Angeles, California two hours after they passed through customs and immigration in London, England, even though the network logs from distant systems show that the transfer took place, it is not a reasonable interpretation to assert that the individual was in Los Angeles. Clearly there is another explanation, whether it is two individuals, a remote control mechanism, alteration of multiple logs in multiple systems, alteration of customs and immigration logs, altered time clocks, or any of a long list of other possibilities. While in some venues, the "don't confuse me with the facts" approach may apply, in a legal setting, digital forensic evidence should reconcile with external reality.

Anchor facts that the analyst can testify to are a good example of the interaction between digital forensic evidence and physical reality. An example of an anchor fact is knowledge of time keeping mechanisms on systems that interact with evidence available in the matter at hand. For example, if the analyst operates a system that retains sound records and was synchronized to network time protocol during the period of time at issue, and that system has a record of an email passing through a relevant system that includes time and date stamps, then the time skew between the analysts system and the relevant system provides an anchor in facts that the analyst can use to make more definitive statements about what took place and when. Interpretation of the evidence can then more definitively assert that, based on the personal knowledge of the witness and the records they have of facts relevant to the matter, a particular record is consistent with a time skew of 18 hours. This may even allow the analyst to explain how the individual could have appeared to have been in London at the same time they appeared to have been in Los Angeles.

Reconstruction

In many cases, the relevance of the evidence is specific to hardware and/or software. While many analysts make the assumption that mechanisms operate according to their specifications, in the information technology arena, where digital forensic evidence originates, there are in fact few standards and they are liberally violated all of the time. Documentation is often at odds with reality, versions of systems and software change at a high rate, and records of what was in place at any given time are often scarce to non-existent. Legal cases also often come to trial many years after the actual events that led to them take place, and evidence that might have been present at the time of the incident at issue may no longer be available by the time is is known to be of import.

In these cases, reconstruction of the mechanisms that produced the records of import may be the only available approach to resolving, to a reasonable level of certainty, what actually could and could not have taken place. For example, if the content of the metadata within a document containing evidence of intent indicates that a particular user identity modified the document on a particular date and at a particular time and that the document was edited for 7 minutes and 23 seconds, but does not show specific modifications made by that individual, and a previous version of the document from an hour earlier written with another user identity does not have the content with the evidence of intent and has an edit time of 5 minutes, and no other documentation exists, then it might appear to be strong evidence that the individual who last wrote the document added the content indicative of intent and did so by editing the document for 2 minutes and 23 seconds.

But this conclusion depends on a set of assumptions surrounding the software in use for editing this document. Even if a current version of this software reliably applies this sorts of metadata, it may be that the version of software in use at the time in question and in the computing environments in question did something quite different. If this is the only evidence of the issue at hand, and the matter is

important enough to justify the effort, then a reconstruction of the process by which the digital forensic evidence was created may be necessary to show that the specific version of the software operating in the specific environment at issue could or could not have produced the results contained in the evidence and that other possibilities do or do not exist.

Given that a reconstruction is to be considered, additional determinations must be made. For example, based on the available information, how can a definitive determination be made about the version of the hardware, software, and operating environment be made, and how important is it to precisely reconstruct the original situation down to what level of accuracy and in what aspects? The answer to these and other related questions are tied intimately to the details at issue in the matter at hand.

Presentation

Evidence, analysis, interpretation, and attribution, must ultimately be presented in the form of expert reports, depositions, and testimony. The presentation of evidence and its analysis, interpretation, and attribution have many challenges, but presentation is only addressed to a limited extent in the literature. [1]

Presentation is more of an art than a science, but there is a substantial amount of scientific literature on methods of presentation and their impact on those who observe those presentations. Aspects ranging from the order of presentation of information to the use of graphics and demonstrations all present significant challenges and are poorly defined.

Destruction

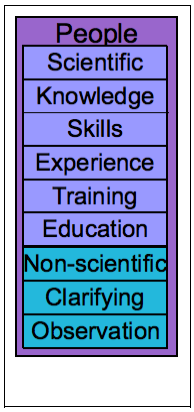
Courts often order evidence and other information associated with a legal matter to be destroyed or returned after its use in the matter ends. This applies to trade secrets, confidential patent and client-related information, copyrighted works, and information that enterprises normally dispose of but must retain for the duration of the legal process. Data retention and disposition has extensive literature involving legal restrictions on and mandates for destruction. [9]

There are also significant technical issues associated with destruction of digital data. The processes for destruction in legal matters rarely rise to the level required for national security issues; however, the efforts involved in evidence recovery do, at times, go the extremes. [10][11][14]

Expert witnesses

The US Federal Rules of Evidence (FRE) [3] and the rulings in the Daubert case [4] express the most commonly applied standards with respect to issues of expert witnesses and will be used as a basis for this discussion (FRE Rules 701-706). Digital forensic evidence is normally introduced by expert witnesses except in cases where non-experts can bring clarity to non-scientific issues by stating what they observed or did. For example, a non-expert who works at a company may introduce the data they extracted from a company database and discuss

how the database works and how it is normally used from a non-technical standpoint. To the extent that the witness is the custodian of the system or its content, they can testify to matters related to that custodial role as well.

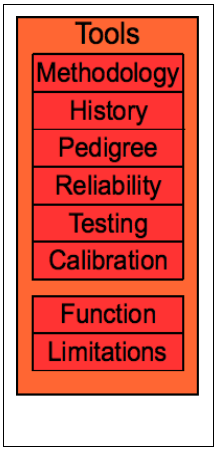


Only expert witnesses can address issues based on scientific, technical, or other specialized knowledge. A witness qualified as an expert by knowledge, skill, experience, training, or education, may testify in the form of an opinion or otherwise, if (1) the testimony is based on sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case. If facts are reasonably relied upon by experts in forming opinions or inferences, the facts need not be admissible for the opinion or inference to be admitted; however, the expert may in any event be required to disclose the underlying facts or data on cross-examination. [3](FRE Rules 701-706) as summarized in [1] (pp 127-8)

Experts typically have very specialized knowledge about specific things of import to the matter at hand. and anyone put up as an expert that doesn't have the requisite specialized knowledge is subject to being seriously challenged by competent experts and counsel on the other side. Experts who are shown to be inadequate to the task are sometimes chastised in the formal decisions made by the courts, and such witnesses are often unable to work in the field for a period of many years thereafter because counsel for the opposition will bring this out at trial.

Tools and tool use in digital forensics

Because digital forensic evidence is normally latent in nature, it must be viewed through the use of tools. In addition, tools are used in all phases of evidence processing. In order for tools used in forensic processes to be accepted by the legal system, the tools have to be properly applied by people who know how to use them properly following a methodology that meets the legal requirements associated with the particular jurisdiction. [3] (FRE 701-706)



One of the key things that experts need to know about is the tools that they use. This is because tools are used in almost all tasks associated with DFE processing and tool failures that yield wrong results or tool output that is not properly interpreted leads to opinions and conclusions that may be wrong. One of the main tasks of the DFE expert witness is to identify a meaningful methodology for applying tools to address the legal issues and use that methodology and tools that implement it with known accuracy and precision by examining the evidence and the claims made with regard to the evidence. While some of the claims may be understood with only the experts knowledge, such as assertions that are inconsistent with each other or that fly in the face of current scientific thinking in

the field of expertise, most claims in legal matters that involve DFE involve the application of scientific methodologies to evidence through tools.

Tools have history and pedigree that helps to indicate their reliability. Depending on the extent to which the tool provides scientific results that are not obviously verifiable by independent means by others, these factors are more important or less important. For example, if a tool, such as the Unix command "wc" counts the number of words, lines, and characters in a file, and the result is used to draw a conclusion about the evidence in the matter, it is something that can be readily confirmed or refuted by any party by simply counting, or in the case of files with many lines, using an independent tool. In this case, the history and pedigree are less important than that the tool has shown reliability at the task it is being relied upon to carry out, that it has been adequately tested, and that it be properly calibrated for its intended use.

Testing of tools is fundamental to their use, and in the field of DFE, an individual brought forth as an expert who has not tested their tools and does not know their function and limitations in adequate detail, is unlikely to be able to withstand cross-examination with regard to those tools or the things those tools are being applied to. This may, ultimately, lead to their disqualification as an expert, or the disregarding of their testimony as not meeting the standards required for credible expert testimony.

While testing of tools may be reasonably done by those who have background in testing of digital systems or by independent bodies, such as NIST, which performs select test of forensic tools in the United States [12], calibration must be done by the digital forensics expert prior to and after the use of the tool, assuming that that is required for validation of the tool's accuracy and precision to the level being used for presentation of the results of its use. Very little testing has been formalized in this field for the specific needs of digital forensics, so examiners wishing to be prudent should undertake their own testing programs, and this should be a normal part of the process used in preparing for legal matters where such tools are used. There is a substantial body of well defined knowledge in testing of digital systems, including refereed professional journals, books, conferences, and classes at the undergraduate and graduate level. As an example, the IEEE has had a refereed journal on the subject since 1984. [13]

The notion of calibration is foreign to many in the digital computer arena, largely because, unlike analog devices which have minor variances due to temperature, pressure, and other physical conditions, digital systems, when working within normal operating ranges, produce either 1s or 0s and do so with very high reliability. Nevertheless, there are calibrations that can and should be done prior to and after the use of DFE tools to validate that what was done did not introduce inaccuracies into the process. As an example, when doing a forensic image of digital media to a different media, the destination media should be pre-configured to a known state so that process failures can be detected. Otherwise, residual data from previous events or from the manufacturing process might be mistakenly intermixed with the new DFE to produce corrupted results. This sort of spoliation has the potential to create enormous problems if the tools and

media are not properly calibrated, if error messages are not carefully preserved and taken into account, if contemporaneous logs of the forensic activities are not produced and retained, and if evidence isn't created to verify that the image taken is a true copy of the original evidence. This is similar to the process of cleaning a pipet for a chemical analysis, testing the cleaned pipet to verify that it is free of contaminants, processing the sample, getting the result, then verifying that the pipet is free of contaminants after the sample is analyzed. Failure to undertake such a process would violate standard procedure in chemical testing that has been shown to produce faulty chemical analysis. Similarly, failure to undertake measures to calibrate and verify digital forensic processing of evidence can introduce contaminants or produce faulty digital analysis.

Digital forensic analysis processes often include the creation of special purpose filters, the development of search criteria, and the authoring of small computer programs, sometimes including combinations of scripts written in languages such as the command language of the Unix shell, the Perl language, and other programs written in other languages, and pre-packaged utility programs that come with systems, such as the stream editor "sed", the regular expression string search program "grep", and many other similar sorts of elements. These are commonly combined with tools that retrieve data from Internet sites and process them in various ways to produce outputs that show some analytical result.

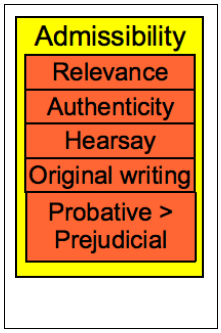
When such tools produce results that are readily verified by inspection, such as counts of how many lines of particular types were at particular locations within particular files, the conclusions themselves constitute a testable result that the opposition can challenge and verify. As such, the tools and techniques need not be shown; however, when introducing such evidence, it is incumbent on the producing party to make certain that the results are accurate and precise. To the extent that they are in error and the opposition can demonstrate this, the court will often levy sanctions and potentially exclude the expert and the results from use in court under the admissibility restriction that the results are less probative than prejudicial, the expert witness is not reliably applying a scientific method to the evidence, and that the expert is not in fact adequately knowledgeable or skilled to express scientific opinions to the trier of fact. It is incumbent on experts to provide details of the limits of their results in terms of the limits of accuracy and precision and to not overstate results. For example, when analyzing text files against a format specification, the expert had better understand the extent to which the formal specification is reflected in actual use, and examine results produced for anomalies before declaring the results of the program to be precise and accurate. To the extent that anomalies are detected, they should be explained and the precision and accuracy of results properly characterized.

Challenges and legal requirements

In order to be accepted in a legal proceeding, certain requirements apply to evidence and expert testimony relating to that evidence. On a global level, the

most commonly applied standards are similar to the U.S. Federal Rules of Evidence [3] and the Daubert decision [4].

Legal challenges to admissibility under the Federal Rules of Evidence in the US generally go under the following categories. Evidence admitted has to be weighed by the trier of fact in making determinations. Depending on specifics of the circumstances and judicial opinion, evidence may or may not be admitted and weight may be expressed by the judge to the jury in formal admonitions for admitted evidence to go to weight.



Relevance: The tendency for evidence to make a fact of consequence determination of the action more or less probable than it would be without the evidence.

Authenticity: Rules 901-903. There is evidence sufficient to support a finding that the matter in question is what its proponent claims. Many illustrative examples are provided, but they are not exhaustive. They include personal knowledge, non-experts familiar with a unique property such as handwriting, comparisons to known samples by trier or experts, distinctive characteristics, public records, ancient documents, reliable process or system, and methods provided for by statute or rule. Some records may be self-authenticating, such as public documents, certified copies of documents, official publications, and certified records of regularly conducted activity.

Hearsay: Rule 801. An out of court statement offered in evidence to prove the truth of the matter asserted is hearsay, but there are many exceptions; most notably business records taken in the normal course of business and relied on for their accuracy and reliability as a matter of course in carrying out that business.

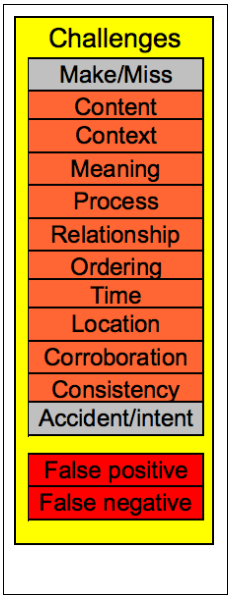
Original writing (best evidence): Rules 1001-1008. To prove content, the original is required unless certain exceptions apply. Exceptions include: (1) originals lost or destroyed, (2) original is not obtainable, (3) the opponent who holds it refuses to produce it upon judicial demand, (4) the content is not closely related to the matter at hand and is thus collateral. Official records are admitted as duplicates. Voluminous records may be represented by statistical samples when they are representative and subject to examination of the originals out of court. When the admission of other evidence depends on facts in this evidence, the court makes the determination, otherwise it goes to weight. When the issue is whether (a) the asserted content ever existed, (b) another piece of content admitted produced it, (c) the evidence in question accurately represents the original, the trier of fact determines it.

More prejudicial than probative: Rule 403. Evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by the considerations of undue delay, waste of time, or needless presentation of cumulative evidence

Scientific evidence (expert testimony): Rules 701-706, Frye, Daubert. Non-expert testimony is only admitted if it is (a) rationally based on the perception of the witness, and (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue, and (c) not based on scientific, technical, or other specialized knowledge within the scope of expert testimony. A witness qualified as an expert by knowledge, skill, experience, training, or education, may testify in the form of an opinion or otherwise, if (1) the testimony is based on sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case. If facts are reasonably relied upon by experts in forming opinions or inferences, the facts need not be admissible for the opinion or inference to be admitted; however, the expert may in any event be required to disclose the underlying facts or data on cross-examination.

The Daubert case [4] dominates in US Federal cases. Frye [5] may apply in many states for non-Federal cases. The Frye standard is basically: (1) whether or not the findings presented are generally accepted within the relevant field; and (2) whether they are beyond the general knowledge of the jurors. Daubert also allows accepted methods of analysis that properly reflect the data they rely on.

In order to be admitted, digital forensic evidence must survive challenges to relevance, authenticity, its hearsay nature, the original writing requirement, must not be far more prejudicial than it is probative, and must be introduced and analyzed by people who meet standards. It is incumbent on the party introducing evidence to meet these criteria and on the party challenging to oppose based on these criteria and to do so in a timely fashion as part of the legal process. Experts can help make this happen by identifying all lines of challenge and providing expert analysis, advice, knowledge, and skills to help create the conditions for challenges.



In cases where there is a lot at stake for the parties involved, DFE is likely to be challenged in significant ways. The basic challenges to DFE can be made to a greater or lesser extent at every step of the process, for every item of evidence, and for every witness presented. The challenges may be thought of in terms of a specific set of known fault types that form a fault model. [1]

Make or miss faults

In the fault model discussed in [1] faults are characterized as errors of omission, commission, or combinations thereof, sometimes called errors of substitution. Errors of omission are also called "miss" faults because they miss an evidence identification, collection, preservation, transportation, storage, analysis, interpretation, attribution, reconstruction, presentation, or destruction (process) step or miss content, context, meaning, relationship, ordering, time, location, corroboration, or consistency results. Errors of commission are also called "make" faults because they introduce evidence

process steps that should not be present or assert content, context, meaning, relationship, ordering, time, location, corroboration, or consistency results that are not real.

Accidental or intentional faults

Accidental miss faults are practically impossible to avoid because there are a potentially unlimited number of different analytical methods and processes that could be applied to evidence, any of which might produce something of relevance.

Accidental make faults are normally the result of inadequate attention to detail, lack of expertise, a non-systematic process, or a lack of thoroughness. These faults are particularly problematic because they produce interpretations that claim things that are not true. The lack of adequate time to thoroughly investigate issues leads to make faults because, in the process of investigation and analysis, theories are produced and tested. The human mind tends to make leaps that are the source of human intelligence, but these leaps may or may not be right. A lack of time, care, or expertise, leads to the acceptance of these theories as if they were facts without adequate verification, or their presentation as definitive when they remain somewhat speculative.

Intentional miss faults are commonplace, particularly in adversarial situations. Each side tends to leave out the things that the other side might find helpful to their case and to focus on the issues that best make their own case. Counsel sometimes limits the information available to DFE experts so that they only see the things that tend to aid the client in their case. The DFE expert should be aware that limited information leads to excessive conclusions and take care in drawing conclusions to explicitly state the limits of their conclusions and their basis. If the basis changes, so might the conclusions. Experts who intentionally ignore facts in front of them and draw conclusions that are contradicted by those facts are likely to face serious and justified challenges.

Intentional make faults are almost always fraudulent in nature. Making up evidence or creating conclusions that the expert knows to be false are unethical and in most cases illegal and sanctionable. The DFE expert should seek to identify intentional make faults by verifying results using redundant methods and verifying evidence consistency through analytical methods. Intentional miss faults are often used to cover up intentional make faults. For example, when identifying evidence, such as log files associated with computers that generated other evidence in the case, the party who produces detailed records of one sort but refuses to provide, intentionally destroys, or fails to adequately retain records of related sorts, should be suspected of fabricating the detailed evidence that they proffer. The DFE expert should identify this issue clearly and assert the potential of spoliation of the detailed evidence provided. If that evidence has internal inconsistencies, the case for intentional spoliation becomes stronger.

False positives and negatives

Faults are important to legal matters when they produce erroneous results or conclusions. The mere presence of an accidental miss does not imply that the expert drew incorrect conclusions or that the evidence doesn't support the matter at hand. In order for a fault to rise to the level of importance that makes it worthy of a legal challenge, that fault should normally produce an error that is material to the case. Even intentional fabrication of evidence doesn't always produce errors that are material. For example, someone who accidentally destroyed a file and created a new version in its place without telling anyone, augmented their accidental miss into an intentional make, but that doesn't mean that the result was inaccurate, only that its pedigree is questionable.

The DFE expert should identify relevant faults, but it is far more important to identify the faults that produce errors and put those errors into the proper legal context. The net effect of faults that are meaningful can be characterized in terms of two kinds of errors; false positives and false negatives.

False positives are results indicating something as true when in fact it is not true. For example, the detection of a condition when the condition was never in fact present, the attribution of an action to a party who did not in fact take that action, or the claim of the presence of contraband when in fact it was not present.

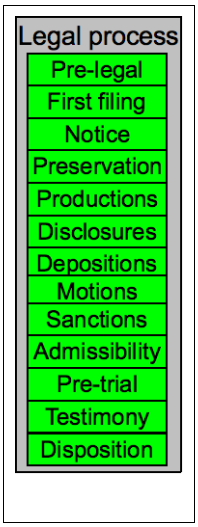
False negatives are results indicating that something was not true when in fact it was true. For example, the failure to detect the presence of a break-in to a computer that was supposed to be reliably storing evidence when claiming that the computer was not broken into, the failure to attribute an action to an actor when it can in fact be attributed reliably based on available information, or the claim of absence of contraband when contraband is in fact present.

In many cases, these sorts of errors are the result of DFE experts making statements that are overly broad, excessively definitive, or otherwise stated as unilateral and sweeping when they are in fact accurate only for a more limited set of conditions. But in other cases, these are simply the result of process errors in which some key piece of evidence was not properly identified, collected, preserved, etc. or in which something that was not in fact reliable was treated as if it were reliable.

The Legal Process

Legal matters start before any legal filing takes place, and at any time, any system or content might be involved in some aspect of a sequence of events that ultimately leads to a legal matter. As a result, the processes associated with DFE should be part and parcel of every entity's operations at all times. There are defined legal duties to protect and preserve DFE and these have been substantially explored in the literature. [9] The discussion provided herein is based on a loose interpretation of the sequence of events that takes place in legal matters. The actual sequence depends on the specifics of the jurisdiction, the matter at hand, the parties involved, and other case-specific factors.

Pre-legal records retention and disposition



Before the first paper is filed for a legal proceeding, entities have responsibilities to preserve evidence that could be reasonably anticipated to be involved in litigation. For corporate entities, this entails the creation and operation of a policy and process associated with records retention and disposition. For individuals, the standards are far more lax; however, any situation in which a legal matter is anticipated leads to duties to preserve evidence. The simplest strategy for individuals is to do regular backups of digital information and, if a legal matter seems to be looming, make a copy of everything and put it somewhere safe. For corporate entities and other businesses, government entities, or organizations, the issue is far more complicated.

Entities have a responsibility to preserve their records for many legal reasons as well as for reasonable and prudent operations. [9] Some records, such as contracts, publications, historical data associated with patents and other intellectual property, prices charged, and fees paid, are retained for business and legal reasons as evidence of the activities of the entity. Other records, such as records of expenditures and income, are retained for external legal reasons such as government regulations and meeting reporting requirements. Still other records, such as electronic mail, internal memoranda, operating manuals, and notes on when what happened, are retained for internal use, entity long-term memory, and convenience.

Where there is a legal mandate to retain records associated with regulatory bodies, such as tax records, records of controlled substances, employee records, and so forth, entities must retain these records for the legally mandated period, and the entity record retention and disposition process should define these minimum times and identify disposition processes and times after legal limits are reached. Where no such mandate is in place, entities should operate for their own operational efficiency, effectiveness, and convenience, should codify these operational, efficiency, and effectiveness requirements and decisions, and should follow these decisions rigorously. In addition, statute of limitations requirements limit the utility of certain information in certain circumstances, and these statutes should be built into the records retention and disposition process in helping to make decisions about time frames. In all cases, a well-defined retention and disposition process should be in place, operated, and verified in its operation. A legal hold process should also be defined and put in place to assure that prior to disposition of any records that can reasonably be anticipated to be required for any legal proceeding, all legal holds on those records are cleared, and when a legal hold has cause to be in place, appropriate records are preserved and prevented from being disposed of.

Prior to the first filing, and contemporaneous to events of interest, it is important to identify, collect, and assure the proper storage and handling of any content that might be involved in a legal matter. Perhaps the most important things to do contemporaneously are things that can preserve evidence that tends to change

over time or will not exist past a particular time frame. For example, network traffic and voices disappear as they are consumed unless explicit preservation is undertaken at the time they occur. When investigating or acting on digital forensic evidence or matters related thereto, it is often helpful to take notes at the time the activities are undertaken and to retain them as contemporaneous evidence of what took place. Similarly, things like network addresses and host names, network-based lookups, and related information, including versions of software in use and other related configuration information, should be collected contemporaneously because these things tend to change with time, and records of their changes are not uniformly kept. Contemporaneous time and date information, when relevant, performance levels, as measured at the time, and justifications for decisions, as they are made, are best documented contemporaneously.

Digital forensic experts brought in prior to the legal process may be used for a wide range of efforts, including without limit, internal investigations, preparation for potential legal work, the creation of forensic data collection and processing capabilities, analysis of potential evidence, and so forth. While these may seem like they have a lower standard of care than work during the legal process, the DFE expert should realize that the work they do in preparation may end up questioned at trial, and reasonable and prudent efforts should be applied, proper contemporaneous information should be collected as appropriate to the matter at hand, and all of the elements of the evidence process should be respected, even though no legal action has been filed.

First filing

As of the first filing in a legal matter, a series of events with time limits start to occur. Historical events that apply to the legal matter are limited by statute of limitations limits depending on the nature of the charges and specifications and the jurisdictions that apply. The Constitution of the United States [15], as well as many other similar legal mandates from other jurisdictions, requires (in the 6th amendment) "In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial,...". The right to a timely trial means that from the first legal filing to the start of the trial must be speedy. But beyond this, courts set calendars and require that they be met. Late filings result in adverse rulings, and as a result, there is often a rush in the legal system for those who are working on issues related to evidence.

In most legal matters, before the force of legal process can be used to secure and process evidence, a legal action must be filed. For example, before a subpoena can be issued, a lawsuit normally has to be filed. The first filing then triggers notice and preservation requirements and allows legal papers to be filed to compel actions on parties.

Notice

Notice is given of various things during the legal process, starting with notice of the existence of a legal action. Various sorts of non-disclosure, confidentiality,

work product, documentation, and other sorts of requirements are given in various forms throughout the legal process. Because the legal environment tends to be relatively unforgiving of those who fail to comply with judicial orders and similar things, it is important to respect all of the notices given and to communicate all such notices with appropriate legal staff in a timely fashion. In the case of an entity that is given notice of a legal matter, it is important to start the legal hold process within the data retention and disposition process, and to immediately and accurately identify, collect, and preserve all relevant evidence. Once notice is given, there is a duty to preserve evidence.

Preservation orders

In many cases, preservation orders are given with respect to evidence. It is important to get timely preservation orders in order to assure that critical evidence is not lost. The DFE expert is often called upon to assist the legal team in identifying the sources and nature of evidence that should be sought, and this is often codified in preservation orders and the language of demands for evidence. Timeliness requirements stem largely from the data retention and disposition issues related to different entities. For example, many Internet Service Providers (ISPs) only retain records for periods of days to weeks, and in some cases, intentionally avoid retaining records to facilitate anonymity for their clients. Jurisdictions sometimes mandate preservation of particular data, like calling information not including the content of calls, as part of their national security or other legal mechanisms, but gaining access to this sort of data requires effort on the part of the legal team, and the costs of such actions may exceed the value they bring to the legal matter. Courts often rule, particularly in civil matters, that the value of the evidence in terms of its probative utility is exceeded by the cost of production, and this effectively limits the preservation and production process in some cases.

Disclosures and productions

Documents are typically produced either as part of disclosures made by the parties or as productions in response to legally authorized demands by parties. These productions and disclosures constitute the bulk of the digital forensic evidence in most cases, but they also include information that brings context to the evidence, including the claims being made, assertions by the parties, and the basis for those claims and assertions. Analysis of the evidence should yield results that are consistent with truthful disclosures. When there are inconsistencies, or when the basis is not adequate to support the contentions made in the claims or disclosures, the digital forensics expert is typically tasked with identifying and clarifying such inconsistencies and lack of basis, and the results of these efforts form the basis for effective challenges to the evidence and the legal case.

Disclosures and productions are often applied tactically by the parties to make their case while preventing challenges. For example, it is fairly common for parties to disclose printed copies of digital information but not offer the digital

forensic evidence. In such a case, it is the responsibility of the other side to demand original writing in digital form so it can be forensically analyzed. Large volumes of data are sometimes provided and select data contained within those large volumes may contain the key information required to understand what took place. It is the responsibility of the party receiving such volumes of data to go through it all and, when that data indicates the presence of other systems or content, to identify those systems and content for further demands of disclosure.

To the extent that a disclosing party intentionally subverts the process and intentionally creates high levels of effort by the other party without basis, it is sometimes possible to get sanctions against the offending party, particularly when the aggrieved party can show that the other side knowingly and intentionally misled. The DFE expert that identifies such instances and helps to bring about those sanctions is bringing added value to their side of the case because the other party may have to pay for the cost of much of the legal effort and the fees of the expert in analyzing materials that were needlessly produced when they were known to be irrelevant, or productions that were contrary to the judicial orders in the matter.

The DFE expert will often write a report on a legal matter and this report will be disclosed to the other parties at some point in time. For a discussion of such reports, the reader is advised to review [1].

Depositions

Depositions are testimony given with lawyers present and a legal recording made of the proceedings. The questions are typically asked by the other side, and the answers are sworn testimony that bears all of the same requirements of testimony in open court. Witnesses, including experts, are typically deposed prior to trial so that the attorney's can gain valuable information related to the matter at hand and to which they have a right. The right to face one's accuser [15] (the fifth amendment) includes the right to question them and any and all witnesses that may be brought. The means that the DFE expert who will ultimately write a report or testify in open court will be deposed and that the DFE expert may be asked to offer assistance to lawyers who will be deposing the opposition when the issues relate to DFE.

DFE experts brought in to help lawyers prepare for depositions have a somewhat different role. For example, they may help to identify and prepare items of evidence that will be used in questioning a witness. They may help the legal team identify the proper sequence in which to present questions in order to make a series of legal points and provide specific items of evidence that allows those questions to be pursued one after the other. For example, to get a witness to admit that they don't know how a process used to develop evidence actually took place, they might provide an example for the lawyer to show the witness with a set of specific questions related to the piece of evidence. Depending on the answers given, different following items of evidence might be presented that show that the answers given were not correct. The witness may end up contradicting themselves, or admitting the limits of their knowledge of the facts in

the case, and this might result in the evidence and the witness losing their credibility. Of course the same may be done by the opposition, and that's why the DFE has to understand these issues even if they are not being asked to help the lawyers prepare for a particular witness.

As the subject of depositions, the DFE expert has a legal obligation to tell the truth, and of course failure to do so may result in enormous problems and legal implications for the expert. But this is only the beginning of the issues that the expert faces. Great care should be taken in answering questions and great precision should be sought in the application of those answers. In many cases, experts answer too quickly, interrupt the questioner, don't answer fully, answer things that were not asked, and make other similar mistakes. [1] Preparation for depositions should be undertaken with the lawyers in the case, and it is always advisable to do a practice deposition the day before the real one to reduce the stress and get a sense of the sorts of questions that will be asked in the particular case and to make certain that the answers are precise, accurate, and address the questions. The DFE expert should think through the totality of issues involved in the matter and recognize the limits of what they may be able to testify about as well as the features so that they are prepared for the potential sequences of evidence and questions they may be asked.

Motions, Sanctions, and Admissibility

Motions in legal matters are often accompanied by expert reports relating to the evidence, and when the evidence in question is digital in nature, the DFE expert will likely end up writing those reports, or at least signing off on declarations written by lawyers. It is vitally important that all such declarations and reports in support of motions or use din legal matters be carefully written and as precise and accurate as the expert can make them. While most non-legal environments instill a sense of coming to consensus and writing an agreeable work product that others will like or buy into, in the legal environment, and particularly in support of motions, it is the precision and accuracy of the product that matters. In such a situation, the DFE expert is writing an opinion based on facts and properly applying a scientific methodology. The DFE expert is the final authority on such a report and must not be convinced by others to say things that they do not truly believe to be the case or things that they do not believe can be demonstrated by the proper application of scientific methodology to evidence in the case.

Typically, the results of such writings are "facts" asserted to be true by the side proffering them. The other side has an opportunity to dispute these facts, but if they are undisputed, they become legal facts for the case, and as such, constitute the basis for the trier of fact to make a judgment. If they are disputed, the other side had better have an expert who also has a scientifically based methodological approach that, using the same evidence, shows that the things one expert asserts as fact are not in fact true. This direct sort of difference of opinion is relatively rare when properly qualified experts testify in legal matters, and in the case of DFE, it is almost never the case that the experts disagree on

the bits. Almost all interpretation of the bits in the DFE arena are testable, and the other side may well test them as the DFE expert may be asked to test them when presented by the other side.

Motions can also result in the exclusion of evidence that may be vital to a case, limits on the interoperation of evidence, the removal of an expert from a case, or any of a wide range of other outcomes, including the end of the proceedings and termination of the case. Motions are used to get sanctions, limit admissibility, and for essentially all other aspects of a legal matter.

Pre-trial

In addition to motions and other legal maneuvering, before trial, DFE must be analyzed, interpreted, attributed, sometimes reconstructed, and prepared for presentation. This includes the preparation of reports, exhibits, and demonstrations, preparation for testimony, and assistance in challenging the testimony of others.

Report preparation consists largely of describing the context of the report and the background of the individual preparing it, the processes and tools used related to the evidence at hand, the interpretation and attribution of the evidence in light of the case, and expert opinions related to the evidence and the context of the case. Depending on the specifics in the matter and the interests and requirements of the legal situation, the report may contain many citations and attachments. In some cases, very short reports are provided, and many lawyers believe that judges will not read more than a few pages of an expert report, but some cases call for a great deal of detail, cover hundreds of thousands of claimed items of evidence, and involve many complex issues.

Preparation of exhibits that support expert opinions have to be accepted by the court and meet standards of admissibility, including being reviewed by the other parties to the case and challenged for all of the factors involved in admissibility. Complex areas of digital forensics may include a short tutorial given to the trier of fact on the underlying operation of the systems involved, such as a depiction of what an IP datagram consists of and how a particular protocol works, with examples provided that are relevant and that demonstrate the issues in the case. Demonstrations, such as a live session where an email is sent using manual entry of the protocol elements, it is received by a receiving computer, and the logs and output generated are shown to the jury are far less common than written reports with examples demonstrating these activities and assertions that these accurately represent the events that transpired. This is not only because live demonstrations are less reliable than pre-recorded ones, but also because these sorts of reconstructions are sometimes more prejudicial than probative, take a lot of time, and are rarely important enough to the legal matter to justify their use. They are also subject to challenges and live counter-demonstrations, and are thus problematic. The most common type of evidence shown to a jury is a computer printout or a large chart that is prepared before the trial and used to bring clarity to the trier of fact. Increasingly, courts are using video displays to show these sorts of charts and other similar evidence, and these technical

means of presentation have to be prepared, shown to the opposition, and presented as evidence supported by expert testimony.

Notes, draft reports, emails, FAXes, and other exchanges of information of which there are records, are often subject to discovery by the other side. As a result, in the pre-trial phase, it is important to use special care in handling and creating these materials. In many cases, counsel makes the requirements for such handling clear in advance of the work by the expert. But in all cases, the well prepared expert should anticipate the needs of handling for DFE and have systems and processes in place to avoid the pitfalls before falling into them. [1]

Testimony

The expert or lay witness who presents digital forensic evidence in front of the triers of fact normally does so live and in person. The members of the jury or the judge trying the case are typically sitting within a few feet of the witness who is asked specific questions similar to those given in a deposition. Evidence is brought up in front of the court and is readily visible to the witness and trier of fact as the expert explains what it is, how it came to be, how it is interpreted, and what it means. Cross-examination allows other parties to ask questions about the evidence and the opinions, and to identify inconsistencies between what is said at trial and what was said in reports and depositions.

Most judges and juries do not have expertise in computers, programming, electronics, or other aspects of DFE, just as they usually know little about the chemistry of DNA or the fluid dynamics of blood as it splatters. As a result, the expert witness is tasked with educating the trier of fact about the underlying facts and the nature of the systems that create, process, store, communicate, and present the DFE. For this reason, the expert usually has a lot of explaining to do, and much of it is about things that most experts find to be rudimentary. However, this explaining lays the foundation for the detailed conclusions and opinions that the expert gives and that make the difference in the case, and it must be accurate and precise, while still explaining the issues to people who don't know much about the subject. As such, it is a challenge.

This explanation of detailed scientific methodology and its proper application applies to each and every step of the process associated with the evidence, and each of those steps may be challenged by the other parties to the case. It is vital that the expert testifying about such evidence be able to explain why they have the opinions they have, how they came to those opinions, and at a detailed level, the mechanisms that cause the opinion they give to be correct. Legal cases have turned on experts who were or were not able to explain the operation of the file system from which they collected DFE and how that file system is used by the low-level system calls within the operating system on the computer that was examined. It is all too easy to answer questions in such a way that they are easily challenged, to assert knowledge that is not really clear, to become sloppy and make guesses, to make a miscalculation, or to make other sorts of errors, particularly when answering complex questions in real-time in front of strangers.

Case closed

After all of the other aspects of a case are done, regardless of who wins or loses, the DFE often has to be disposed of in keeping with court orders. Legal matters rarely require that the evidence be destroyed using techniques that are difficult to apply, but it is common that confidential information must be removed using reasonably sound techniques so as to assure that it is no longer available to the expert or anyone else. This includes backup copies, data collected by internal search mechanisms, cached copies, copies on paper, tape, and other media, and residing on all affected systems and peripherals. For this reason, it is useful for the DFE expert to use special precautions when originating, processing, and storing matters related to legal cases so that the back-end process does not become complicated or overly burdensome. While it is prudent to keep backups, it also implies the need to remove copies from those backups.

Duties

While duties have been discussed throughout this article, it is worth the effort to reiterate the major duties identified for digital forensic evidence with regard to experts and entities.

Honesty, Integrity, and Due Care

While it may seem obvious, those working in the digital forensics field have special requirements for honesty, integrity, and diligence in their work. Above and beyond the normal level of care seen in common use, those working in legal settings really should meet a higher standard.

Previous writings, public statements, legal proceedings, and other records of past performance are all subject to challenge in legal settings, as long as they are relevant to the issues in the case, which in the case of an expert witness, includes their credibility as an independent expert in the subject at hand. The Internet and other digital fora and media produce a great deal of history that may come into play in legal settings, and the expert in DFE is most likely to have a lot of such information about them readily available on the Internet because that's where much of the work in their field is done. A search of a well known person who has done a career worth of work using the Internet can easily yield hundreds of thousands of pages of material, and not all of it will be factually accurate, but it is all available to be used in challenges to the credibility of the witness.

The challenge of due care is far more daunting in that there are really no well established standards of care associated with information and information technology, despite the common use of the term "best practice". There is a lot of misinformation in the world, and the DFE expert who relies on information from sources that are less than credible may lose their own credibility by believing them without taking the proper precautions in evaluating what they assert. The use of non-authoritative sources, such as online encyclopedias that are created by the Internet community, while useful in everyday applications, may not be up

to the standards required for a legal proceeding, and if they are used as sources without proper verification, they may end up destroying the credibility of both the case and the witness in the process.

A diligent effort in a legal setting typically means relying predominantly on things that the witness has personal knowledge of. For example, in validating a time and date, lacking any other basis for its validity, the DFE expert should do some testing or seek out some independent evidence that supports the claims being made. The "take it on faith" approach is problematic when the issue is important to the case. On the other hand, legal counsel in a case may direct the expert to only attend to certain issues, and in these cases, the expert cannot realistically refuse to do what they are being hired to do. The solution typically comes in being diligent in how information is presented and in how questions are answered. If independent validation was not undertaken, the results should be stated with appropriate caveats, even if that presentation may make it seem "legalistic". It is, after all, a legal matter.

Competence

Professional societies like the IEEE have codes of ethics that are worthy of particular attention to those engaged in working on DFE. In particular, the IEEE code of ethics insists that member agree "... 6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations". In the digital computing arena, as in many other businesses, there is a history of successful individuals exaggerating their backgrounds or qualifications in order to make progress in their careers. But in working on legal issues, this is problematic for all concerned. It is incumbent on anyone working in this field to recognize what they do and do not know and to limit their work and testimony to areas in which they are professionally competent to do the work they are doing. In addition, to the extent that the potential expert is not comfortable with their knowledge of the particular issues in a case, they have a duty to their clients as well as the courts to identify their limitations to counsel. To the extent that the expert can gain additional competence, knowledge, and experience in a specific subfield through diligent effort in a very short time frame, this is certainly something worth doing, but the expert who is not adequately knowledgeable is risking the well being of their client on their ability to learn quickly, and to do so without notice is certainly unethical.

Retention and disposition

There are specific legal duties associated with retention and disposition of DFE and other materials related to digital forensic matters. The pre-legal requirements are largely described above under the "Legal Process" section above in the "Pre-legal" subsection, and the post-legal requirements are discussed briefly in the "Disposition" subsection of that same section. The interested reader should read [9] thoroughly and look for updates as they become available.

Other resources

There are many books that describe digital forensics techniques, particularly in the area of the use of specific tools and the aspects of identification, collection, analysis, and attribution. But there are far fewer books that deal with the issues of interpretation and none on reconstruction.

There are some conferences in the digital forensics area, such as the "IFIP Working Group 11.9 International Conference on Digital Forensics",[6] tracks within other conferences, such as the "Hawaiian International Conference on System Sciences", emerging refereed journals, such as the "Journal on Computer Crime", and some books suitable for use in graduate courses. [1][7][8] However, as a field, digital forensics is still young, and much of the current technical effort largely ignores the legal aspects of the field.

References:

[1] Fred Cohen, “Challenges to Digital Forensic Evidence”, ASP Press, 2008.

[2] Paul H. Suegel, “Recording Codes for Digital Magnetic Storage”, IEEE Transactions Magnetics Mag-21#5, September, 1985.

[3] The U.S. Federal Rules of Evidence.

[4] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 125 L. Ed. 2d 469, 113 S. Ct. 2786 (1993)

[5] Frye v. United States, 293 F 1013 D.C. Cir, 1923

[6] "Advances in Digital Forensics II", 364 pages, Springer; August 30, 2006, ISBN-13: 978-0387368900

[7] T. Johnson, Ed. "Forensic Computer Crime Investigation", Taylor and Francis, 2006

[8] E. Casey, "Digital Evidence and Computer Crime, Second Edition", 688 pages, Academic Press, March 8, 2004, ISBN 0121631048

[9] "The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, A Project of The Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production", September 2004 Public Comment Draft.

[10] "A Guide to Understanding Data Remanence in Automated Information Systems", NCSC-TG-025 - Library No. 5-236,082 - Version-2, available at http://all.net/books/standards/remnants/index.html

[11] Craig Wright, Dave Kleiman, and Shyaam Sundhar R., "Overwriting Hard Drive Data: The Great Wiping Controversy". Information Systems Security, 4th International Conference, ICISS 2008, Hyderabad, India, December 16-20, 2008, Proceedings; Series: Lecture Notes in Computer Science Subseries: Security and Cryptology , Vol. 5352 Sekar, R.; Pujari, Arun K. (Eds.) 2008, XIII, 307 p., Softcover ISBN: 978-3-540-89861-0

[12] James R. Lyle, Douglas R. White, Richard P. Ayers, "Digital Forensics at the National Institute of Standards and Technology", NISTIR 7490

[13] IEEE Design & Test of Computers, issues available starting in 1985 from http://www2.computer.org/portal/web/csdl/magazines/dt#1

[14] Peter Gutmann, "Secure Deletion of Data from Magnetic and Solid-State Memory", Department of Computer Science, University of Auckland, first published in the Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996.
[15] The Constitution of the United States of America, which can be viewed at http://www.archives.gov/exhibits/charters/constitution.html
[16] The IEEE Code of Ethics (IEEE Policy 7.8) is available online at http://www.ieee.org/portal/pages/iportals/aboutus/ethics/code.html